Guide för säkerhetsfunktioner

Innehållsförteckning

Inledning 1
Definitioner av anteckningar 2
Varumärken 3
Upphovsrätt 4
Innan du använder nätverkssäkerhetsfunktioner 5
Inaktivera onödiga protokoll 6
Nätverkssäkerhet 7
Konfigurera certifikat för enhetssäkerhet 8
Översikt över funktioner för säkerhetscertifikat 9
Hur man skapar och installerar ett certifikat 10
Skapa ett självsignerat certifikat 11
Skapa en CSR (Certificate Signing Request) och installera ett certifikat från en CA (Certificate Authority, certifikatmyndighet) 12
Importera och exportera certifikat och privat nyckel 16
Importera och exportera ett CA-certifikat 19
Använda SSL/TLS 22
Hantera nätverksmaskinen säkert med SSL/TLS 23
Säker utskrift av dokument med SSL/TLS 27
Använda SNMPv3 29
Hantera nätverksmaskinen säkert med SNMPv3 30
Använd IPsec 32
Introduktion till IPsec 33
Konfigurera IPsec med hjälp av webbaserad hantering 34
Konfigurera en IPsec-adressmall med hjälp av webbaserad hantering 36
Konfigurera en IPsec-mall med hjälp av webbaserad hantering 38
Använd IEEE 802.1x-autentisering för nätverket 47
Vad är IEEE 802.1x-autentisering? 48
Konfigurera IEEE 802.1x-autentisering för ditt nätverk med hjälp av webbaserad hantering (webbläsare) 49
IEEE 802.1x-autentiseringsmetoder 51
Användarautentisering 52
Använda autentisering av Active Directory 53
Introduktion till autentisering av Active Directory 54
Konfigurera autentisering av Active Directory med hjälp av webbaserad hantering 55
Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (autentisering av Active Directory) 57
Använd LDAP-autentisering 58
Introduktion till LDAP-autentisering 59
Konfigurera LDAP-autentisering med hjälp av webbaserad hantering 60
Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (LDAP-autentisering) 62
Använd Secure Function Lock 3.0 (säkert funktionslås) 63
Innan du använder Secure Function Lock 3.0 64
Konfigurera Secure Function Lock 3.0 med hjälp av webbaserad hantering 65
Skanna med hjälp av Secure Function Lock 3.0 66
Konfigurera offentligt läge för Secure Function Lock 3.0 67
Konfigurera personliga startskärmsinställningar med hjälp av webbaserad hantering. 68

Ytterligare funktioner i Secure Function Lock 3.0 ... 69
Registrera ett nytt IC-kort via maskinens kontrollpanel ... 70
Registrera en extern IC-kortläsare ... 71
Sända eller ta emot e-post säkert ... 72
Konfigurera e-postsändning eller -mottagning med hjälp av Webbaserad hantering ... 73
Skicka ett e-postmeddelande med användarautentisering ... 74
Skicka eller ta emot e-post säkert med SSL/TLS ... 75
Spara utskriftsloggen på nätverket ... 76
Spara utskriftslogg till nätverk – översikt ... 77
Konfigurera inställningarna för Spara utskriftslogg på nätverket med hjälp av webbaserad hantering ... 78
Använd inställningen för felidentifiering under Spara utskriftsloggen på nätverket ... 80
Använda Spara utskriftslogg på nätverket med Secure Function Lock 3.0 ... 82

Inledning

- Definitioner av anteckningar
- Varumärken
- Upphovsrätt
- Innan du använder nätverkssäkerhetsfunktioner

Definitioner av anteckningar

Följande symboler och anvisningar används i den här bruksanvisningen:

VIKTIGT	VIKTIGT anger en potentiellt farlig situation som om den inte undviks kan medföra skada på materiell egendom eller förlust av produktfunktioner.
OBS	OBS anger driftmiljön, villkor för installation, eller särskilda villkor för användningen.
	Tipsikoner ger dig hjälpfulla tips och ytterligare information.
Fetstil	Fetstil motsvarar knappar på maskinens kontrollpanel eller på datorskärmen.
Kursiv	Text med Italicized stil gör dig emphasizes på en viktig punkt eller hänvisar dig till ett närliggande avsnitt.

Närliggande information

- Inledning

Varumärken

Adobe® och Reader® är antingen registrerade varumärken eller varumärken som tillhör Adobe Systems Incorporated i USA och/eller andra länder.

Alla företag vars programvara nämns i denna handbok har ett License enligt egendomsprogrammet.

Alla företags handelsnamn och produktnamn som förekommer på Brother-produkter, i relaterade dokument och i annat material är varumärken eller registrerade varumärken som tillhör respektive företag.

Närliggande information

- Inledning

Upphovsrätt

Närliggande information

- Inledning

Innan du använder nätverkssäkerhetsfunktioner

Maskinen använder några av de allra senaste protokollen för nätverkssäkerhet och kryptering. De här nätverksfunktionerna kan integreras i den övergripande planen för nätverkssäkerhet, och på så vis bidra till att skydda dina data och hindra unauthorized åtkomst till maskinen.

Vi rekommenderar att du inaktiverar FTP- och TFTP-protokollen. Åtkomst till maskinen med de här protokollen är inte säker.

Närliggande information

- Inledning
  - Inaktivera onödiga protokoll

Inaktivera onödiga protokoll

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

   Exempel:

   https://192.168.1.2

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

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

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

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

5. Avmarkera alla kryssrutor för onödiga protokoll för att inaktivera dem.
6. Klicka på **Submit (Skicka)**.
7. Starta om Brother-maskinen för att aktivera konfigurationen.

Närliggande information

- Innan du använder nätverkssäkerhetsfunktioner

Nätverkssäkerhet

- Konfigurera certifikat för enhetssäkerhet
- Använda SSL/TLS
- Använda SNMPv3
- Använd IPsec
- Använd IEEE 802.1x-autentisering för nätverket

Konfigurera certifikat för enhetssäkerhet

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

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

Översikt över funktioner för säkerhetscertifikat

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

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

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

Skrivaren har stöd för följande:

- Förinstallerat certifikat

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

  Det förinstallerade självsignerade certifikatet skyddar din kommunikation till en viss nivå. Vi rekommenderar att du använder ett certifikat som utfärdats av en pålitlig organization för bättre skydd.

- Självsignerat certifikat

  Den här skrivarservern kan utfärda ett eget certifikat. Med hjälp av det certifikatet kan du enkelt använda SSL/TLS-kommunikation utan att du behöver skapa eller installera ett annat certifikat från en CA.

- Certifikat från en Certificate Authority (CA)

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

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

- Certificate Authority (CA) certifikat

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

- Om du tänker använda SSL/TLS-kommunikation rekommenderar vi att du först kontaktar din systemadministratör.
- När du återställer skrivarserverns fabriksinställningar raderas det certifikat och den privata nyckel som finns installerade. Om du vill behålla certifikatet och den privata nyckeln efter att du återställt skrivarservern måste du exportera dem innan återställning och sedan installera dem igen.

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

Liknande ämnen:

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

Hur man skapar och installerar ett certifikat

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

Alternativ 1

Självsignerat certifikat

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

Alternativ 2

Certifikat från en CA

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

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

Skapa ett självsignerat certifikat

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

   Exempel:

   https://192.168.1.2

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

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

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

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

5. Klicka på **Create Self-Signed Certificate (Skapa självsignerat certifikat)**.
6. Ange **Common Name (Gemensamt namn)** och **Valid Date (Giltigt datum)**.
   - Längden på **Common Name (Gemensamt namn)** är mindre än 64 bytes. Ange ett ID som t.ex. en IP-adress, ett nodnamn eller domännamn som ska användas för åtkomst till maskinen med SSL/TSL-kommunikation. Nodnamnet visas som standard.
   - En varning visas om du använder IPPS- eller HTTPS-protokollet och anger ett annat namn i adressfältet än det **Common Name (Gemensamt namn)** som användes för det självsignerade certifikatet.
7. Välj inställningen i rullgardinsmenyn **Public Key Algorithm (Offentlig nyckelalgoritm)**.
8. Välj inställningen i rullgardinsmenyn **Digest Algorithm (Digest Algoritm)**.
9. Klicka på **Submit (Skicka)**.

Närliggande information

- Konfigurera certifikat för enhetssäkerhet

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

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

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

Skapa en CSR (Certificate Signing Request)

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

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

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

   Exempel:

   https://192.168.1.2

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

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

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

   - Din företagsinformation krävs för att en CA ska kunna bekräfta din identitet och attestera den för en utomstående.
   - Längden på **Common Name (Gemensamt namn)** måste vara mindre än 64 bytes. Ange ett ID som t.ex. en IP-adress, ett nodnamn eller domännamn som ska användas för åtkomst till maskinen med SSL/TSL-kommunikation. Nodnamnet visas som standard. **Common Name (Gemensamt namn)** krävs.
   - Ett varningsmeddelande visas om du anger ett annat namn i webbadressfältet än det Common Name som användes för certifikatet.
   - Längden på **Organization (Organisation)**, **Organization Unit (Organisationsenhet)**, **City/Locality (Ort/Lokalitet)** och **State/Province (Stat/Provins)** måste vara mindre än 64 byte.
   - **Country/Region (Land/Region)** ska vara en två tecken lång landskod enligt ISO 3166.
   - Om du konfigurerar certifikatförlängningen X.509v3 markerar du kryssrutan **Configure extended partition (Konfigurera utökad partition)** och väljer sedan **Auto (Register IPv4) (Auto (Registrera IPv4))** eller **Manual (Manuell)**.
7. Välj inställningen i rullgardinsmenyn **Public Key Algorithm (Offentlig nyckelalgoritm)**.
8. Välj inställningen i rullgardinsmenyn **Digest Algorithm (Digest Algoritm)**.
9. Klicka på **Submit (Skicka)**.

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

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

Närliggande information

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

Installera ett certifikat på maskinen

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

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

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

   Exempel:

   https://192.168.1.2

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

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

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

   Nu skapas och sparas certifikatet i maskinens minne.

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

Närliggande information

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

Importera och exportera certifikat och privat nyckel

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

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

Importera ett certifikat och den privata nyckeln

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

   Exempel:

   https://192.168.1.2

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

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

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

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

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

Certifikatet och den privata nyckeln importeras till maskinen.

Närliggande information

- Importera och exportera certifikat och privat nyckel

Exportera certifikatet och privata nyckeln

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

   Exempel:

   https://192.168.1.2

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

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

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

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

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

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

Certifikatet och den privata nyckeln har nu exporterats till datorn.

Du kan även importera certifikatet till din dator.

Närliggande information

- Importera och exportera certifikat och privat nyckel

Importera och exportera ett CA-certifikat

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

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

Importera ett CA-certifikat

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

   Exempel:

   https://192.168.1.2

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

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

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

Närliggande information

- Importera och exportera ett CA-certifikat

Exportera ett CA-certifikat

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

   Exempel:

   https://192.168.1.2

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

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

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

Närliggande information

- Importera och exportera ett CA-certifikat

Använda SSL/TLS

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

Hantera nätverksmaskinen säkert med SSL/TLS

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

Konfigurera ett certifikat för SSL/TLS och tillgängliga protokoll

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

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

   Exempel:

   https://192.168.1.2

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

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

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

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

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

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Liknande ämnen:

- Säker utskrift av dokument med SSL/TLS

Få åtkomst till Webbaserad hantering med hjälp av SSL/TLS

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

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

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

   Exempel:

   https://192.168.1.2

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

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

4. Du kan nu komma åt maskinen över HTTPS.

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Installera det självsignerade certifikatet för Windows-användare som administratör

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

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

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

   Exempel:

   https://192.168.1.2

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

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

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

Närliggande information

- Hantera nätverksmaskinen säkert med SSL/TLS

Säker utskrift av dokument med SSL/TLS

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

Skriv ut dokument med hjälp av IPPS

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

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

   Exempel:

   https://192.168.1.2

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

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

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

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

   Starta om maskinen för att aktivera konfigurationen.

   När maskinen har startats går du tillbaka till maskinens webbsida, anger lösenordet och går sedan till det vänstra navigeringsfältet och klickar på **Network (Nätverk)** > **Network (Nätverk)** > **Protocol (Protokoll)**.
6. Klicka på **HTTP Server Settings (HTTP-serverinställningar)**.
7. Markera kryssrutan **HTTPS(Port 443)** under **IPP** och klicka sedan på **Submit (Skicka)**.
8. Starta om maskinen för att aktivera konfigurationen.

Kommunikation med IPPS kan inte förhindra unauthorized åtkomst till skrivarservern.

Närliggande information

- Säker utskrift av dokument med SSL/TLS

Använda SNMPv3

- Hantera nätverksmaskinen säkert med SNMPv3

Hantera nätverksmaskinen säkert med SNMPv3

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

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

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

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

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

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

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

7. Konfigurera inställningarna för SNMPv3-läget.

Alternativ	Beskrivning
Enabled (Aktiverad)	Skrivarservern använder version 3 av SNMP-protokollet. Använd SNMPv3-läget för att hantera skrivarservern säkert.
Disabled (Avaktiverad)	Inaktivera version 3 och av SNMP-protokollet. Alla program som använder SNMPv3 kommer att begränsas. För att tillåta användning av SNMPv3-program använder du SNMPv3-läget.

8. Klicka på **Submit (Skicka)**.

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

9. Starta om maskinen för att aktivera konfigurationen.

Närliggande information

- Använda SNMPv3

Använd IPsec

- Introduktion till IPsec
- Konfigurera IPsec med hjälp av webbaserad hantering
- Konfigurera en IPsec-adressmall med hjälp av webbaserad hantering
- Konfigurera en IPsec-mall med hjälp av webbaserad hantering

Introduktion till IPsec

IPsec (Internet Protocol Security) är ett säkerhetsprotokoll som använder en valfri internetprotokollsfunktion som förhindrar datamanipulation och ser till att data som skickas som IP-paket hålls hemliga. IPsec krypterar data som överförs på ett nätverk, t.ex. utskriftsdata som skickas från datorer till en skrivare. Eftersom data krypteras i nätverkslager, använder applikationer med en högre protokollnivå IPsec, även om användaren inte känner till det.

IPsec har stöd för följande funktioner:

- IPsec-överföring

  Enligt inställningsvillkoren för IPsec sänder en nätverksansluten dator data till och tar emot data från en specificerad enhet med IPsec. När enheter börjar kommunicera med IPsec utbyts nycklar med Internet Key Exchange (IKE) först och sedan överförs krypterade data med hjälp av nycklarna.

  Dessutom har IPsec två funktionslägen: transportläge och tunnelläge. Transportläget används huvudsakligen för kommunikation mellan enheter och tunnelläget används i miljöer som t.ex. ett VPN (Virtual Private Network).

  För IPsec-överföring krävs följande villkor:
  - En dator som kan kommunicera med IPsec är ansluten till nätverket.
  - Maskinen är konfigurerad för IPsec-kommunikation.
  - Datorn som är ansluten till din maskin är konfigurerad för IPsec-anslutningar.

- IPsec-inställningar

  Inställningarna som krävs för anslutning med IPsec. Dessa inställningar kan konfigureras med hjälp av webbaserad hantering.

  Du måste använda en webbläsare på en dator som är ansluten till nätverket för att kunna konfigurera IPsec-inställningarna.

Närliggande information

- Använd IPsec

Konfigurera IPsec med hjälp av webbaserad hantering

Det finns två typer av anslutningsvillkor för IPsec**Template (Mall)**: **Address (adress)** och **IPsec**. Du kan konfigurera upp till 10 anslutningsvillkor.

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

   Exempel:

   https://192.168.1.2

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

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

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

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

5. Konfigurera inställningarna.

Alternativ	Beskrivning
Status	Aktivera eller inaktivera IPsec.
Negotiation Mode (Förhandlingsläge)	Välj **Negotiation Mode (Förhandlingsläge)** för IKE fas 1. IKE är ett protokoll som används för att byta krypteringsnycklar för krypterad kommunikation med hjälp av IPsec. I läget **Main (Huvud)** är bearbetningstiden längre, men säkerheten är hög. I läget **Aggressive (Aggressiv)** är överföringshastigheten högre än i läget **Main (Huvud)** men säkerheten är lägre.
All Non-IPsec Traffic (All icke-IPsec trafik)	Välj den åtgärd som ska vidtas för icke IPsec-paket. När du använder webbtjänster måste du välja **Allow (Tillåt)** för **All Non-IPsec Traffic (All icke-IPsec trafik)**. Om du väljer **Drop (Släpp)** går det inte att använda webbtjänster.
Broadcast/Multicast Bypass (Gruppsändning/Multicast Bypass)	Välj **Enabled (Aktiverad)** eller **Disabled (Avaktiverad)**.
Protocol Bypass (Förbigå protokoll)	Välj kryssrutorna för de alternativ du önskar.
Rules (Regler)	Aktivera mallen genom att markera kryssrutan **Enabled (Aktiverad)**. Om du väljer flera kryssrutor har kryssrutorna med de lägre numren prioritet om inställningarna för valda kryssrutor hamnar i konflikt. Klicka på motsvarande rullgardinsmeny för att välja den **Address Template (Adressmall)** som används för IPsec-anslutningsvillkoren. Lägg till en **Address Template (Adressmall)** genom att klicka på **Add Template (Lägg till mall)**. Klicka på motsvarande rullgardinsmeny för att välja den **IPsec Template (IPsec-mall)** som används för IPsec-anslutningsvillkoren. Lägg till en **IPsec Template (IPsec-mall)** genom att klicka på **Add Template (Lägg till mall)**.

6. Klicka på **Submit (Skicka)**.

   Om maskinen måste startas om för att aktivera nya inställningar visas bekräftelseskärmen för omstart.

   Om det finns en tom post i den mall du aktiverade i **Rules (Regler)**-tabellen visas ett felmeddelande. Bekräfta dina val och klicka på **Submit (Skicka)** igen.

Närliggande information

- Använd IPsec

Liknande ämnen:

- Konfigurera certifikat för enhetssäkerhet

Konfigurera en IPsec-adressmall med hjälp av webbaserad hantering

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **IPsec Address Template (IPsec Adressmall)**.

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

5. Klicka på knappen **Delete (Ta bort)** för att radera en **Address Template (Adressmall)**. När en **Address Template (Adressmall)** används går det inte att radera den.
6. Klicka på den **Address Template (Adressmall)** som du vill skapa. Fönstret **IPsec Address Template (IPsec Adressmall)** öppnas.
7. Konfigurera inställningarna.

Alternativ	Beskrivning
Template Name (Mallnamn)	Ange namn för mallen (upp till 16 tecken).
Local IP Address (Lokal IP-adress)	• **IP Address (IP-adress)** Ange IP-adressen. Välj alternativet **ALL IPv4 Address (ALL IPv4 adress)**, **ALL IPv6 Address (ALL IPv6 adress)**, **ALL Link Local IPv6 (All Link Local IPv6)** eller **Custom (Egna inställningar)** i rullgardinsmenyn. Om du väljer **Custom (Egna inställningar)** i rullgardinsmenyn anger du IP-adressen (IPv4 eller IPv6) i textrutan. • **IP Address Range (IP Adressintervall)** Ange IP-adresser för IP-adressintervallet i textrutorna. Ett funktionsfel uppstår om den första och sista IP-adressen inte är standardized enligt IPv4 eller IPv6 eller om den sista IP-adressen är kortare än den första. • **IP Address / Prefix (IP Adressintervall/prefix)** Ange IP-adressen med hjälp av CIDR-notation. Exempelvis: 192.168.1.1/24 Eftersom prefixet anges i form av en 24-bitars nätmask (255.255.255.0) för 192.168.1.1, är adresserna 192.168.1.### giltiga.
Remote IP Address (Fjärr IP Adress)	• **Any (Valfri)** Om du väljer **Any (Valfri)** aktiveras alla IP-adresser. • **IP Address (IP-adress)** Skriv in angiven IP-adress (IPv4 eller IPv6) i textrutan. • **IP Address Range (IP Adressintervall)** Ange den första och sista IP-adressen för IP-adressintervallet. Ett funktionsfel uppstår om den första och sista IP-adressen inte är

Alternativ	Beskrivning
	standardized enligt IPv4 eller IPv6 eller om den sista IP-adressen är kortare än den första. • **IP Address / Prefix (IP Adressintervall/prefix)** Ange IP-adressen med hjälp av CIDR-notation. Exempelvis: 192.168.1.1/24 Eftersom prefixet anges i form av en 24-bitars nätmask (255.255.255.0) för 192.168.1.1, är adresserna 192.168.1.### giltiga.

8. Klicka på **Submit (Skicka)**.

Starta om skrivaren om du ändrar inställningarna för den aktuella mallen som används för att aktivera konfigurationen.

Närliggande information

- Använd IPsec

Konfigurera en IPsec-mall med hjälp av webbaserad hantering

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Network (Nätverk)** > **Security (Säkerhet)** > **IPsec Template (IPsec-mall)**.

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

5. Klicka på knappen **Delete (Ta bort)** för att radera en **IPsec Template (IPsec-mall)**. När en **IPsec Template (IPsec-mall)** används går det inte att radera den.
6. Klicka på den **IPsec Template (IPsec-mall)** du vill skapa. Skärmbilden **IPsec Template (IPsec-mall)** visas. Konfigurationsfälten skiljer sig åt beroende på vilka inställningar du väljer för **Use Prefixed Template (Använd prefixad mall)** och **Internet Key Exchange (IKE)**.
7. I fältet **Template Name (Mallnamn)** anger du ett namn för mallen (upp till 16 tecken).
8. Om du valde **Custom (Egna inställningar)** i rullgardinsmenyn **Use Prefixed Template (Använd prefixad mall)** väljer du alternativet **Internet Key Exchange (IKE)** och ändrar vid behov sedan inställningen.
9. Klicka på **Submit (Skicka)**.

Närliggande information

- Använd IPsec
  - IKEv1-inställningar för en IPsec-mall
  - IKEv2-inställningar för en IPsec-mall
  - Manuella inställningar för en IPsec-mall

IKEv1-inställningar för en IPsec-mall

Alternativ	Beskrivning
Template Name (Mallnamn)	Ange namn för mallen (upp till 16 tecken).
Use Prefixed Template (Använd prefixad mall)	Välj **Custom (Egna inställningar)**, **IKEv1 High Security (IKEv1 Hög säkerhet)** eller **IKEv1 Medium Security (IKEv1 Medelhög säkerhet)**. Inställningsalternativen skiljer sig åt beroende på vald mall.
Internet Key Exchange (IKE)	IKE är ett kommunikationsprotokoll som används för att byta krypteringsnycklar för krypterad kommunikation med hjälp av IPsec. För att använda krypterad kommunikation för endast en enstaka gång, avgörs krypteringsalgoritmen som behövs för IPsec och krypteringsnycklarna delas ut. För IKE byter man krypteringsnycklar med bytesmetoden Diffie-Hellman och krypterad kommunikation som begränsas till IKE används. Om du valde **Custom (Egna inställningar)** för **Use Prefixed Template (Använd prefixad mall)**, väljer du **IKEv1**.
Authentication Type (Autentiseringstyp)	• **Diffie-Hellman Group** Denna nyckelöverföringsmetod gör att hemliga nycklar kan överföras på ett säkert sätt via ett oskyddat nätverk. Nyckelöverföringsmetoden Diffie-Hellman använder en diskret logaritm, inte en hemlig nyckel, för att skicka och ta emot öppen information som genererades med ett slumpmässigt nummer och en hemlig nyckel. Välj **Group1 (Grupp1)**, **Group2 (Grupp2)**, **Group5 (Grupp5)** eller **Group14 (Grupp14)**. • **Encryption (Kryptering)** Välj **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Välj **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SA livslängd)** Ange livstid för IKE SA. Ange tiden (sekunder) och antalet kilobyte (KByte).
Encapsulating Security (Inbäddad säkerhet)	• **Protocol (Protokoll)** Välj **ESP**, **AH**, eller **AH+ESP**. - ESP är ett protokoll som används för krypterad kommunikation med IPsec. ESP krypterar innehållet (kommunicerat innehåll) och lägger till ytterligare information. IP-paketet består av rubriken och den krypterade nyttolasten, som följer rubriken. Utöver krypterade data ingår även information om krypteringsmetoden, krypteringsnyckeln, autentiseringsdata o.s.v. i IP-paketet. - AH är en del av IPsec-protokollet som autentiserar avsändaren och förhindrar att informationen manipuleras (försäkrar att informationen levereras i sin helhet). Iinformationen infogas omedelbart efter rubriken i IP-paketet. Paketen innehåller dessutom hashvärden, som beräknas med en ekvation från det innehåll som kommuniceras, den hemliga nyckeln och så vidare, för att förhindra att förfalskning av avsändaren och manipulering av informationen sker. Till skillnad från ESP krypteras inte kommunicerat innehåll och informationen skickas och tas emot som vanlig text. • **Encryption (Kryptering) (Inte tillgänglig för alternativet AH.)** Välj **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**.

Alternativ	Beskrivning
	• **Hash** Välj **None (Inget)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Inget)** kan endast väljas när **ESP** är valt för **Protocol (Protokoll)**. • **SA Lifetime (SA livslängd)** Ange livslängden för IKE SA. Ange tiden (sekunder) och antalet kilobyte (KB). • **Encapsulation Mode (Inkapslingssläge)** Välj **Transport (Transport)** eller **Tunnel (Tunnel)**. • **Remote Router IP-Address (Fjärrouter IP Adress)** Ange IP-adressen (IPv4 eller IPv6) för fjärroutern. Ange endast denna information när du valt läget **Tunnel (Tunnel)**. SA (Security Association) är en krypterad kommunikationsmetod som använder IPsec eller IPv6 som överför och delar information, som t.ex. krypteringsmetod och krypteringsnyckel, för att kunna upprätta en säker kommunikationskanal innan kommunikationen påbörjas. SA kan också hänvisa till en virtuell, krypterad kommunikationskanal som har upprättats. SA som används för IPsec upprättar krypteringsmetod, överför nycklar och utför gemensam autentisering i enlighet med standardförfarandet IKE (Internet Key Exchange). SA uppdateras dessutom regelbundet.
Perfect Forward Secrecy (PFS) (Perfekt framåtriktad sekretess)	PFS erhåller inte nycklar från tidigare nycklar som användes för att kryptera meddelanden. Dessutom gäller att om en nyckel som användes för att kryptera ett meddelande härleddes från en överordnad nyckel, används inte den överordnade nyckeln till att härleda andra nycklar. Därför begränsas endast skadorna till de meddelanden som krypterades med nyckeln även om en nyckel kompromitterats. Välj **Enabled (Aktiverad)** eller **Disabled (Avaktiverad)**.
Authentication Method (Autentiseringsmetod)	Välj autentiseringsmetod. Välj **Pre-Shared Key (Delad nyckel på förhand)** eller **Certificates (Certifikat)**.
Pre-Shared Key (Delad nyckel på förhand)	När kommunikation krypteras utbyts och delas krypteringsnyckeln i förväg med en annan kanal. Om du valde **Pre-Shared Key (Delad nyckel på förhand)** för **Authentication Method (Autentiseringsmetod)**, anger du **Pre-Shared Key (Delad nyckel på förhand)** (högst 32 tecken). • **Local/ID Type/ID (Lokal/ID-typ/ID)** Välj avsändarens ID-typ och ange sedan ID. Välj **IPv4 Address (IPv4 adress)**, **IPv6 Address (IPv6 adress)**, **FQDN**, **E-mail Address (E-postadress)** eller **Certificate (Certifikat)** för typ. Om du väljer **Certificate (Certifikat)** ange du certifikatets vanliga namn i fältet **ID**. • **Remote/ID Type/ID (Extern/ID-typ/ID)** Välj mottagarens ID-typ och ange sedan ID. Välj **IPv4 Address (IPv4 adress)**, **IPv6 Address (IPv6 adress)**, **FQDN**, **E-mail Address (E-postadress)** eller **Certificate (Certifikat)** för typ. Om du väljer **Certificate (Certifikat)** ange du certifikatets vanliga namn i fältet **ID**.
Certificate (Certifikat)	Om du valde **Certificates (Certifikat)** för **Authentication Method (Autentiseringsmetod)**, väljer du certifikatet.

Alternativ	Beskrivning
	Du kan endast välja certifikatet som skapades på sidan **Certificate (Certifikat)** på skärmen för säkerhetskonfiguration i Webbaserad hantering.

Närliggande information

- Konfigurera en IPsec-mall med hjälp av webbaserad hantering

IKEv2-inställningar för en IPsec-mall

Alternativ	Beskrivning
Template Name (Mallnamn)	Ange namn för mallen (upp till 16 tecken).
Use Prefixed Template (Använd prefixad mall)	Välj **Custom (Egna inställningar)**, **IKEv2 High Security (IKEv2 Hög säkerhet)** eller **IKEv2 Medium Security (IKEv2 Medelhög säkerhet)**. Inställningsalternativen skiljer sig åt beroende på vald mall.
Internet Key Exchange (IKE)	IKE är ett kommunikationsprotokoll som används för att byta krypteringsnycklar för krypterad kommunikation med hjälp av IPsec. För att använda krypterad kommunikation för endast en enstaka gång, avgörs krypteringsalgoritmen som behövs för IPsec och krypteringsnycklarna delas ut. För IKE byter man krypteringsnycklar med bytesmetoden Diffie-Hellman och krypterad kommunikation som begränsas till IKE används. Om du valde **Custom (Egna inställningar)** för **Use Prefixed Template (Använd prefixad mall)**, väljer du **IKEv2**.
Authentication Type (Autentiseringstyp)	• **Diffie-Hellman Group** Denna nyckelöverföringsmetod gör att hemliga nycklar kan överföras på ett säkert sätt via ett oskyddat nätverk. Nyckelöverföringsmetoden Diffie-Hellman använder en diskret logaritm, inte en hemlig nyckel, för att skicka och ta emot öppen information som genererades med ett slumpmässigt nummer och en hemlig nyckel. Välj **Group1 (Grupp1)**, **Group2 (Grupp2)**, **Group5 (Grupp5)** eller **Group14 (Grupp14)**. • **Encryption (Kryptering)** Välj **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Välj **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. • **SA Lifetime (SA livslängd)** Ange livstid för IKE SA. Ange tiden (sekunder) och antalet kilobyte (KByte).
Encapsulating Security (Inbäddad säkerhet)	• **Protocol (Protokoll)** Välj **ESP**. ESP är ett protokoll som används för krypterad kommunikation med IPsec. ESP krypterar innehållet (kommunicerat innehåll) och lägger till ytterligare information. IP-paketet består av rubriken och den krypterade nyttolasten, som följer rubriken. Utöver krypterade data ingår även information om krypteringsmetoden, krypteringsnyckeln, autentiseringsdata o.s.v. i IP-paketet. • **Encryption (Kryptering)** Välj **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Välj **MD5**, **SHA1**, **SHA256**, **SHA384**, eller **SHA512**. • **SA Lifetime (SA livslängd)** Ange livslängden för IKE SA. Ange tiden (sekunder) och antalet kilobyte (KB). • **Encapsulation Mode (Inkapslingssläge)** Välj **Transport (Transport)** eller **Tunnel (Tunnel)**.

Alternativ	Beskrivning
	• **Remote Router IP-Address (Fjärrouter IP Adress)** Ange IP-adressen (IPv4 eller IPv6) för fjärroutern. Ange endast denna information när du valt läget **Tunnel (Tunnel)**. SA (Security Association) är en krypterad kommunikationsmetod som använder IPsec eller IPv6 som överför och delar information, som t.ex. krypteringsmetod och krypteringsnyckel, för att kunna upprätta en säker kommunikationskanal innan kommunikationen påbörjas. SA kan också hänvisa till en virtuell, krypterad kommunikationskanal som har upprättats. SA som används för IPsec upprättar krypteringsmetod, överför nycklar och utför gemensam autentisering i enlighet med standardförfarandet IKE (Internet Key Exchange). SA uppdateras dessutom regelbundet.
Perfect Forward Secrecy (PFS) (Perfekt framåtriktad sekretess)	PFS erhåller inte nycklar från tidigare nycklar som användes för att kryptera meddelanden. Dessutom gäller att om en nyckel som användes för att kryptera ett meddelande härleddes från en överordnad nyckel, används inte den överordnade nyckeln till att härleda andra nycklar. Därför begränsas endast skadorna till de meddelanden som krypterades med nyckeln även om en nyckel kompromitterats. Välj **Enabled (Aktiverad)** eller **Disabled (Avaktiverad)**.
Authentication Method (Autentiseringsmetod)	Välj autentiseringsmetod. Välj **Pre-Shared Key (Delad nyckel på förhand)**, **Certificates (Certifikat)**, **EAP - MD5** eller **EAP - MS-CHAPv2**. EAP är ett autentiseringsprotokoll som är ett tillägg till PPP. Genom att använda EAP tillsammans med IEEE802.1x, används en annan nyckel för användarautentisering och vid varje session. Följande inställningar är endast nödvändiga när du väljer **EAP - MD5** eller **EAP - MS-CHAPv2** för **Authentication Method (Autentiseringsmetod)**: • **Mode (läge)** Välj **Server-Mode (Serverläge)** eller **Client-Mode (Klientläge)**. • **Certificate (Certifikat)** Välj certifikat. • **User Name (Användarnamn)** Ange användarnamn (upp till 32 tecken). • **Password (Lösenord)** Ange lösenordet (upp till 32 tecken). Lösenordet måste anges två gånger för att bekräfta.
Pre-Shared Key (Delad nyckel på förhand)	När kommunikation krypteras utbyts och delas krypteringsnyckeln i förväg med en annan kanal. Om du valde **Pre-Shared Key (Delad nyckel på förhand)** för **Authentication Method (Autentiseringsmetod)**, anger du **Pre-Shared Key (Delad nyckel på förhand)** (högst 32 tecken). • **Local/ID Type/ID (Lokal/ID-typ/ID)** Välj avsändarens ID-typ och ange sedan ID. Välj **IPv4 Address (IPv4 adress)**, **IPv6 Address (IPv6 adress)**, **FQDN**, **E-mail Address (E-postadress)** eller **Certificate (Certifikat)** för typ. Om du väljer **Certificate (Certifikat)** ange du certifikatets vanliga namn i fältet **ID**. • **Remote/ID Type/ID (Extern/ID-typ/ID)** Välj mottagarens ID-typ och ange sedan ID.

Alternativ	Beskrivning
	Välj **IPv4 Address (IPv4 adress)**, **IPv6 Address (IPv6 adress)**, **FQDN**, **E-mail Address (E-postadress)** eller **Certificate (Certifikat)** för typ. Om du väljer **Certificate (Certifikat)** ange du certifikatets vanliga namn i fältet **ID**.
Certificate (Certifikat)	Om du valde **Certificates (Certifikat)** för **Authentication Method (Autentiseringsmetod)**, väljer du certifikatet. Du kan endast välja certifikatet som skapades på sidan **Certificate (Certifikat)** på skärmen för säkerhetskonfiguration i Webbaserad hantering.

Närliggande information

- Konfigurera en IPsec-mall med hjälp av webbaserad hantering

Manuella inställningar för en IPsec-mall

Alternativ	Beskrivning
Template Name (Mallnamn)	Ange namn för mallen (upp till 16 tecken).
Use Prefixed Template (Använd prefixad mall)	Välj **Custom (Egna inställningar)**.
Internet Key Exchange (IKE)	IKE är ett kommunikationsprotokoll som används för att byta krypteringsnycklar för krypterad kommunikation med hjälp av IPsec. För att använda krypterad kommunikation för endast en enstaka gång, avgörs krypteringsalgoritmen som behövs för IPsec och krypteringsnycklarna delas ut. För IKE byter man krypteringsnycklar med bytesmetoden Diffie-Hellman och krypterad kommunikation som begränsas till IKE används. Välj **Manual (Manuell)**.
Authentication Key (ESP, AH) (Autentiseringsnycket (ESP, AH))	Ange värdet för **In/Out (In/ut)**. Dessa inställningar är nödvändiga när du väljer **Custom (Egna inställningar)** för **Use Prefixed Template (Använd prefixad mall)** och **Manual (Manuell)** väljs för **Internet Key Exchange (IKE)**, och någon annan inställning än **None (Inget)** väljs för **Hash** under avsnittet **Encapsulating Security (Inbäddad säkerhet)**. Det antal tecken du kan ange kan skilja sig åt beroende på vilken inställning du väljer för **Hash** under avsnittet **Encapsulating Security (Inbäddad säkerhet)**. Om längden för den angivna autentiseringsnyckeln skiljer sig från den valda hash-algoritmen uppstår ett fel. • **MD5**: 128 bitar (16 byte) • **SHA1**: 160 bitar (20 byte) • **SHA256**: 256 bitar (32 byte) • **SHA384**: 384 bitar (48 byte) • **SHA512**: 512 bitar (64 byte) Om du anger nyckeln med ASCII-kod markerar du tecknen med dubbla citattecken (").
Code key (ESP) (Kodnyckel (ESP))	Ange värdet för **In/Out (In/ut)**. Dessa inställningar är nödvändiga när **Custom (Egna inställningar)** väljs för **Use Prefixed Template (Använd prefixad mall)**, **Manual (Manuell)** väljs för **Internet Key Exchange (IKE)**, och **ESP** väljs för **Protocol (Protokoll)** i **Encapsulating Security (Inbäddad säkerhet)**. Det antal tecken du kan ange kan skilja sig åt beroende på vilken inställning du väljer för **Encryption (Kryptering)** under avsnittet **Encapsulating Security (Inbäddad säkerhet)**. Om längden för den angivna nyckelkoden skiljer sig från den valda krypteringsalgoritmen uppstår ett fel. • **DES**: 64 bitar (8 byte) • **3DES**: 192 bitar (24 byte) • **AES-CBC 128**: 128 bitar (16 byte) • **AES-CBC 256**: 256 bitar (32 byte) Om du anger nyckeln med ASCII-kod markerar du tecknen med dubbla citattecken (").
SPI	Dessa parametrar används för att identifiera säkerhetsinformationen. En värd har vanligtvis flera SA (Security Associations) för flera olika typer av IPsec-kommunikation. Det är därför nödvändigt att identifiera

Alternativ	Beskrivning
	lämplig SA när ett IPsec-paket tas emot. SPI-parametern, som identifierar SA, finns i AH- (Authentication Header) och ESP-rubriken (Encapsulating Security Payload). Dessa inställningar är nödvändiga när du väljer **Custom (Egna inställningar)** för **Use Prefixed Template (Använd prefixad mall)** och **Manual (Manuell)** väljs för **Internet Key Exchange (IKE)**. Ange värdet för **In/Out (In/ut)**. (3-10 tecken)
Encapsulating Security (Inbäddad säkerhet)	• **Protocol (Protokoll)** Välj **ESP** eller **AH**. - ESP är ett protokoll som används för krypterad kommunikation med IPsec. ESP krypterar innehållet (kommunicerat innehåll) och lägger till ytterligare information. IP-paketet består av rubriken och den krypterade nyttolasten, som följer rubriken. Utöver krypterade data ingår även information om krypteringsmetoden, krypteringsnyckeln, autentiseringsdata o.s.v. i IP-paketet. - AH är en del av IPsec-protokollet som autentiserar avsändaren och förhindrar att informationen manipuleras (försäkrar att informationen levereras i sin helhet). Informationen infogas omedelbart efter rubriken i IP-paketet. Paketen innehåller dessutom hashvärden, som beräknas med en ekvation från det innehåll som kommuniceras, den hemliga nyckeln och så vidare, för att förhindra att förfalskning av avsändaren och manipulering av informationen sker. Till skillnad från ESP krypteras inte kommunicerat innehåll och informationen skickas och tas emot som vanlig text. • **Encryption (Kryptering) (Inte tillgänglig för alternativet AH.)** Välj **DES**, **3DES**, **AES-CBC 128** eller **AES-CBC 256**. • **Hash** Välj **None (Inget)**, **MD5**, **SHA1**, **SHA256**, **SHA384** eller **SHA512**. **None (Inget)** kan endast väljas när **ESP** är valt för **Protocol (Protokoll)**. • **SA Lifetime (SA livslängd)** Ange livslängden för IKE SA. Ange tiden (sekunder) och antalet kilobyte (KB). • **Encapsulation Mode (Inkapslingssläge)** Välj **Transport (Transport)** eller **Tunnel (Tunnel)**. • **Remote Router IP-Address (Fjärrouter IP Adress)** Ange IP-adressen (IPv4 eller IPv6) för fjärroutern. Ange endast denna information när du valt läget **Tunnel (Tunnel)**. SA (Security Association) är en krypterad kommunikationsmetod som använder IPsec eller IPv6 som överför och delar information, som t.ex. krypteringsmetod och krypteringsnyckel, för att kunna upprätta en säker kommunikationskanal innan kommunikationen påbörjas. SA kan också hänvisa till en virtuell, krypterad kommunikationskanal som har upprättats. SA som används för IPsec upprättar krypteringsmetod, överför nycklar och utför gemensam autentisering i enlighet med standardförfarandet IKE (Internet Key Exchange). SA uppdateras dessutom regelbundet.

Närliggande information

- Konfigurera en IPsec-mall med hjälp av webbaserad hantering

Använd IEEE 802.1x-autentisering för nätverket

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

Vad är IEEE 802.1x-autentisering?

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

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket

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

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

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

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

   Exempel:

   https://192.168.1.2

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

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

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

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

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

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

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

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

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

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

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

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

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

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket

Liknande ämnen:

- Översikt över funktioner för säkerhetscertifikat
- Konfigurera certifikat för enhetssäkerhet

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

IEEE 802.1x-autentiseringsmetoder

EAP-FAST

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

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

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

EAP-MD5 (trådbundet nätverk)

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

PEAP

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

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

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

Din Brother-maskin har stöd för följande inre autentiseringsmetoder:

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

EAP-TLS

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

Närliggande information

- Använd IEEE 802.1x-autentisering för nätverket

Användarautentisering

- Använda autentisering av Active Directory
- Använd LDAP-autentisering
- Använd Secure Function Lock 3.0 (säkert funktionslås)

Använda autentisering av Active Directory

- Introduktion till autentisering av Active Directory
- Konfigurera autentisering av Active Directory med hjälp av webbaserad hantering
- Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (autentisering av Active Directory)

Introduktion till autentisering av Active Directory

Active Directory-autentisering begränsar användningen av maskinen. Om du aktiverar autentisering av Active Directory kommer maskinens kontrollpanel att låsas. Det går inte att ändra maskinens inställningar förrän användaren anger användar-ID och lösenord.

Vid autentisering av Active Directory ingår följande funktioner:

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

- Lagrar inkommande utskriftsdata
- Lagrar inkommande faxdata
- E-postadressen erhålls från Active Directory-servern baserat på ditt användar-ID när skannade data skickas till en e-postserver.

  Välj **On (På)** alternativet för **Get Mail Address (Hämta e-postadress)** inställningen samt **LDAP + kerberos** eller **LDAP + NTLMv2** autentiseringsmetoden för att använda denna funktion. Din e-postadress ställs in som avsändare när maskinen skickar skannade data till en e-postserver eller som mottagare om du vill skicka skannade data till din e-postadress.

Maskinen lagrar alla inkommande faxdata när autentisering av Active Directory är aktiverat. Efter att du loggat in skriver maskinen ut alla lagrade faxdata.

Du kan ändra inställningarna för autentisering av Active Directory med Webbaserad hantering.

Närliggande information

- Använda autentisering av Active Directory

Konfigurera autentisering av Active Directory med hjälp av webbaserad hantering

Funktionen för autentisering av Active Directory stöder Kerberos-autentisering och NTLMv2-autentisering. Du måste konfigurera SNTP-protokollet (tidsserver i nätverket) och DNS-serverkonfiguration för autentisering.

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **User Restriction Function (Användarbegränsad funktion)** eller **Restriction Management (Hantera begränsningar)**.

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

5. Välj **Active Directory Authentication (Autentisering av aktiv mapp)**.
6. Klicka på **Submit (Skicka)**.
7. Klicka på **Active Directory Authentication (Autentisering av aktiv mapp)**.
8. Konfigurera följande inställningar:

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

Alternativ	Beskrivning
Storage Fax RX Data (Lagra mottagen faxdata)	Välj detta alternativ för att lagra inkommande fax. Du kan skriva ut alla inkommande fax när du har loggat in på maskinen.
Remember User ID (Kom ihåg användar-ID)	Välj detta alternativ för att spara ditt användar-ID.
Active Directory Server Address (Serveradress till aktiv mapp)	Ange IP-adressen eller servernamnet (t.ex.: ad.example.com) för Active Directory-servern.
Active Directory Domain Name (Domännamn för Active Directory)	Ange domännamnet för Active Directory.
Protocol & Authentication Method (Protokoll & Autentiseringsmetod)	Välj protokoll och autentiseringsmetod.
SSL/TLS	Välj alternativet **SSL/TLS**.
LDAP Server Port (LDAP-serverport)	Ange portnumret som du vill använda för att ansluta Active Directory-servern via LDAP (endast tillgängligt för **LDAP + kerberos** eller **LDAP + NTLMv2** -autentiseringsmetoden).

Alternativ	Beskrivning
LDAP Search Root (LDAP-sökrot)	Ange LDAP-sökroten (endast tillgänglig för autentiseringsmetod **LDAP + kerberos** eller **LDAP + NTLMv2**).
Get Mail Address (Hämta e-postadress)	Välj detta alternativ för att erhålla inloggade användares e-postadresser från Active Directory-servern. (endast tillgänglig för autentiseringsmetod **LDAP + kerberos** eller **LDAP + NTLMv2**)
Get User's Home Directory (Hämta användares hemregister)	Välj detta alternativ för att erhålla ditt hemregister som destination för Skanna till nätverk. (endast tillgänglig för autentiseringsmetod **LDAP + kerberos** eller **LDAP + NTLMv2**)

9. Klicka på **Submit (Skicka)**.

Närliggande information

- Använda autentisering av Active Directory

Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (autentisering av Active Directory)

När du aktiverat Active Directory-autentisering blir maskinens kontrollpanel låst tills du anger användar-ID och lösenord på maskinens kontrollpanel.

1. Ange ditt användar-ID och lösenord på maskinens kontrollpanel.
2. När autentiseringen är genomförd kommer maskinens kontrollpanel att låsas upp.

Närliggande information

- Använda autentisering av Active Directory

Använd LDAP-autentisering

- Introduktion till LDAP-autentisering
- Konfigurera LDAP-autentisering med hjälp av webbaserad hantering
- Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (LDAP-autentisering)

Introduktion till LDAP-autentisering

LDAP-autentisering begränsar användningen av maskinen. Om du aktiverar LDAP-autentisering kommer maskinens kontrollpanel att låsas. Det går inte att ändra maskinens inställningar förrän användaren anger användar-ID och lösenord.

LDAP-autentisering erbjuder följande funktioner:

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

- Lagrar inkommande utskriftsdata
- Lagrar inkommande faxdata
- E-postadressen erhålls från LDAP-servern baserat på din användar-ID när skannade data skickas till en e-postserver.

  Välj alternativet **On (På)** för inställningen **Get Mail Address (Hämta e-postadress)** för att kunna använda denna funktion. Din e-postadress ställs in som avsändare när maskinen skickar skannade data till en e-postserver eller som mottagare om du vill skicka skannade data till din e-postadress.

Maskinen lagrar alla inkommande faxdata när LDAP-autentisering är aktiverat. Efter att du loggat in skriver maskinen ut alla lagrade faxdata.

Du kan ändra inställningarna för LDAP-autentisering med Webbaserad hantering.

Närliggande information

- Använd LDAP-autentisering

Konfigurera LDAP-autentisering med hjälp av webbaserad hantering

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **User Restriction Function (Användarbegränsad funktion)** eller **Restriction Management (Hantera begränsningar)**.

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

5. Välj **LDAP Authentication (LDAP-verifiering)**.
6. Klicka på **Submit (Skicka)**.
7. Klicka på menyn **LDAP Authentication (LDAP-verifiering)**.
8. Konfigurera följande inställningar:

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

Alternativ	Beskrivning
Storage Fax RX Data (Lagra mottagen faxdata)	Välj detta alternativ för att lagra inkommande fax. Du kan skriva ut alla inkommande fax när du har loggat in på maskinen.
Remember User ID (Kom ihåg användar-ID)	Välj detta alternativ för att spara ditt användar-ID.
LDAP Server Address (LDAP-serveradress)	Ange IP-adressen eller servernamnet (till exempel: ldap.example.com) för LDAP-servern.
SSL/TLS	Välj alternativet **SSL/TLS** för att använda LDAP framför SSL/TLS.
LDAP Server Port (LDAP-serverport)	Ange LDAP-serverportnummer.
LDAP Search Root (LDAP-sökrot)	Ange register för LDAP-sökroten.
Attribute of Name (Search Key) (Namnattribut (söknyckel))	Ange attributet som du vill använda som söknyckel.
Get Mail Address (Hämta e-postadress)	Välj detta alternativ för att erhålla den inloggade användarens e-postadress från LDAP-servern.
Get User's Home Directory (Hämta användares hemregister)	Välj detta alternativ för att erhålla ditt hemregister som destination för Skanna till nätverk.

9. Klicka på **Submit (Skicka)**.

Närliggande information

- Använd LDAP-autentisering

Logga in för att ändra maskinens inställningar via maskinens kontrollpanel (LDAP-autentisering)

När du aktiverat LDAP-autentisering blir maskinens kontrollpanel låst tills du anger användar-ID och lösenord på maskinens kontrollpanel.

1. Ange ditt användar-ID och lösenord på maskinens kontrollpanel.
2. När autentiseringen är genomförd kommer maskinens kontrollpanel att låsas upp.

Närliggande information

- Använd LDAP-autentisering

Använd Secure Function Lock 3.0 (säkert funktionslås)

Secure Function Lock 3.0 (säkert funktionslås) ger ökad säkerhet genom att begränsa de tillgängliga funktionerna på maskinen.

- Innan du använder Secure Function Lock 3.0
- Konfigurera Secure Function Lock 3.0 med hjälp av webbaserad hantering
- Skanna med hjälp av Secure Function Lock 3.0
- Konfigurera offentligt läge för Secure Function Lock 3.0
- Konfigurera personliga startskärmsinställningar med hjälp av webbaserad hantering.
- Ytterligare funktioner i Secure Function Lock 3.0
- Registrera ett nytt IC-kort via maskinens kontrollpanel
- Registrera en extern IC-kortläsare

Innan du använder Secure Function Lock 3.0

Använd Secure Function Lock (Säkert funktionslås) för att konfigurera lösenord, ställa in sidbegränsningar för användare och neka tillgång till vissa eller alla funktioner som listas här.

Du kan konfigurera och ändra följande inställningar för Secure Function Lock 3.0 (Säkert funktionslås 3.0) genom att använda Webbaserad hantering:

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

- **Print (Skriv ut)**
- **Copy (Kopiera)**
- **Scan (Skanna)**
- **Fax**
- **Media**
- **Web Connect (Anslut till webben)**
- **Apps (Appar)**
- **Page Limits (Sidbegränsning)**
- **Page Counters (Sidräknare)**
- **Card ID (NFC ID) (Kort-ID (NFC ID))**

Modeller med LCD-pekskärm:

När Secure Function Lock (Säkert funktionslås) är aktiverat går maskinen automatiskt in i offentligt läge och vissa av maskinens funktioner blir begränsade till authorized användare. För att komma åt de begränsade maskinfunktionerna, tryck på , välj ditt användarnamn och ange ditt lösenord.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Konfigurera Secure Function Lock 3.0 med hjälp av webbaserad hantering

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **User Restriction Function (Användarbegränsad funktion)** eller **Restriction Management (Hantera begränsningar)**.

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

5. Välj **Secure Function Lock (Säkert funktionslås)**.
6. Klicka på **Submit (Skicka)**.
7. Klicka på menyn **Restricted Functions (Begränsade funktioner)**.
8. Konfigurera inställningarna för att hantera begränsningar per användare eller grupp.
9. Klicka på **Submit (Skicka)**.
10. Klicka på menyn **User List (Användarlista)**.
11. Konfigurera användarlistan.
12. Klicka på **Submit (Skicka)**.

Du kan även ändra spärrinställningarna för användarlistan i menyn **Secure Function Lock (Säkert funktionslås)**.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Skanna med hjälp av Secure Function Lock 3.0

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

Ställa in skanningsrestriktioner (för administratörer)

Med funktionen Secure Function Lock 3.0 (säkert funktionslås) kan administratören begränsa vilka användare som får skanna. När skanningsfunktionen är avstängd för de allmänna användarna kan bara användare med **Scan (Skanna)** markerat i kryssrutan använda skanningsfunktionen.

Använda skanningsfunktionen (för begränsade användare)

- Skanna med maskinens kontrollpanel:

  Begränsade användare måste ange sina lösenord på maskinens kontrollpanel för att få åtkomst till skanningsläget.
- Skanna från en dator:

  Begränsade användare måste ange sina lösenord på maskinens kontrollpanel innan de skannar från sina datorer. Om lösenordet inte anges på maskinens kontrollpanel visas ett felmeddelande på användarens dator.

Om maskinen stödjer IC-kortsautentisering kan användare med begränsad behörighet även använda läget Skanna genom att vidröra NCF-symbolen på maskinens kontrollpanel med sitt registrerade IC-kort.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Konfigurera offentligt läge för Secure Function Lock 3.0

Använd skärmen Secure Function Lock för att ställa in Offentligt läge, vilket begränsar funktioner som finns tillgängliga för offentliga användare. Offentliga användare behöver inte ange lösenord för att använda funktionerna som är tillgängliga via inställningarna för allmänt läge.

Offentligt läge omfattar utskriftsjobb som skickats via Brother iPrint&Scan och Brother Mobile Connect.

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **User Restriction Function (Användarbegränsad funktion)** eller **Restriction Management (Hantera begränsningar)**.

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

5. Välj **Secure Function Lock (Säkert funktionslås)**.
6. Klicka på **Submit (Skicka)**.
7. Klicka på menyn **Restricted Functions (Begränsade funktioner)**.
8. I raden **Public Mode (Offentligt läge)** väljer du en kryssruta för att tillåta eller ta bort markeringen i en kryssruta för att begränsa den angivna funktionen.
9. Klicka på **Submit (Skicka)**.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Konfigurera personliga startskärmsinställningar med hjälp av webbaserad hantering.

Som en administratör kan du ange vilka flikar användare kan se på sina personliga startskärmar. De här flikarna ger snabb åtkomst till användarnas favorite, som de kan tilldela sina personliga hemskärmsflikar från skannerns kontrollpanel.

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

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **User Restriction Function (Användarbegränsad funktion)** eller **Restriction Management (Hantera begränsningar)**.

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

5. Välj **Secure Function Lock (Säkert funktionslås)**.
6. I fältet **Tab Settings (Flikinställningar)** väljer du **Personal (Personlig)** för fliknamnen som du vill använda som din personliga startskärm.
7. Klicka på **Submit (Skicka)**.
8. Klicka på menyn **Restricted Functions (Begränsade funktioner)**.
9. Konfigurera inställningarna för att hantera begränsningarna per användare eller grupp.
10. Klicka på **Submit (Skicka)**.
11. Klicka på menyn **User List (Användarlista)**.
12. Konfigurera användarlistan.
13. Välj **User List / Restricted Functions (Användarlista / Begränsade funktioner)** för varje användare i rullgardinsmenyn.
14. Välj fliknamnet för varje användare i rullgardinsmenyn **Home Screen (Startskärm)**.
15. Klicka på **Submit (Skicka)**.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Ytterligare funktioner i Secure Function Lock 3.0

Du kan ställa in följande funktioner i skärmen för Secure Function Lock:

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

All Counter Reset (Nollställ alla räknare)

Klicka på **All Counter Reset (Nollställ alla räknare)** i kolumnen **Page Counters (Sidräknare)** för att nollställa sidräknaren.

Export to CSV file (Exportera till CSV-fil)

Klicka på **Export to CSV file (Exportera till CSV-fil)** för att exportera den aktuella och sista sidräkningen inklusive information om **User List / Restricted Functions (Användarlista / Begränsade funktioner)** som en CSV-fil.

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

Klicka på menyn **User List (Användarlista)** och ange sedan en användares kort-ID i fältet **Card ID (NFC ID) (Kort-ID (NFC ID))**. Du kan använda ditt IC-kort för autentisering.

Output (Destination)

Välj utmatningsfack för varje användare i rullgardinsmenyn när enheten med sorteringsfack har installerats på maskinen.

Last Counter Record (Registrering av senaste räkneverk)

Klicka på **Last Counter Record (Registrering av senaste räkneverk)** om du vill att maskinen ska behålla sidräkningen efter det att räknaren har nollställts.

Counter Auto Reset (Återställ räkneverk automatiskt)

Klicka på **Counter Auto Reset (Återställ räkneverk automatiskt)** för att konfigurera det tidsintervall du vill ha mellan nollställning av sidräknaren. Välj intervallen dagligen, veckovis eller månadsvis.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Registrera ett nytt IC-kort via maskinens kontrollpanel

Du kan registrera integrerade kretskort (IC-kort) på din maskin.

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

1. Håll ett registrerat integrerat kretskort (IC-kort) mot symbolen för NFC (Near-Field Communication) på maskinens kontrollpanel.
2. Tryck på ditt användar-ID på LCD-skärmen.
3. Tryck på knappen Registrera kort.
4. Håll ett nytt IC-kort över NFC-symbolen.

   Det nya IC-kortets nummer är sedan registrerat för maskinen.
5. Tryck på knappen OK.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Registrera en extern IC-kortläsare

När du ansluter en extern IC-kortläsare (integrerad krets) använder du Webbaserad hantering för att registrera kortläsaren. Din maskin har stöd för externa IC-kortläsare som stöds av HID-klassade drivrutiner.

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

   Exempel:

   https://192.168.1.2

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

   Standardlösenordet för att hantera maskinens inställningar finns på maskinens baksida eller undersida och är märkt med texten “**Pwd**”. Ändra standardlösenordet genom att följa anvisningarna på skärmen första gången du loggar in.
4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **External Card Reader (Extern kortläsare)**.

   Om det vänstra navigeringsfältet inte är synligt börjar du navigera från ☰.
5. Ange den information som behövs och klicka sedan på **Submit (Skicka)**.
6. Starta om Brother-maskinen för att aktivera konfigurationen.
7. Anslut kortläsaren till maskinen.
8. Håll kortet mot kortläsare vid användning av kortautentisering.

Närliggande information

- Använd Secure Function Lock 3.0 (säkert funktionslås)

Sända eller ta emot e-post säkert

- Konfigurera e-postsändning eller -mottagning med hjälp av Webbaserad hantering
- Skicka ett e-postmeddelande med användarautentisering
- Skicka eller ta emot e-post säkert med SSL/TLS

Konfigurera e-postsändning eller -mottagning med hjälp av Webbaserad hantering

- Mottagning av e-post är endast tillgängligt för vissa modeller.
- Vi rekommenderar att du använder Webbaserad hantering för att konfigurera säkrad e-postsändning med användarautentisering eller e-postsändning eller e-postmottagning med hjälp av SSL/TLS (endast modeller som stöds).

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

   Exempel:

   https://192.168.1.2

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

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

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

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

5. Klicka på fältet **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**, klicka på **Advanced Settings (Avancerade inställningar)** och se till att status för **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)** är **Enabled (Aktiverad)**.

- Tillgängliga protokoll kan variera beroende på din maskin.
- Om valskärmen **Authentication Method (Autentiseringsmetod)** visas, väljer du din autentiseringsmetod och följer sedan anvisningarna på skärmen.

6. Konfigurera inställningarna för **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**.
   - Kontrollera att e-postinställningarna är korrekta efter konfigurationen genom att skicka ett e-postmeddelande som test.
   - Om du inte känner till inställningarna för POP3/IMAP4/SMTP-servern kan du kontakta din nätverksadministratör eller ISP (Internetleverantör).
7. Klicka på **Submit (Skicka)** när du är klar.

   Dialogrutan **Test Send/Receive E-mail Configuration (Testa konfiguration för att sända/ta emot e-post)** visas.
8. Följ anvisningarna i dialogrutan för att testa de aktuella inställningarna.

Närliggande information

- Sända eller ta emot e-post säkert

Liknande ämnen:

- Skicka eller ta emot e-post säkert med SSL/TLS

Skicka ett e-postmeddelande med användarautentisering

Din maskin skickar e-postmeddelanden via en e-postserver som kräver användarautentisering. Denna metod förhindrar att unauthorized användare får åtkomst till e-postservern.

Du kan skicka e-postmeddelanden, e-postrapporter och I-Fax (endast tillgängligt för vissa modeller) med användarautentisering.

- Tillgängliga protokoll kan variera beroende på din maskin.
- Vi rekommenderar att du använder webbaserad hantering för att konfigurera SMTP-autentisering.

Inställningar för e-postserver

Du måste konfigurera maskinens SMTP-autentiseringsmetod så att den överensstämmer med den metod som används för e-postservern. Din nätverksadministratör eller Internetleverantör (ISP) kan ge dig detaljer om inställningarna för e-postservern.

För att aktivera SMTP-serverautentisering med webbaserad hantering, välj din autentiseringsmetod under **Server Authentication Method (Serverns autentiseringsmetod)** på **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP-klient)**-skärmen.

Närliggande information

- Sända eller ta emot e-post säkert

Skicka eller ta emot e-post säkert med SSL/TLS

Maskinen har stöd för SSL/TLS-kommunikationsmetoder. Om du vill använda en e-postserver som använder SSL/TLS-kommunikation måste du konfigurera följande inställningar.

- Mottagning av e-post är endast tillgängligt för vissa modeller.
- Vi rekommenderar att du använder webbaserad hantering för att konfigurera SSL/TLS.

Verifiera servercertifikat

Under **SSL/TLS** eller om du väljer **SSL** eller **TLS**, kommer kryssrutan **Verify Server Certificate (Verifiera servercertifikat)** att markeras automatiskt.

- Innan du verifierar servercertifikatet måste du importera CA-certifikatet som har utfärdats av den CA som signerade servercertifikatet. Kontakta din nätverksadministratör eller Internetleverantör (ISP) för att bekräfta om ett CA-certifikat måste importeras eller inte.
- Om du inte behöver verifiera servercertifikatet, avmarkera **Verify Server Certificate (Verifiera servercertifikat)**.

Portnummer

Om du väljer **SSL** eller **TLS** kommer värdet **Port** att ändras för att överensstämma med protokollet. För att ändra portnumret manuellt, ange portnumret sedan du har valt **SSL/TLS**-inställningar.

Du måste konfigurera maskinens kommunikationsmetod så att den överensstämmer med den metod som används för din e-postserver. Din nätverksadministratör eller Internetleverantör kan ge dig detaljer om inställningarna för e-postservern.

I de flesta fallen krävs följande inställningar för säkra tjänster för webbaserad e-post:

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

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

Närliggande information

- Sända eller ta emot e-post säkert

Liknande ämnen:

- Konfigurera e-postsändning eller -mottagning med hjälp av Webbaserad hantering
- Konfigurera certifikat för enhetssäkerhet

Spara utskriftsloggen på nätverket

- Spara utskriftslogg till nätverk – översikt
- Konfigurera inställningarna för Spara utskriftslogg på nätverket med hjälp av webbaserad hantering
- Använd inställningen för felidentifiering under Spara utskriftsloggen på nätverket
- Använda Spara utskriftslogg på nätverket med Secure Function Lock 3.0

Spara utskriftslogg till nätverk – översikt

Med funktionen Spara utskriftsloggen till nätverk kan du spara utskriftsloggfilen från maskinen till en nätverksserver med hjälp av CIFS-protokoll (Common Internet File System). Du kan registrera ID, typ av utskriftsjobb, jobbnamn, användarnamn, datum, tid och antalet utskrivna sidor för varje utskriftsjobb. CIFS är ett protokoll som körs på TCP/IP som gör det möjligt för datorer i ett nätverk att dela filer via ett intranät eller på Internet.

Följande utskriftsfunktioner registreras i utskriftsloggen:

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

- Utskriftsjobb från din dator
- Direktutskrift från USB
- Kopiera
- Mottaget fax
- Web Connect-utskrift

- Funktionen Spara utskriftslogg på nätverket stödjer Kerberos-autentisering och NTLMv2-autentisering. Du måste konfigurera SNTP-protokollet (tidsserver i nätverket) eller så måste du ställa in korrekt datum, tid och tidszon på kontrollpanelen för autentisering.
- Du kan ange att filtypen ska vara TXT eller CSV när du sparar en fil på servern.

Närliggande information

- Spara utskriftsloggen på nätverket

Konfigurera inställningarna för Spara utskriftslogg på nätverket med hjälp av webbaserad hantering

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **Store Print Log to Network (Spara utskriftsloggen på nätverket)**.

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

5. I fältet **Print Log (Utskriftslogg)** klickar du på **On (På)**.
6. Konfigurera följande inställningar:

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

Alternativ	Beskrivning
Network Folder Path (Sökväg till nätverksmapp)	Ange målmappen där utskriftsloggen ska sparas på CIFS-servern (t.ex. \\datornamn\Delat).
File Name (Filnamn)	Ange filnamnet du vill använda för utskriftsloggen (högst 32 tecken).
File Type (Filtyp)	Välj alternativet **TXT** eller **CSV** för utskriftsloggens filtyp.
Time Source for Log (Tidskälla för logg)	Välj tidskälla för utskriftsloggen.
Auth. Method (Autentiseringsmetod)	Välj den autentiseringsmetod som krävs för åtkomst till CIFS-servern: **Auto**, **Kerberos** eller **NTLMv2**. Kerberos är ett autentiseringsprotokoll som gör det möjligt för enheter eller personer att på ett säkert sätt bevisa sin identitet för nätverksservrar med en enda inloggning. NTLMv2 är autentiseringsmetoden som används av Windows för att logga in på servrar. • **Auto**: Om du väljer **Auto**, kommer NTLMv2 att användas som autentiseringsmetod. • **Kerberos**: Välj alternativet **Kerberos** för att endast använda Kerberos-autentisering. • **NTLMv2**: Välj alternativet **NTLMv2** för att endast använda NTLMv2-autentisering.

Alternativ	Beskrivning
	• För autentisering med **Kerberos** och **NTLMv2** måste du också konfigurera inställningen för **Date&Time (Datum och tid)** eller SNTP-protokollet (tidsserver i nätverket) och DNS-server. • Du kan också konfigurera inställningarna för datum och tid via maskinens kontrollpanel.
Username (Användarnamn)	Ange användarnamnet för autentisering (högst 96 tecken). Om användarnamnet är en del av en domän anger du användarnamnet enligt något av följande format: användare@domän eller domän\användare.
Password (Lösenord)	Ange lösenordet för autentisering (högst 32 tecken).
Kerberos Server Address (Kerberos serveradress) (vid behov)	Ange värdadressen till Key Distribution Center (KDC) (t.ex.: kerberos.exempel.com; med högst 64 tecken) eller IP-adressen (t.ex.: 192.168.56.189).
Error Detection Setting (Inställning för feldetektering)	Välj vilken åtgärd som ska vidtas när utskriftsloggen inte kan sparas på servern på grund av nätverksfel.

7. I fältet **Connection Status (Anslutningsstatus)** bekräftar du den senaste loggstatusen.

Du kan också bekräfta felstatus på maskinens LCD-skärm.

8. Klicka på **Submit (Skicka)** för att visa **Test Print Log to Network (Testa utskrift av logg till nätverk)**-sidan.
   Klicka på **Yes (Ja)** för att testa dina inställningarna och fortsätt sedan till nästa steg.
   Klicka på **No (Nej)** för att hoppa över testet. Inställningarna skickas automatiskt.
9. Maskinen testar inställningarna.
10. Om inställningarna godkänns så visas **Test OK** på skärmen.
    Om **Test Error (Testfel)** visas så kontrollerar du alla inställningar och klickar sedan på **Submit (Skicka)** för att visa testsidan på nytt.

Närliggande information

- Spara utskriftsloggen på nätverket

Använd inställningen för felidentifiering under Spara utskriftsloggen på nätverket

Använd inställningen för felidentifiering för att avgöra åtgärd som ska tas när utskriftsloggen inte kan sparas på servern på grund av ett nätverksfel.

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

   Exempel:

   https://192.168.1.2

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

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

4. I det vänstra navigeringsfältet klickar du på **Administrator (Administratör)** > **Store Print Log to Network (Spara utskriftsloggen på nätverket)**.

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

5. Under avsnittet **Error Detection Setting (Inställning för feldetektering)** väljer du alternativet **Cancel Print (Avbryt utskrift)** eller **Ignore Log & Print (Ignorera logg och utskrift)**.

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

Alternativ	Beskrivning
Cancel Print (Avbryt utskrift)	Om du väljer alternativet **Cancel Print (Avbryt utskrift)** canceled utskriftsjobben när utskriftsloggen inte kan sparas på servern. Även om du väljer alternativet **Cancel Print (Avbryt utskrift)**, skriver maskinen ut ett mottaget fax.

Ignore Log & Print (Ignorera logg och utskrift)	Om du väljer alternativet **Ignore Log & Print (Ignorera logg och utskrift)** skriver maskinen ut dokumentet även om utskriftsloggen inte kan sparas på servern.
	När funktionen för att spara utskriftsloggen har återställts registreras utskriftsloggen enligt nedan:
	`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. Om utskriftsloggen inte kan sparas vid avslutad utskrift registreras inte antalet utskrivna sidor.
	b. Om utskriftsloggen inte kan sparas vid påbörjad och avslutad utskrift registreras inte utskriftsloggen. Felet visas i utskriftsloggen när funktionen återställts.

6. Klicka på **Submit (Skicka)** för att visa **Test Print Log to Network (Testa utskrift av logg till nätverk)**-sidan.

   Klicka på **Yes (Ja)** för att testa dina inställningarna och fortsätt sedan till nästa steg.

Klicka på **No (Nej)** för att hoppa över testet. Inställningarna skickas automatiskt.

7. Maskinen testar inställningarna.
8. Om inställningarna godkänns så visas **Test OK** på skärmen.

   Om **Test Error (Testfel)** visas så kontrollerar du alla inställningar och klickar sedan på **Submit (Skicka)** för att visa testsidan på nytt.

Närliggande information

- Spara utskriftsloggen på nätverket

Använda Spara utskriftslogg på nätverket med Secure Function Lock 3.0

När Secure Function Lock 3.0 (Säkert funktionslås) är aktivt sparas namnen på de användare som är registrerade för kopiering, faxmottagning, WebConnect-utskrift och direktutskrift med USB (om detta är tillgängligt) i rapporten för Spara utskriftslogg på nätverket. När autentisering av Active Directory är aktiverat sparas användarnamnet i rapporten Spara utskriftslogg på nätverket:

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

```
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
```

Närliggande information

- Spara utskriftsloggen på nätverket

brother

Brother Earth

www.brotherearth.com

SWE
Version 0