SSL-guide

(Secure Socket Layer)

För att hitta grundläggande information om nätverket och avancerade nätverksfunktioner för din Brother-maskin: ➤➤ Bruksanvisning för nätverksanvändare.

Den senaste handboken kan du ladda ner från Brother Solutions Center på (http://solutions.brother.com/). På Brother Solutions Center kan du även ladda ner de senaste drivrutinerna och verktygen för din maskin, läsa igenom avsnittet med vanliga frågor och felsökningstips, eller lära dig mer om särskilda utskriftslösningar.

Alla modeller är inte tillgängliga i alla länder.

Version 0

SWE

Gällande modeller

Denna bruksanvisning gäller följande modeller.

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

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

Beskrivning av anmärkningar

Följande ikoner används i den här bruksanvisningen:

Obs	I anmärkningar får du information om hur du ska agera i olika situationer som kan uppstå samt tips på hur en funktion samverkar med andra funktioner.

Varumärken

Brother-logotypen är ett registrerat varumärke som tillhör Brother Industries, Ltd.

Microsoft, Windows, Windows Server och Internet Explorer är antingen registrerade varumärken eller varumärken som tillhör Microsoft Corporation i USA och/eller andra länder.

Windows Vista är antingen ett registrerat varumärke eller ett varumärke som tillhör Microsoft Corporation i USA och/eller andra länder.

För varje företag vars program omnämns i den här bruksanvisningen finns ett licensavtal avseende de upphovsrättsskyddade programmen i fråga.

Alla handelsnamn och produktnamn för företag som visas på Brother-produkter, relaterade dokument och annat material, är alla varumärken eller registrerade varumärken som tillhör respektive företag.

VIKTIGT MEDDELANDE

- Denna produkt är godkänd för användning endast i det land där den köptes. Använd inte denna produkt i något annat land eftersom det kan strida mot lagar för trådlös telekommunikation och energiförbrukning i det landet.
- I denna handbok visas skärmbilderna för MFC-8950DW(T) om inte annat anges.
- I det här dokumentet står Windows® XP för Windows® XP Professional, Windows® XP Professional x64 Edition och Windows® XP Home Edition.
- I det här dokumentet står Windows Server® 2003 för Windows Server® 2003 och Windows Server® 2003 x64 Edition.
- I det här dokumentet står Windows Server® 2008 för Windows Server® 2008 och Windows Server® 2008 R2.
- Windows Vista® i detta dokument representerar alla versioner av Windows Vista®.
- Windows® 7 i detta dokument representerar alla versioner av Windows® 7.
- Gå till Brother Solutions Center på http://solutions.brother.com/ och klicka Bruksanvisningar på sidan för din modell för att ladda ner övriga handböcker.

Innehållsförteckning

1 Introduktion

Översikt

SSL (Secure Socket Layer) är en effektiv metod för att skydda data som skickas över ett lokalt eller utbrett nätverk. Data som skickas över nätverket t.ex. ett utskriftsjobb krypteras och de som försöker, kan inte läsa den eftersom all data krypteras.

Detta kan konfigureras för både trådbundna och trådlösa nätverk och fungerar med annan typ av skydd som t.ex. WPA-nycklar och brandväggar.

Kort historik gällande SSL

SSL skapades ursprungligen för att skydda information på Internet, speciellt data som skickas mellan webbläsare och servrar. Om du t.ex. använder Internet Explorer® för bankärenden på Internet och du ser https:// och det lilla hänglåset i din webbläsare använder du SSL. Det växte sedan till att fungera med andra program som t.ex. Telnet, skrivare och FTP-programvara till att bli en universell lösning säkerheten online. Konstruktionens ursprungliga syfte används fortfarande idag av många återförsäljare och banker online för att skydda känslig data som t.ex. kreditkortsnummer, kundregister osv.

SSL använder extremt hög krypteringsnivå och har bankernas förtroende över hela världen eftersom den troligtvis aldrig kommer att knäckas.

Fördelarna med att använda SSL

Den oöverträffade fördelen med att använda SSL på Brother-maskiner är att det ger en säker utskrift över IP-nätverk genom att begränsa obehöriga användare från att kunna läsa data som skickas till maskinen. Dess huvudsakliga säljargument är att det kan användas för att skriva ut konfidentiell information på ett säkert sätt. Personalavdelningen på ett stort företag skriver t.ex. kanske regelbundet ut lönebesked. Informationen som finns på dessa lönebesked kan, utan kryptering, läsas av en annan nätverksanvändare. Med SSL, kommer däremot den som försöker hämta informationen endast att se en konstig sida med koder och inte det verkliga lönebeskedet.

Använda certifikat för enhetssäkerhet

Din Brother-maskin stödjer användning av flera säkerhetscertifikat vilket leder till säker hantering, autentisering och kommunikation med maskinen. Följande funktioner inom säkerhetscertifikat kan användas med maskinen. När du skriver ut ett dokument eller använder webbaserad hantering (webbläsare) på ett säkert sätt med SSL, måste du installera certifikatet på din dator. Se *Installation av digitalt certifikat* ➤➤ sidan 4.

- SSL/TLS-kommunikation
- SSL-kommunikation för SMTP/POP3

Brother-maskinen stöder följande certifikat.

- Förinstallerat certifikat

  Det finns ett förinstallerat självsignerat certifikat på din dator.

  Med hjälp av det certifikatet kan du enkelt använda SSL/TLS-kommunikation utan att du behöver skapa eller installera ett certifikat. Om du vill använda din maskins funktion Google Cloud Print, kan du använda det förinstallerade certifikatet för att konfigurera inställningarna för Google Cloud Print på ett säkert sätt. Mer information om Google Cloud Print finns hos Brother Solutions Center på http://solutions.brother.com/ där du klickar på Bruksanvisningar på sidan för din modell för att ladda ner Guide för Google Cloud Print.

Obs

Det förinstallerade självsignerade certifikatet kan inte skydda från intrång i din kommunikation. Vi rekommenderar att du använder ett certifikat som utfärdats av en pålitlig organisation för ett bättre skydd.

- Självsignerat certifikat

  Den här skrivarservern kan utfärda ett eget certifikat. Med hjälp av det certifikatet kan du enkelt använda SSL/TLS-kommunikation utan att du behöver ett certifikat från en CA. (se *Skapa ett självsignerat certifikat* ➤➤ sidan 6).

- Certifikat från en CA

  Det finns två metoder för att installera ett certifikat från en CA. Om du redan har ett certifikat från en CA eller om du vill använda ett certifikat från en extern, betrodd CA:

  - När du använder ett CSR-meddelande (Certificate Signing Request) från skrivarservern. (se *Skapa en CSR (Certificate Signing Request)* ➤➤ sidan 7).
  - När du importerar ett certifikat och en privat nyckel. (se *Importera och exportera certifikat och privat nyckel* ➤➤ sidan 17).

■ CA-certifikat

Om du använder ett CA-certifikat som självt identifierar CA:n (Certificate Authority) måste du importera ett CA-certifikat från CA:n innan du konfigurerar. (se *Importera och exportera ett CA-certifikat* ➤➤ sidan 18).

Obs

- Om du tänker använda SSL/TLS-kommunikation rekommenderar vi att du först kontaktar din systemadministratör.
- När du återställer skrivarserverns fabriksinställningar raderas det certifikat och den privata nyckel som finns installerade. Om du vill behålla certifikatet och den privata nyckeln efter att du återställt skrivarservern måste du exportera dem innan du återställer och sedan installera dem igen. (se *Importera det självsignerade certifikatet, certifikatet utfärdat av CA och den privata nyckeln* ➤➤ sidan 17).

2 Digitalt certifikat för SSL-kommunikation

Installation av digitalt certifikat

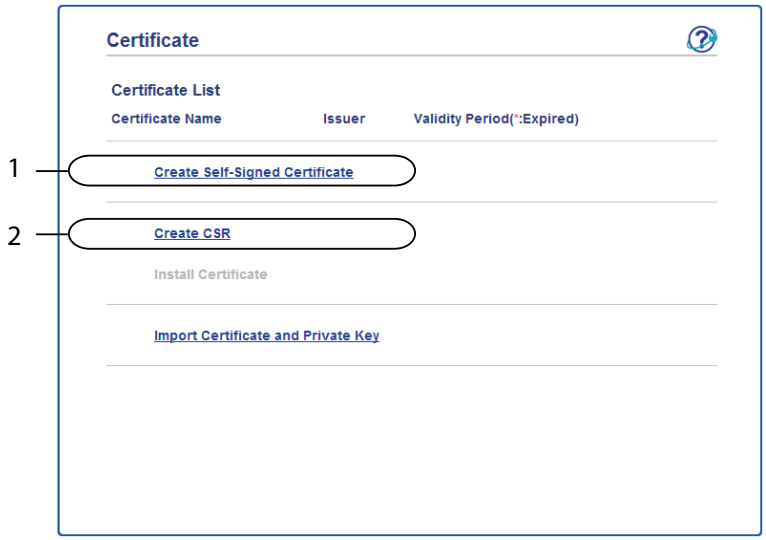
Att skriva ut över ett säkert nätverk eller säker hantering med webbaserad hantering (webbläsare) kräver att ett digitalt certifikat installeras på både maskinen och enheten som skickar information till maskinen, t.ex. en dator. Din maskin har ett förinstallerat certifikat. För att kunna konfigurera certifikatet måste användaren logga in på maskinen på distans via en webbläsare med IP-adressen.

Obs

Vi rekommenderar Windows® Internet Explorer® 7.0/8.0 eller Firefox® 3.6 för Windows® och Safari 4.0/5.0 för Macintosh. Se alltid till att ha JavaScript och cookies aktiverade, oavsett vilken webbläsare du använder. Om en annan webbläsare används måste du kontrollera att den är kompatibel med HTTP 1.0 och HTTP 1.1.

1. Starta webbläsaren.
2. Ange ”http://maskinens IP-adress/” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress eller skrivarserverns namn).
   - Till exempel: http://192.168.1.2/
3. Lösenord krävs inte som standard. Om du tidigare har ställt in ett lösenord ska du ange det och trycka på  .
4. Klicka på **Network** (Nätverk).
5. Klicka på **Security** (Säkerhet).
6. Klicka på **Certificate** (Certifikat).

7 Du kan konfigurera certifikatinställningarna.
För att skapa ett självsignerat certifikat med webbaserad hantering, gå till *Skapa ett självsignerat certifikat* ➤➤ sidan 6.
För att skapa en CSR (Certificate Signing Request), gå till *Skapa en CSR (Certificate Signing Request)* ➤➤ sidan 7.



1 Skapa och installera ett självsignerat certifikat

2 Använda ett certifikat från en CA (Certificate Authority)

Obs

- De funktioner som är gråtonade och inte länkade är inte tillgängliga.
- Mer information om konfigurering finns i hjälptexten för webbaserad hantering.

Skapa ett självsignerat certifikat

1. Klicka på **Create Self-Signed Certificate** (Skapa självsignerat certifikat).
2. Ange **Common Name** (Gemensamt namn) och **Valid Date** (Giltighetsdatum).

Obs

- Längden på **Common Name** (Gemensamt namn) måste vara kortare än 64 tecken. Ange ett ID som t.ex. en IP-adress, ett nodnamn eller domännamn som ska användas för åtkomst till maskinen med SSL/TSL-kommunikation. Nodnamnet visas som standard.
- En varning visas om du använder IPPS- eller HTTPS-protokollet och anger ett annat namn i adressfältet än det **Common Name** (Gemensamt namn) som användes för det självsignerade certifikatet.

3. Du kan välja inställningarna **Public Key Algorithm** (Algoritm med offentlig nyckel) och **Digest Algorithm** (Algoritmsammandrag) i rullgardinslistan. Standardinställningarna är **RSA(2048bit)** (RSA (2048-bitars)) för **Public Key Algorithm** (Algoritm med offentlig nyckel) och **SHA256** för **Digest Algorithm** (Algoritmsammandrag).
4. Klicka på **Submit** (Skicka).
5. Nu skapas och sparas det självsignerade certifikatet i maskinens minne.

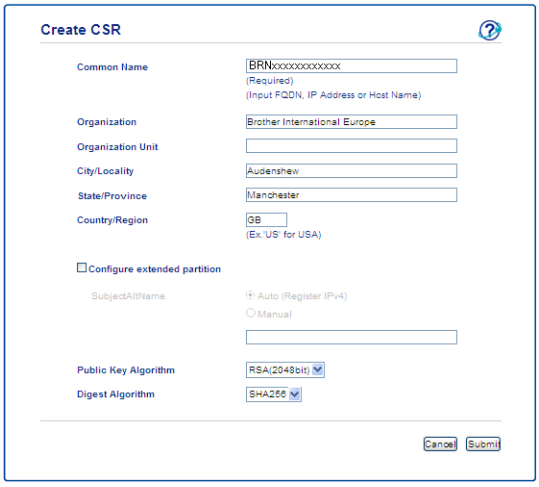
Skapa en CSR (Certificate Signing Request)

En CSR (Certificate Signing Request) är en förfrågan som skickas till en CA för att verifiera kreditiven i certifikatet.

Obs

Vi rekommenderar att du installerar rotcertifikatet från CA innan du skapar CSR-begäran.

1. Klicka på **Create CSR** (Skapa CSR).
2. Ange ett **Common Name** (Gemensamt namn) och din information, som t.ex. **Organization** (Organisation).
   Din företagsinformation krävs för att en CA ska kunna bekräfta din identitet och attestera den för världen.



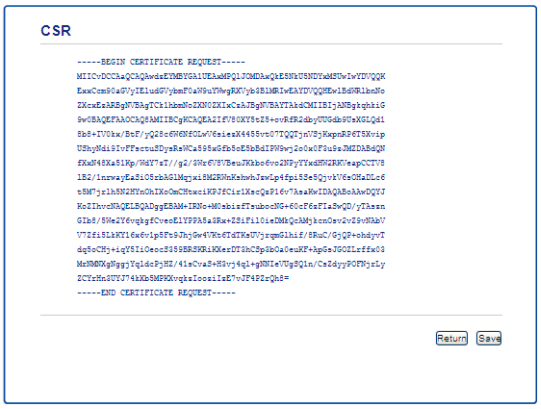
Obs

- Längden på **Common Name** (Gemensamt namn) måste vara kortare än 64 tecken. Ange ett ID som t.ex. en IP-adress, ett nodnamn eller domännamn som ska användas för åtkomst till maskinen med SSL/TSL-kommunikation. Nodnamnet visas som standard. **Common Name** (Gemensamt namn) krävs.
- Ett varningsmeddelande visas om du anger ett annat namn i webbadressfältet än det vanliga namn som användes för certifikatet.
- Längden på **Organization** (Organisation), **Organization Unit** (Organisationsenhet), **City/Locality** (Stad/Ort) och **State/Province** (Delstat/Provins) måste vara kortare än 64 tecken.
- **Country/Region** (Land/Region) ska vara en landskod enligt ISO 3166 bestående av två tecken.
- Om du konfigurerar certifikatförlängningen X.509v3 markerar du kryssrutan **Configure extended partition** (Konfigurera utökad del) och väljer sedan **Auto (Register IPv4)** (Auto (Register IPv4)) eller **Manual**.

3 Du kan välja inställningarna **Public Key Algorithm** (Algoritm med offentlig nyckel) och **Digest Algorithm** (Algoritmsammandrag) i rullgardinslistan. Standardinställningarna är **RSA(2048bit)** (RSA (2048-bitars)) för **Public Key Algorithm** (Algoritm med offentlig nyckel) och **SHA256** för **Digest Algorithm** (Algoritmsammandrag).

4 Klicka på **Submit** (Skicka). Följande skärmbild visas.

5 Efter några sekunder visas certifikatet, som kan sparas i en liten fil eller kopieras och klistras in direkt i ett CSR-formulär som en CA har. Klicka på **Save** (Spara) för att spara CSR-filen på din dator.



Obs

Följ den CA-policy som gäller för att skicka en CSR till din CA.

6 Du har nu skapat en CSR. Gå till *Så här installerar du certifikatet på maskinen* ➤➤ sidan 9 för mer information om hur du installerar certifikatet på din maskin.

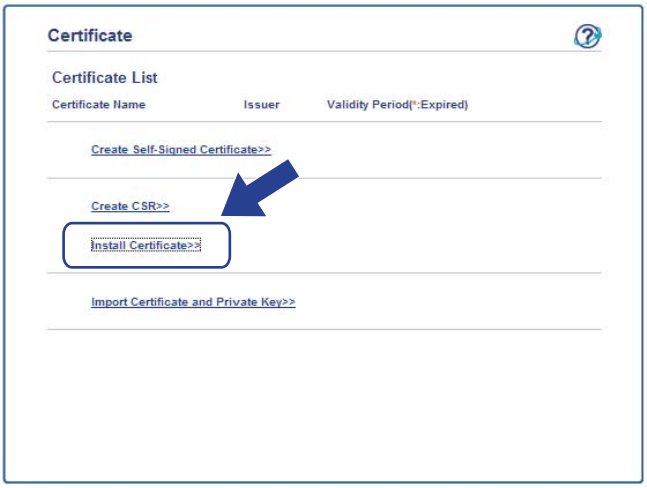
Så här installerar du certifikatet på maskinen

När du får ett certifikat från en CA installerar du det på skrivarservern genom att följa stegen nedan.

Obs

Endast ett certifikat utfärdat med den här maskinens CSR kan installeras. När du vill skapa ytterligare en CSR, se till att certifikatet är installerat innan du skapar ytterligare en CSR. Skapa ytterligare en CSR sedan du har installerat certifikatet på maskinen. I annat fall blir den CSR du gjorde innan du installerade ogiltig.

1. Klicka på **Install Certificate** (Installera certifikat) på sidan **Certificate** (Certifikat) page.



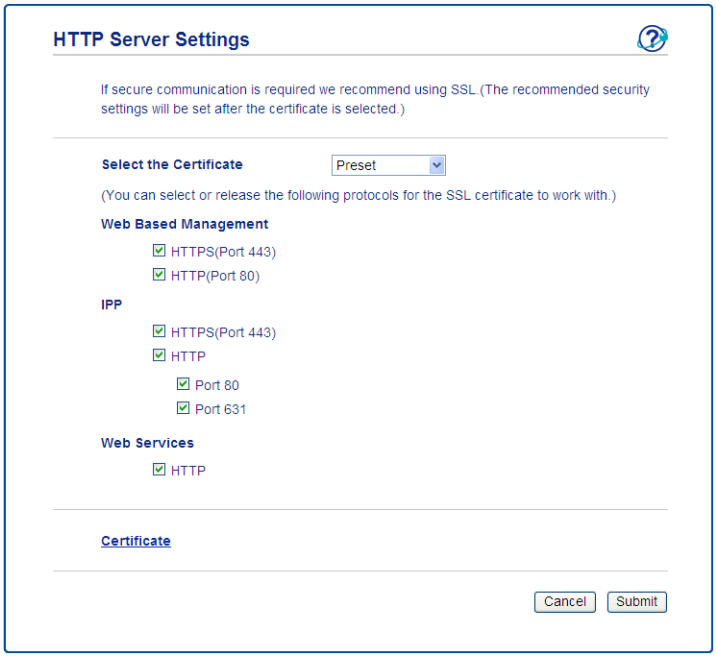
2. Ange filen för det certifikat som har utfärdats av en CA och klicka sedan på **Submit** (Skicka).

3. Nu har certifikatet skapats och sparats i maskinens minne.
För att du ska kunna använda SSL/TLS-kommunikation måste rotcertifikatet från din CA även installeras på din dator. Kontakta din nätverksadministratör angående den installationen.
Du har konfigurerat det digitala certifikatet. Om du vill skicka eller ta emot e-post med SSL, se *Sända eller Ta emot (för DCP- och MFC-modeller) ett e-postmeddelande på ett säkert sätt* ➤➤ sidan 25 för nödvändiga konfigureringssteg.

Välja certifikatet

Följ stegen nedan när du installerat certifikatet för att välja det certifikat du vill använda.

1. Klicka på **Network** (Nätverk).
2. Klicka på **Protocol** (Protokoll).
3. Klicka på **HTTP Server Settings** (Inställningar för HTTP-server) och välj sedan certifikatet från rullgardinsmenyn **Select the Certificate** (Välj certifikatet).



Obs

- Om följande dialogruta dyker upp rekommenderar Brother att du avaktiverar Telnet-, FTP-, TFTP-protokollen och nätverkshanteringen med äldre versioner av BRAdmin Professional (2,8 eller tidigare) för en säker kommunikation. Användarautentiseringen blir inte säker om du aktiverar dem.

- För DCP- och MFC-modeller:

  Om du avaktiverar FTP, avaktiveras funktionen Skanna till FTP.

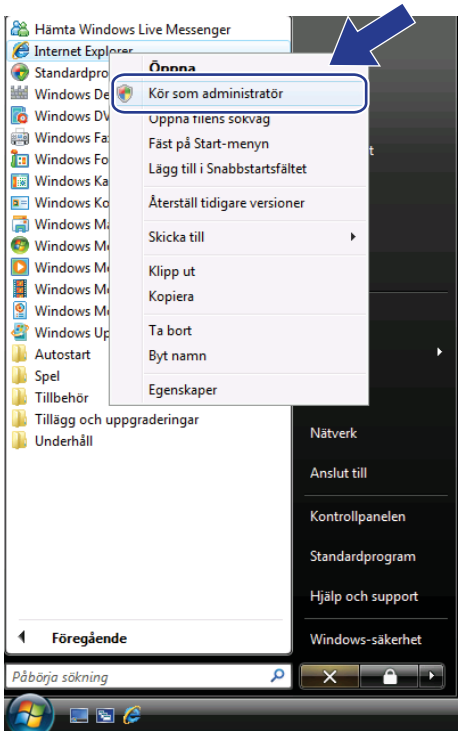
4 Klicka på **Submit** (Skicka).

Installera det självsignerade certifikatet eller förinstallerade certifikatet för användare av Windows Vista®, Windows® 7 och Windows Server® 2008 som har administratörsrättigheter

Obs

- Följande steg är avsedda för Windows® Internet Explorer®. Om du använder en annan webbläsare följer du webbläsarens hjälptext.
- Du måste ha administratörsrättigheter för att installera det självsignerade certifikatet eller det förinstallerade certifikatet.

1. Klicka på -knappen och sedan på **Alla program**.
2. Högerklicka på **Internet Explorer** och klicka sedan på **Kör som administratör**.



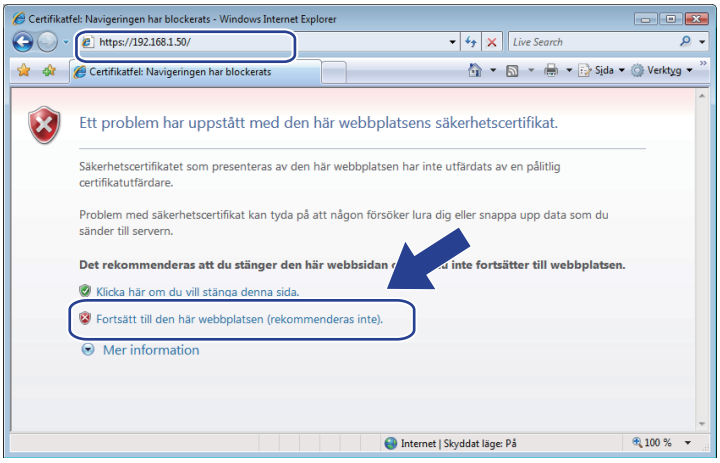
Obs

Om skärmen **Kontroll av användarkonto** visas,

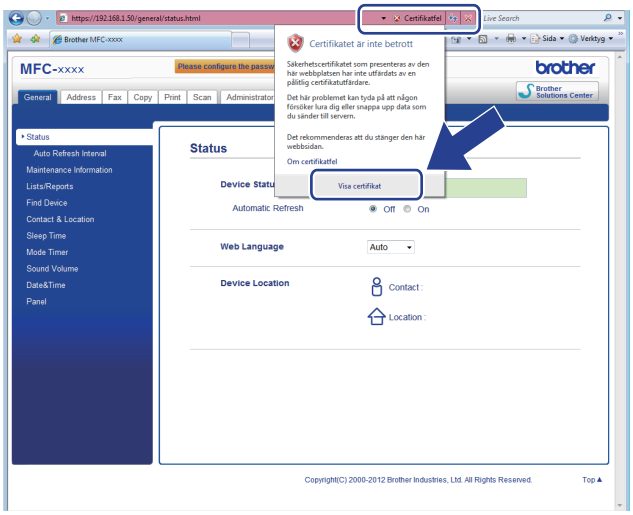
(Windows Vista®), klickar du på **Fortsätt (Tillåt)**.

(Windows® 7) Klicka på **Ja**.

c Ange ”https://maskinens IP-adress/” i webbläsaren för att komma åt maskinen (där ”maskinens IP-adress” är maskinens IP-adress eller nodnamn som du tilldelat certifikatet).
Klicka sedan på **Fortsätt till den här webbplatsen (rekommenderas inte).**.

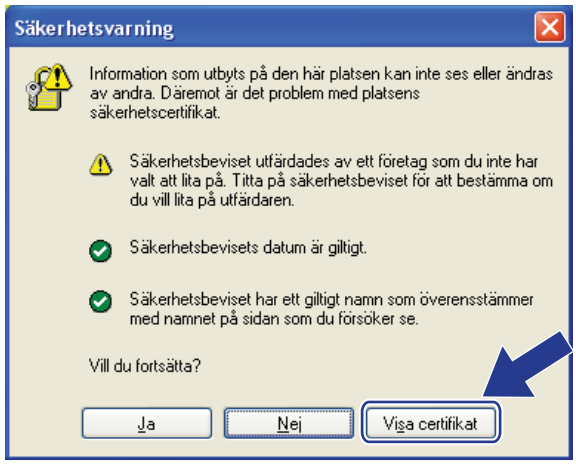


d Klicka på **Certifikatfel** och klicka sedan på **Visa certifikat**. För resten av instruktionerna följer du stegen från ❹ under *Installera det självsignerade certifikatet eller det förinstallerade certifikatet åt användare med Windows® XP och Windows Server® 2003* ➤➤ sidan 14.



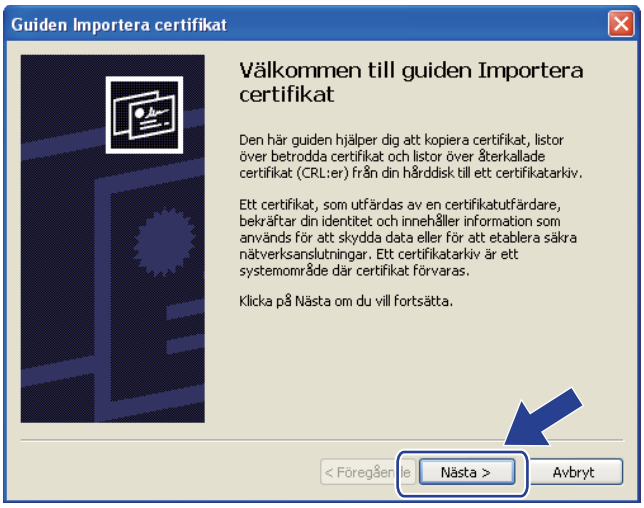
Installera det självsignerade certifikatet eller det förinstallerade certifikatet åt användare med Windows® XP och Windows Server® 2003

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress/” i webbläsaren för att komma åt maskinen (där ”maskinens IP-adress” är IP-adressen eller nodnamnet som du tilldelat certifikatet).
3. När dialogrutan med säkerhetsmeddelandet visas, gör något av följande:
   - Klicka på **Fortsätt till den här webbplatsen (rekommenderas inte).**. Klicka på **Certifikatfel** och klicka sedan på **Visa certifikat**.
   - Om följande dialogruta visas klickar du på **Visa certifikat**.



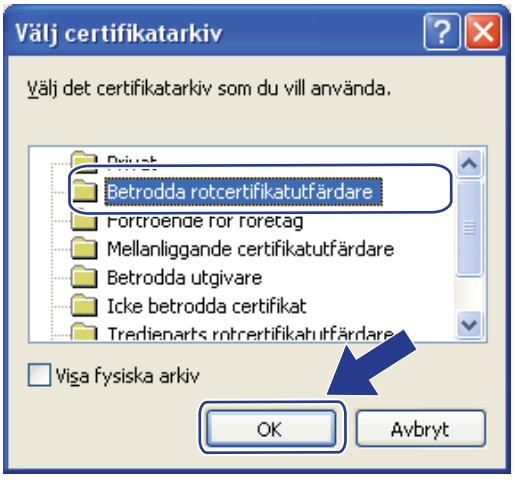
4. Välj **Installera certifikat...** från fliken **Allmänt**.

5 När **Guiden Importera certifikat** visas klickar du på **Nästa**.

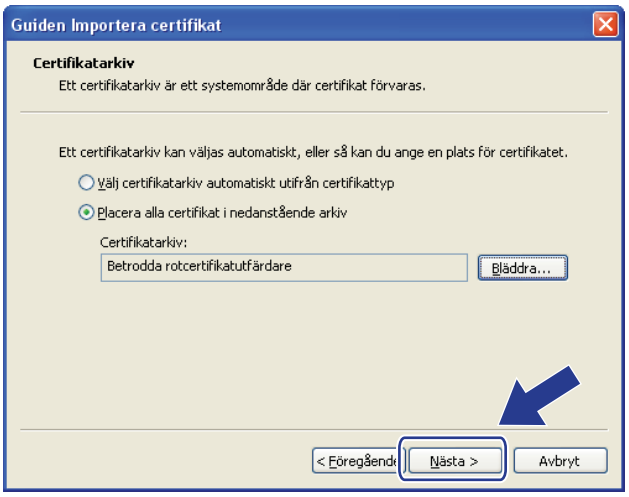


6 Du måste ange en plats där certifikatet ska installeras. Vi rekommenderar att du väljer **Placera alla certifikat i nedanstående arkiv** och sedan klickar på **Bläddra...**.

7 Välj **Betrodda rotcertifikatutfärdare** och klicka sedan på **OK**.



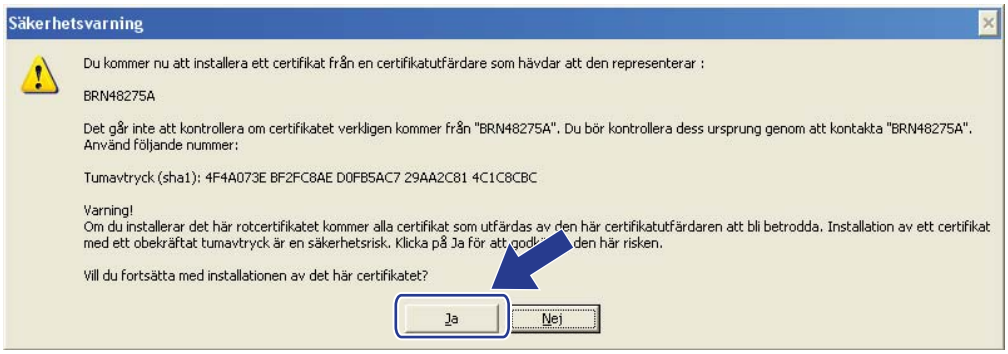
8 Klicka på **Nästa**.



9 Klicka på **Slutför** på nästa skärmbild.

10 Du blir sedan ombedd att installera certifikatet.
Gör ett av följande:

- Om du installerar det självsignerade certifikatet, bekräfta ditt fingeravtryck (tumavtryck) och klicka sedan på **Ja**.
- Klicka på **Ja** om du installerar det förinstallerade certifikatet.



Obs

- Fingeravtrycket (tumavtryck) skrivs ut på nätverkskonfigurationslistan för det självsignerade certifikatet. Information om hur du skriver ut nätverkskonfigurationslistan finns i *Skriva ut sidan med skrivarinställningar (för HL-5450DN(T))* ➤➤ sidan 29 eller *Skriva ut nätverkskonfigurationsrapport (för andra modeller)* ➤➤ sidan 29.
- Fingeravtrycket skrivs inte ut på nätverkskonfigurationslistan för det förinstallerade certifikatet.

11 Klicka på **OK**.

12 Nu är det självsignerade certifikatet eller förinstallerade certifikatet installerat på din dator och du kan använda SSL/TLS-kommunikation.

Du måste göra samma sak för alla datorer du vill skriva ut säkert med. När det väl har installerats behöver du inte upprepa stegen om inte certifikatet ändras.

Importera och exportera certifikat och privat nyckel

Du kan spara certifikatet och den privata nyckeln på maskinen och hantera dem genom att importera och exportera.

Importera det självsignerade certifikatet, certifikatet utfärdat av CA och den privata nyckeln

1. Klicka på **Import Certificate and Private Key** (Importera certifikat och privat nyckel) på sidan **Certificate** (Certifikat) page.
2. Specificera den fil du vill importera.
3. Ange lösenordet om filen är krypterad och klicka sedan på **Submit** (Skicka).
4. Certifikatet och den privata nyckeln har nu importerats till maskinen.

Exportera det självsignerade certifikatet, certifikatet utfärdat av CA och den privata nyckeln

1. Klicka på **Export** (Exportera) som visas med **Certificate List** (Certifieringslista) på sidan **Certificate** (Certifikat).
2. Ange ett lösenord om du vill kryptera filen.

Obs

Om du lämnar lösenordsfältet tomt krypteras inte filen.

3. Ange lösenordet en gång till för att bekräfta det och klicka sedan på **Submit** (Skicka).
4. Specificera den plats du vill spara filen på.
5. Certifikatet och den privata nyckeln har nu exporterats till datorn.

Importera och exportera ett CA-certifikat

Du kan spara ett CA-certifikat på maskinen genom att importera och exportera.

Importera ett CA-certifikat

1. Klicka på **CA Certificate** (CA-certifikat) på sidan **Security** (Säkerhet) page.
2. Klicka på **Import CA Certificate** (Importera CA-certifikat) och välj certifikatet. Klicka på **Submit** (Skicka).

Exportera ett CA-certifikat

1. Klicka på **CA Certificate** (CA-certifikat) på sidan **Security** (Säkerhet) page.
2. Välj det certifikat som du vill exportera och klicka på **Export** (Exportera). Klicka på **Submit** (Skicka).
3. Klicka på **Save** (Spara) för att välja målmappen.
4. Välj den målmapp där du vill spara det exporterade certifikatet och spara sedan certifikatet.

Hantera flera certifikat

Med denna funktion för flera certifikat kan du hantera varje certifikat som du har installerat med webbaserad hantering. När certifikaten har installerats kan du visa vilka certifikat som finns installerade på sidan **Certificate** (Certifikat) och sedan visa respektive certifikats innehåll och radera eller exportera certifikatet. Mer information om hur du öppnar sidan **Certificate** (Certifikat) finns på *Installation av digitalt certifikat* ➤➤ sidan 4.

- För skrivarmodeller

  Med Brother-maskinen kan du spara högst tre självsignerade certifikat eller högst tre certifikat som utfärdats av en CA. Du kan använda de sparade certifikaten när du använder HTTPS/IPPS-protokollet eller autentisering med IEEE 802.1x.

- För DCP- och MFC-modeller

  Med Brother-maskinen kan du spara högst fyra självsignerade certifikat eller högst fyra certifikat som utfärdats av en CA. Du kan använda de sparade certifikaten när du använder HTTPS/IPPS-protokollet, autentisering med IEEE 802.1x eller en signerad PDF.

Du kan också spara högst fyra CA-certifikat till när du använder autentisering med IEEE 802.1x och SSL för SMTP/POP3.

Vi rekommenderar att du sparar ett certifikat mindre och håller det sista ledigt för att hantera certifikaten när de går ut. Om du till exempel vill spara ett CA-certifikat, spara tre certifikat och lämna en som reserv. Vid återutfärdande av certifikatet, till exempel när certifikatet har gått ut, kan du importera ett nytt certifikat som reserv och sedan kan du radera det utgångna certifikatet så att det inte blir fel på konfigurationen.

Obs

- När du använder HTTPS/IPPS, IEEE 802.1x eller signerad PDF (för DCP- och MFC-modeller) måste du välja vilket certifikat du använder.
- När du använder SSL för SMTP-/POP3- kommunikationer (för DCP- och MFC-modeller) behöver du inte välja certifikatet. Det nödvändiga certifikatet väljs automatiskt.

3 Hantera nätverksmaskinen säkert med SSL/TLS

För att kunna hantera nätverksmaskinen säkert måste du använda hanteringsverktyg med säkerhetsprotokoll.

Säker webbaserad hantering (webbläsare)

Vi rekommenderar att du använder HTTPS-protokoll för säker hantering. Dessa protokoll kräver följande maskininställningar.

Obs

- HTTPS-protokollet aktiveras som standard.

  Du kan ändra inställningarna för HTTPS-protokollet och det certifikat som ska användas på skärmen för webbaserad hantering genom att klicka på **Network** (Nätverk), **Protocol** (Protokoll) och sedan på **HTTP Server Settings** (Inställningar för HTTP-server).

- Du måste också installera det certifikat du installerade på maskinen på din dator. Se *Installera det självsignerade certifikatet eller förinstallerade certifikatet för användare av Windows Vista®, Windows® 7 och Windows Server® 2008 som har administratörsrättigheter* ➤➤ sidan 12 eller *Installera det självsignerade certifikatet eller det förinstallerade certifikatet åt användare med Windows® XP och Windows Server® 2003* ➤➤ sidan 14.

1. Starta webbläsaren.
2. Skriv in ”https://maskinens IP-adress/” i din webbläsare. (Om du använder det certifikat som skapats skriver du ”https://Common Name/” i din webbläsare. Där är ”Common Name” det namn som du tilldelat certifikatet, t.ex. en IP-adress, ett nodnamn eller ett domännamn. För information om hur du tilldelar certifikatet ett Common Name, se *Använda certifikat för enhetssäkerhet* ➤➤ sidan 2.)

   ■ Till exempel:

   https://192.168.1.2/ (om Common Name är maskinens IP-adress)
3. Lösenord krävs inte som standard. Ange ett lösenord om du har ställt in ett sådant och tryck på .

4 Säker dokumentutskrift med SSL

Säker dokumentutskrift med IPPS för Windows®

Vi rekommenderar att du använder IPPS-protokoll för säker hantering. IPPS-protokollet kräver följande maskininställningar.

Obs

- Kommunikation med IPPS kan inte förhindra obehörig åtkomst till skrivarservern.
- Du måste också installera det certifikat du installerade på maskinen på din dator. Se *Installera det självsignerade certifikatet eller förinstallerade certifikatet för användare av Windows Vista®, Windows® 7 och Windows Server® 2008 som har administratörsrättigheter* ➤➤ sidan 12 eller *Installera det självsignerade certifikatet eller det förinstallerade certifikatet åt användare med Windows® XP och Windows Server® 2003* ➤➤ sidan 14.
- IPPS-protokollet måste vara aktiverat. Standardinställningen är aktiverat. Du kan ändra inställningarna för IPPS-protokollet och det certifikat som ska användas på skärmen för webbaserad hantering genom att klicka på **Network** (Nätverk), **Protocol** (Protokoll) och sedan på **HTTP Server Settings** (Inställningar för HTTP-server).

Windows® XP och Windows Server® 2003

1. Klicka på **Start** och välj **Skrivare och fax**.
2. Klicka på **Lägg till en skrivare** för att starta **Guiden Lägg till skrivare**.
3. Klicka på **Nästa** när du ser skärmen **Välkommen till guiden Lägg till skrivare**.
4. Välj **En nätverksskrivare eller skrivare som är ansluten till en annan dator**.
5. Klicka på **Nästa**.
6. Välj **Anslut till en skrivare på Internet eller i hem- eller kontorsnätverket** och ange sedan följande i webbadressfältet:
   ”https://maskinens IP-adress/ipp” (där ”maskinens IP-adress” är maskinens IP-adress eller nodnamn.)

Obs

- Det är viktigt att du använder ”https://” och inte ”http://” annars blir utskriften över IPP inte säker.
- Om du har redigerat värdfilen på din dator eller använder DNS (Domain Name System) kan du också skriva in skrivarserverns DNS-namn. Eftersom skrivarservern stöder TCP/IP och NetBIOS, kan även skriva in skrivarserverns NetBIOS-namn. NetBIOS-namnet hittar du i nätverkskonfigurationslistan. (Information om hur du skriver ut nätverkskonfigurationslistan finns i *Skriva ut sidan med skrivarinställningar (för HL-5450DN(T))* ➤➤ sidan 29 eller *Skriva ut nätverkskonfigurationsrapport (för andra modeller)* ➤➤ sidan 29.) NetBIOS-namnet som tilldelas är de 15 första tecknen av nodnamnet och i standard visas det som ”BRNxxxxxxxxxxxx” för ett trådbundet nätverk eller ”BRWxxxxxxxxxxxx” för ett trådlöst nätverk. (”xxxxxxxxxxxx” är din maskins MAC-adress/Ethernet-adress.)

7 När du klickar på **Nästa** ansluter Windows® XP och Windows Server® 2003 till den angivna webbadressen.

- Om skrivardrivrutinen redan har installerats:

  Skärmen för val av skrivare visas i **Guiden Lägg till skrivare**.

  Gå till steg ⓫.

- Om skrivardrivrutinen INTE har installerats:

  En av fördelarna med utskriftsprotokollet IPP är att det identifierar skrivarens modellnamn när du kommunicerar med den. När kommunikationen fungerar visas skrivarens modellnamn automatiskt.

  Detta innebär att du inte behöver tala om för Windows® XP och Windows Server® 2003 vilken typ av skrivardrivrutin som ska användas.

  Gå till steg ❽.

Obs

Om den skrivardrivrutin som du installerar inte har ett digitalt certifikat visas ett varningsmeddelande. Klicka på **Fortsätt ändå** för att fortsätta med installationen.

8 Klicka på **Diskett finns**. Du blir då ombedd att sätta i skivan med skrivardrivrutinen.

9 Klicka på **Bläddra** och välj rätt Brotherskrivardrivrutin som finns på cd-skivan eller nätverksresursen. Klicka på **OK**.

10 Klicka på **OK**.

11 Välj din maskin och klicka på **OK**.

12 Markera **Ja** om du vill använda denna maskin som standardskrivare. Klicka på **Nästa**.

13 Klicka på **Slutför** och maskinen är nu konfigurerad och redo att skriva ut. Skriv ut en testsida för att testa skrivaranslutningen.

Windows Vista®, Windows® 7 och Windows Server® 2008

1. (Windows Vista®)
   Klicka på -knappen, **Kontrollpanelen**, **Maskinvara och ljud** och därefter **Skrivare**.
   (Windows® 7)
   Klicka på -knappen och sedan på **Enheter och skrivare**.
   (Windows Server® 2008)
   Klicka på **Start**, **Kontrollpanelen**, **Maskinvara och ljud** och sedan **Skrivare**.
2. Klicka på **Lägg till en skrivare**.
3. Välj **Lägg till en nätverksskrivare, trådlös skrivare eller Bluetooth-skrivare**.
4. Klicka på **Skrivaren jag vill använda finns inte med i listan**.
5. Välj **Välj en delad skrivare efter namm** och ange sedan följande i webbadressfältet:
   ”https://maskinens IP-adress/ipp” (där ”maskinens IP-adress” är maskinens IP-adress eller nodnamn.)

Obs

- Det är viktigt att du använder ”https://” och inte ”http://” annars blir utskriften över IPP inte säker.
- Om du har redigerat värdfilen på din dator eller använder DNS (Domain Name System) kan du också skriva in skrivarserverns DNS-namn. Eftersom skrivarservern stöder TCP/IP och NetBIOS, kan även skriva in skrivarserverns NetBIOS-namn. NetBIOS-namnet hittar du i nätverkskonfigurationslistan. (Information om hur du skriver ut nätverkskonfigurationslistan finns i *Skriva ut sidan med skrivarinställningar (för HL-5450DN(T))* ➤➤ sidan 29 eller *Skriva ut nätverkskonfigurationsrapport (för andra modeller)* ➤➤ sidan 29.) NetBIOS-namnet som tilldelas är de 15 första tecknen av nodnamnet och i standard visas det som ”BRNxxxxxxxxxxxx” för ett trådbundet nätverk eller ”BRWxxxxxxxxxxxx” för ett trådlöst nätverk. (”xxxxxxxxxxxx” är din maskins MAC-adress/Ethernet-adress.)

6. När du klickar på **Nästa** ansluter Windows Vista® och Windows Server® 2008 till den angivna webbadressen.
   - Om skrivardrivrutinen redan har installerats:

     Skärmen för val av skrivare visas i guiden Lägg till skrivare. Klicka på **OK**.

     Om passande skrivardrivrutin redan installerats på din dator kommer Windows Vista® och Windows Server® 2008 automatiskt att använda den drivrutinen. Om så är fallet blir du bara tillfrågad om du vill göra drivrutinen till standardskrivare och därefter slutförs guiden Installera drivrutin. Du kan nu skriva ut.

     Gå till steg ⓫.

■ Om skrivardrivrutinen INTE har installerats:

En av fördelarna med utskriftsprotokollet IPP är att det identifierar skrivarens modellnamn när du kommunicerar med den. När kommunikationen fungerar visas skrivarens modellnamn automatiskt. Detta innebär att du inte behöver tala om för Windows Vista® eller Windows Server® 2008 vilken typ av skrivardrivrutin som ska användas.

Gå till steg ❼.

7 Om din maskin inte finns med på listan över skrivare som stöds klickar du på **Disk finns**. Du blir då ombedd att sätta i skivan med skrivardrivrutinen.

8 Klicka på **Bläddra** och välj rätt Brotherskrivardrivrutin som finns på cd-skivan eller nätverksresursen. Klicka på **Öppna**.

9 Klicka på **OK**.

10 Ange maskinens modellnamn. Klicka på **OK**.

Obs

- När skärmen för Kontroll av användarkonto visas, klickar du på **Fortsätt**.
- Om den skrivardrivrutin som du installerar inte har ett digitalt certifikat visas ett varningsmeddelande. Klicka på **Installera drivrutinen ändå** för att fortsätta med installationen. **Guiden Lägg till skrivare** slutförs.

11 Du kommer att se skärmen **Skriv ett skrivarnamn** i **Lägg till skrivare**-guiden. Markera kryssrutan för **Använd som standardskrivare** om du vill använda den här maskinen som standardskrivare och klicka sedan på **Nästa**.

12 Du kan testa skrivaranslutningen genom att klicka på **Skriv ut en testsida** och därefter på **Slutför**. Maskinen är nu konfigurerad och redo att skriva ut.

5 Sända eller Ta emot (för DCP- och MFC-modeller) ett e-postmeddelande på ett säkert sätt

Konfigurera med webbaserad hantering (webbläsare)

Du kan konfigurera säker sändning av e-post med användarautentisering eller sändning och mottagning (för DCP- och MFC-modeller) av e-post med SSL/TLS på skärmen för webbaserad hantering.

1. Starta webbläsaren.
2. Ange ”http://maskinens ip-adress/” i webbläsaren (där ”maskinens ip-adress” är maskinens IP-adress).
   - Till exempel:

     http://192.168.1.2/
3. Lösenord krävs inte som standard. Ange ett lösenord om du har ställt in ett sådant och tryck på .
4. Klicka på **Network** (Nätverk).
5. Klicka på **Protocol** (Protokoll).
6. Klicka på **Advanced Setting** (Avancerad inställning) på **POP3/SMTP** och se till att status för **POP3/SMTP** är **Enabled** (Aktivera).
7. Du kan konfigurera **POP3/SMTP**-inställningarna på den här sidan.

Obs

- Mer information finns i hjälptexten för webbaserad hantering.
- Du kan även kontrollera att e-postinställningarna har konfigurerats rätt genom att skicka ett testmeddelande via e-post.
- Om du inte känner till inställningarna för POP3/SMTP-servern kan du kontakta din systemadministratör eller ISP (Internetleverantör) för mer information.

8. Klicka på **Submit** (Skicka) när du är klar med konfigurationen. Skärmbilden **Test E-mail Send Configuration** (Testa Konfiguration för att skicka e-post) eller **Test E-mail Send/Receive Configuration** (Testa Konfiguration för att skicka/ta emot e-post) visas.
9. Följ anvisningarna på skärmen om du vill testa de aktuella inställningarna.

Sända eller Ta emot (för DCP- och MFC-modeller) ett e-postmeddelande på ett säkert sätt med SSL/TLS

Denna maskin stödjer metoderna SSL/TLS för att skicka eller ta emot (för DCP- och MFC-modeller) e-post via en e-postserver som kräver säker SSL/TLS-kommunikation. För att kunna sända eller ta emot e-post via en e-postserver som använder SSL/TLS-kommunikation måste du konfigurera SMTP över SSL/TLS eller POP3 över SSL/TLS korrekt.

Verifiera servercertifikat

- Om du väljer SSL eller TLS för **SMTP over SSL/TLS** (SMTP över SSL/TLS) eller **POP3 over SSL/TLS** (POP3 över SSL/TLS) markeras kryssrutan **Verify Server Certificate** (Verifiera servercertifikat) automatiskt för att verifiera servercertifikatet.
  - Innan du verifierar servercertifikatet måste du importera CA-certifikatet som har utfärdats av det CA som signerade servercertifikatet. Kontakta din nätverksadministratör eller Internetleverantör angående om ett CA-certifikat måste importeras. Information om att importera certifikatet finns i *Importera och exportera ett CA-certifikat* ➤➤ sidan 18.
  - Om du inte behöver verifiera servercertifikatet, avmarkera **Verify Server Certificate** (Verifiera servercertifikat).

Portnummer

- Om du väljer SSL eller TLS ändras värdet för **SMTP Port** (SMTP-port) eller **POP3 Port** (POP3-port) så att det stämmer med protokollet. Om du vill ändra portnumret manuellt, ange portnumret sedan du har valt **SMTP over SSL/TLS** (SMTP över SSL/TLS) eller **POP3 over SSL/TLS** (POP3 över SSL/TLS).
- Du måste konfigurera kommunikationsmetoden för POP3/SMTP så att det stämmer med e-postservern. Din nätverksadministratör eller Internetleverantör kan ge dig detaljer om inställningarna för e-postservern. I de flesta fallen krävs följande inställningar för säkra webbposttjänster:
  - **SMTP**
    - **SMTP-port**: 587
    - **SMTP-serverautentiseringsmetod**: SMTP-AUTH
    - **SMTP över SSL/TLS**: TLS
  - **POP3**
    - **POP3-port**: 995
    - **POP3 över SSL/TLS**: SSL

6 Felsökning

Översikt

I det här kapitlet får du information om hur du löser typiska nätverksproblem som du kan stöta på när du använder Brother-maskinen. Om du fortfarande inte kan lösa ett visst problem efter att ha läst det här kapitlet kan du gå till Brother Solutions Center på: (http://solutions.brother.com/).

Gå till Brother Solutions Center på (http://solutions.brother.com/) och klicka på Bruksanvisningar på sidan för din modell för att ladda ner andra handböcker.

Identifiera problemet

Se till att följande är konfigurerade innan du läser detta kapitel.

Kontrollera först att:
Nätkabeln är ordentligt ansluten och Brother-maskinen är påslagen.
Alla skyddsförpackning tagits bort från maskinen.
Tonerkassetterna och trumenheten har installerats på rätt sätt.
de främre och bakre luckorna är helt stängda
papperet har lagts i på rätt sätt i pappersfacket
Maskinen är korrekt ansluten till nätverket.

Gå till sidan för din lösning enligt listorna nedan.

- Jag kan inte skriva ut dokumentet via Internet med IPPS.

  Se *Jag kan inte skriva ut dokumentet via Internet med IPPS.* ➤➤ sidan 28.

- Jag vill kontrollera att mina nätverksenheter fungerar korrekt.

  Se *Jag vill kontrollera att mina nätverksenheter fungerar korrekt.* ➤➤ sidan 28.

Jag kan inte skriva ut dokumentet via Internet med IPPS.

Fråga	Lösning
Jag kan inte kommunicera med Brother-maskinen via SSL.	■ Erhåll giltigt certifikat och installera på både din maskin och dator igen. ■ Se till att portinställningen på din maskin är korrekt. Du kan bekräfta din maskins portinställning på skärmen webbaserad hantering genom att klicka på **Network** (Nätverk), **Protocol** (Protokoll) och sedan på **HTTP Server Settings** (Inställningar för HTTP-server).

Jag vill kontrollera att mina nätverksenheter fungerar korrekt.

Fråga	Lösning
Är din Brother-maskin påslagen?	Kontrollera att du följt alla instruktioner i *Kontrollera först att:* ➤➤ sidan 27.
Var hittar jag Brother-maskinens nätverksinställningar, som t.ex. IP-adressen?	Skriva ut nätverkskonfigurationslistan. Se *Skriva ut sidan med skrivarinställningar (för HL-5450DN(T))* ➤➤ sidan 29 eller *Skriva ut nätverkskonfigurationsrapport (för andra modeller)* ➤➤ sidan 29.

Skriva ut sidan med skrivarinställningar (för HL-5450DN(T))

Obs

Nodnamn: Nodnamnet visas i nätverkskonfigurationslistan. Standardinställt nodnamn är ”BRNxxxxxxxxxxxx”. (”xxxxxxxxxxxx” är din maskins MAC-adress/Ethernet-adress.)

Sidan med skrivarinställningar skriver ut en rapport där alla aktuella skrivarinställningar ställs upp inklusive inställningar för nätverksskrivarservern.

Du kan skriva ut sidan med skrivarinställningar genom att använda **Go**-knappen på maskinen.

1. Kontrollera att den främre luckan är stängd och att nätsladden är isatt.
2. Slå på maskinen och vänta tills maskinen är i beredskapsläge.
3. Tryck på **Go** tre gånger inom 2 sekunder. Maskinen skriver ut den aktuella sidan med skrivarinställningar.

Skriva ut nätverkskonfigurationsrapport (för andra modeller)

Obs

Nodnamn: Nodnamnet visas i nätverkskonfigurationslistan. Standardnodnamn är ”BRNxxxxxxxxxxxx” för ett trådbundet nätverk eller ”BRWxxxxxxxxxxxx” för ett trådlöst nätverk. (”xxxxxxxxxxxx” är din maskins MAC-adress/Ethernet-adress.)

Nätverkskonfigurationslistan skriver ut en rapport med alla aktuella nätverkskonfigurationer, inklusive skrivarserverns nätverksinställningar.

För HL-5470DW(T) och HL-6180DW(T)

1. Tryck på ▲ eller ▼ för att välja `Maskininform.`.
   Tryck på **OK**.
2. Tryck på ▲ eller ▼ för att välja `Utskr. nätinst.`.
   Tryck på **OK**.

För DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW och MFC-8910DW

1. Tryck på **Menu**.
2. (För MFC-modeller) Tryck på ▲ eller ▼ för att välja `Skriv rapport`.
   (För DCP-modeller) Tryck på ▲ eller ▼ för att välja `Maskininform.`.
   Tryck på **OK**.
3. Tryck på ▲ eller ▼ för att välja `Nätverksinst.`.
   Tryck på **OK**.
4. Tryck på **Start**.

För DCP-8250DN och MFC-8950DW(T)

1. Tryck på `Meny`.
2. Tryck på ▲ eller ▼ för att visa `Skriv rapport` och tryck därefter på `Skriv rapport`.
3. Tryck på `Nätverksinst.`.
4. Tryck på **Start**.

Obs

Om **IP Address** i nätverkskonfigurationslistan visar **0.0.0.0** ska du vänta i en minut och därefter försöka igen.

Nätverkstermer och begrepp

Teknisk översikt gällande SSL

Secure Socket Layer (SSL) är en metod för att skydda data på transportlager som skickas över ett lokalt eller utbrett nätverk med Internet Printing Protocol (IPP) för att förhindra att obehöriga användare ska kunna läsa dem.

Detta uppnås genom autentiseringsprotokoll i form av digitala nycklar, av vilka det finns 2 olika:

- En allmän nyckel - som alla som skriver ut känner till.
- En privat nyckel - som endast maskinen som används för att kryptera paket och göra dem läsbara igen, känner till.

Allmänna nycklar använder antingen 1 024 bitars eller 2 048 bitars kryptering och finns i ett digitalt certifikat. Dessa certifikat kan antingen vara självsignerade eller godkända av en CA (Certificate Authority).

Först finns det tre olika nycklar, privat, allmän och delad.

Den privata nyckeln, som endast maskinen känner till, är kopplad till den öppna nyckeln men finns inte i klientens (sändarens) digitala certifikat. När användaren först upprättar anslutningen skickar maskinen en Öppen nyckel med certifikatet. Klientens dator litar på att den öppna nyckeln kommer från maskinen med certifikatet. Klienten genererar den delade nyckeln och kodar den med den öppna nyckeln, och skickar den sedan till maskinen. Maskinen kodar den delade nyckeln med den privata nyckeln. Nu har maskinen och klienten delat den delade nyckeln på ett säkert sätt och upprättat den säkra anslutningen för överföring av utskriftsdata.

Utskriftsdatan kodas och avkodas med den delade nyckeln.

SSL hindrar inte obehöriga användare från att öppna paketen men, utan den privata nyckeln går de inte att läsa, vilken inte lämnas ut till någon annan än maskinen.

Detta kan konfigureras för både trådbundna och trådlösa nätverk och fungerar med annan typ av skydd som t.ex. WPA-nycklar och brandväggar under förutsättning att rätt konfiguration anges.

Nätverkstermer

- SSL (Secure Socket Layer)

  Säkerhetsprotokollet för kommunikation krypterar data som skydd mot säkerhetshot.

- IPP (Internet Printing Protocol)

  IPP är ett standardutskriftsprotokoll som används för hantering och administrering av utskriftsjobb. Det kan användas både lokalt och globalt så att du oavsett var du befinner dig i världen kan skriva ut på samma maskin.

- IPPS

  Versionen av utskriftsprotokollet IPP (Internet Printing Protocol Version 1.0) som använder SSL.

- HTTPS

  Internetprotokollets (HTTP (Hyper Text Transfer Protocol)) som använder SSL.

- CA (Certificate Authority)

  En CA är en organisation som utfärdar digitala certifikat (särskilt X.509-certifikat) och går i godo för kopplingen mellan dataobjekt i ett certifikat.

- CSR (Certificate Signing Request)

  Ett CSR-meddelande är en ansökan om utfärdande av ett certifikat från en CA. CSR-meddelandet innehåller information som identifierar den ansökande personen, den offentliga nyckeln som genererats av den ansökande och den ansökandes digitala underskrift.

- Certifikat

  Ett certifikat är den information som sammankopplar en offentlig nyckel med en identitet. Certifikatet kan användas för att verifiera att en offentlig nyckel tillhör en individ. Formatet definieras av standarden x.509.

- Kryptosystem med offentlig nyckel

  Ett kryptosystem med offentlig nyckel är en modern kryptografisk metod som fungerar på så vis att algoritmerna använder ett nyckelpar (en offentlig nyckel och en privat nyckel) och använder olika komponenter av paret för olika steg i algoritmen.

- Kryptosystem med delad nyckel

  Ett kryptosystem med delad nyckel är en modern kryptografisk metod vars algoritmer använder samma nyckel för två olika steg i algoritmen (som t.ex. kryptering och dekryptering).