Guide för säkerhetsfunktioner

© 2025 Brother Industries, Ltd. Med ensamrätt.

Viktig information för säkerhet

- Standardlösenordet för att hantera skrivarens inställningar finns på undersidan av skrivaren och är märkt med texten ”**Pwd:**”. Vi rekommenderar att du omedelbart ändrar standardlösenordet för att skydda maskinen mot oauktoriserad åtkomst.
- När du ansluter din maskin till ett externt nätverk som internet ska du se till att din nätverksmiljö skyddas av en separat brandvägg eller på annat sätt för att förhindra informationsläckor på grund av otillräckliga inställningar eller oauktoriserad åtkomst av tredjeparter med onda avsikter.
- Trådlöst LAN gör att du enkelt kan upprätta en LAN-anslutning om det finns en signal i närheten. Om säkerhetsinställningarna inte är korrekt konfigurerade kan signalen dock avlyssnas av tredjeparter med onda avsikter, vilket kan leda till:
  - Stöld av personlig eller konfidentiell information
  - Otillbörlig överföring av information till parter där man utger sig för att vara de specificerade personerna
  - Spridning av transkriberat kommunikationsinnehåll som avlyssnats

Närliggande information

- Nätverk

Konfigurera certifikat för enhetssäkerhet

Du måste konfigurera ett certifikat för att kunna hantera den nätverksanslutna maskinen säkert med hjälp av SSL/TLS. Du måste använda Webbaserad hantering för att konfigurera ett certifikat.

- Översikt över funktioner för säkerhetscertifikat
- Hur man skapar och installerar ett certifikat
- Skapa ett självsignerat certifikat
- Skapa en CSR (Certificate Signing Request) och installera ett certifikat från en CA (Certificate Authority, certifikatmyndighet)
- Importera och exportera certifikat och privat nyckel
- Importera och exportera ett CA-certifikat

Översikt över funktioner för säkerhetscertifikat

Skrivaren har stöd för användning av flera säkerhetscertifikat, vilket ger säker autentisering och kommunikation med skrivaren. Följande funktioner för säkerhetscertifikat kan användas med skrivaren:

Vilka funktioner, alternativ och inställningar som stöds kan variera beroende på modell.

- SSL/TLS-kommunikation
- Autentisering med IEEE 802.1x
- IPsec

Skrivaren har stöd för följande:

- Förinstallerat certifikat

  Det finns ett förinstallerat självsignerat certifikat på din dator. Med hjälp av detta certifikat kan du använda SSL/TLS-kommunikation utan att behöva skapa eller installera ett annat certifikat.

  Det förinstallerade självsignerade certifikatet skyddar din kommunikation till en viss nivå. Vi rekommenderar att du använder ett certifikat som utfärdats av en pålitlig organisation för 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 skapa eller installera ett annat certifikat från en CA.

- Certifikat från en Certificate Authority (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 (Certificate Signing Request) från skrivarservern.
  - När du importerar ett certifikat och en privat nyckel.

- Certificate Authority (CA) certifikat

  För att använda ett CA-certifikat som självt identifierar CA:n och äger sin privata nyckel måste du importera detta CA-certifikat från CA:n innan du konfigurerar säkerhetsfunktionerna i nätverket.

- 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 återställning och sedan installera dem igen.

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

Liknande ämnen:

- Konfigurera IEEE 802.1x-autentisering för ditt nätverk med hjälp av webbaserad hantering (webbläsare)

Hur man skapar och installerar ett certifikat

Det finns två alternativ när du väljer ett säkerhetscertifikat: använda ett självsignerat certifikat eller använda ett certifikat från CA (Certificate Authority).

Alternativ 1

Självsignerat certifikat

1. Skapa ett självsignerat certifikat med webbaserad hantering.
2. Installera det självsignerade certifikatet på din dator.

Alternativ 2

Certifikat från en CA

1. Skapa en CSR (Certificate Signing Request) via webbaserad hantering.
2. Installera det certifikat som utfärdats av CA på Brother-maskinen med hjälp av Webbaserad hantering.
3. Installera certifikatet på din dator.

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

Skapa ett självsignerat certifikat

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.

5. Klicka på **Create Self-Signed Certificate (Skapa självsignerat certifikat)**.
6. Ange **Common Name (Gemensamt namn)** och **Valid Date (Giltigt datum)**.
   - Längden på **Common Name (Gemensamt namn)** är mindre än 64 bytes. 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.
7. Välj inställningen i rullgardinsmenyn **Public Key Algorithm (Offentlig nyckelalgoritm)**.
8. Välj inställningen i rullgardinsmenyn **Digest Algorithm (Digest Algoritm)**.
9. Klicka på **Submit (Skicka)**.

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

Skapa en CSR (Certificate Signing Request) och installera ett certifikat från en CA (Certificate Authority, certifikatmyndighet)

Om du redan har ett certifikat från en extern, betrodd certifikat myndighet (CA), kan du spara certifikatet och den privata nyckeln på maskinen och hantera dem genom att importera och exportera. Om du inte har ett certifikat från en extern, betrodd CA kan du skapa en CSR (Certificate Signing Request), skicka den till en CA för autentisering och installera det återsända certifikatet på din maskin.

- Skapa en CSR (Certificate Signing Request)
- Installera ett certifikat på maskinen

Skapa en CSR (Certificate Signing Request)

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

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

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Klicka på **Create CSR (Skapa CSR)**.
6. Ange ett **Common Name (Gemensamt namn)** (obligatoriskt) och lägg till annan information om din **Organization (Organisation)** (valfritt).

   - Din företagsinformation krävs för att en CA ska kunna bekräfta din identitet och attestera den för en utomstående.
   - Längden på **Common Name (Gemensamt namn)** måste vara mindre än 64 bytes. 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 Common Name som användes för certifikatet.
   - Längden på **Organization (Organisation)**, **Organization Unit (Organisationsenhet)**, **City/Locality (Ort/Lokalitet)** och **State/Province (Stat/Provins)** måste vara mindre än 64 byte.
   - **Country/Region (Land/Region)** ska vara en två tecken lång landskod enligt ISO 3166.
   - Om du konfigurerar certifikatförlängningen X.509v3 markerar du kryssrutan **Configure extended partition (Konfigurera utökad partition)** och väljer sedan **Auto (Register IPv4) (Auto (Registrera IPv4))** eller **Manual (Manuell)**.
7. Välj inställningen i rullgardinsmenyn **Public Key Algorithm (Offentlig nyckelalgoritm)**.
8. Välj inställningen i rullgardinsmenyn **Digest Algorithm (Digest Algoritm)**.
9. Klicka på **Submit (Skicka)**.

   CSR visas på skärmen. Spara CSR som en fil eller kopiera och klistra in den i ett CSR-formulär online som erbjuds av din CA.
10. Klicka på **Spara**.

- Följ den CA-policy som gäller för att skicka en CSR till din CA.
- Om du använder Enterprise root CA för Windows Server rekommenderar vi att du använder webbservern som certifikatmall för att säkert skapa klientcertifikatet. Om du skapar ett klientcertifikat för en IEEE 802.1x-miljö med EAP-TLS-autentisering rekommenderar vi att du använder Användare som certifikatmall.

Närliggande information

- Skapa en CSR (Certificate Signing Request) och installera ett certifikat från en CA (Certificate Authority, certifikatmyndighet)

Installera ett certifikat på maskinen

När du får ett certifikat från en Certifierande myndighet (CA) installerar du det på skrivarservern genom att följa stegen nedan:

Endast ett certifikat utfärdat med den här maskinens Begäran om certifikatsignering (CSR) kan installeras på din maskin. När du vill skapa ytterligare en CSR, se till att certifikatet är installerat innan du skapar en ny CSR. Skapa bara ytterligare en CSR efter att du installerat certifikatet på maskinen, annars blir den CSR du skapade innan installationen av en ny CSR ogiltig.

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Klicka på **Install Certificate (Installera certifikat)**.
6. Bläddra till den fil som innehåller certifikatet som utfärdats av en CA och klicka sedan på **Submit (Skicka)**.

   Nu skapas och sparas certifikatet i maskinens minne.

För att du ska kunna använda SSL/TLS-kommunikation måste rotcertifikatet från din CA installeras på din dator. Kontakta din nätverksadministratör.

Närliggande information

- Skapa en CSR (Certificate Signing Request) och installera ett certifikat från en CA (Certificate Authority, certifikatmyndighet)

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 ett certifikat och den privata nyckeln
- Exportera certifikatet och privata nyckeln

Importera ett certifikat och den privata nyckeln

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.

5. Klicka på **Import Certificate and Private Key (Importera CA-certifikat och privat nyckel)**.
6. Sök efter och markera den fil du vill importera.
7. Ange lösenordet om filen är krypterad och klicka sedan på **Submit (Skicka)**.

Certifikatet och den privata nyckeln importeras till maskinen.

Närliggande information

- Importera och exportera certifikat och privat nyckel

Exportera certifikatet och privata nyckeln

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ≡.

5. Klicka på **Export (Exportera)** som visas med **Certificate List (Certifikatlista)**.
6. Ange ett lösenord om du vill kryptera filen.

   Om du lämnar lösenordsfältet tomt krypteras inte filen.
7. Ange lösenordet en gång till för att bekräfta det och klicka sedan på **Submit (Skicka)**.
8. Klicka på **Spara**.

Certifikatet och den privata nyckeln har nu exporterats till datorn.

Du kan även importera certifikatet till din dator.

Närliggande information

- Importera och exportera certifikat och privat nyckel

Importera och exportera ett CA-certifikat

Du kan importera, exportera och spara CA-certifikat på Brother-maskinen.

- Importera ett CA-certifikat
- Exportera ett CA-certifikat

Importera ett CA-certifikat

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **CA Certificate (CA-certifikat)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Klicka på **Import CA Certificate (Importera CA-certifikat)**.
6. Sök efter den fil du vill importera.
7. Klicka på **Submit (Skicka)**.

Närliggande information

- Importera och exportera ett CA-certifikat

Exportera ett CA-certifikat

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **CA Certificate (CA-certifikat)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Välj det certifikat som du vill exportera och klicka på **Export (Exportera)**.
6. Klicka på **Submit (Skicka)**.

Närliggande information

- Importera och exportera ett CA-certifikat

Använda SSL/TLS

- Hantera nätverksmaskinen säkert med SSL/TLS
- Säker utskrift av dokument med SSL/TLS
- Skicka eller ta emot e-post säkert med SSL/TLS

Hantera nätverksmaskinen säkert med SSL/TLS

- Konfigurera ett certifikat för SSL/TLS och tillgängliga protokoll
- Få åtkomst till Webbaserad hantering med hjälp av SSL/TLS
- Installera det självsignerade certifikatet för Windows-användare som administratör
- Konfigurera certifikat för enhetssäkerhet

Konfigurera ett certifikat för SSL/TLS och tillgängliga protokoll

Konfigurera ett certifikat på maskinen med hjälp av Webbaserad hantering innan du använder SSL/TLS-kommunikation.

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Network (Nätverk)** > **Protocol (Protokoll)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.

5. Klicka på **HTTP Server Settings (HTTP-serverinställningar)**.
6. Välj det certifikat du vill konfigurera i rullgardinsmenyn **Select the Certificate (Välj certifikatet)**.
7. Klicka på **Submit (Skicka)**.
8. Klicka på **Yes (Ja)** för att starta om skrivarservern.

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Liknande ämnen:

- Säker utskrift av dokument med SSL/TLS

Få åtkomst till Webbaserad hantering med hjälp av SSL/TLS

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

- HTTPS måste vara aktiverat på maskinen för att du ska kunna använda HTTPS-protokoll. HTTPS-protokollet aktiveras som standard.
- Du kan ändra inställningar för HTTPS-protokollet med skärmen för webbaserad hantering.

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. Du kan nu komma åt maskinen över HTTPS.

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Installera det självsignerade certifikatet för Windows-användare som administratör

- Följande steg är avsedda för Microsoft Edge. Om du använder en annan webbläsare, se din webbläsares dokumentation eller onlinehjälp för instruktioner om hur du installerar certifikat.
- Se till att du har skapat ditt självsignerade certifikat med Webbaserad hantering.

1. Högerklicka på ikonen **Microsoft Edge** och klicka sedan på **Kör som administratör**.

   Om skärmen **User Account Control** visas klickar du på **Ja**.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om din anslutning inte är privat klickar du på knappen **Avancerat** och fortsätter sedan till webbplatsen.
4. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
5. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **Certificate (Certifikat)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
6. Klicka på **Export (Exportera)**.
7. För att kryptera utdatafilen, skriv in ett lösenord i fältet **Enter password (Ange lösenord)**. Om fältet **Enter password (Ange lösenord)** lämnas tomt krypteras inte filen för utmatning.
8. Ange lösenordet igen i fältet **Retype password (Ange lösenord igen)** och klicka sedan på **Submit (Skicka)**.
9. Klicka på den nedladdade filen för att öppna den.
10. När **Guiden Importera certifikat** visas klickar du på **Nästa**.
11. Klicka på **Nästa**.
12. Vid efterfrågan skriver du in ett lösenord och klickar sedan på **Nästa**.
13. Välj **Placera alla certifikat i nedanstående arkiv** och klicka sedan på **Bläddra...**.
14. Välj **Betrodda rotcertifikatutfärdare** och klicka sedan på **OK**.
15. Klicka på **Nästa**.
16. Klicka på **Slutför**.
17. Klicka på **Ja** om fingeravtrycket (tumavtrycket) är korrekt.
18. Klicka på **OK**.

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Säker utskrift av dokument med SSL/TLS

- Skriv ut dokument med hjälp av IPPS
- Konfigurera ett certifikat för SSL/TLS och tillgängliga protokoll
- Konfigurera certifikat för enhetssäkerhet

Skriv ut dokument med hjälp av IPPS

För säker dokumentutskrift med IPP-protokoll kan du använda IPPS-protokollet.

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Network (Nätverk)** > **Protocol (Protokoll)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Se till så att du markerat kryssrutan **IPP**.

   Om du inte har markerat kryssrutan **IPP**, markerar du kryssrutan **IPP** och klickar sedan på **Submit (Skicka)**.

   Starta om maskinen för att aktivera konfigurationen.

   När maskinen har startats går du tillbaka till maskinens webbsida, anger lösenordet och går sedan till det vänstra navigeringsfältet och klickar på **Network (Nätverk)** > **Network (Nätverk)** > **Protocol (Protokoll)**.
6. Klicka på **HTTP Server Settings (HTTP-serverinställningar)**.
7. Markera kryssrutan **HTTPS** under **IPP** och klicka sedan på **Submit (Skicka)**.
8. Starta om maskinen för att aktivera konfigurationen.

Kommunikation med IPPS kan inte förhindra otillåten åtkomst till skrivarservern.

Närliggande information

- Säker utskrift av dokument med SSL/TLS

Använda SNMPv3

- Hantera nätverksmaskinen säkert med SNMPv3

Hantera nätverksmaskinen säkert med SNMPv3

SNMPv3 (Simple Network Management-protokollet version 3) tillhandahåller användarautentisering och datakryptering för säker hantering av nätverksenheter.

1. Starta webbläsaren.
2. Skriv in ”https://Common Name” i webbläsarens adressfält (där ”Common Name” är det namn du gav certifikatet. Det kan vara din IP-adress, nodnamnet eller domännamnet).
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Network (Nätverk)** > **Protocol (Protokoll)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.

5. Se till att **SNMP**-inställningen är aktiverad och klicka sedan på **Advanced Settings (Avancerade inställningar)**.
6. Konfigurera inställningar för SNMPv1/v2c-läget.

Alternativ	Beskrivning
SNMP v1/v2c read-write access (SNMP v1/v2c läs-skrivåtkomst)	Skrivarservern använder version 1 och version 2c av SNMP-protokollet. I det här läget kan du använda alla skrivarens program. Det är dock inte säkert eftersom det inte autentiserar användaren och data inte krypteras.
SNMP v1/v2c read-only access (SNMP v1/v2c skrivskyddad åtkomst)	Skrivarservern använder skrivskyddad åtkomst till version 1 och version 2c av SNMP-protokollet.
Disabled (Avaktiverad)	Inaktivera version 1 och version 2c av SNMP-protokollet. Alla program som använder SNMPv1/v2c kommer att begränsas. För att tillåta användning av SNMPv1/v2c-program använder du läget **SNMP v1/v2c read-only access (SNMP v1/v2c skrivskyddad åtkomst)** eller **SNMP v1/v2c read-write access (SNMP v1/v2c läs-skrivåtkomst)**.

7. Konfigurera inställningarna för SNMPv3-läget.

Alternativ	Beskrivning
Enabled (Aktiverad)	Skrivarservern använder version 3 av SNMP-protokollet. För att använda skrivarservern på ett säkert sätt ska du använda SNMPv3-läget och sedan konfigurera inställningarna.
Disabled (Avaktiverad)	Inaktivera version 3 och av SNMP-protokollet. Alla program som använder SNMPv3 kommer att begränsas. För att tillåta användning av SNMPv3-program använder du SNMPv3-läget.

8. Klicka på **Submit (Skicka)**.

Om din maskin visar alternativen för protokollinställning, välj de alternativ du vill ha.

9. Starta om maskinen för att aktivera konfigurationen.

Närliggande information

- Använda SNMPv3

Använd IEEE 802.1x-autentisering för nätverket

Vad är IEEE 802.1x-autentisering?

IEEE 802.1x är en IEEE-standard som begränsar åtkomst från oauktoriserade nätverksenheter. Din Brother-maskin skickar en autentiseringsförfrågan till en RADIUS-server (autentiseringsserver) via din åtkomstpunkt eller hubb. När din förfrågan har verifierats av RADIUS-servern får din maskin tillträde till nätverket.

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket

Konfigurera IEEE 802.1x-autentisering för ditt nätverk med hjälp av webbaserad hantering (webbläsare)

- Om du konfigurerar maskinen med EAP-TLS-autentisering måste du installera klientcertifikatet från CA innan du påbörjar konfigurationen. Kontakta din nätverksadministratör rörande klientcertifikatet. Om du har installerat mer än ett klientcertifikat rekommenderar vi att du antecknar namnet på det certifikat du vill använda.
- Innan du verifierar servercertifikatet måste du importera CA-certifikatet som har utfärdats av den CA som signerade servercertifikatet. Kontakta din nätverksadministratör eller Internetleverantör (ISP) för att bekräfta om ett CA-certifikat måste importeras eller inte.

Du kan även konfigurera IEEE 802.1x-autentisering med hjälp av guiden för trådlös konfiguration från kontrollpanelen (trådlöst nätverk).

1. Starta webbläsaren.
2. Ange ”https://maskinens IP-adress” i webbläsarens adressfält (där ”maskinens IP-adress” är maskinens IP-adress).

   Exempel:

   https://192.168.1.2

   Maskinens IP-adress finns i nätverkskonfigurationsrapporten.
3. Om så krävs skriver du in lösenordet i **Login (Logga in)**-fältet och klickar därefter på **Login (Logga in)**.

Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)**.

Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ≡.

5. Gör något av följande:
   - För det trådbundna nätverket

     Klicka på **Wired (Trådbunden)** > **Wired 802.1x Authentication (Trådbunden 802.1x-autentisering)**.
   - För det trådlösa nätverket

     Klicka på **Wireless (Trådlös)** > **Wireless (Enterprise) (Trådlös (företag))**.
6. Konfigurera autentiseringsinställningar för IEEE 802.1x.

- Om du vill aktivera autentisering med IEEE 802.1x för ett trådbundet nätverk väljer du **Enabled (Aktiverad)** för **Wired 802.1x status (Status för trådbunden 802.1x)** på sidan **Wired 802.1x Authentication (Trådbunden 802.1x-autentisering)**.
- Om du använder **EAP-TLS**-autentisering måste du välja det klientcertifikat som är installerat (visas med certifikatets namn) för verifiering i rullgardinsmenyn **Client Certificate (Klientcertifikat)**.
- Om du väljer **EAP-FAST**, **PEAP**, **EAP-TTLS** eller **EAP-TLS**-autentisering kan du välja verifieringsmetoden i rullgardinsmenyn **Server Certificate Verification (Verifiering av servercertifikat)**. Verifiera servercertifikatet med det CA-certifikat som har importerats till maskinen i förväg och utfärdats av det CA som signerat servercertifikatet.

Välj en av följande verifieringsmetoder i rullgardinsmenyn **Server Certificate Verification (Verifiering av servercertifikat)**:

Alternativ	Beskrivning
No Verification (Ingen verifiering)	Man kan alltid ha förtroende för servercertifikatet. Verifieringen utförs inte.
CA Cert. (CA-certifikat)	Verifieringsmetoden att kontrollera servercertifikatets CA-tillförlitlighet med hjälp av det CA-certifikat som utfärdats av det CA som signerat servercertifikatet.
CA Cert. + ServerID (CA-certifiering + Server-ID)	Verifieringsmetoden för kontroll av värdet för det vanliga namnet [1]-värdet för servercertifikatet, förutom servercertifikatets CA-tillförlitlighet.

7. Klicka på **Submit (Skicka)** när konfigurationen genomförts.

   För trådbundet nätverk: När konfigurationen är klar, anslut din maskin till nätverket som stöds av IEEE 802.1x. Efter några minuter ska du skriva ut nätverkskonfigurationsrapporten för att kontrollera <**Wired IEEE 802.1x**>-statusen.

Alternativ	Beskrivning
Success	Den trådbundna funktionen för IEEE 802.1x aktiveras och autentiseringen har lyckats.
Failed	Den trådbundna funktionen för IEEE 802.1x aktiveras men autentiseringen misslyckades.
Off	Den trådburna funktionen för IEEE 802.1x är inte tillgänglig.

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket

Liknande ämnen:

- Översikt över funktioner för säkerhetscertifikat
- Konfigurera certifikat för enhetssäkerhet

[1] Verifieringen av det vanliga namnet jämför det vanliga namnet på servercertifikatet och teckensträngen som konfigurerats för **Server ID (Server-ID)**. Kontakta din systemadministratör om servercertifikatets vanliga namn och konfigurera sedan **Server ID (Server-ID)** innan du använder denna metod.

IEEE 802.1x-autentiseringsmetoder

EAP-FAST

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel) har utvecklats av Cisco Systems, Inc. som använder ett användar-ID och lösenord för autentisering och symmetriska nyckelalgoritmer för att skapa en tunnlad autentiseringsprocess.

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

- EAP-FAST/INGEN
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (trådbundet nätverk)

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) använder ett användar-ID och ett lösenord för challenge-response-autentisering.

PEAP

PEAP (Protected Extensible Authentication Protocol) är en version av metoden EAP som är utvecklad av Cisco Systems, Inc., Microsoft Corporation samt RSA Security. PEAP skapar en krypterad SSL- (Secure Sockets Layer)/TLS-tunnel (Transport Layer Security) mellan en klient och en autentiseringsserver för att skicka ett användar-ID och ett lösenord. PEAP ger ömsesidig autentisering mellan servern och klienten.

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) har utvecklats av Funk Software och Certicom. EAP-TTLS skapar en liknande krypterad SSL-tunnel till PEAP, mellan en klient och en autentiseringsserver, för att skicka ett användar-ID och lösenord. EAP-TTLS ger ömsesidig autentisering mellan servern och klienten.

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

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

EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) kräver autentisering av digitala certifikat både på en klient och en autentiseringsserver.

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket