Vejledning til netværkssikkerhedsfunktioner

Indholdsfortegnelse

Introduktion

Definitioner af bemærkninger

Vi bruger følgende symboler og konventioner gennem hele brugsanvisningen:

VIGTIGT	VIGTIGT indikerer en potentielt farlig situation, som, hvis den ikke undgås, kan resultere i materielle skader eller tab af produktfunktionalitet.
BEMÆRK	BEMÆRK angiver driftsmiljøet, betingelserne for installation eller særlige betingelser for brug.
	Tip-ikoner angiver nyttige hint og supplerende oplysninger.
Fed	Fed skrift angiver knapper på maskinens betjeningspanel eller computerskærmen.
Kursiv	Italicized skrift emphasizes et vigtigt punkt eller henviser til et relateret emne.

Relaterede informationer

- Introduktion

Varemærker

Adobe® og Reader® er enten registrerede varemærker eller varemærker tilhørende Adobe Systems Incorporated i USA og/eller andre lande.

De enkelte selskaber, hvis softwaretitler er nævnt i denne brugsanvisning, har en softwareLicenseaftale specifikt for deres navnebeskyttede programmer.

Alle handelsnavne og produktnavne, der forekommer på Brother-produkter, relaterede dokumenter og eventuelle andre materialer er alle varemærker eller registrerede varemærker, som tilhører deres respektive virksomheder.

Relaterede informationer

- Introduktion

Ophavsret

Relaterede informationer

- Introduktion

Før brug af netværkssikkerhedsfunktioner

Maskinen anvender nogle af de nyeste protokoller til netværkssikkerhed og kryptering, der fås på markedet i dag. Disse netværksfunktioner kan integreres i din overordnede plan for netværkssikkerhed og være med til at beskytte dine data samt forhindre unauthorized adgang til maskinen.

Vi anbefaler, at du deaktiverer FTP- og TFTP-protokollerne. Adgang til maskinen via disse protokoller er ikke sikker.

Relaterede informationer

- Introduktion
  - Deaktiver unødvendige protokoller

Deaktiver unødvendige protokoller

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. Fjern unødvendige protokolafkrydsningsfelter for at deaktivere dem.
6. Klik på **Submit (Send)**.
7. Genstart Brother-maskinen for at aktivere konfigurationen.

Relaterede informationer

- Før brug af netværkssikkerhedsfunktioner

Netværkssikkerhed

- Konfigurer certifikater for enhedssikkerhed
- Brug SSL/TLS
- Brug SNMPv3
- Brug IPsec
- Brug IEEE 802.1x-godkendelse til dit 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
- Sådan oprettes og installeres et certifikat
- Oprettelse af selvsigneret certifikat
- Opret en anmodning om certifikatunderskrift (CSR) og installer et certifikat fra en certifikatudstedende myndighed (CA)
- Import og eksport af certifikat og privat nøgle
- Import og eksport af et nøglecentercertifikat

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 organization, 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
- Adgang til webbaseret administration ved hjælp af SSL/TLS
- Installation af det selvsignerede certifikat for Windows-brugere som administrator
- Konfigurer certifikater for enhedssikkerhed

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
- Konfiguration af et certifikat for SSL/TLS og tilgængelige protokoller
- Konfigurer certifikater for enhedssikkerhed

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(Port 443)** i området **IPP**, og klik derefter på **Submit (Send)**.
8. Genstart maskinen for at aktivere konfigurationen.

Kommunikation med IPPS kan ikke forhindre unauthorized 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. Brug SNMPv3-tilstanden for at administrere printerserveren sikkert.
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 IPsec

Introduktion til IPsec

IPsec (Internet Protocol Security) er en sikkerhedsprotokol, der bruger en internetprotokolfunktion (valgfrit) til at forhindre datamanipulation og sikre fortroligheden for data, der overføres som IP-pakker. IPsec krypterer data, der sendes over et netværk, f.eks. udskriftsdata fra computere til en printer. Dataene krypteres i netværkslaget, og programmer, der bruger en protokol på et højere niveau, bruger IPsec, selvom brugeren ikke er klar over det.

IPsec understøtter følgende funktioner:

- IPsec-overførsler

  I henhold til IPsec-indstillingsforholdene sender en netværksforbundet computer data til og modtager data fra en angivet enhed ved hjælp af IPsec. Når enheder begynder at kommunikere ved hjælp af IPsec, udveksles først nøgler vha. Internet Key Exchange (IKE), og derefter overføres de krypterede data ved hjælp af nøglerne.

  Derudover har IPsec to driftstilstande: tilstanden Transport og tilstanden Tunnel. Tilstanden Transport bruges hovedsageligt til kommunikation mellem enheder, og tilstanden Tunnel bruges i miljøer som f.eks. Virtual Private Network (VPN).

For IPsec-overførsler er følgende forhold nødvendige:

- Den netværkstilsluttede computer kan kommunikere med IPsec.
- Maskinen er konfigureret til IPsec-kommunikation.
- Den computer, der er tilsluttet til maskinen, er konfigureret til IPsec-forbindelser.

- IPsec-indstillinger

  Indstillinger, der er nødvendige for at oprette forbindelse via IPsec. Indstillingerne kan konfigureres med Web Based Management.

For at konfigurere IPsec-indstillingerne, skal du bruge browseren på en computer, der er tilsluttet netværket.

Relaterede informationer

- Brug IPsec

Konfiguration af IPsec med Web Based Management

IPsec-forbindelsesbetingelserne omfatter to **Template (Skabelon)**-typer: **Address (adresse)** og **IPsec**. Du kan konfigurere op til 10 forbindelsesforhold.

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)** > **IPsec**i venstre navigationsbjælke.

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

Indstilling	Beskrivelse
Status	Aktiver eller deaktiver IPsec.
Negotiation Mode (Aftaletilstand)	Vælg **Negotiation Mode (Aftaletilstand)** for IKE Phase 1. IKE er en protokol, der bruges til at udveksle krypteringsnøgler med det formål at udføre krypteret kommunikation via IPsec. Hvis du vælger tilstanden **Main (Hoved)**, er behandlingshastigheden lav, men sikkerheden er høj. I tilstanden **Aggressive (Aggressiv)** er behandlingshastigheden hurtigere end i tilstanden **Main (Hoved)**, men sikkerheden er lavere.
All Non-IPsec Traffic (Al ikke-IPsec-traffik)	Vælg den handling, der skal udføres for ikke-IPsec-pakker. Når der bruges webtjenester, skal du vælge **Allow (Tillad)** for **All Non-IPsec Traffic (Al ikke-IPsec-traffik)**. Hvis du vælger **Drop (Ophæv)**, kan der ikke bruges webtjenester.
Broadcast/Multicast Bypass (Omgå udsendelse/multicast)	Markér **Enabled (Aktiveret)** eller **Disabled (Deaktiveret)**.
Protocol Bypass (Omgå protokol)	Markér afkrydsningsfelterne for den eller de ønskede indstillinger.
Rules (Regler)	Markér afkrydsningsfeltet for **Enabled (Aktiveret)** for at aktivere skabelonen. Når du vælger flere afkrydsningsfelter, har de lavere nummererede afkrydsningsfelter prioritet, hvis der er konflikt mellem indstillingerne for de valgte afkrydsningsfelter. Klik på den tilsvarende rulleliste for at vælge den **Address Template (Skabelon for adresse)**, der anvendes for IPsec-forbindelsesforholdene. Hvis du vil tilføje en **Address Template (Skabelon for adresse)**, skal du klikke på **Add Template (Skabelon for Tilføj)**. Klik på den tilsvarende rulleliste for at vælge den **IPsec Template (Skabelon for IPsec)**, der anvendes for IPsec-forbindelsesforholdene. Hvis du vil tilføje en **IPsec Template (Skabelon for IPsec)**, skal du klikke på **Add Template (Skabelon for Tilføj)**.

6. Klik på **Submit (Send)**.

   Hvis maskinen skal genstartes for at aktivere de nye indstillinger, vises skærmbilledet til bekræftelse af genstart.

Hvis der er en tom post i den skabelon, du aktiverer i tabellen **Rules (Regler)**, vises en fejlmeddelelse. Bekræft dine valg, og klik på **Submit (Send)** igen.

Relaterede informationer

- Brug IPsec

Relaterede emner:

- Konfigurer certifikater for enhedssikkerhed

Konfiguration af en IPsec-adresse med Web Based Management

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)** > **IPsec Address Template (Skabelon for IPsec-adresse)**i venstre navigationsbjælke.

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

5. Klik på knappen **Delete (Slet)** for at slette en **Address Template (Skabelon for adresse)**. Når en **Address Template (Skabelon for adresse)** er i brug, kan den ikke slettes.
6. Klik på nummeret for den **Address Template (Skabelon for adresse)**, der skal oprettes. **IPsec Address Template (Skabelon for IPsec-adresse)** bliver vist.
7. Konfigurer indstillingerne.

Indstilling	Beskrivelse
Template Name (Navn på skabelon)	Angiv et navn for skabelonen (op til 16 tegn).
Local IP Address (Lokal IP-adresse)	• **IP Address (IP-adresse)** Angiv IP-adressen. Vælg **ALL IPv4 Address (ALLE IPv4-adresser)**, **ALL IPv6 Address (ALLE IPv6-adresser)**, **ALL Link Local IPv6 (Alle Link-local-IPv6)** eller **Custom (Bruger)** fra rullelisten. Hvis du vælger **Custom (Bruger)** fra rullelisten, skal du skrive IP-adresse (IPv4 eller IPv6) i tekstfeltet. • **IP Address Range (IP-adresseområde)** Skriv den første og sidste IP-adresse i IP-adresseintervallet i tekstfelterne. Der opstår en fejl, hvis start- og slut-IP-adressen ikke understøtter IPv4 eller IPv6 standardized, eller hvis slut-IP-adressen er lavere end startadressen. • **IP Address / Prefix (IP-adresse/præfiks)** Angiv IP-adressen vha. CIDR-notation. Eksempelvis: 192.168.1.1/24 Da præfikset angives i form af en 24-bit undernetmaske (255.255.255.0) for 192.168.1.1, er adresserne 192.168.1.### er gyldige.
Remote IP Address (Fjern-IP-adresse)	• **Any (Enhver)** Hvis du vælger **Any (Enhver)**, bliver IP-adresser aktiveret. • **IP Address (IP-adresse)** Indtast den angivne IP-adresse (IPv4 eller IPv6) i tekstboksen. • **IP Address Range (IP-adresseområde)**

Indstilling	Beskrivelse
	Indtast første og sidste IP-adresse for IP-adresseområdet. Der vil opstå en fejl, hvis den første og sidste IP-adresse ikke er standardized til IPv4 eller IPv6, eller den sidste IP-adresse er lavere end den første adresse. • **IP Address / Prefix (IP-adresse/præfiks)** Angiv IP-adressen vha. CIDR-notation. Eksempelvis: 192.168.1.1/24 Da præfikset angives i form af en 24-bit undernetmaske (255.255.255.0) for 192.168.1.1, er adresserne 192.168.1.### er gyldige.

8. Klik på **Submit (Send)**.

Når du ændrer indstillingerne for den skabelon, der aktuelt er i brug, skal du genstarte maskinen for at aktivere konfigurationen.

Relaterede informationer

- Brug IPsec

Konfiguration af IPsec-skabelon med Web Based Management

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)** > **IPsec Template (Skabelon for IPsec)**i venstre navigationsbjælke.

   Start navigationen fra ☰, hvis venstre navigationsbjælke ikke er synlig.
5. Klik på knappen **Delete (Slet)** for at slette en **IPsec Template (Skabelon for IPsec)**. Når en **IPsec Template (Skabelon for IPsec)** er i brug, kan den ikke slettes.
6. Klik på den **IPsec Template (Skabelon for IPsec)**, der skal oprettes. Hvis skærmen **IPsec Template (Skabelon for IPsec)** vises. Konfigurationsfelterne varierer baseret på de indstillinger for **Use Prefixed Template (Brug skabelon med præfiks)** og **Internet Key Exchange (IKE)**, du vælger.
7. Gå til feltet **Template Name (Navn på skabelon)**, og navngiv skabelonen (op til 16 tegn).
8. Hvis du har valgt **Custom (Bruger)** i **Use Prefixed Template (Brug skabelon med præfiks)** rullelisten, skal du vælge **Internet Key Exchange (IKE)** indstillingerne og derefter ændre indstillingerne efter behov.
9. Klik på **Submit (Send)**.

Relaterede informationer

- Brug IPsec
  - IKEv1-indstillinger for en IPsec-skabelon
  - IKEv2-indstillinger for en IPsec-skabelon
  - Manuel indstilling af en IPsec-skabelon

IKEv1-indstillinger for en IPsec-skabelon

Indstilling	Beskrivelse
Template Name (Navn på skabelon)	Angiv et navn for skabelonen (op til 16 tegn).
Use Prefixed Template (Brug skabelon med præfiks)	Vælg **Custom (Bruger)**, **IKEv1 High Security (IKEv1 med høj sikkerhed)** eller **IKEv1 Medium Security (IKEv1 med middel sikkerhed)**. Indstillingselementerne varierer afhængigt af den valgte skabelon.
Internet Key Exchange (IKE)	IKE er en kommunikationsprotokol, der bruges til at udveksle krypteringsnøgler med det formål at udføre krypteret kommunikation via IPsec. Den krypterede kommunikation udføres kun på det pågældende tidspunkt, og derfor fastsættes den krypteringsalgoritme, der er nødvendig for IPsec, og krypteringsnøglerne deles. Ved IKE udveksles krypteringsnøglerne via Diffie-Hellman-nøgleudvekslingsmetoden, og der udføres en krypterede kommunikation, der er begrænset til IKE. Hvis du har valgt **Custom (Bruger)** i **Use Prefixed Template (Brug skabelon med præfiks)**, skal du vælge **IKEv1**.
Authentication Type (Godkendelsestype)	• **Diffie-Hellman Group** Denne nøgleudvekslingsmetode muliggør sikker udveksling af hemmelige nøgler på et ubeskyttet netværk. Diffie-Hellman-nøgleudvekslingsmetoden bruger et diskret logaritmeproblem, ikke en hemmelig nøgle, til at sende og modtage åbne oplysninger, der er genereret ved hjælp af et vilkårligt tal og den hemmelige nøgle. Vælg **Group1 (Gruppe1)**, **Group2 (Gruppe2)**, **Group5 (Gruppe5)** eller **Group14 (Gruppe14)**. • **Encryption (Kryptering)** Vælg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Vælg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SF-levetid)** Angiv IKE SA-livstiden. Indtast tid (sekunder) og antal kilobytes (kB).
Encapsulating Security (Indkapsling af sikkerhed)	• **Protocol (Protokol)** Vælg **ESP**, **AH** eller **AH+ESP**. - ESP er en protokol til gennemførsel af krypteret kommunikation vha. IPsec. ESP krypterer dataene (kommunikeret indhold) og tilføjer yderligere oplysninger. En IP-pakke består af en header og de krypterede data, der følger headeren. Ud over de krypterede data indeholder IP-pakken også oplysninger om krypteringsmetoden og krypteringsnøglen, godkendelsesdataene osv. - AH er en del af IPsec-protokollen, der godkender afsenderen og forhindrer datamanipulation (sikrer fuldstændighed). I en IP-pakke indsættes dataene umiddelbart efter headeren. Derud over indeholder pakkerne en hash-værdi, der beregnes ved hjælp af en ligning fra det kommunikerede indhold, hemmelig nøgle osv., for at undgå forfalskning af afsenderen og datamanipulation. Modsat ESP sker der ingen kryptering af det kommunikerede indhold, og dataene sendes og modtages som almindelig tekst. • **Encryption (Kryptering) (Ikke tilgængelig for valgmuligheden AH).** Vælg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**.

Indstilling	Beskrivelse
	• **Hash** Vælg **None (Ingen)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Ingen)** kan kun vælges, når **ESP** er valgt for **Protocol (Protokol)**. • **SA Lifetime (SF-levetid)** Angiv levetiden for IKE SA. Indtast tiden (sekunder) og antallet af kilobytes (kbytes). • **Encapsulation Mode (Indkapslingstilstand)** Markér **Transport (Transport)** eller **Tunnel (Tunnel)**. • **Remote Router IP-Address (Fjernrouter-IP-adresse)** Indtast IP-adressen (IPv4 eller IPv6) for fjernrouteren. Disse oplysninger skal kun indtastes, når tilstanden **Tunnel (Tunnel)** er valgt. SA (Security Association) er en krypteret kommunikationsmetode, der udveksler og deler oplysninger via IPsec eller IPv6, f.eks. krypteringsmetode og krypteringsnøgle, med henblik på at skabe en sikker kommunikationskanal, før kommunikationen starter. SA kan også henvise til en oprettet virtuel krypteret kommunikationskanal. SA til IPsec opretter krypteringsmetoden, udveksler nøglerne og udfører fælles godkendelse i overensstemmelse med standardproceduren IKE (Internet Key Exchange). Derudover opdateres SA med jævne mellemrum.
Perfect Forward Secrecy (PFS) (Perfekt videresending i fortrolighed)	PFS henter ikke nøgler fra tidligere nøgler, der er blevet brugt til kryptering af meddelelser. Hvis en nøgle, der bruges til at kryptere en meddelelse, blev afledt fra en overordnet nøgle, bruges den pågældende overordnede nøgle ikke til at aflede andre nøgler. Hvis en nøgle kompromitteres, begrænses skadens omfang til de beskeder, der er blevet krypteret med den pågældende nøgle. Vælg **Enabled (Aktiveret)** eller **Disabled (Deaktiveret)**.
Authentication Method (Godkendelsesmetode)	Vælg godkendelsesmetoden. Vælg **Pre-Shared Key (Forhåndsdelt nøgle)** eller **Certificates (Certifikater)**.
Pre-Shared Key (Forhåndsdelt nøgle)	Ved kryptering af kommunikation udveksles og deles krypteringsnøglen på forhånd ved hjælp af en anden kanal. Hvis du har valgt **Pre-Shared Key (Forhåndsdelt nøgle)** til **Authentication Method (Godkendelsesmetode)**, skal du indtaste **Pre-Shared Key (Forhåndsdelt nøgle)** (op til 32 tegn). • **Local/ID Type/ID (Sprog/ID-type/ID)** Vælg afsenderens ID-type, og indtast derefter ID'et. Vælg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-mailadresse)** eller **Certificate (Certifikat)** for den pågældende type. Hvis du vælger **Certificate (Certifikat)**, skal du indtaste fællesnavnet for certifikatet i feltet **ID (Id)**. • **Remote/ID Type/ID (Fjern/ID-type/ID)** Vælg modtagerens ID-type, og indtast derefter ID'et. Vælg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-mailadresse)** eller **Certificate (Certifikat)** for den pågældende type. Hvis du vælger **Certificate (Certifikat)**, skal du indtaste fællesnavnet for certifikatet i feltet **ID (Id)**.
Certificate (Certifikat)	Hvis du har valgt **Certificates (Certifikater)** for **Authentication Method (Godkendelsesmetode)**, skal du vælge certifikatet.

Indstilling	Beskrivelse
	Du kan kun vælge de certifikater, der blev oprettet ved hjælp af siden **Certificate (Certifikat)** i Webbaseret administrations skærmbillede til konfiguration af sikkerheden.

Relaterede informationer

- Konfiguration af IPsec-skabelon med Web Based Management

IKEv2-indstillinger for en IPsec-skabelon

Indstilling	Beskrivelse
Template Name (Navn på skabelon)	Angiv et navn for skabelonen (op til 16 tegn).
Use Prefixed Template (Brug skabelon med præfiks)	Vælg **Custom (Bruger)**, **IKEv2 High Security (IKEv2 med høj sikkerhed)** eller **IKEv2 Medium Security (IKEv2 med middel sikkerhed)**. Indstillingselementerne varierer afhængigt af den valgte skabelon.
Internet Key Exchange (IKE)	IKE er en kommunikationsprotokol, der bruges til at udveksle krypteringsnøgler med det formål at udføre krypteret kommunikation via IPsec. Den krypterede kommunikation udføres kun på det pågældende tidspunkt, og derfor fastsættes den krypteringsalgoritme, der er nødvendig for IPsec, og krypteringsnøglerne deles. Ved IKE udveksles krypteringsnøglerne via Diffie-Hellman-nøgleudvekslingsmetoden, og der udføres en krypterede kommunikation, der er begrænset til IKE. Hvis du har valgt **Custom (Bruger)** i **Use Prefixed Template (Brug skabelon med præfiks)**, skal du vælge **IKEv2**.
Authentication Type (Godkendelsestype)	• **Diffie-Hellman Group** Denne nøgleudvekslingsmetode muliggør sikker udveksling af hemmelige nøgler på et ubeskyttet netværk. Diffie-Hellman-nøgleudvekslingsmetoden bruger et diskret logaritmeproblem, ikke en hemmelig nøgle, til at sende og modtage åbne oplysninger, der er genereret ved hjælp af et vilkårligt tal og den hemmelige nøgle. Vælg **Group1 (Gruppe1)**, **Group2 (Gruppe2)**, **Group5 (Gruppe5)** eller **Group14 (Gruppe14)**. • **Encryption (Kryptering)** Vælg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Vælg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SF-levetid)** Angiv IKE SA-livstiden. Indtast tid (sekunder) og antal kilobytes (kB).
Encapsulating Security (Indkapsling af sikkerhed)	• **Protocol (Protokol)** Vælg **ESP**. ESP er en protokol til gennemførsel af krypteret kommunikation vha. IPsec. ESP krypterer dataene (kommunikeret indhold) og tilføjer yderligere oplysninger. En IP-pakke består af en header og de krypterede data, der følger headeren. Ud over de krypterede data indeholder IP-pakken også oplysninger om krypteringsmetoden og krypteringsnøglen, godkendelsesdataene osv. • **Encryption (Kryptering)** Vælg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Vælg **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SF-levetid)** Angiv levetiden for IKE SA. Indtast tiden (sekunder) og antallet af kilobytes (kbytes). • **Encapsulation Mode (Indkapslingstilstand)** Markér **Transport (Transport)** eller **Tunnel (Tunnel)**.

Indstilling	Beskrivelse
	• **Remote Router IP-Address (Fjernrouter-IP-adresse)** Indtast IP-adressen (IPv4 eller IPv6) for fjernrouteren. Disse oplysninger skal kun indtastes, når tilstanden **Tunnel (Tunnel)** er valgt. SA (Security Association) er en krypteret kommunikationsmetode, der udveksler og deler oplysninger via IPsec eller IPv6, f.eks. krypteringsmetode og krypteringsnøgle, med henblik på at skabe en sikker kommunikationskanal, før kommunikationen starter. SA kan også henvise til en oprettet virtuel krypteret kommunikationskanal. SA til IPsec opretter krypteringsmetoden, udveksler nøglerne og udfører fælles godkendelse i overensstemmelse med standardproceduren IKE (Internet Key Exchange). Derudover opdateres SA med jævne mellemrum.
Perfect Forward Secrecy (PFS) (Perfekt videresending i fortrolighed)	PFS henter ikke nøgler fra tidligere nøgler, der er blevet brugt til kryptering af meddelelser. Hvis en nøgle, der bruges til at kryptere en meddelelse, blev afledt fra en overordnet nøgle, bruges den pågældende overordnede nøgle ikke til at aflede andre nøgler. Hvis en nøgle kompromitteres, begrænses skadens omfang til de beskeder, der er blevet krypteret med den pågældende nøgle. Vælg **Enabled (Aktiveret)** eller **Disabled (Deaktiveret)**.
Authentication Method (Godkendelsesmetode)	Vælg godkendelsesmetoden. Vælg **Pre-Shared Key (Forhåndsdelt nøgle)**, **Certificates (Certifikater)**, **EAP - MD5** eller **EAP - MS-CHAPv2**. EAP er en godkendelsesprotokol, der er en udvidelse af PPP. Ved anvendelse af EAP med IEEE802.1x bruges der en ny nøgle til brugergodkendelse under hver session. Du skal kun bruge følgende indstillinger, når der er valgt **EAP - MD5** eller **EAP - MS-CHAPv2** under **Authentication Method (Godkendelsesmetode)**: • **Mode (tilstand)** Markér **Server-Mode (Servertilstand)** eller **Client-Mode (Klienttilstand)**. • **Certificate (Certifikat)** Vælg certifikatet. • **User Name (Brugernavn)** Indtast brugernavnet (op til 32 tegn). • **Password (Adgangskode)** Indtast adgangskoden (op til 32 tegn). Adgangskoden skal indtastes to gange for at bekræfte den.
Pre-Shared Key (Forhåndsdelt nøgle)	Ved kryptering af kommunikation udveksles og deles krypteringsnøglen på forhånd ved hjælp af en anden kanal. Hvis du har valgt **Pre-Shared Key (Forhåndsdelt nøgle)** til **Authentication Method (Godkendelsesmetode)**, skal du indtaste **Pre-Shared Key (Forhåndsdelt nøgle)** (op til 32 tegn). • **Local/ID Type/ID (Sprog/ID-type/ID)** Vælg afsenderens ID-type, og indtast derefter ID'et. Vælg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-mailadresse)** eller **Certificate (Certifikat)** for den pågældende type. Hvis du vælger **Certificate (Certifikat)**, skal du indtaste fællesnavnet for certifikatet i feltet **ID (Id)**. • **Remote/ID Type/ID (Fjern/ID-type/ID)** Vælg modtagerens ID-type, og indtast derefter ID'et.

Indstilling	Beskrivelse
	Vælg **IPv4 Address (IPv4-adresse)**, **IPv6 Address (IPv6-adresse)**, **FQDN**, **E-mail Address (E-mailadresse)** eller **Certificate (Certifikat)** for den pågældende type. Hvis du vælger **Certificate (Certifikat)**, skal du indtaste fællesnavnet for certifikatet i feltet **ID (Id)**.
Certificate (Certifikat)	Hvis du har valgt **Certificates (Certifikater)** for **Authentication Method (Godkendelsesmetode)**, skal du vælge certifikatet. Du kan kun vælge de certifikater, der blev oprettet ved hjælp af siden **Certificate (Certifikat)** i Webbaseret administrations skærmbillede til konfiguration af sikkerheden.

Relaterede informationer

- Konfiguration af IPsec-skabelon med Web Based Management

Manuel indstilling af en IPsec-skabelon

Indstilling	Beskrivelse
Template Name (Navn på skabelon)	Angiv et navn for skabelonen (op til 16 tegn).
Use Prefixed Template (Brug skabelon med præfiks)	Vælg **Custom (Bruger)**.
Internet Key Exchange (IKE)	IKE er en kommunikationsprotokol, der bruges til at udveksle krypteringsnøgler med det formål at udføre krypteret kommunikation via IPsec. Den krypterede kommunikation udføres kun på det pågældende tidspunkt, og derfor fastsættes den krypteringsalgoritme, der er nødvendig for IPsec, og krypteringsnøglerne deles. Ved IKE udveksles krypteringsnøglerne via Diffie-Hellman-nøgleudvekslingsmetoden, og der udføres en krypterede kommunikation, der er begrænset til IKE. Vælg **Manual (Manuel)**.
Authentication Key (ESP, AH) (Godkendelsesnøgle (ESP, AH))	Indtast **In/Out (In/out)**-værdierne. Disse indstillinger er nødvendige, når **Custom (Bruger)** er valgt for **Use Prefixed Template (Brug skabelon med præfiks)**, **Manual (Manuel)** er valgt for **Internet Key Exchange (IKE)** og en anden indstilling end **None (Ingen)** er valgt for **Hash** for afsnittet **Encapsulating Security (Indkapsling af sikkerhed)**. Det tilgængelige antal tegn varierer, afhængigt af den valgte indstilling for **Hash** i afsnittet **Encapsulating Security (Indkapsling af sikkerhed)**. Hvis længden af den angivne godkendelsesnøgle er forskellig fra den valgte firkantalgoritme, opstår der en fejl. • **MD5**: 128 bit (16 bytes) • **SHA1**: 160 bit (20 bytes) • **SHA256**: 256 bit (32 bytes) • **SHA384**: 384 bit (48 bytes) • **SHA512**: 512 bit (64 bytes) Når du angiver nøglen i ASCII-kode, skal tegnene omgives af dobbelte anførselstegn (").
Code key (ESP) (Kodenøgle (ESP))	Indtast **In/Out (In/out)**-værdierne. Disse indstillinger er nødvendige, når **Custom (Bruger)** er valgt for **Use Prefixed Template (Brug skabelon med præfiks)**, **Manual (Manuel)** er valgt for **Internet Key Exchange (IKE)** og **ESP** er valgt for **Protocol (Protokol)** i **Encapsulating Security (Indkapsling af sikkerhed)**. Det tilgængelige antal tegn varierer, afhængigt af den valgte indstilling for **Encryption (Kryptering)** i afsnittet **Encapsulating Security (Indkapsling af sikkerhed)**. Hvis længden af den angivne kodenøgle er forskellig fra den valgte krypteringsalgoritme, opstår der en fejl. • **DES**: 64 bit (8 bytes) • **3DES**: 192 bit (24 bytes) • **AES-CBC 128**: 128 bit (16 bytes) • **AES-CBC 256**: 256 bit (32 bytes) Når du angiver nøglen i ASCII-kode, skal tegnene omgives af dobbelte anførselstegn (").
SPI	Disse parametre bruges til at identificere sikkerhedsoplysninger. En vært har generelt flere SA'er (Security Association) for flere typer IPsec-kommunikation. Det er derfor nødvendigt at identificere den gældende

Indstilling	Beskrivelse
	SA, når der modtages en IPsec-pakke. SPI-parameteren, som identificerer SA, er inkluderet i Authentication Header (AH) og Encapsulating Security Payload (ESP) header. Indstillingerne er nødvendige, når der er valgt **Custom (Bruger)** for **Use Prefixed Template (Brug skabelon med præfiks)**, og når der er valgt **Manual (Manuel)** for **Internet Key Exchange (IKE)**. Indtast værdierne **In/Out (In/out)**. Der må være 3-10 tegn.
Encapsulating Security (Indkapsling af sikkerhed)	• **Protocol (Protokol)** Vælg **ESP** eller **AH**. - ESP er en protokol til gennemførsel af krypteret kommunikation vha. IPsec. ESP krypterer dataene (kommunikeret indhold) og tilføjer yderligere oplysninger. En IP-pakke består af en header og de krypterede data, der følger headeren. Ud over de krypterede data indeholder IP-pakken også oplysninger om krypteringsmetoden og krypteringsnøglen, godkendelsesdataene osv. - AH er en del af IPsec-protokollen, der godkender afsenderen og forhindrer datamanipulation (sikrer, at dataene er fuldstændige). I en IP-pakke indsættes dataene umiddelbart efter headeren. Derud over indeholder pakkerne en hashværdi, der beregnes ved hjælp af en ligning fra det kommunikerede indhold, hemmelig nøgle osv., for at undgå forfalskning af afsenderen og datamanipulation. Modsat ESP sker der ingen kryptering af det kommunikerede indhold, og dataene sendes og modtages som almindelig tekst. • **Encryption (Kryptering) (Ikke tilgængelig for valgmuligheden AH).** Vælg **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Vælg **None (Ingen)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Ingen)** kan kun vælges, når **ESP** er valgt for **Protocol (Protokol)**. • **SA Lifetime (SF-levetid)** Angiv levetiden for IKE SA. Indtast tiden (sekunder) og antallet af kilobytes (kbytes). • **Encapsulation Mode (Indkapslingstilstand)** Markér **Transport (Transport)** eller **Tunnel (Tunnel)**. • **Remote Router IP-Address (Fjernrouter-IP-adresse)** Indtast IP-adressen (IPv4 eller IPv6) for fjernrouteren. Disse oplysninger skal kun indtastes, når tilstanden **Tunnel (Tunnel)** er valgt. SA (Security Association) er en krypteret kommunikationsmetode, der udveksler og deler oplysninger via IPsec eller IPv6, f.eks. krypteringsmetode og krypteringsnøgle, med henblik på at skabe en sikker kommunikationskanal, før kommunikationen starter. SA kan også henvise til en oprettet virtuel krypteret kommunikationskanal. SA til IPsec opretter krypteringsmetoden, udveksler nøglerne og udfører fælles godkendelse i overensstemmelse med standardproceduren IKE (Internet Key Exchange). Derudover opdateres SA med jævne mellemrum.

Relaterede informationer

- Konfiguration af IPsec-skabelon med Web Based Management

Brug IEEE 802.1x-godkendelse til dit netværk

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

Hvad er IEEE 802.1x-godkendelse?

IEEE 802.1x er en IEEE-standard, der begrænser adgangen fra unauthorized 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 tunneled 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

Brugergodkendelse

- Brug Active Directory-godkendelse
- Brug LDAP-godkendelse
- Brug af Secure Function Lock (sikker funktionslås) 3.0

Brug Active Directory-godkendelse

- Introduktion til Active Directory Authentication
- Konfiguration af Active Directory Authentication med Web Based Management
- Log på for at ændre maskinens indstillinger via kontrolpanelet (Active Directory Authentication)

Introduktion til Active Directory Authentication

Active Directory Authentication begrænser brugen af maskinen. Hvis Active Directory Authentication er aktiveret, låses maskinens kontrolpanel. Du kan ikke ændre maskinens indstillinger, før du indtaster et bruger-id og en adgangskode.

Active Directory Authentication indeholder følgende funktioner:

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

- Lagring af indgående udskriftsdata
- Lagring af indgående faxdata
- Henter e-mailadressen fra Active Directory-serveren baseret på dit bruger-ID ved afsendelse af scannede data til en e-mailserver.

  For at bruge denne funktion skal du vælge muligheden **On (Til)** for indstillingen **Get Mail Address (Hent mailadresse)** og godkendelsesmetode **LDAP + kerberos** eller **LDAP + NTLMv2**. Din e-mailadresse vil blive angivet som afsender, når maskinen sender scannede data til en e-mailserver, eller som modtager, hvis du vil sende de scannede data til din e-mailadresse.

Når Active Directory Authentication er aktiveret, gemmer maskinen alle indgående faxdata. Når du logger på, udskriver maskinen alle lagrede faxdata.

Du kan ændre indstillingerne for Active Directory Authentication ved hjælp af webbaseret administration.

Relaterede informationer

- Brug Active Directory-godkendelse

Konfiguration af Active Directory Authentication med Web Based Management

Funktionen Active Directory Authentication understøtter Kerberos-godkendelse og NTLMv2-godkendelse. Du skal konfigurere SNTP-protokollen (netværkstidsserver) og DNS-serverkonfiguration til godkendelse.

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 **Administrator** > **User Restriction Function (Brugerbegrænsning)** eller **Restriction Management (Begrænsningshåndtering)** i venstre navigationsbjælke.

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

5. Vælg **Active Directory Authentication (Active Directory-godkendelse)**.
6. Klik på **Submit (Send)**.
7. Klik på **Active Directory Authentication (Active Directory-godkendelse)**.
8. Konfigurer følgende indstillinger:

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

Indstilling	Beskrivelse
Storage Fax RX Data (Lagring af indgående data på fax)	Vælg denne indstilling for at gemme indgående faxdata. Alle indgående faxdata kan udskrives, når du er logget på maskinen.
Remember User ID (Husk bruger-id)	Vælg denne indstilling for at gemme dit bruger-id.
Active Directory Server Address (Active Directory-serveradresse)	Indtast IP-adressen eller servernavnet (for eksempel ad.eksempel.dk) på Active Directory-serveren.
Active Directory Domain Name (Active Directory-domænenavn)	Skriv domænenavnet for det aktive bibliotek.
Protocol & Authentication Method (Protokol- og godkendelsesmetode)	Vælg protokol- og godkendelsesmetoden.
SSL/TLS	Vælg **SSL/TLS**.
LDAP Server Port (LDAP-serverport)	Indtast portnummeret for at oprette forbindelse til Active Directory-serveren via LDAP (kun tilgængeligt for godkendelsesmetoderne **LDAP + kerberos** eller **LDAP + NTLMv2**).

Indstilling	Beskrivelse
LDAP Search Root (LDAP-søgningsrod)	Indtast LDAP-søgningens rod (kun tilgængeligt for godkendelsesmetoderne **LDAP + kerberos** eller **LDAP + NTLMv2**).
Get Mail Address (Hent mailadresse)	Vælg denne indstilling for at hente e-mailadressen for brugeren, der er logget på, fra Active Directory-serveren. (kun tilgængeligt for godkendelsesmetoderne **LDAP + kerberos** eller **LDAP + NTLMv2**)
Get User's Home Directory (Hent brugers hjemmemappe)	Vælg denne indstilling for at få din startmappe som destination for scanning til netværk. (kun tilgængeligt for godkendelsesmetoderne **LDAP + kerberos** eller **LDAP + NTLMv2**)

9. Klik på **Submit (Send)**.

Relaterede informationer

- Brug Active Directory-godkendelse

Log på for at ændre maskinens indstillinger via kontrolpanelet (Active Directory Authentication)

Når Active Directory Authentication er aktiveret, låses maskinens kontrolpanel, indtil du indtaster et bruger-ID og en adgangskode på maskinens kontrolpanel.

1. På maskinens kontrolpanel skal du indtaste dit bruger-id og din adgangskode for at logge på.
2. Når godkendelsen er fuldført, låses maskinens kontrolpanel op.

Relaterede informationer

- Brug Active Directory-godkendelse

Brug LDAP-godkendelse

- Introduktion til LDAP-godkendelse
- Konfiguration af LDAP-godkendelse med Web Based Management
- Log på for at ændre maskinens indstillinger via kontrolpanelet (LDAP-godkendelse)

Introduktion til LDAP-godkendelse

LDAP-godkendelse begrænser brugen af maskinen. Hvis du har aktiveret LDAP-godkendelse, deaktiveres maskinens kontrolpanel. Du kan ikke ændre maskinens indstillinger, før du indtaster et bruger-id og en adgangskode.

LDAP-godkendelse tilbyder følgende funktioner:

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

- Lagring af indgående udskriftsdata
- Lagring af indgående faxdata
- Henter e-mailadressen fra LDAP-serveren baseret på dit bruger-ID ved afsendelse af scannede data til en e-mailserver.

  For at bruge denne funktion skal du vælge muligheden **On (Til)** for indstillingen **Get Mail Address (Hent mailadresse)** . Din e-mailadresse vil blive angivet som afsender, når maskinen sender scannede data til en e-mailserver, eller som modtager, hvis du vil sende de scannede data til din e-mailadresse.

Når du har aktiveret LDAP-godkendelse, gemmer maskinen alle indgående faxdata. Når du logger på, udskriver maskinen alle lagrede faxdata.

Du kan ændre LDAP-godkendelsesindstillingerne ved hjælp af webbaseret administration.

Relaterede informationer

- Brug LDAP-godkendelse

Konfiguration af LDAP-godkendelse med Web Based Management

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 **Administrator** > **User Restriction Function (Brugerbegrænsning)** eller **Restriction Management (Begrænsningshåndtering)** i venstre navigationsbjælke.

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

5. Vælg **LDAP Authentication (LDAP-godkendelse)**.
6. Klik på **Submit (Send)**.
7. Klik på menuen **LDAP Authentication (LDAP-godkendelse)**.
8. Konfigurer følgende indstillinger:

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

Indstilling	Beskrivelse
Storage Fax RX Data (Lagring af indgående data på fax)	Vælg denne indstilling for at gemme indgående faxdata. Alle indgående faxdata kan udskrives, når du er logget på maskinen.
Remember User ID (Husk bruger-id)	Vælg denne indstilling for at gemme dit bruger-id.
LDAP Server Address (LDAP-serveradresse)	Indtast IP-adressen eller servernavnet (for eksempel ldap.eksempel.dk) for LDAP-serveren.
SSL/TLS	Vælg indstillingen **SSL/TLS** for at bruge LDAP over SSL/TLS.
LDAP Server Port (LDAP-serverport)	Skriv LDAP-serverportens nummer.
LDAP Search Root (LDAP-søgningsrod)	Indtast LDAP-søgningens rodmappe.
Attribute of Name (Search Key) (Attributnavn (Søgenøgle))	Skriv den attribut, du vil bruge som søgenøgle.
Get Mail Address (Hent mailadresse)	Vælg denne indstilling for at hente e-mailadresse for brugeren, der er logget på, fra LDAP-serveren.
Get User's Home Directory (Hent brugers hjemmemappe)	Vælg denne indstilling for at få din startmappe som destination for scanning til netværk.

9. Klik på **Submit (Send)**.

Relaterede informationer

- Brug LDAP-godkendelse

Log på for at ændre maskinens indstillinger via kontrolpanelet (LDAP-godkendelse)

Når LDAP-godkendelse er aktiveret, låses maskinens kontrolpanel, indtil du indtaster et bruger-ID og en adgangskode på maskinens kontrolpanel.

1. På maskinens kontrolpanel skal du indtaste dit bruger-id og din adgangskode for at logge på.
2. Når godkendelsen er fuldført, låses maskinens kontrolpanel op.

Relaterede informationer

- Brug LDAP-godkendelse

Brug af Secure Function Lock (sikker funktionslås) 3.0

Secure Function Lock (sikker funktionslås) 3.0 øger sikkerheden ved at begrænse tilgængelige funktioner på maskinen.

Før brug af Secure Function Lock 3.0

Brug Secure Function Lock (sikker funktionslås) til at konfigurere adgangskoder, indstille specifikke brugersidebegrænsninger og give adgang til nogle af eller alle de angivne funktioner.

Du kan konfigurere og ændre følgende indstillinger for Secure Function Lock (sikker funktionslås) 3.0 med webbaseret administration:

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

- **Print (Udskriv)**
- **Copy (Kopi)**
- **Scan**
- **Fax**
- **Media (Medier)**
- **Web Connect (Webtilslutning)**
- **Apps**
- **Page Limits (Sidebegrænsning)**
- **Page Counters (Sidetæller)**
- **Card ID (NFC ID) (Kort-id (NFC-id))**

Modeller med touchskærmdisplay:

Når Secure Function Lock (sikker funktionslås) er aktiveret, skifter maskinen automatisk til offentlig tilstand, og nogle af maskinens funktioner begrænses til udelukkende at kunne bruges af authorized brugere. For at få adgang til de begrænsede maskinfunktioner skal du trykke på , vælge dit brugernavn og indtaste din adgangskode.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Konfiguration af Secure Function Lock 3.0 med Web Based Management

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 **Administrator** > **User Restriction Function (Brugerbegrænsning)** eller **Restriction Management (Begrænsningshåndtering)** i venstre navigationsbjælke.

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

5. Vælg **Secure Function Lock (Sikker funktionslås)**.
6. Klik på **Submit (Send)**.
7. Klik på menuen **Restricted Functions (Begrænsede funktioner)**.
8. Konfigurer indstillingerne for at administrere begrænsningerne pr. bruger eller pr. gruppe.
9. Klik på **Submit (Send)**.
10. Klik på menuen **User List (Brugerliste)**.
11. Konfigurer brugerlisten.
12. Klik på **Submit (Send)**.

Du kan også ændre brugerlistespærreindstillingerne i menuen **Secure Function Lock (Sikker funktionslås)**.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Scanning med Secure Function Lock 3.0

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

Indstilling af scanningsbegrænsning (for administratorer)

Secure Function Lock (sikker funktionslås) 3.0 gør det muligt for en administrator at begrænse, hvilke brugere der kan scanne. Når scanningsfunktionen er indstillet til Fra for adgang for offentlige brugere, kan kun brugere, for hvem afkrydsningsfeltet **Scan** er markeret, scanne.

Brug af scanning (for brugere med begrænsede rettigheder)

- Sådan scannes ved hjælp af maskinens kontrolpanel:

  Brugere med begrænsede rettigheder skal indtaste deres adgangskode på maskinens betjeningspanel for at få adgang til scanningsfunktionen.
- Sådan scannes fra en computer:

  Brugere med begrænsede rettigheder skal indtaste deres adgangskode på maskinens betjeningspanel, før de kan scanne fra deres computere. Hvis adgangskoden ikke indtastes på maskinens betjeningspanel, vises en fejlmeddelelse på brugerens computer.

Hvis maskinen understøtter IC-kortgodkendelse, kan brugere med begrænsede rettigheder også få adgang til scanningsfunktionen ved at holde deres registrerede IC-kort mod NFC-symbolet på maskinens betjeningspanel.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Konfiguration af offentlig tilstand for Secure Function Lock 3.0

Brug skærmen Secure Function Lock til at konfigurere offentlig tilstand, der begrænser de funktioner, som er tilgængelige for offentlige brugere. Offentlige brugere behøver ikke at indtaste en adgangskode for at bruge funktionerne, der vælges under denne indstilling.

Offentlig tilstand omfatter udskriftsjob sendt via Brother iPrint&Scan og Brother Mobile Connect.

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 **Administrator** > **User Restriction Function (Brugerbegrænsning)** eller **Restriction Management (Begrænsningshåndtering)** i venstre navigationsbjælke.

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

5. Vælg **Secure Function Lock (Sikker funktionslås)**.
6. Klik på **Submit (Send)**.
7. Klik på menuen **Restricted Functions (Begrænsede funktioner)**.
8. Markér et afkrydsningsfelt i rækken **Public Mode (Offentlig tilstand)** for at tillade, eller fjern markeringen i et afkrydsningsfelt for at begrænse, den anførte funktion.
9. Klik på **Submit (Send)**.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Konfigurer indstillinger for den personlige startskærm ved hjælp af Webbaseret administration

Som administrator kan du angive, hvilke faner brugere kan se på deres personlige startskærme. Disse faner giver hurtig adgang til brugernes favorite genveje, som de kan tildele til fanerne på deres personlige startskærm fra maskinens betjeningspanel.

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

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 **Administrator** > **User Restriction Function (Brugerbegrænsning)** eller **Restriction Management (Begrænsningshåndtering)** i venstre navigationsbjælke.

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

5. Vælg **Secure Function Lock (Sikker funktionslås)**.
6. I feltet **Tab Settings (Faneindstillinger)** skal du vælge **Personal (Personligt)** for de fanenavne, som du vil bruge som din personlige startskærm.
7. Klik på **Submit (Send)**.
8. Klik på menuen **Restricted Functions (Begrænsede funktioner)**.
9. Konfigurer indstillingerne for at administrere begrænsningerne pr. bruger eller pr. gruppe.
10. Klik på **Submit (Send)**.
11. Klik på menuen **User List (Brugerliste)**.
12. Konfigurer brugerlisten.
13. Vælg **User List / Restricted Functions (Brugerliste/begrænsede funktioner)** fra rullelisten for den enkelte bruger.
14. Vælg fanenavnet **Home Screen (Startskærm)** på rullelisten for hver bruger.
15. Klik på **Submit (Send)**.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Yderligere funktioner i Secure Function Lock 3.0

Konfigurer følgende funktioner på skærmen Secure Function Lock (sikker funktionslås):

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

All Counter Reset (Nulstil alle tællere)

Klik på **All Counter Reset (Nulstil alle tællere)** i kolonnen **Page Counters (Sidetæller)** for at nulstille sidetælleren.

Export to CSV file (Eksportér til CSV-fil)

Klik på **Export to CSV file (Eksportér til CSV-fil)** for at eksportere den aktuelle og sidste sidetæller inklusive **User List / Restricted Functions (Brugerliste/begrænsede funktioner)**-information som CSV-fil.

Card ID (NFC ID) (Kort-id (NFC-id))

Klik på menuen **User List (Brugerliste)**, og skriv derefter en brugers kort-id i feltet **Card ID (NFC ID) (Kort-id (NFC-id))**. Du kan bruge dit IC-kort til godkendelse.

Output

Hvis Mailboks-enheden er installeret på maskinen, skal du vælge outputbakke for hver bruger fra rullelisten.

Last Counter Record (Sidste tællerregistrering)

Klik på **Last Counter Record (Sidste tællerregistrering)**, hvis maskinen skal bevare sidetællingen, efter at tælleren er nulstillet.

Counter Auto Reset (Aut. tællernulstilling)

Klik på **Counter Auto Reset (Aut. tællernulstilling)** for at konfigurere det ønskede tidsinterval mellem sidetællernulstillinger. Vælg dagligt, ugentligt eller månedligt.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Registrer et nyt IC-kort vha. maskinens betjeningspanel

Du kan registrere integrerede kredsløbskort (IC-kort) på maskinen.

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

1. Rør ved symbolet NFC-symbolet (Near-Field Communication) på maskinens betjeningspanel med et registreret, integreret kredsløbskort (IC-kort).
2. Tryk på dit bruger-id på displayet.
3. Tryk på knappen Registrer kort.
4. Rør ved NFC-symbolet med et nyt IC-kort.

   Det nye IC-korts nummer registreres derefter i maskinen.
5. Tryk på knappen OK.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Registrer en ekstern IC-kortlæser

Når du tilslutter en ekstern IC-kortlæser (integreret kredsløb), skal du bruge webbaseret administration til at registrere kortlæseren. Din maskine understøtter eksterne IC-kortlæsere, der bruger en HID-klassedriver.

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 **Administrator** > **External Card Reader (Ekstern kortlæser)** i venstre navigationsbjælke.

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

5. Indtast de nødvendige oplysninger, og klik derefter på **Submit (Send)**.
6. Genstart Brother-maskinen for at aktivere konfigurationen.
7. Tilslut kortlæseren til maskinen.
8. Rør ved kortlæseren, hvis du bruger kortgodkendelse.

Relaterede informationer

- Brug af Secure Function Lock (sikker funktionslås) 3.0

Sikker afsendelse eller modtagelse af en e-mail

- Konfiguration af e-mailafsendelse eller -modtagelse ved hjælp af webbaseret administration
- Afsendelse af en e-mail med brugergodkendelse
- Send eller modtag en e-mail sikkert ved hjælp af SSL/TLS

Konfiguration af e-mailafsendelse eller -modtagelse ved hjælp af webbaseret administration

- Modtagelse af e-mail er kun tilgængelig for visse modeller.
- Vi anbefaler, at du bruger webbaseret administration til at konfigurere sikker afsendelse af e-mails med brugergodkendelse eller afsendelse og modtagelse af e-mails ved hjælp af SSL/TLS (kun understøttede modeller).

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 feltet **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**, klik på **Advanced Settings (Avancerede indstillinger)** og kontroller, at status for **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)** er **Enabled (Aktiveret)**.

   - Tilgængelige protokoller kan variere afhængigt af din maskine.
   - Hvis **Authentication Method (Godkendelsesmetode)** muligheden vises, så vælg din godkendelsesmetode, og følg derefter vejledningen på skærmen.
6. Konfigurer **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**-indstillingerne.
   - Kontroller, at e-mailindstillingerne er korrekte efter konfigurationen ved at sende en test-e-mail.
   - Hvis du ikke kender indstillingerne for POP3/IMAP4/SMTP-serveren, skal du kontakte din netværksadministrator eller internet-serviceudbyder (ISP).
7. Klik på **Submit (Send)**, når du er færdig.

   Dialogboksen **Test Send/Receive E-mail Configuration (Test konfigurationen for send/modtag e-mail)** vises.
8. Følg vejledningen i dialogboksen for at teste de aktuelle indstillinger.

Relaterede informationer

- Sikker afsendelse eller modtagelse af en e-mail

Relaterede emner:

- Send eller modtag en e-mail sikkert ved hjælp af SSL/TLS

Afsendelse af en e-mail med brugergodkendelse

Din maskine sender e-mails via en e-mail-server, der kræver brugergodkendelse. Denne metode forhindrer unauthorized brugere i at få adgang til e-mailserveren.

Du kan sende e-mail-meddelelser, e-mail-rapporter og I-fax (kun tilgængelig for visse modeller) ved hjælp af brugergodkendelse.

- Tilgængelige protokoller kan variere afhængigt af din maskine.
- Vi anbefaler, at du bruger webbaseret administration til at konfigurere SMTP-godkendelsen.

Indstillinger for e-mailserver

Du skal konfigurere din maskines SMTP-godkendelsesmetode for at matche den metode, der bruges af e-mailserveren. Kontakt din netværksadministrator eller internetudbyder for at få flere oplysninger om dine indstillinger for e-mailserveren.

For at aktivere SMTP-servergodkendelse ved hjælp af webbaseret administration skal du vælge din godkendelsesmetode under **Server Authentication Method (Servergodkendelsesmetode)** på **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)** skærmbilledet.

Relaterede informationer

- Sikker afsendelse eller modtagelse af en e-mail

Send eller modtag en e-mail sikkert ved hjælp af SSL/TLS

Maskinen understøtter kommunikationsmetoderne SSL/TLS. Hvis du vil bruge en e-mailserver, der anvender SSL/TLS-kommunikation, skal du konfigurere følgende indstillinger.

- Modtagelse af e-mail er kun tilgængelig for visse modeller.
- Vi anbefaler, at du bruger Web Based Management til konfiguration af SSL/TLS.

Verifikation af servercertifikat

Hvis du vælger **SSL/TLS** eller **SSL** under **TLS**, markeres afkrydsningsfeltet **Verify Server Certificate (Verificer servercertifikat)** automatisk.

- Før du verificerer servercertifikatet, skal du importere det nøglecentercertifikat, der er udstedt af det nøglecenter, der signerede servercertifikatet. Kontakt din netværksadministrator eller internetserviceudbyder for at få oplyst, om det er nødvendigt at importere et nøglecentercertifikat.
- Fjern markeringen i afkrydsningsfeltet **Verify Server Certificate (Verificer servercertifikat)**, hvis det ikke er nødvendigt at verificere servercertifikatet.

Portnummer

Hvis du vælger **SSL** eller **TLS**, ændres værdien **Port**, så den stemmer overens med protokollen. Hvis du vil ændre portnummeret manuelt, skal du skrive portnummeret, efter at du har valgt indstillinger for **SSL/TLS**.

Du skal konfigurere maskinens kommunikationsmetode, så den stemmer overens med den metode, der bruges af din e-mailserver. Kontakt din netværksadministrator eller internetudbyder for at få flere oplysninger om dine indstillinger for e-mailserveren.

I de fleste tilfælde kræver de sikre webmail-tjenester følgende indstillinger:

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

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

Relaterede informationer

- Sikker afsendelse eller modtagelse af en e-mail

Relaterede emner:

- Konfiguration af e-mailafsendelse eller -modtagelse ved hjælp af webbaseret administration
- Konfigurer certifikater for enhedssikkerhed

Gem udskriftslog på netværk

Oversigt over Gem udskriftslog på netværk

Funktionen Gem udskriftslog på netværk gør det muligt at gemme en udskriftslogfil fra maskinen på en netværksserver med protokollen Common Internet File System (CIFS). Du kan registrere id'et, typen af udskriftsjob, jobnavn, brugernavn, dato, klokkeslæt og antal udskrevne sider for hvert udskriftsjob. CIFS er en protokol, der kører over TCP/IP og gør det muligt for computere på et netværk at dele filer over et intranet eller internettet.

Følgende udskriftsfunktioner registreres i udskriftsloggen:

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

- Udskriftsjob fra din computer
- USB Direct Print
- Kopi
- Modtaget fax
- Web Connect Print

- Funktionen Gem udskriftslog på netværk understøtter Kerberos-godkendelse og NTLMv2-godkendelse. Du skal konfigurere SNTP-protokollen (netværkstidsserver), eller du skal indstille dato, klokkeslæt og tidszone korrekt på kontrolpanelet for godkendelse.
- Du kan indstille filtypen til TXT eller CSV, når der gemmes en fil på serveren.

Relaterede informationer

- Gem udskriftslog på netværk

Konfiguration af indstillingerne Gem udskriftslog på netværk med Web Based Management

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 **Administrator** > **Store Print Log to Network (Gem udskriftslog til netværk)** i venstre navigationsbjælke.

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

5. I feltet **Print Log (Udskriv log)** skal du klikke på **On (Til)**.
6. Konfigurer følgende indstillinger:

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

Indstilling	Beskrivelse
Network Folder Path (Sti til netværksmappe)	Indtast den destinationsmappe, hvor din udskriftslog bliver gemt på CIFS-serveren (f.eks.: \\ComputerName\SharedFolder).
File Name (Filnavn)	Indtast det ønskede filnavn for udskriftslogfilen (op til 32 tegn).
File Type (Filtype)	Vælg **TXT (Tekst)** eller **CSV** som filtype for udskriftsloggen.
Time Source for Log (Tidskilde for log)	Vælg tidskilden for udskriftsloggen.
Auth. Method (Godkendelsesmetode)	Vælg den godkendelsesmetode, der skal bruges til at få adgang til CIFS-serveren: **Auto**, **Kerberos** eller **NTLMv2**. Kerberos er en godkendelsesprotokol, der gør det sikkert for enheder eller personer at bevise deres identitet over for netværksserverne med et enkelt logon. NTLMv2 er den godkendelsesmetode, der bruges af Windows til at logge ind på servere. • **Auto**: Hvis du vælger **Auto**, anvendes NTLMv2 som godkendelsesmetode. • **Kerberos**: Vælg indstillingen **Kerberos** for kun at bruge Kerberos-godkendelse. • **NTLMv2**: Vælg indstillingen **NTLMv2** for kun at bruge NTLMv2-godkendelse. • For både **Kerberos**- og **NTLMv2**-godkendelse skal du også konfigurere **Date&Time (Dato&klokkeslæt)**-indstillingerne eller SNTP-protokollen (netværkstidsserver) og DNS-server. • Du kan også konfigurere indstillingerne for dato og klokkeslæt fra maskinens kontrolpanel.

Indstilling	Beskrivelse
Username (Brugernavn)	Indtast et brugernavn for godkendelsen (op til 96 tegn). Hvis brugernavnet er en del af et domæne, skal du indtaste brugernavnet på en af følgende måder: bruger@domæne eller domæne \bruger.
Password (Adgangskode)	Indtast adgangskoden for godkendelsen (op til 32 tegn).
Kerberos Server Address (Kerberos-serveradresse) (om nødvendigt)	Indtast KDC-værtsadressen (Key Distribution Center) (f.eks. minpc.eksempel.com; op til 64 tegn) eller IP-adressen (for eksempel: 192.168.56.189).
Error Detection Setting (Fejlregistreringsindstilling)	Vælg, hvilken handling der skal udføres, når en udskriftslog ikke kan lagres på serveren på grund af en netværksfejl.

7. I feltet **Connection Status (Forbindelsesstatus)** skal du bekræfte den sidste logstatus.

Du kan også bekræfte fejlstatus på maskinens display.

8. Klik på **Submit (Send)** for at få vist siden **Test Print Log to Network (Testudskriftlog til netværk)**.

   For at teste dine indstillinger, skal du klikke på **Yes (Ja)** og derefter gå videre til næste trin.

   Klik på **No (Nej)** for at springe testen over. Indstillingerne sendes automatisk.
9. Maskinen tester indstillingerne.
10. Hvis indstillingerne accepteres, vises **Test OK** på skærmen.

    Hvis **Test Error (Testfejl)** vises, skal du markere alle indstillinger og klikke på **Submit (Send)** for at få vist testsiden igen.

Relaterede informationer

- Gem udskriftslog på netværk

Brug fejlregistreringsindstillingen i Gem udskriftslog til netværk

Brug fejlregisteringsindstillingerne til at afgøre, hvilken handling der skal udføres, når en udskriftslog ikke kan gemmes på serveren på grund af en netværksfejl.

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 **Administrator** > **Store Print Log to Network (Gem udskriftslog til netværk)** i venstre navigationsbjælke.

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

5. I afsnittet **Error Detection Setting (Fejlregistreringsindstilling)** skal du vælge muligheden **Cancel Print (Annuller udskrivning)** eller **Ignore Log & Print (Ignorer log og udskriv)**.

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

Indstilling	Beskrivelse
Cancel Print (Annuller udskrivning)	Hvis du vælger indstillingen **Cancel Print (Annuller udskrivning)**, canceled udskriftsjobbene, når udskriftsloggen ikke kan gemmes på serveren. Selvom du vælger indstillingen **Cancel Print (Annuller udskrivning)**, udskriver maskinen den indgående fax.

Ignore Log & Print (Ignorer log og udskriv)	Hvis du vælger indstillingen **Ignore Log & Print (Ignorer log og udskriv)**, udskriver maskinen dokumentationen, selvom udskriftsloggen ikke kan gemmes på serveren.
	Når funktionen til lagring af udskriftslog er gendannet, registreres udskriftsloggen som følger:
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	a. Hvis udskriftsloggen ikke kan gemmes ved slutningen af udskrivningen, vil antallet af udskrevne sider ikke blive registreret.
	b. Hvis udskriftsloggen ikke kan gemmes ved slutning af udskrivningen, registreres udskriftsloggen uden antallet af udskrevne sider. Når funktionen er gendannet, vises fejlen i udskriftsloggen.

6. Klik på **Submit (Send)** for at få vist siden **Test Print Log to Network (Testudskriftlog til netværk)**.

   For at teste dine indstillinger, skal du klikke på **Yes (Ja)** og derefter gå videre til næste trin.

Klik på **No (Nej)** for at springe testen over. Indstillingerne sendes automatisk.

7. Maskinen tester indstillingerne.
8. Hvis indstillingerne accepteres, vises **Test OK** på skærmen.

   Hvis **Test Error (Testfejl)** vises, skal du markere alle indstillinger og klikke på **Submit (Send)** for at få vist testsiden igen.

Relaterede informationer

- Gem udskriftslog på netværk

Brug af Gem udskriftslog på netværk med Secure Function Lock 3.0

Når Secure Function Lock (secure Function Lock (sikker funktionslås) 3.0 er aktiv, registreres navnene på de registrerede brugere for kopi, fax RX, Web Connect Print og USB Direct Print i rapporten Gem udskriftslog på netværk. Når Active Directory-godkendelsen er aktiveret, registreres brugernavnet i rapporten Gem udskriftslog på netværk:

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

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Relaterede informationer

- Gem udskriftslog på netværk

www.brotherearth.com

DAN
Version 0