Vejledning til netværkssikkerhedsfunktioner

Vigtig information vedrørende sikkerhed

- Standardadgangskoden til at styre maskinens indstillinger er placeret i bunden af maskinen og mærket “**Pwd:**“. Vi anbefaler, at du med det samme ændrer standardadgangskoden for at beskytte maskine mod uautoriseret adgang.
- Når du tilslutter maskinen til et eksternt netværk som f.eks. internettet, skal du sikre dig, at dit netværksmiljø er beskyttet af en separat firewall eller på anden vis for at forhindre, at information lækker på grund af utilstrækkelige indstillinger eller uønskede tredjeparters uautoriserede adgang.
- Hvis der er et signal i nærheden, giver trådløst LAN dig mulighed for frit at oprette en LAN-forbindelse. Hvis sikkerhedsindstillingerne imidlertid ikke er konfigureret korrekt, kan signalet blive opsnappet af uønskede tredjeparter, hvilket kan medføre:
  - Tyveri af personlige eller fortrolige oplysninger
  - Upassende transmission af oplysninger til parter, der udgiver sig for specifikke personer
  - Udbredelse af transskriberet, opfanget kommunikationsindhold

Relaterede informationer

- Netværk

Konfigurer certifikater for enhedssikkerhed

Du skal konfigurere et certifikat til sikker administration af din netværksmaskine vha. SSL/TLS. Du skal bruge Web Based Management til konfiguration af et certifikat.

Oversigt over funktioner i sikkerhedscertifikater

Din maskine understøtter brugen af flere sikkerhedscertifikater, som giver mulighed for sikker godkendelse og kommunikation med maskinen. Følgende sikkerhedscertifikatfunktioner kan bruges med maskinen:

De understøttede funktioner, muligheder og indstillinger kan variere afhængigt af model

- SSL/TLS-kommunikation
- IEEE 802.1x-godkendelse
- IPsec

Din maskine understøtter følgende:

- Præinstalleret certifikat

  Din maskine har et præinstalleret, selvsigneret certifikat. Med dette certifikat kan du bruge SSL/TLS-kommunikation uden at oprette eller installere et andet certifikat.

Det præinstallerede, selvsignerede certifikat beskytter din kommunikation op til et vist niveau. Vi anbefaler brug af et certifikat, der er udstedt af en pålidelig organisation, for at opnå bedre sikkerhed.

- Selvsigneret certifikat

  Denne printserver udsteder sit eget certifikat. Med dette certifikat kan du nemt bruge SSL/TLS-kommunikation uden at oprette eller installere et andet certifikat fra et nøglecenter.

- Certifikat fra et nøglecenter

  Der er to måder, hvorpå du kan installere et certifikat fra et nøglecenter. Hvis du allerede har et certifikat fra et nøglecenter, eller hvis du vil bruge et certifikat fra et eksternt nøglecenter, der er tillid til:

  - Ved brug af en CSR (Certificate Signing Request) fra denne printserver.
  - Import af et certifikat og en privat nøgle.

- Nøglecentercertifikat

  For at bruge et certifikat fra et nøglecenter, der identificerer nøglecenteret og ejer sin private nøgle, skal du importere dette nøglecertifikat fra nøglecenteret, før du konfigurer netværkssikkerhedsfunktioner.

- Hvis du skal bruge SSL/TLS-kommunikation, anbefaler vi, at du kontakter systemadministratoren først.
- Når du nulstiller printserveren til standardfabriksindstilling, slettes det installerede certifikat og den private nøgle. Hvis du vil bevare samme certifikat og den private nøgle efter nulstilling af serveren, skal disse eksporteres før nulstilling og derefter installeres igen.

Relaterede informationer

- Konfigurer certifikater for enhedssikkerhed

Relaterede emner:

- Konfigurer IEEE 802.1x-godkendelse til dit netværk ved hjælp af webbaseret administration (webbrowser)

Sådan oprettes og installeres et certifikat

Der er to indstillinger ved valg af et sikkerhedscertifikat: brug et selvsigneret certifikat eller brug et certifikat fra et nøglecenter (CA).

Indstilling 1

Selvsigneret certifikat

1. Opret et selvsigneret certifikat med Web Based Management.
2. Installer det selvsignerede certifikat på computeren.

Indstilling 2

Certifikat fra et nøglecenter

1. Opret en anmodning om certifikatunderskrift (CSR) ved at bruge Web Based Management.
2. Installer det certifikat, der er udstedt af nøglecenteret, på Brother-maskinen ved hjælp af webbaseret administration.
3. Installer certifikatet på computeren.

Relaterede informationer

- Konfigurer certifikater for enhedssikkerhed

Oprettelse af selvsigneret certifikat

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Klik på **Create Self-Signed Certificate (Opret selvsigneret certifikat)**.
6. Indtast et **Common Name (Fællesnavn)** og en **Valid Date (Gyldig dato)**.
   - Længden af **Common Name (Fællesnavn)** er mindre end 64 byte. Indtast en identifikator, f.eks. en IP-adresse, et nodenavn eller domænenavn, der skal bruges til at få adgang til maskinen via SSL/TLS-kommunikation. Nodenavnet vises som standard.
   - Der vises en advarsel, hvis du bruger en IPPS- eller HTTPS-protokol og indtaster et andet navn i URL'en end det **Common Name (Fællesnavn)**, der bruges til det selvsignerede certifikat.
7. Vælg din indstilling på rullelisten **Public Key Algorithm (Algoritme til offentlig nøgle)**.
8. Vælg din indstilling på rullelisten **Digest Algorithm (Indlæs og afprøv algoritme)**.
9. Klik på **Submit (Send)**.

Relaterede informationer

- Konfigurer certifikater for enhedssikkerhed

Opret en anmodning om certifikatunderskrift (CSR) og installer et certifikat fra en certifikatudstedende myndighed (CA)

Hvis du allerede har et certifikat fra et ekstern, pålidelig, certifikatudstedende myndighed (CA) kan du gemme certifikatet og den private nøgle på maskinen og administrere dem via import og eksport. Hvis du ikke har et certifikat fra en ekstern, pålidelig certifikatudstedende myndighed, skal du oprette en anmodning om certifikatunderskrift (CSR), sende den til en certifikatudstedende myndighed til godkendelse og installere det returnerede certifikat på din maskine.

- Oprettelse af Certificate Signing Request (CSR)
- Installation af et certifikat på maskinen

Oprettelse af Certificate Signing Request (CSR)

En Certificate Signing Request (CSR) er en anmodning, der sendes til et nøglecenter (CA) for at få godkendt de oplysninger, som findes i certifikatet.

Vi anbefaler, at du installerer et nøglecenter-rodcertifikat på din computer, før der oprettes en CSR.

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Klik på **Create CSR (Opret CSR)**.
6. Indtast et **Common Name (Fællesnavn)** (obligatorisk), og tilføj andre oplysninger om din **Organization (Virksomhed)** (valgfrit).

- Virksomhedsoplysningerne er nødvendige, så nøglecenteret kan bekræfte din identitet og verificere den over for en udenforstående.
- Længden af **Common Name (Fællesnavn)** skal være mindre end 64 byte. Indtast en identifikator, f.eks. en IP-adresse, et nodenavn eller domænenavn, der skal bruges til at få adgang til maskinen via SSL/TLS-kommunikation. Nodenavnet vises som standard. **Common Name (Fællesnavn)** er obligatorisk.
- Der vises en advarsel, hvis du indtaster et andet navn i URL'en end det fællesnavn, der blev brugt til certifikatet.
- Længden af **Organization (Virksomhed)**, **Organization Unit (Virksomhedsenhed)**, **City/Locality (By/Sted)** og **State/Province (Stat/Landsdel)** skal være mindre end 64 byte.
- **Country/Region (Land/Område)** skal være en ISO 3166-landekode på to tegn.
- Hvis du konfigurerer en X.509v3-certifikatudvidelse, skal du markere afkrydsningsfeltet **Configure extended partition (Konfigurer udvidet partition)** og derefter vælge **Auto (Register IPv4) (Auto (Registrer IPv4))** eller **Manual (Manuel)**.

7. Vælg din indstilling på **Public Key Algorithm (Algoritme til offentlig nøgle)**rullelisten.
8. Vælg din indstilling på **Digest Algorithm (Indlæs og afprøv algoritme)**rullelisten.
9. Klik på **Submit (Send)**.

   CSR'et vises på skærmen. Gem CSR'et som en fil, eller kopier og indsæt det i en online CSR-formular tilbudt af et nøglecenter.
10. Klik på **Gem**.

- Følg nøglecenterets politik vedrørende metoden til at afsende en CSR til nøglecenteret.
- Hvis du bruger et rodnøglecenter for virksomheder til Windows Server, anbefaler vi, at du bruger webserveren til certifikatskabelonen til at oprette klientcertifikatet på sikker vis. Hvis du opretter et klientcertifikat til et IEEE 802.1x-miljø med EAP-TLS-godkendelse, anbefaler vi anvendelsen Bruger for certifikatskabelonen.

Relaterede informationer

- Opret en anmodning om certifikatunderskrift (CSR) og installer et certifikat fra en certifikatudstedende myndighed (CA)

Installation af et certifikat på maskinen

Når du modtager et certifikat fra et CA (nøglecenter), skal du følge trinnene nedenfor for at installere det på printserveren:

Kun et certifikat, der er udstedt med din maskines CSR (anmodning om signering af certifikat), kan installeres på maskinen. Når du vil oprette yderligere et CSR, skal du kontrollere, at certifikatet er installeret, før det nye CSR oprettes. Opret først det andet CSR, når du har installeret certifikatet på maskinen, ellers vil det tidligere oprettede CSR være ugyldigt.

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

   Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.
4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

   Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.
5. Klik på **Install Certificate (Installation af certifikat)**.
6. Gennemse for at finde den fil, der indeholder certifikatet udstedt af nøglecenteret, og klik derefter på **Submit (Send)**.

   Certifikatet oprettes og gemmes i maskinens hukommelse.

Hvis du vil bruge SSL/TLS-kommunikation, skal rodcertifikatet fra nøglecenteret også installeres på computeren. Kontakt din netværksadministrator.

Relaterede informationer

- Opret en anmodning om certifikatunderskrift (CSR) og installer et certifikat fra en certifikatudstedende myndighed (CA)

Import og eksport af certifikat og privat nøgle

Gem certifikatet og den private nøgle på maskinen, og administrer dem ved at importere og eksportere dem.

- Import af et certifikat og en privat nøgle
- Eksport af certifikat og privat nøgle

Import af et certifikat og en privat nøgle

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Klik på **Import Certificate and Private Key (Import af certifikat og privat nøgle)**.
6. Gennemse og vælg den fil, du vil importere.
7. Indtast adgangskoden, hvis filen er krypteret, og klik derefter på **Submit (Send)**.

Certifikatet og den private nøgle importeres til maskinen.

Relaterede informationer

- Import og eksport af certifikat og privat nøgle

Eksport af certifikat og privat nøgle

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

> Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

> Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Klik på **Export (Eksport)**, der vises med **Certificate List (Certifikatliste)**.
6. Indtast en adgangskode, hvis du vil kryptere filen.

   Hvis der ikke indtastes en adgangskode, krypteres udskriften ikke.
7. Gentag adgangskoden for at bekræfte den, og klik derefter på **Submit (Send)**.
8. Klik på **Gem**.

Certifikatet og den private nøgle eksporteres til computeren.

Du kan også importere certifikatet til din computer.

Relaterede informationer

- Import og eksport af certifikat og privat nøgle

Import og eksport af et nøglecentercertifikat

Du kan importere, eksportere og gemme nøglecentercertifikater på Brother-maskinen.

- Import af et nøglecentercertifikat
- Eksport af et nøglecentercertifikat

Import af et nøglecentercertifikat

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **CA Certificate (Nøglecentercertifikat)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Klik på **Import CA Certificate (Import af nøglecentercertifikat)**.
6. Gennemse for den fil, du vil importere.
7. Klik på **Submit (Send)**.

Relaterede informationer

- Import og eksport af et nøglecentercertifikat

Eksport af et nøglecentercertifikat

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **CA Certificate (Nøglecentercertifikat)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Vælg det certifikat, du vil eksportere, og klik på **Export (Eksport)**.
6. Klik på **Submit (Send)**.

Relaterede informationer

- Import og eksport af et nøglecentercertifikat

Brug SSL/TLS

- Sikker administration af din netværksmaskine med SSL/TLS
- Udskriv dokumenter sikkert med SSL/TLS
- Send eller modtag en e-mail sikkert ved hjælp af SSL/TLS

Sikker administration af din netværksmaskine med SSL/TLS

Konfiguration af et certifikat for SSL/TLS og tilgængelige protokoller

Konfigurer et certifikat på maskinen ved hjælp af webbaseret administration, før du bruger SSL/TLS-kommunikation.

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

   Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.
4. Klik på **Network (Netværk)** > **Network (Netværk)** > **Protocol (Protokol)**i venstre navigationsbjælke.

   Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.
5. Klik på **HTTP Server Settings (HTTP-serverindstillinger)**.
6. Vælg det certifikat, der skal konfigureres, på rullelisten **Select the Certificate (Vælg certifikatet)**.
7. Klik på **Submit (Send)**.
8. Klik på **Yes (Ja)** for at genstarte printserveren.

Relaterede informationer

- Sikker administration af din netværksmaskine med SSL/TLS

Relaterede emner:

- Udskriv dokumenter sikkert med SSL/TLS

Adgang til webbaseret administration ved hjælp af SSL/TLS

Sikker administration af netværksmaskinen kræver brug af administrationshjælpeprogrammer med sikkerhedsprotokoller.

- For at bruge HTTPS-protokollen skal HTTPS være aktiveret på maskinen. HTTPS-protokollen er aktiveret som standard.
- Du kan ændre HTTPS-protokolindstillingerne ved hjælp af Web Based Management-skærmen.

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

   Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.
4. Du kan nu få adgang til maskinen med HTTPS.

Relaterede informationer

- Sikker administration af din netværksmaskine med SSL/TLS

Installation af det selvsignerede certifikat for Windows-brugere som administrator

- Følgende trin gælder Microsoft Edge. Hvis du bruger en anden webbrowser, se da din webbrowserdokumentation eller webbrowserens onlinevejledning i installation af certifikater.
- Kontroller, at du har oprettet dit selvsignerede certifikat ved hjælp af webbaseret administration.

1. Højreklik på ikonet **Microsoft Edge**, og klik derefter på **Kør som administrator**.

   Hvis skærmbilledet **Kontrol af brugerkonti** vises, skal du klikke på **Ja**.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis din forbindelse ikke er privat, skal du klikke på knappen **Avanceret** og derefter fortsætte til websiden.
4. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

   Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.
5. Klik på **Network (Netværk)** > **Security (Sikkerhed)** > **Certificate (Certifikat)**i venstre navigationsbjælke.

   Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.
6. Klik på **Export (Eksport)**.
7. Indtast en adgangskode i feltet **Enter password (Indtast adgangskode)** for at kryptere outputfilen. Hvis feltet **Enter password (Indtast adgangskode)** er tomt, bliver din outputfil ikke krypteret.
8. Indtast printerens adgangskoden igen i feltet **Retype password (Gentag adgangskode)**, og klik dernæst på **Submit (Send)**.
9. Klik på den downloadede fil for at åbne den.
10. Når **Guiden Certifikatimport** vises, skal du klikke på **Næste**.
11. Klik på **Næste**.
12. Indtast om nødvendigt en adgangskode, og klik derefter på **Næste**.
13. Vælg **Placer alle certifikater i følgende certifikatlager**, og klik derefter på **Gennemse...**.
14. Vælg **Rodnøglecentre, der er tillid til**, og klik derefter på **OK**.
15. Klik på **Næste**.
16. Klik på **Udfør**.
17. Klik på **Ja**, hvis aftrykket er korrekt.
18. Klik på **OK**.

Relaterede informationer

- Sikker administration af din netværksmaskine med SSL/TLS

Udskriv dokumenter sikkert med SSL/TLS

Udskrivning af dokumenter ved hjælp af IPPS

Sikker udskrivning af dokumenter med IPP-protokol, brug IPPS-protokollen.

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

   Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.
4. Klik på **Network (Netværk)** > **Network (Netværk)** > **Protocol (Protokol)**i venstre navigationsbjælke.

   Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.
5. Kontrollér, at afkrydsningsfeltet **IPP** er markeret.

   Hvis afkrydsningsfeltet **IPP** ikke er markeret, skal du markere afkrydsningsfeltet **IPP** og derefter klikke på **Submit (Send)**.

   Genstart maskinen for at aktivere konfigurationen.

   Når maskinen er genstartet, skal du vende tilbage til maskinens webside, skrive adgangskoden, og i navigationsmenuen klikke på **Network (Netværk)** > **Network (Netværk)** > **Protocol (Protokol)**.
6. Klik på **HTTP Server Settings (HTTP-serverindstillinger)**.
7. Markér afkrydsningsfeltet **HTTPS** i området **IPP**, og klik derefter på **Submit (Send)**.
8. Genstart maskinen for at aktivere konfigurationen.

Kommunikation med IPPS kan ikke forhindre uautoriseret adgang til printserveren.

Relaterede informationer

- Udskriv dokumenter sikkert med SSL/TLS

Brug SNMPv3

- Sikker administration af din netværksmaskine vha. SNMPv3

Sikker administration af din netværksmaskine vha. SNMPv3

SNMPv3 (Simple Network Management Protocol version 3) giver brugergodkendelse og datakryptering til sikker administration af netværksenheder.

1. Start din webbrowser.
2. Indtast "https://Fællesnavn" i browserens adresselinje (hvor "Fællesnavn" er det fællesnavn, du har tildelt for certifikatet; det kan være din IP-adresse, dit nodenavn eller dit domænenavn).
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** > **Network (Netværk)** > **Protocol (Protokol)**i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Kontroller, at indstillingen **SNMP** er aktiveret, og klik derefter på **Advanced Settings (Avancerede indstillinger)**.
6. Konfigurer indstillingerne for SNMPv1/v2c-tilstand.

Indstilling	Beskrivelse
SNMP v1/v2c read-write access (SNMP v1/v2c læse-skrive-adgang)	Printserveren bruger version 1 og version 2c af SNMP-protokollen. Du kan bruge alle maskinens programmer i denne tilstand. Den er dog ikke sikker, da brugeren ikke godkendes, og dataene krypteres ikke.
SNMP v1/v2c read-only access (SNMP v1/v2c skrivebeskyttet adgang)	Printserveren bruger skrivebeskyttet adgang til version 1 og version 2c af SNMP-protokollen.
Disabled (Deaktiveret)	Deaktiver version 1 og version 2c af SNMP-protokollen. Alle applikationer, der anvender SNMPv1/v2c, vil være begrænset. Brug tilstanden **SNMP v1/v2c read-only access (SNMP v1/v2c skrivebeskyttet adgang)** eller **SNMP v1/v2c read-write access (SNMP v1/v2c læse-skrive-adgang)** til at tillade brugen af SNMPv1/v2c-programmer.

7. Konfigurer indstillingerne for SNMPv3-tilstand.

Indstilling	Beskrivelse
Enabled (Aktiveret)	Printserveren bruger version 3 af SNMP-protokollen. For at administrere printserveren sikkert skal du bruge SNMPv3-tilstanden og derefter konfigurere indstillingerne.
Disabled (Deaktiveret)	Deaktiver version 3 af SNMP-protokollen. Alle programmer, der anvender SNMPv3, vil være begrænset. Brug SNMPv3-tilstanden for at tillade brugen af SNMPv3-applikationer.

8. Klik på **Submit (Send)**.

Hvis din maskine viser valgmulighederne for protokolindstilling, skal du vælge de ønskede indstillinger.

9. Genstart maskinen for at aktivere konfigurationen.

Relaterede informationer

- Brug SNMPv3

Brug IEEE 802.1x-godkendelse til dit netværk

Hvad er IEEE 802.1x-godkendelse?

IEEE 802.1x er en IEEE-standard, der begrænser adgangen fra uautoriserede netværksenheder. Din Brother-maskine sender en godkendelsesanmodning til en RADIUS-server (godkendelsesserver) via dit accesspoint eller hub'en. Når din anmodning er blevet bekræftet af RADIUS-serveren, kan maskinen få adgang til netværket.

Relaterede informationer

- Brug IEEE 802.1x-godkendelse til dit netværk

Konfigurer IEEE 802.1x-godkendelse til dit netværk ved hjælp af webbaseret administration (webbrowser)

- Hvis du konfigurerer maskinen vha. EAP-TLS-godkendelse, skal du installere klientcertifikatet udstedt af CA, før du kan starte konfigurationen. Kontakt din netværksadministrator vedrørende klientcertifikatet. Hvis du har installeret mere end ét certifikat, anbefaler vi, at du noterer navnet på det certifikat, du vil bruge.
- Før du verificerer servercertifikatet, skal du importere det nøglecentercertifikat, der er udstedt af det nøglecenter, der signerede servercertifikatet. Kontakt din netværksadministrator eller internetudbyder for at få oplyst, hvorvidt det er nødvendigt at importere et nøglecentercertifikat.

Du kan også konfigurere IEEE 802.1x-godkendelse ved hjælp af guiden til trådløs konfiguration fra betjeningspanelet (trådløst netværk).

1. Start din webbrowser.
2. Indtast "https://maskinens IP-adresse" i browserens adresselinje (hvor "maskinens IP-adresse" er IP-adressen på din maskine).

   F.eks.:

   https://192.168.1.2

   Maskinens IP-adresse kan findes i netværkskonfigurationsrapporten.
3. Hvis det er påkrævet, skal du skrive en adgangskode i feltet **Login (Logon)** og derefter klikke på **Login (Logon)**.

Standardadgangskoden til at administrere denne maskines indstillinger er placeret på bagsiden eller i bunden af maskinen og mærket "**Pwd**". Skift standardadgangskoden ved at følge vejledningen på skærmen, når du logger ind første gang.

4. Klik på **Network (Netværk)** i venstre navigationsbjælke.

Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.

5. Følg en af nedenstående fremgangsmåder:
   - For det kabelbaserede netværk

     Klik på **Wired (Kabelbaseret)** > **Wired 802.1x Authentication (Kabelført 802.1x-godkendelse)**.
   - For det trådløse netværk

     Klik på **Wireless (Trådløs)** > **Wireless (Enterprise) (Trådløs (virksomhed))**.
6. Konfigurer IEEE 802.1x godkendelsesindstillingerne.

- Hvis du vil aktivere IEEE 802.1x-godkendelse for kabelbaserede netværk, skal du vælge **Enabled (Aktiveret)** for **Wired 802.1x status (Kabelbaseret 802.1x-status)** på siden **Wired 802.1x Authentication (Kabelført 802.1x-godkendelse)**.
- Hvis du bruger godkendelsen **EAP-TLS**, skal du vælge det klientcertifikat, der er installeret (vises med certifikatnavn), til verifikation på rullelisten **Client Certificate (Kundecertifikat)**.
- Hvis du vælger godkendelsen **EAP-FAST**, **PEAP**, **EAP-TTLS** eller **EAP-TLS**, kan du vælge en verificeringsmetode på rullelisten **Server Certificate Verification (Verificering af servercertifikat)**. Verificer servercertifikatet med et nøglecentercertifikat, der er importeret til maskinen på forhånd og er udstedt af det nøglecenter, der har signeret servercertifikatet.

Vælg en af følgende verificeringsmetoder på rullelisten **Server Certificate Verification (Verificering af servercertifikat)**:

Indstilling	Beskrivelse
No Verification (Ingen verificering)	Du kan altid have tillid til et servercertifikat. Verifikationen udføres ikke.
CA Cert. (CA-certifikat)	Verifikationsmetoden, der bruges til at kontrollere nøglecenterets pålidelighed for servercertifikatet, ved hjælp af det nøglecentercertifikat, der er udstedt af det nøglecenter, der har signeret servercertifikatet.
CA Cert. + ServerID (CA-certifikat + server-id)	Godkendelsesmetode til kontrol af fællesnavnet [1] værdi for servercertifikatet, foruden CA-serverens pålidelighedscertifikat.

7. Klik på **Submit (Send)**, når du er færdig med konfigurationen.

   For kabelbaserede netværk: Efter konfigureringen skal du slutte maskinen til et IEEE 802.1x-understøttet netværk. Efter nogle få minutter skal du udskrive en netværkskonfigurationsrapport for at kontrollere status for <**Wired IEEE 802.1x**>.

Indstilling	Beskrivelse
Success	Den kabelbaserede IEEE 802.1x-funktion aktiveres, og godkendelsen blev fuldført.
Failed	Den kabelbaserede IEEE 802.1x-funktion aktiveres, men godkendelsen blev ikke fuldført.
Off	Den kabelbaserede IEEE 802.1x-funktion er ikke tilgængelig.

Relaterede informationer

- Brug IEEE 802.1x-godkendelse til dit netværk

Relaterede emner:

- Oversigt over funktioner i sikkerhedscertifikater
- Konfigurer certifikater for enhedssikkerhed

1 Verificeringen af fællesnavnet sammenligner fællesnavnet for servercertifikatet med den tegnstreng, der er konfigureret for **Server ID (Server-id)**. Før du bruger denne metode, skal du kontakte din systemadministrator for at få oplysninger om servercertifikatets fællesnavn og derefter konfigurere **Server ID (Server-id)**.

IEEE 802.1x-godkendelsesmetoder

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) er udviklet af Cisco Systems, Inc. og udfører godkendelse via et bruger-id og en adgangskode og bruger symmetriske nøglealgoritmer til at opnå en tunnelforbundet godkendelsesproces.

Brother-maskinen understøtter følgende interne godkendelsesmetoder:

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

EAP-MD5 (kabelbaseret netværk)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) udfører challenge-response-godkendelse via et bruger-id og en adgangskode.

PEAP

PEAP (Protected Extensible Authentication Protocol) er en version af EAP-metoden udviklet af Cisco Systems, Inc., Microsoft Corporation og RSA Security. PEAP opretter en krypteret SSL/TLS-tunnel (Secure Sockets Layer/Transport Layer Security) mellem en klient og en godkendelsesserver til afsendelse af et bruger-id og en adgangskode. PEAP sørger for indbyrdes godkendelse mellem serveren og klienten.

Brother-maskinen understøtter følgende interne godkendelsesmetoder:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) er udviklet af Funk Software og Certicom. EAP-TTLS skaber en lignende krypteret SSL-tunnel til PEAP, mellem en klient og en godkendelsesserver, til afsendelse af et bruger-id og en adgangskode. EAP-TTLS sørger for indbyrdes godkendelse mellem serveren og klienten.

Brother-maskinen understøtter følgende interne godkendelsesmetoder:

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

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) kræver digital certifikatgodkendelse hos både en klient og en godkendelsesserver.

Relaterede informationer

- Brug IEEE 802.1x-godkendelse til dit netværk