Ghidul caracteristicilor de securitate

Cuprins

Introducere

Definiţia notelor

În acest manual de utilizare sunt utilizate următoarele simboluri şi convenţii:

IMPORTANT	IMPORTANT indică o situație potențial periculoasă care, dacă nu este evitată, ar putea cauza pagube materiale sau defectarea produsului.
NOTĂ	NOTĂ specifică mediul de utilizare, condiţiile de instalare sau condiţiile speciale de utilizare.
	Pictogramele cu sfaturi oferă indicii utile şi informaţii suplimentare.
Aldin	Stilul aldin identifică butoane de pe panoul de control al aparatului sau de pe ecranul computerului.
Cursiv	Italicized cursiv emphasizes un aspect important sau se referă la un subiect asociat.

Informaţii similare

- Introducere

Mărci comerciale

Adobe® și Reader® sunt fie mărci comerciale înregistrate, fie mărci comerciale ale Adobe Systems Incorporated în Statele Unite și/sau în alte țări.

Fiecare companie care are un titlu de software menționat în acest manual deține un License Software specific programelor sale brevetate.

Toate denumirile comerciale și denumirile de produs ale companiilor care apar pe produsele Brother, documentele aferente și orice alte materiale sunt mărci comerciale sau mărci comerciale înregistrate ale companiilor respective.

Informaţii similare

- Introducere

Copyright

Informaţii similare

- Introducere

Înainte de a utiliza caracteristicile de securitate ale rețelei

Aparatul dumneavoastră utilizează cele mai recente protocoale de securitate și de criptare ale rețelei disponibile în prezent. Aceste funcţii de reţea pot fi integrate în planul general de securitate pentru a ajuta la protejarea datelor şi pentru a preveni accesul unauthorized la aparat.

Recomandăm dezactivarea protocoalelor FTP şi TFTP. Accesarea aparatului folosind aceste protocoale nu este sigură.

Informaţii similare

- Introducere
  - Dezactivarea protocoalelor care nu sunt necesare

Dezactivarea protocoalelor care nu sunt necesare

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Anulați orice bifă inutilă din casetele de selectare ale protocoalelor pentru a le dezactiva.
6. Faceţi clic pe **Submit (Remitere)**.
7. Reporniți aparatul Brother pentru a activa configurația.

Informaţii similare

- Înainte de a utiliza caracteristicile de securitate ale rețelei

Securitatea rețelei

- Configurarea certificatelor pentru securitatea dispozitivului
- Utilizarea SSL/TLS
- Utilizarea SNMPv3
- Utilizarea IPsec
- Utilizarea autentificării IEEE 802.1x pentru rețeaua dumneavoastră

Configurarea certificatelor pentru securitatea dispozitivului

Trebuie să configurați un certificat pentru gestionarea în siguranță a aparatului conectat la rețea folosind SSL/TLS. Pentru configurarea certificatului trebuie să folosiţi Administrarea online a reţelei folosind Web Based Management.

- Prezentarea funcțiilor certificatului de securitate
- Crearea și instalarea unui certificat
- Crearea unui certificat auto semnat
- Crearea unei cereri de semnare a certificatului (CSR) și instalarea unui certificat emis de o autoritate de certificare (CA)
- Importul şi exportul certificatului şi al cheii de decriptare personală
- Importarea şi exportarea unui certificat AC

Prezentarea funcțiilor certificatului de securitate

Aparatul este compatibil și poate utiliza mai multe certificate de securitate, care permit autentificarea și comunicarea în siguranță cu aparatul. Următoarele caracteristici ale certificatului de securitate pot fi utilizate cu aparatul:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

- Comunicare SSL/TLS
- Autentificare IEEE 802.1x
- IPsec

Aparatul dvs. este compatibil cu următoarele:

- Certificat preinstalat

  Aparatul are un certificat preinstalat autosemnat. Acest certificat permite utilizarea comunicării SSL/TLS fără crearea sau instalarea unui alt certificat.

Certificatul autosemnat preinstalat vă protejează comunicațiile până la un anumit nivel. Vă recomandăm ca pentru îmbunătăţirea securităţii să utilizaţi un certificat emis de o organization acreditată.

- Certificat autosemnat

  Acest server de imprimare îşi emite propriul certificat. Utilizând acest certificat, puteţi folosi cu uşurinţă comunicarea SSL/TLS fără a crea sau instala un alt certificat emis de o autoritate de certificare (AC).
- Certificat emis de o autoritate de certificare (AC)

  Sunt disponibile două metode de instalare a unui certificat emis de o autoritate de certificare. Dacă aveţi deja un certificat emis de o AC sau dacă doriţi să folosiţi un certificat emis de o AC externă acreditată:
  - Dacă utilizaţi o cerere de semnare (Certificate Signing Request (CSR)) de la acest server de imprimare.
  - La importarea unui certificat sau a unei chei private.
- Certificatul autorităţii de certificare (AC)

  Pentru a utiliza un certificat CA care identifică CA și are o cheie proprie, trebuie să importați respectivul certificat CA emis de CA înainte de configurarea funcțiilor de securitate ale rețelei.

- Dacă veţi utiliza comunicarea SSL/TLS, vă recomandăm să contactaţi mai întâi administratorul de sistem.
- Dacă resetaţi serverul de imprimare la valorile implicite din fabricaţie, atunci certificatul şi cheia privată instalate vor fi şterse. Dacă doriţi să păstraţi acelaşi certificat şi cheie privată şi după resetarea serverului de imprimare, exportaţi-le înainte de resetare şi apoi reinstalaţi-le.

Informaţii similare

- Configurarea certificatelor pentru securitatea dispozitivului

Subiecte conexe:

- Configurați autentificarea IEEE 802.1x pentru rețeaua dumneavoastră utilizând Web Based Management (browser web)

Crearea și instalarea unui certificat

Există două opţiuni atunci când alegeţi un certificat de securitate: utilizarea unui certificat autosemnat sau utilizarea unui certificat emise de Autoritatea de certificare (CA).

Opţiunea 1

Certificat auto semnat

1. Creaţi un certificat auto semnat utilizând Web Based Management.
2. Instalaţi certificatul autosemnat pe computerul dvs.

Opţiunea 2

Certificat de la o Autoritate de certificat (CA)

1. Creaţi o cerere de semnare a certificatului (CSR) utilizând Administrarea bazată pe web.
2. Instalați certificatul emis de Autoritatea de certificare (CA) pe aparatul Brother utilizând Web Based Management.
3. Instalaţi certificatul pe calculatorul dumneavoastră.

Informaţii similare

- Configurarea certificatelor pentru securitatea dispozitivului

Crearea unui certificat auto semnat

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Faceţi clic pe **Create Self-Signed Certificate (Creare certificat semnat automat)**.
6. Introduceţi **Common Name (Nume comun)** şi **Valid Date (Dată validă)**.
   - Lungimea pentru **Common Name (Nume comun)** este de sub 64 de octeţi. Introduceţi un identificator, de exemplu o adresă IP, un nume de nod sau un nume de domeniu, care să fie folosit la accesarea acestui aparat prin comunicaţie SSL/TLS. Numele de nod este afişat în mod implicit.
   - Va apărea o avertizare dacă folosiţi protocolul IPPS sau HTTPS şi introduceţi un alt nume în URL decât **Common Name (Nume comun)** folosit pentru certificatul autosemnat.
7. Selectaţi setarea dvs. din **Public Key Algorithm (Algoritm cheie publică)** lista derulantă.
8. Selectaţi setarea dvs. din **Digest Algorithm (Algoritm de asimilare)** lista derulantă.
9. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Configurarea certificatelor pentru securitatea dispozitivului

Crearea unei cereri de semnare a certificatului (CSR) și instalarea unui certificat emis de o autoritate de certificare (CA)

Dacă aveți deja un certificat emis de o autoritate de certificare externă (CA), puteți să stocați certificatul și cheia de decriptare personală pe aparat și să le gestionați prin import și export. Dacă nu aveţi un certificat emis de CA externă acreditată, creaţi o cerere de semnare a certificatului (CSR), trimiteţi-o către CA pentru autentificare şi instalaţi certificatul returnat pe aparatul dvs.

- Crearea unei cereri de semnare a certificatului (CSR)
- Instalarea unui certificat pe aparatul dumneavoastră

Crearea unei cereri de semnare a certificatului (CSR)

O cerere de semnare a certificatului (CSR) este o solicitare trimisă către o autoritate de certificare (CA) de a autentifica acreditările incluse în certificat.

Recomandăm instalarea unui certificat rădăcină de la Autoritatea de certificare pe computer înainte de crearea unei CSR.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Faceţi clic pe **Create CSR (Creare CSR)**.
6. Introduceţi un **Common Name (Nume comun)** (obligatoriu) şi adăugaţi alte informaţii despre **Organization (Organizaţie)** (opţional).

   - Detaliile companiei sunt necesare pentru ca o autoritate de certificare să vă poată confirma identitatea și să o poată verifica cu un terț extern.
   - Lungimea pentru **Common Name (Nume comun)** trebuie să fie de sub 64 de octeţi. Introduceţi un identificator, de exemplu o adresă IP, un nume de nod sau un nume de domeniu, care să fie folosit la accesarea acestui aparat prin comunicaţie SSL/TLS. Numele de nod este afişat în mod implicit. **Common Name (Nume comun)** este obligatoriu.
   - O avertizare va apărea dacă introduceţi un alt nume în adresa URL decât numele comun care a fost folosit pentru certificat.
   - Lungimea **Organization (Organizaţie)**, **Organization Unit (Unitate organizaţională)**, **City/Locality (Oraş/localitate)** și **State/Province (Stat/provincie)** trebuie să fie mai mică de 64 de octeți.
   - **Country/Region (Ţară/regiune)** trebuie să fie un cod de țară cu două caractere ISO 3166.
   - În cazul în care configuraţi o extensie de certificat X.509v3, selectaţi caseta de validare **Configure extended partition (Configurare partiţie extinsă)** şi apoi selectaţi **Auto (Register IPv4) (Automat (înregistrare IPv4))** sau **Manual**.
7. Selectaţi setarea dvs. din **Public Key Algorithm (Algoritm cheie publică)** lista derulantă.
8. Selectaţi setarea dvs. din **Digest Algorithm (Algoritm de asimilare)** lista derulantă.
9. Faceţi clic pe **Submit (Remitere)**.

   CSR apare pe ecranul dvs. Salvaţi CSR ca un fişier sau ca o copie şi inseraţi-l într-un formular CSR online oferit de o autoritate de certificare.
10. Faceţi clic pe **Salvare**.

- Respectaţi politica autorităţii de certificare referitoare la metoda de trimitere a unei CSR către autoritatea de certificare.
- Dacă utilizați Enterprise Root CA pentru Windows Server, vă recomandăm să utilizați serverul web pentru șablonul certificatului pentru a crea în siguranță certificatul de client. În cazul în care creați un certificat de client pentru un mediu IEEE 802.1x cu autentificare EAP-TLS, vă recomandăm să utilizați Utilizator pentru modelul de certificat.

Informaţii similare

- Crearea unei cereri de semnare a certificatului (CSR) și instalarea unui certificat emis de o autoritate de certificare (CA)

Instalarea unui certificat pe aparatul dumneavoastră

Când primiți un certificat de la o autoritate de certificare (CA), urmați pașii de mai jos pentru a-l instala pe serverul de imprimare:

Se poate instala numai un certificat emis printr-o cerere de semnare a certificatului (CSR) a aparatului. Dacă doriți să creați alt CSR, asigurați-vă că certificatul este instalat înainte de crearea unui alt CSR. Creați un alt CSR numai după instalarea certificatului pe aparat. În caz contrar, CSR-ul creat înainte de instalarea noului CSR va fi nevalid.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Faceţi clic pe **Install Certificate (Instalare certificat)**.
6. Navigaţi până la fişierul care conţine certificatul emis de CA, apoi faceţi clic pe **Submit (Remitere)**.

   Certificatul este creat și salvat în memoria aparatului.

Pentru a utiliza comunicarea SSL/TLS, certificatul rădăcină de la Autoritatea de certificare trebuie să fie instalat pe computer. Contactaţi administratorul de reţea.

Informaţii similare

- Crearea unei cereri de semnare a certificatului (CSR) și instalarea unui certificat emis de o autoritate de certificare (CA)

Importul şi exportul certificatului şi al cheii de decriptare personală

Stocaţi certificatul şi cheia de decriptare personală pe aparatul dvs. şi gestionaţi-le prin import şi export.

- Importul certificatului şi al cheii de decriptare personală
- Exportul certificatului şi al cheii de decriptare personală

Importul certificatului şi al cheii de decriptare personală

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Faceţi clic pe **Import Certificate and Private Key (Import certificat şi cheie privată)**.
6. Navigați și selectați fișierul pe care doriți să îl importați.
7. Introduceţi parola dacă fişierul este criptat şi apoi faceţi clic **Submit (Remitere)**.

Certificatul şi cheia de decriptare personală sunt importate pe aparat.

Informaţii similare

- Importul şi exportul certificatului şi al cheii de decriptare personală

Exportul certificatului şi al cheii de decriptare personală

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ≡.

5. Faceţi clic pe **Export** arătat cu **Certificate List (Listă de certificate)**.
6. Introduceţi parola dacă doriţi să criptaţi fişierul.

   Dacă folosiţi o parolă vidă, rezultatul nu este criptat.
7. Introduceţi parola din nou pentru confirmare, apoi faceţi clic pe **Submit (Remitere)**.
8. Faceţi clic pe **Salvare**.

Certificatul şi cheia de decriptare personală sunt exportate pe computer.

De asemenea, puteţi importa certificatul în computer.

Informaţii similare

- Importul şi exportul certificatului şi al cheii de decriptare personală

Importarea şi exportarea unui certificat AC

Puteți importa, exporta și stoca certificate AC pe aparatul dumneavoastră Brother.

- Importarea unui certificat AC
- Exportarea unui certificat AC

Importarea unui certificat AC

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **CA Certificate (Certificat CA)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Faceţi clic pe **Import CA Certificate (Import certificat CA)**.
6. Navigaţi la fişierul pe care doriţi să îl importaţi.
7. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Importarea şi exportarea unui certificat AC

Exportarea unui certificat AC

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **CA Certificate (Certificat CA)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi certificatul pe care doriţi să îl exportaţi şi faceţi clic pe **Export**.
6. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Importarea şi exportarea unui certificat AC

Utilizarea SSL/TLS

- Gestionarea aparatului în reţea în siguranţă folosind SSL/TLS
- Imprimarea securizată a documentelor utilizând SSL/TLS
- Trimiterea sau primirea unui mesaj de e-mail în siguranță folosind SSL/TLS

Gestionarea aparatului în reţea în siguranţă folosind SSL/TLS

- Configurarea unui certificat pentru SSL/TLS și protocoalele disponibile
- Accesarea Web Based Management utilizând SSL/TLS
- Instalarea certificatului autosemnat pentru utilizatorii Windows ca administratori
- Configurarea certificatelor pentru securitatea dispozitivului

Configurarea unui certificat pentru SSL/TLS și protocoalele disponibile

Utilizând Web Based Management, configurați pe aparatul dumneavoastră un certificat înainte de a utiliza comunicarea SSL/TLS.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Faceţi clic pe **HTTP Server Settings (Setări server HTTP)**.
6. Selectaţi certificatul pe care doriţi să îl configuraţi din lista derulantă **Select the Certificate (Selectaţi certificatul)**.
7. Faceţi clic pe **Submit (Remitere)**.
8. Faceţi clic pe **Yes (Da)** pentru a reporni serverul de imprimare.

Informaţii similare

- Gestionarea aparatului în reţea în siguranţă folosind SSL/TLS

Subiecte conexe:

- Imprimarea securizată a documentelor utilizând SSL/TLS

Accesarea Web Based Management utilizând SSL/TLS

Pentru a administra în siguranță aparatul conectat la rețea, trebuie să folosiți utilitare de administrare cu protocoale de securitate.

- Pentru a utiliza protocolul HTTPS, este necesar ca HTTPS să fie activat la aparat. Protocolul HTTPS este activat în mod implicit.
- Puteţi modifica setările protocolului HTTPS utilizând ecranul Management bazat pe web.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. Acum puteţi accesa aparatul folosind HTTPS.

Informaţii similare

- Gestionarea aparatului în reţea în siguranţă folosind SSL/TLS

Instalarea certificatului autosemnat pentru utilizatorii Windows ca administratori

- Pașii următori sunt valabili pentru Microsoft Edge. Dacă folosiți un alt browser web, consultați documentația browserului web sau asistența online pentru instrucțiuni privind instalarea certificatelor.
- Asigurați-vă că ați creat certificatul cu semnătură automată folosind Web Based Management.

1. Faceți clic dreapta pe pictograma **Microsoft Edge** și apoi clic pe **Executare ca administrator**.

   Dacă se afişează ecranul **Control cont utilizator**, executaţi clic pe **Da**.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. În cazul în care conexiunea nu este privată, faceți clic pe butonul **Avansat** și apoi continuați cu pagina web.
4. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

5. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **Certificate (Certificat)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

6. Faceţi clic pe **Export**.
7. Pentru a cripta fișierul de ieșire, introduceți o parolă în câmpul **Enter password (Introduceţi parola)**. În cazul în care câmpul **Enter password (Introduceţi parola)** este necompletat, fişierul de ieşire nu va fi criptat.
8. Introduceţi din nou parola în câmpul **Retype password (Introduceţi din nou parola)** şi faceţi clic pe **Submit (Remitere)**.
9. Faceți clic pe fișierul descărcat pentru a-l deschide.
10. Când apare **Expertul Import certificate**, faceţi clic pe **Următorul**.
11. Faceţi clic pe **Următorul**.
12. Dacă este necesar, introduceți o parolă și apoi faceți clic pe **Următorul**.
13. Selectaţi **Plasează toate certificatele în următorul depozit** şi apoi faceţi clic pe **Răsfoire...**.
14. Selectați **Autorități rădăcină de certificare de încredere** și apoi faceți clic pe **OK**.
15. Faceţi clic pe **Următorul**.
16. Faceţi clic pe **Finalizare**.
17. Faceţi clic pe **Da**, dacă amprenta (imaginea degetului) este corectă.
18. Faceţi clic pe **OK**.

Informaţii similare

- Gestionarea aparatului în reţea în siguranţă folosind SSL/TLS

Imprimarea securizată a documentelor utilizând SSL/TLS

- Imprimarea documentelor folosind IPPS
- Configurarea unui certificat pentru SSL/TLS și protocoalele disponibile
- Configurarea certificatelor pentru securitatea dispozitivului

Imprimarea documentelor folosind IPPS

Pentru a imprima documentele în mod securizat prin protocolul IPP, utilizaţi protocolul IPPS.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Asiguraţi-vă că aţi selectat caseta de validare **IPP**.

   În cazul în care caseta de validare **IPP** nu este selectată, selectaţi caseta de validare **IPP** şi faceţi clic pe **Submit (Remitere)**.

   Reporniţi aparatul pentru a activa configurarea.

   După repornirea aparatului, reveniți la pagina web a aparatului, introduceți parola și apoi, în bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.
6. Faceţi clic pe **HTTP Server Settings (Setări server HTTP)**.
7. Bifați caseta de selectare **HTTPS(Port 443)** din zona **IPP**, apoi faceți clic pe **Submit (Remitere)**.
8. Reporniţi aparatul pentru a activa configurarea.

Comunicarea prin IPPS nu poate preveni accesul unauthorized la serverul de imprimare.

Informaţii similare

- Imprimarea securizată a documentelor utilizând SSL/TLS

Utilizarea SNMPv3

- Administrarea în siguranță a aparatului în rețea, utilizând SNMPv3

Administrarea în siguranță a aparatului în rețea, utilizând SNMPv3

Simple Network Management Protocol versiunea 3 (SNMPv3) asigură autentificarea utilizatorului și criptarea datelor pentru gestionarea în siguranță a dispozitivelor de rețea.

1. Porniţi browserul web.
2. Introduceţi „https://Nume comun” în bara de adrese a browser-ului (unde „Nume comun” este Numele comun atribuit certificatului; acesta poate fi adresa IP, numele nodului sau numele domeniului).
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Asiguraţi-vă că setarea **SNMP** este activată şi faceţi clic pe **Advanced Settings (Setări avansate)**.
6. Configurați setările modului SNMPv1/v2c.

Opţiune	Descriere
SNMP v1/v2c read-write access (Acces SNMP~v1/ v2c~citire~şi scriere)	Serverul de imprimare utilizează versiunile 1 și 2c ale protocolului SNMP. În acest mod puteți folosi toate aplicațiile aparatului dvs. Totuși, acest mod nu este securizat, deoarece nu va autentifica utilizatorul și datele nu vor fi criptate.
SNMP v1/v2c read-only access (SNMP v1/v2c acces doar la citire)	Serverul de imprimare utilizează accesul în regim doar pentru citire al versiunilor 1 și 2c ale protocolului SNMP.
Disabled (Inactiv)	Dezactivați versiunile 1 și 2c ale protocolului SNMP. Toate aplicațiile care utilizează SNMPv1/v2c vor fi restricționate. Pentru a permite utilizarea aplicațiilor SNMPv1/v2c, folosiți modul **SNMP v1/v2c read-only access (SNMP v1/v2c acces doar la citire)** sau **SNMP v1/v2c read-write access (Acces SNMP~v1/v2c~citire~şi scriere)**.

7. Configurați setările modului SNMPv3.

Opţiune	Descriere
Enabled (Activ)	Serverul de imprimare utilizează versiunea 3 a protocolului SNMP. Pentru a administra serverul de imprimare în condiții de siguranță, utilizați modul SNMPv3.
Disabled (Inactiv)	Dezactivați versiunea 3 a protocolului SNMP. Toate aplicațiile care utilizează SNMPv3 vor fi restricționate. Pentru a permite utilizarea aplicațiilor SNMPv3, folosiți modul SNMPv3.

8. Faceţi clic pe **Submit (Remitere)**.

Dacă aparatul afișează opțiunile de setare a protocolului, selectați opțiunile dorite.

9. Reporniţi aparatul pentru a activa configurarea.

Informaţii similare

- Utilizarea SNMPv3

Utilizarea IPsec

- Introducere în IPsec
- Configurarea IPsec utilizând Web Based Management
- Configurarea un şablon pentru adresă IPsec utilizând Web Based Management
- Configurarea un şablon IPsec utilizând Web Based Management

Introducere în IPsec

IPsec (Securitate protocol internet) este un protocol de securitate care utilizează o funcţie opţională a Protocolului Internet, pentru prevenirea manipulării datelor şi asigurarea confidenţialităţii datelor transmise ca pachete IP. IPsec criptează datele transmise printr-o rețea, cum ar fi datele imprimării trimise de la computere către o imprimantă. Deoarece datele sunt criptate la nivel de reţea, aplicaţiile care folosesc un protocol de nivel superior utilizează IPsec chiar dacă utilizatorul nu conştientizează acest lucru.

IPsec acceptă următoarele funcţii:

- Transmisii IPsec

  Conform condițiilor de configurare IPsec, computerul conectat la rețea transmite date și primește date de la dispozitivul specificat, utilizând IPsec. După ce dispozitivele încep să comunice utilizând IPsec, cheile se schimbă utilizând mai întâi Internet Key Exchange (Schimb chei Internet) (IKE), apoi datele criptate sunt transmise cu ajutorul cheilor.

  În plus, IPsec are două moduri de operare: modul Transport și modul Tunel. Modul Transport este utilizat în special pentru comunicarea între dispozitive iar modul Tunel este utilizat pentru medii precum Reţea privată virtuală (VPN).

Pentru transmisii IPsec sunt necesare următoarele condiţii:

- Un computer care poate comunica utilizând IPsec este conectat la reţea.
- Aparatul este configurat pentru comunicarea IPsec.
- Calculatorul conectat la aparat este configurat pentru conexiuni IPsec.

- Setările IPsec

  Setările necesare pentru conexiuni utilizând IPsec. Aceste setări pot fi configurate numai utilizând Web Based Management.

Pentru a configura setările IPsec, trebuie să utilizaţi browserul de pe un computer care este conectat la reţea.

Informaţii similare

- Utilizarea IPsec

Configurarea IPsec utilizând Web Based Management

Condiţiile de conectare IPsec includ două tipuri de **Template (Şablon)**: **Address (Adresă)** şi **IPsec**. Puteţi seta până la 10 condiţii de conectare.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **IPsec**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Configuraţi setările.

Opţiune	Descriere
Status (Stare)	Activaţi sau dezactivaţi IPSec.
Negotiation Mode (Mod de negociere)	Selectaţi **Negotiation Mode (Mod de negociere)** pentru IKE Phase 1. IKE este un protocol utilizat pentru a schimba chei de criptare pentru a efectua o comunicare criptată utilizând IPsec. În modul **Main (Principal)**, viteza de procesare este mică, dar nivelul de securitate este ridicat. În modul **Aggressive (Agresiv)**, viteza de procesare este mai mare decât în modul **Main (Principal)**, dar nivelul de securitate este mai mic.
All Non-IPsec Traffic (Tot traficul non-IPsec)	Selectați acțiunea care va fi efectuată pentru pachetele non-IPsec. La utilizarea protocolului Servicii web, trebuie să selectaţi **Allow (Permiteţi)** pentru **All Non-IPsec Traffic (Tot traficul non-IPsec)**. Dacă aţi selectat **Drop (Renunţaţi)**, protocolul Servicii web nu poate fi utilizat.
Broadcast/Multicast Bypass (Bypass transmisie/difuzare multiplă)	Selectaţi **Enabled (Activ)** sau **Disabled (Inactiv)**.
Protocol Bypass (Bypass protocol)	Bifați casetele de selectare pentru opțiunea sau opțiunile pe care le doriți.
Rules (Reguli)	Pentru a activa acest şablon, bifaţi caseta de validare **Enabled (Activ)**. Atunci când selectaţi mai multe casete de validare, casetele de validare cu numerele mai mici sunt prioritare dacă setările pentru casetele de validare selectate sunt în conflict. Faceți clic pe lista derulantă corespunzătoare pentru a selecta **Address Template (Şablon adresă)** utilizată pentru condițiile de conexiune IPsec. Pentru a adăuga **Address Template (Şablon adresă)**, face clic pe **Add Template (Adăugare şablon)**. Faceți clic pe lista derulantă corespunzătoare pentru a selecta **IPsec Template (Şablon IPsec)** utilizată pentru condițiile de conexiune IPsec. Pentru a adăuga **IPsec Template (Şablon IPsec)**, face clic pe **Add Template (Adăugare şablon)**.

6. Faceţi clic pe **Submit (Remitere)**.

În cazul în care aparatul trebuie repornit pentru a înregistra noile setări, va fi afișat ecranul de confirmare a repornirii.

Dacă există un element gol în şablonul activat în tabelul **Rules (Reguli)**, pe ecran va fi afișat un mesaj de eroare. Confirmaţi alegerile şi faceți din nou clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea IPsec

Subiecte conexe:

- Configurarea certificatelor pentru securitatea dispozitivului

Configurarea un şablon pentru adresă IPsec utilizând Web Based Management

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **IPsec Address Template (Şablon adresă IPsec)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Faceți clic pe butonul **Delete (Ştergere)** pentru a șterge un **Address Template (Şablon adresă)**. Atunci când **Address Template (Şablon adresă)** este utilizată, aceasta nu poate fi ştearsă.
6. Faceţi clic pe **Address Template (Şablon adresă)** pe care doriţi să o creaţi. Este afişat ecranul **IPsec Address Template (Şablon adresă IPsec)**.
7. Configuraţi setările.

Opţiune	Descriere
Template Name (Nume şablon)	Introduceţi un nume pentru şablon (până la 16 caractere).
Local IP Address (Adresă IP locală)	• **IP Address (Adresa IP)** Specificaţi adresa IP. Selectaţi **ALL IPv4 Address (TOATE adresele IPv4)**, **ALL IPv6 Address (TOATE adresele IPv6)**, **ALL Link Local IPv6 (Toate linkurile IPv6 locale)** sau **Custom (Personalizat)** din lista derulantă. Dacă aţi selectat **Custom (Personalizat)** din lista derulantă, tastaţi adresa IP (IPv4 sau IPv6) în caseta de text. • **IP Address Range (Interval de adrese IP)** Introduceţi adresele IP de început şi de sfârşit, pentru intervalul de adrese IP din casetele de text. Dacă adresele IP de început şi de sfârşit nu sunt standardized conform IPv4 sau IPv6, sau dacă adresa de sfârşit are alocat un număr mai mic decât adresa de început, va apărea o eroare. • **IP Address / Prefix (Adresă IP/prefix)** Specificaţi adresa IP utilizând sistemul de notare CIDR. De exemplu: 192.168.1.1/24 Deoarece prefixul este specificat în forma unei măști de subrețea de 24 de biți (255.255.255.0) pentru 192.168.1.1, sunt valide adresele 192.168.1.###.
Remote IP Address (Adresă IP la distanţă)	• **Any (Oricare)** Dacă aţi selectat **Any (Oricare)**, sunt activate toate adresele IP. • **IP Address (Adresa IP)** Tastaţi adresa IP specificată (IPv4 sau IPv6) în caseta de text. • **IP Address Range (Interval de adrese IP)**

Opţiune	Descriere
	Introduceți prima adresă și ultima adresă IP pentru intervalul de adrese IP. Dacă prima adresă și ultima adresă IP nu sunt standardized conform IPv4 sau IPv6 sau dacă ultima adresă IP are alocat un număr mai mic decât prima adresă, va apărea o eroare. • **IP Address / Prefix (Adresă IP/prefix)** Specificaţi adresa IP utilizând sistemul de notare CIDR. De exemplu: 192.168.1.1/24 Deoarece prefixul este specificat în forma unei măști de subrețea de 24 de biți (255.255.255.0) pentru 192.168.1.1, sunt valide adresele 192.168.1.###.

8. Faceţi clic pe **Submit (Remitere)**.

La modificarea setărilor pentru șablonul aflat în uz, reporniți aparatul pentru a activa configurația.

Informaţii similare

- Utilizarea IPsec

Configurarea un şablon IPsec utilizând Web Based Management

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Security (Securitate)** > **IPsec Template (Şablon IPsec)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Faceți clic pe butonul **Delete (Ştergere)** pentru a șterge un **IPsec Template (Şablon IPsec)**. Atunci când **IPsec Template (Şablon IPsec)** este utilizată, aceasta nu poate fi ştearsă.
6. Faceți clic pe **IPsec Template (Şablon IPsec)** pe care doriți să îl creați. Apare ecranul **IPsec Template (Şablon IPsec)**. Câmpurile de configurare diferă în funcție de setările **Use Prefixed Template (Utilizare şablon cu prefix)** și **Internet Key Exchange (IKE) (Schimb de chei internet (IKE))** pe care le selectați.
7. În câmpul **Template Name (Nume şablon)**, tastaţi un nume pentru şablon (până la 16 caractere).
8. Dacă aţi selectat **Custom (Personalizat)** în lista derulantă **Use Prefixed Template (Utilizare şablon cu prefix)**, selectaţi opţiunile **Internet Key Exchange (IKE) (Schimb de chei internet (IKE))** şi modificaţi setările, dacă este necesar.
9. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea IPsec
  - Setări IKEv1 pentru un şablon IPsec
  - Setări IKEv2 pentru un şablon IPsec
  - Setări manuale pentru un şablon IPsec

Setări IKEv1 pentru un şablon IPsec

Opţiune	Descriere
Template Name (Nume şablon)	Introduceți un nume pentru șablon (până la 16 caractere).
Use Prefixed Template (Utilizare şablon cu prefix)	Selectaţi **Custom (Personalizat)**, **IKEv1 High Security (Securitate~ridicată~IKEv1)** sau **IKEv1 Medium Security (Securitate~medie~IKEv1)**. Elementele de setare sunt diferite în funcţie de şablonul selectat.
Internet Key Exchange (IKE) (Schimb de chei internet (IKE))	IKE este un protocol de comunicare utilizat pentru a schimba chei de criptare pentru a efectua o comunicare criptată utilizând IPsec. Pentru a efectua o comunicare criptată, algoritmul de criptare necesar pentru IPsec este determinat şi cheile de criptare sunt partajate. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda Diffie-Hellman de schimbare a cheilor, iar comunicarea criptată limitată la IKE este efectuată. Dacă aţi selectat **Custom (Personalizat)** în **Use Prefixed Template (Utilizare şablon cu prefix)**, selectaţi **IKEv1**.
Authentication Type (Tip de autentificare)	• **Diffie-Hellman Group (Grupul Diffie-Hellman)** Această metodă de schimbare a cheilor permite cheilor secrete să fie schimbate în mod securizat prin intermediul unei reţele neprotejate. Metoda Diffie-Hellman de schimbare a cheilor utilizează o problemă cu algoritmi discreți, nu cheia secretă, pentru a trimite şi primi informaţii neprotejate generate utilizând un număr aleatoriu şi cheia secretă. Selectați **Group1 (Grup1)**, **Group2 (Grup2)**, **Group5 (Grup5)** sau **Group14 (Grup14)**. • **Encryption (Criptare)** Selectați **DES**, **3DES**, **AES-CBC 128** sau **AES-CBC 256**. • **Hash** Selectați **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**. • **SA Lifetime (Durată de viaţă SA)** Specificaţi durata de viaţă IKE SA. Introduceţi timpul (secunde) şi numărul de kilobaiți (KByte).
Encapsulating Security (Se încapsulează securitatea)	• **Protocol** Selectaţi **ESP**, **AH** sau **AH+ESP**. - ESP este un protocol pentru efectuarea comunicaţiilor criptate utilizând IPsec. ESP criptează sarcina (conţinutul comunicat) şi adaugă informaţii suplimentare. Pachetul IP conţine antetul şi sarcina criptată, care urmează după antet. Suplimentar, pe lângă datele criptate, pachetul IP include şi informaţii referitoare la metoda de criptare şi cheia de criptare, datele de autentificare şi altele. - AH face parte din protocolul IPsec care autentifică expeditorul şi previne manipularea datelor (asigură completitudinea datelor). În pachetul IP, datele sunt introduse imediat după header. În plus, pachetele includ valori hash care sunt calculate utilizând o ecuaţie din conţinutul comunicat, cheia secretă şi altele, pentru a preveni falsificarea expeditorului şi manipularea datelor. Spre deosebire de ESP, conţinutul comunicat nu este criptat, iar datele sunt trimise şi primite ca text simplu. • **Encryption (Criptare) (Nu este disponibilă pentru opțiunea AH.)** Selectați **DES**, **3DES**, **AES-CBC 128** sau **AES-CBC 256**.

Opţiune	Descriere
	• **Hash** Selectaţi **None (Niciunul)**, **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**. Opțiunea **None (Niciunul)** poate fi selectată doar dacă opțiunea **ESP** este selectată pentru **Protocol**. • **SA Lifetime (Durată de viaţă SA)** Specificaţi durata de viaţă a IKE SA. Tastaţi durata (secunde) şi numărul de kilobiţi (Kbyte). • **Encapsulation Mode (Mod de încapsulare)** Selectaţi **Transport** sau **Tunnel (Tunel)**. • **Remote Router IP-Address (Adresă IP router la distanţă)** Introduceţi adresa IP (IPv4 sau IPv6) a routerului aflat la distanţă. Introduceţi aceste informaţii doar atunci când modul **Tunnel (Tunel)** este selectat. SA (asociere de securitate) este o metodă de comunicare criptare care utilizează IPsec sau IPv6 şi care schimbă şi partajează informaţii precum metoda de criptare şi cheia de criptare, pentru a stabili un canal de comunicare securizat înainte de a efectua comunicarea. De asemenea, SA se poate referi la un canal de comunicare criptat virtual care a fost stabilit. SA utilizat pentru IPsec stabileşte metoda de criptare, schimbă cheile şi efectuează autentificarea reciprocă în conformitate cu procedura standard IKE (Schimb de chei prin Internet). În plus, SA este actualizat periodic.
Perfect Forward Secrecy (PFS) (Redirecţionare perfectă a confidenţialităţii (PFS))	PFS nu derivează cheile din cheile anterioare care au fost utilizate pentru a cripta mesajele. În plus, dacă o cheie utilizată pentru criptarea unui mesaj a fost derivată dintr-o cheie-părinte, acea cheie-părinte nu este utilizată pentru derivarea altor chei. În consecință, chiar dacă o cheie este compromisă, daunele vor fi limitate doar la mesajele care au fost criptate utilizând acea cheie. Selectaţi **Enabled (Activ)** sau **Disabled (Inactiv)**.
Authentication Method (Metodă de autentificare)	Selectaţi metoda de autentificare. Selectaţi **Pre-Shared Key (Cheie prepartajată)** sau **Certificates (Certificate)**.
Pre-Shared Key (Cheie prepartajată)	Dacă se criptează comunicarea, cheia de criptare este schimbată și partajată înainte de a utiliza alt canal. Dacă aţi selectat **Pre-Shared Key (Cheie prepartajată)** pentru **Authentication Method (Metodă de autentificare)**, tastaţi **Pre-Shared Key (Cheie prepartajată)** (până la 32 de caractere). • **Local/ID Type/ID (Local/Tip ID/ID)** Selectaţi tipul ID-ului expeditorului şi apoi tastaţi ID-ul. Selectaţi **IPv4 Address (Adresă IPv4)**, **IPv6 Address (Adresă IPv6)**, **FQDN**, **E-mail Address (Adresă de e-mail)** sau **Certificate (Certificat)** pentru tip. Dacă aţi selectat **Certificate (Certificat)**, tastaţi numele comun al certificatului în câmpul **ID**. • **Remote/ID Type/ID (La distanţă/Tip ID/ID)** Selectaţi tipul ID-ului destinatarului şi apoi tastaţi ID-ul. Selectaţi **IPv4 Address (Adresă IPv4)**, **IPv6 Address (Adresă IPv6)**, **FQDN**, **E-mail Address (Adresă de e-mail)** sau **Certificate (Certificat)** pentru tip. Dacă aţi selectat **Certificate (Certificat)**, tastaţi numele comun al certificatului în câmpul **ID**.
Certificate (Certificat)	Dacă aţi selectat **Certificates (Certificate)** pentru **Authentication Method (Metodă de autentificare)**, selectaţi certificatul.

Opţiune	Descriere
	Puteți să selectați numai certificatele care au fost create folosind pagina **Certificate (Certificat)** a ecranului de configurare a securității pentru Web Based Management.

Informaţii similare

- Configurarea un şablon IPsec utilizând Web Based Management

Setări IKEv2 pentru un şablon IPsec

Opţiune	Descriere
Template Name (Nume şablon)	Introduceți un nume pentru șablon (până la 16 caractere).
Use Prefixed Template (Utilizare şablon cu prefix)	Selectaţi **Custom (Personalizat)**, **IKEv2 High Security (Securitate~ridicată~IKEv2)**, sau **IKEv2 Medium Security (Securitate~medie~IKEv2)**. Elementele de setare sunt diferite în funcţie de şablonul selectat.
Internet Key Exchange (IKE) (Schimb de chei internet (IKE))	IKE este un protocol de comunicare utilizat pentru a schimba chei de criptare pentru a efectua o comunicare criptată utilizând IPsec. Pentru a efectua o comunicare criptată, algoritmul de criptare necesar pentru IPsec este determinat şi cheile de criptare sunt partajate. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda Diffie-Hellman de schimbare a cheilor, iar comunicarea criptată limitată la IKE este efectuată. Dacă aţi selectat **Custom (Personalizat)** în **Use Prefixed Template (Utilizare şablon cu prefix)**, selectaţi **IKEv2**.
Authentication Type (Tip de autentificare)	• **Diffie-Hellman Group (Grupul Diffie-Hellman)** Această metodă de schimbare a cheilor permite cheilor secrete să fie schimbate în mod securizat prin intermediul unei reţele neprotejate. Metoda Diffie-Hellman de schimbare a cheilor utilizează o problemă cu algoritmi discreți, nu cheia secretă, pentru a trimite şi primi informaţii neprotejate generate utilizând un număr aleatoriu şi cheia secretă. Selectați **Group1 (Grup1)**, **Group2 (Grup2)**, **Group5 (Grup5)** sau **Group14 (Grup14)**. • **Encryption (Criptare)** Selectați **DES**, **3DES**, **AES-CBC 128** sau **AES-CBC 256**. • **Hash** Selectați **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**. • **SA Lifetime (Durată de viaţă SA)** Specificaţi durata de viaţă IKE SA. Introduceţi timpul (secunde) şi numărul de kilobaiți (KByte).
Encapsulating Security (Se încapsulează securitatea)	• **Protocol** Selectaţi **ESP**. ESP este un protocol pentru efectuarea comunicaţiilor criptate utilizând IPsec. ESP criptează sarcina (conţinutul comunicat) şi adaugă informaţii suplimentare. Pachetul IP conţine antetul şi sarcina criptată, care urmează după antet. Suplimentar, pe lângă datele criptate, pachetul IP include şi informaţii referitoare la metoda de criptare şi cheia de criptare, datele de autentificare şi altele. • **Encryption (Criptare)** Selectaţi **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**. • **Hash** Selectați **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**. • **SA Lifetime (Durată de viaţă SA)** Specificaţi durata de viaţă a IKE SA. Tastaţi durata (secunde) şi numărul de kilobiţi (Kbyte). • **Encapsulation Mode (Mod de încapsulare)** Selectaţi **Transport** sau **Tunnel (Tunel)**.

Opţiune	Descriere
	• **Remote Router IP-Address (Adresă IP router la distanţă)** Introduceţi adresa IP (IPv4 sau IPv6) a routerului aflat la distanţă. Introduceţi aceste informaţii doar atunci când modul **Tunnel (Tunel)** este selectat. SA (asociere de securitate) este o metodă de comunicare criptare care utilizează IPsec sau IPv6 şi care schimbă şi partajează informaţii precum metoda de criptare şi cheia de criptare, pentru a stabili un canal de comunicare securizat înainte de a efectua comunicarea. De asemenea, SA se poate referi la un canal de comunicare criptat virtual care a fost stabilit. SA utilizat pentru IPsec stabileşte metoda de criptare, schimbă cheile şi efectuează autentificarea reciprocă în conformitate cu procedura standard IKE (Schimb de chei prin Internet). În plus, SA este actualizat periodic.
Perfect Forward Secrecy (PFS) (Redirecţionare perfectă a confidenţialităţii (PFS))	PFS nu derivează cheile din cheile anterioare care au fost utilizate pentru a cripta mesajele. În plus, dacă o cheie utilizată pentru criptarea unui mesaj a fost derivată dintr-o cheie-părinte, acea cheie-părinte nu este utilizată pentru derivarea altor chei. În consecință, chiar dacă o cheie este compromisă, daunele vor fi limitate doar la mesajele care au fost criptate utilizând acea cheie. Selectaţi **Enabled (Activ)** sau **Disabled (Inactiv)**.
Authentication Method (Metodă de autentificare)	Selectaţi metoda de autentificare. Selectați **Pre-Shared Key (Cheie prepartajată)**, **Certificates (Certificate)**, **EAP - MD5** sau **EAP - MS-CHAPv2**. EAP este un protocol de autentificare care este o extensie a PPP. Prin utilizarea EAP cu IEEE802.1x, se utilizează o cheie diferită pentru autentificarea utilizatorului în timpul fiecărei sesiuni. Setările următoare sunt necesare doar atunci când este selectat **EAP - MD5** sau **EAP - MS-CHAPv2** din **Authentication Method (Metodă de autentificare)**: • **Mode (Mod)** Selectaţi **Server-Mode (Mod server)** sau **Client-Mode (Mod client)**. • **Certificate (Certificat)** Selectaţi certificatul. • **User Name (Nume utilizator)** Introduceţi un nume de utilizator (până la 32 caractere). • **Password (Parola)** Introduceţi o parolă (până la 32 caractere). Parola trebuie introdusă de două ori pentru confirmare.
Pre-Shared Key (Cheie prepartajată)	Dacă se criptează comunicarea, cheia de criptare este schimbată și partajată înainte de a utiliza alt canal. Dacă aţi selectat **Pre-Shared Key (Cheie prepartajată)** pentru **Authentication Method (Metodă de autentificare)**, tastaţi **Pre-Shared Key (Cheie prepartajată)** (până la 32 de caractere). • **Local/ID Type/ID (Local/Tip ID/ID)** Selectaţi tipul ID-ului expeditorului şi apoi tastaţi ID-ul. Selectaţi **IPv4 Address (Adresă IPv4)**, **IPv6 Address (Adresă IPv6)**, **FQDN**, **E-mail Address (Adresă de e-mail)** sau **Certificate (Certificat)** pentru tip. Dacă aţi selectat **Certificate (Certificat)**, tastaţi numele comun al certificatului în câmpul **ID**.

Opţiune	Descriere
	• **Remote/ID Type/ID (La distanţă/Tip ID/ID)** Selectaţi tipul ID-ului destinatarului şi apoi tastaţi ID-ul. Selectaţi **IPv4 Address (Adresă IPv4)**, **IPv6 Address (Adresă IPv6)**, **FQDN**, **E-mail Address (Adresă de e-mail)** sau **Certificate (Certificat)** pentru tip. Dacă aţi selectat **Certificate (Certificat)**, tastaţi numele comun al certificatului în câmpul **ID**.
Certificate (Certificat)	Dacă aţi selectat **Certificates (Certificate)** pentru **Authentication Method (Metodă de autentificare)**, selectaţi certificatul. Puteți să selectați numai certificatele care au fost create folosind pagina **Certificate (Certificat)** a ecranului de configurare a securității pentru Web Based Management.

Informaţii similare

- Configurarea un şablon IPsec utilizând Web Based Management

Setări manuale pentru un şablon IPsec

Opţiune	Descriere
Template Name (Nume şablon)	Introduceți un nume pentru șablon (până la 16 caractere).
Use Prefixed Template (Utilizare şablon cu prefix)	Selectaţi **Custom (Personalizat)**.
Internet Key Exchange (IKE) (Schimb de chei internet (IKE))	IKE este un protocol de comunicare utilizat pentru a schimba chei de criptare pentru a efectua o comunicare criptată utilizând IPsec. Pentru a efectua o comunicare criptată, algoritmul de criptare necesar pentru IPsec este determinat şi cheile de criptare sunt partajate. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda Diffie-Hellman de schimbare a cheilor, iar comunicarea criptată limitată la IKE este efectuată. Selectaţi **Manual**.
Authentication Key (ESP, AH) (Cheie de autentificare (ESP, AH))	Tastaţi valorile **In/Out (Intrare/Ieşire)**. Aceste setări sunt necesare atunci când se selectează **Custom (Personalizat)** pentru **Use Prefixed Template (Utilizare şablon cu prefix)**, **Manual** pentru **Internet Key Exchange (IKE) (Schimb de chei internet (IKE))** şi o setare diferită de **None (Niciunul)** este selectată pentru **Hash** pentru **Encapsulating Security (Se încapsulează securitatea)**. Numărul de caractere pe care îl puteţi seta diferă în funcţie de setarea pe care o alegeţi pentru **Hash** pentru secţiunea **Encapsulating Security (Se încapsulează securitatea)**. Dacă lungimea cheii de autentificare specificate diferă de algoritmul hash selectat, va apărea o eroare. • **MD5**: 128 biţi (16 bytes) • **SHA1**: 160 biţi (20 bytes) • **SHA256**: 256 biţi (32 bytes) • **SHA384**: 384 biţi (48 bytes) • **SHA512**: 512 biţi (64 bytes) Dacă specificaţi cheia în Cod ASCII, scrieţi caracterele între ghilimele (").
Code key (ESP) (Cheie cod (ESP))	Tastaţi valorile **In/Out (Intrare/Ieşire)**. Aceste setări sunt necesare dacă **Custom (Personalizat)** este selectat pentru **Use Prefixed Template (Utilizare şablon cu prefix)**, **Manual** este selectat pentru **Internet Key Exchange (IKE) (Schimb de chei internet (IKE))** și **ESP** este selectat pentru **Protocol** în **Encapsulating Security (Se încapsulează securitatea)**. Numărul de caractere pe care îl puteţi seta diferă în funcţie de setarea pe care o alegeţi pentru **Encryption (Criptare)** pentru secţiunea **Encapsulating Security (Se încapsulează securitatea)**. Dacă lungimea cheii de cod specificate diferă de algoritmul de criptare selectat, va apărea o eroare. • **DES**: 64 biţi (8 bytes) • **3DES**: 192 biţi (24 bytes) • **AES-CBC 128**: 128 biţi (16 bytes) • **AES-CBC 256**: 256 biţi (32 bytes) Dacă specificaţi cheia în Cod ASCII, scrieţi caracterele între ghilimele (").

Opţiune	Descriere
SPI	Aceşti parametri sunt utilizaţi pentru a identifica informaţiile de securitate. În general, o gazdă are mai multe Asocieri de securitate (SAs) pentru mai multe tipuri de comunicări IPsec. Prin urmare, este necesară identificarea SA aplicabil atunci când este primit un pachet IPsec. Parametrul SPI, care identifică SA, este inclus în AH Headerul de autentificare (AH) şi în headerul Încărcăturii utile a securităţii încapsulării (ESP). Aceste setări sunt necesare atunci când se selectează **Custom (Personalizat)** pentru **Use Prefixed Template (Utilizare şablon cu prefix)**, şi **Manual** pentru **Internet Key Exchange (IKE) (Schimb de chei internet (IKE))**. Introduceţi valorile **In/Out (Intrare/Ieşire)**. (3-10 caractere)
Encapsulating Security (Se încapsulează securitatea)	• **Protocol** Selectaţi **ESP** sau **AH**. - ESP este un protocol pentru efectuarea comunicaţiilor criptate utilizând IPsec. ESP criptează sarcina (conţinutul comunicat) şi adaugă informaţii suplimentare. Pachetul IP conţine antetul şi sarcina criptată, care urmează după antet. Suplimentar, pe lângă datele criptate, pachetul IP include şi informaţii referitoare la metoda de criptare şi cheia de criptare, datele de autentificare şi altele. - AH face parte din protocolul IPsec care autentifică expeditorul şi previne manipularea datelor (asigură completitudinea datelor). În pachetul IP, datele sunt introduse imediat după header. În plus, pachetele includ valori hash care sunt calculate utilizând o ecuaţie din conţinutul comunicat, cheia secretă şi altele, pentru a preveni falsificarea expeditorului şi manipularea datelor. Spre deosebire de ESP, conţinutul comunicat nu este criptat şi datele sunt trimise şi primite ca text simplu. • **Encryption (Criptare) (Nu este disponibilă pentru opțiunea AH.)** Selectați **DES**, **3DES**, **AES-CBC 128** sau **AES-CBC 256**. • **Hash** Selectaţi **None (Niciunul)**, **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**. Opțiunea **None (Niciunul)** poate fi selectată doar dacă opțiunea **ESP** este selectată pentru **Protocol**. • **SA Lifetime (Durată de viaţă SA)** Specificaţi durata de viaţă a IKE SA. Tastaţi durata (secunde) şi numărul de kilobiţi (Kbyte). • **Encapsulation Mode (Mod de încapsulare)** Selectaţi **Transport** sau **Tunnel (Tunel)**. • **Remote Router IP-Address (Adresă IP router la distanţă)** Introduceţi adresa IP (IPv4 sau IPv6) a routerului aflat la distanţă. Introduceţi aceste informaţii doar atunci când modul **Tunnel (Tunel)** este selectat.

Opţiune	Descriere
	SA (asociere de securitate) este o metodă de comunicare criptare care utilizează IPsec sau IPv6 şi care schimbă şi partajează informaţii precum metoda de criptare şi cheia de criptare, pentru a stabili un canal de comunicare securizat înainte de a efectua comunicarea. De asemenea, SA se poate referi la un canal de comunicare criptat virtual care a fost stabilit. SA utilizat pentru IPsec stabileşte metoda de criptare, schimbă cheile şi efectuează autentificarea reciprocă în conformitate cu procedura standard IKE (Schimb de chei prin Internet). În plus, SA este actualizat periodic.

Informaţii similare

- Configurarea un şablon IPsec utilizând Web Based Management

Utilizarea autentificării IEEE 802.1x pentru rețeaua dumneavoastră

- Ce este autentificarea IEEE 802.1x?
- Configurați autentificarea IEEE 802.1x pentru rețeaua dumneavoastră utilizând Web Based Management (browser web)
- Metode de autentificare IEEE 802.1x

Ce este autentificarea IEEE 802.1x?

IEEE 802.1x este un standard IEEE care limitează accesul de la dispozitive de rețea unauthorized. Aparatul Brother trimite o cerere de autentificare către un server RADIUS (server de autentificare) prin punctul de acces sau hubul dvs. Aparatul poate accesa rețeaua după ce serverul RADIUS verifică solicitarea dumneavoastră.

Informaţii similare

- Utilizarea autentificării IEEE 802.1x pentru rețeaua dumneavoastră

Configurați autentificarea IEEE 802.1x pentru rețeaua dumneavoastră utilizând Web Based Management (browser web)

- În cazul în care configuraţi aparatul folosind autentificarea EAP-TLS, trebuie să instalaţi certificatul de client emis de AC înainte de a începe configurarea. Contactaţi administratorul de reţea pentru informaţii despre certificatul de client. Dacă aveţi instalate mai multe certificate, vă recomandăm să vă notaţi numele certificatului pe care doriţi să îl utilizaţi.
- Înainte de a verifica certificatul serverului, trebuie să importaţi certificatul AC emis de AC care a semnat certificatul serverului. Contactaţi administratorul de reţea sau furnizorul de servicii internet (ISP) pentru a confirma dacă este necesar să importaţi certificatul AC.

De asemenea, puteți configura autentificarea IEEE 802.1x utilizând expertul de setare wireless din panoul de control (rețea wireless).

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Efectuaţi una dintre următoarele operaţii:
   - Pentru rețea cablată

     Faceţi clic pe **Wired (Cu fir)** > **Wired 802.1x Authentication (Autentificare 802.1x cu fir)**.
   - Pentru rețea wireless

     Faceţi clic pe **Wireless (Fără fir)** > **Wireless (Enterprise) (Fără fir (întreprindere))**.
6. Configuraţi setările de autentificare IEEE 802.1x.

- Pentru activarea autentificării IEEE 802.1x pentru reţele prin cablu, selectaţi **Enabled (Activat)** pentru **Wired 802.1x status (Stare 802.1x cu fir)** în pagina **Wired 802.1x Authentication (Autentificare 802.1x cu fir)**.
- Dacă utilizați autentificarea **EAP-TLS**, pentru verificare trebuie să selectați certificatul de client instalat (afișat cu numele certificatului) din lista derulantă **Client Certificate (Certificat client)**.
- Dacă selectaţi autentificarea **EAP-FAST**, **PEAP**, **EAP-TTLS**, sau **EAP-TLS**, selectaţi metoda de verificare din lista derulantă **Server Certificate Verification (Verificare certificat server)**. Verificați certificatul serverului utilizând certificatul CA, importat anterior pe aparat, emis de autoritatea de certificare (CA) care a semnat certificatul serverului.

Selectaţi una dintre următoarele metode de verificare din lista derulantă **Server Certificate Verification (Verificare certificat server)**:

Opţiune	Descriere
No Verification (Fără verificare)	Certificatul serverului este întotdeauna de încredere. Verificarea nu se efectuează.
CA Cert. (Cert. CA)	Metoda de control folosită pentru verificarea siguranței CA a certificatului serverului utilizând certificatul CA emis de autoritatea de certificare (CA) care a semnat certificatul serverului.
CA Cert. + ServerID (Cert. CA + ID server)	Metoda de verificare a valorii numelui comun [1] a certificatului serverului în completarea siguranţei CA a certificatului serverului.

7. După ce aţi terminat configurarea, faceţi clic pe **Submit (Remitere)**.

   Pentru reţelele cablate: după configurare, conectaţi aparatul la reţeaua IEEE 802.1x acceptată. După câteva minute, imprimați pagina cu raportul de configurare rețea pentru a verifica starea <**Wired IEEE 802.1x**>.

Opţiune	Descriere
Success	Funcţia IEEE 802.1x prin cablu este activată şi autentificarea a reuşit.
Failed	Funcţia IEEE 802.1x prin cablu este activată, însă autentificarea nu a reuşit.
Off	Funcţia IEEE 802.1x prin cablu nu este disponibilă.

Informaţii similare

- Utilizarea autentificării IEEE 802.1x pentru rețeaua dumneavoastră

Subiecte conexe:

- Prezentarea funcțiilor certificatului de securitate
- Configurarea certificatelor pentru securitatea dispozitivului

1 La verificarea numelui comun se compară numele comun al certificatului serverului cu şirul de caractere configurat pentru **Server ID (ID server)**. Înainte de a utiliza această metodă, contactaţi administratorul de sistem privind numele comun al certificatului serverului şi apoi configuraţi **Server ID (ID server)**.

Metode de autentificare IEEE 802.1x

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) a fost realizat de Cisco Systems, Inc. şi utilizează un identificator de utilizator şi o parolă pentru autentificare, precum şi algoritmi cu chei simetrice pentru a se obţine un proces de autentificare tunneled.

Aparatul Brother acceptă următoarele metode de autentificare internă:

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

EAP-MD5 (Rețea cablată)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) utilizează un ID utilizator şi parolă pentru autentificarea cu răspuns la cerere.

PEAP

Protected Extensible Authentication Protocol (PEAP) este o versiune a metodei EAP dezvoltată de Cisco Systems, Inc., Microsoft Corporation şi RSA Security. PEAP creează un canal SSL (Secure Sockets Layer)/TLS (Transport Layer Security) criptat între un client şi un server de autentificare pentru a trimite ID-ul de utilizator şi parola. PEAP asigură autentificarea reciprocă între server şi client.

Aparatul Brother acceptă următoarele metode de autentificare internă:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) a fost dezvoltat de Funk Software și Certicom. EAP-TTLS creează un canal SSL criptat similar cu PEAP între un client și un server de autentificare pentru a trimite ID-ul de utilizator și parola. EAP-TTLS asigură autentificarea reciprocă între server şi client.

Aparatul Brother acceptă următoarele metode de autentificare internă:

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

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) solicită autentificarea certificatului digital atât pentru client cât şi pentru serverul de autentificare.

Informaţii similare

- Utilizarea autentificării IEEE 802.1x pentru rețeaua dumneavoastră

Autentificarea utilizatorului

- Utilizarea autentificării Active Directory
- Utilizarea autentificării prin LDAP
- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Utilizarea autentificării Active Directory

- Introducere în autentificarea Active Directory
- Configurarea autentificării Active Directory utilizând Management bazat pe web
- Autentificarea pentru a modifica setările aparatului utilizând panoul de control al aparatului (autentificare Active Directory)

Introducere în autentificarea Active Directory

Autentificarea Active Directory restricționează utilizarea aparatului. Dacă autentificarea Active Directory este activată, panoul de control al aparatului va fi blocat. Nu puteţi schimba setările aparatului până când nu introduceţi un ID de utilizator şi o parolă.

Autentificarea Active Directory oferă următoarele caracteristici:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

- Stochează datele de imprimare primite
- Stochează datele de fax primite
- Obţine adresa de e-mail de la serverul Active Directory pe baza codului de identificare al utilizatorului (ID) la trimiterea datelor scanate către un server de e-mail.

  Pentru a utiliza această caracteristică, selectați opțiunea **On (Pornit)** pentru setarea **Get Mail Address (Obţinere adresă de e-mail)** și **LDAP + kerberos** sau **LDAP + NTLMv2** pentru metoda de autentificare. Adresa dumneavoastră de e-mail va fi setată ca expeditor atunci când aparatul trimite date scanate la un server de e-mail, respectiv ca destinatar dacă doriţi să trimiteţi datele scanate la adresa dumneavoastră de e-mail.

Atunci când autentificarea Active Directory Authentication este activată, aparatul dvs. stochează toate datele faxurilor primite. După ce vă autentificaţi, aparatul va imprima toate datele faxurilor stocate.

Puteți modifica setările folosite pentru autentificarea Active Directory utilizând Web Based Management.

Informaţii similare

- Utilizarea autentificării Active Directory

Configurarea autentificării Active Directory utilizând Management bazat pe web

Autentificarea în Active Directory acceptă autentificarea Kerberos şi autentificarea NTLMv2. Trebuie să configuraţi protocolul SNTP (server de oră reţea) şi să configuraţi serverul DNS pentru autentificare.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **User Restriction Function (Funcţie restricţie utilizator)** sau pe **Restriction Management (Gestionare restricţii)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi **Active Directory Authentication (Autentificare director activ)**.
6. Faceţi clic pe **Submit (Remitere)**.
7. Faceţi clic pe **Active Directory Authentication (Autentificare director activ)**.
8. Configuraţi setările următoare:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

Opţiune	Descriere
Storage Fax RX Data (Stocare date retransmitere fax)	Selectaţi această opţiune pentru a stoca datele de fax primite. Puteţi imprima toate datele de fax primite după ce vă autentificaţi la aparat.
Remember User ID (Memorare ID utilizator)	Selectaţi această opţiune pentru a vă salva ID-ul de utilizator.
Active Directory Server Address (Adresă server director activ)	Introduceţi adresa IP sau numele serverului (de exemplu: ad.example.com) Active Directory.
Active Directory Domain Name (Nume domeniu director activ)	Introduceţi Numele domeniului Active Directory.
Protocol & Authentication Method (Protocol şi metodă de autentificare internă)	Selectaţi protocolul şi metoda de autentificare.
SSL/TLS	Selectaţi opţiunea **SSL/TLS**.
LDAP Server Port (Port de server LDAP)	Introduceți numărul portului pentru conectarea serverului Active Directory prin LDAP (disponibil numai pentru metoda de autentificare **LDAP + kerberos** sau **LDAP + NTLMv2**).

Opţiune	Descriere
LDAP Search Root (Rădăcină de căutare LDAP)	Introduceți rădăcina de căutare LDAP (disponibil numai pentru metoda de autentificare **LDAP + kerberos** sau **LDAP + NTLMv2**).
Get Mail Address (Obţinere adresă de e-mail)	Selectaţi această opţiune pentru a obţine adresa de e-mail a utilizatorului autentificat de la serverul Active Directory. (disponibil numai pentru **LDAP + kerberos** sau pentru metoda de autentificare **LDAP + NTLMv2**)
Get User's Home Directory (Obţinere director de pornire utilizator)	Selectaţi această opţiune pentru a obţine directorul principal ca destinaţie pentru Scanare către reţea. (disponibil numai pentru **LDAP + kerberos** sau pentru metoda de autentificare **LDAP + NTLMv2**)

9. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea autentificării Active Directory

Autentificarea pentru a modifica setările aparatului utilizând panoul de control al aparatului (autentificare Active Directory)

Dacă autentificarea Active Directory este activată, panoul de control al aparatului va fi blocat până când introduceţi ID-ul de utilizator şi parola la panoul de control al aparatului.

1. Pentru conectare, de la panoul de control al aparatului introduceți ID-ul de utilizator și parola.
2. După ce autentificarea a fost efectuată cu succes, panoul de control al aparatului este deblocat.

Informaţii similare

- Utilizarea autentificării Active Directory

Utilizarea autentificării prin LDAP

- Introducere în autentificarea LDAP
- Configurarea autentificării LDAP utilizând Management bazat pe web
- Autentificarea pentru a schimba setările utilizând panoul de control al aparatului (Autentificarea LDAP)

Introducere în autentificarea LDAP

Autentificarea prin LDAP restricționează utilizarea aparatului. Dacă autentificarea LDAP este activată, panoul de control al aparatului va fi blocat. Nu puteţi schimba setările aparatului până când nu introduceţi un ID de utilizator şi o parolă.

Autentificarea LDAP oferă următoarele caracteristici:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

- Stochează datele de imprimare primite
- Stochează datele de fax primite
- Obţine adresa de e-mail de la serverul LDAP pe baza ID-ului de utilizator atunci când se trimit date scanate la un server de e-mail.

  Pentru a utiliza această caracteristică, selectați opțiunea **On (Pornit)** pentru setarea **Get Mail Address (Obţinere adresă de e-mail)**. Adresa dumneavoastră de e-mail va fi setată ca expeditor atunci când aparatul trimite date scanate la un server de e-mail, respectiv ca destinatar dacă doriţi să trimiteţi datele scanate la adresa dumneavoastră de e-mail.

Atunci când autentificarea LDAP este activată, aparatul dvs. stochează toate datele faxurilor primite. După ce vă autentificaţi, aparatul va imprima toate datele faxurilor stocate.

Puteți modifica setările de autentificare prin LDAP folosind Web Based Management.

Informaţii similare

- Utilizarea autentificării prin LDAP

Configurarea autentificării LDAP utilizând Management bazat pe web

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **User Restriction Function (Funcţie restricţie utilizator)** sau pe **Restriction Management (Gestionare restricţii)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi **LDAP Authentication (Autentificare LDAP)**.
6. Faceţi clic pe **Submit (Remitere)**.
7. Faceţi clic pe meniul **LDAP Authentication (Autentificare LDAP)**.
8. Configuraţi setările următoare:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

Opţiune	Descriere
Storage Fax RX Data (Stocare date retransmitere fax)	Selectaţi această opţiune pentru a stoca datele de fax primite. Puteţi imprima toate datele de fax primite după ce vă autentificaţi la aparat.
Remember User ID (Memorare ID utilizator)	Selectaţi această opţiune pentru a vă salva ID-ul de utilizator.
LDAP Server Address (Adresă de server LDAP)	Introduceţi adresa IP sau numele serverului (spre exemplu: ldap.example.com) pentru serverul LDAP.
SSL/TLS	Selectați opțiunea **SSL/TLS** pentru a folosi LDAP în loc de SSL/TLS.
LDAP Server Port (Port de server LDAP)	Introduceţi numărul portului serverului LDAP.
LDAP Search Root (Rădăcină de căutare LDAP)	Introduceţi directorul rădăcină de căutare LDAP.
Attribute of Name (Search Key) (Atributul numelui (cheie de căutare))	Introduceţi atributul pe care doriţi să-l utilizaţi drept cheie de căutare.
Get Mail Address (Obţinere adresă de e-mail)	Selectaţi această opţiune pentru a obţine adresa de e-mail a utilizatorului conectat de la serverul LDAP.
Get User's Home Directory (Obţinere director de pornire utilizator)	Selectaţi această opţiune pentru a obţine directorul principal ca destinaţie pentru Scanare către reţea.

9. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea autentificării prin LDAP

Autentificarea pentru a schimba setările utilizând panoul de control al aparatului (Autentificarea LDAP)

Dacă autentificarea LDAP este activată, panoul de control al aparatului va fi blocat până când introduceţi ID-ul de utilizator şi parola pe panoul de control al aparatului.

1. Pentru conectare, de la panoul de control al aparatului introduceți ID-ul de utilizator și parola.
2. După ce autentificarea a fost efectuată cu succes, panoul de control al aparatului este deblocat.

Informaţii similare

- Utilizarea autentificării prin LDAP

Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Utilizarea funcției Secure Function Lock 3.0 (Blocarea securizată a funcțiilor) determină creșterea securității prin limitarea funcțiilor disponibile de la aparatul dumneavoastră.

Înainte de a utiliza Secure Function Lock 3.0 (Blocarea securizată a funcţiilor 3.0)

Utilizaţi funcţia Secure Function Lock (Blocarea securizată a funcţiilor) pentru configurarea parolelor, limitarea numărului de pagini pentru anumiţi utilizatori şi oferirea accesului la anumite funcţii sau la toate funcţiile enumerate aici.

Puteți configura și modifica următoarele setări ale Secure Function Lock 3.0 (Blocarea securizată a funcțiilor 3.0) utilizând Web Based Management:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

- **Print (Imprimare)**
- **Copy (Copiere)**
- **Scan (Scanare)**
- **Fax**
- **Suport media**
- **Web Connect**
- **Apps (Aplicaţii)**
- **Page Limits (Limite de pagini)**
- **Page Counters (Contor de pagini)**
- **Card ID (NFC ID) (ID card (ID NFC))**

Modelele cu ecran tactil LCD:

Atunci când Secure Function Lock (Blocare securizată a funcțiilor) este activată, aparatul intră automat în modul Public și unele dintre funcțiile aparatului devin restricționate numai la utilizatorii authorized. Pentru a accesa funcțiile restricționate ale aparatului, apăsați pe , selectați numele de utilizator și introduceți parola dvs.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Configurarea funcţiei Secure Function Lock 3.0 (Blocarea securizată a funcţiilor 3.0) folosind Web Based Management

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **User Restriction Function (Funcţie restricţie utilizator)** sau pe **Restriction Management (Gestionare restricţii)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi **Secure Function Lock (Blocare funcţii în siguranţă)**.
6. Faceţi clic pe **Submit (Remitere)**.
7. Faceţi clic pe meniul **Restricted Functions (Funcţii restricţionate)**.
8. Configurați setările pentru gestionarea restricțiilor pentru utilizator sau pentru grup.
9. Faceţi clic pe **Submit (Remitere)**.
10. Faceţi clic pe meniul **User List (Listă de utilizatori)**.
11. Configurați lista utilizatorului.
12. Faceţi clic pe **Submit (Remitere)**.

De asemenea, din meniul **Secure Function Lock (Blocare funcţii în siguranţă)** puteți modifica setările de blocare pentru lista utilizatorului.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Scanarea folosind Secure Function Lock 3.0 (Blocarea securizată a funcţiilor 3.0)

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

Setarea restricţiilor de scanare (pentru administratori)

Secure Function Lock 3.0 (Blocarea securizată a funcțiilor) permite restricționarea de către administrator a utilizatorilor care au permisiunea de a scana documente. Dacă funcţia de scanare este dezactivată din setările utilizatorilor publici, numai utilizatorii pentru care a fost bifată caseta de validare **Scan (Scanare)** vor putea să scaneze documente.

Utilizarea caracteristicii de scanare (pentru utilizatorii restricţionaţi)

- Scanarea utilizând panoul de control al aparatului:

  Utilizatorii restricționați trebuie să-și introducă parola de la panoul de control al aparatului pentru a accesa modul Scanare.
- Pentru a scana de la un computer:

  Utilizatorii restricționați trebuie să-și introducă parola de la panoul de control al aparatului înainte de a scana documentul de la computer. În cazul în care parola nu este introdusă de la panoul de control al aparatului, pe ecranul computerului utilizatorului va fi afișat un mesaj de eroare.

Dacă aparatul suportă autentificarea cu card IC, utilizatorii restricționați pot accesa modul Scanare atingând simbolul NFC de pe panoul de control al aparatului cu cardurile IC înregistrate.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Configurarea modului public pentru Secure Function Lock 3.0 (Blocarea securizată a funcţiilor 3.0)

Utilizaţi ecranul aplicaţiei Secure Function Lock (Blocarea securizată a funcţiilor) pentru a configura modul public, care limitează funcţiile disponibile utilizatorilor publici. Utilizatorii publici nu vor fi nevoiţi să introducă o parolă pentru a accesa funcţiile disponibile prin setările modului public.

Modul public include comenzi de imprimare trimise prin Brother iPrint&Scan și Brother Mobile Connect.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **User Restriction Function (Funcţie restricţie utilizator)** sau pe **Restriction Management (Gestionare restricţii)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi **Secure Function Lock (Blocare funcţii în siguranţă)**.
6. Faceţi clic pe **Submit (Remitere)**.
7. Faceţi clic pe meniul **Restricted Functions (Funcţii restricţionate)**.
8. În rândul **Public Mode (Modul public)**, bifați o casetă de selectare pentru a permite utilizarea funcției respective sau debifați caseta pentru a restricționa funcția respectivă.
9. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Configurarea setărilor ecranului principal personal utilizând Web Based Management

În calitate de administrator, puteți să indicați ce file pot vizualiza utilizatorii pe ecranele principale personale. Aceste file oferă acces rapid la comenzile rapide favorite ale utilizatorilor, pe care le pot atribui filelor de pe ecranul principal personal din panoul de control al aparatului.

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **User Restriction Function (Funcţie restricţie utilizator)** sau pe **Restriction Management (Gestionare restricţii)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi **Secure Function Lock (Blocare funcţii în siguranţă)**.
6. În câmpul **Tab Settings (Setări file)**, selectați **Personal** pentru numele filelor pe care vreți să le utilizați ca ecran principal personal.
7. Faceţi clic pe **Submit (Remitere)**.
8. Faceţi clic pe meniul **Restricted Functions (Funcţii restricţionate)**.
9. Configurați setările pentru gestionarea restricțiilor pentru utilizator sau grup.
10. Faceţi clic pe **Submit (Remitere)**.
11. Faceţi clic pe meniul **User List (Listă de utilizatori)**.
12. Configurați lista utilizatorului.
13. Selectaţi **User List / Restricted Functions (Listă de utilizatori/funcţii restricţionate)** din lista derulantă pentru fiecare utilizator.
14. Selectați numele filei din lista derulantă **Home Screen (Ecran de pornire)** pentru fiecare utilizator.
15. Faceţi clic pe **Submit (Remitere)**.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Caracteristici suplimentare ale Secure Function Lock 3.0 (Blocarea securizată a funcţiilor 3.0)

Configuraţi următoarele caracteristici în ecranul Secure Function Lock:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

All Counter Reset (Resetare toate contoarele)

Faceţi clic pe **All Counter Reset (Resetare toate contoarele)**, din coloana **Page Counters (Contor de pagini)** pentru a reseta contorul de pagini.

Export to CSV file (Export în fişier CSV)

Faceţi clic pe **Export to CSV file (Export în fişier CSV)** pentru a exporta contorul curent şi contorul ultimei pagini, inclusiv informaţiile **User List / Restricted Functions (Listă de utilizatori/funcţii restricţionate)** ca fişier CSV.

Card ID (NFC ID) (ID card (ID NFC))

Faceți clic pe meniul **User List (Listă de utilizatori)** și apoi introduceți numărul de identificare al cardului ID al unui utilizator în câmpul **Card ID (NFC ID) (ID card (ID NFC))**. Puteţi utiliza cardul dumneavoastră IC pentru autentificare.

Output (Ieşire)

După instalarea unităţii cutiei poştale pe aparat, selectaţi tava de ieşire pentru fiecare utilizator din lista derulantă.

Last Counter Record (Ultima înregistrare de contor)

Faceţi clic pe **Last Counter Record (Ultima înregistrare de contor)** dacă doriţi ca aparatul să reţină numărul de pagini după resetarea contorului.

Counter Auto Reset (Resetare automată contor)

Faceți clic pe **Counter Auto Reset (Resetare automată contor)** pentru a configura intervalul de timp dorit între două resetări succesive ale contorului. Selectaţi un interval zilnic, săptămânal sau lunar.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Înregistrarea unui nou card IC utilizând panoul de control al aparatului

Puteți înregistra cardurile de circuit integrate (carduri IC) pe aparatul dumneavoastră.

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

1. Atingeți simbolul NFC de pe panoul de control al aparatului cu un card cu circuit integrat înregistrat (card IC).
2. Apăsați pe ID utilizator de pe LCD.
3. Apăsați pe butonul Înregistrare card.
4. Atingeţi cu un nou card IC simbolul NFC.
   Numărul noului card IC este apoi înregistrat pe aparat.
5. Apăsați pe butonul OK.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Înregistrarea unui cititor extern de carduri IC

La conectarea unui cititor extern de carduri IC (circuit integrat), utilizați Web Based Management pentru a înregistra cititorul de carduri. Aparatul dumneavoastră acceptă cititoare externe de carduri IC compatibile cu drivere din clasa HID.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

   Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.
4. În bara de navigare din stânga, faceți clic pe **Administrator** > **External Card Reader (Cititor de card extern)**.

   Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.
5. Introduceți informațiile necesare și apoi faceți clic pe **Submit (Remitere)**.
6. Reporniți aparatul Brother pentru a activa configurația.
7. Conectați cititorul de carduri la aparat.
8. Atingeţi cu cardul cititorul de carduri dacă utilizaţi autentificarea cardului.

Informaţii similare

- Utilizarea Secure Function Lock (Blocarea securizată a funcțiilor) 3.0

Trimiterea sau primirea unui mesaj de e-mail în siguranță

Configurarea trimiterii sau primirii mesajelor de e-mail folosind Web Based Management

- Funcția de primire e-mail este disponibilă numai pentru anumite modele.
- Vă recomandăm să utilizați Web Based Management pentru configurarea trimiterii securizate a mesajelor de e-mail cu autentificarea utilizatorului sau trimiterea și primirea mesajelor de e-mail folosind SSL/TLS (numai modelele acceptate).

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Network (Reţea)** > **Network (Reţea)** > **Protocol**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. În câmpul **POP3/IMAP4/SMTP Client (Client POP3/IMAP4/SMTP)**, faceţi clic pe **Advanced Settings (Setări avansate)** şi asiguraţi-vă că starea selectată pentru **POP3/IMAP4/SMTP Client (Client POP3/IMAP4/SMTP)** este **Enabled (Activ)**.

- Protocoalele disponibile pot să difere, în funcție de aparatul dumneavoastră.
- Dacă apare ecranul de selecție **Authentication Method (Metodă de autentificare)**, selectați metoda de autentificare și apoi urmați instrucțiunile pas cu pas.

6. Configuraţi setările pentru **POP3/IMAP4/SMTP Client (Client POP3/IMAP4/SMTP)**.
   - După configurare, confirmaţi dacă setările adresei de e-mail sunt corecte prin trimiterea unui mesaj de test.
   - Dacă nu cunoaşteţi setările serverului POP3/IMAP4/SMTP, contactaţi administratorul de reţea sau Furnizorul de servicii internet (ISP).
7. Când aţi terminat, faceţi clic pe **Submit (Remitere)**.

   Este afişată caseta de dialog **Test Send/Receive E-mail Configuration (Testare configurare trimitere/primire e-mail)**.
8. Urmaţi instrucţiunile din caseta de dialog pentru a testa setările curente.

Informaţii similare

- Trimiterea sau primirea unui mesaj de e-mail în siguranță

Subiecte conexe:

- Trimiterea sau primirea unui mesaj de e-mail în siguranță folosind SSL/TLS

Trimiterea unui mesaj de e-mail cu autentificarea utilizatorului

Aparatul dumneavoastră trimite mesaje de e-mail printr-un server de e-mail care necesită autentificarea utilizatorului. Această metodă împiedică accesul utilizatorilor unauthorized la serverul de e-mail.

Puteți trimite mesaje e-mail de notificare, rapoarte și I-Fax (numai pentru anumite modele) utilizând autentificarea utilizatorului.

- Protocoalele disponibile pot să difere, în funcție de aparatul dumneavoastră.
- Vă recomandăm să utilizați Web Based Management pentru a configura autentificarea SMTP.

Setările serverului de e-mail

Trebuie să configuraţi metoda de autentificare SMTP a aparatului pentru ca aceasta să corespundă cu metoda utilizată de serverul de e-mail. Pentru detalii despre setările serverului de e-mail, contactaţi administratorul reţelei sau furnizorul de servicii internet (ISP).

Pentru a activa autentificarea la serverului SMTP folosind Web Based Management, selectați metoda de autentificare din **Server Authentication Method (Metodă de autentificare server)** de pe ecranul **POP3/IMAP4/SMTP Client (Client POP3/IMAP4/SMTP)**.

Informaţii similare

- Trimiterea sau primirea unui mesaj de e-mail în siguranță

Trimiterea sau primirea unui mesaj de e-mail în siguranță folosind SSL/TLS

Aparatul este compatibil cu metodele de comunicare SSL/TLS. Pentru a utiliza un server de e-mail care foloseşte comunicarea SSL/TLS, trebuie să configurați următoarele setări.

- Funcția de primire e-mail este disponibilă numai pentru anumite modele.
- Pentru configurarea SSL/TLS, vă recomandăm să utilizaţi Administrarea online a reţelei folosind Web Based Management.

Verificarea certificatului serverului

Din **SSL/TLS**, dacă selectaţi **SSL** sau **TLS**, caseta de validare **Verify Server Certificate (Verificare certificat server)** va fi selectată automat.

- Înainte de a verifica certificatul serverului, trebuie să importaţi certificatul AC emis de AC care a semnat certificatul serverului. Contactaţi administratorul de reţea sau Furnizorul de servicii internet (ISP) pentru a confirma dacă este necesar să importaţi certificatul CA.
- Dacă nu trebuie să verificaţi certificatul serverului, deselectaţi caseta de validare **Verify Server Certificate (Verificare certificat server)**.

Numărul portului

Dacă selectaţi **SSL** sau **TLS**, valoarea **Port** va fi modificată în funcţie de protocol. Pentru a modifica manual numărul portului, introduceţi numărul portului după ce aţi selectat setările pentru **SSL/TLS**.

Trebuie să configuraţi metoda de comunicare a aparatului pentru ca aceasta să corespundă cu metoda utilizată de serverul dumneavoastră de e-mail. Pentru detalii despre setările serverului de e-mail, contactaţi administratorul reţelei sau furnizorul de servicii internet (ISP).

În majoritatea cazurilor, serviciile securizate de poştă electronică web necesită următoarele setări:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

SMTP	**Port**	587
	Server Authentication Method (Metodă de autentificare server)	**SMTP-AUTH (AUTENTIF. SMTP)**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Informaţii similare

- Trimiterea sau primirea unui mesaj de e-mail în siguranță

Subiecte conexe:

- Configurarea trimiterii sau primirii mesajelor de e-mail folosind Web Based Management
- Configurarea certificatelor pentru securitatea dispozitivului

Stocarea jurnalului de imprimare în rețea

Prezentarea stocării jurnalului de imprimare în rețea

Caracteristica Stocare jurnal de imprimare în rețea vă permite să salvați fișierul cu jurnalul de imprimare din aparat pe un server din rețea utilizând protocolul CIFS (Common Internet File System). Puteți înregistra codul de identificare (ID), tipul acțiunii de imprimare, numele acțiunii, numele utilizatorului, data, ora și numărul de pagini imprimate pentru fiecare acțiune de imprimare. CIFS este un protocol care se execută prin TCP/IP şi permite calculatoarelor dintr-o reţea să partajeze fişiere într-un intranet sau pe Internet.

În jurnalul de imprimare se înregistrează următoarele funcţii de imprimare:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

- Acţiuni de imprimare de la calculatorul dumneavoastră
- Imprimarea directă USB
- Copiere
- Faxuri primite
- Web Connect Print

- Caracteristica Stocare jurnal de imprimare în rețea acceptă autentificarea Kerberos și autentificarea NTLMv2. Trebuie să configurați protocolul SNTP (server de sincronizare a orei în rețea) sau trebuie să setați corect data, ora și fusul orar în panoul de control pentru autentificare.
- Puteţi seta tipul de fişier la TXT sau CSV atunci când stocaţi un fişier pe server.

Informaţii similare

- Stocarea jurnalului de imprimare în rețea

Configurarea Stocare jurnal de imprimare în reţea utilizând Web Based Management

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **Store Print Log to Network (Stocare jurnal de imprimare pe reţea)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. În câmpul **Print Log (Jurnal imprimare)**, faceţi clic pe **On (Pornit)**.
6. Configuraţi setările următoare:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

Opţiune	Descriere
Network Folder Path (Cale folder reţea)	Tastați folderul de destinație unde va fi stocat jurnalul de imprimate pe serverul CIFS (de exemplu: \\ComputerName\SharedFolder).
File Name (Nume fişier)	Tastaţi numele de fişier pe care doriţi să îl utilizaţi (până la 32 de caractere).
File Type (Tip fişier)	Selectați opțiunea **TXT** sau **CSV** pentru tipul de fișier pentru jurnalul de imprimare.
Time Source for Log (Sursă timp pentru jurnal)	Selectați sursa orei pentru jurnalul de imprimare.
Auth. Method (Metodă de autentificare)	Selectați metoda de autentificare necesară pentru accesarea serverului CIFS: **Auto (Automat)**, **Kerberos** sau **NTLMv2**. Kerberos este un protocol de autentificare care permite dispozitivelor sau persoanelor să se identifice în siguranță pe serverele de rețea utilizând o singură deschidere de sesiune. NTLMv2 este metoda de autentificare utilizată de Windows pentru conectare la servere. • **Auto (Automat)**: Dacă selectaţi **Auto (Automat)**, NTLMv2 va fi utilizat pentru metoda de autentificare. • **Kerberos**: Selectaţi opţiunea **Kerberos** pentru a utiliza numai autentificarea Kerberos. • **NTLMv2**: Selectaţi **NTLMv2** pentru a utiliza numai autentificarea NTLMv2.

Opţiune	Descriere
	• Pentru autentificările **Kerberos** şi **NTLMv2** trebuie să configuraţi şi setările **Date&Time (Data şi ora)** sau protocolul SNTP (server oră reţea) şi serverul DNS. • De asemenea, puteți configura setările pentru dată și oră de la panoul de control al aparatului.
Username (Nume util.)	Tastaţi numele de utilizator pentru autentificare (până la 96 de caractere). Dacă numele utilizatorului face parte dintr-un domeniu, introduceţi numele utilizatorului folosind următoarele formate: utilizator@domeniu sau domeniu\utilizator.
Password (Parola)	Tastaţi parola pentru autentificare (până la 32 de caractere).
Kerberos Server Address (Adresă de server Kerberos) (dacă este necesar)	Tastați adresa gazdei Centrului de distribuire a cheilor (KDC) (de exemplu: kerberos.exemplu.com; până la 64 de caractere) sau adresa IP (de exemplu: 192.168.56.189).
Error Detection Setting (Setare detectare erori)	Selectați acțiunea care ar trebui efectuată atunci când jurnalul de imprimare nu se poate stoca pe server din cauza unei erori de rețea.

7. În câmpul **Connection Status (Starea conexiunii)**, confirmaţi ultima stare de autentificare.

De asemena, puteţi confirma starea de eroare pe ecranul LCD al aparatului dvs.

8. Faceţi clic pe **Submit (Remitere)** pentru a afişa pagina **Test Print Log to Network (Test jurnal de imprimare pe reţea)**.

   Pentru a testa setările, faceţi clic pe **Yes (Da)** şi apoi treceţi la pasul următor.

   Pentru a trece peste test, faceţi clic pe **No (Nu)**. Setările dumneavoastră vor fi remise automat.
9. Aparatul va testa setările.
10. Dacă setările sunt acceptate, pe pagină apare **Test OK (Testare OK)**.

    Dacă apare **Test Error (Eroare la testare)**, verificaţi toate setările şi apoi faceţi clic pe **Submit (Remitere)** pentru a afişa din nou pagina de test.

Informaţii similare

- Stocarea jurnalului de imprimare în rețea

Utilizarea Setării de detecţie a erorilor pentru Stocare jurnal de imprimare în reţea

Utilizaţi Setările de detecţie a erorilor pentru a determina acţiunea care să fie efectuată atunci când jurnalul de imprimare nu se poate stoca pe server datorită unei erori de reţea.

1. Porniţi browserul web.
2. Introduceți „https://adresa IP a aparatului” în bara de adrese a browserului (unde „adresa IP a aparatului” este adresa IP a aparatului dvs.).

   De exemplu:

   https://192.168.1.2

   Adresa IP a aparatului se găsește în Raportul de configurare a rețelei.
3. Dacă este necesar, introduceți parola în câmpul **Login (Conectare)** și apoi faceți clic pe **Login (Conectare)**.

Parola implicită pentru gestionarea setărilor acestui aparat se află în spatele sau pe baza aparatului și este marcată cu „**Pwd**”. Dacă vă conectați pentru prima dată, schimbați parola implicită urmând instrucțiunile pas cu pas.

4. În bara de navigare din stânga, faceți clic pe **Administrator** > **Store Print Log to Network (Stocare jurnal de imprimare pe reţea)**.

Dacă bara de navigare din stânga nu este vizibilă, începeți navigarea din ☰.

5. Selectaţi opţiunea **Cancel Print (Anulare imprimare)** sau **Ignore Log & Print (Ignorare jurnal şi imprimare)** din secţiunea **Error Detection Setting (Setare detectare erori)**.

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

Opţiune	Descriere
Cancel Print (Anulare imprimare)	Dacă selectaţi opţiunea **Cancel Print (Anulare imprimare)**, acţiunile de imprimare se canceled atunci când jurnalul de imprimare nu poate fi stocat pe server. Chiar dacă selectaţi opţiunea **Cancel Print (Anulare imprimare)**, aparatul va imprima un fax recepţionat.

Ignore Log & Print (Ignorare jurnal şi imprimare)	Dacă selectaţi opţiunea **Ignore Log & Print (Ignorare jurnal şi imprimare)**, aparatul imprimă documentul chiar dacă jurnalul de imprimare nu se poate stoca pe server.
	După restabilirea funcției Stocare jurnal de imprimare, jurnalul de imprimare se înregistrează astfel:
	`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. Dacă jurnalul nu se poate stoca la sfârșitul imprimării, numărul de pagini imprimate nu va fi înregistrat.
	b. Dacă jurnalul de imprimare nu se poate stoca la începutul şi la sfârşitul imprimării, jurnalul de imprimare al acţiunii de imprimare nu se va înregistra. După restabilirea funcției, eroarea apare în jurnal.

6. Faceţi clic pe **Submit (Remitere)** pentru a afişa pagina **Test Print Log to Network (Test jurnal de imprimare pe reţea)**.

   Pentru a testa setările, faceţi clic pe **Yes (Da)** şi apoi treceţi la pasul următor.

   Pentru a trece peste test, faceţi clic pe **No (Nu)**. Setările dumneavoastră vor fi remise automat.
7. Aparatul va testa setările.
8. Dacă setările sunt acceptate, pe pagină apare **Test OK (Testare OK)**.

   Dacă apare **Test Error (Eroare la testare)**, verificaţi toate setările şi apoi faceţi clic pe **Submit (Remitere)** pentru a afişa din nou pagina de test.

Informaţii similare

- Stocarea jurnalului de imprimare în rețea

Utilizarea Stocare jurnal de imprimare în reţea cu Secure Function Lock 3.0

Atunci când Secure Function Lock 3.0 (Blocarea securizată a funcţiilor) este activă, numele utilizatorilor înregistrați pentru funcțiile copiere, Fax RX, Web Connect Print și Imprimare directă USB se vor înregistra în raportul Stocare jurnal de imprimare în rețea. Atunci când autentificarea Active Directory este activată, numele de utilizator autentificat va fi înregistrat în raportul Stocare jurnal de imprimare în rețea:

Funcțiile, opțiunile și setările acceptate pot să difere în funcție de model.

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

Informaţii similare

- Stocarea jurnalului de imprimare în rețea

brother

Brother Earth

www.brotherearth.com

ROM
Versiunea 0