

Tietoturvaopas

Tärkeitä turvallisuuteen liittyviä tietoja

- Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen pohjassa, ja sen yhteydessä on merkintä **"Pwd"**. Suosittelemme, että vaihdat oletussalasanan välittömästi, jotta voit suojata laitettasi luvattomalta käytöltä.
- Kun yhdistät laitteen ulkopuoliseen verkkoon, kuten Internetiin, varmista, että verkkoympäristösi on suojattu erillisellä palomuurilla tai muulla menetelmällä, jotta estetään puutteellisten asetusten tai haitallisten kolmansien osapuolten luvattoman käytön aiheuttamat tietovuodot.
- Jos läheltä löytyy signaali, langattoman lähiverkon avulla voit muodostaa vapaasti lähiverkkoyhteyden. Jos suojausasetuksia ei ole kuitenkaan määritetty oikein, pahantahtoinen kolmas osapuoli voi siepata signaalin, mistä voi seurata mahdollisesti
 - henkilökohtaisten tai luottamuksellisten tietojen varastaminen
 - tietojen asiaton lähetys osapuolille, jotka teeskentelevät olevansa tiettyjä henkilöitä
 - siepatun jäljennetyn viestintäsisällön levittäminen.



Aiheeseen liittyviä tietoja

- [Verkko](#)
-

Varmenteiden määrittäminen laitteen suojaukselle

Verkotetun laitteen turvallista hallintaa varten SSL/TLS:n avulla on määritettävä varmenne. Varmenteen määrittämiseen on käytettävä WWW-pohjaista hallintaa.

- [Suojausvarmteen ominaisuuksien yleiskuvaus](#)
- [Varmenteen luominen ja asentaminen](#)
- [Itseallekirjoitetun varmenteen luominen](#)
- [Varmenteen allekirjoituspyynnön \(CSR\) luonti ja varmentajan \(CA\) varmenteen asentaminen](#)
- [Varmenteen ja yksityisen avaimen tuominen ja vieminen](#)
- [CA-varmenteen tuonti ja vienti](#)

Suojausvarmteen ominaisuuksien yleiskuvaus

Laitteesi tukee useiden suojausvarmenteiden käyttöä, mikä mahdollistaa suojatun todennuksen ja tiedonsiirron laitteen kanssa. Laitteessa voidaan käyttää seuraavia suojausvarmteen ominaisuuksia:



Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

- SSL/TLS-tiedonsiirto
- IEEE 802.1x -todennus
- IPsec

Laitteesi tukee seuraavia:

- Esiasennettu varmenne

Laitteessa on esiasennettu itseallekirjoitettu varmenne. Tämän varmteen avulla voit käyttää SSL/TLS-tiedonsiirtoa luomatta tai asentamatta eri varmennetta.



Esiasennettu itseallekirjoitettu varmenne suojaa tiedonsiirtoasi tiettyyn pisteeseen asti. Suosittelemme käyttämään luotettavan organisaation julkaisemaa varmennetta paremman turvallisuuden varmistamiseksi.

- Itseallekirjoitettu varmenne

Tämä tulostuspalvelin myöntää oman varmenteensa. Tämän varmteen avulla voit käyttää kätevästi SSL/TLS-tiedonsiirtoa luomatta tai asentamatta eri CA-varmennetta.

- Varmentajan (CA) myöntämä varmenne

CA:lta saadun varmteen asennukseen on olemassa kaksi tapaa. Jos sinulla on jo CA-varmenne tai jos haluat käyttää ulkopuolista luotettavaa CA:ta:

- Kun käytetään varmennepyyntöä (CSR) tästä tulostuspalvelimesta.
- Kun tuodaan varmenne ja yksityinen avain.

- Varmentajan (CA) varmenne

Kun halutaan käyttää CA-varmennetta, joka tunnistaa itse varmentajan (CA) ja jolla on oma yksityisavain, kyseinen CA-varmenne on tuotava CA:lta ennen verkon suojausominaisuuksien määrittämistä.



- Jos aiot käyttää SSL/TLS-tiedonsiirtoa, suosittelemme ottamaan yhteyttä ensin järjestelmänvalvojaan.
- Kun palautat tulostuspalvelimen takaisin tehdasasetuksiin, asennettu varmenne ja yksityinen avain poistetaan. Jos haluat säilyttää saman varmteen ja yksityisen avaimen tulostuspalvelimen palautuksen jälkeen, vie ne ennen palauttamista ja asenna ne uudelleen.



Aiheeseen liittyviä tietoja

- [Varmenteiden määrittäminen laitteen suojaukselle](#)

Liittyvät aiheet:

- [IEEE 802.1x -todennuksen määrittäminen verkolle WWW-pohjaisen hallinnan avulla \(verkkoselaimella\)](#)

Varmenteen luominen ja asentaminen

Varmenteita on kahdentyyppisiä: itseallekirjoitettu varmenne tai CA:n myöntämä varmenne.

Vaihtoehto 1

Itseallekirjoitettu varmenne

1. Luo itseallekirjoitettu varmenne WWW-pohjaisella hallinnalla.
2. Asenna itseallekirjoitettu varmenne tietokoneeseesi.

Vaihtoehto 2

CA:n myöntämä varmenne

1. Luo CSR-pyyntö WWW-pohjaisen hallinnan avulla.
2. Asenna CA:n myöntämä varmenne Brother-laitteeseen WWW-pohjaisen hallinnan avulla.
3. Asenna varmenne tietokoneeseesi.



Aiheeseen liittyviä tietoja

- [Varmenteiden määrittäminen laitteen suojaukselle](#)
-

Itseallekirjoitetun varmenteen luominen

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvässä, aloita selaus kohdasta ☰.

5. Napsauta **Create Self-Signed Certificate (Luo itseallekirjoitettu varmenne)**.
6. Syötä **Common Name (Yleinen nimi)** ja **Valid Date (Kelvollinen päivämäärä)**.
 - **Common Name (Yleinen nimi)** -pituus on alle 64 tavua. Kirjoita tunniste, kuten IP-osoite tai solmun tai toimialueen nimi, kun muodostat laitteeseen SSL/TLS-yhteyden. Solmun nimi on oletusarvoisesti näkyvässä.
 - Näkyviin tulee varoitus, jos käytät IPPS- tai HTTPS-protokollaa ja kirjoitat URL-kenttään eri nimen kuin kohtaan **Common Name (Yleinen nimi)**, jota käytettiin itse allekirjoitetussa varmenteessa.
7. Valitse laitteesi **Public Key Algorithm (Julkisen avaimen algoritmi)** pudotusluettelosta.
8. Valitse laitteesi **Digest Algorithm (Käsittelyalgoritmi)** pudotusluettelosta.
9. Napsauta **Submit (Lähetä)**.



Aiheeseen liittyviä tietoja

- [Varmenteiden määrittäminen laitteen suojausluomiseen](#)

Varmenteen allekirjoituspyynnön (CSR) luonti ja varmentajan (CA) varmenteen asentaminen

Jos sinulla on varmenne ulkoiselta luotetulta varmentajalta (CA), voit tallentaa varmenteen ja yksityisen avaimen laitteeseen ja hallita niitä tuomalla ja viemällä. Jos sinulla ei ole ulkoiselta, luotetulta varmentajalta (CA) saatua varmennetta, luo varmenteen allekirjoituspyyntö (CSR), lähetä se CA:lle todentamista varten ja asenna saamasi varmenne tietokoneeseesi.

- [CSR:n luominen](#)
- [Varmenteen asentaminen laitteeseen](#)

CSR:n luominen

CSR (Certificate Signing Request) on CA:lle lähetetty pyyntö varmenteen sisältämien valtuuksien todentamiseksi.

On suositeltavaa asentaa CA:n päävarmenne tietokoneeseen ennen CSR:n luomista.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "Pwd". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko) > Security (Suojaus) > Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvässä, aloita selaus kohdasta ☰.

5. Napsauta **Create CSR (Luo varmennepyyntö)**.
6. Syötä **Common Name (Yleinen nimi)** (pakollinen) ja lisää muita liittyen kohteeseen **Organization (Organisaatio)** (valinnainen).



- Sinun on toimitettava yrityksesi tiedot, jotta CA voi varmistaa henkilöllisyytesi ja todistaa sen ulkopuolisille.
- **Common Name (Yleinen nimi)** -pituuden on oltava alle 64 tavua. Kirjoita tunnistetieto, kuten IP-osoite tai solmun tai toimialueen nimi, kun muodostat laitteeseen SSL/TLS-yhteyden. Solmun nimi on oletusarvoisesti näkyvässä. **Common Name (Yleinen nimi)** on määritettävä.
- Näkyviin tulee varoitus, jos kirjoitat URL-kenttään eri nimen kuin varmenteessa käytetty yleinen nimi.
- Kohteiden **Organization (Organisaatio)**, **Organization Unit (Organisaatioyksikkö)**, **City/Locality (Kaupunki/paikkakunta)** ja **State/Province (Osavaltio/provinssi)** pituuksien on oltava alle 64 tavua.
- Kohteen **Country/Region (Maa/alue)** on oltava kaksimerkinäinen, ISO 3166 -standardin mukainen maakoodi.
- Jos määrität X.509v3-varmenteen jatketta, valitse **Configure extended partition (Määritä laajennettu osio)** -valintaruutu ja valitse sitten **Auto (Register IPv4) (Automaattinen (Rekisteri IPv4))** tai **Manual (Manuaalinen)**.

7. Valitse laitteesi **Public Key Algorithm (Julkisen avaimen algoritmi)** -pudotusluettelosta.
8. Valitse laitteesi **Digest Algorithm (Käsittelyalgoritmi)** -pudotusluettelosta.
9. Napsauta **Submit (Lähetä)**.
CSR ilmestyy näytölle. Tallenna CSR tiedostona tai kopioi ja liitä se CA:n CSR-verkkolomakkeeseen.
10. Napsauta **Tallenna**.



- Noudata CA-käytäntöä, kun lähetät CSR:n CA:lle.
- Jos käytät Windows Server -käyttöjärjestelmän Enterprise Root CA -toimintoa, on suositeltavaa käyttää WWW-palvelimen varmennemallia työasemavarmenteen suojattuun luontiin. Jos olet luomassa työasemavarmennetta IEEE 802.1x -ympäristöön EAP-TLS-todennuksen kanssa, suosittelemme varmenteen malliksi Käyttäjää.



Aiheeseen liittyviä tietoja

- Varmenteen allekirjoituspyynnön (CSR) luonti ja varmentajan (CA) varmenteen asentaminen

Varmenteen asentaminen laitteeseen

Kun saat varmenteen myöntäjältä (CA), asenna se tulostuspalvelimelle seuraavien ohjeiden mukaan:

Vain tämän laitteen varmenteen allekirjoituspyynnöllä (CSR) hankittu varmenne voidaan asentaa laitteeseen. Varmista ennen toisen CSR:n luomista, että varmenne on asennettu. Luo toinen CSR vain, kun olet asentanut varmenteen laitteeseen. Muussa tapauksessa ennen asennusta luotu CSR ei kelpaa.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "Pwd". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Napsauta **Install Certificate (Asenna varmenne)**.
6. Selaa tiedostoon, joka sisältää CA:n myöntämän varmenteen, ja napsauta **Submit (Lähetä)**.
Varmenne on nyt luotu ja tallennettu laitteen muistiin.

SSL/TLS-yhteyden käyttäminen edellyttää, että CA:lta saatu päävarmenne on tallennettu tietokoneeseesi. Ota yhteys verkon valvojaan.



Aiheeseen liittyviä tietoja

- [Varmenteen allekirjoituspyynnön \(CSR\) luonti ja varmentajan \(CA\) varmenteen asentaminen](#)

Varmenteen ja yksityisen avaimen tuominen ja vieminen

Voit tallentaa varmenteen ja yksityisen avaimen laitteeseen ja hallita niitä tuomalla ja viemällä.

- [Varmenteen ja yksityisen avaimen tuominen](#)
- [Varmenteen ja yksityisen avaimen vieminen](#)

Varmenteen ja yksityisen avaimen tuominen

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Napsauta **Import Certificate and Private Key (Tuo CA-varmenne ja yksityinen avain)**.
6. Selaa tuotavaan tiedostoon ja valitse se.
7. Kirjoita salasana, jos tiedosto on salattu, ja valitse sitten **Submit (Lähetä)**.

Varmenne ja yksityinen avain on tuotu laitteeseesi.



Aiheeseen liittyviä tietoja

- [Varmenteen ja yksityisen avaimen tuominen ja vieminen](#)

Varmenteen ja yksityisen avaimen vieminen

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Napsauta **Export (Vienti)**, joka näkyy **Certificate List (Varmenneluettelo)**in kanssa.
6. Kirjoita salasana, jos haluat salata tiedoston.
Jos salasanaa ei kirjoiteta, tiedostoa ei salata.
7. Vahvista salasana kirjoittamalla se uudelleen ja valitse sitten **Submit (Lähetä)**.
8. Napsauta **Tallenna**.

Varmenne ja yksityinen avain vietään tietokoneeseesi.

Voit myös tuoda varmenteen tietokoneeseen.



Aiheeseen liittyviä tietoja

- [Varmenteen ja yksityisen avaimen tuominen ja vieminen](#)

CA-varmenteen tuonti ja vienti

Voit tuoda ja tallentaa CA-varmenteita Brother-laitteeseesi ja viedä niitä laitteestasi.

- [CA-varmenteen tuonti](#)
- [CA-varmenteen vienti](#)

CA-varmenteen tuonti

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "Pwd". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **CA Certificate (CA-varmenne)**.



Jos vasen selauspalkki ei ole näkyvässä, aloita selaus kohdasta ☰.

5. Napsauta **Import CA Certificate (Tuo CA-varmenne)**.
6. Selaa tuotavaan tiedostoon.
7. Napsauta **Submit (Lähetä)**.



Aiheeseen liittyviä tietoja

- [CA-varmenteen tuonti ja vienti](#)

CA-varmenteen vienti

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **CA Certificate (CA-varmenne)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Valitse vietävä varmenne ja napsauta **Export (Vienti)**.
6. Napsauta **Submit (Lähetä)**.



Aiheeseen liittyviä tietoja

- [CA-varmenteen tuonti ja vienti](#)

SSL/TLS:n käyttö

- [Verkkolaitteen turvallinen hallinta SSL/TLS:n avulla](#)
- [Asiakirjojen SSL/TLS-suojattu tulostus](#)
- [Sähköpostin suojattu lähetys tai vastaanotto SSL/TLS:n avulla](#)

Verkkolaitteen turvallinen hallinta SSL/TLS:n avulla

- [Varmenteen määrittäminen SSL/TLS- ja käytössä oleville protokollille](#)
- [WWW-pohjaisen hallinnan käyttö SSL/TLS:n avulla](#)
- [Itse allekirjoitetun varmenteen asentaminen Windows-käyttäjille järjestelmänvalvojan käyttöoikeuksilla](#)
- [Varmenteiden määrittäminen laitteen suojaukselle](#)

Varmenteen määrittäminen SSL/TLS- ja käytössä oleville protokollille

Määritä varmenne laitteelle käyttämällä WWW-pohjaista hallintaa, ennen kuin käytät SSL/TLS-tiedonsiirtoa.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Network (Verkko)** > **Protocol (Protokolla)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Valitse **HTTP Server Settings (HTTP-palvelinasetukset)**.
6. Valitse määritettävä varmenne **Select the Certificate (Valitse varmenne)** -pudotusluettelosta.
7. Valitse **Submit (Lähetä)**.
8. Käynnistä tulostuspalvelin napsauttamalla **Yes (Kyllä)**.



Aiheeseen liittyviä tietoja

- [Verkkolaitteen turvallinen hallinta SSL/TLS:n avulla](#)

Liittyvät aiheet:

- [Asiakirjojen SSL/TLS-suojattu tulostus](#)

WWW-pohjaisen hallinnan käyttö SSL/TLS:n avulla

Verkkolaitteen turvallinen hallinta edellyttää, että hallinta-apuohjelmia käytetään suojausprotokollien kanssa.



- HTTPS-protokollan käyttö edellyttää, että laitteessa on käytössä HTTPS. HTTPS-protokolla on oletusarvon mukaan käytössä.
- Voit muokata HTTPS-protokollan asetuksia WWW-pohjaisen hallinnan avulla.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Voit nyt käyttää tulostinta HTTPS-protokollalla.



Aiheeseen liittyviä tietoja

- [Verkkolaitteen turvallinen hallinta SSL/TLS:n avulla](#)

Itse allekirjoitetun varmenteen asentaminen Windows-käyttäjille järjestelmänvalvojan käyttöoikeuksilla

- Seuraavat vaiheet koskevat Microsoft Edge -selainta. Jos käytät toista verkkoselainta, katso verkkoselaimen asiakirjoista tai verkko-ohjeesta varmenteiden asennusohjeet.
- Varmista, että olet luonut itse allekirjoitetun varmenteen WWW-pohjaisen hallinnan avulla.

1. Napsauta kuvaketta **Microsoft Edge** hiiren kakkospainikkeella ja valitse sitten **Suorita järjestelmänvalvojana**.

Jos **Käyttäjätilien valvonta** -näyttö tulee näkyviin, valitse **Kyllä**.

2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.

https://192.168.1.2

Laitteen IP-osoite näkyy verkkoasetusraportissa.

3. Jos yhteytesi ei ole yksityinen, napsauta painiketta **Lisäasetukset** ja jatka sitten verkkosivulle.

4. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "Pwd". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

5. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **Certificate (Sertifikaatti)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

6. Valitse **Export (Vienti)**.

7. Jos haluat salata tiedoston, kirjoita salasana kenttään **Enter password (Syötä salasana)**. Jos **Enter password (Syötä salasana)** -kenttä on tyhjä, tiedostoa ei salata.

8. Kirjoita salasana uudelleen **Retype password (Anna salasana uudelleen)**-kenttään ja napsauta sitten **Submit (Lähetä)**.

9. Avaa ladattu tiedosto napsauttamalla sitä.

10. Kun **Ohjattu varmenteiden tuominen** -ikkuna tulee näkyviin, valitse **Seuraava**.

11. Napsauta **Seuraava**.

12. Kirjoita tarvittaessa salasana ja napsauta **Seuraava**.

13. Valitse **Sijoita kaikki varmenteet seuraavaan säilöön** ja **Selaa....**

14. Valitse **Luotetut varmenteiden päämyöntäjät** ja napsauta **OK**.

15. Napsauta **Seuraava**.

16. Napsauta **Valmis**.

17. Valitse **Kyllä**, jos tunnistetieto (allekirjoitus) on oikea.

18. Napsauta **OK**.



Aiheeseen liittyviä tietoja

- [Verkkolaitteen turvallinen hallinta SSL/TLS:n avulla](#)

Asiakirjojen SSL/TLS-suojattu tulostus

- Tulosta asiakirja käyttäen IPPS:ää
- Varmenteen määrittäminen SSL/TLS- ja käytössä oleville protokollille
- Varmenteiden määrittäminen laitteen suojaukselle

Tulosta asiakirja käyttäen IPPS:ää

Voit tulostaa asiakirjoja suojatusti IPP-protokollan avulla kautta käyttämällä IPPS-protokollaa.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Network (Verkko)** > **Protocol (Protokolla)**.



Jos vasen selauspalkki ei ole näkyvässä, aloita selaus kohdasta ☰.

5. Varmista, että **IPP**-valintaruutu on valittuna.



Jos **IPP**-valintaruutu ei ole valittuna, valitse **IPP**-valintaruutu ja napsauta **Submit (Lähetä)**.

Aktivoi määrytykset käynnistämällä laite uudelleen.

Kun laite käynnistyy uudelleen, palaa laitteen verkkosivulle, kirjoita salasana ja napsauta sitten vasemmanpuoleisessa siirtymispalkissa **Network (Verkko)** > **Network (Verkko)** > **Protocol (Protokolla)**.

6. Napsauta **HTTP Server Settings (HTTP-palvelinasetukset)**.
7. Valitse **HTTPS** -valintaruutu **IPP**-alueella ja napsauta **Submit (Lähetä)**.
8. Aktivoi määrytykset käynnistämällä laite uudelleen.

IPPS-protokollan käyttäminen tietoliikenteessä ei estä tulostuspalvelimen luvattonta käyttöä.



Aiheeseen liittyviä tietoja

- [Asiakirjojen SSL/TLS-suojattu tulostus](#)

SNMPv3:n käyttö

- [Verkkolaitteen hallinta suojatusti SNMPv3-protokollan avulla](#)

Verkkolaitteen hallinta suojatusti SNMPv3-protokollan avulla

Simple Network Management Protocol -versio 3 (SNMPv3) tarjoaa käyttäjän todennuksen ja tietojen salauksen verkon laitteiden suojattua hallintaa varten.

1. Käynnistä WWW-selain.
2. Kirjoita "https://yleinen nimi" selaimen osoitepalkkiin (missä "yleinen nimi" on varmenteelle määrittämäsi yleinen nimi, esimerkiksi IP-osoite, osoitteen nimi tai verkkoalueen nimi).
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko) > Network (Verkko) > Protocol (Protokolla)**.



Jos vasen selauspalkki ei ole näkyvässä, aloita selaus kohdasta ☰.

5. Varmista, että **SNMP**-asetus on käytössä, ja valitse sitten **Advanced Settings (Lisäasetukset)**.
6. Määritä SNMPv1/v2c-tilan asetukset.

Valinta	Kuvaus
SNMP v1/v2c read-write access (SNMP v1/v2c -luku-kirjoitus-käyttö)	Tulostuspalvelin käyttää SNMP-protokollan versioita 1 ja 2c. Tässä tilassa voit käyttää kaikkia laitteesi sovelluksia. Tila ei kuitenkaan ole suojattu, sillä käyttäjiä ei varmenneta eikä tietoja salata.
SNMP v1/v2c read-only access (SNMP v1/v2c, vain luku -käyttöoikeus)	Tulostuspalvelin käyttää SNMP-protokollan version 1 ja version 2c vain luku -käyttöoikeutta.
Disabled (Ei käytössä)	Poista SNMP-protokollan versio 1 ja 2c käytöstä. Kaikkien SNMPv1/v2c-protokollaa käyttävien sovellusten käyttö estetään. Jos haluat sallia SNMPv1/v2c-sovellusten käytön, käytä SNMP v1/v2c read-only access (SNMP v1/v2c, vain luku -käyttöoikeus) - tai SNMP v1/v2c read-write access (SNMP v1/v2c -luku-kirjoitus-käyttö) -tilaa.

7. Määritä SNMPv3-tilan asetukset.

Valinta	Kuvaus
Enabled (Käytössä)	Tulostuspalvelin käyttää SNMP-protokollan versiota 3. Jos haluat hallita tulostuspalvelinta turvallisesti, käytä SNMPv3-tilaa ja määritä sitten asetukset.
Disabled (Ei käytössä)	Poista SNMP-protokollan versio 3 käytöstä. Kaikkien SNMPv3-protokollaa käyttävien sovellusten käyttö estetään. Jos haluat sallia SNMPv3-sovellusten käytön, käytä SNMPv3-tilaa.

8. Valitse **Submit (Lähetä)**.



Jos laitteesi näyttää protokollan asetusvaihtoehdot, valitse haluamasi vaihtoehdot.

9. Aktivoi määritykset käynnistämällä laite uudelleen.



Aiheeseen liittyviä tietoja

- [SNMPv3:n käyttö](#)

IEEE 802.1x -verkkotodennuksen käyttö

- [Mitä on IEEE 802.1x -todennus?](#)
- [IEEE 802.1x -todennuksen määrittäminen verkolle WWW-pohjaisen hallinnan avulla \(verkkoselaimella\)](#)
- [IEEE 802.1x -todennusmenetelmät](#)

Mitä on IEEE 802.1x -todennus?

IEEE 802.1x on IEEE-standardi, joka rajoittaa valtuuttamattomien verkkolaitteiden yhteyksiä. Brother-laitteesi lähettää todennuspyynnön RADIUS-palvelimelle (todennuspalvelimelle) tukiaseman tai keskittimen kautta. Kun RADIUS-palvelin on varmistanut pyyntösi, laitteesi voi muodostaa yhteyden verkkoon.



Aiheeseen liittyviä tietoja

- [IEEE 802.1x -verkkotodennuksen käyttö](#)
-

IEEE 802.1x -todennuksen määrittäminen verkolle WWW-pohjaisen hallinnan avulla (verkkoselaimella)

- Jos määrität laitteesi EAP-TLS-todennuksella, CA:n myöntämä asiakassertifikaatti on asennettava ennen määrittämisen aloittamista. Pyydä asiakassertifikaattia verkonvalvojalta. Jos olet asentanut useamman kuin yhden sertifikaatin, suosittelemme, että kirjoitat käyttämäsi sertifikaatin nimen muistiin.
- Ennen kuin tarkistat palvelinvarmenteen, sinun on tuotava CA-varmenne, jonka palvelinvarmenteen allekirjoittanut CA on myöntänyt. Ota yhteys verkonvalvojaan tai Internet-palveluntarjoajaan (ISP) varmistaaksesi, onko CA-varmenteen tuonti välttämätöntä.



Voit määrittää myös IEEE 802.1x -todennuksen käyttämällä langattoman verkon ohjattua asennusta ohjauspaneelista (langaton verkko).

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoiteriville "https://laitteen IP-osoite" (jossa "laitteen IP-osoite" on laitteen IP-osoite).
esim.
https://192.168.1.2
Laitteen IP-osoite näkyy verkkoasetusraportissa.
3. Kirjoita tarvittaessa salasana **Login (Sisäänkirjaus)**-kenttään ja napsauta sitten **Login (Sisäänkirjaus)**.



Tämän laitteen asetusten hallinnan oletussalasana sijaitsee laitteen takaosassa tai pohjassa, ja sen yhteydessä on merkintä "**Pwd**". Vaihda oletussalasana noudattamalla näytössä näkyviä ohjeita, kun kirjaudut sisään ensimmäisen kerran.

4. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)**.



Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.

5. Tee jokin seuraavista:
 - Kiinteä verkko
Napsauta **Wired (Kiinteä) > Wired 802.1x Authentication (Kiinteän verkon 802.1x-todennus)**-painiketta.
 - Langaton verkko
Napsauta **Wireless (Langaton) > Wireless (Enterprise) (Langaton (yritys))**-painiketta.
6. Määritä IEEE 802.1x -todennusasetukset.



- Jos haluat ottaa IEEE 802.1x -todennuksen käyttöön lankaverkossa, valitse **Enabled (Käytössä)** -sivulla **Wired 802.1x status (Langallisen 802.1x-yhteyden tila)** -asetukseksi **Wired 802.1x Authentication (Kiinteän verkon 802.1x-todennus)**.
- Jos käytetään **EAP-TLS**-todennusta on valittava asiakasvarmenne, joka on asennettu (näytetään varmenteen nimen kanssa) vahvistusta varten **Client Certificate (Asiakasvarmenne)** -pudotusluettelosta.
- Jos valitset **EAP-FAST**, **PEAP**, **EAP-TTLS**, tai **EAP-TLS** -todennuksen, voit valita vahvistustavan **Server Certificate Verification (Palvelinvarmenteen varmistus)** -pudotusluettelosta. Vahvista palvelimen varmenne laitteeseen etukäteen tuodun CA-varmenteen avulla, jonka on myöntänyt palvelinvarmenteen allekirjoittanut CA.

Voit valita jonkin seuraavista vahvistustavoista **Server Certificate Verification (Palvelinvarmenteen varmistus)** -pudotusluettelosta:

Valinta	Kuvaus
No Verification (Ei varmistusta)	Palvelinvarmenteeseen voidaan aina luottaa. Vahvistusta ei suoriteta.
CA Cert. (CA-varmenne)	Vahvistustapa, jolla tarkistetaan palvelinvarmenteen CA-luotettavuus CA-varmenteen avulla, jonka on myöntänyt palvelinvarmenteen allekirjoittanut CA.
CA Cert. + ServerID (CA-varmenne ja palvelimen tunnus)	Vahvistusmenetelmä, jolla tarkistetaan palvelinvarmenteen ¹ yleisen nimen arvo sekä CA-luotettavuus.

7. Kun olet valmis, napsauta **Submit (Lähetä)**.

Kiinteä verkko: Kun olet tehnyt asetukset, yhdistä laitteesi IEEE 802.1x -yhteensopivaan verkkoon. Muutaman minuutin kuluttua voit tulostaa verkkomäärittäysraportin tarkistaaksesi <**Wired IEEE 802.1x**> -tilan.

Valinta	Kuvaus
Success	Kiinteän verkon IEEE 802.1x -toiminto on nyt käytössä ja todennus onnistui.
Failed	Kiinteän verkon IEEE 802.1x -toiminto on nyt käytössä, mutta todennus epäonnistui.
Off	Kiinteän verkon IEEE 802.1x -toiminto ei ole käytössä.



Aiheeseen liittyviä tietoja

- [IEEE 802.1x -verkkotodennuksen käyttö](#)

Liittyvät aiheet:

- [Suojausvarmenteen ominaisuuksien yleiskuvaus](#)
- [Varmenteiden määrittäminen laitteen suojaukselle](#)

¹ Yleisen nimen vahvistus vertaa palvelinvarmenteen yleistä nimeä **Server ID (Palvelimen tunnus)**lle määritettyyn merkkijonoon. Ennen kuin käytät tätä menetelmää, kysy järjestelmänvalvojalta lisätietoja palvelinvarmenteen yleisestä nimestä ja määritä sitten **Server ID (Palvelimen tunnus)**.

IEEE 802.1x -todennusmenetelmät

EAP-FAST

EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secured Tunnel) on Cisco Systems, Inc.:n kehittämä protokolla, jossa todennus tapahtuu käyttäjätunnuksen ja salasanan avulla ja jossa käytetään symmetristä avainalgoritmia tunneloidun käyttäjätunnistuksen saavuttamiseksi.

Brother-laite tukee seuraavia sisäisiä todennusmenetelmiä:

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

EAP-MD5 (Kiinteä verkko)

EAP-MD5 (Extensible Authentication Protocol Message Digest Algorithm 5) -protokollassa käytetään käyttäjätunnusta ja salasanaa kysymys-vastaus-todennukseen.

PEAP

Protected Extensible Authentication Protocol (PEAP) on EAP-menetelmän versio, jonka ovat kehittäneet Cisco Systems, Inc., Microsoft Corporation ja RSA Security. PEAP luo salatun SSL (Secure Sockets Layer)/TLS (Transport Layer Security) -tunnelin asiakkaan ja todennuspalvelimen välille. Tunnelia käytetään käyttäjätunnuksen ja salasanan lähetykseen. PEAP luo keskinäisen todennuksen palvelimen ja asiakkaan välille.

Brother-laite tukee seuraavia sisäisiä todennusmenetelmiä:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) -protokollan ovat kehittäneet Funk Software ja Certicom. EAP-TTLS luo samanlaisen salatun SSL-tunnelin asiakkaan ja todennuspalvelimen väliin käyttäjätunnuksen ja salasanan lähettämistä varten kuin PEAP. EAP-TTLS tuottaa kaksisuuntaisen todennuksen palvelimen ja asiakkaan välille.

Brother-laite tukee seuraavia sisäisiä todennusmenetelmiä:

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

EAP-TLS

EAP-TLS (Extensible Authentication Protocol Transport Layer Security) vaatii digitaalisen sertifikaatin todennuksen sekä asiakkaalta että todennuspalvelimelta.



Aiheeseen liittyviä tietoja

- [IEEE 802.1x -verkkotodennuksen käyttö](#)