SSL-veiledning

(Secure Socket Layer)

For å finne grunnleggende informasjon om nettverket og Brother-maskinens avanserte nettverksfunksjoner: ➤➤ Brukerhåndbok for nettverket.

For å laste ned den aller nyeste brukerhåndboken, besøk Brother Solutions Center på (http://solutions.brother.com/). På Brother Solutions Center kan du også laste ned de nyeste driverne og verktøyene til maskinen din, lese svar på vanlige spørsmål, få tips om problemløsing eller finne informasjon om spesielle utskriftsløsninger.

Ikke alle modeller er tilgjengelige i alle land.

Version 0

NOR

Relevante modeller

Denne brukermanualen gjelder for følgende modeller.

HL-5450DN(T)/5470DW(T)/6180DW(T)

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Definisjoner for merknader

Vi bruker følgende ikoner i denne brukermanualen:

Merk	Merknader forteller hvordan du bør reagere på en situasjon som kan oppstå eller du får tips om hvordan bruken fungerer sammen med andre funksjoner.

Varemerker

Brother-logoen er et registrert varemerke for Brother Industries, Ltd.

Microsoft, Windows, Windows Server og Internet Explorer er enten registrerte varemerker eller varemerker for Microsoft Corporation i USA og/eller andre land.

Windows Vista er enten et registrert varemerke eller et varemerke for Microsoft Corporation i USA og/eller andre land.

Hvert selskap som eier en programvaretittel som nevnes i denne håndboken har en programvarelisensavtale som er spesifikk for dets egenutviklede programmer.

Alle handelsnavn og produktnavn som vises på Brother-produkter, men som tilhører andre selskaper, relaterte dokumenter og eventuelt andre materialer, er varemerker eller registrerte varemerker for disse respektive selskapene.

VIKTIG

- Dette produktet er kun godkjent for bruk i landet der det er kjøpt. Produktet må ikke brukes utenfor landet der det ble kjøpt, da dette kan være i strid med regelverk for trådløs kommunikasjon og strømnettverk i andre land.
- I denne manualen, brukes skjermbildene på MFC-8950DW(T) med mindre annet er oppgitt.
- Windows® XP i dette dokumentet representerer Windows® XP Professional, Windows® XP Professional x64 Edition og Windows® XP Home Edition.
- Windows Server® 2003 i dette dokumentet representerer Windows Server® 2003 og Windows Server® 2003 x64 Edition.
- Windows Server® 2008 i dette dokumentet representerer Windows Server® 2008 og Windows Server® 2008 R2.
- Windows Vista® i dette dokumentet representerer alle utgavene av Windows Vista®.
- Windows® 7 i dette dokumentet representerer alle utgavene av Windows® 7.
- Gå til Brother Solutions Center på http://solutions.brother.com/ og klikk på Håndbøker på siden til din modell for å laste ned de andre brukerhåndbøkene.

Innholdsfortegnelse

1 Innledning

Oversikt

Secure Socket Layer (SSL) er en effektiv metode for å beskytte data som sendes over et lokalt eller bredere områdenettverk. Det fungerer ved å kryptere data som sendes over et nettverk, f.eks. en utskriftsjobb, slik at noen som prøver å fange det opp ikke vil være i stand til å lese den, ettersom alle data vil være kryptert.

Den kan konfigureres på både kablede og trådløse nettverk og vil fungere med andre former for sikkerhet, som for eksempel WPA-nøkler og brannmurer.

En kort historie om SSL

SSL ble opprinnelig laget for å sikre informasjon i nettrafikk, spesielt data som sendes mellom nettlesere og servere. Når du for eksempel bruker Internet Explorer® for å gjøre ting i nettbanken og du ser https:// og den lille hengelåsen i nettleseren, så bruker du SSL. Den vokste til å fungere med andre applikasjoner som Telnet, skrivere og FTP-programvare slik at den ble en universell løsning for nettsikkerhet. De opprinnelige designintensjonene brukes fremdeles i dag av mange nettbutikker og -banker for å sikre sensitive data, som kredittkortnumre, kundeopplysninger osv.

SSL bruker meget høye krypteringsnivåer og stoles på av banker over hele verden, siden det er usannsynlig at krypteringen kan brytes.

Fordeler ved bruk av SSL

Den eneste fordelen med å bruke SSL på Brother-maskiner er å gi sikker utskrift over et IP-nettverk ved å begrense uautoriserte brukere fra å være i stand til å lese data som sendes til maskinen. Det viktigste salgspoenget er at det kan brukes til skrive ut konfidensielle data på en sikker måte. HR-avdelingen til en stor bedrift skriver for eksempel kanskje regelmessig ut lønnsslipper. Uten kryptering kan data på disse lønnsslippene leses av andre nettverksbrukere. Med SSL vil imidlertid alle som prøver å fange opp data bare se en forvirrende side med kode og ikke den faktiske lønnsslippen.

Bruke sertifikater for enhetssikkerhet

Brother-maskinen din støtter bruk av flere sikkerhetssertifikater som muliggjør sikker administrering, godkjenning og kommunikasjon med maskinen. Følgende sikkerhetssertifikatfunksjoner kan brukes med maskinen. Når du skriver ut et dokument eller bruker Internett-basert styring (nettleser) på en sikker måte med SSL, må du installere sertifikatet på datamaskinen. Se *Installasjon av digitalt sertifikat* ➤➤ side 4.

- SSL/TLS-kommunikasjon
- SSL-kommunikasjon for SMTP/POP3

Brother-maskinen støtter følgende sertifikater.

- Forhåndsinstallert sertifikat

  Maskinen din har et forhåndsinstallert selvsignert sertifikat.

  Med dette sertifikatet kan du enkelt bruke SSL/TLS-kommunikasjonen uten å opprette eller installere et sertifikat. Hvis du ønsker å bruke maskinens Google Cloud Print-funksjon, kan du bruke dette forhåndsinstallerte sertifikatet til å konfigurere Google Cloud Print-innstillingene på en sikker måte. For mer informasjon om Google Cloud Print, gå til Brother Solutions Center på http://solutions.brother.com/ og klikk på Håndbøker på siden for din modell for å laste ned Google Cloud Print-guide.

Merk

Det forhåndsinstallert, selvsignerte sertifikatet kan ikke beskytte din kommunikasjon mot spoofing. Vi anbefaler at du bruker et sertifikat som er utstedt av en organisasjon du stoler på for å få bedre sikkerhet.

- Selvsignert sertifikat

  Denne utskriftsserveren utsteder sitt eget sertifikat. Med dette sertifikatet kan du enkelt bruke SSL/TLS-kommunikasjonen uten at du har et sertifikat fra en sertifikatinstans. (Se *Opprette et egensignert sertifikat* ➤➤ side 6.)

- Sertifikat fra en CA

  Det er to metoder for installasjon av et sertifikat fra en sertifikatinstans. Hvis du allerede har et sertifikat fra en CA eller du vil bruke et sertifikat fra en ekstern pålitelig CA:

  - Når du bruker et CSR (Certificate Signing Request) fra denne utskriftsserveren. (Se *Opprette en sertifikatsigneringsordre (CSR)* ➤➤ side 7.)
  - Når du importerer et sertifikat og en privat nøkkel. (Se *Importer og eksporter sertifikatet og den private nøkkelen* ➤➤ side 17.)

■ CA-sertifikat

Hvis du bruker et CA-sertifikat som identifiserer selve CA (Certificate Authority), må du importere et CA-sertifikat fra CA før konfigurasjonen. (Se *Importere og eksporter et CA-sertifikat* ➤➤ side 18.)

Merk

- Hvis du skal bruke SSL/TLS-kommunikasjon, anbefaler vi at du kontakter systemadministratoren din først.
- Når du tilbakestiller utskriftsserveren til fabrikkinnstillingene, slettes sertifikatet og den private nøkkelen som er installert. Hvis du vil beholde samme sertifikat og private nøkkel etter tilbakestilling av utskriftsserveren, må du eksportere dem før tilbakestillingen og deretter installere dem på nytt. (Se *Slik importerer du det selvsignerte sertifikatet, sertifikatet som er utstedt av en CA og den private nøkkelen* ➤➤ side 17.)

2 Digitalt sertifikat for SSL-kommunikasjon

Installasjon av digitalt sertifikat

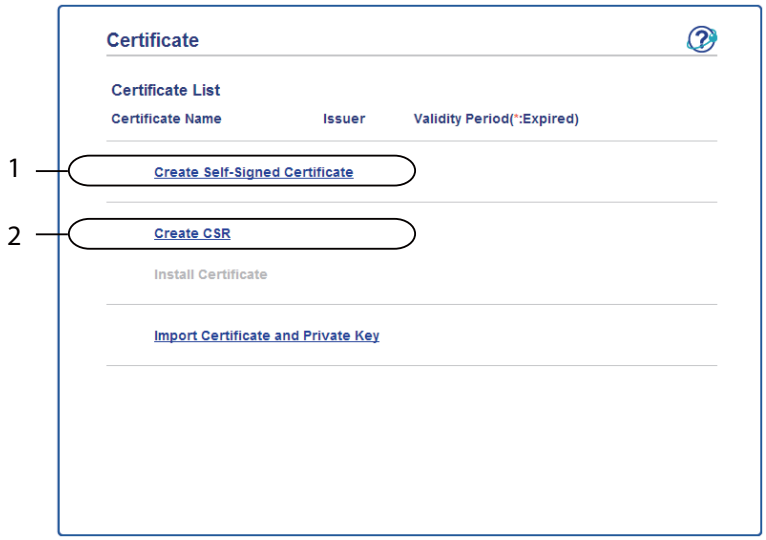
Utskrift over et sikret nettverk eller sikker styring ved bruk av Internett-basert styring (nettleser), krever et digitalt sertifikat som må installeres på både maskinen og enheten som sender data til maskinen, f.eks. en datamaskin. Maskinen din har et forhåndsinstallert sertifikat. For å konfigurere sertifikatet, må brukeren logge seg på maskinen eksternt gjennom en nettleser ved bruk av dens IP-adresse.

Merk

Vi anbefaler Windows® Internet Explorer® 7.0/8.0 eller Firefox® 3.6 for Windows® og Safari 4.0/5.0 for Macintosh. Påse også at JavaScript og informasjonskapsler alltid er aktivert i alle nettlesere du bruker. Hvis du bruker en annen nettleser må du kontrollere at den er kompatibel med HTTP 1.0 og HTTP 1.1.

1. Start nettleseren.
2. Skriv inn "http://maskinens IP-adresse/" i nettleserens adresselinje (der "maskinens IP-adresse" er IP-adressen til maskinen eller utskriftsserverens navn).
   - For eksempel: http://192.168.1.2/
3. Intet passord kreves som standard. Hvis du tidligere har stilt inn et passord, tast det inn og trykk på →.
4. Klikk på **Network** (Nettverk).
5. Klikk på **Security** (Sikkerhet).
6. Klikk på **Certificate** (Sertifikat).

7 Du kan konfigurere sertifikatinnstillingene.
For å opprette et selvsignert sertifikat med Internett-basert styring, gå til *Opprette et egensignert sertifikat* ➤➤ side 6.
Gå til *Opprette en sertifikatsigneringsordre (CSR)* ➤➤ side 7 for å opprette en sertifikatsigneringsordre (CSR).



1 Opprette og installere et egensignert sertifikat

2 Bruke et sertifikat fra en Certificate Authority (CA)

Merk

- Funksjonene som er skyggelagt og mangler en kobling er ikke tilgjengelige.
- For mer informasjon om konfigurasjon, se hjelpeteksten i Internett-basert styring.

Opprette et egensignert sertifikat

1. Klikk på **Create Self-Signed Certificate** (Opprett selvsignert sertifikat).
2. Oppgi et **Common Name** (Fellesnavn) og et **Valid Date** (Gyldig dato).

Merk

- Lengden på **Common Name** (Fellesnavn) må være mindre enn 64 tegn. Oppgi 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 egensignerte sertifikatet.

3. Du kan velge **Public Key Algorithm** (Fellesnøkkelalgoritme)- og **Digest Algorithm** (Sammendragsalgoritme)-innstillingene fra rullegardinlisten. Standardinnstillingene er **RSA(2048bit)** for **Public Key Algorithm** (Fellesnøkkelalgoritme) og **SHA256** for **Digest Algorithm** (Sammendragsalgoritme).
4. Klikk på **Submit** (Send).
5. Det selvsignerte sertifikatet er opprettet og lagret i minnet til maskinen.

Opprette en sertifikatsigneringsordre (CSR)

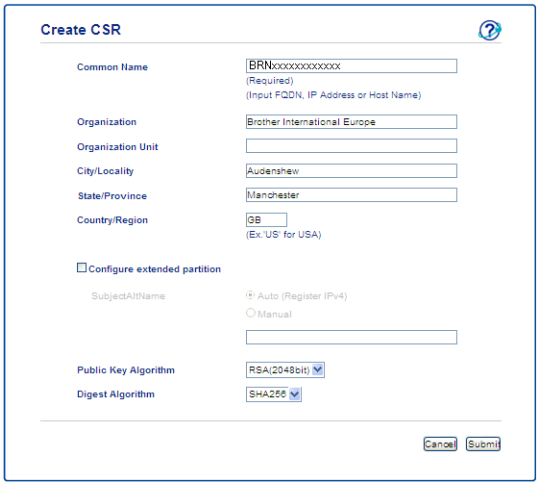
En sertifikatsigneringsordre (CSR) er en ordre som sendes til en CA for å autentisere referansene i sertifikatet.

Merk

Vi anbefaler at rotsertifikatet fra CA installeres på datamaskinen før du oppretter CSR.

1. Klikk på **Create CSR** (Opprett CSR).

2. Oppgi **Common Name** (Fellesnavn) og informasjonen din, som **Organization** (Organisasjon). Du må oppgi opplysninger om bedriften slik at CA kan bekrefte din identitet og bevitne dette til resten av verden.



Merk

- Lengden på **Common Name** (Fellesnavn) må være mindre enn 64 tegn. Oppgi 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 oppgir et annet navn i URL-adressen enn fellesnavnet som ble brukt for sertifikatet.
- Lengden på **Organization** (Organisasjon), **Organization Unit** (Organisasjonsenhet), **City/Locality** (By/sted) og **State/Province** (Fylke) må være mindre enn 64 tegn.
- **Country/Region** (Land/område) bør være en ISO 3166 landskode bestående av to bokstaver.
- Hvis du konfigurerer X.509v3-sertifikatutvidelsen, kryss av i **Configure extended partition** (Konfigurer utvidet partisjon)-avmerkingsboksen og velg deretter **Auto (Register IPv4)** (Automatisk (Registrer IPv4)) eller **Manual** (Manuell).

3. Du kan velge **Public Key Algorithm** (Fellesnøkkelalgoritme)- og **Digest Algorithm** (Sammendragsalgoritme)-innstillingene fra rullegardinlisten. Standardinnstillingene er **RSA(2048bit)** for **Public Key Algorithm** (Fellesnøkkelalgoritme) og **SHA256** for **Digest Algorithm** (Sammendragsalgoritme).

4 Klikk på **Submit** (Send). Det følgende skjermbildet vises.

5 Etter en liten stund vil du bli presentert med et sertifikat, som kan lagres i en liten fil eller kopieres og limes inn direkte i et nett-CSR-formular som Certificate Authority tilbyr. Klikk på **Save** (Lagre) for å lagre CSR-filen på datamaskinen.

Merk

Følg CA-policyen din for sendemetoden for en CSR til din CA.

6 CSR er opprettet. Gå til *Hvordan du installerer sertifikatet på maskinen* ➤➤ side 9 for å få anvisninger om hvordan du installerer sertifikatet på din maskin.

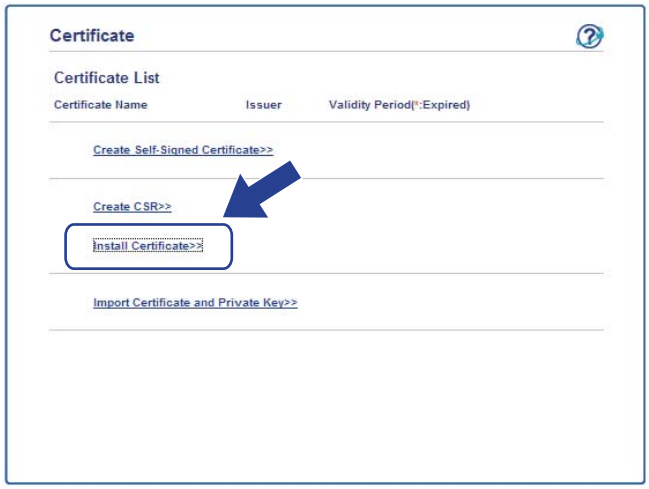
Hvordan du installerer sertifikatet på maskinen

Når du mottar sertifikatet fra en CA, følg trinnene under for å installere det på utskriftsserveren.

Merk

Kun et sertifikat som er utstedt med denne maskinens CSR kan installeres. Hvis du vil opprette et annet CSR, må du sørge for at sertifikatet er installert før du oppretter et annet CSR. Opprett et annet CSR etter at du har installert sertifikatet til maskinen. Ellers vil CSR-et som du laget før installasjonen være ugyldig.

1. Klikk på **Install Certificate** (Installer sertifikat) på **Certificate** (Sertifikat)-siden.



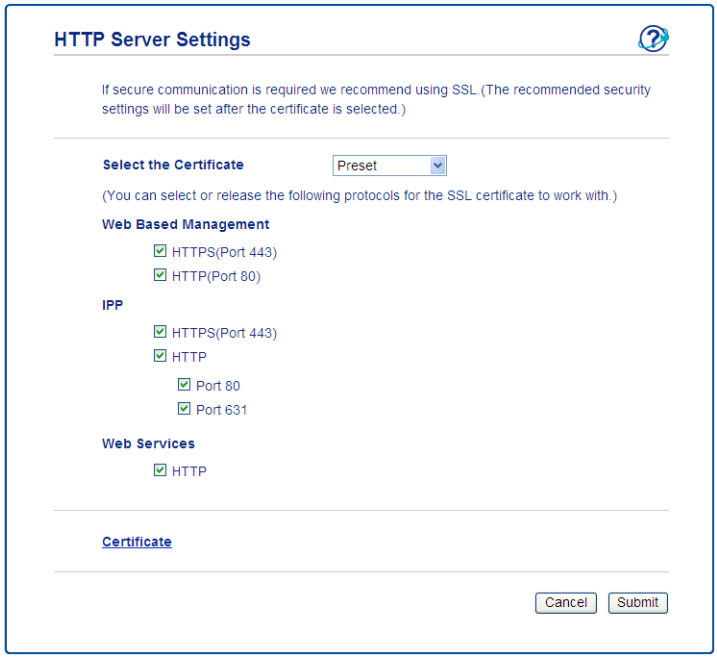
2. Spesifiser filen til sertifikatet som har blitt utstedt av en CA, og klikk deretter på **Submit** (Send).

3. Sertifikatet er nå opprettet og lagret i minnet til maskinen.
For å bruke SSL/TLS-kommunikasjon må det rotsertifikatet fra CA også installeres på datamaskinen. Kontakt nettverksadministratoren om installasjonen.
Du har fullført den digitale sertifikatkonfigurasjonen. Hvis du ønsker å sende eller motta en e-post ved bruk av SSL, se *Sende eller motta (for DCP- og MFC-modeller) e-post på en sikker måte* ➤➤ side 25 for nødvendige konfigurasjonstrinn.

Velge sertifikatet

Etter at du har installert sertifikatet, følger du fremgangsmåten nedenfor for å velge det sertifikatet du ønsker å bruke.

1. Klikk på **Network** (Nettverk).
2. Klikk på **Protocol** (Protokoll).
3. Klikk på **HTTP Server Settings** (HTTP-serverinnstillinger) og velg deretter sertifikatet fra rullegardinlisten **Select the Certificate** (Velg sertifikatet).



Merk

- Hvis følgende dialogboks vises, anbefaler Brother å deaktivere Telnet-, FTP-, TFTP-protokollene og nettverksstyringen med eldre versjoner av BRAdmin Professional (2,8 tidligere) for sikker kommunikasjon. Hvis du aktiverer dem, er bruker autentisering ikke sikker.

- For DCP- og MFC-modeller:

  Hvis du deaktiverer FTP, deaktiveres Skann til FTP-funksjonen.

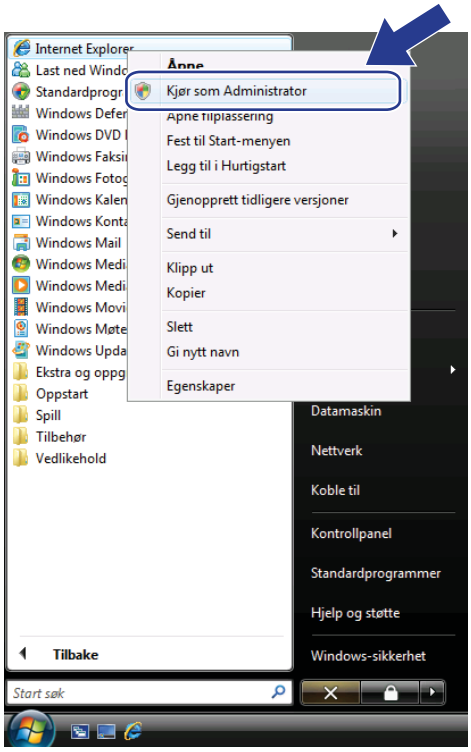
4. Klikk på **Submit** (Send).

Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet på Windows Vista®, Windows® 7 og Windows Server® 2008 for brukere med administratorrettigheter

Merk

- Følgende trinn gjelder for Windows® Internet Explorer®. Hvis du bruker en annen nettleser må du følge hjelpeteksten i den nettleseren.
- Du må ha administratorrettigheter for å installere det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet.

1. Klikk på -knappen og **Alle programmer**.
2. Høyreklikk på **Internet Explorer** og klikk deretter på **Kjør som Administrator**.



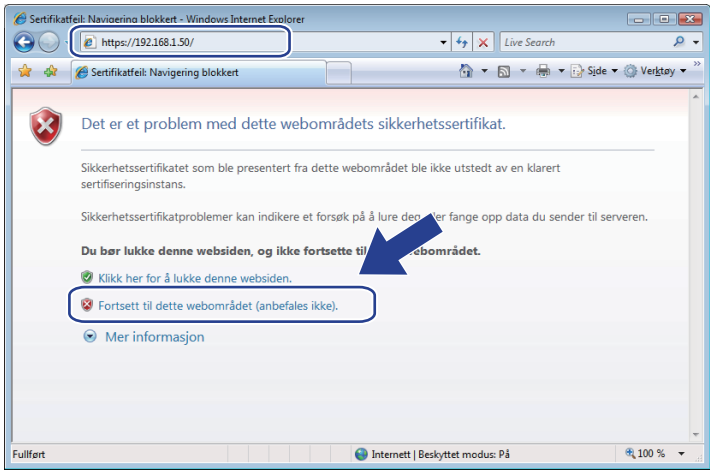
Merk

Hvis **Brukerkontokontroll**-skjermen vises,

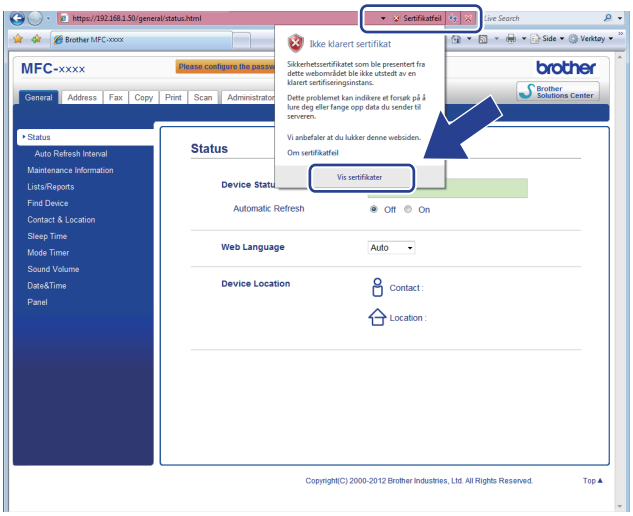
(Windows Vista®) Klikk på **Fortsett (Tillat)**.

(Windows® 7) Klikk på **Ja**.

3 Skriv inn "https://maskinens IP-adresse/" i nettleseren for å få tilgang til maskinen (der "maskinens IP-adresse" er maskinens IP-adresse eller nodenavnet som du tildelte sertifikatet).
Klikk deretter på **Fortsett til dette webområdet (anbefales ikke).**.

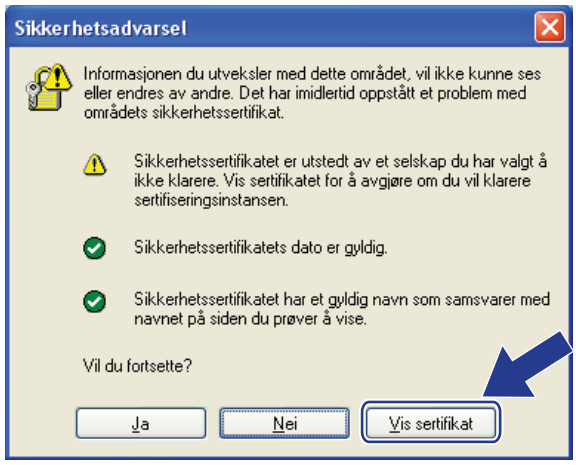


4 Klikk på **Sertifikatfeil** og klikk deretter på **Vis sertifikater**. For resten av instruksjonene, følg trinnene fra trinn ❹ i *Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet for Windows® XP- og Windows Server® 2003-brukere* ➤➤ side 14.

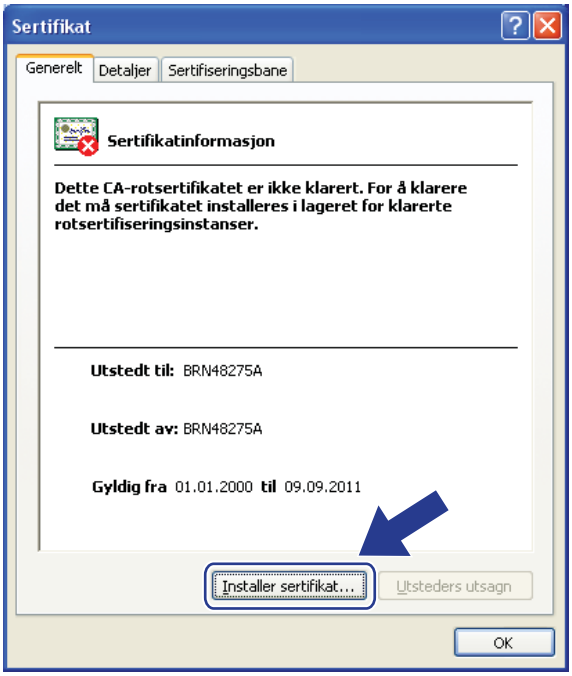


Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet for Windows® XP- og Windows Server® 2003-brukere

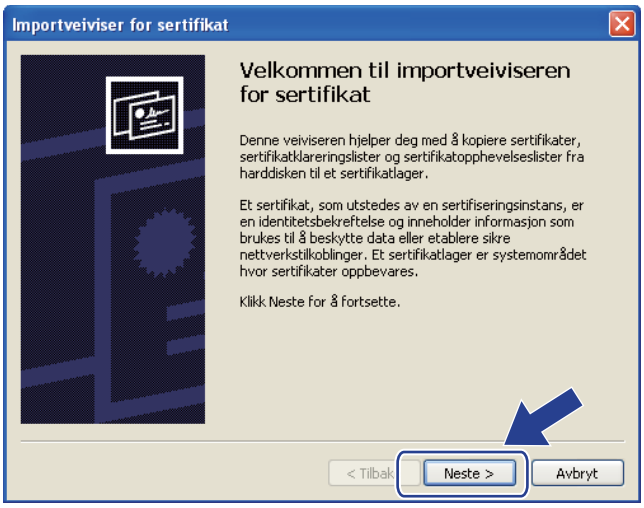
1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse/" i nettleseren for å få tilgang til maskinen (der "maskinens IP-adresse" er IP-adressen eller nodenavnet som du tildelte sertifikatet).
3. Gjør et av følgende når dialogboksen om sikkerhetsvarsel vises:
   - Klikk på **Fortsett til dette webområdet (anbefales ikke).**. Klikk på **Sertifikatfeil** og klikk deretter på **Vis sertifikater**.
   - Hvis følgende dialogboks vises, klikk på **Vis sertifikat**.



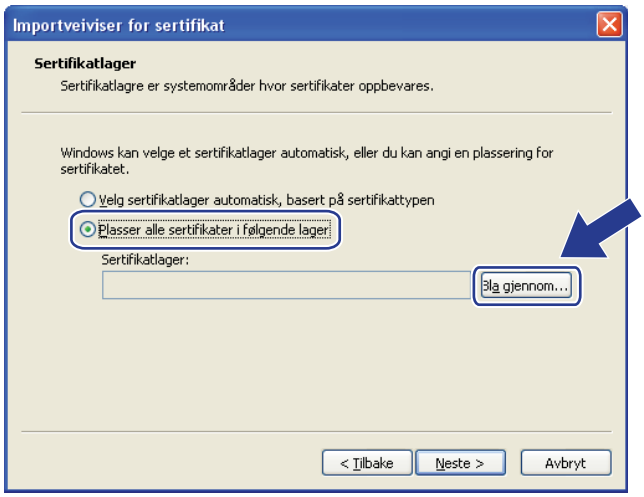
4. Klikk på **Installer sertifikat...** fra **Generelt**-kategorien.



5 Når **Importveiviser for sertifikat** vises, klikk på **Neste**.

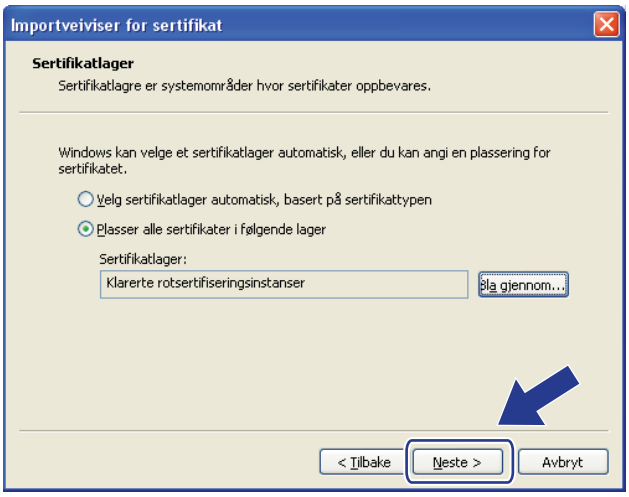


6 Du må spesifisere et sted å installere sertifikatet. Vi anbefaler at du velger **Plasser alle sertifikater i følgende lager** og deretter klikker på **Bla gjennom...**.



7 Velg **Klarerte rotsertifiseringsinstanser** og klikk på **OK**.

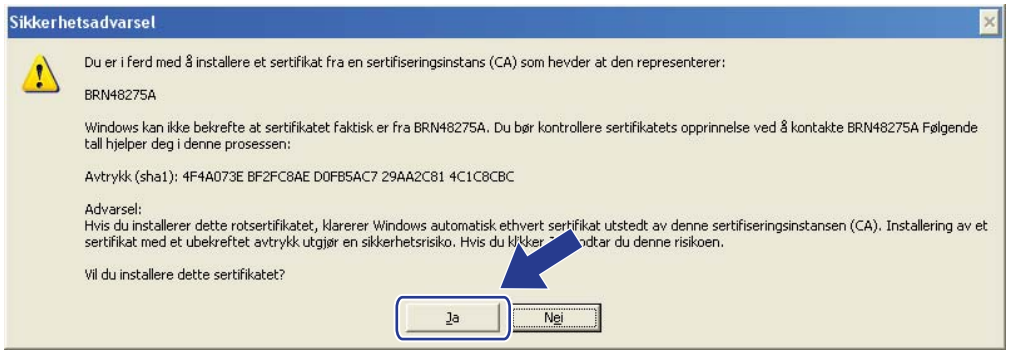
8 Klikk på **Neste**.



9 Klikk på **Fullfør** på neste skjermbilde.

10 Du vil deretter bli bedt om å installere sertifikatet.
Gjør ett av følgende:

- Hvis du installerer det selvsignerte sertifikatet, må du bekrefte fingeravtrykket (tommelavtrykk) og deretter klikke på **Ja**.
- Klikk på **Ja** hvis du installerer det forhåndsinstallerte sertifikatet.



Merk

- For det selvsignerte sertifikatet skrives fingeravtrykket (tommelfingeravtrykk) på Nettverksinnstillingsrapporten.

  For å lære hvordan du skriver ut Nettverksinnstillingsrapporten, se *Skrive ut Skriverinnstillingsside (for HL-5450DN(T))* ➤➤ side 29 eller *Skrive ut Nettverksinnstillingsrapporten (for andre modeller)* ➤➤ side 29.
- For det forhåndsinstallerte sertifikatet skrives ikke fingeravtrykket på Nettverksinnstillingsrapporten.

11 Klikk på **OK**.

12 Det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet er nå installert på datamaskinen, og SSL/TLS-kommunikasjonen er tilgjengelig.

Hver datamaskin som ønsker å skrive ut sikkert må gjøre det samme. Når den først er installert, er det imidlertid ikke nødvendig å gjenta disse skrittene med mindre sertifikatet endres.

Importer og eksporter sertifikatet og den private nøkkelen

Du kan lagre sertifikatet og den private nøkkelen på maskinen og administrere dem med importering og eksportering.

Slik importerer du det selvsignerte sertifikatet, sertifikatet som er utstedt av en CA og den private nøkkelen

1 Klikk på **Import Certificate and Private Key** (Importer sertifikat og privat nøkkel) på **Certificate** (Sertifikat)-siden.

2 Spesifiser filen som du vil importere.

3 Oppgi passordet hvis filen er kryptert, og klikk på **Submit** (Send).

4 Nå er sertifikatet og den private nøkkelen importert til maskinen.

Slik eksporterer du det selvsignerte sertifikatet, sertifikatet som er utstedt av en CA og den private nøkkelen

1 Klikk på **Export** (Eksporter) vist med **Certificate List** (Sertifikatliste) på **Certificate** (Sertifikat)-siden.

2 Oppgi et passord hvis du vil kryptere filen.

Merk

Hvis et tomt passord brukes, fungerer ikke krypteringen.

3 Oppgi passordet på nytt for bekreftelse, og klikk på **Submit** (Send).

4 Spesifiser plasseringen hvor du vil lagre filen.

5 Nå er sertifikatet og den private nøkkelen eksportert til datamaskinen.

Importere og eksporter et CA-sertifikat

Du kan lagre et CA-sertifikat på maskinen via importering og eksportering.

Slik importerer du et CA-sertifikat

1. Klikk på **CA Certificate** (CA-sertifikat) på **Security** (Sikkerhet)-siden.
2. Klikk på **Import CA Certificate** (Importer CA-sertifikat) og velg sertifikatet. Klikk på **Submit** (Send).

Slik eksporterer du et CA-sertifikat

1. Klikk på **CA Certificate** (CA-sertifikat) på **Security** (Sikkerhet)-siden.
2. Velg sertifikatet du ønsker å eksportere, og klikk på **Export** (Eksporter). Klikk på **Submit** (Send).
3. Klikk på **Save** (Lagre) for å velge målmappen.
4. Velg målet der du ønsker å lagre det eksporterte sertifikatet og lagre deretter sertifikatet.

Administrere flere sertifikater

Multi-sertifikatfunksjonen lar deg behandle hvert sertifikat som du har installert med Internett-basert styring. Etter at du har installert sertifikater, kan du se hvilke sertifikater som er installert fra **Certificate** (Sertifikat)-siden og deretter se innholdet i hvert sertifikat, samt slette eller eksportere sertifikatet. Hvis du vil vite mer om hvordan du får tilgang til **Certificate** (Sertifikat), se *Installasjon av digitalt sertifikat* ➤➤ side 4.

- For skrivermodeller

  Brother-maskinen kan brukes til å lagre opptil tre selvsignerte sertifikater eller opptil tre sertifikater som er utstedt av en CA. Du kan bruke de lagrede sertifikatene for bruk av HTTPS/IPPS-protokollen eller IEEE 802.1x-autentisering.

- For DCP- og MFC-modeller

  Brother-maskinen kan brukes til å lagre opptil fire selvsignerte sertifikater eller opptil fire sertifikater som er utstedt av en CA. Du kan bruke de lagrede sertifikatene for bruk av HTTPS/IPPS-protokollen, IEEE 802.1x-autentisering eller en signert PDF.

Du kan også lagre opptil fire CA-sertifikater for bruk med IEEE 802.1x-godkjenning og SSL for SMTP/POP3.

Vi anbefaler at du lagrer ett sertifikat mindre og holder det siste ledig for når sertifikater utløper. For eksempel, hvis du vil lagre et CA-sertifikat, lagrer du tre sertifikater og lar den siste plassen brukes som backup. Hvis sertifikatet utstedes på nytt, som når det har utløpt, kan du importere et nytt sertifikat til backupen og deretter slette det utløpte sertifikatet, og på denne måten unngå feil med konfigurasjonen.

Merk

- Når du bruker HTTPS/IPPS, IEEE 802.1x eller signert PDF (for DCP- og MFC-modeller), må du velge hvilket sertifikat du bruker.
- Når du bruker SSL for SMTP/POP3-kommunikasjon (for DCP- og MFC-modeller), trenger du ikke å velge sertifikatet. Det nødvendige sertifikatet vil bli valgt automatisk.

3 Behandle din nettverksmaskin på en sikker måte med SSL/TLS

For sikker behandling av nettverksmaskinen, må du bruke styringsverktøyene med sikkerhetsprotokoller.

Sikker administrering med Internett-basert styring (nettleser)

Vi anbefaler at du bruker HTTPS-protokoll for sikker administrering. For å bruke disse protokollene, kreves følgende maskininnstillinger.

Merk

- HTTPS-protokollen er aktivert som standard.

  Du kan endre HTTPS-protokollinnstillingene og sertifikatet som skal brukes på Internett-basert styring-skjermen, ved å klikke på **Network** (Nettverk), **Protocol** (Protokoll) og deretter **HTTP Server Settings** (HTTP-serverinnstillinger).

- Du må også installere sertifikatet du har installert på maskinen, på datamaskinen. Se *Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet på Windows Vista®, Windows® 7 og Windows Server® 2008 for brukere med administratorrettigheter* ➤➤ side 12 eller *Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet for Windows® XP- og Windows Server® 2003-brukere* ➤➤ side 14.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse/" i nettleseren. (Hvis du bruker det opprettede sertifikatet, skriv inn "https://Fellesnavn/" i nettleseren. Hvor "Fellesnavn" er fellesnavnet som du tildelte sertifikatet, som en IP-adresse, nodenavn eller domenenavn. For informasjon om hvordan du tildeler et fellesnavn for sertifikatet, se *Bruke sertifikater for enhetssikkerhet* ➤➤ side 2.)

   ■ Eksempel:

   https://192.168.1.2/ (hvis fellesnavnet er maskinens IP-adresse)
3. Intet passord kreves som standard. Tast inn et passord hvis du har stilt inn et og trykk på .

4 Skrive ut dokumenter på en sikker måte med SSL

Skrive ut dokumenter på en sikker måte med IPPS for Windows®

Vi anbefaler at du bruker IPPS-protokoll for sikker administrering. For å bruke IPPS-protokollen, kreves følgende maskininnstillinger.

Merk

- Kommunikasjon med IPPS kan ikke forhindre uautorisert tilgang til utskriftsserveren.
- Du må også installere sertifikatet du har installert på maskinen, på datamaskinen. Se *Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet på Windows Vista®, Windows® 7 og Windows Server® 2008 for brukere med administratorrettigheter* ➤➤ side 12 eller *Installasjon av det selvsignerte sertifikatet eller det forhåndsinstallerte sertifikatet for Windows® XP- og Windows Server® 2003-brukere* ➤➤ side 14.
- IPPS-protokollen må aktiveres. Standardinnstillingen er aktivert. Du kan endre IPPS-protokollinnstillingene og sertifikatet som skal brukes på Internett-basert styring-skjermen, ved å klikke på **Network** (Nettverk), **Protocol** (Protokoll) og deretter **HTTP Server Settings** (HTTP-serverinnstillinger).

Windows® XP og Windows Server® 2003

1. Klikk på **Start** og velg **Skrivere og telefakser**.
2. Klikk på **Legg til skriver** for å starte **Veiviser for skriver**.
3. Klikk på **Neste** når du ser **Velkommen til veviseren for skriver**-skjermbildet.
4. Velg **En nettverksskriver eller en skriver koblet til en annen datamaskin**.
5. Klikk på **Neste**.
6. Velg **Koble til en skriver på Internett eller på et hjemme- eller kontornettverk** og skriv deretter følgende i URL-feltet:
"https://maskinens IP-adresse/ipp" (der "maskinens IP-adresse" er maskinens IP-adresse eller nodenavnet).

Merk

- Det er viktig at du bruker "https://" og ikke "http://", ellers vil ikke utskrift over IPP være sikker.
- Hvis du har redigert vertsfilene på datamaskinen eller bruker Domain Name System (DNS), kan du også bruke DNS-navnet til utskriftsserveren. Ettersom utskriftsserveren støtter TCP/IP- og NetBIOS-navn, kan du også bruke NetBIOS-navnet til utskriftsserveren. NetBIOS-navnet vises i Nettverksinnstillingsrapporten. (For informasjon om hvordan du skriver ut Nettverksinnstillingsrapporten, se *Skrive ut Skriverinnstillingsside (for HL-5450DN(T))* ➤➤ side 29 eller *Skrive ut Nettverksinnstillingsrapporten (for andre modeller)* ➤➤ side 29.) NetBIOS-navnet som gis er de 15 første tegnene i nodenavnet, og vil som standard vises som "BRNxxxxxxxxxxxx" for et kabelnettverk eller som "BRWxxxxxxxxxxxx" for et trådløst nettverk. ("xxxxxxxxxxxx" er maskinens MAC-adresse / Ethernet-adresse.)

7. Når du klikker på **Neste**, vil Windows® XP og Windows Server® 2003 opprette en forbindelse med URL-en som du anga.
   - Hvis skriverdriveren allerede er installert:

     Du vil se skrivervalgskjermbildet i **Veiviser for skriver**.

     Gå til trinn ⓫.
   - Hvis skriverdriveren IKKE er installert:

     En av fordelene ved IPP-utskriftsprotokollen er at den etablerer modellnavnet til skriveren når du kommuniserer med den. Etter vellykket kommunikasjon vil du se modellnavnet til skriveren automatisk. Dette betyr at du ikke behøver å informere Windows® XP og Windows Server® 2003 om hvilken type skriver som brukes.

     Gå til trinn ❽.

Merk

Hvis skriverdriveren som du installerer ikke har et digitalt sertifikat, vil du se en varselmelding. Klikk på **Fortsett likevel** for å fortsette installasjonen.

8. Klikk på **Har diskett**. Du vil deretter bli bedt om å sette inn skriver-CDen.
9. Klikk på **Bla gjennom** og velg den aktuelle Brother-skriverdriveren som ligger på CDen eller nettverksressursen.
   Klikk på **OK**.
10. Klikk på **OK**.
11. Velg maskinen din og klikk på **OK**.
12. Kryss av **Ja** hvis du vil bruke denne maskinen som standardskriver. Klikk på **Neste**.
13. Klikk på **Fullfør** og maskinen er nå konfigurert og klar til å skrive ut. Skriv ut en testside for å teste skriverforbindelsen.

Windows Vista®, Windows® 7 og Windows Server® 2008

1. (Windows Vista®)
   Klikk på -knappen, **Kontrollpanel**, **Maskinvare og lyd**, og deretter på **Skrivere**.
   (Windows® 7)
   Klikk på -knappen og deretter **Enheter og skrivere**.
   (Windows Server® 2008)
   Klikk på **Start**, **Control Panel** (Kontrollpanel), **Maskinvare og lyd** og deretter på **Printers** (Skrivere).
2. Klikk på **Legg til skriver**.
3. Velg **Legg til en nettverksskriver, trådløs skriver eller Bluetooth-skriver**.
4. Klikk på **Skriveren jeg vil ha er ikke listet**.
5. Velg **Velg en delt skriver, etter navn** og skriv følgende i URL-feltet: "https://maskinens IP-adresse/ipp" (der "maskinens IP-adresse" er maskinens IP-adresse eller nodenavnet).

Merk

- Det er viktig at du bruker "https://" og ikke "http://", ellers vil ikke utskrift over IPP være sikker.
- Hvis du har redigert vertsfilene på datamaskinen eller bruker Domain Name System (DNS), kan du også bruke DNS-navnet til utskriftsserveren. Ettersom utskriftsserveren støtter TCP/IP- og NetBIOS-navn, kan du også bruke NetBIOS-navnet til utskriftsserveren. NetBIOS-navnet vises i Nettverksinnstillingsrapporten. (For informasjon om hvordan du skriver ut Nettverksinnstillingsrapporten, se *Skrive ut Skriverinnstillingsside (for HL-5450DN(T))* ➤➤ side 29 eller *Skrive ut Nettverksinnstillingsrapporten (for andre modeller)* ➤➤ side 29.) NetBIOS-navnet som gis er de 15 første tegnene i nodenavnet, og vil som standard vises som "BRNxxxxxxxxxxxx" for et kabelnettverk eller som "BRWxxxxxxxxxxxx" for et trådløst nettverk. ("xxxxxxxxxxxx" er maskinens MAC-adresse / Ethernet-adresse.)

6. Når du klikker på **Neste** vil Windows Vista® og Windows Server® 2008 opprette en forbindelse med URL-en som du anga.
   - Hvis skriverdriveren allerede er installert:

     Du vil se skrivervalgskjermbildet i veiviseren Legg til skriver. Klikk på **OK**.

     Hvis den aktuelle skriverdriveren allerede er installert på datamaskinen, vil Windows Vista® og Windows Server® 2008 automatisk bruke denne driveren. I så fall vil du ganske enkelt bli spurt om du ønsker å gjøre driveren til standardskriver, og etter dette fullfører driverinstallasjonsveiviseren oppgaven. Du er nå klar til å skrive ut.

     Gå til trinn ⓫.

■ Hvis skriverdriveren IKKE er installert:

En av fordelene ved IPP-utskriftsprotokollen er at den etablerer modellnavnet til skriveren når du kommuniserer med den. Etter vellykket kommunikasjon vil du se modellnavnet til skriveren automatisk. Dette betyr at du ikke behøver å informere Windows Vista® og Windows Server® 2008 om hvilken type skriver som brukes.

Gå til trinn ❼.

7 Hvis maskinen ikke er på listen over støttede skriver, må du klikke på **Har disk**. Du vil deretter bli bedt om å sette inn skriver-CDen.

8 Klikk på **Bla gjennom** og velg den aktuelle Brother-skriverdriveren som ligger på CDen eller nettverksressursen. Klikk på **Åpne**.

9 Klikk på **OK**.

10 Skriv maskinens modellnavn. Klikk på **OK**.

Merk

- Klikk på **Fortsett** når Brukerkontokontroll-skjermbildet vises.
- Hvis skriverdriveren som du installerer ikke har et digitalt sertifikat, vil du se en varselmelding. Klikk på **Installer denne driver programvaren allikevel** for å fortsette installasjonen. **veiviseren for skriverinstallasjon** vil deretter fullføres.

11 Du vil se skjermbildet **Skriv inn et skrivernavn** i veiviseren **Legg til skriver**. Kryss av boksen **Angi som standardskriver** hvis du ønsker å bruke denne maskinen som standardskriver, og klikk deretter på **Neste**.

12 Klikk på **Skriv ut en testside** og deretter på **Fullfør** for å teste skriverforbindelsen. Maskinen er nå konfigurert og klar til å skrive ut.

5 Sende eller motta (for DCP- og MFC-modeller) e-post på en sikker måte

Konfigurasjon med Internett-basert styring (nettleser)

Du kan konfigurere sikker e-postsending med brukerpålitelighetskontroll eller e-postsending og mottak (for DCP- og MFC-modeller) med SSL/TLS på Internett-basert styring-skjermen.

1. Start nettleseren.
2. Skriv inn "http://maskinens IP-adresse/" i nettleseren (der "maskinens IP-adresse" er maskinens IP-adresse).
   - Eksempel:

     http://192.168.1.2/
3. Intet passord kreves som standard. Tast inn et passord hvis du har stilt inn et og trykk på .
4. Klikk på **Network** (Nettverk).
5. Klikk på **Protocol** (Protokoll).
6. Klikk på **Advanced Setting** (Avansert innstilling) for **POP3/SMTP** og sørg for at statusen til **POP3/SMTP** er **Enabled** (Aktiver).
7. Du kan konfigurere **POP3/SMTP**-innstillingene på denne siden.

Merk

- For mer informasjon, se hjelpeteksten i Internett-basert styring.
- Du kan også bekrefte om e-postinnstillingene er korrekte etter konfigurasjon ved å sende en test-e-post.
- Hvis du ikke kjenner POP3/SMTP-serverinnstillingene, kontakter du systemadministratoren eller Internettleverandøren for informasjon.

8. Etter konfigurering, velg **Submit** (Send). Skjermbildet **Test E-mail Send Configuration** (Test konfigurering for sending av e-post) eller **Test E-mail Send/Receive Configuration** (Test konfigurering for sending/mottak av e-post).
9. Følg instruksene på skjermen hvis du vil teste med gjeldende innstillinger.

Sende eller motta (for DCP- og MFC-modeller) e-post på en sikker måte med SSL/TLS

Denne maskinen støtter SSL/TLS-metoder for å sende eller motta (for DCP- og MFC-modeller) e-post via en e-postserver som krever sikker SSL/TLS-kommunikasjonsmetode. For å sende eller motta e-post via en e-postserver som bruker SSL/TLS-kommunikasjon, må du konfigurere SMTP over SSL/TLS eller POP3 over SSL/TLS på riktig måte.

Bekrefte serversertifikat

- Hvis du velger SSL eller TLS for **SMTP over SSL/TLS** eller **POP3 over SSL/TLS**, krysses boksen **Verify Server Certificate** (Bekreft serversertifikat) automatisk av for å bekrefte serversertifikatet.
  - Før du bekrefter serversertifikatet, må du importere CA-sertifikatet som har blitt utstedt av den CA som signerte serversertifikatet. Kontakt din nettverksadministrator eller din Internett-leverandør om hvorvidt en importering av et CA-sertifikat er nødvendig. For å importere sertifikatet, se *Importere og eksporter et CA-sertifikat* ➤➤ side 18.
  - Hvis du ikke må bekrefte serversertifikatet, fjerner du krysset for **Verify Server Certificate** (Bekreft serversertifikat).

Portnummer

- Hvis du velger SSL eller TLS, endres **SMTP Port** (SMTP-port)- eller **POP3 Port** (POP3-port)-verdien slik at den samsvarer med protokollen. Hvis du vil endre portnummeret manuelt, skriver du inn portnummeret etter at du velger **SMTP over SSL/TLS** eller **POP3 over SSL/TLS**.
- Du må konfigurere POP3/SMTP-kommunikasjonsmetoden slik at de samsvarer med e-postserveren. For detaljert informasjon om innstillingene for e-postserveren, tar du kontakt med nettverksadministratoren din eller Internett-leverandøren. I de fleste tilfeller, krever den sikre Internett e-posttjenesten følgende innstillinger:
  - **SMTP**
    - **SMTP-port**: 587
    - **SMTP-serverens autentiseringsmetode**: SMTP-AUTH
    - **SMTP over SSL/TLS**: TLS
  - **POP3**
    - **POP3-port**: 995
    - **POP3 over SSL/TLS**: SSL

6 Feilsøking

Oversikt

Dette kapittelet forklarer hvordan du kan løse typiske nettverksproblemer som du kan møte når du bruker Brother-maskinen. Hvis du etter å ha lest kapittelet fortsatt ikke kan løse problemet, gå til Brother Solutions Center på: (http://solutions.brother.com/).

Gå til Brother Solutions Center på (http://solutions.brother.com/) og klikk på Håndbøker på siden til din modell for å laste ned de andre brukerhåndbøkene.

Identifisere problemet ditt

Sørg for at følgende elementer er konfigurert før du leser dette kapitlet.

Sjekk først følgende:
Strømledningen er riktig koblet til og Brother-maskinen er slått på.
All beskyttende emballasje har blitt fjernet fra maskinen.
Tonerkassettene og trommelenheten er riktig installert.
Front- og bakdeksler er helt lukket.
Papiret er riktig lagt inn i papirmagasinet.
Maskinen din er korrekt koblet til nettverket.

Fra listene under velger du siden med løsningen på ditt problem

- Jeg kan ikke skrive ut dokumentet over Internett med IPPS.

  Se *Jeg kan ikke skrive ut dokumentet over Internett med IPPS.* ➤➤ side 28.

- Jeg vil sjekke at nettverksenhetene mine fungerer ordentlig.

  Se *Jeg vil sjekke at nettverksenhetene mine fungerer ordentlig.* ➤➤ side 28.

Jeg kan ikke skrive ut dokumentet over Internett med IPPS.

Spørsmål	Løsning
Jeg kan ikke kommunisere med min Brother-maskin ved bruk av SSL.	■ Skaff et gyldig sertifikat og installer det på både maskinen og datamaskinen på nytt. ■ Sørg for at port-innstillingen på maskinen er korrekt. Du kan bekrefte maskinens port-innstilling på Internett-basert styring-skjermbildet, ved å klikke på **Protocol** (Protokoll), **Network** (Nettverk) og deretter **HTTP Server Settings** (HTTP-serverinnstillinger).

Jeg vil sjekke at nettverksenhetene mine fungerer ordentlig.

Spørsmål	Løsning
Er Brother-maskinen slått på?	Sørg for at du har bekreftet alle instruksene i *Sjekk først følgende:* ➤➤ side 27.
Hvor finner jeg Brother-maskinens nettverksinnstillinger, som IP-adresse?	Skriv ut Nettverksinnstillingsrapporten. Se *Skrive ut Skriverinnstillingsside (for HL-5450DN(T))* ➤➤ side 29 eller *Skrive ut Nettverksinnstillingsrapporten (for andre modeller)* ➤➤ side 29.

Skrive ut Skriverinnstillingsside (for HL-5450DN(T))

Merk

Nodenavn: Nodenavnet vises i Nettverksinnstillingsrapporten. Standardnodenavnet er "BRNxxxxxxxxxxxx". ("xxxxxxxxxxxx" er maskinens MAC-adresse / Ethernet-adresse.)

Skriverinnstillingsside skriver ut en rapport som viser alle nåværende skriverinnstillinger, inkludert innstillinger for nettverksutskriftsserver.

Du kan skrive ut siden Skriverinnstillinger med knappen **Go** på maskinen.

1. Sørg for at frontdekselet er lukket og at strømledningen er koblet til.
2. Slå på maskinen og vent til maskinen er i driftsklar modus.
3. Trykk tre ganger på **Go** innen 2 sekunder. Maskinen vil skrive ut den gjeldende versjonen av Skriverinnstillingsside.

Skrive ut Nettverksinnstillingsrapporten (for andre modeller)

Merk

Nodenavn: Nodenavnet vises i Nettverksinnstillingsrapporten. Standardnodenavnet er "BRNxxxxxxxxxxxx" for et kablet nettverk eller "BRWxxxxxxxxxxxx" for et trådløst nettverk. ("xxxxxxxxxxxx" er maskinens MAC-adresse / Ethernet-adresse.)

Nettverksinnstillingsrapporten skriver ut en rapport med oversikt over alle de gjeldende nettverkskonfigurasjonene inkludert innstillingene for nettverksutskriftsserveren.

For HL-5470DW(T) og HL-6180DW(T)

1. Trykk på ▲ eller ▼ for å velge `Maskin Info`.
   Trykk på **OK**.
2. Trykk på ▲ eller ▼ for å velge `Skriv nettv.inn.`.
   Trykk på **OK**.

For DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW og MFC-8910DW

1. Trykk på **Menu**.
2. (For MFC-modeller) Trykk på ▲ eller ▼ for å velge `Skriv rapport`.
   (For DCP-modeller) Trykk på ▲ eller ▼ for å velge `Maskin Info`.
   Trykk på **OK**.
3. Trykk på ▲ eller ▼ for å velge `Nettverk Konf.`.
   Trykk på **OK**.
4. Trykk på **Start**.

For DCP-8250DN og MFC-8950DW(T)

1. Trykk på `Meny`.
2. Trykk på ▲ eller ▼ for å vise `Skriv rapport`, og trykk deretter på `Skriv rapport`.
3. Trykk på `Nettverkskonf.`.
4. Trykk på **Start**.

Merk

Hvis **IP Address** i Nettverksinnstillingsrapporten viser **0.0.0.0**, vent ett minutt og prøv igjen.

Nettverkstermer og begreper

Teknisk oversikt over SSL

Secure Socket Layer (SSL) er en metode for å beskytte transportlagdata som sendes over et lokalt eller bredere områdenettverk ved bruk av Internet Printing Protocol (IPP), for å forhindre at uautoriserte brukere kan lese dem.

Den oppnår dette ved å bruke pålitelighetskontrollprotokoller i form av digitale nøkler, som det er 2 av:

- En fellesnøkkel - som kjennes av alle som skriver ut.
- En privatnøkkel - som kun kjennes av maskinen som brukes til å dechiffrere pakker og gjøre dem leselige igjen av maskinen.

Fellesnøkkelen bruker enten 1024-bit eller 2048-bit kryptering og ligger i et digitalt sertifikat. Disse sertifikatene kan enten selvsigneres eller godkjennes av et Certificate Authority (CA).

For det første er det tre forskjellige nøkler, private, felles og delte.

Privatnøkkelen, som kun er kjent av maskinen, er forbundet med fellesnøkkelen, men står ikke i klientenes (sendernes) digitalsertifikater. Når brukeren først etablerer forbindelsen, vil maskinen sende fellesnøkkelen med sertifikatet. Klient-PCen stoler på at fellesnøkkelen er fra maskinen som har sertifikatet. Klienten genererer den delte nøkkelen og krypterer den med fellesnøkkelen, før den sender til maskinen. Maskinen krypterer den delte nøkkelen med privatnøkkelen. Nå deler maskinen og klienten sikkert den delte nøkkelen, og etablerer en trygg forbindelse for overføringer av utskriftsdata.

Utskriftsdataene krypteres og dechiffreres med den delte nøkkelen.

SSL vil ikke hindre at uautoriserte brukere får tilgang til pakker, men vil gjøre dem uleselige uten privatnøkkelen, som ikke røpes til noen utenom maskinen.

Den kan konfigureres på både kablede og trådløse nettverk og vil fungere med andre former for sikkerhet, som for eksempel WPA-nøkler og brannmurer, gitt riktig konfigurasjon.

Nettverkstermer

- Secure Socket Layer (SSL)

  Sikkerhetskommunikasjonsprotokollen krypterer data for å forhindre sikkerhetstrusler.

- Internet Printing Protocol (IPP)

  IPP er en standard utskriftsprotokoll som brukes til å styre og administrere utskriftsjobber. Den kan brukes både lokalt og globalt, slik at det kan skrives ut på samme maskin, samme hvor i verden man befinner seg.

- IPPS

  Versjonen til utskriftsprotokollen Internet Printing Protocol (IPP Version 1.0) som bruker SSL.

- HTTPS

  Versjonen til Internett-protokollen Hyper Text Transfer Protocol (HTTP) som bruker SSL.

- CA (Certificate Authority)

  En CA er en enhet som utsteder digitale sertifikater (spesielt X.509-sertifikater) og garanterer for bindingen mellom dataelementene i et sertifikat.

- CSR (Certificate Signing Request)

  En CSR er en melding som sendes fra en søker til en CA for å kunne søke om utstedelse av et sertifikat. CSR inneholder informasjon som identifiserer søkeren, den offentlige nøkkelen som er generert av søkeren og den digitale signaturen til søkeren.

- Sertifikat

  Et sertifikat er informasjonen som binder sammen en offentlig nøkkel med en identitet. Sertifikatet kan brukes for å bekrefte at en offentlig nøkkel tilhører et individ. Formatet defineres av x.509-standarden.

- Offentlig nøkkelkrypteringssystem

  Et offentlig nøkkelkrypteringssystem er en moderne del av kryptografi hvor algoritmene bruker et par nøkler (en offentlig og en privat nøkkel) og bruker ulike komponenter av paret for ulike trinn i algoritmen.

- Delt nøkkelkrypteringssystem

  Et delt nøkkelkrypteringssystem er en del av kryptografi som involverer algoritmer som bruker samme nøkkel for to ulike trinn av algoritmen (som kryptering og dekryptering).