Tietoturvaopas

Sisällysluettelo

Johdanto

Kuvakkeiden selitykset

Tässä Käyttöoppaassa käytetään seuraavia symboleita ja käytäntöjä:

TÄRKEÄÄ	TÄRKEÄÄ ilmaisee vaaratilanteen, joka saattaa aiheuttaa aineellisia vahinkoja tai laitteen toiminnallisuuden heikkenemistä, jos tilannetta ei vältetä.
HUOMAUTUS	HUOMAUTUS määrittää käyttöympäristön, asennusolosuhteet tai erityiset käyttöolosuhteet.
	Käyttövinkkikuvakkeet tarkoittavat hyödyllisiä ohjeita ja lisätietoja.
Lihavoitu teksti	Lihavoitu tekstityyli tarkoittaa laitteen ohjauspaneelin tai tietokoneen näyttöruudun painikkeita.
Kursivoitu teksti	Italicized tekstityylillä emphasizes tärkeää kohtaa tai sillä viitataan asiaan liittyvään toiseen aiheeseen.

Aiheeseen liittyviä tietoja

- Johdanto

Tavaramerkit

Adobe® ja Reader® ovat Adobe Systems Incorporated -yhtiön rekisteröityjä tavaramerkkejä tai tavaramerkkejä Yhdysvalloissa ja/tai muissa maissa.

Kullakin yrityksellä, jonka ohjelmiston nimi mainitaan tässä oppaassa, on omia ohjelmiaan koskeva Licensesopimus.

Brotherin tuotteissa, liittyvissä tavaramerkeissä ja muussa materiaalissa olevat yritysten tavaramerkit ja tuotteiden nimet ovat kaikki kyseisten yritysten tavaramerkkejä tai rekisteröityjä tavaramerkkejä.

Aiheeseen liittyviä tietoja

- Johdanto

Tekijänoikeustiedot

Tämän asiakirjan tietoja voidaan muuttaa ilman erillistä ilmoitusta. Tässä asiakirjassa kuvattu ohjelmisto toimitetaan lisenssisopimusten alaisena. Ohjelmistoa saa käyttää tai kopioida vain näiden sopimusten ehtojen mukaisesti. Mitään tämän julkaisun osaa ei saa jäljentää missään muodossa tai millään tavalla ilman Brother Industries, Ltd:n etukäteen myöntämää kirjallista lupaa.

Aiheeseen liittyviä tietoja

- Johdanto

Ennen verkkosuojaustoimintojen käyttöä

Laitteessa käytetään joitakin uusimmista käytettävissä olevista verkkosuojaus- ja salausprotokollista. Nämä verkkotoiminnot voidaan yhdistää yleisiin verkkosuojaustoimintoihin. Ne auttavat tietojen suojauksessa ja laitteen unauthorized käytön estämisessä.

Suosittelemme FTP- ja TFTP-protokollien poistamista käytöstä. Laitteen käyttö näillä protokollilla ei ole suojattua.

Aiheeseen liittyviä tietoja

- Johdanto
  - Tarpeettomien protokollien poistaminen käytöstä

Tarpeettomien protokollien poistaminen käytöstä

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. Poista tarpeettomat protokollat käytöstä poistamalla valinnat vastaavista valintaruuduista.
6. Napsauta **Submit (Lähetä)**.
7. Ota asetukset käyttöön käynnistämällä Brother-laite uudelleen.

Aiheeseen liittyviä tietoja

- Ennen verkkosuojaustoimintojen käyttöä

Verkon suojaus

- Varmenteiden määritys laitteen suojaukselle
- SSL/TLS:n käyttö
- SNMPv3:n käyttö
- IPsec-protokollan käyttö
- IEEE 802.1x -verkkotodennuksen käyttö

Varmenteiden määritys laitteen suojaukselle

Verkotetun laitteen turvallista hallintaa varten SSL/TLS:n avulla on määritettävä varmenne. Varmenteen määritykseen 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 suojausvarmenteen 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 varmenteen avulla voit käyttää SSL/TLS-tiedonsiirtoa luomatta tai asentamatta eri varmennetta.

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

- Itseallekirjoitettu varmenne

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

- Varmentajan (CA) myöntämä varmenne

  CA:lta saadun varmenteen 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 varmenteen ja yksityisen avaimen tulostuspalvelimen palautuksen jälkeen, vie ne ennen palauttamista ja asenna ne uudelleen.

Aiheeseen liittyviä tietoja

- Varmenteiden määritys 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 määritys 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 näkyvissä, 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 näkyvissä.
   - 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 määritys laitteen suojaukselle

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 näkyvissä, 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 tunniste, kuten IP-osoite tai solmun tai toimialueen nimi, kun muodostat laitteeseen SSL/TLS-yhteyden. Solmun nimi on oletusarvoisesti näkyvissä. **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 kaksimerkkinen, 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:llesi.
    - 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 viedään 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 näkyvissä, 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 määritys 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 määritys SSL/TLS- ja käytössä oleville protokollille
- Varmenteiden määritys 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 näkyvissä, aloita selaus kohdasta ≡.
5. Varmista, että **IPP**-valintaruutu on valittuna.

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

   Aktivoi määritykset 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(Port 443) (HTTPS (portti 443))** -valintaruutu **IPP**-alueella ja napsauta **Submit (Lähetä)**.
8. Aktivoi määritykset käynnistämällä laite uudelleen.

IPPS-protokollan käyttäminen tietoliikenteessä ei estä tulostuspalvelimen unauthorized 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 näkyvissä, 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. Voit hallita tulostuspalvelinta suojatusti käyttämällä SNMPv3-tilaa.
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

IPsec-protokollan käyttö

Johdanto IPSec-suojausprotokollaan

IPsec (Internet Protocol Security) on suojausprotokolla, joka käyttää valinnaista internetprotokollatoimintoa tietojen manipuloinnin estämiseen ja IP-paketteina lähetettyjen tietojen luottamuksellisuuden varmistamiseen. IPsec salaa verkon kautta kuljetettuja tietoja, kuten esimerkiksi tietokoneelta tulostimeen lähetettyjä tietoja. Tiedot salataan verkkotasolla, joten korkeampitasoisia protokollia hyödyntävät sovellukset käyttävät IPsec-protokollaa, vaikka käyttäjä ei tietäisi tästä.

IPsec tukee seuraavia toimintoja:

- IPsec-lähetykset

  IPsec-asetusehtojen mukaan verkkoon liitetty tietokone lähettää tietoja määritetylle laitteelle ja vastaanottaa siltä tietoja IPsec-protokollapakettia käyttäen. Kun laitteet alkavat viestiä IPsec-protokollapakettia käyttäen, ne vaihtavat avaimia käyttämällä ensin Internet Key Exchange (IKE) -menetelmää, minkä jälkeen salatut tiedot lähetetään avaimia käyttäen.

  Lisäksi IPsec-protokollalla on kaksi toimintatilaa: siirtotila ja tunnelitila. Siirtotilaa käytetään pääasiassa laitteiden väliseen tiedonsiirtoon ja tunnelitilaa käytetään verkkoympäristöissä, kuten VPN (Virtual Private Network) -verkossa.

Seuraavat ehdot ovat välttämättömiä IPsec-tiedonsiirron osalta:

- Tietokone, joka pystyy käyttämään IPsec-protokollaa, on yhdistetty verkkoon.
- Laitteesi on määritetty käyttämään IPsec-tiedonsiirtoa.
- Laitteeseesi yhdistetty tietokone on määritetty käyttämään IPsec-yhteyksiä.

- IPsec-asetukset

  IPsec-protokollaa käyttävien yhteyksien vaatimat asetukset. Nämä asetukset voidaan määrittää WWW-pohjaisen hallinnan avulla.

IPsec-asetusten määrittäminen edellyttää, että selainta käytetään verkkoon yhdistetyllä tietokoneella.

Aiheeseen liittyviä tietoja

- IPsec-protokollan käyttö

IPsecin määrittäminen WWW-pohjaisen hallinnan avulla

IPsec-yhteyden ehdot koostuvat kahdesta **Template (Malli)**-tyypistä: **Address (osoite)** ja **IPsec**. Voit määrittää enintään 10 yhteysehtoa.

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)** > **IPsec**.

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

Valinta	Kuvaus
Status (Tila)	Ota tai poista IPsec käytöstä.
Negotiation Mode (Neuvottelutila)	Valitse **Negotiation Mode (Neuvottelutila)** IKE Phase 1:lle. IKE on protokolla, jonka avulla voidaan vaihtaa salausavaimia salatun tietoliikenteen käyttämiseksi IPsec-protokollan avulla. **Main (Päätila)** -tilassa käsittelynopeus on hidas, mutta suojaustaso korkea. **Aggressive (Aggressiivinen tila)** -tilassa käsittelynopeus on nopeampi kuin **Main (Päätila)** -tilassa, mutta suojaustaso on alempi.
All Non-IPsec Traffic (Muu kuin IPsec-liikenne)	Valitse muiden kuin IPsec-pakettien kohdalla käytettävä toimenpide. Web Services -protokollaa käytettäessä on valittava **Allow (Salli)** toiminnolle **All Non-IPsec Traffic (Muu kuin IPsec-liikenne)**. Web Services -protokollaa ei voi käyttää, jos valitset **Drop (Pudota)**-valinnan.
Broadcast/Multicast Bypass (Lähetys/multicast-ohitus)	Valitse **Enabled (Käytössä)** tai **Disabled (Ei käytössä)**.
Protocol Bypass (Protokollan ohitus)	Valitse haluamiesi asetusten valintaruudut.
Rules (Säännöt)	Aktivoi malli valitsemalla **Enabled (Käytössä)** -valintaruutu. Jos valitset useita valintaruutuja, pienemmillä luvuilla numeroidut valintaruudut ovat etusijalla, mikäli valintaruutujen asetukset ovat ristiriidassa. Napsauta sen **Address Template (Osoitemalli)** -asetuksen pudotusluetteloa, jota käytetään IPsec-yhteysolosuhteisiin. Napsauta **Add Template (Lisää malli)** lisätäksesi **Address Template (Osoitemalli)**n. Napsauta sen **IPsec Template (IPsec-malli)** -asetuksen pudotusluetteloa, jota käytetään IPsec-yhteysolosuhteisiin. Napsauta **Add Template (Lisää malli)** lisätäksesi **IPsec Template (IPsec-malli)**n.

6. Valitse **Submit (Lähetä)**.

   Jos asetusten käyttöönotto edellyttää laitteen käynnistämistä uudelleen, uudelleenkäynnistyksen vahvistusikkuna ilmestyy näytölle.

   Jos **Rules (Säännöt)** -taulukossa käyttöön ottamassasi mallissa on tyhjä kohde, näyttöön tulee virhesanoma. Vahvista valintasi ja valitse **Submit (Lähetä)** uudelleen.

Aiheeseen liittyviä tietoja

- IPsec-protokollan käyttö

Liittyvät aiheet:

- Varmenteiden määritys laitteen suojaukselle

IPsec-osoitemallin määrittäminen 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. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **IPsec Address Template (IPsec-osoitemalli)**.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.
5. Voit poistaa **Delete (Poista)** napsauttamalla **Address Template (Osoitemalli)** -painiketta. Jos **Address Template (Osoitemalli)** on käytössä, sitä ei voi poistaa.
6. Napsauta **Address Template (Osoitemalli)**a, jonka haluat luoda. **IPsec Address Template (IPsec-osoitemalli)** ilmestyy näytölle.
7. Määritä asetukset.

Valinta	Kuvaus
Template Name (Mallin nimi)	Anna mallin nimi (enintään 16 merkkiä).
Local IP Address (Paikallinen IP-osoite)	• **IP Address (IP-osoite)** Määritä IP-osoite. Valitse pudotusluettelosta **ALL IPv4 Address (Kaikki IPv4-osoitteet)**, **ALL IPv6 Address (Kaikki IPv6-osoitteet)**, **ALL Link Local IPv6 (Kaikki yhdistetyt paikalliset IPv6-osoitteet)** tai **Custom (Mukautettu)**. Jos valitset pudotusluettelosta valinnan **Custom (Mukautettu)**, syötä IP-osoite (IPv4 tai IPv6) tekstiruutuun. • **IP Address Range (IP-osoitealue)** Kirjoita IP-alueen aloittava ja lopettava IP-osoite tekstiruutuihin. Jos alueen aloittava ja lopettava IP-osoite eivät ole IPv4- tai IPv6-muotoon standardized tai jos lopettava IP-osoite on lyhyempi kuin aloittava osoite, seurauksena on virhe. • **IP Address / Prefix (IP-osoite/-etuliite)** Määritä IP-osoite CIDR-mallin mukaisesti. Esimerkiksi 192.168.1.1/24 Koska etuliite on määritetty 24-bittisen aliverkon peitteen (255.255.255.0) muodossa osoitteelle 192.168.1.1, osoitteet 192.168.1.### ovat kelvollisia.
Remote IP Address (IP-etäosoite)	• **Any (Mikä tahansa)** Jos valitset **Any (Mikä tahansa)**, kaikki IP-osoitteet ovat käytössä. • **IP Address (IP-osoite)** Kirjoita IP-osoite (IPv4 tai IPv6) tekstiruutuun. • **IP Address Range (IP-osoitealue)**

Valinta	Kuvaus
	Kirjoita IP-alueen ensimmäinen ja viimeinen IP-osoite. Jos alueen ensimmäinen ja viimeinen IP-osoite eivät ole IPv4- tai IPv6-muotoon standardized tai jos viimeinen IP-osoite on pienempi kuin ensimmäinen osoite, seurauksena on virhe. • **IP Address / Prefix (IP-osoite/-etuliite)** Määritä IP-osoite CIDR-mallin mukaisesti. Esimerkiksi 192.168.1.1/24 Koska etuliite on määritetty 24-bittisen aliverkon peitteen (255.255.255.0) muodossa osoitteelle 192.168.1.1, osoitteet 192.168.1.### ovat kelvollisia.

8. Napsauta **Submit (Lähetä)**.

Jos muutat käytössä olevan mallin asetuksia, määritysten aktivointi edellyttää laitteen käynnistämistä uudelleen.

Aiheeseen liittyviä tietoja

- IPsec-protokollan käyttö

IPsec-mallin määrittäminen 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. Napsauta vasemmassa siirtymispalkissa **Network (Verkko)** > **Security (Suojaus)** > **IPsec Template (IPsec-malli)**.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ≡.
5. Voit poistaa **Delete (Poista)** napsauttamalla **IPsec Template (IPsec-malli)** -painiketta. Jos **IPsec Template (IPsec-malli)** on käytössä, sitä ei voi poistaa.
6. Napsauta kohdetta **IPsec Template (IPsec-malli)**, jonka haluat luoda. **IPsec Template (IPsec-malli)**-näyttö avautuu. Määrityskentät vaihtelevat valitsemasi **Use Prefixed Template (Käytä esimääritettyä mallia)**- ja **Internet Key Exchange (IKE)** -asetusten mukaan.
7. Kirjoita mallille nimi **Template Name (Mallin nimi)** -kenttään (enintään 16 merkkiä).
8. Jos valitset **Custom (Mukautettu) Use Prefixed Template (Käytä esimääritettyä mallia)** -pudotusluettelosta, valitse **Internet Key Exchange (IKE)** -valinnat ja muokkaa asetuksia tarpeen mukaan.
9. Napsauta **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- IPsec-protokollan käyttö
  - IKEv1-asetukset IPsec-mallille
  - IKEv2-asetukset IPsec-mallille
  - Manuaaliset asetukset IPsec-mallille

IKEv1-asetukset IPsec-mallille

Valinta	Kuvaus
Template Name (Mallin nimi)	Kirjoita mallin nimi (enintään 16 merkkiä).
Use Prefixed Template (Käytä esimääritettyä mallia)	Valitse **Custom (Mukautettu)**, **IKEv1 High Security (IKEv1 Korkea suojaus)** tai **IKEv1 Medium Security (IKEv1 Keskitason suojaus)**. Asetukset vaihtelevat valitun mallin mukaan.
Internet Key Exchange (IKE)	IKE on protokolla, jonka avulla voidaan vaihtaa salausavaimia salatun tietoliikenteen käyttämiseksi IPsec-protokollan avulla. Kertaluontoisen salatun tiedonsiirron mahdollistamiseksi protokolla määrittää IPsec-protokollan vaatiman salausalgoritmin ja jakaa salausavaimet. IKE-protokollan salausavaimet vaihdetaan Diffie-Hellman-menetelmän avulla ja IKE-protokollalle rajattu, salattu tiedonsiirto voidaan suorittaa. Jos valitsit **Custom (Mukautettu)** kohdassa **Use Prefixed Template (Käytä esimääritettyä mallia)**, valitse **IKEv1**.
Authentication Type (Todennustyyppi)	• **Diffie-Hellman Group** Tämä avaintenvaihtomenetelmä mahdollistaa salaisten avainten vaihdon turvallisesti suojaamattoman verkon yli. Diffie-Hellman-avaintenvaihtomenetelmä käyttää erillistä logaritmiongelmaa (ei salaista avainta) satunnaisella numerolla ja salaisella avaimella luotujen, avoimien tietojen lähettämiseen ja vastaanottamiseen. Valitse **Group1 (Ryhmä 1)**, **Group2 (Ryhmä 2)**, **Group5 (Ryhmä 5)** tai **Group14 (Ryhmä 14)**. • **Encryption (Salaus)** Valitse **DES**, **3DES**, **AES-CBC 128** tai **AES-CBC 256**. • **Hash (Haja-arvo)** Valitse **MD5**, **SHA1**, **SHA256**, **SHA384** tai **SHA512**. • **SA Lifetime (SA-käyttöikä)** Määritä IKE SA -kestoaika. Anna aika (sekunteina) ja kilotavujen (kb) määrä.
Encapsulating Security (Kapselointisuojaus)	• **Protocol (Protokolla)** Valitse **ESP**, **AH** tai **AH+ESP**. - ESP on protokolla, jolla suoritetaan salattu tiedonsiirto IPsec-iä käyttäen. ESP salaa nettotiedot (siirretyn sisällön) ja lisää lisätietoja. IP-paketti koostuu otsakkeesta ja salatuista nettotiedoista, jotka seuraavat otsaketta. Salattujen tietojen lisäksi IP-paketti sisältää myös salausmenetelmää ja salausavainta koskevia tietoja, todennustietoja jne. - AH on osa IPsec-protokollaa, joka todentaa lähettäjän ja ehkäisee tietojen manipulointia (varmistaen tietojen eheyden). IP-paketissa tiedot sijaitsevat välittömästi otsikon perässä. Lisäksi paketit sisältävät haja-arvoja, jotka lasketaan siirretystä sisällöstä, salaisesta avaimesta, jne. koostuvalla kaavalla ehkäisten lähettäjän väärentämistä tai tietojen manipulointia. ESP:stä poiketen siirrettyä sisältöä ei salata ja tiedot lähetetään ja vastaanotetaan tavallisena tekstinä. • **Encryption (Salaus) (Ei käytettävissä, kun käytössä on AH.)** Valitse **DES**, **3DES**, **AES-CBC 128** tai **AES-CBC 256**. • **Hash (Haja-arvo)** valitse **None (Ei mitään)**, **MD5**, **SHA1**, **SHA256**, **SHA384**, tai **SHA512**. **None (Ei mitään)** voidaan valita ainoastaan silloin, kun **ESP** on valittu kohdassa **Protocol (Protokolla)**.

Valinta	Kuvaus
	• **SA Lifetime (SA-käyttöikä)** Määritä IKE SA -käyttöikä. Syötä aika (sekunteja) ja kilotavujen määrä (KByte). • **Encapsulation Mode (Kapselointitila)** Valitse **Transport (Siirto)** tai **Tunnel (Tunneli)**. • **Remote Router IP-Address (Etäreitittimen IP-osoite)** Syötä etäreitittimen IP-osoite (IPv4 tai IPv6). Syötä tiedot ainoastaan **Tunnel (Tunneli)** -tilan ollessa valittuna. SA (Security Association) on IPsec- tai IPv6-pohjainen salattu tiedonsiirtomenetelmä, joka vaihtaa ja jakaa tietoa, kuten salausmenetelmän ja salausavaimen, suojatun tiedonsiirtokanavan luomiseksi ennen tiedonsiirron aloittamista. SA voi myös viitata luotuun, virtuaaliseen suojattuun tiedonsiirtokanavaan. IPsec-protokollaan käytetty SA luo salausmenetelmän, vaihtaa avaimet ja suorittaa kahdenkeskeisen todennuksen IKE (Internet Key Exchange) -vakioprotokollan avulla. Lisäksi SA-menetelmää päivitetään ajoittain.
Perfect Forward Secrecy (PFS)	PFS ei johda avaimia aiemmista viestien salaukseen käytetyistä avaimista. Tämän lisäksi, jos viestin salaamiseen käytetty avain johdettiin pääavaimesta, kyseistä pääavainta ei käytetä muiden avainten johtamiseen. Tästä johtuen, mikäli avaimen luottamuksellisuus vaarantuu, mahdolliset vahingot rajoittuvat vain kyseisellä avaimella salattuihin viesteihin. Valitse **Enabled (Käytössä)** tai **Disabled (Ei käytössä)**.
Authentication Method (Todennusmenetelmä)	Valitse todennusmenetelmä. Valitse **Pre-Shared Key (Esijaettu avain)** tai **Certificates (Varmenteet)**.
Pre-Shared Key (Esijaettu avain)	Tiedonsiirtoa salattaessa salausavain vaihdetaan ja jaetaan etukäteen toista kanavaa käyttäen. Jos valitset **Authentication Method (Todennusmenetelmä)** -tyypiksi **Pre-Shared Key (Esijaettu avain)**, kirjoita **Pre-Shared Key (Esijaettu avain)** (enintään 32 merkkiä). • **Local/ID Type/ID (Lähettäjä/Tunnistetyyppi/Tunniste)** Valitse lähettäjän tunnustyyppi ja kirjoita tunnus. Valitse tyypiksi **IPv4 Address (IPv4-osoite)**, **IPv6 Address (IPv6-osoite)**, **FQDN**, **E-mail Address (Sähköpostiosoite)** tai **Certificate (Sertifikaatti)**. Jos valitset **Certificate (Sertifikaatti)**, syötä varmenteen yleinen nimi **ID (Tunniste)**-kenttään. • **Remote/ID Type/ID (Vastaanottaja/Tunnistetyyppi/Tunniste)** Valitse vastaanottajan tunnustyyppi ja kirjoita tunnus. Valitse tyypiksi **IPv4 Address (IPv4-osoite)**, **IPv6 Address (IPv6-osoite)**, **FQDN**, **E-mail Address (Sähköpostiosoite)** tai **Certificate (Sertifikaatti)**. Jos valitset **Certificate (Sertifikaatti)**, syötä varmenteen yleinen nimi **ID (Tunniste)**-kenttään.
Certificate (Sertifikaatti)	Jos valitsit **Certificates (Varmenteet)** kohdassa **Authentication Method (Todennusmenetelmä)**, valitse varmenne. Voit valita ainoastaan WWW-pohjaisen hallinnan suojausmääritysnäytön **Certificate (Sertifikaatti)** -sivulla luotuja varmenteita.

Aiheeseen liittyviä tietoja

- IPsec-mallin määrittäminen WWW-pohjaisen hallinnan avulla

IKEv2-asetukset IPsec-mallille

Valinta	Kuvaus
Template Name (Mallin nimi)	Kirjoita mallin nimi (enintään 16 merkkiä).
Use Prefixed Template (Käytä esimääritettyä mallia)	Valitse **Custom (Mukautettu)**, **IKEv2 High Security (IKEv2 Korkea suojaus)** tai **IKEv2 Medium Security (IKEv2 Keskitason suojaus)**. Asetukset vaihtelevat valitun mallin mukaan.
Internet Key Exchange (IKE)	IKE on protokolla, jonka avulla voidaan vaihtaa salausavaimia salatun tietoliikenteen käyttämiseksi IPsec-protokollan avulla. Kertaluontoisen salatun tiedonsiirron mahdollistamiseksi protokolla määrittää IPsec-protokollan vaatiman salausalgoritmin ja jakaa salausavaimet. IKE-protokollan salausavaimet vaihdetaan Diffie-Hellman-menetelmän avulla ja IKE-protokollalle rajattu, salattu tiedonsiirto voidaan suorittaa. Jos valitsit **Custom (Mukautettu)** kohdassa **Use Prefixed Template (Käytä esimääritettyä mallia)**, valitse **IKEv2**.
Authentication Type (Todennustyyppi)	• **Diffie-Hellman Group** Tämä avaintenvaihtomenetelmä mahdollistaa salaisten avainten vaihdon turvallisesti suojaamattoman verkon yli. Diffie-Hellman-avaintenvaihtomenetelmä käyttää erillistä logaritmiongelmaa (ei salaista avainta) satunnaisella numerolla ja salaisella avaimella luotujen, avoimien tietojen lähettämiseen ja vastaanottamiseen. Valitse **Group1 (Ryhmä 1)**, **Group2 (Ryhmä 2)**, **Group5 (Ryhmä 5)** tai **Group14 (Ryhmä 14)**. • **Encryption (Salaus)** Valitse **DES**, **3DES**, **AES-CBC 128** tai **AES-CBC 256**. • **Hash (Haja-arvo)** Valitse **MD5**, **SHA1**, **SHA256**, **SHA384** tai **SHA512**. • **SA Lifetime (SA-käyttöikä)** Määritä IKE SA -kestoaika. Anna aika (sekunteina) ja kilotavujen (kb) määrä.
Encapsulating Security (Kapselointisuojaus)	• **Protocol (Protokolla)** Valitse **ESP**. ESP on protokolla, jolla suoritetaan salattu tiedonsiirto IPseciä käyttäen. ESP salaa nettotiedot (siirretyn sisällön) ja lisää lisätietoja. IP-paketti koostuu otsakkeesta ja salatuista nettotiedoista, jotka seuraavat otsaketta. Salattujen tietojen lisäksi IP-paketti sisältää myös salausmenetelmää ja salausavainta koskevia tietoja, todennustietoja jne. • **Encryption (Salaus)** Valitse **DES**, **3DES**, **AES-CBC 128** tai **AES-CBC 256**. • **Hash (Haja-arvo)** Valitse **MD5**, **SHA1**, **SHA256**, **SHA384** tai **SHA512**. • **SA Lifetime (SA-käyttöikä)** Määritä IKE SA -käyttöikä. Syötä aika (sekunteja) ja kilotavujen määrä (KByte). • **Encapsulation Mode (Kapselointitila)** Valitse **Transport (Siirto)** tai **Tunnel (Tunneli)**. • **Remote Router IP-Address (Etäreitittimen IP-osoite)** Syötä etäreitittimen IP-osoite (IPv4 tai IPv6). Syötä tiedot ainoastaan **Tunnel (Tunneli)** -tilan ollessa valittuna.

Valinta	Kuvaus
	SA (Security Association) on IPsec- tai IPv6-pohjainen salattu tiedonsiirtomenetelmä, joka vaihtaa ja jakaa tietoa, kuten salausmenetelmän ja salausavaimen, suojatun tiedonsiirtokanavan luomiseksi ennen tiedonsiirron aloittamista. SA voi myös viitata luotuun, virtuaaliseen suojattuun tiedonsiirtokanavaan. IPsec-protokollaan käytetty SA luo salausmenetelmän, vaihtaa avaimet ja suorittaa kahdenkeskeisen todennuksen IKE (Internet Key Exchange) -vakioprotokollan avulla. Lisäksi SA-menetelmää päivitetään ajoittain.
Perfect Forward Secrecy (PFS)	PFS ei johda avaimia aiemmista viestien salaukseen käytetyistä avaimista. Tämän lisäksi, jos viestin salaamiseen käytetty avain johdettiin pääavaimesta, kyseistä pääavainta ei käytetä muiden avainten johtamiseen. Tästä johtuen, mikäli avaimen luottamuksellisuus vaarantuu, mahdolliset vahingot rajoittuvat vain kyseisellä avaimella salattuihin viesteihin. Valitse **Enabled (Käytössä)** tai **Disabled (Ei käytössä)**.
Authentication Method (Todennusmenetelmä)	Valitse todennusmenetelmä. Valitse **Pre-Shared Key (Esijaettu avain)**, **Certificates (Varmenteet)**, **EAP - MD5** tai **EAP - MS-CHAPv2**. EAP on todennusprotokolla, joka on PPP:n laajennus. EAP:n käyttö yhdessä IEEE802.1x-standardin kanssa mahdollistaa eri avaimen käytön käyttäjän todennukseen jokaisen istunnon aikana. Seuraavat asetukset ovat tarpeen vain, jos **EAP - MD5** tai **EAP - MS-CHAPv2** on valittu **Authentication Method (Todennusmenetelmä)** -asetukselle: • **Mode (tila)** Valitse **Server-Mode (Palvelintila)** tai **Client-Mode (Asiakastila)**. • **Certificate (Sertifikaatti)** Valitse varmenne. • **User Name (Käyttäjänimi)** Anna käyttäjätunnus (enintään 32 merkkiä). • **Password (Salasana)** Anna salasana (enintään 32 merkkiä). Salasana on annettava kahteen kertaan, jotta sen varmistetaan olevan varmasti oikein.
Pre-Shared Key (Esijaettu avain)	Tiedonsiirtoa salattaessa salausavain vaihdetaan ja jaetaan etukäteen toista kanavaa käyttäen. Jos valitset **Authentication Method (Todennusmenetelmä)** -tyypiksi **Pre-Shared Key (Esijaettu avain)**, kirjoita **Pre-Shared Key (Esijaettu avain)** (enintään 32 merkkiä). • **Local/ID Type/ID (Lähettäjä/Tunnistetyyppi/Tunniste)** Valitse lähettäjän tunnustyyppi ja kirjoita tunnus. Valitse tyypiksi **IPv4 Address (IPv4-osoite)**, **IPv6 Address (IPv6-osoite)**, **FQDN**, **E-mail Address (Sähköpostiosoite)** tai **Certificate (Sertifikaatti)**. Jos valitset **Certificate (Sertifikaatti)**, syötä varmenteen yleinen nimi **ID (Tunniste)**-kenttään. • **Remote/ID Type/ID (Vastaanottaja/Tunnistetyyppi/Tunniste)** Valitse vastaanottajan tunnustyyppi ja kirjoita tunnus. Valitse tyypiksi **IPv4 Address (IPv4-osoite)**, **IPv6 Address (IPv6-osoite)**, **FQDN**, **E-mail Address (Sähköpostiosoite)** tai **Certificate (Sertifikaatti)**.

Valinta	Kuvaus
	Jos valitset **Certificate (Sertifikaatti)**, syötä varmenteen yleinen nimi **ID (Tunniste)**-kenttään.
Certificate (Sertifikaatti)	Jos valitsit **Certificates (Varmenteet)** kohdassa **Authentication Method (Todennusmenetelmä)**, valitse varmenne.  Voit valita ainoastaan WWW-pohjaisen hallinnan suojausmäärityksnäytön **Certificate (Sertifikaatti)** -sivulla luotuja varmenteita.

Aiheeseen liittyviä tietoja

- IPsec-mallin määrittäminen WWW-pohjaisen hallinnan avulla

Manuaaliset asetukset IPsec-mallille

Valinta	Kuvaus
Template Name (Mallin nimi)	Kirjoita mallin nimi (enintään 16 merkkiä).
Use Prefixed Template (Käytä esimääritettyä mallia)	Valitse **Custom (Mukautettu)**.
Internet Key Exchange (IKE)	IKE on protokolla, jonka avulla voidaan vaihtaa salausavaimia salatun tietoliikenteen käyttämiseksi IPsec-protokollan avulla. Kertaluontoisen salatun tiedonsiirron mahdollistamiseksi protokolla määrittää IPsec-protokollan vaatiman salausalgoritmin ja jakaa salausavaimet. IKE-protokollan salausavaimet vaihdetaan Diffie-Hellman-menetelmän avulla ja IKE-protokollalle rajattu, salattu tiedonsiirto voidaan suorittaa. Valitse **Manual (Manuaalinen)**.
Authentication Key (ESP, AH) (Todennusavain (ESP, AH))	Kirjoita **In/Out (Tulo/lähtö)**-arvot. Asetukset ovat tarpeen, jos **Custom (Mukautettu)**-asetuksena on **Use Prefixed Template (Käytä esimääritettyä mallia)**, **Manual (Manuaalinen)**-asetuksena on **Internet Key Exchange (IKE)** ja **None (Ei mitään)**-kohdassa **Hash (Haja-arvo)**-asetuksena on muu kuin **Encapsulating Security (Kapselointisuojaus)**. Määritettävien merkkien määrä riippuu **Hash (Haja-arvo)** -kohdan **Encapsulating Security (Kapselointisuojaus)**-valinnasta. Jos määritetyn todennusavaimen pituus eroaa valitusta hajautusalgoritmista, järjestelmä ilmoittaa virheestä. • **MD5**: 128 bittiä (16 bittiryhmää) • **SHA1**: 160 bittiä (20 bittiryhmää) • **SHA256**: 256 bittiä (32 bittiryhmää) • **SHA384**: 384 bittiä (48 bittiryhmää) • **SHA512**: 512 bittiä (64 bittiryhmää) Kun määrität avaimen ASCII-koodimuodossa, sulje merkit kaksoislainausmerkkien (") sisään.
Code key (ESP) (Koodiavain (ESP))	Kirjoita **In/Out (Tulo/lähtö)**-arvot. Asetukset ovat tarpeen, jos **Use Prefixed Template (Käytä esimääritettyä mallia)**-asetuksena on **Custom (Mukautettu)**, **Internet Key Exchange (IKE)**-asetuksena on **Manual (Manuaalinen)** ja **Encapsulating Security (Kapselointisuojaus)**-kohdassa **Protocol (Protokolla)**-asetuksena on **ESP**. Määritettävien merkkien määrä riippuu **Encapsulating Security (Kapselointisuojaus)** -kohdan **Encryption (Salaus)**-valinnasta. Jos määritetyn koodiavaimen pituus eroaa valitusta salausalgoritmista, järjestelmä ilmoittaa virheestä. • **DES**: 64 bittiä (8 bittiryhmää) • **3DES**: 192 bittiä (24 bittiryhmää) • **AES-CBC 128**: 128 bittiä (16 bittiryhmää) • **AES-CBC 256**: 256 bittiä (32 bittiryhmää) Kun määrität avaimen ASCII-koodimuodossa, sulje merkit kaksoislainausmerkkien (") sisään.

Valinta	Kuvaus
SPI	Parametrien avulla tunnistetaan turvallisuustietoja. Yleensä isännällä on useita SA-varmenteita useille eri IPsec-tiedonsiirtotyypeille. Tästä syystä on tarpeellista tunnistaa asianmukainen SA IPsec-pakettia vastaanotettaessa. SA-varmenteen määrittävä SPI-parametri sisältyy AH- ja ESP-otsikoihin. Asetukset ovat tarpeellisia, kun **Custom (Mukautettu)** -asetuksena on **Use Prefixed Template (Käytä esimääritettyä mallia)** ja **Manual (Manuaalinen)**-asetuksena on **Internet Key Exchange (IKE)**. Syötä **In/Out (Tulo/lähtö)** -arvot. (3–10 merkkiä)
Encapsulating Security (Kapselointisuojaus)	• **Protocol (Protokolla)** Valitse **ESP** tai **AH**. - ESP on protokolla, jolla suoritetaan salattu tiedonsiirto IPsec-iä käyttäen. ESP salaa nettotiedot (siirretyn sisällön) ja lisää lisätietoja. IP-paketti koostuu otsakkeesta ja salatuista nettotiedoista, jotka seuraavat otsaketta. Salattujen tietojen lisäksi IP-paketti sisältää myös salausmenetelmää ja salausavainta koskevia tietoja, todennustietoja jne. - AH on osa IPsec-protokollaa, joka todentaa lähettäjän ja ehkäisee tietojen manipulointia (varmistaen tietojen eheyden). IP-paketissa tiedot sijaitsevat välittömästi otsikon perässä. Lisäksi paketit sisältävät haja-arvoja, jotka lasketaan siirretystä sisällöstä, salaisesta avaimesta, jne. koostuvalla kaavalla ehkäisten lähettäjän väärentämistä tai tietojen manipulointia. ESP:stä poiketen siirrettyä sisältöä ei salata ja tiedot lähetetään ja vastaanotetaan tavallisena tekstinä. • **Encryption (Salaus) (Ei käytettävissä, kun käytössä on AH.)** Valitse **DES**, **3DES**, **AES-CBC 128** tai **AES-CBC 256**. • **Hash (Haja-arvo)** valitse **None (Ei mitään)**, **MD5**, **SHA1**, **SHA256**, **SHA384**, tai **SHA512**. **None (Ei mitään)** voidaan valita ainoastaan silloin, kun **ESP** on valittu kohdassa **Protocol (Protokolla)**. • **SA Lifetime (SA-käyttöikä)** Määritä IKE SA -käyttöikä. Syötä aika (sekunteja) ja kilotavujen määrä (KByte). • **Encapsulation Mode (Kapselointitila)** Valitse **Transport (Siirto)** tai **Tunnel (Tunneli)**. • **Remote Router IP-Address (Etäreitittimen IP-osoite)** Syötä etäreitittimen IP-osoite (IPv4 tai IPv6). Syötä tiedot ainoastaan **Tunnel (Tunneli)** -tilan ollessa valittuna. SA (Security Association) on IPsec- tai IPv6-pohjainen salattu tiedonsiirtomenetelmä, joka vaihtaa ja jakaa tietoa, kuten salausmenetelmän ja salausavaimen, suojatun tiedonsiirtokanavan luomiseksi ennen tiedonsiirron aloittamista. SA voi myös viitata luotuun, virtuaaliseen suojattuun tiedonsiirtokanavaan. IPsec-protokollaan käytetty SA luo salausmenetelmän, vaihtaa avaimet ja suorittaa kahdenkeskeisen todennuksen IKE (Internet Key Exchange) -vakioprotokollan avulla. Lisäksi SA-menetelmää päivitetään ajoittain.

Aiheeseen liittyviä tietoja

- IPsec-mallin määrittäminen WWW-pohjaisen hallinnan avulla

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 unauthorized 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 määrityksen 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 verkkomääritysraportin 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:

- Suojausvarmteen ominaisuuksien yleiskuvaus
- Varmenteiden määritys 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 tunneled 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 ProtocolMessage 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

Käyttäjän todennus

- Active Directory -todennuksen käyttö
- LDAP-todennuksen käyttö
- Secure Function Lock 3.0 -toiminnon käyttö

Active Directory -todennuksen käyttö

Johdanto Active Directory -todennukseen

Active Directory Authentication (Active Directory -todennus) rajoittaa laitteen käyttöä. Jos Active Directory -todennus otetaan käyttöön, laitteen ohjauspaneeli lukitaan.Et voi muuttaa laitteen asetuksia ennen kuin syötät käyttäjätunnuksen ja salasanan.

Active Directory -todennus sisältää seuraavat ominaisuudet:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

- Saapuvien tulostustietojen tallennus
- Saapuvien faksitietojen tallennus
- Hakee käyttäjätunnuksesi mukaisen sähköpostiosoitteen Active Directory -palvelimesta lähetettäessä skannattuja tietoja sähköpostipalvelimeen.

  Voit käyttää ominaisuutta valitsemalla **On (Päälle)**-asetuksen **Get Mail Address (Hae sähköpostiosoite)** -toiminnolle ja valitsemalla todennusmenetelmäksi **LDAP + kerberos** tai **LDAP + NTLMv2**. Sähköpostiosoitteesi asetetaan lähettäjäksi, kun skannattuja tietoja lähetetään sähköpostipalvelimelle, tai vastaanottajaksi, jos lähetät skannatut tiedot sähköpostiosoitteeseesi.

Kun Active Directory -todennus on käytössä, laite tallentaa kaikki saapuvat faksitiedot. Kun olet kirjautunut sisään, laite tulostaa tallennetut faksitiedot.

Voit muuttaa Active Directoryn todennusasetuksia WWW-pohjaisen hallinnan avulla.

Aiheeseen liittyviä tietoja

- Active Directory -todennuksen käyttö

Active Directory -todennuksen määrittäminen WWW-pohjaisen hallinnan avulla

Active Directory -todennus tukee Kerberos- ja NTLMv2-todennusta. Sinun on määritettävä SNTP-protokolla (verkon aikapalvelin) ja DNS-palvelin todennusta varten.

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 **Administrator (Järjestelmänvalvoja)** > **User Restriction Function (Käyttäjän rajoitustoiminto)** tai **Restriction Management (Rajoitusten hallinta)**.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ≡.
5. Valitse **Active Directory Authentication (Active Directoryn todennus)**.
6. Napsauta **Submit (Lähetä)**.
7. Valitse **Active Directory Authentication (Active Directoryn todennus)**.
8. Määritä seuraavat asetukset:

   Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

Valinta	Kuvaus
Storage Fax RX Data (Tallennetut vastaanotetut faksitiedot)	Tämän valinnan avulla voit tallentaa saapuvia tulostustietoja. Voit tulostaa kaikki saapuvat faksitiedot kirjauduttuasi sisään laitteeseen.
Remember User ID (Muista käyttäjätunnus)	Tämän valinnan avulla voit tallentaa käyttäjätunnuksesi.
Active Directory Server Address (Active Directoryn palvelinosoite)	Active Directoryn palvelimen IP-osoite tai palvelimen nimi (esim. ad.example.com).
Active Directory Domain Name (Active Directoryn verkkoalueen nimi)	Anna Active Directory -toimialueen nimi.
Protocol & Authentication Method (Protokolla ja todennustapa)	Valitse protokolla ja todennusmenetelmä.
SSL/TLS	Valitse **SSL/TLS** -vaihtoehto.
LDAP Server Port (LDAP-palvelinportti)	Kirjoita portin numero, jos haluat yhdistää Active Directory -palvelimen LDAP:n kautta (käytettävissä vain todennusmenetelmälle **LDAP + kerberos** tai **LDAP + NTLMv2**).

Valinta	Kuvaus
LDAP Search Root (LDAP-haku-hakemisto)	Kirjoita LDAP-haun juurihakemisto (käytettävissä vain todennusmenetelmälle **LDAP + kerberos** tai **LDAP + NTLMv2**).
Get Mail Address (Hae sähköpostiosoite)	Tämän asetuksen avulla voit hakea sisäänkirjautuneen käyttäjän sähköpostiosoitteen Active Directory -palvelimesta. (käytettävissä vain todennusmenetelmälle **LDAP + kerberos** tai **LDAP + NTLMv2**)
Get User's Home Directory (Hae käyttäjän kotihakemisto)	Tämän valinnan avulla voit määrittää kotihakemistosi skannaa verkkoon -kohteeksi. (käytettävissä vain todennusmenetelmälle **LDAP + kerberos** tai **LDAP + NTLMv2**)

9. Napsauta **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- Active Directory -todennuksen käyttö

Kirjautuminen sisään laitteen asetusten muokkaamiseksi laitteen ohjauspaneelin avulla (Active Directory -todennus)

Active Directory -todennuksen ollessa käytössä laite pysyy lukittuna, kunnes syötät käyttäjätunnuksen, verkkoalueen nimen sekä salasanan laitteen ohjauspaneelin avulla.

1. Syötä kirjautumista varten käyttäjätunnus ja salasana laitteen ohjauspaneelin avulla.
2. Jos todennus onnistuu, laitteen ohjauspaneelin lukitus avautuu.

Aiheeseen liittyviä tietoja

- Active Directory -todennuksen käyttö

LDAP-todennuksen käyttö

- Johdanto LDAP-todennukseen
- LDAP-todennuksen määrittäminen WWW-pohjaisen hallinnan avulla
- Kirjaudu sisään muuttaaksesi laitteen asetuksia laitteen ohjauspaneelin avulla (LDAP-todennus)

Johdanto LDAP-todennukseen

LDAP Authentication (LDAP-todennus) rajoittaa laitteen käyttöä. Jos LDAP-todennus otetaan käyttöön, laitteen ohjauspaneeli lukitaan. Et voi muuttaa laitteen asetuksia ennen kuin syötät käyttäjätunnuksen ja salasanan.

LDAP-todennus tarjoaa seuraavat ominaisuudet:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

- Saapuvien tulostustietojen tallennus
- Saapuvien faksitietojen tallennus
- Hakee käyttäjätunnuksesi mukaisen sähköpostiosoitteen LDAP-palvelimelta skannattuja tietoja lähetettäessä sähköpostipalvelimelle.

  Voit käyttää ominaisuutta asettamalla **Get Mail Address (Hae sähköpostiosoite)** -asetuksen **On (Päälle)**-tilaan. Sähköpostiosoitteesi asetetaan lähettäjäksi, kun skannattuja tietoja lähetetään sähköpostipalvelimelle, tai vastaanottajaksi, jos lähetät skannatut tiedot sähköpostiosoitteeseesi.

Kun LDAP-todennus on käytössä, laite tallentaa kaikki saapuvat faksitiedot. Kun olet kirjautunut sisään, laite tulostaa tallennetut faksitiedot.

Voit muuttaa LDAP-todennusasetukset WWW-pohjaisen hallinnan avulla.

Aiheeseen liittyviä tietoja

- LDAP-todennuksen käyttö

LDAP-todennuksen määrittäminen 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. Napsauta vasemmassa siirtymispalkissa **Administrator (Järjestelmänvalvoja)** > **User Restriction Function (Käyttäjän rajoitustoiminto)** tai **Restriction Management (Rajoitusten hallinta)**.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.
5. Valitse **LDAP Authentication (LDAP-todennus)**.
6. Napsauta **Submit (Lähetä)**.
7. Napsauta **LDAP Authentication (LDAP-todennus)** -valikkoa.
8. Määritä seuraavat asetukset:

   Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

Valinta	Kuvaus
Storage Fax RX Data (Tallennetut vastaanotetut faksitiedot)	Tämän valinnan avulla voit tallentaa saapuvia tulostustietoja. Voit tulostaa kaikki saapuvat faksitiedot kirjauduttuasi sisään laitteeseen.
Remember User ID (Muista käyttäjätunnus)	Tämän valinnan avulla voit tallentaa käyttäjätunnuksesi.
LDAP Server Address (LDAP-palvelimen osoite)	Kirjoita LDAP-palvelimen IP-osoite tai palvelinnimi (esimerkiksi ldap.esimerkki.com).
SSL/TLS	Käytä LDAP:tä SSL:n/TLS:n sijaan valitsemalla vaihtoehto **SSL/TLS**.
LDAP Server Port (LDAP-palvelinportti)	Kirjoita LDAP-palvelinporttinumero.
LDAP Search Root (LDAP-hakuhakemisto)	Syötä LDAP-haun juurihakemisto.
Attribute of Name (Search Key) (Ominaisuuden nimi (hakuavain))	Anna määrite, jota haluat käyttää hakuavaimena.
Get Mail Address (Hae sähköpostiosoite)	Tämän valinnan avulla voit hakea sisäänkirjautuneen käyttäjän sähköpostiosoitteen LDAP-palvelimelta.
Get User's Home Directory (Hae käyttäjän kotihakemisto)	Tämän valinnan avulla voit määrittää kotihakemistosi skannaa verkkoon -kohteeksi.

9. Napsauta **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- LDAP-todennuksen käyttö

Kirjaudu sisään muuttaaksesi laitteen asetuksia laitteen ohjauspaneelin avulla (LDAP-todennus)

LDAP-todennuksen ollessa käytössä laite pysyy lukittuna, kunnes syötät käyttäjätunnuksen, verkkoalueen nimen sekä salasanan laitteen ohjauspaneelin avulla.

1. Syötä kirjautumista varten käyttäjätunnus ja salasana laitteen ohjauspaneelin avulla.
2. Jos todennus onnistuu, laitteen ohjauspaneelin lukitus avautuu.

Aiheeseen liittyviä tietoja

- LDAP-todennuksen käyttö

Secure Function Lock 3.0 -toiminnon käyttö

Brotherin Toimintalukko 3.0 parantaa suojausta rajoittamalla Brother-laitteessa käytössä olevia toimintoja.

Ennen Secure Function Lock 3.0 -toiminnon käyttämistä

Määritä salasanat, aseta tiettyjä käyttäjäsivujen rajoituksia ja myönnä pääsy joihinkin tai kaikkiin tässä mainittuihin toimintoihin.

Voit määrittää ja muuttaa seuraavia Toimintalukko 3.0 -asetuksia käyttämällä WWW-pohjaista hallintaa:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

- **Print (Tulosta)**
- **Copy (Kopio)**
- **Scan (Skannaa)**
- **Fax (Faksi)**
- **Media (Tietoväline)**
- **Web Connect**
- **Apps**
- **Page Limits (Sivurajoitus)**
- **Page Counters (Sivulaskuri)**
- **Card ID (NFC ID) (Kortin tunnus (NFC ID))**

Nestekidenäyttömallit:

Kun Toimintalukko on käytössä, laite siirtyy automaattisesti julkiseen tilaan ja joidenkin laitteen toimintojen käyttö rajoitetaan vain authorized käyttäjille. Käytä laitteen rajoitettuja toimintoja painamalla , valitsemalla käyttäjätunnuksesi ja antamalla salasanasi.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Secure Function Lock 3.0 -toiminnon määritys 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. Napsauta vasemmassa siirtymispalkissa **Administrator (Järjestelmänvalvoja)** > **User Restriction Function (Käyttäjän rajoitustoiminto)** tai **Restriction Management (Rajoitusten hallinta)**.

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

5. Valitse **Secure Function Lock (Toimintalukko)**.
6. Napsauta **Submit (Lähetä)**.
7. Napsauta **Restricted Functions (Rajoitetut toiminnot)** -valikkoa.
8. Määritä asetukset rajoitusten hallitsemiseksi käyttäjä- tai ryhmäkohtaisesti.
9. Napsauta **Submit (Lähetä)**.
10. Napsauta **User List (Käyttäjäluettelo)** -valikkoa.
11. Määritä käyttäjäluettelo.
12. Napsauta **Submit (Lähetä)**.

> Voit myös muuttaa käyttäjäluettelon sulkuasetukset **Secure Function Lock (Toimintalukko)** -valikossa.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Skannaus Secure Function Lock 3.0 -toiminnolla

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

Skannauksen rajoitusten määrittäminen (järjestelmänvalvojille)

Toimintalukko 3.0 -toiminnon avulla järjestelmänvalvoja voi rajoittaa käyttäjien skannausoikeutta. Kun skannaustoiminto on estetty yleiseltä käyttäjäasetukselta, vain ne käyttäjät, joilla on valittuna **Scan (Skannaa)** -valintaruutu, pystyvät skannaamaan.

Skannausominaisuuden käyttö (rajoitetuille käyttäjille)

- Skannaus laitteen ohjauspaneelista:

  Rajoitetut käyttäjät voivat siirtyä skannaustilaan antamalla salasanat laitteen ohjauspaneelista.
- Skannaus tietokoneelta:

  Rajoitettujen käyttäjien on annettava salasanat laitteen ohjauspaneelista ennen tietokoneesta skannausta. Jos laitteen ohjauspaneelista ei anneta salasanaa, käyttäjän tietokoneeseen tulee virheviesti.

Jos laite tukee IC-kortin todennusta, rajoitetut käyttäjät voivat käyttää skannaustilaa myös koskettamalla laitteen ohjauspaneelissa olevaa NFC-symbolia rekisteröidyillä IC-korteillaan.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Määritä yleinen tila Secure Function Lock 3.0 -toiminnolle

Tee yleisen tilan asetukset, jotka rajoittavat yleisten käyttäjien käytettävissä olevia toimintoja, käyttämällä Secure Function Lock -toiminnon näyttöä. Yleisten käyttäjien ei tarvitse antaa salasanaa käyttääkseen yleisessä tilassa käytössä oleviksi määritettyjä toimintoja.

Julkinen tila sisältää tulostustyöt, jotka on lähetetty Brother iPrint&Scan- ja Brother Mobile Connect -sovelluksilla.

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 **Administrator (Järjestelmänvalvoja)** > **User Restriction Function (Käyttäjän rajoitustoiminto)** tai **Restriction Management (Rajoitusten hallinta)**.

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

5. Valitse **Secure Function Lock (Toimintalukko)**.
6. Napsauta **Submit (Lähetä)**.
7. Napsauta **Restricted Functions (Rajoitetut toiminnot)** -valikkoa.
8. Salli annettu toiminto valitsemalla valintaruutu tai rajoita annettua toimintoa poistamalla valintaruudun valinta **Public Mode (Julkinen tila)** -rivillä.
9. Napsauta **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Henkilökohtaisen aloitusnäytön asetusten määrittäminen WWW-pohjaisen hallinnan avulla

Järjestelmänvalvojana voit määrittää, mitkä välilehdet käyttäjät voivat nähdä henkilökohtaisissa aloitusnäytöissään. Näiden välilehtien kautta pääsee nopeasti käyttäjien favorite, jotka voivat yhdistää henkilökohtaisen aloitusnäyttönsä välilehtiin laitteen ohjauspaneelin kautta.

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

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 **Administrator (Järjestelmänvalvoja)** > **User Restriction Function (Käyttäjän rajoitustoiminto)** tai **Restriction Management (Rajoitusten hallinta)**.

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

5. Valitse **Secure Function Lock (Toimintalukko)**.
6. Valitse **Tab Settings (Välilehtiasetukset)**-kentästä **Personal (Henkilökohtainen)** niille välilehden nimille, joita haluat käyttää henkilökohtaisena aloitusnäyttönäsi.
7. Napsauta **Submit (Lähetä)**.
8. Napsauta **Restricted Functions (Rajoitetut toiminnot)** -valikkoa.
9. Määritä asetukset rajoitusten hallitsemiseksi käyttäjä- tai ryhmäkohtaisesti.
10. Napsauta **Submit (Lähetä)**.
11. Napsauta **User List (Käyttäjäluettelo)** -valikkoa.
12. Määritä käyttäjäluettelo.
13. Valitse pudotusluettelosta **User List / Restricted Functions (Käyttäjäluettelo / rajoitetut toiminnot)** jokaiselle käyttäjälle.
14. Valitse välilehden nimi kullekin käyttäjälle **Home Screen (Aloitusnäyttö)**-pudotusluettelosta.
15. Napsauta **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Secure Function Lock 3.0 -toiminnon lisäominaisuudet

Määritä seuraavat ominaisuudet Secure Function Lock -toiminnon näytöllä:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

All Counter Reset (Nollaa kaikki laskurit)

Voit nollata sivulaskurin napsauttamalla **All Counter Reset (Nollaa kaikki laskurit)** kohdassa **Page Counters (Sivulaskuri)**.

Export to CSV file (Vienti CSV-tiedostoon)

Voit viedä nykyisen sivulaskurin, mukaan lukien **User List / Restricted Functions (Käyttäjäluettelo / rajoitetut toiminnot)**-tiedot CSV-tiedostona napsauttamalla **Export to CSV file (Vienti CSV-tiedostoon)**.

Card ID (NFC ID) (Kortin tunnus (NFC ID))

Napsauta **User List (Käyttäjäluettelo)**-valikkoa ja kirjoita käyttäjän kortin tunniste **Card ID (NFC ID) (Kortin tunnus (NFC ID))** -kenttään. Voit käyttää IC-korttiasi todennukseen.

Output (Tulostus)

Mikäli lajittelija on asennettu laitteeseesi, valitse jokaiselle käyttäjälle luovutusalusta pudotusluettelosta.

Last Counter Record (Viimeinen laskurin tietue)

Napsauta **Last Counter Record (Viimeinen laskurin tietue)**, jos haluat laitteen säilyttävän sivulukeman sen jälkeen, kun laskuri on nollattu.

Counter Auto Reset (Laskurin automaattinen palautus)

Määritä aikaväli, jolloin haluat nollata sivulaskurin, napsauttamalla **Counter Auto Reset (Laskurin automaattinen palautus)**. Valitse aikaväliksi päivä, viikko tai kuukausi.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Uuden sirukortin rekisteröinti laitteen ohjauspaneelin avulla

Voit rekisteröidä laitteeseen älykortteja (IC-kortteja).

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

1. Kosketa laitteen ohjauspaneelin Near-Field Communication (NFC) -symbolia rekisteröidyllä Integrated Circuit -kortilla (IC-kortilla).
2. Paina käyttäjätunnustasi nestekidenäytössä.
3. Paina Rekisteröi kortti -painiketta.
4. Kosketa NFC-symbolia uudella IC-kortilla.

   Uuden IC-kortin numero rekisteröidään sitten laitteeseen.
5. Paina OK-painiketta.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Ulkoisen sirukortinlukijan rekisteröiminen

Kun yhdistät ulkoisen sirukortinlukijan (integroitu piiri), rekisteröi kortinlukija käyttämällä WWW-pohjaista hallintaa. Laitteesi tukee HID-luokkaohjaimen tukemia ulkoisia sirukortinlukijoita.

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 **Administrator (Järjestelmänvalvoja)** > **External Card Reader (Ulkoinen kortinlukija)** vasemmassa selauspalkissa.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ≡.
5. Syötä tarvitut tiedot ja napsauta sitten **Submit (Lähetä)**.
6. Ota asetukset käyttöön käynnistämällä Brother-laite uudelleen.
7. Liitä kortinlukija laitteeseen.
8. Kosketa kortilla kortinlukijaa kun kortin todennus on käytössä.

Aiheeseen liittyviä tietoja

- Secure Function Lock 3.0 -toiminnon käyttö

Sähköpostin suojattu lähetys ja vastaanotto

Sähköpostin lähetyksen tai vastaanoton määritys WWW-pohjaisen hallinnan avulla

- Sähköpostin vastaanotto on käytettävissä vain tietyissä malleissa.
- Suosittelemme, että määrität suojatun sähköpostin lähetyksen käyttäjän todennuksella tai sähköpostin lähetyksen ja vastaanoton SSL/TLS-protokollan avulla (koskee vain tuettuja malleja) käyttämällä WWW-pohjaista hallintaa.

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. Napsauta **POP3/IMAP4/SMTP Client (POP3-/IMAP4-/SMTP-asiakas)**-kentässä **Advanced Settings (Lisäasetukset)** ja varmista, että **POP3/IMAP4/SMTP Client (POP3-/IMAP4-/SMTP-asiakas)**-tila on **Enabled (Käytössä)**.

   - Käytettävissä olevat protokollat voivat vaihdella laitteittain.
   - Jos **Authentication Method (Todennusmenetelmä)**-valintanäyttö tulee näkyviin, valitse todentamismenetelmä ja noudata sitten näyttöön tulevia ohjeita.
6. Määritä **POP3/IMAP4/SMTP Client (POP3-/IMAP4-/SMTP-asiakas)**-asetukset.
   - Voit varmistaa, että sähköpostiasetukset on määritetty oikein lähettämällä testisähköpostiviestin.
   - Ota yhteys verkonvalvojaan tai Internet-palveluntarjoajaan (ISP), jos et tiedä POP3/IMAP4/SMTP-palvelimen asetuksia.
7. Kun olet valmis, napsauta **Submit (Lähetä)**.

   Test Send/Receive E-mail Configuration (Testaa sähköpostin lähetys-/vastaanottoasetuksia) -valintaikkuna avautuu.
8. Testaa nykyisiä asetuksia noudattamalla valintaikkunan ohjeita.

Aiheeseen liittyviä tietoja

- Sähköpostin suojattu lähetys ja vastaanotto

Liittyvät aiheet:

- Sähköpostin suojattu lähetys tai vastaanotto SSL/TLS:n avulla

Sähköpostin lähetys käyttäjän todennuksella

Laitteesi lähettää sähköpostit käyttäjän todennusta edellyttävän sähköpostipalvelimen kautta. Tämä menetelmä estää unauthorized käyttäjiä käyttämästä sähköpostipalvelinta.

Voit lähettää sähköposti-ilmoituksia, sähköpostiraportteja ja I-Fax (I-Faksi) -asiakirjoja (käytettävissä vain tietyissä malleissa) käyttämällä käyttäjän todennusta.

- Käytettävissä olevat protokollat voivat vaihdella laitteittain.
- Suosittelemme WWW-pohjaisen hallinnan käyttöä SMTP-todennuksen määritykseen.

Sähköpostipalvelimen asetukset

Laitteen SMTP-todennusmenetelmä on määritettävä sopimaan sähköpostipalvelimesi käyttämään menetelmään. Kysy lisätietoja sähköpostipalvelimen asetuksista verkonvalvojalta tai Internet-palveluntarjoalta (ISP).

Jos haluat ottaa SMTP-palvelimen todennuksen käyttöön WWW-pohjaisen hallinnan avulla, valitse todennusmenetelmä **POP3/IMAP4/SMTP Client (POP3-/IMAP4-/SMTP-asiakas)**-näytön kohdasta **Server Authentication Method (Palvelimen todennustapa)**.

Aiheeseen liittyviä tietoja

- Sähköpostin suojattu lähetys ja vastaanotto

Sähköpostin suojattu lähetys tai vastaanotto SSL/TLS:n avulla

Laitteesi tukee SSL/TLS-yhteysmenetelmiä. SSL/TLS-tiedonsiirtoa käyttävän sähköpostipalvelimen käyttöä varten sinun on määritettävä seuraavat asetukset.

- Sähköpostin vastaanotto on käytettävissä vain tietyissä malleissa.
- Suosittelemme WWW-pohjaisen hallinnan käyttöä SSL/TLS:n määritykseen.

Tarkista palvelinvarmenne

Jos kohdassa **SSL/TLS** valitaan **SSL** tai **TLS**, **Verify Server Certificate (Tarkista palvelinvarmenne)** -valintaruutu valitaan automaattisesti.

- 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.
- Jos palvelinvarmennetta ei tarvitse tarkistaa, tyhjennä **Verify Server Certificate (Tarkista palvelinvarmenne)** -valintaruutu.

Portin numero

Jos valitset **SSL** tai **TLS**, **Port (Portti)** -arvo muutetaan protokollaan sopivaksi. Jos haluat muuttaa portin numeron manuaalisesti, kirjoita portin numero sen jälkeen, kun olet valinnut **SSL/TLS**-asetukset.

Laitteen yhteysmenetelmä on määritettävä sopimaan sähköpostipalvelimen käyttämään menetelmään. Kysy lisätietoja sähköpostipalvelimen asetuksista verkonvalvojalta tai Internet-palveluntarjoalta (ISP).

Useimmissa tapauksissa suojatut webmail-verkkosähköpostipalvelut vaativat seuraavat asetukset:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

SMTP	**Port (Portti)**	587
	Server Authentication Method (Palvelimen todennus-tapa)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port (Portti)**	995
	SSL/TLS	**SSL**
IMAP4	**Port (Portti)**	993
	SSL/TLS	**SSL**

Aiheeseen liittyviä tietoja

- Sähköpostin suojattu lähetys ja vastaanotto

Liittyvät aiheet:

- Sähköpostin lähetyksen tai vastaanoton määritys WWW-pohjaisen hallinnan avulla
- Varmenteiden määritys laitteen suojaukselle

Tulostuslokin tallennus verkkoon

- Tulostuslokin verkkoon tallentamisen yleiskatsaus
- Tulostuslokin tallennus verkkoon -toiminnon asetusten määrittäminen WWW-pohjaisen hallinnan avulla
- Käytä Tallenna tulostusloki verkkoon -kohdan Virheenjäljitys-asetusta
- Tulostustyön tallennus verkkoon -toiminnon käyttäminen Secure Function Lock 3.0 -toiminnon kanssa

Tulostuslokin verkkoon tallentamisen yleiskatsaus

Tulostuslokin tallennus verkkoon -ominaisuuden avulla voit tallentaa laitteen tulostuslokitiedoston verkkopalvelimeen CIFS (Common Internet File System) -protokollan avulla. Voit tallentaa tunnuksen, tulostustyön tyypin, työn nimen, käyttäjänimen, päivämäärän, ajan ja tulostettujen sivujen määrän kullekin tulostustyölle. CIFS protokolla, jota käytetään TCP/IP:n yli, jolloin verkon tietokoneet voivat jakaa tiedostoja intranetin tai Internetin kautta.

Tulostuslokiin tallennetaan seuraavat tulostustoiminnot:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

- Tulostustyöt tietokoneeltasi
- USB-suoratulostus
- Kopiointi
- Vastaanotettu faksi
- Web Connect -tulostus

- Tulostuslokin tallennus verkkoon -toiminto tukee Kerberos- ja NTLMv2-todennusta. SNTP-protokolla (verkon aikapalvelin) on määritettävä tai päivämäärä, aika ja aikavyöhyke on määritettävä ohjauspaneelissa oikein todennusta varten.
- Voit määrittää tiedostotyypiksi TXT tai CSV, kun tallennat tiedoston palvelimelle.

Aiheeseen liittyviä tietoja

- Tulostuslokin tallennus verkkoon

Tulostuslokin tallennus verkkoon -toiminnon asetusten määrittäminen 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. Napsauta vasemmassa siirtymispalkissa **Administrator (Järjestelmänvalvoja)** > **Store Print Log to Network (Tallenna tulostusloki verkkoon)**.

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

5. Napsauta **Print Log (Tulosta loki)** -kentässä **On (Päälle)**.
6. Määritä seuraavat asetukset:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

Valinta	Kuvaus
Network Folder Path (Verkkokansion polku)	Kirjoita kohdekansio, johon tulostusloki tallennetaan CIFS-palvelimelle (esimerkiksi \\TietokoneenNimi\JaettuKansio).
File Name (Tiedostonimi)	Anna tulostuslokille tiedostonimi, jota haluat käyttää (enintään 32 merkkiä).
File Type (Tiedostotyyppi)	Valitse vaihtoehto **TXT (Teksti)** tai **CSV** tulostuslokin tiedostotyypille.
Time Source for Log (Lokin aikalähde)	Valitse tulostuslokin aikalähde.
Auth. Method (Todentamismenetelmä)	Valitse todennusmenetelmä, joka tarvitaan CIFS-palvelimen käyttämiseen: **Auto (Automaattinen)**, **Kerberos** tai **NTLMv2**. Kerberos on todennusmenetelmä, joka sallii laitteiden tai henkilöiden todistaa henkilöllisyytensä verkkopalvelimille yhdellä sisäänkirjautumisella. NTLMv2 on todennusmenetelmä, jota Windows käyttää palvelimiin kirjauduttaessa. • **Auto (Automaattinen)**: Jos valitset **Auto (Automaattinen)**, käytetään NTLMv2-todennusmenetelmää. • **Kerberos**: Valitse **Kerberos**-valinta käyttääksesi vain Kerberos-todennusta. • **NTLMv2**: Valitse **NTLMv2**-valinta käyttääksesi vain NTLMv2-todennusta. • - ja **Kerberos**-todennusmenetelmää varten sinun on määritettävä myös **NTLMv2**-asetukset tai SNTP-protokolla (verkon aikapalvelin) ja DNS-palvelin.**Date&Time (Päivämäärä ja aika)** • Voit määrittää päiväys- ja aika-asetukset myös laitteen ohjauspaneelin avulla.

Valinta	Kuvaus
Username (Käyttäjätunnus)	Kirjoita todennuksen käyttäjätunnus (enintään 96 merkkiä). Jos käyttäjätunnus on verkkoalueen osa, syötä käyttäjätunnus jommallakummalla seuraavista tyyleistä: käyttäjä@verkkoalue tai verkkoalue\käyttäjä.
Password (Salasana)	Anna todennuksen salasana (enintään 32 merkkiä).
Kerberos Server Address (Kerberos-palvelimen osoite) (tarvittaessa)	Kirjoita avaintenjakelukeskuksen (Key Distribution Center (KDC)) isäntäosoite (esimerkiksi kerberos.example.com, enintään 64 merkkiä) tai IP-osoite (esimerkiksi 192.168.56.189).
Error Detection Setting (Virheen tunnistusasetus)	Valitse tehtävät toimenpiteet, jos tulostuslokia ei voi tallentaa palvelimeen verkkovirheen vuoksi.

7. Vahvista viimeisen lokin tila **Connection Status (Yhteyden tila)** -kentässä.

Voit myös vahvistaa virheen tilan laitteen LCD-näytöllä.

8. Avaa **Submit (Lähetä)** -sivu napsauttamalla **Test Print Log to Network (Testaa tulostuslokin lähettämistä verkkoon)**.

   Voit testata asetuksia napsauttamalla **Yes (Kyllä)** ja siirtymällä seuraavaan vaiheeseen.

   Ohita testi napsauttamalla **No (Ei)**. Asetukset lähetetään automaattisesti.
9. Laite testaa asetuksesi.
10. Jos asetukset ovat sopivat, **Test OK (Testi onnistui)** sivulla näkyy.

    Jos näkyviin tulee **Test Error (Testivirhe)**, tarkista kaikki asetukset ja tuo testisivu uudelleen näkyviin napsauttamalla **Submit (Lähetä)**.

Aiheeseen liittyviä tietoja

- Tulostuslokin tallennus verkkoon

Käytä Tallenna tulostusloki verkkoon -kohdan Virheenjäljitys-asetusta

Virheenjäljitysasetusten avulla voit määrittää tehtävän toimenpiteen, jos tulostuslokia ei voi tallentaa palvelimeen verkkovirheen vuoksi.

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 **Administrator (Järjestelmänvalvoja)** > **Store Print Log to Network (Tallenna tulostusloki verkkoon)**.

   Jos vasen selauspalkki ei ole näkyvissä, aloita selaus kohdasta ☰.
5. Valitse **Error Detection Setting (Virheen tunnistusasetus)** -kohdassa **Cancel Print (Peruuta tulostus)** tai **Ignore Log & Print (Ohita loki ja tulosta)**-vaihtoehto.

   Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.

Valinta	Kuvaus
Cancel Print (Peruuta tulostus)	Jos valitset **Cancel Print (Peruuta tulostus)**, tulostustyöt canceled, mikäli tulostuslokia ei voida tallentaa palvelimeen. Laite tulostaa vastaanotetun faksin, vaikka valitsisitkin **Cancel Print (Peruuta tulostus)**.

Ignore Log & Print (Ohita loki ja tulosta)	Jos valitset **Ignore Log & Print (Ohita loki ja tulosta)**, laite tulostaa dokumentin, vaikka tulostuslokia ei voisi tallentaa palvelimeen.
	Kun tulostuslokin tallennus on taas toiminnassa, tulostusloki tallennetaan seuraavasti:
	`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. Jos tulostuslokia ei voi tallentaa tulostuksen lopussa, tulostettujen sivujen määrää ei kirjata.
	b. Jos tulostuslokia ei voi tallentaa tulostuksen alussa ja lopussa, työn tulostuslokia ei tallenneta. Kun toiminto on palautunut, virhe näkyy tulostuslokissa.

6. Avaa **Submit (Lähetä)** -sivu napsauttamalla **Test Print Log to Network (Testaa tulostuslokin lähettämistä verkkoon)**.

   Voit testata asetuksia napsauttamalla **Yes (Kyllä)** ja siirtymällä seuraavaan vaiheeseen.

   Ohita testi napsauttamalla **No (Ei)**. Asetukset lähetetään automaattisesti.

7. Laite testaa asetuksesi.
8. Jos asetukset ovat sopivat, **Test OK (Testi onnistui)** sivulla näkyy.

   Jos näkyviin tulee **Test Error (Testivirhe)**, tarkista kaikki asetukset ja tuo testisivu uudelleen näkyviin napsauttamalla **Submit (Lähetä)**.

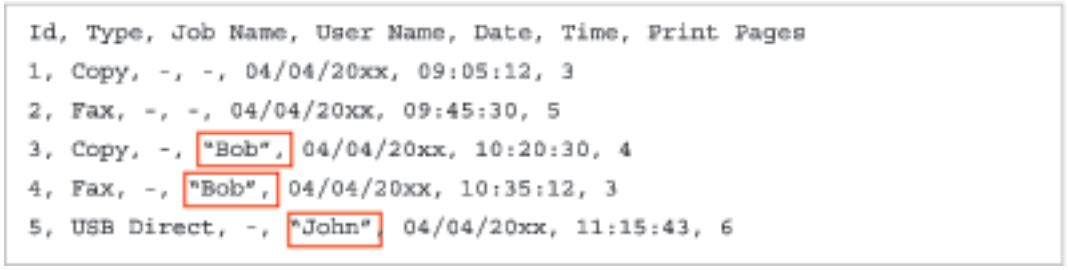
Aiheeseen liittyviä tietoja

- Tulostuslokin tallennus verkkoon

Tulostustyön tallennus verkkoon -toiminnon käyttäminen Secure Function Lock 3.0 -toiminnon kanssa

Kun Toimintalukko 3.0 on käytössä, kopiointia, faksin vastaanottamista, Web Connect -tulostusta ja USB-suoratulostusta varten rekisteröityjen käyttäjien nimet tallennetaan Tulostuslokin tallennus verkkoon -raporttiin. Kun Active Directory -todennus on käytössä, käyttäjätunnus tallennetaan Tulostuslokin tallennus verkkoon -raporttiin:

Tuetut ominaisuudet, vaihtoehdot ja asetukset voivat vaihdella malleittain.



```
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
```

Aiheeseen liittyviä tietoja

- Tulostuslokin tallennus verkkoon

brother

Brother Earth

www.brotherearth.com

FIN
Versio 0