Veiledning for nettverkssikkerhetsfunksjoner

Innholdsfortegnelse

Innføring

Merknadsdefinisjoner

Vi bruker følgende symboler og konvensjoner i denne brukermanualen:

VIKTIG	VIKTIG viser en potensielt farlig situasjon som kan føre til skade på eiendom eller redusert funksjonalitet på produktet hvis den ikke unngås.
MERK	MERK angir driftsmiljøet, forutsetninger for installasjon eller spesielle bruksforutsetninger.
	Tips-ikoner gir nyttige tips og tilleggsinformasjon.
Fet skrift	Fet skrift angir knapper på maskinens kontrollpanel eller på dataskjermen.
Kursiv	Italicized skrift emphasizes et viktig punkt eller refererer til et relatert emne.

Beslektet informasjon

- Innføring

Varemerker

Adobe® og Reader® er enten registrerte varemerker eller varemerker tilhørende Adobe Systems Incorporated i USA og/eller andre land.

Alle selskaper som har programvare nevnt ved navn i denne brukerveiledningen, har en egen programvareLicense for de programmene som de har eiendomsretten til.

Alle vare- og produktnavn for selskaper som vises på Brother-produkter, i relaterte dokumenter og annet materiale, er varemerker eller registrerte varemerker som tilhører disse respektive selskapene.

Beslektet informasjon

- Innføring

Opphavsrett

Beslektet informasjon

- Innføring

Før du bruker nettverkssikkerhetsfunksjoner

Maskinen bruker noen av markedets nyeste protokoller for nettverkssikkerhet og kryptering. Disse nettverksfunksjonene kan integreres i den generelle sikkerhetsplanen for nettverket ditt, slik at du kan beskytte dataene dine og forhindre unauthorized tilgang til maskinen.

Vi anbefaler at du deaktiverer FTP- og TFTP-protokoller. Tilgang til maskinen ved hjelp av disse protokollene er ikke sikker.

Beslektet informasjon

- Innføring
  - Deaktivere unødvendige protokoller

Deaktivere unødvendige protokoller

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. Fjern alle unødvendige avmerkingsbokser for protokollen for å deaktivere dem.
6. Klikk på **Submit (Send inn)**.
7. Start Brother-maskinen på nytt for å aktivere konfigurasjonen.

Beslektet informasjon

- Før du bruker nettverkssikkerhetsfunksjoner

Nettverkssikkerhet

- Konfigurere sertifikater for enhetssikkerhet
- Bruke SSL/TLS
- Bruke SNMPv3
- Bruke IPsec
- Bruke IEEE 802.1x-pålitelighetskontroll for nettverket ditt

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

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 organization 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(Port 443)** 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 unauthorized 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. Bruk SNMPv3-modus for å administrere utskriftsserveren på en sikker måte.
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 IPsec

Introduksjon av IPsec

IPsec (Internet Protocol Security) er en sikkerhetsprotokoll som bruker en valgfri Internett-protokollfunksjon til å forhindre datamanipulering og sikre konfidensialiteten til data som overføres som IP-pakker. IPsec krypterer data sendt over nettverket, som utskriftsdata sendt fra datamaskiner til en skriver. Fordi dataene er kryptert på nettverksnivået, vil programmer som bruker en protokoll av et høyere nivå bruke IPsec selv om brukeren ikke er klar over at den brukes.

IPsec støtter følgende funksjoner:

- IPsec-overføringer

  I henhold til IPsec-innstillingens betingelser sender og mottar den nettverkstilkoblede datamaskinen data til og fra den angitte enheten ved hjelp av IPsec. Når enhetene begynner å kommunisere ved hjelp av IPsec, utveksles nøkler ved hjelp av IKE (Internet Key Exchange) først. Deretter overføres de krypterte dataene ved hjelp av nøklene.

  I tillegg har IPsec to driftsmoduser: transportmodus og tunnelmodus. Transportmodus brukes hovedsakelig for kommunikasjon mellom enheter og Tunnelmodus brukes i miljø som et VPN (Virtual Private Network).

  For IPsec-overføringer er følgende betingelser nødvendige:
  - En datamaskin som kan kommunisere med IPsec er koblet til nettverket.
  - Maskinen er konfigurert for IPsec-kommunikasjon.
  - Datamaskinen som er koblet til maskinen, er konfigurert for IPsec-tilkoblinger.

- IPsec-innstillinger

  Innstillingene som er nødvendige for tilkoblinger med IPsec. Disse innstillingene kan konfigureres med Webbasert administrasjon.

  For å konfigurere IPsec-innstillingene må du bruke nettleseren på en datamaskin som er koblet til nettverket.

Beslektet informasjon

- Bruke IPsec

Konfigurere IPsec via Webbasert administrasjon

Tilkoblingsbetingelsene for IPsec omfatter to **Template (Mal)** typer: **Address (Adresse)** og **IPsec**. Du kan konfigurere opptil 10 tilkoblingsbetingelser.

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)** > **IPsec**.

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

Alternativ	Beskrivelse
Status	Aktiver eller deaktiver IPsec.
Negotiation Mode (Forhandlingsmodus)	Velg **Negotiation Mode (Forhandlingsmodus)** for IKE fase 1. IKE er en protokoll som brukes til å utveksle krypteringsnøkler slik at kryptert kommunikasjon kan gjøres ved hjelp av IPsec. I **Main (Hoved)**-modus er behandlingshastigheten treg, men sikkerheten er høy. I **Aggressive (Aggressiv)**-modus er behandlingshastigheten raskere enn i **Main (Hoved)**-modusen, men sikkerheten er lavere.
All Non-IPsec Traffic (All ikke-IPsec-trafikk)	Velg hvilken handling som skal utføres for ikke-IPsec-pakker. Når du bruker webtjenester, må du velge **Allow (Tillat)** for **All Non-IPsec Traffic (All ikke-IPsec-trafikk)**. Hvis du velger **Drop (Dropp)**, kan ikke webtjenester brukes.
Broadcast/Multicast Bypass (Forbikobling gruppesending/flere gruppesendinger)	Velg **Enabled (Aktivert)** eller **Disabled (Deaktivert)**.
Protocol Bypass (Forbikobling protokoll)	Merk av i avkrysningsboksene for alternativet eller alternativene du vil ha.
Rules (Regler)	Merk av for **Enabled (Aktivert)** for å aktivere malen. Når du velger flere avmerkingsbokser, har avmerkingsboksene med lavere tall prioritering hvis innstillingene for de valgte avmerkingsboksene er i konflikt. Klikk på tilhørende rullegardinliste for å velge **Address Template (Adressemal)** som skal brukes til IPsec-tilkoblingsbetingelsene. For å legge til en **Address Template (Adressemal)** klikker du på **Add Template (Legg til mal)**. Klikk på tilhørende rullegardinliste for å velge **IPsec Template (IPsec-mal)** som skal brukes til IPsec-tilkoblingsbetingelsene. For å legge til en **IPsec Template (IPsec-mal)** klikker du på **Add Template (Legg til mal)**.

6. Klikk på **Submit (Send inn)**.

Hvis maskinen må startes på nytt for å aktivere de nye innstillingene, vises skjermbildet for bekreftelse av omstart.

Hvis det er et tomt element i malen som du aktiverte i **Rules (Regler)**-tabellen, vises en feilmelding. Bekreft valgene dine, og klikk en gang til på **Submit (Send inn)**.

Beslektet informasjon

- Bruke IPsec

Beslektede emner:

- Konfigurere sertifikater for enhetssikkerhet

Konfigurere IPsec-adressemal via Webbasert administrasjon

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)** > **IPsec Address Template (IPsec-adressemal)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Klikk på **Delete (Slett)**-knappen for å slette en **Address Template (Adressemal)**. Når en **Address Template (Adressemal)** er i bruk, kan den ikke slettes.
6. Klikk på den **Address Template (Adressemal)** som du vil opprette. **IPsec Address Template (IPsec-adressemal)** vises.
7. Konfigurer innstillingene.

Alternativ	Beskrivelse
Template Name (Malnavn)	Skriv inn et navn på malen (på opptil 16 tegn).
Local IP Address (Lokal IP-adresse)	• **IP Address (IP-adresse)** Angi IP-adressen. Velg **ALL IPv4 Address (ALLE IPv4-adresse)**, **ALL IPv6 Address (ALLE IPv6-adresse)**, **ALL Link Local IPv6 (ALLE Link Local IPv6)** eller **Custom (Egendefiner)** fra rullegardinmenyen. Hvis du velger **Custom (Egendefiner)** fra rullegardinmenyen, skriv inn IP-adressen (IPv4 eller IPv6) i tekstfeltet. • **IP Address Range (IP-adresseområde)** Skriv inn den første og siste IP-adressen for IP-adresseområdet. Hvis den første og siste IP-adressen ikke er standardized etter IPv4 eller IPv6, eller den siste IP-adressen er mindre enn den første IP-adressen, oppstår det en feil. • **IP Address / Prefix (IP-adresse/-prefiks)** Angi IP-adressen ved hjelp av CIDR-notasjon. For eksempel: 192.168.1.1/24 Siden prefikset er spesifisert i form av en 24-biters nettverksmaske (255.255.255.0) for 192.168.1.1, er adressene 192.168.1### gyldige.
Remote IP Address (Ekstern IP-adresse)	• **Any (Alle)** Når du velger **Any (Alle)**, er alle IP-adresser aktivert. • **IP Address (IP-adresse)** Skriv den spesifiserte IP-adressen (IPv4 eller IPv6) i tekstfeltet. • **IP Address Range (IP-adresseområde)** Skriv inn den første og siste IP-adressen for IP-adresseområdet. Hvis den første og siste IP-adressen ikke er standardized etter

Alternativ	Beskrivelse
	IPv4 eller IPv6, eller den siste IP-adressen er mindre enn den første IP-adressen, oppstår det en feil. • **IP Address / Prefix (IP-adresse/-prefiks)** Angi IP-adressen ved hjelp av CIDR-notasjon. For eksempel: 192.168.1.1/24 Siden prefikset er spesifisert i form av en 24-biters nettverksmaske (255.255.255.0) for 192.168.1.1, er adressene 192.168.1### gyldige.

8. Klikk på **Submit (Send inn)**.

Når du endrer innstillingene for malen som for øyeblikket er i bruk, starter du maskinen på nytt for å aktivere konfigurasjonen.

Beslektet informasjon

- Bruke IPsec

Konfigurere IPsec-mal via Webbasert administrasjon

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)** > **IPsec Template (IPsec-mal)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.
5. Klikk på **Delete (Slett)**-knappen for å slette en **IPsec Template (IPsec-mal)**. Når en **IPsec Template (IPsec-mal)** er i bruk, kan den ikke slettes.
6. Klikk på den **IPsec Template (IPsec-mal)** som du vil opprette. Skjermbildet **IPsec Template (IPsec-mal)** vises. Konfigurasjonsfeltene varierer avhengig av **Use Prefixed Template (Bruk forhåndsinnstilt mal)**- og **Internet Key Exchange (IKE)**-innstillingene du velger.
7. I feltet **Template Name (Malnavn)** skriver du inn et navn for malen (opptil 16 tegn).
8. Hvis du valgte **Custom (Egendefiner)** i **Use Prefixed Template (Bruk forhåndsinnstilt mal)**-rullegardinlisten, velg **Internet Key Exchange (IKE)**-alternativene, og endre deretter innstillingene ved behov.
9. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Bruke IPsec
  - IKEv1-innstillinger for en IPsec-mal
  - IKEv2-innstillinger for en IPsec-mal
  - Manuelle innstillinger for en IPsec-mal

IKEv1-innstillinger for en IPsec-mal

Alternativ	Beskrivelse
Template Name (Malnavn)	Skriv inn et navn på malen (på opptil 16 tegn).
Use Prefixed Template (Bruk forhåndsinnstilt mal)	Velg **Custom (Egendefiner)**, **IKEv1 High Security (IKEv1 Høy sikkerhet)** eller **IKEv1 Medium Security (IKEv1 Medium sikkerhet)**. Innstillingselementene er forskjellig avhengig av den valgte malen.
Internet Key Exchange (IKE)	IKE er en kommunikasjonsprotokoll som brukes til å utveksle krypteringsnøkler slik at kryptert kommunikasjon kan gjøres ved hjelp av IPsec. For å utføre kryptert kommunikasjon for bare den ene gangen bestemmes krypteringsalgoritmen som er nødvendig for IPsec og krypteringsnøklene deles. For IKE, utveksles krypteringsnøklene med Diffie-Hellman-nøkkelutvekslingsmetoden, og kryptert kommunikasjon som er begrenset til IKE utføres. Hvis du valgte **Custom (Egendefiner)** i **Use Prefixed Template (Bruk forhåndsinnstilt mal)**, velg **IKEv1**.
Authentication Type (Pålitelighetskontrolltype)	• **Diffie-Hellman Group** Denne nøkkelutvekslingsmetoden gjør at hemmelige nøkler kan utveksles over et ubeskyttet nettverk på en sikker måte. Diffie-Hellman-nøkkelutvekslingsmetoden bruker et diskret logaritmeproblem, ikke den hemmelige nøkkelen, til å sende og motta åpen informasjon som ble generert med et vilkårlig nummer og den hemmelige nøkkelen. Velg **Group1 (Gruppe1)**, **Group2 (Gruppe2)**, **Group5 (Gruppe5)** eller **Group14 (Gruppe14)**. • **Encryption (Kryptering)** Velg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Velg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SA-levetid)** Angi IKE SA-levetiden. Skriv inn tiden (i sekunder) og antall kilobyte (kB).
Encapsulating Security (Sikkerhetsinnkapsling)	• **Protocol (Protokoll)** Velg **ESP**, **AH** eller **AH+ESP**. - ESP er en protokoll for kryptert kommunikasjon med IPsec. ESP krypterer nyttelasten (det kommuniserte innholdet) og legger til tilleggsinformasjon. IP-pakken består av topptekst og det krypterte innholdet, som følger topptekst. I tillegg til krypterte data inneholder IP-pakken også informasjon om krypteringsmetoden og krypteringsnøkkelen, pålitelighetskontrolldata osv. - AH er en del av IPsec-protokollen som godkjenner senderen og forhindrer endring (sikrer at dataen er fullstendig). Dataen settes inn rett etter topptekst i IP-pakken. I tillegg inneholder pakkene nummerverdier, som er kalkulert med en ligning fra det kommuniserte innholdet, den hemmelige nøkkelen, osv., for å forhindre forfalskning av senderen og endring av dataene. Til forskjell fra ESP, krypteres ikke det kommuniserte innholdet, og dataen sendes og mottas som vanlig tekst. • **Encryption (Kryptering) (Ikke tilgjengelig for AH-alternativet.)** Velg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**.

Alternativ	Beskrivelse
	• **Hash** Velg **None (Ingen)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Ingen)** kan kun velges når **ESP** er valgt for **Protocol (Protokoll)**. • **SA Lifetime (SA-levetid)** Spesifiser IKE SA-levetiden. Skriv inn tiden (i sekunder) og antall kilobyte (KByte). • **Encapsulation Mode (Innkapslingsmodus)** Velg **Transport** eller **Tunnel**. • **Remote Router IP-Address (IP-adresse for ekstern ruter)** Skriv inn IP-adressen (IPv4 eller IPv6) til den eksterne ruteren. Skriv bare inn denne informasjonen når **Tunnel**-modusen er valgt. SA (Security Association) er en kryptert kommunikasjonsmetode som bruker IPsec eller IPv6 som utveksler og deler informasjon, som krypteringsmetoden og krypteringsnøkkelen, for å kunne etablere en sikker kommunikasjonskanal før kommunikasjonen starter. SA kan også henvise til en virtuell kryptert kommunikasjonskanal som har blitt etablert. SA som brukes for IPsec etablerer krypteringsmetoden, utveksler nøklene og utfører felles pålitelighetskontroll i henhold til IKE-standardprosedyren (Internet Key Exchange). SA oppdateres også periodisk.
Perfect Forward Secrecy (PFS)	PFS henter ikke ut nøkler fra tidligere nøkler som ble brukt til å kryptere meldinger. Hvis en nøkkel brukt til å kryptere en melding ble utledet fra en overordnet nøkkel, vil den overordnede nøkkelen ikke brukes til å utlede andre nøkler. Selv om en nøkkel lekkes, er skaden derfor begrenset til meldingene som ble kryptert med den nøkkelen. Velg **Enabled (Aktivert)** eller **Disabled (Deaktivert)**.
Authentication Method (Pålitelighetskontrollmetode)	Velg pålitelighetskontrollmetoden. Velg **Pre-Shared Key (Forhåndsdelt nøkkel)** eller **Certificates (Sertifikater)**.
Pre-Shared Key (Forhåndsdelt nøkkel)	Prinsippet for kryptert kommunikasjon er at krypteringsnøkkelen utveksles og deles på forhånd ved hjelp av en annen kanal. Hvis du valgte **Pre-Shared Key (Forhåndsdelt nøkkel)** for **Authentication Method (Pålitelighetskontrollmetode)**, skriv inn **Pre-Shared Key (Forhåndsdelt nøkkel)** (opptil 32 tegn). • **Local/ID Type/ID (Lokal/ID-type/ID)** Velg senderens ID-type, og skriv deretter inn ID-en. Velg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-postadresse)** eller **Certificate (Sertifikat)** som typen. Hvis du velger **Certificate (Sertifikat)**, skriver du inn fellesnavnet til sertifikatet i **ID**-feltet. • **Remote/ID Type/ID (Ekstern/ID-type/ID)** Velg mottakerens ID-type, og skriv deretter inn ID-en. Velg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-postadresse)** eller **Certificate (Sertifikat)** som typen. Hvis du velger **Certificate (Sertifikat)**, skriver du inn fellesnavnet til sertifikatet i **ID**-feltet.
Certificate (Sertifikat)	Hvis du valgte **Certificates (Sertifikater)** for **Authentication Method (Pålitelighetskontrollmetode)**, velger du sertifikatet. Du kan velge kun sertifikatene som ble opprettet ved hjelp av **Certificate (Sertifikat)**-siden på konfigurasjonsskjermbildet i Webbasert administrasjon.

Beslektet informasjon

- Konfigurere IPsec-mal via Webbasert administrasjon

IKEv2-innstillinger for en IPsec-mal

Alternativ	Beskrivelse
Template Name (Malnavn)	Skriv inn et navn på malen (på opptil 16 tegn).
Use Prefixed Template (Bruk forhåndsinnstilt mal)	Velg **Custom (Egendefiner)**, **IKEv2 High Security (IKEv2 Høy sikkerhet)** eller **IKEv2 Medium Security (IKEv2 Medium sikkerhet)**. Innstillingselementene er forskjellig avhengig av den valgte malen.
Internet Key Exchange (IKE)	IKE er en kommunikasjonsprotokoll som brukes til å utveksle krypteringsnøkler slik at kryptert kommunikasjon kan gjøres ved hjelp av IPsec. For å utføre kryptert kommunikasjon for bare den ene gangen bestemmes krypteringsalgoritmen som er nødvendig for IPsec og krypteringsnøklene deles. For IKE, utveksles krypteringsnøklene med Diffie-Hellman-nøkkelutvekslingsmetoden, og kryptert kommunikasjon som er begrenset til IKE utføres. Hvis du valgte **Custom (Egendefiner)** i **Use Prefixed Template (Bruk forhåndsinnstilt mal)**, velg **IKEv2**.
Authentication Type (Pålitelighetskontrolltype)	• **Diffie-Hellman Group** Denne nøkkelutvekslingsmetoden gjør at hemmelige nøkler kan utveksles over et ubeskyttet nettverk på en sikker måte. Diffie-Hellman-nøkkelutvekslingsmetoden bruker et diskret logaritmeproblem, ikke den hemmelige nøkkelen, til å sende og motta åpen informasjon som ble generert med et vilkårlig nummer og den hemmelige nøkkelen. Velg **Group1 (Gruppe1)**, **Group2 (Gruppe2)**, **Group5 (Gruppe5)** eller **Group14 (Gruppe14)**. • **Encryption (Kryptering)** Velg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Velg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SA-levetid)** Angi IKE SA-levetiden. Skriv inn tiden (i sekunder) og antall kilobyte (kB).
Encapsulating Security (Sikkerhetsinnkapsling)	• **Protocol (Protokoll)** Velg **ESP**. ESP er en protokoll for kryptert kommunikasjon med IPsec. ESP krypterer nyttelasten (det kommuniserte innholdet) og legger til tilleggsinformasjon. IP-pakken består av toppteksten og det krypterte innholdet, som følger toppteksten. I tillegg til krypterte data inneholder IP-pakken også informasjon om krypteringsmetoden og krypteringsnøkkelen, pålitelighetskontrolldata osv. • **Encryption (Kryptering)** Velg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Velg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SA-levetid)** Spesifiser IKE SA-levetiden. Skriv inn tiden (i sekunder) og antall kilobyte (KByte). • **Encapsulation Mode (Innkapslingsmodus)** Velg **Transport** eller **Tunnel**.

Alternativ	Beskrivelse
	• **Remote Router IP-Address (IP-adresse for ekstern ruter)** Skriv inn IP-adressen (IPv4 eller IPv6) til den eksterne ruteren. Skriv bare inn denne informasjonen når **Tunnel**-modusen er valgt.  SA (Security Association) er en kryptert kommunikasjonsmetode som bruker IPsec eller IPv6 som utveksler og deler informasjon, som krypteringsmetoden og krypteringsnøkkelen, for å kunne etablere en sikker kommunikasjonskanal før kommunikasjonen starter. SA kan også henvise til en virtuell kryptert kommunikasjonskanal som har blitt etablert. SA som brukes for IPsec etablerer krypteringsmetoden, utveksler nøklene og utfører felles pålitelighetskontroll i henhold til IKE-standardprosedyren (Internet Key Exchange). SA oppdateres også periodisk.
Perfect Forward Secrecy (PFS)	PFS henter ikke ut nøkler fra tidligere nøkler som ble brukt til å kryptere meldinger. Hvis en nøkkel brukt til å kryptere en melding ble utledet fra en overordnet nøkkel, vil den overordnede nøkkelen ikke brukes til å utlede andre nøkler. Selv om en nøkkel lekkes, er skaden derfor begrenset til meldingene som ble kryptert med den nøkkelen. Velg **Enabled (Aktivert)** eller **Disabled (Deaktivert)**.
Authentication Method (Pålitelighetskontrollmetode)	Velg pålitelighetskontrollmetoden. Velg **Pre-Shared Key (Forhåndsdelt nøkkel)**, **Certificates (Sertifikater)**, **EAP - MD5** eller **EAP - MS-CHAPv2**.  EAP er en autentiseringsprotokoll som er en utvidelse av PPP. Ved å bruke EAP med IEEE802.1x, brukes en annen nøkkel for brukerpålitelighetskontroll under hver økt. Følgende innstillinger er bare nødvendige når **EAP - MD5** eller **EAP - MS-CHAPv2** er valgt i **Authentication Method (Pålitelighetskontrollmetode)**: • **Mode (Modus)** Velg **Server-Mode (Servermodus)** eller **Client-Mode (Klientmodus)**. • **Certificate (Sertifikat)** Velg sertifikatet. • **User Name (Brukernavn)** Skriv inn brukernavnet (opptil 32 tegn). • **Password (Passord)** Skriv inn passordet (opptil 32 tegn). Passordet må angis to ganger for bekreftelse.
Pre-Shared Key (Forhåndsdelt nøkkel)	Prinsippet for kryptert kommunikasjon er at krypteringsnøkkelen utveksles og deles på forhånd ved hjelp av en annen kanal. Hvis du valgte **Pre-Shared Key (Forhåndsdelt nøkkel)** for **Authentication Method (Pålitelighetskontrollmetode)**, skriv inn **Pre-Shared Key (Forhåndsdelt nøkkel)** (opptil 32 tegn). • **Local/ID Type/ID (Lokal/ID-type/ID)** Velg senderens ID-type, og skriv deretter inn ID-en. Velg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-postadresse)** eller **Certificate (Sertifikat)** som typen. Hvis du velger **Certificate (Sertifikat)**, skriver du inn fellesnavnet til sertifikatet i **ID**-feltet. • **Remote/ID Type/ID (Ekstern/ID-type/ID)** Velg mottakerens ID-type, og skriv deretter inn ID-en.

Alternativ	Beskrivelse
	Velg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-postadresse)** eller **Certificate (Sertifikat)** som typen. Hvis du velger **Certificate (Sertifikat)**, skriver du inn fellesnavnet til sertifikatet i **ID**-feltet.
Certificate (Sertifikat)	Hvis du valgte **Certificates (Sertifikater)** for **Authentication Method (Pålitelighetskontrollmetode)**, velger du sertifikatet. Du kan velge kun sertifikatene som ble opprettet ved hjelp av **Certificate (Sertifikat)**-siden på konfigurasjonsskjermbildet i Webbasert administrasjon.

Beslektet informasjon

- Konfigurere IPsec-mal via Webbasert administrasjon

Manuelle innstillinger for en IPsec-mal

Alternativ	Beskrivelse
Template Name (Malnavn)	Skriv inn et navn på malen (på opptil 16 tegn).
Use Prefixed Template (Bruk forhåndsinnstilt mal)	Velg **Custom (Egendefiner)**.
Internet Key Exchange (IKE)	IKE er en kommunikasjonsprotokoll som brukes til å utveksle krypteringsnøkler slik at kryptert kommunikasjon kan gjøres ved hjelp av IPsec. For å utføre kryptert kommunikasjon for bare den ene gangen bestemmes krypteringsalgoritmen som er nødvendig for IPsec og krypteringsnøklene deles. For IKE, utveksles krypteringsnøklene med Diffie-Hellman-nøkkelutvekslingsmetoden, og kryptert kommunikasjon som er begrenset til IKE utføres. Velg **Manual (Manuell)**.
Authentication Key (ESP, AH) (Pålitelighetskontrollnøkkel (ESP, AH))	Skriv inn **In/Out (In/ut)**-verdiene. Disse innstillingene er nødvendige når **Custom (Egendefiner)** er valgt for **Use Prefixed Template (Bruk forhåndsinnstilt mal)**, **Manual (Manuell)** er valgt for **Internet Key Exchange (IKE)** og en annen innstilling enn **None (Ingen)** er valgt for **Hash** for **Encapsulating Security (Sikkerhetsinnkapsling)**-delen. Antall tegn du kan angi varierer avhengig av innstillingen du valgte i **Hash** i **Encapsulating Security (Sikkerhetsinnkapsling)**-delen. Hvis lengden på den angitte autentiseringsnøkkelen er forskjellig fra den valgte hashalgoritmen, vil det oppstå en feil. • **MD5**: 128 biter (16 byte) • **SHA1**: 160 biter (20 byte) • **SHA256**: 256 biter (32 byte) • **SHA384**: 384 biter (48 byte) • **SHA512**: 512 biter (64 byte) Når du angir nøkkelen i ASCII-koder, avgrenser du tegnene med anførselstegn (").
Code key (ESP) (Kodenøkkel (ESP))	Skriv inn **In/Out (In/ut)**-verdiene. Disse innstillingene er nødvendige når **Custom (Egendefiner)** er valgt for **Use Prefixed Template (Bruk forhåndsinnstilt mal)**, **Manual (Manuell)** er valgt for **Internet Key Exchange (IKE)** og **ESP** er valgt for **Protocol (Protokoll)** i **Encapsulating Security (Sikkerhetsinnkapsling)**. Antall tegn du kan angi varierer avhengig av innstillingen du valgte i **Encryption (Kryptering)** i **Encapsulating Security (Sikkerhetsinnkapsling)**-delen. Hvis lengden til den angitte kodenøkkelen er forskjellig fra den valgte krypteringsalgoritmen, vil det oppstå en feil. • **DES**: 64 biter (8 byte) • **3DES**: 192 biter (24 byte) • **AES-CBC 128**: 128 biter (16 byte) • **AES-CBC 256**: 256 biter (32 byte) Når du angir nøkkelen i ASCII-koder, avgrenser du tegnene med anførselstegn (").
SPI	Disse parametrene brukes for å identifisere sikkerhetsinformasjon. Vanligvis har en vert flere SA-er (Security Associations) for flere typer

Alternativ	Beskrivelse
	IPsec-kommunikasjon. Derfor er det nødvendig å identifisere gjeldende SA når en IPsec-pakke er mottatt. SPI-parameteren, som identifiserer SA, er inkludert i toppteksten AH (Authentication Header) og ESP (Encapsulating Security Payload). Disse innstillingene er nødvendige når **Custom (Egendefiner)** er valgt for **Use Prefixed Template (Bruk forhåndsinnstilt mal)**, og **Manual (Manuell)** er valgt for **Internet Key Exchange (IKE)**. Angi **In/Out (In/ut)**-verdiene. (3-10 tegn)
Encapsulating Security (Sikkerhetsinnkapsling)	• **Protocol (Protokoll)** Velg **ESP** eller **AH**. - ESP er en protokoll for kryptert kommunikasjon med IPsec. ESP krypterer nyttelasten (det kommuniserte innholdet) og legger til tilleggsinformasjon. IP-pakken består av toppteksten og det krypterte innholdet, som følger toppteksten. I tillegg til krypterte data inneholder IP-pakken også informasjon om krypteringsmetoden og krypteringsnøkkelen, pålitelighetskontrolldata osv. - AH er en del av IPsec-protokollen som godkjenner senderen og forhindrer endring av dataen (sikrer at dataen er fullstendig). Dataen settes inn rett etter toppteksten i IP-pakken. I tillegg inneholder pakkene nummerverdier, som er kalkulert med en ligning fra det kommuniserte innholdet, den hemmelige nøkkelen, osv., for å forhindre forfalskning av senderen og endring av dataene. Til forskjell fra ESP, krypteres ikke det kommuniserte innholdet, og dataen sendes og mottas som vanlig tekst. • **Encryption (Kryptering) (Ikke tilgjengelig for AH-alternativet.)** Velg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Velg **None (Ingen)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Ingen)** kan kun velges når **ESP** er valgt for **Protocol (Protokoll)**. • **SA Lifetime (SA-levetid)** Spesifiser IKE SA-levetiden. Skriv inn tiden (i sekunder) og antall kilobyte (KByte). • **Encapsulation Mode (Innkapslingsmodus)** Velg **Transport** eller **Tunnel**. • **Remote Router IP-Address (IP-adresse for ekstern ruter)** Skriv inn IP-adressen (IPv4 eller IPv6) til den eksterne ruteren. Skriv bare inn denne informasjonen når **Tunnel**-modusen er valgt. SA (Security Association) er en kryptert kommunikasjonsmetode som bruker IPsec eller IPv6 som utveksler og deler informasjon, som krypteringsmetoden og krypteringsnøkkelen, for å kunne etablere en sikker kommunikasjonskanal før kommunikasjonen starter. SA kan også henvise til en virtuell kryptert kommunikasjonskanal som har blitt etablert. SA som brukes for IPsec etablerer krypteringsmetoden, utveksler nøklene og utfører felles pålitelighetskontroll i henhold til IKE-standardprosedyren (Internet Key Exchange). SA oppdateres også periodisk.

Beslektet informasjon

- Konfigurere IPsec-mal via Webbasert administrasjon

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 unauthorized 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 (Kontroll av serversertifikat)**-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 (Kontroll av serversertifikat)**-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 tunneledpålitelighetsprosess.

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

Brukerautentisering

- Bruke Active Directory-pålitelighetskontroll
- Bruke LDAP-pålitelighetskontroll
- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Bruke Active Directory-pålitelighetskontroll

Introduksjon av Active Directory-pålitelighetskontroll

Active Directory-pålitelighetskontroll begrenser bruken av maskinen. Hvis Active Directory-pålitelighetskontroll er aktivert, vil maskinens kontrollpanel være låst. Du kan ikke endre maskinens innstillinger før du angir en bruker-ID og et passord.

Active Directory-pålitelighetskontroll tilbyr følgende funksjoner:

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

- lagring av innkommende utskriftsdata
- lagring av innkommende faksdata
- henting av e-postadressen fra Active Directory-serveren basert på din bruker-ID, ved sending av skannede data til en e-postserver

  Hvis du vil bruke denne funksjonen, velger du alternativet **On (På)** for innstillingen **Get Mail Address (Få e-postadresse)** og pålitelighetskontrollmetoden **LDAP + kerberos** eller **LDAP + NTLMv2**. E-postadressen din angis som senderen når maskinen sender skannede data til en e-postserver, eller som mottakeren hvis du vil sende skannede data til e-postadressen din.

Når Active Directory-pålitelighetskontroll er aktivert, lagrer maskinen all innkommende faksdata. Maskinen skriver ut lagret faksdata etter at du logger på.

Du kan endre innstillingene for Active Directory-pålitelighetskontroll ved hjelp av Webbasert administrasjon.

Beslektet informasjon

- Bruke Active Directory-pålitelighetskontroll

Konfigurere Active Directory-godkjenning via Webbasert administrasjon

Active Directory-pålitelighetskontrollen støtter Kerberos-pålitelighetskontroll og NTLMv2-pålitelighetskontroll. Du må konfigurere SNTP-protokollen (tidsserver for nettverk) og DNS-serverkonfigurasjon for pålitelighetskontroll.

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 **Administrator** > **User Restriction Function (Brukerrestriksjonsfunksjon)** eller **Restriction Management (Begrensingsadministrasjon)**.

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

5. Velg **Active Directory Authentication (Active Directory-godkjenning)**.
6. Klikk på **Submit (Send inn)**.
7. Klikk på **Active Directory Authentication (Active Directory-godkjenning)**.
8. Konfigurerer følgende innstillinger:

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

Alternativ	Beskrivelse
Storage Fax RX Data (Lagring av data for mottatt faks)	Velg dette alternativet for å lagre innkommende faksdata. Du kan skrive ut all innkommende faksdata etter at du logger på maskinen.
Remember User ID (Husk bruker-ID)	Velg dette alternativet for å lagre bruker-ID.
Active Directory Server Address (Active Directory-serveradresse)	Skriv inn IP-adressen eller servernavnet (for eksempel, ad.eksempel.no) til Active Directory-serveren.
Active Directory Domain Name (Active Directory-domenenavn)	Skriv inn domenenavnet for Active Directory.
Protocol & Authentication Method (Protokoll og godkjenningsmetode)	Velg protokoll- og pålitelighetskontrollmetode.
SSL/TLS	Velg **SSL/TLS**-alternativet.

Alternativ	Beskrivelse
LDAP Server Port (LDAP-serverport)	Skriv inn portnummeret for å koble til Active Directory-serveren via LDAP (kun tilgjengelig for pålitelighetskontrollmetoden **LDAP + kerberos** eller **LDAP + NTLMv2**).
LDAP Search Root (LDAP-søkerot)	Skriv inn LDAP-søkeroten (kun tilgjengelig for pålitelighetskontrollmetoden **LDAP + kerberos** eller **LDAP + NTLMv2**).
Get Mail Address (Få e-postadresse)	Velg dette alternativet for å hente den påloggede brukerens e-postadresse fra Active Directory-serveren. (kun tilgjengelig for pålitelighetskontrollmetoden **LDAP + kerberos** eller **LDAP + NTLMv2**)
Get User's Home Directory (Få brukers startmappe)	Velg dette alternativet for å hente hjemmekatalogen som Skann til nettverk-destinasjonen. (kun tilgjengelig for pålitelighetskontrollmetoden **LDAP + kerberos** eller **LDAP + NTLMv2**)

9. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Bruke Active Directory-pålitelighetskontroll

Logge på for å endre maskininnstillingene med maskinens kontrollpanel (Active Directory-godkjenning)

Når Active Directory-godkjenning er aktivert, vil maskinens kontrollpanel være låst inntil du skriver inn bruker-ID og passord på maskinens kontrollpanel.

1. På maskinens kontrollpanel skriver du inn bruker-ID-en og passordet for å logge på.
2. Når pålitelighetskontrollen er vellykket, låses maskinens kontrollpanel opp.

Beslektet informasjon

- Bruke Active Directory-pålitelighetskontroll

Bruke LDAP-pålitelighetskontroll

- Introduksjon til LDAP-pålitelighetskontroll
- Konfigurere LDAP-godkjenning via Webbasert administrasjon
- Logg på for å endre maskininnstillingene med maskinens kontrollpanel (LDAP-godkjenning)

Introduksjon til LDAP-pålitelighetskontroll

LDAP-pålitelighetskontroll begrenser bruken av maskinen. Hvis LDAP-pålitelighetskontroll er aktivert, vil maskinens kontrollpanel være låst. Du kan ikke endre maskinens innstillinger før du angir en bruker-ID og et passord.

LDAP-pålitelighetskontroll tilbyr følgende funksjoner:

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

- lagring av innkommende utskriftsdata
- lagring av innkommende faksdata
- henting av e-postadressen fra LDAP-serveren basert på din bruker-ID, ved sending av skannede data til en e-postserver

  Hvis du vil bruke denne funksjonen, velger du alternativet **On (På)** for innstillingen **Get Mail Address (Få e-postadresse)**. E-postadressen din angis som senderen når maskinen sender skannede data til en e-postserver, eller som mottakeren hvis du vil sende skannede data til e-postadressen din.

Når LDAP-pålitelighetskontroll er aktivert, lagrer maskinen all innkommende faksdata. Maskinen skriver ut lagret faksdata etter at du logger på.

Du kan endre innstillingene for LDAP-pålitelighetskontroll ved hjelp av Webbasert administrasjon.

Beslektet informasjon

- Bruke LDAP-pålitelighetskontroll

Konfigurere LDAP-godkjenning via Webbasert administrasjon

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 **Administrator** > **User Restriction Function (Brukerrestriksjonsfunksjon)** eller **Restriction Management (Begrensingsadministrasjon)**.

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

5. Velg **LDAP Authentication (LDAP-pålitelighetskontroll)**.
6. Klikk på **Submit (Send inn)**.
7. Klikk på **LDAP Authentication (LDAP-pålitelighetskontroll)**-menyen.
8. Konfigurerer følgende innstillinger:

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

Alternativ	Beskrivelse
Storage Fax RX Data (Lagring av data for mottatt faks)	Velg dette alternativet for å lagre innkommende faksdata. Du kan skrive ut all innkommende faksdata etter at du logger på maskinen.
Remember User ID (Husk bruker-ID)	Velg dette alternativet for å lagre bruker-ID.
LDAP Server Address (LDAP-serveradresse)	Skriv inn IP-adressen eller servernavnet (eksempel: ldap.eksempel.com) til LDAP-serveren.
SSL/TLS	Velg alternativet **SSL/TLS** for å bruke LDAP fremfor SSL/TLS.
LDAP Server Port (LDAP-serverport)	Skriv inn LDAP-serverens portnummer.
LDAP Search Root (LDAP-søkerot)	Skriv inn LDAP-søkerotkatalogen.
Attribute of Name (Search Key) (Navnets attributt (Søkenøkkel))	Skriv inn attributtet du vil bruke som søkenøkkel.
Get Mail Address (Få e-postadresse)	Velg dette alternativet for å hente den påloggede brukerens e-postadresse fra LDAP-serveren.
Get User's Home Directory (Få brukers startmappe)	Velg dette alternativet for å hente hjemmekatalogen som Skann til nettverk-destinasjonen.

9. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Bruke LDAP-pålitelighetskontroll

Logg på for å endre maskininnstillingene med maskinens kontrollpanel (LDAP-godkjenning)

Når LDAP-godkjenning er aktivert, vil maskinens kontrollpanel være låst inntil du skriver inn bruker-ID og passord på maskinens kontrollpanel.

1. På maskinens kontrollpanel skriver du inn bruker-ID-en og passordet for å logge på.
2. Når pålitelighetskontrollen er vellykket, låses maskinens kontrollpanel opp.

Beslektet informasjon

- Bruke LDAP-pålitelighetskontroll

Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Secure Function Lock 3.0 øker sikkerheten ved å begrense hvilke funksjoner som er tilgjengelige på maskinen.

Før du bruker Secure Function Lock 3.0

Bruk Secure Function Lock (Sikkerfunksjonslås) til å konfigurere passord, angi begrensninger for bestemte brukersider og gi tilgang til noen av eller alle funksjonene som står oppført her.

Du kan konfigurere og endre følgende innstillinger for Secure Function Lock 3.0 via Webbasert administrasjon:

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

- **Print (Skriv ut)**
- **Copy (Kopier)**
- **Scan (Skann)**
- **Faks**
- **Medier**
- **Web Connect**
- **Apps (Appar)**
- **Page Limits (Sidebegrensninger)**
- **Page Counters (Sideteller)**
- **Card ID (NFC ID) (Kort ID (NFC ID))**

Modeller med LCD-pekeskjerm:

Når Secure Function Lock (Sikkerfunksjonslås) er aktivert, går maskinen automatisk over i fellesmodus, og noen av maskinens funksjoner blir begrenset til kun authorized brukere. Hvis du vil ha tilgang til begrensede maskinfunksjoner, må du trykke på , velge brukernavnet ditt og skrive inn passordet.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Konfigurere Secure Function Lock 3.0 via Webbasert administrasjon

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 **Administrator** > **User Restriction Function (Brukerrestriksjonsfunksjon)** eller **Restriction Management (Begrensingsadministrasjon)**.

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

5. Velg **Secure Function Lock**.
6. Klikk på **Submit (Send inn)**.
7. Klikk på **Restricted Functions (Begrensede funksjoner)**-menyen.
8. Konfigurer innstillingene for å behandle begrensninger per bruker eller per gruppe.
9. Klikk på **Submit (Send inn)**.
10. Klikk på **User List (Brukerliste)**-menyen.
11. Konfigurer brukerlisten.
12. Klikk på **Submit (Send inn)**.

Du kan også endre låseinnstillingene for brukerlisten i **Secure Function Lock**-menyen.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Skanne ved hjelp av Secure Function Lock 3.0

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

Angi begrensninger for skanning (for administratorer)

Med Secure Function Lock 3.0 kan administrator begrense hvilke brukere som har lov til å skanne. Når skannefunksjonen er deaktivert i innstillingen for fellesbrukere, kan skanning bare utføres av brukere der det er merket av for **Scan (Skann)**.

Bruke skannefunksjonen (for begrensede brukere)

- Skanne med maskinens kontrollpanel:

  Begrensede brukere må angi passordet på maskinens kontrollpanel for å få tilgang til skannemodus.
- Skanne fra en datamaskin:

  Begrensede brukere må angi passordet på maskinens kontrollpanel før de kan skanne fra datamaskinen. Hvis passordet ikke angis på maskinens kontrollpanel, vises det en feilmelding på brukerens datamaskin.

Hvis maskinen støtter godkjenning av IC-kort, kan begrensede brukere også få tilgang til skannemodus ved å berøre NFC-symbolet på maskinens kontrollpanel med sitt registrerte IC-kort.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Konfigurere fellesmodus for Secure Function Lock 3.0

Bruk Secure Function Lock-skjermbildet til å konfigurere fellesmodus, som begrenser hvilke funksjoner som er tilgjengelige for fellesbrukere. Fellesbrukere trenger ikke angi et passord for å få tilgang til funksjonene som er gjort tilgjengelige via Offentlig modus-innstillinger.

Offentlig modus inkluderer utskriftsjobber som er sendt via Brother iPrint&Scan og Brother Mobile Connect.

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 **Administrator** > **User Restriction Function (Brukerrestriksjonsfunksjon)** eller **Restriction Management (Begrensingsadministrasjon)**.

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

5. Velg **Secure Function Lock**.
6. Klikk på **Submit (Send inn)**.
7. Klikk på **Restricted Functions (Begrensede funksjoner)**-menyen.
8. På raden **Public Mode (Fellesmodus)** merker du av i avkrysningsboksene for å tillate, eller fjerner merket i avkrysningsboksene for å tillate eller begrense den oppgitte funksjonen.
9. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Konfigurere personlige startskjerminnstillinger ved hjelp av Webbasert administrasjon

Som administrator kan du spesifisere hvilke faner brukerne kan se på sine personlige startskjermbilder. Disse fanene gir brukerne rask tilgang til favoritesnarveiene sine, som kan de kan tilordne til fanene på deres personlige startskjermbilder via maskinens kontrollpanel.

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

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 **Administrator** > **User Restriction Function (Brukerrestriksjonsfunksjon)** eller **Restriction Management (Begrensingsadministrasjon)**.

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

5. Velg **Secure Function Lock**.
6. I **Tab Settings (Faneinnstillinger)**-feltet velger du **Personal (Personlig)** for fanenavnene du vil bruke som ditt personlige startskjermbilde.
7. Klikk på **Submit (Send inn)**.
8. Klikk på **Restricted Functions (Begrensede funksjoner)**-menyen.
9. Konfigurer innstillingene for å behandle begrensningene per bruker eller gruppe.
10. Klikk på **Submit (Send inn)**.
11. Klikk på **User List (Brukerliste)**-menyen.
12. Konfigurer brukerlisten.
13. Velg **User List / Restricted Functions (Brukerliste / Begrensede funksjoner)** fra rullegardinmenyen for hver bruker.
14. Velg fanenavnet fra **Home Screen (Startside)**-rullegardinlisten for hver bruker.
15. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Flere funksjoner for Secure Function Lock 3.0

Konfigurer følgende funksjoner på skjermbildet Secure Function Lock:

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

All Counter Reset (Tilbakestill alle tellere)

Klikk på **All Counter Reset (Tilbakestill alle tellere)** i kolonnen **Page Counters (Sideteller)** for å nullstille sidetelleren.

Export to CSV file (Eksporter til CSV-fil)

Klikk på **Export to CSV file (Eksporter til CSV-fil)** for å eksportere gjeldende og siste sideteller inkludert **User List / Restricted Functions (Brukerliste / Begrensede funksjoner)**-informasjon som en CSV-fil.

Card ID (NFC ID) (Kort ID (NFC ID))

Klikk på **User List (Brukerliste)**-menyen, og skriv deretter inn en brukers kort-ID i **Card ID (NFC ID) (Kort ID (NFC ID))**-feltet. Du kan bruke IC-kortet ditt til pålitelighetskontroll.

Output (Utgang)

Når postboksenheten er installert på maskinen, velg utgangsmagasinet for hver bruker fra rullegardinlisten.

Last Counter Record (Siste tellerregistrering)

Klikk på **Last Counter Record (Siste tellerregistrering)** hvis du vil at maskinen skal beholde sideantallet etter at telleren er nullstilt.

Counter Auto Reset (Nullstill teller automatisk)

Klikk på **Counter Auto Reset (Nullstill teller automatisk)** hvis du vil konfigurere tidsintervallet for hvor ofte sidetelleren skal nullstilles. Velg et daglig, ukentlig eller månedlig intervall.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Registrere et nytt IC-kort med maskinens kontrollpanel

Du kan registrere Integrated Circuit Cards (IC-kort) på maskinen.

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

1. Berør NFC-ikonet (nærfeltkommunikasjon) på maskinens kontrollpanel med et registrert IC-kort (Integrated Circuit).
2. Trykk bruker-ID-en din mot LCD-skjermen.
3. Trykk på Register Card-knappen (Registrer kort).
4. Berør NFC-symbolet med et nytt IC-kort.

   Det nye IC-kortets nummer registreres deretter på maskinen.
5. Trykk på OK-knappen.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Registrere en ekstern IC-kortleser

Når du kobler til en ekstern IC-kortleser (Integrated Circuit), bruker du webbasert administrasjon for å registrere kortleseren. Maskinen din støtter IC-kortlesere som støtter drivere av HID-klasse.

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 **Administrator** > **External Card Reader (Ekstern kortleser)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Skriv inn nødvendig informasjon, og klikk deretter på **Submit (Send inn)**.
6. Start Brother-maskinen på nytt for å aktivere konfigurasjonen.
7. Koble kortleseren til maskinen.
8. Hold kortet inntil kortleseren når du bruker kortet til pålitelighetskontroll.

Beslektet informasjon

- Bruke Secure Function Lock (Sikkerfunksjonslås) 3.0

Sende eller motta e-post på en sikker måte

- Konfigurere sending eller mottak av e-post via Webbasert administrasjon
- Sende e-post med brukerautentisering
- Sende eller motta e-post på en sikker måte med SSL/TLS

Konfigurere sending eller mottak av e-post via Webbasert administrasjon

- Mottak av e-post er kun tilgjengelig på visse modeller.
- Vi anbefaler at du bruker Webbasert administrasjon til å konfigurere sikker sending av e-post med brukerautentisering eller sending og mottak av e-post med SSL/TLS.

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. I feltet **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)** klikker du på **Advanced Settings (Avanserte innstillinger)** og kontrollerer at statusen til **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)** er **Enabled (Aktivert)**.

   - Tilgjengelige protokoller kan variere, avhengig av maskinen din.
   - Hvis skjermbildet for valg av **Authentication Method (Pålitelighetskontrollmetode)** vises, velg pålitelighetskontrollmetode og følg deretter skjerminstruksjonene.
6. Konfigurer innstillingene for **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**.
   - Bekreft at e-postinnstillingene er riktige etter konfigurasjonen ved å sende en testmelding.
   - Hvis du ikke vet innstillingene for POP3-/SMTP-/IMAP4-serveren, tar du kontakt med nettverksadministrator eller Internett-leverandøren.
7. Når du er ferdig, klikker du på **Submit (Send inn)**.

   Dialogboksen **Test Send/Receive E-mail Configuration (Test Send/motta e-postkonfigurasjon)** vises.
8. Følg instruksjonene i dialogboksen hvis du vil teste gjeldende innstillinger.

Beslektet informasjon

- Sende eller motta e-post på en sikker måte

Beslektede emner:

- Sende eller motta e-post på en sikker måte med SSL/TLS

Sende e-post med brukerautentisering

Maskinen din sender e-poster gjennom en e-postserver som krever brukerautentisering. Denne metoden hindrer at unauthorized brukere får tilgang til e-postserveren.

Du kan sende e-postvarsling, e-postrapporter og I-Fax (finnes kun på visse modeller) ved hjelp av brukerautentisering.

- Tilgjengelige protokoller kan variere, avhengig av maskinen din.
- Vi anbefaler at du bruker Webbasert administrasjon til å konfigurere SMTP-pålitelighetskontroll.

Innstillinger for e-postserver

Du må konfigurere maskinens SMTP-pålitelighetskontrollmetode slik at den samsvarer med metoden som brukes av e-postserveren din. Vil du vite mer om innstillingene for e-postserveren, kontakter du nettverksadministrator eller Internett-leverandøren.

Du aktiverer SMTP-serverpålitelighetskontroll ved bruk av Webbasert administrasjon, ved å velge pålitelighetskontrollmetode under **Server Authentication Method (Server-pålitelighetskontrollmetode)** på **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**-skjermen..

Beslektet informasjon

- Sende eller motta e-post på en sikker måte

Sende eller motta e-post på en sikker måte med SSL/TLS

Maskinen støtter metoder for SSL/TLS-kommunikasjon. Vil du bruke en e-postserver som benytter SSL/TLS-kommunikasjon, må du konfigurere innstillingene nedenfor.

- Mottak av e-post er kun tilgjengelig på visse modeller.
- Vi anbefaler at du bruker Webbasert administrasjon til å konfigurere SSL/TLS.

Bekrefte serversertifikat

Hvis du under **SSL/TLS** velger **SSL** eller **TLS**, blir det automatisk merket av for **Verify Server Certificate**.

- 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.
- Hvis du ikke må bekrefte serversertifikatet, fjerner du merket for **Verify Server Certificate**.

Portnummer

Hvis du velger **SSL** eller **TLS**, vil **Port**-verdien endres slik at den samsvarer med protokollen. Vil du endre portnummeret manuelt, skriver du inn portnummeret etter at du har valgt innstillingene **SSL/TLS**.

Du må konfigurere maskinens kommunikasjonsmetode slik at den samsvarer med metoden som brukes av e-postserveren din. Vil du vite mer om innstillingene for e-postserveren, kan du ta kontakt med nettverksadministrator eller Internett-leverandøren.

I de fleste tilfeller krever den sikre Internett-baserte e-posttjenesten følgende innstillinger:

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

SMTP	**Port**	587
	Server Authentication Method (Server-pålitelighets-kontrollmetode)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Beslektet informasjon

- Sende eller motta e-post på en sikker måte

Beslektede emner:

- Konfigurere sending eller mottak av e-post via Webbasert administrasjon
- Konfigurere sertifikater for enhetssikkerhet

Lagre utskriftslogg til nettverk

Lagre utskriftslogg til nettverksoversikt

Med funksjonen Lagre utskriftslogg til nettverk kan du lagre utskriftsloggfilen fra maskinen på en nettverksserver ved hjelp av CIFS-protokollen (Common Internet File System). Du kan lagre ID, type utskriftsjobb, jobbnavn, brukernavn, dato, tidspunkt og antall utskrevne sider for hver utskriftsjobb. CIFS er en protokoll som kjører over TCP/IP som lar datamaskiner på et nettverk dele filer over et Intranett eller Internett.

Følgende utskriftsfunksjoner lagres i utskriftsloggen:

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

- utskriftsjobber fra datamaskinen
- Direkteutskrift fra USB
- kopiere
- Mottatt faks
- Web Connect-utskrift

- Lagre utskriftslogg til nettverk-funksjonen støtter Kerberos-pålitelighetskontroll og NTLMv2-pålitelighetskontroll. Du må konfigurere SNTP-protokollen (tidsserver for nettverk), eller du må angi riktig dato, klokkeslett og tidssone på kontrollpanelet for pålitelighetskontroll.
- Du kan stille inn filtypen til TXT eller CSV når du lagrer en fil til serveren.

Beslektet informasjon

- Lagre utskriftslogg til nettverk

Konfigurere Lagre utskriftslogg på nettverk med Webbasert administrasjon

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 **Administrator** > **Store Print Log to Network (Lagre utskriftslogg på nettverk)**.

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

5. I **Print Log (Skriv ut logg)**-feltet, klikker du på **On (På)**.
6. Konfigurerer følgende innstillinger:

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

Alternativ	Beskrivelse
Network Folder Path (Nettverksmappebane)	Angi destinasjonsmappen hvor utskriftsloggene skal lagres på CIFS-serveren (for eksempel: \\DatamaskinNavn\DeltMappe).
File Name (Filnavn)	Skriv inn filnavnet som du vil bruke for utskriftsloggen (opptil 32 tegn).
File Type (Filtype)	Velg **TXT (Tekst)**- eller **CSV**-alternativet for utskriftslogg-filtypen.
Time Source for Log (Tidskilde for logg)	Velg tidskilden for utskriftsloggen.
Auth. Method (Godkj. Metode)	Velg pålitelighetskontrollmetoden som kreves for tilgang til CIFS-serveren: **Auto**, **Kerberos** eller **NTLMv2**. Kerberos er en pålitelighetskontroll-protokoll som lar enheter eller individer bevise identiteten sin overfor nettverksservere på en sikker måte med én enkel pålogging. NTLMv2 er pålitelighetskontrollmetoden som brukes av Windows for å logge på servere. • **Auto**: Hvis du velger **Auto**, brukes NTLMv2 som pålitelighetskontrollmetoden. • **Kerberos**: Velg **Kerberos**-alternativet for å bruke bare Kerberos-pålitelighetskontroll. • **NTLMv2**: Velg **NTLMv2**-alternativet for å bruke bare NTLMv2-pålitelighetskontroll.

Alternativ	Beskrivelse
	• For **Kerberos**- og **NTLMv2**-pålitelighetskontroll, må du også konfigurere **Date&Time (Dato og tid)**-innstillingene eller SNTP-protokollen (nettverkstidserver) og DNS-server. • Du kan også konfigurere innstillingene for Dato og klokkeslett på maskinens kontrollpanel.
Username (Brukernavn)	Skriv inn brukernavnet for pålitelighetskontrollen (opptil 96 tegn). Hvis brukernavnet er en del av et domene, skriver du inn brukernavnet i én av følgende stiler: bruker@domene eller domene\bruker.
Password (Passord)	Skriv inn passordet for pålitelighetskontrollen (opptil 32 tegn).
Kerberos Server Address (Kerberos-serveradresse) (hvis nødvendig)	Skriv inn KDC (Key Distribution Center)-vertsadressen (for eksempel, kerberos.eksempel.no, opptil 64 tegn) eller IP-adressen (for eksempel: 192.168.56.189).
Error Detection Setting (Innstilling for feilregistrering)	Velg hvilken handling som skal utføres når utskriftsloggen ikke kan lagres på serveren på grunn av en nettverksfeil.

7. I **Connection Status (Tilkoblingsstatus)**-feltet, bekreft siste loggstatus.

Du kan også bekrefte feilstatusen på LCD-skjermen til maskinen.

8. Klikk på **Submit (Send inn)** for å vise **Test Print Log to Network (Test utskriftslogg til nettverk)**-siden.
   Klikk på **Yes (Ja)** for å teste innstillingene og gå deretter til neste trinn.
   Klikk på **No (Nei)** for å hoppe over testen. Innstillingene sendes automatisk.
9. Maskinen tester innstillingene.
10. Hvis innstillingene blir godtatt, vises **Test OK** på skjermen.
    Hvis **Test Error (Test feil)** vises, sjekk alle innstillingene og klikk så **Submit (Send inn)** for å vise testsiden på nytt.

Beslektet informasjon

- Lagre utskriftslogg til nettverk

Bruke Lagre utskriftslogg på nettverkets feiloppdagelsesinnstilling

Bruk feiloppdagelsesinnstillinger til å bestemme handlingen som tas når utskriftsloggen ikke kan lagres på serveren på grunn av en nettverksfeil.

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 **Administrator** > **Store Print Log to Network (Lagre utskriftslogg på nettverk)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. I **Error Detection Setting (Innstilling for feilregistrering)**-delen, velger du alternativet **Cancel Print (Avbryt utskrift)** eller **Ignore Log & Print (Ignorer logg og skriv ut)**.

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

Alternativ	Beskrivelse
Cancel Print (Avbryt utskrift)	Hvis du velger **Cancel Print (Avbryt utskrift)**-alternativet, canceled utskriftsjobbene når utskriftsloggen ikke kan lagres på serveren. Selv om du velger **Cancel Print (Avbryt utskrift)**-alternativet, skriver maskinen ut en mottatt faks.

Ignore Log & Print (Ignorer logg og skriv ut)	Hvis du velger **Ignore Log & Print (Ignorer logg og skriv ut)**-alternativet, skriver maskinen ut dokumentasjonen selv om utskriftsloggen ikke kan lagres på serveren.
	Når funksjonen for å lagre utskriftslogg er gjenopprettet, lagres utskriftsloggen på følgende måte:
	`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. Hvis utskriftsloggen ikke kan lagres på slutten av utskriften, registreres ikke antall utskrevne sider.
	b. Hvis loggen ikke kan lagres på begynnelsen og slutten av utskriften, lagres ikke utskriftsloggen av jobben. Når funksjonen har blitt gjenopprettet, gjenspeiles feilen i utskriftsloggen.

6. Klikk på **Submit (Send inn)** for å vise **Test Print Log to Network (Test utskriftslogg til nettverk)**-siden.

   Klikk på **Yes (Ja)** for å teste innstillingene og gå deretter til neste trinn.

Klikk på **No (Nei)** for å hoppe over testen. Innstillingene sendes automatisk.

7. Maskinen tester innstillingene.
8. Hvis innstillingene blir godtatt, vises **Test OK** på skjermen.

   Hvis **Test Error (Test feil)** vises, sjekk alle innstillingene og klikk så **Submit (Send inn)** for å vise testsiden på nytt.

Beslektet informasjon

- Lagre utskriftslogg til nettverk

Bruke Lagre utskriftslogg til nettverk med Secure Function Lock 3.0

Når Secure Function Lock 3.0 er aktiv, lagres navnene på de registrerte brukerne for kopiering, Faks RX, Web Connect-utskrift og USB-direkteutskrift i Lagre utskriftslogg til nettverk-rapporten. Når Active Directory-pålitelighetskontroll er aktivert, lagres brukernavnet i rapporten Lagre utskriftslogg i nettverk:

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

```
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
```

Beslektet informasjon

- Lagre utskriftslogg til nettverk

brother

Brother Earth

www.brotherearth.com

NOR
Version 0