Biztonsági funkciók útmutatója

Tartalomjegyzék

Bevezetés

Megjegyzések meghatározása

Ez a használati útmutató a következő szimbólumokat és egyezményes jeleket használja:

FONTOS	FONTOS potenciálisan veszélyes helyzetet jelöl, amelyet ha nem sikerül megelőzni, akkor az a vagyontárgy sérüléséhez vagy a termékfunkcionalitás elvesztéséhez vezethet.
MEGJEGYZÉS	A MEGJEGYZÉS a működési környezetet, a telepítési feltételeket és a használat speciális feltételeit határozza meg.
	A tippikonok hasznos ötleteket és kiegészítő információkat kínálnak.
Félkövér	Félkövér betűkkel a készülék kezelőpanelén található vagy a számítógép képernyőjén megjelenő gombokat jelöltük.
Dőlt	A Italicized betűstílus egy fontos pont emphasizes szolgál, vagy kapcsolódó témákhoz irányít.

Kapcsolódó tájékoztatás

- Bevezetés

Védjegyek

Az Adobe® és a Reader® az Adobe Systems Incorporated Egyesült Államokban és/vagy más országokban bejegyzett védjegye.

Mindazon cégek, amelyek szoftvereinek nevei szerepelnek a kézikönyvben, rendelkeznek a tulajdonukban levő programhoz tartozó License-szerződéssel.

A Brother-termékeken, kapcsolódó dokumentumokon és egyéb anyagokon feltüntetett minden vállalati márkanév és terméknév a megfelelő vállalat védjegye vagy bejegyzett védjegye.

Kapcsolódó tájékoztatás

- Bevezetés

Szerzői jog

Kapcsolódó tájékoztatás

- Bevezetés

A Hálózati biztonság funkciók használata előtt

Az Ön készüléke a ma elérhető legújabb hálózati biztonsági és titkosítási protokollokat használja. Ezek a hálózati funkciók integrálhatók az Ön általános hálózati biztonsági tervébe, ami így segíti adatainak védelmét és megakadályozza a készülékhez való unauthorized hozzáférést.

Javasoljuk az FTP és TFTP protokollok letiltását. A készülék elérése ezeken a protokollokon keresztül nem biztonságos.

Kapcsolódó tájékoztatás

- Bevezetés
  - A szükségtelen protokollok letiltása

A szükségtelen protokollok letiltása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)** gombjára.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.

5. A szükségtelen protokollok letiltásához szüntesse meg a hozzájuk tartozó jelölőnégyzetek kijelölését.
6. Kattintson a **Submit (Küldés)** gombra.
7. Indítsa újra Brother készülékét a konfiguráció aktiválásához.

Kapcsolódó tájékoztatás

- A Hálózati biztonság funkciók használata előtt

Hálózati biztonság

Tanúsítványok konfigurálása az eszközbiztonság számára

A hálózati készülék SSL/TLS használatával történő biztonságos felügyeletéhez konfigurálnia kell egy tanúsítványt. A tanúsítványt Web alapú kezelés használatával kell konfigurálnia.

Biztonsági tanúsítvány jellemzőinek áttekintése

Az Ön készüléke támogatja számos biztonsági tanúsítvány használatát, melyek lehetővé teszik a készülék biztonságos kezelését, azonosítását és a biztonságos kommunikációt. A készüléken a következő biztonsági tanúsítvány funkciók használhatók:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

- SSL/TLS kommunikáció
- IEEE 802.1x hitelesítés
- IPsec

Az Ön készüléke a következőket támogatja:

- Előre telepített tanúsítvány

  Készüléke egy előre telepített, önaláírt tanúsítvánnyal rendelkezik. Ez a tanúsítvány lehetővé teszi az SSL/TLS kommunikáció használatát anélkül, hogy egy másik tanúsítványt kellene létrehoznia vagy telepítenie.

Az előre telepített, önaláírt tanúsítvány a kommunikáció védelmét egy adott szintig képes biztosítani. Azt javasoljuk, hogy egy olyan tanúsítványt használjon, amit egy megbízható organization adott ki.

- Önaláírt tanúsítvány

  Ez a nyomtatószerver ki tud adni egy saját tanúsítványt. Ezzel a tanúsítvánnyal könnyedén használni tudja az SSL/TLS kommunikációt anélkül, hogy egy másik CA által kiadott tanúsítványt kellene létrehoznia vagy telepítenie.

- Egy Tanúsítványszolgáltató (CA) által kiadott tanúsítvány

  Kétféle módon telepíthet egy CA által kiadott tanúsítványt. Ha már rendelkezik egy CA által kiadott tanúsítvánnyal, vagy ha egy külső, megbízható CA tanúsítványát kívánja használni:

  - Ha ettől a nyomtató-kiszolgálótól származó Hitelesítési kérelmet (CSR) használ.
  - Ha importálja a tanúsítványt és a privát kulcsot.

- Tanúsítványszolgáltató (CA) tanúsítványa

  Olyan CA-tanúsítvány használatához, amely azonosítja magát a CA (hitelesítésszolgáltató) szervezetet, és tartalmazza annak saját kulcsát, importálnia kell az adott CA-tanúsítványt a hitelesítésszolgáltatóról, mielőtt beállítaná a Hálózati biztonság funkcióit.

- Ha SSL/TLS kommunikációt fog használni, akkor azt javasoljuk, hogy először vegye fel a kapcsolatot a rendszergazdával.
- Amikor visszaállítja a nyomtatószervert gyári alapbeállításaira, a telepített tanúsítvány és privát kulcs törlésre kerül. Ha meg kívánja tartani ugyanazt a tanúsítványt és privát kulcsot a nyomtatószerver visszaállítása után is, akkor a visszaállítás előtt exportálja őket, majd telepítse fel újra.

Kapcsolódó tájékoztatás

- Tanúsítványok konfigurálása az eszközbiztonság számára

Kapcsolódó témák:

- Az IEEE 802.1x hitelesítés beállítása a hálózaton a Web alapú kezelés (böngésző) segítségével

A tanúsítványok létrehozása és telepítése

A biztonsági tanúsítvány kiválasztásakor kétféle lehetősége van: használhat önaláírt tanúsítvány vagy egy CA által kiadott tanúsítvány.

1. opció

Önaláírt tanúsítvány

1. Hozzon létre önaláírt tanúsítványt a Web alapú kezelővel.
2. Az önaláírt tanúsítvány telepítése a számítógépre.

2. opció

Hitelesítésszolgáltatótól származó tanúsítvány

1. Hozzon létre egy tanúsítvány-aláírási kérelmet (CSR) a Web alapú kezelés használatával.
2. Telepítse a Web alapú kezelővel a Brother készülékhez a CA által kibocsátott tanúsítványt.
3. Telepítse a számítógépre a tanúsítványt.

Kapcsolódó tájékoztatás

- Tanúsítványok konfigurálása az eszközbiztonság számára

Önaláírt tanúsítvány létrehozása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Kattintson a **Create Self-Signed Certificate (Ön-aláírt tanúsítvány létrehozása)** gombra.
6. Adjon meg egy **Common Name (Köznapi név)** és egy **Valid Date (Érvényességi idő)** értéket.
   - A **Common Name (Köznapi név)** hossza kisebb mint 64 bájt. Adjon meg egy azonosítót, amelyet az SSL/TLS kommunikáció során használni kíván a készülék elérésére. Ez lehet egy IP-cím, csomópontnév vagy tartománynév. Alapértelmezés szerint a csomópont neve jelenik meg.
   - Egy figyelmeztetés jelenik meg, ha IPPS vagy HTTPS protokollt használ, és az URL-címként beírt név nem ugyanaz, mint az önaláírt tanúsítványhoz megadott **Common Name (Köznapi név)**.
7. Válassza ki a beállítást a **Public Key Algorithm (Nyilvános kulcsú algoritmus)** legördülő listából.
8. Válassza ki a beállítást a **Digest Algorithm (Kivonatoló algoritmus)** legördülő listából.
9. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- Tanúsítványok konfigurálása az eszközbiztonság számára

Tanúsítvány-aláírási kérés (CSR) létrehozása és hitelesítésszolgáltatótól (CA) származó tanúsítvány telepítése

Ha már rendelkezik külső, megbízható hitelesítésszolgáltatótól (CA) származó tanúsítvánnyal, a tanúsítványt és a saját kulcsot a készüléken tárolhatja, illetve importálással és exportálással kezelheti őket. Ha nem rendelkezik tanúsítvánnyal külső megbízható CA-tól, akkor hozzon létre egy tanúsítvány-aláírási kérelmet (CSR), küldje el egy CA-nak a hitelesítéshez, majd telepítse a visszakapott tanúsítványt a készüléken.

- Tanúsítvány-aláírási kérelem (CSR) létrehozása
- Tanúsítvány telepítése az Ön készülékén

Tanúsítvány-aláírási kérelem (CSR) létrehozása

A tanúsítvány-aláírási kérelem (CSR) egy hitelesítésszolgáltató (CA) számára küldött, a tanúsítványban található hitelesítő adatok megerősítésére irányuló kérés.

Javasoljuk, hogy tanúsítvány-aláírási kérelem létrehozása előtt telepítse számítógépére a hitelesítésszolgáltató legfelső szintű tanúsítványát.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Kattintson a **Create CSR (CSR létrehozása)** gombra.
6. Adjon meg egy **Common Name (Köznapi név)** (kötelező) elemet, majd adjon meg további **Organization (Szervezet)** adatokat (opcionális).

   - A vállalati adatokra azért van szükség, hogy a hitelesítésszolgáltató megerősíthesse azonosságát, és igazolhassa azt a külvilág számára.
   - A **Common Name (Köznapi név)** hossza kisebb mint 64 bájt. Adjon meg egy azonosítót, amelyet az SSL/TLS kommunikáció során használni kíván a készülék elérésére. Ez lehet egy IP-cím, csomópontnév vagy tartománynév. Alapértelmezés szerint a csomópont neve jelenik meg. A **Common Name (Köznapi név)** megadása kötelező.
   - Egy figyelmeztetés jelenik meg, ha olyan nevet ír be az URL-címként, amely különbözik attól a köznapi névtől, amelyet a tanúsítványnál megadott.
   - Az **Organization (Szervezet)**, **Organization Unit (Szervezeti egység)**, **City/Locality (Város/Helység)** és **State/Province (Állam/Megye)** hossza nem haladhatja meg a 64 bájtot.
   - A(z) **Country/Region (Megye/Régió)** értékének egy kétkarakteres ISO 3166 országkódnak kell lennie.
   - Ha az X.509v3 tanúsítvány bővítését állítja be, jelölje be a **Configure extended partition (Kiterjesztett partíció konfigurálása)** jelölőnégyzetet, majd válassza az **Auto (Register IPv4) (Automatikus (IPv4 regisztráció))** vagy **Manual (Kézikönyv)** lehetőséget.
7. Válassza ki a beállítást a **Public Key Algorithm (Nyilvános kulcsú algoritmus)** legördülő listából.
8. Válassza ki a beállítást a **Digest Algorithm (Kivonatoló algoritmus)** legördülő listából.
9. Kattintson a **Submit (Küldés)** gombra.

   A képernyőn megjelenik a tanúsítvány-aláírási kérelem. Mentse el a tanúsítvány-aláírási kérelmet fájlként, vagy másolja és illessz be egy online tanúsítvány-aláírási kérelem űrlapba, amelyet egy hitelesítésszolgáltató biztosít.
10. Kattintson a(z) **Mentés** gombra.

- Kövesse a hitelesítésszolgáltató irányelveit a tanúsítvány-aláírási kérelem elküldésekor a hitelesítésszolgáltatónak.
- Ha a Windows Server vállalati legfelső szintű hitelesítésszolgáltató szolgáltatását használja, a tanúsítványok létrehozásakor javasoljuk a webkiszolgáló használatát a tanúsítványsablonokhoz az ügyféltanúsítvány biztonságos létrehozása érdekében. Ha egy IEEE 802.1x környezetben hoz létre ügyféltanúsítványt EAP-TLS hitelesítéssel, akkor javasoljuk a Felhasználói tanúsítványsablon használatát.

Kapcsolódó tájékoztatás

- Tanúsítvány-aláírási kérés (CSR) létrehozása és hitelesítésszolgáltatótól (CA) származó tanúsítvány telepítése

Tanúsítvány telepítése az Ön készülékén

Ha megkapja a tanúsítványt a hitelesítésszolgáltatótól (CA), akkor a nyomtatókiszolgálóra történő telepítéskor kövesse az alábbi lépéseket:

Csak olyan tanúsítvány telepíthető erre a készülékre, amelyet e készülék tanúsítvány-aláírási kérelmével (CSR) bocsátottak ki. Ha újabb tanúsítvány-aláírási kérelmet (CSR) szeretne létrehozni, előtte győződjön meg arról, hogy telepítve van a tanúsítvány. Csak a tanúsítvány készülékre való telepítését követően hozzon létre új tanúsítvány-aláírási kérelmet (CSR), különben a telepítés előtt készített tanúsítvány-aláírási kérelem érvénytelen lesz.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Kattintson a **Install Certificate (Tanúsítvány telepítése)** gombra.
6. Keresse meg a CA által kiadott tanúsítványt tartalmazó fájlt, majd kattintson a **Submit (Küldés)** gombra.

   Létrejön a tanúsítvány és a készülék elmenti a memóriába.

Az SSL/TLS kommunikáció használatához a hitelesítésszolgáltató legfelső szintű tanúsítványát a számítógépre kell telepíteni. Vegye fel a kapcsolatot a hálózati rendszergazdával.

Kapcsolódó tájékoztatás

- Tanúsítvány-aláírási kérés (CSR) létrehozása és hitelesítésszolgáltatótól (CA) származó tanúsítvány telepítése

A tanúsítvány és a saját kulcs importálása és exportálása

A tanúsítványt és a saját kulcsot a készüléken tárolhatja, illetve importálással és exportálással kezelheti őket.

- A tanúsítvány és a saját kulcs importálása
- A tanúsítvány és a saját kulcs exportálása

A tanúsítvány és a saját kulcs importálása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Kattintson a **Import Certificate and Private Key (Tanúsítvány és saját kulcs importálása)** gombra.
6. Keresse meg és válassza ki az importálni kívánt fájlt.
7. Ha a fájl titkosított, adja meg a jelszót, majd kattintson a **Submit (Küldés)** gombra.

Sikeresen importálta a készülékre a tanúsítványt és a saját kulcsot.

Kapcsolódó tájékoztatás

- A tanúsítvány és a saját kulcs importálása és exportálása

A tanúsítvány és a saját kulcs exportálása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Kattintson a **Export (Exportálás)** területén található **Certificate List (Tanúsítványlista)** lehetőségre.
6. Ha a fájlt titkosítani kívánja, írjon be egy jelszót.

   Ha üres jelszót használ, a kimenet nem lesz titkosítva.
7. A megerősítéshez adja meg újra a jelszót, majd kattintson a **Submit (Küldés)** gombra.
8. Kattintson a(z) **Mentés** gombra.

A tanúsítványt és a saját kulcsot sikeresen exportálta a számítógépre.

A tanúsítványt is importálhatja a számítógépén.

Kapcsolódó tájékoztatás

- A tanúsítvány és a saját kulcs importálása és exportálása

Egy CA tanúsítvány exportálása és importálása

Brother készülékén importálhatja, exportálhatja és tárolhatja a CA tanúsítványokat.

- CA tanúsítvány importálása
- CA tanúsítvány exportálása

CA tanúsítvány importálása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **CA Certificate (CA tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Kattintson a(z) **Import CA Certificate (CA tanúsítvány importálása)** gombra.
6. Böngésszen az importálni kívánt fájlhoz.
7. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- Egy CA tanúsítvány exportálása és importálása

CA tanúsítvány exportálása

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **CA Certificate (CA tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Válassza ki az exportálni kívánt tanúsítványt, és kattintson az **Export (Exportálás)** lehetőségre.
6. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- Egy CA tanúsítvány exportálása és importálása

SSL/TLS használata

- A hálózati készülék biztonságos felügyelete SSL/TLS használatával
- Dokumentumok biztonságos nyomtatása SSL/TLS használatával
- E-mail biztonságos küldése vagy fogadása SSL/TLS használatával

A hálózati készülék biztonságos felügyelete SSL/TLS használatával

Tanúsítvány konfigurálása az SSL/TLS és az elérhető protokollok számára

Az SSL/TLS kommunikáció használata előtt konfiguráljon egy tanúsítványt a készüléken a Web alapú kezelés segítségével.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Kattintson a **HTTP Server Settings (HTTP szerver beállításai)** gombra.
6. Válassza ki a konfigurálni kívánt tanúsítványt a **Select the Certificate (A tanúsítvány kiválasztása)** legördülő listából.
7. Kattintson a **Submit (Küldés)** gombra.
8. Kattintson a **Yes (Igen)** gombra a nyomtatókiszolgáló újraindításához.

Kapcsolódó tájékoztatás

- A hálózati készülék biztonságos felügyelete SSL/TLS használatával

Kapcsolódó témák:

- Dokumentumok biztonságos nyomtatása SSL/TLS használatával

SSL/TLS használatával történő hozzáférés a Web alapú kezeléshez

A hálózati készülék biztonságos kezeléséhez a kezelőalkalmazásokat biztonsági protokollokkal kell használnia.

- A HTTPS protokoll a használatához a HTTPS-t engedélyezni kell a készülékén. A HTTPS protokoll alapértelmezés szerint engedélyezett.
- A HTTPS protokollbeállításokat módosíthatja a Web alapú kezelő képernyőn.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Most már hozzáférhet a készülékhez a HTTPS használatával.

Kapcsolódó tájékoztatás

- A hálózati készülék biztonságos felügyelete SSL/TLS használatával

Önaláírt tanúsítvány telepítése rendszergazdai jogokkal rendelkező Windows-felhasználók számára

- A következő lépések a Microsoft Edge használata esetén érvényesek. Ha másik webböngészőt használ, olvassa el a böngészője dokumentációját, vagy az online útmutatót a tanúsítványok telepítésére vonatkozóan.
- Bizonyosodjon meg arról, hogy az önaláírt tanúsítványát a Web alapú kezelés használatával hozta létre.

1. A jobb gombbal kattintson a **Microsoft Edge** ikonra, és válassza a **Futtatás rendszergazdaként** lehetőséget.

   Ha megjelenik a(z) **Felhasználói fiókok felügyelete** képernyő, kattintson a(z) **Igen** elemre.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Ha a kapcsolata nem privát, kattintson a **Speciális** gombra, majd lépjen a weboldalra.
4. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
5. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **Certificate (Tanúsítvány)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
6. Kattintson a **Export (Exportálás)** gombra.
7. A kimeneti fájl titkosításához adjon meg egy jelszót a **Enter Password (Jelszó megadása)** mezőben. Amennyiben a **Enter Password (Jelszó megadása)** mező üres, a kimeneti fájl titkosítására nem kerül sor.
8. Írja be a jelszót ismét a **Retype Password (Jelszó újbóli megadása)** mezőbe, majd kattintson a **Submit (Küldés)** gombra.
9. Kattintással nyissa meg a letöltött fájlt.
10. Amikor megjelenik a **Tanúsítványimportáló varázsló**, kattintson a **Tovább** gombra.
11. Kattintson a **Tovább** gombra.
12. Szükség esetén adja meg a jelszót, majd kattintson a **Tovább** gombra.
13. Jelölje be a **Minden tanúsítvány tárolása ebben a tárolóban** jelölőnégyzetet, majd kattintson a **Tallózás...** gombra.
14. Válassza az **Megbízható gyökérhitelesítő hatóságok** opciót, majd kattintson az **OK** gombra.
15. Kattintson a **Tovább** gombra.
16. Kattintson a **Befejezés** gombra.
17. Ha az ujjlenyomat megfelelő, kattintson az **Igen** gombra.
18. Kattintson a **OK** gombra.

Kapcsolódó tájékoztatás

- A hálózati készülék biztonságos felügyelete SSL/TLS használatával

Dokumentumok biztonságos nyomtatása SSL/TLS használatával

- Dokumentum nyomtatása IPPS használatával
- Tanúsítvány konfigurálása az SSL/TLS és az elérhető protokollok számára
- Tanúsítványok konfigurálása az eszközbiztonság számára

Dokumentum nyomtatása IPPS használatával

A dokumentumok IPP protokollal történő biztonságos nyomtatásához használja az IPPS protokollt.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Ellenőrizze, hogy be van-e jelölve a **IPP** jelölőnégyzet.

   Amennyiben a **IPP** jelölőnégyzet nincs kiválasztva, jelölje be a **IPP** négyzetet, majd kattintson a **Submit (Küldés)** lehetőségre.

   A konfiguráció aktiválásához indítsa újra a készüléket.

   Miután a készülék újraindul, térjen vissza a készülék weboldalára, írja be a jelszót, majd a bal oldali navigációs sávban kattintson erre: **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)**.
6. Kattintson a **HTTP Server Settings (HTTP szerver beállításai)** gombra.
7. Jelölje be a **HTTPS(Port 443)** jelölőnégyzetet a **IPP** területen, majd kattintson a **Submit (Küldés)** elemre.
8. A konfiguráció aktiválásához indítsa újra a készüléket.

Az IPPS használatával végzett kommunikáció nem képes a nyomtatókiszolgálóhoz való unauthorized hozzáférés megakadályozására.

Kapcsolódó tájékoztatás

- Dokumentumok biztonságos nyomtatása SSL/TLS használatával

SNMPv3 használata

- Hálózati készülék biztonságos felügyelete SNMPv3 használatával

Hálózati készülék biztonságos felügyelete SNMPv3 használatával

Az SNMPv3 (Simple Network Management Protocol version 3) biztosítja a felhasználók hitelesítését és az adatok titkosítását annak érdekében, hogy a hálózati eszközöket biztonságosan lehessen felügyelni.

1. Indítsa el a webböngészőt.
2. Írja be a „https://tanúsítványnév” szöveget a böngésző címsávjába (ahol a „tanúsítványnév” a tanúsítványhoz rendelt név; ez lehet az Ön IP-címe, a csomópont neve vagy a domain neve).
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)** gombjára.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Győződjön meg arról, hogy a **SNMP** beállítás engedélyezve van, majd kattintson a **Advanced Settings (Speciális beállítások)** lehetőségre.
6. Az SNMPv1/v2c mód beállításainak megadása.

Beállítás	Leírás
SNMP v1/v2c read-write access (SNMP v1/v2c írási-olvasási hozzáférés)	A nyomtatókiszolgáló az SNMP protokoll 1-es és 2c verzióját használja. Ebben a módban az összes készülékének alkalmazása használható. Ez a mód azonban nem biztonságos, mert nem hitelesíti a felhasználót és nem titkosítja az adatokat.
SNMP v1/v2c read-only access (SNMP v1/v2c csak olvasási hozzáférés)	A nyomtatókiszolgáló az SNMP protokoll 1 és 2c verziójának csak olvasási hozzáférését használja.
Disabled (Letiltva)	Tiltsa le az SNMP protokoll 1 és 2c verzióját. Korlátozva lesz minden olyan alkalmazás, amely az SNMPv1/v2c-t használja. Az SNMPv1/v2c alkalmazások engedélyezéséhez használja az **SNMP v1/v2c read-only access (SNMP v1/v2c csak olvasási hozzáférés)** vagy az **SNMP v1/v2c read-write access (SNMP v1/v2c írási-olvasási hozzáférés)** módot.

7. Az SNMPv3 mód beállításainak megadása.

Beállítás	Leírás
Enabled (Engedélyezve)	A nyomtatókiszolgáló az SNMP protokoll 3-as verzióját használja. A nyomtatókiszolgáló biztonságos kezeléséhez használja az SNMPv3 módot.
Disabled (Letiltva)	Tiltsa le az SNMP protokoll 3 verzióját. Korlátozva lesz minden olyan alkalmazás, amely az SNMPv3-at használja. Az SNMPv3 alkalmazások engedélyezéséhez használja az SNMPv3 módot.

8. Kattintson a **Submit (Küldés)** gombra.

Ha a készülék megjeleníti a protokoll-beállítási opciókat, válassza ki a kívánt beállításokat.

9. A konfiguráció aktiválásához indítsa újra a készüléket.

Kapcsolódó tájékoztatás

- SNMPv3 használata

IPsec használata

- Az IPsec bemutatása
- Az IPsec konfigurálása a Web alapú kezelővel
- IPsec címsablon konfigurálása a Web alapú kezelővel
- IPsec sablon konfigurálása a Web alapú kezelővel

Az IPsec bemutatása

Az IPsec (Internet Protocol Security – Internetbiztonsági protokoll) egy olyan biztonsági protokoll, amely egy kiegészítő internetprotokoll-funkciót használ az adatmanipuláció megelőzéséhez és az IP-csomagokként átvitt adatok védelmének biztosításához. Az IPsec titkosítja a hálózaton keresztül továbbított adatokat, így például a számítógépekről egy nyomtatóra küldött adatokat. Mivel az adatok titkosítása a hálózati rétegben történik, a magasabb szintű protokollt használó alkalmazások IPsec funkciót használnak még akkor is, ha erről a felhasználó nem tud.

Az IPsec a következő funkciókat támogatja

- IPsec-átvitelek

  Az IPsec beállításoknak megfelelően a hálózatra csatlakoztatott számítógép adatokat küld és adatokat fogad a megadott eszközzel IPsec segítségével felépített kapcsolaton keresztül. Amikor az eszközök IPsec használatával kommunikálni kezdenek, a kulcsok először az internetes kulcscsere (IKE) használatával vannak kicserélve, majd a titkosított adatok a kulcsok használatával vannak elküldve.

  Ezenfelül az IPsec két működési móddal rendelkezik: az Átvitel móddal és a Csatorna móddal. Az Átviteli mód többnyire az eszközök közötti kommunikáció, a Bújtatás mód pedig például a virtuális magánhálózat (VPN) és a hasonló környezetek esetén használatos.

Az IPsec-átvitelnél a következő feltételek szükségesek:

- IPsec-alapú kommunikációra alkalmas számítógép csatlakozik a hálózathoz.
- Készülékét IPsec-kommunikációhoz kell konfigurálni.
- A készülékéhez csatlakozó számítógép IPsec-kapcsolatokhoz van konfigurálva.

- IPsec-beállítások

  Az IPsec protokollt használó kapcsolatok esetében szükséges beállítások. Ezen beállítások a Web alapú kezelő használatával konfigurálhatók.

Az IPsec-beállítások konfigurálásához egy, a hálózathoz csatlakoztatott számítógép böngészőjét kell használnia.

Kapcsolódó tájékoztatás

- IPsec használata

Az IPsec konfigurálása a Web alapú kezelővel

Az IPsec csatlakozás feltételei két **Template (Sablon)** típusra oszthatók: **Address (cím)** és **IPsec**. Legfeljebb 10 kapcsolatfeltételt konfigurálhat.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **IPsec** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Konfigurálja be a beállításait.

Beállítás	Leírás
Status (Állapot)	Engedélyezze vagy tiltsa le az IPsec opciót.
Negotiation Mode (Egyeztetés módja)	Válassza ki az IKE 1. fázisának **Negotiation Mode (Egyeztetés módja)** beállítását. Az IKE egy protokoll, amely titkosítási kulcsok cseréjére szolgál az IPsec-alapú titkosított kommunikáció kivitelezése érdekében. A **Main (Fő)** módban a feldolgozási sebesség alacsony, a biztonsági szint azonban magas. **Aggressive (Agresszív)** módban a feldolgozási sebesség gyorsabb, mint **Main (Fő)** módban, de a biztonság alacsonyabb.
All Non-IPsec Traffic (Minden nem IPsec forgalom)	Adja meg a nem IPsec csomagok esetén érvényes akciót. A Webszolgáltatások használatakor az **Allow (Engedélyezés)** lehetőséget kell kiválasztania az **All Non-IPsec Traffic (Minden nem IPsec forgalom)** beállításhoz. Ha kiválasztja a **Drop (Elvetés)** lehetőséget, a webszolgáltatások nem használhatók.
Broadcast/Multicast Bypass (Üzenetszórás/csoportos küldés megkerülése)	Jelölje ki az **Enabled (Engedélyezve)** vagy a **Disabled (Letiltva)** lehetőséget.
Protocol Bypass (Protokoll megkerülése)	Jelölje be a kívánt opciók jelölőnégyzetét.
Rules (Szabályok)	Jelölje be az **Enabled (Engedélyezve)** jelölőnégyzetet a sablon aktiválásához. Ha több jelölőnégyzet is bejelöl, akkor az alacsonyabb számmal jelölt jelölőnégyzetek kapnak prioritást abban az esetben, ha a jelölőnégyzetek használatával megadott beállítások ütköznek egymással. A kapcsolódó legördülő listára kattintva válassza ki az IPsec kapcsolati feltételekhez használt **Address Template (Címsablon)** opciót. **Address Template (Címsablon)** hozzáadásához kattintson az **Add Template (Sablon hozzáadása)** lehetőségre. A kapcsolódó legördülő listára kattintva válassza ki az IPsec kapcsolati feltételekhez használt **IPsec Template (IPsec-sablon)**

Beállítás	Leírás
	opciót. **IPsec Template (IPsec-sablon)** hozzáadásához kattintson az **Add Template (Sablon hozzáadása)** lehetőségre.

6. Kattintson a **Submit (Küldés)** gombra.

   Ha a készüléket újra kell indítani az új beállítások aktiválásához, megjelenik az újraindítást megerősítő képernyő.

   Ha üres elem található az engedélyezett sablonon a **Rules (Szabályok)** táblázatban, megjelenik egy hibaüzenet. Hagyja jóvá a választásokat, és kattintson ismét a **Submit (Küldés)** lehetőségre.

Kapcsolódó tájékoztatás

- IPsec használata

Kapcsolódó témák:

- Tanúsítványok konfigurálása az eszközbiztonság számára

IPsec címsablon konfigurálása a Web alapú kezelővel

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **IPsec Address Template (IPsec-címsablon)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Kattintson a **Delete (Törlés)** gombra, ha törölni szeretne egy **Address Template (Címsablon)**-t. Ha egy **Address Template (Címsablon)** használatban van, nem lehet törölni.
6. Kattintson a létrehozni kívánt **Address Template (Címsablon)** elemre. Megjelenik az **IPsec Address Template (IPsec-címsablon)**.
7. Konfigurálja be a beállításait.

Beállítás	Leírás
Template Name (Sablon neve)	Írja be a sablon nevét (legfeljebb 16 karakter).
Local IP Address (Helyi IP-cím)	• **IP Address (IP-cím)** Adja meg az IP-címet. Válassza ki az **ALL IPv4 Address (MINDEN IPv4-cím)**, **ALL IPv6 Address (MINDEN IPv6-cím)**, **All Link Local IPv6 (Minden Link Local IPv6)** vagy **Custom (Egyedi)** elemet a legördülő listából. Ha a **Custom (Egyedi)** lehetőséget választotta ki a legördülő listából, írja be a meghatározott IP-címet (IPv4 vagy IPv6) a szövegmezőbe. • **IP Address Range (IP-cím tartománya)** A szövegmezőkben adja meg az IP-címtartomány kezdő és befejező IP-címét. Ha a kezdő és záró IP-cím nem standardized IPv4 vagy IPv6 IP-cím, vagy a záró IP-cím kisebb, mint a kezdő cím, akkor hibaüzenet jelenik meg. • **IP Address / Prefix (IP-cím / Előtag)** Adja meg az IP-címet CIDR formátumban. Például: 192.168.1.1/24 Mivel a 192.168.1.1 cím előtagja 24 bites alhálózati maszk (255.255.255.0) formájában van megadva, a 192.168.1.### címek érvényesek.
Remote IP Address (Távoli IP-cím)	• **Any (Bármilyen)** Ha az **Any (Bármilyen)** beállítást választja, minden IP-cím engedélyezve van. • **IP Address (IP-cím)** Írja be a meghatározott IP-címet (IPv4 vagy IPv6) a szövegmezőbe. • **IP Address Range (IP-cím tartománya)**

Beállítás	Leírás
	Írja be a kezdő és a záró IP-címet az IP-címtartomány számára. Ha az első és az utolsó IP-cím nem standardized IPv4 vagy IPv6 IP-cím, vagy az utolsó IP-cím kisebb, mint az első cím, akkor hibaüzenet jelenik meg. • **IP Address / Prefix (IP-cím / Előtag)** Adja meg az IP-címet CIDR formátumban. Például: 192.168.1.1/24 Mivel a 192.168.1.1 cím előtagja 24 bites alhálózati maszk (255.255.255.0) formájában van megadva, a 192.168.1.### címek érvényesek.

8. Kattintson a **Submit (Küldés)** gombra.

Az aktuálisan használt sablon beállításainak a módosításakor indítsa újra a készüléket a konfiguráció alkalmazásához.

Kapcsolódó tájékoztatás

- IPsec használata

IPsec sablon konfigurálása a Web alapú kezelővel

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Security (Biztonság)** > **IPsec Template (IPsec-sablon)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Kattintson a **Delete (Törlés)** gombra, ha törölni szeretne egy **IPsec Template (IPsec-sablon)**-t. Ha egy **IPsec Template (IPsec-sablon)** használatban van, nem lehet törölni.
6. Kattintson a létrehozni kívánt **IPsec Template (IPsec-sablon)** elemre. Megjelenik a **IPsec Template (IPsec-sablon)** képernyő. A konfigurációs mezők különböznek a kiválasztott **Use Prefixed Template (Előtaggal ellátott sablon használata)** és **Internet Key Exchange (IKE)** beállítások alapján.
7. A **Template Name (Sablon neve)** mezőbe írja be a sablon nevét (legfeljebb 16 karakter).
8. Amennyiben a **Custom (Egyedi)** opciót választotta ki a **Use Prefixed Template (Előtaggal ellátott sablon használata)** legördülő listából, válassza ki a **Internet Key Exchange (IKE)** opciókat, majd szükség szerint módosítsa a beállításokat.
9. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- IPsec használata
  - IPsec sablonok IKEv1-beállításai
  - IPsec sablonok IKEv2-beállításai
  - IPsec sablonok kézi beállításai

IPsec sablonok IKEv1-beállításai

Beállítás	Leírás
Template Name (Sablon neve)	Írja be a sablon nevét (legfeljebb 16 karakter).
Use Prefixed Template (Előtaggal ellátott sablon használata)	Válassza a **Custom (Egyedi)**, **IKEv1 High Security (IKEv1 magas szintű biztonság)** vagy **IKEv1 Medium Security (IKEv1 közepes szintű biztonság)** lehetőséget. A beállítási elemek a kiválasztott sablontól függően eltérnek.
Internet Key Exchange (IKE)	Az IKE egy kommunikációs protokoll, amely titkosítási kulcsok cseréjére szolgál az IPsec-alapú titkosított kommunikáció kivitelezése érdekében. A titkosított kommunikáció kizárólag az adott alkalomkor való kivitelezése érdekében a rendszer meghatározza az IPsec használatához szükséges titkosítási algoritmust, majd megosztja a titkosítási kulcsokat. Az IKE esetében a titkosítási kulcsok cseréje a Diffie-Hellman kulcscserélési módszer használatával történik, és az internetes kulcscserére korlátozott titkosított kommunikáció valósul meg. Amennyiben a **Custom (Egyedi)** opciót választotta ki a **Use Prefixed Template (Előtaggal ellátott sablon használata)** területen, válassza a **IKEv1** lehetőséget.
Authentication Type (Hitelesítés típusa)	• **Diffie_Hellman_Group** Ez a kulcscserélési módszer lehetővé teszi a titkos kulcsok nem védett hálózaton keresztül történő biztonságos cseréjét. A Diffie-Hellman kulcscserélési módszer a titkos kulcs helyett egy diszkrét logaritmus problémát használ a nyílt információ küldésére és fogadására, amely egy véletlenszerű szám és a titkos kulcs használatával jött létre. Válassza a(z) **Group1 (1. csoport)**, **Group2 (2. csoport)**, **Group5 (5. csoport)**, vagy **Group14 (14. csoport)** lehetőséget. • **Encryption (Titkosítás)** Válassza a(z) **DES**, **3DES**, **AES-CBC 128**, vagy **AES-CBC 256** lehetőséget. • **Hash (Kivonat)** Válassz a(z) **MD5**, **SHA1**, **SHA256**, **SHA384** vagy **SHA512** lehetőséget. • **SA Lifetime (SA-élettartam)** Adja meg az IKE SA-élettartamot. Írja be az időt (másodpercben) és a kilobájtok (Kbájt) számát.
Encapsulating Security (Beágyazó biztonság)	• **Protocol (Protokoll)** Válassza a(z) **ESP**, **AH**, vagy **AH+ESP** lehetőséget.

Beállítás	Leírás
	- Az ESP egy, az IPsec használatával kivitelezett titkosított kommunikációhoz kifejlesztett protokoll. Az ESP titkosítja az adatokat (küldött tartalmat), és további információkat ad hozzá. Az IP-csomagok a fejlécből és a titkosított adatokból állnak, amelyeket a fejléc követ. A titkosított adatok mellett az IP-csomag információkat tartalmaz a titkosítási módszerrel, a titkosítási kulccsal, a hitelesítési adatokkal stb. kapcsolatban is. - Az AH az IPsec protokoll része, amely hitelesíti a feladót, és megakadályozza az adatok manipulálását (biztosítja az adatok teljességét). Az IP-csomagban az adatok közvetlenül a fejléc után állnak. A csomagok továbbá kivonatértékeket is tartalmaznak, amelyek kiszámítása az adatküldő hamisításának, valamint az adatok manipulálásának megakadályozása érdekében a kommunikált tartalmakból, titkos kulcsból stb. származó egyenlet használatával történik. Az ESP protokollal ellentétben a kommunikált tartalmak nincsenek titkosítva, és az adatok fogadása és küldése egyszerű szöveg formátumban történik. • **Encryption (Titkosítás) (Nem elérhető a AH opció esetén.)** Válassza a(z) **DES**, **3DES**, **AES-CBC 128**, vagy **AES-CBC 256** lehetőséget. • **Hash (Kivonat)** Válassza ki a **None (Semmi)**, **MD5**, **SHA1**, **SHA256**, **SHA384** vagy **SHA512** lehetőséget. A **None (Semmi)** csak akkor választható, ha az **ESP** lehetőség van kiválasztva a **Protocol (Protokoll)** beállításhoz. • **SA Lifetime (SA-élettartam)** Adja meg az IKE SA élettartamát. Adja meg az időtartamot (másodperc) és a kilobájtok számát (Kbájt). • **Encapsulation Mode (Beágyazási mód)** Válassza az **Transport (Átvitel)** vagy a **Tunnel (Alagút)** lehetőséget. • **Remote Router IP-Address (Távoli útválasztó IP-címe)** Írja be a távoli router IP-címét (IPv4 vagy IPv6). Csak akkor adja meg ezt az információt, ha a **Tunnel (Alagút)** mód van kiválasztva. Az SA (Biztonsági társítás) egy IPsec vagy IPv6 szabványt használó titkosított kommunikációs módszer, amely információt (például a titkosítási módszert és a titkosítási kulcsot) cserél és oszt meg, és ezáltal biztonságos kommunikációs csatornát hoz létre a kommunikáció megkezdése előtt. Az SA egy létrejött virtuális titkosított kommunikációs csatornára is utalhat. Az IPsec-kommunikációhoz használt SA megállapítja a titkosítási módszert, kicseréli a kulcsokat, valamint kölcsönös hitelesítést végez az IKE (internetes kulcscsere) szabványos eljárásnak megfelelően. Az SA továbbá rendszeresen frissül.
Perfect Forward Secrecy (PFS) (Sérülés utáni titkosságvédelem)	A PFS nem származtat kulcsokat a korábbi, üzenetek titkosítására használt kulcsokból. Ezenfelül, ha egy üzenet titkosításához használt kulcs egy szülőkulcsból származik, az a szülőkulcs többé nem lesz más kulcsok származtatásához használva. Így egy kulcs feltörésekor a sérülés kizárólag azokra az üzenetekre korlátozódik, amelyek titkosítása az adott kulcs használatával történt. Válassza ki a **Enabled (Engedélyezve)** vagy a **Disabled (Letiltva)** lehetőséget.

Beállítás	Leírás
Authentication Method (Hitelesítési módszer)	Válassza ki a hitelesítési módszert. Válassza ki a **Pre-Shared Key (Előmegosztott kulcs)** vagy a **Certificates (Tanúsítványok)** lehetőséget.
Pre-Shared Key (Előmegosztott kulcs)	A kommunikáció titkosításakor a titkosítókulcsot előre ki kell cserélni és meg kell osztani egy másik csatorna használatával. Ha az **Authentication Method (Hitelesítési módszer)** beállításaként a **Pre-Shared Key (Előmegosztott kulcs)** lehetőséget választotta, adja meg a **Pre-Shared Key (Előmegosztott kulcs)** értékét (legfeljebb 32 karakter). • **Local/ID Type/ID (Helyi/Azonosítótípus/Azonosító)** Válassza ki a feladó azonosítójának típusát, majd adja meg az azonosítót. Válassza ki az **IPv4 Address (IPv4-cím)**, **IPv6 Address (IPv6-cím)**, **FQDN**, **E-mail Address (E-mail cím)** vagy **Certificate (Tanúsítvány)** lehetőséget a típushoz. Ha a **Certificate (Tanúsítvány)** lehetőséget választja, írja be a tanúsítvány közös nevét az **ID (Azonosító)** mezőbe. • **Remote/ID Type/ID (Távoli/Azonosítótípus/Azonosító)** Válassza ki a fogadó azonosítójának típusát, majd adja meg az azonosítót. Válassza ki az **IPv4 Address (IPv4-cím)**, **IPv6 Address (IPv6-cím)**, **FQDN**, **E-mail Address (E-mail cím)** vagy **Certificate (Tanúsítvány)** lehetőséget a típushoz. Ha a **Certificate (Tanúsítvány)** lehetőséget választja, írja be a tanúsítvány közös nevét az **ID (Azonosító)** mezőbe.
Certificate (Tanúsítvány)	Ha az **Authentication Method (Hitelesítési módszer)** beállításaként a **Certificates (Tanúsítványok)** lehetőséget választotta, válassza ki a tanúsítványt. Csak azokat a tanúsítványokat választhatja ki, amelyeket a Web alapú kezelő Biztonsági konfiguráció képernyőjének **Certificate (Tanúsítvány)** lapján hoztak létre.

Kapcsolódó tájékoztatás

- IPsec sablon konfigurálása a Web alapú kezelővel

IPsec sablonok IKEv2-beállításai

Beállítás	Leírás
Template Name (Sablon neve)	Írja be a sablon nevét (legfeljebb 16 karakter).
Use Prefixed Template (Előtaggal ellátott sablon használata)	Válassza a **Custom (Egyedi)**, a **IKEv2 High Security (IKEv2 magas szintű biztonság)** vagy a **IKEv2 Medium Security (IKEv2 közepes szintű biztonság)** lehetőséget. A beállítási elemek a kiválasztott sablontól függően eltérnek.
Internet Key Exchange (IKE)	Az IKE egy kommunikációs protokoll, amely titkosítási kulcsok cseréjére szolgál az IPsec-alapú titkosított kommunikáció kivitelezése érdekében. A titkosított kommunikáció kizárólag az adott alkalomkor való kivitelezése érdekében a rendszer meghatározza az IPsec használatához szükséges titkosítási algoritmust, majd megosztja a titkosítási kulcsokat. Az IKE esetében a titkosítási kulcsok cseréje a Diffie-Hellman kulcscserélési módszer használatával történik, és az internetes kulcscserére korlátozott titkosított kommunikáció valósul meg. Amennyiben a **Custom (Egyedi)** opciót választotta ki a **Use Prefixed Template (Előtaggal ellátott sablon használata)** területen, válassza a **IKEv2** lehetőséget.
Authentication Type (Hitelesítés típusa)	• **Diffie_Hellman_Group** Ez a kulcscserélési módszer lehetővé teszi a titkos kulcsok nem védett hálózaton keresztül történő biztonságos cseréjét. A Diffie-Hellman kulcscserélési módszer a titkos kulcs helyett egy diszkrét logaritmus problémát használ a nyílt információ küldésére és fogadására, amely egy véletlenszerű szám és a titkos kulcs használatával jött létre. Válassza a(z) **Group1 (1. csoport)**, **Group2 (2. csoport)**, **Group5 (5. csoport)**, vagy **Group14 (14. csoport)** lehetőséget. • **Encryption (Titkosítás)** Válassza a(z) **DES**, **3DES**, **AES-CBC 128**, vagy **AES-CBC 256** lehetőséget. • **Hash (Kivonat)** Válassz a(z) **MD5**, **SHA1**, **SHA256**, **SHA384** vagy **SHA512** lehetőséget. • **SA Lifetime (SA-élettartam)** Adja meg az IKE SA-élettartamot. Írja be az időt (másodpercben) és a kilobájtok (Kbájt) számát.
Encapsulating Security (Beágyazó biztonság)	• **Protocol (Protokoll)** Válassza ki a **ESP** elemet. Az ESP egy, az IPsec használatával kivitelezett titkosított kommunikációhoz kifejlesztett protokoll. Az ESP titkosítja az adatokat (küldött tartalmat), és további információkat ad hozzá. Az IP-csomagok a fejlécből és a titkosított adatokból állnak, amelyeket a fejléc követ. A titkosított adatok mellett az IP-csomag információkat tartalmaz a titkosítási módszerrel, a titkosítási kulccsal, a hitelesítési adatokkal stb. kapcsolatban is. • **Encryption (Titkosítás)** Válassza a **DES**, a **3DES**, az **AES-CBC 128** vagy az **AES-CBC 256** lehetőséget. • **Hash (Kivonat)** Válassza a(z) **MD5**, **SHA1**, **SHA256**, **SHA384** vagy **SHA512** lehetőséget.

Beállítás	Leírás
	• **SA Lifetime (SA-élettartam)** Adja meg az IKE SA élettartamát. Adja meg az időtartamot (másodperc) és a kilobájtok számát (Kbájt). • **Encapsulation Mode (Beágyazási mód)** Válassza az **Transport (Átvitel)** vagy a **Tunnel (Alagút)** lehetőséget. • **Remote Router IP-Address (Távoli útválasztó IP-címe)** Írja be a távoli router IP-címét (IPv4 vagy IPv6). Csak akkor adja meg ezt az információt, ha a **Tunnel (Alagút)** mód van kiválasztva. Az SA (Biztonsági társítás) egy IPsec vagy IPv6 szabványt használó titkosított kommunikációs módszer, amely információt (például a titkosítási módszert és a titkosítási kulcsot) cserél és oszt meg, és ezáltal biztonságos kommunikációs csatornát hoz létre a kommunikáció megkezdése előtt. Az SA egy létrejött virtuális titkosított kommunikációs csatornára is utalhat. Az IPsec-kommunikációhoz használt SA megállapítja a titkosítási módszert, kicseréli a kulcsokat, valamint kölcsönös hitelesítést végez az IKE (internetes kulcscsere) szabványos eljárásnak megfelelően. Az SA továbbá rendszeresen frissül.
Perfect Forward Secrecy (PFS) (Sérülés utáni titkosságvédelem)	A PFS nem származtat kulcsokat a korábbi, üzenetek titkosítására használt kulcsokból. Ezenfelül, ha egy üzenet titkosításához használt kulcs egy szülőkulcsból származik, az a szülőkulcs többé nem lesz más kulcsok származtatásához használva. Így egy kulcs feltörésekor a sérülés kizárólag azokra az üzenetekre korlátozódik, amelyek titkosítása az adott kulcs használatával történt. Válassza ki a **Enabled (Engedélyezve)** vagy a **Disabled (Letiltva)** lehetőséget.
Authentication Method (Hitelesítési módszer)	Válassza ki a hitelesítési módszert. Válassza a **Pre-Shared Key (Előmegosztott kulcs)**, **Certificates (Tanúsítványok)**, **EAP - MD5** vagy a **EAP - MS-CHAPv2** lehetőséget. Az EAP egy olyan hitelesítési protokoll, amely a PPP kiterjesztése. Az EAP és az IEEE802.1x együttes használatával a rendszer különböző kulcsot használ a felhasználók hitelesítésére az egyes munkamenetek során. A következő beállítások csak akkor szükségesek, ha az **EAP - MD5** vagy **EAP - MS-CHAPv2** lehetőség van kiválasztva a **Authentication Method (Hitelesítési módszer)** beállításaiban: • **Mode (üzemmód)** Jelölje ki az **Server-Mode (Kiszolgáló mód)** vagy a **Client-Mode (Ügyfél mód)** lehetőséget. • **Certificate (Tanúsítvány)** Válassza ki a tanúsítványt. • **User Name (Felhasználónév)** Írja be a felhasználónevet (legfeljebb 32 karakter). • **Password (Jelszó)** Írja be a jelszót (legfeljebb 32 karakter). A jelszót kétszer kell megadni a megerősítéshez.
Pre-Shared Key (Előmegosztott kulcs)	A kommunikáció titkosításakor a titkosítókulcsot előre ki kell cserélni és meg kell osztani egy másik csatorna használatával. Ha az **Authentication Method (Hitelesítési módszer)** beállításaként a **Pre-Shared Key (Előmegosztott kulcs)** lehetőséget választotta, adja

Beállítás	Leírás
	meg a **Pre-Shared Key (Előmegosztott kulcs)** értékét (legfeljebb 32 karakter). • **Local/ID Type/ID (Helyi/Azonosítótípus/Azonosító)** Válassza ki a feladó azonosítójának típusát, majd adja meg az azonosítót. Válassza ki az **IPv4 Address (IPv4-cím)**, **IPv6 Address (IPv6-cím)**, **FQDN**, **E-mail Address (E-mail cím)** vagy **Certificate (Tanúsítvány)** lehetőséget a típushoz. Ha a **Certificate (Tanúsítvány)** lehetőséget választja, írja be a tanúsítvány közös nevét az **ID (Azonosító)** mezőbe. • **Remote/ID Type/ID (Távoli/Azonosítótípus/Azonosító)** Válassza ki a fogadó azonosítójának típusát, majd adja meg az azonosítót. Válassza ki az **IPv4 Address (IPv4-cím)**, **IPv6 Address (IPv6-cím)**, **FQDN**, **E-mail Address (E-mail cím)** vagy **Certificate (Tanúsítvány)** lehetőséget a típushoz. Ha a **Certificate (Tanúsítvány)** lehetőséget választja, írja be a tanúsítvány közös nevét az **ID (Azonosító)** mezőbe.
Certificate (Tanúsítvány)	Ha az **Authentication Method (Hitelesítési módszer)** beállításaként a **Certificates (Tanúsítványok)** lehetőséget választotta, válassza ki a tanúsítványt. Csak azokat a tanúsítványokat választhatja ki, amelyeket a Web alapú kezelő Biztonsági konfiguráció képernyőjének **Certificate (Tanúsítvány)** lapján hoztak létre.

Kapcsolódó tájékoztatás

- IPsec sablon konfigurálása a Web alapú kezelővel

IPsec sablonok kézi beállításai

Beállítás	Leírás
Template Name (Sablon neve)	Írja be a sablon nevét (legfeljebb 16 karakter).
Use Prefixed Template (Előtaggal ellátott sablon használata)	Jelölje ki a(z) **Custom (Egyedi)** elemet.
Internet Key Exchange (IKE)	Az IKE egy kommunikációs protokoll, amely titkosítási kulcsok cseréjére szolgál az IPsec-alapú titkosított kommunikáció kivitelezése érdekében. A titkosított kommunikáció kizárólag az adott alkalomkor való kivitelezése érdekében a rendszer meghatározza az IPsec használatához szükséges titkosítási algoritmust, majd megosztja a titkosítási kulcsokat. Az IKE esetében a titkosítási kulcsok cseréje a Diffie-Hellman kulcscserélési módszer használatával történik, és az internetes kulcscserére korlátozott titkosított kommunikáció valósul meg. Jelölje ki a(z) **Manual (Kézikönyv)** elemet.
Authentication Key (ESP, AH) (Hitelesítési kulcs (ESP, AH))	Adja meg az **In/Out (Be/Ki)** értékeket. Ezek a beállítások akkor szükségesek, ha a **Custom (Egyedi)** lehetőség van kiválasztva a **Use Prefixed Template (Előtaggal ellátott sablon használata)** beállításhoz, a **Manual (Kézikönyv)** lehetőség van kiválasztva az **Internet Key Exchange (IKE)** beállításhoz, valamint nem a **None (Semmi)** lehetőség van kiválasztva a **Hash (Kivonat)** beállításhoz az **Encapsulating Security (Beágyazó biztonság)** szakaszban. A beállítható karakterek száma attól függően változik, hogy milyen beállításokat adott meg az **Hash (Kivonat)** lehetőséghez az **Encapsulating Security (Beágyazó biztonság)** szakaszban. Ha a megadott hitelesítési kulcs hossza eltér a kiválasztott hash-algoritmustól, akkor hiba történik. • **MD5**: 128 bit (16 bájt) • **SHA1**: 160 bit (20 bájt) • **SHA256**: 256 bit (32 bájt) • **SHA384**: 384 bit (48 bájt) • **SHA512**: 512 bit (64 bájt) Ha ASCII-kódokkal adja meg a kulcsot, akkor zárja a karaktereket idézőjelek (") közé.
Code key (ESP) (Kódkulcs (ESP))	Adja meg az **In/Out (Be/Ki)** értékeket. Ezek a beállítások akkor szükségesek, ha **Custom (Egyedi)** van kiválasztva **Use Prefixed Template (Előtaggal ellátott sablon használata)** beállításhoz, **Manual (Kézikönyv)** van kiválasztva **Internet Key Exchange (IKE)** beállításhoz, és **ESP** beállítás van megadva **Protocol (Protokoll)** beállításhoz a **Encapsulating Security (Beágyazó biztonság)** lehetőségben.

Beállítás	Leírás
	A beállítható karakterek száma attól függően változik, hogy milyen beállításokat adott meg az **Encryption (Titkosítás)** lehetőséghez az **Encapsulating Security (Beágyazó biztonság)** szakaszban. Ha a megadott kulcs hossza eltér a kiválasztott titkosítási algoritmustól, akkor hiba történik. • **DES**: 64 bit (8 bájt) • **3DES**: 192 bit (24 bájt) • **AES-CBC 128**: 128 bit (16 bájt) • **AES-CBC 256**: 256 bit (32 bájt) Ha ASCII-kódokkal adja meg a kulcsot, akkor zárja a karaktereket idézőjelek (") közé.
SPI	Ezek a paraméterek a biztonsági adatok azonosítására szolgálnak. Egy gazdagép általában több biztonsági társítással (SA) rendelkezik az IPsec-kommunikáció különböző típusai számára. Ezért az IPsec-csomagok fogadásakor meg kell határozni az alkalmazandó biztonsági társítást. Az SPI paraméter, amely meghatározza a biztonsági társítást, a hitelesítési fejlécben (AH) és az ESP (Encapsulating Security Payload) fejlécben található. Ezek a beállítások akkor szükségesek, amikor a **Custom (Egyedi)** lehetőség van megadva a **Use Prefixed Template (Előtaggal ellátott sablon használata)** beállításhoz, illetve a **Manual (Kézikönyv)** lehetőség van megadva az **Internet Key Exchange (IKE)** beállításhoz. Írja be az **In/Out (Be/Ki)** értékeket. (3-10 karakter)
Encapsulating Security (Beágyazó biztonság)	• **Protocol (Protokoll)** Válassza ki a **ESP** vagy a **AH** lehetőséget. - Az ESP egy, az IPsec használatával kivitelezett titkosított kommunikációhoz kifejlesztett protokoll. Az ESP titkosítja az adatokat (küldött tartalmat), és további információkat ad hozzá. Az IP-csomagok a fejlécből és a titkosított adatokból állnak, amelyeket a fejléc követ. A titkosított adatok mellett az IP-csomag információkat tartalmaz a titkosítási módszerrel, a titkosítási kulccsal, a hitelesítési adatokkal stb. kapcsolatban is. - Az AH az IPsec protokoll része, amely hitelesíti a feladót, és megakadályozza az adatok manipulálását (biztosítja az adatok teljességét). Az IP-csomagban az adatok közvetlenül a fejléc után állnak. A csomagok továbbá kivonatértékeket is tartalmaznak, amelyek kiszámítása az adatküldő hamisításának, valamint az adatok manipulálásának megakadályozása érdekében a kommunikált tartalmakból, titkos kulcsból stb. származó egyenlet használatával történik. Az ESP protokollal ellentétben a kommunikált tartalmak nincsenek titkosítva, és az adatok fogadása és küldése egyszerű szöveg formátumban történik. • **Encryption (Titkosítás) (Nem elérhető a AH opció esetén.)** Válassza a(z) **DES**, **3DES**, **AES-CBC 128**, vagy **AES-CBC 256** lehetőséget. • **Hash (Kivonat)** Válassza ki a **None (Semmi)**, **MD5**, **SHA1**, **SHA256**, **SHA384** vagy **SHA512** lehetőséget. A **None (Semmi)** csak akkor választható, ha az **ESP** lehetőség van kiválasztva a **Protocol (Protokoll)** beállításhoz. • **SA Lifetime (SA-élettartam)** Adja meg az IKE SA élettartamát.

Beállítás	Leírás
	Adja meg az időtartamot (másodperc) és a kilobájtok számát (Kbájt). • **Encapsulation Mode (Beágyazási mód)** Válassza az **Transport (Átvitel)** vagy a **Tunnel (Alagút)** lehetőséget. • **Remote Router IP-Address (Távoli útválasztó IP-címe)** Írja be a távoli router IP-címét (IPv4 vagy IPv6). Csak akkor adja meg ezt az információt, ha a **Tunnel (Alagút)** mód van kiválasztva. Az SA (Biztonsági társítás) egy IPsec vagy IPv6 szabványt használó titkosított kommunikációs módszer, amely információt (például a titkosítási módszert és a titkosítási kulcsot) cserél és oszt meg, és ezáltal biztonságos kommunikációs csatornát hoz létre a kommunikáció megkezdése előtt. Az SA egy létrejött virtuális titkosított kommunikációs csatornára is utalhat. Az IPsec-kommunikációhoz használt SA megállapítja a titkosítási módszert, kicseréli a kulcsokat, valamint kölcsönös hitelesítést végez az IKE (internetes kulcscsere) szabványos eljárásnak megfelelően. Az SA továbbá rendszeresen frissül.

Kapcsolódó tájékoztatás

- IPsec sablon konfigurálása a Web alapú kezelővel

IEEE 802.1x hitelesítés használata a hálózaton

Mi az az IEEE 802.1x hitelesítés?

Az IEEE 802.1x az IEEE egyik szabványa, amely korlátozza a unauthorized hálózati eszközökről történő hozzáférést. Brother készüléke hitelesítési kérést küld egy RADIUS kiszolgálónak (hitelesítési kiszolgálónak) a hozzáférési ponton vagy HUB-on keresztül. Miután a RADIUS kiszolgáló ellenőrizte a kérést, az adott készülék hozzáférhet a hálózathoz.

Kapcsolódó tájékoztatás

- IEEE 802.1x hitelesítés használata a hálózaton

Az IEEE 802.1x hitelesítés beállítása a hálózaton a Web alapú kezelés (böngésző) segítségével

- Ha készülékét EAP-TLS hitelesítés használatára állítja be, akkor a konfiguráció megkezdése előtt előbb a CA által kiadott kliens tanúsítványt kell telepítenie. A klienstanúsítvánnyal kapcsolatban keresse a hálózati rendszergazdát. Ha egynél több tanúsítványt telepített, azt ajánljuk, hogy írja fel a használni kívánt tanúsítvány nevét.
- A kiszolgáló tanúsítványának ellenőrzése előtt először importálnia kell a CA tanúsítványt attól a CA-tól, amelyik aláírta a kiszolgáló tanúsítványát. Vegye fel a kapcsolatot a hálózat rendszergazdájával vagy az internetszolgáltatóval, hogy biztos lehessen abban, hogy a CA tanúsítvány importálása valóban szükséges.

Az IEEE 802.1x hitelesítést a vezeték nélküli beállítási varázslót használva, a kezelőpanelen keresztül (Vezeték nélküli hálózat) is konfigurálhatja.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Tegye az alábbiak valamelyikét:
   - Vezetékes hálózat esetében

     Kattintson a(z) **Wired (Vezetékes)** > **Wired 802.1x Authentication (Vezetékes 802.1x-hitelesítés)** gombra.
   - Vezeték nélküli hálózat esetében

     Kattintson a(z) **Wireless (Vezeték nélküli)** > **Wireless (Enterprise) (Vezeték nélküli (vállalati))** gombra.
6. Konfigurálja az IEEE 802.1x hitelesítési beállításokat.

   - Az IEEE 802.1x hitelesítés engedélyezéséhez a vezetékes hálózaton, válassza ki a **Enabled (Engedélyezve)** opciót a **Wired 802.1x status (Vezetékes 802.1x-hitelesítés állapota)** elemhez a **Wired 802.1x Authentication (Vezetékes 802.1x-hitelesítés)** oldalon.
   - Ha **EAP-TLS** hitelesítést használ, az ellenőrzésre a telepített ügyféltanúsítványt kell kiválasztania (a tanúsítvány neve szerint megjelenítve) a **Client Certificate (Ügyféltanúsítvány)** legördülő listából.
   - Ha az **EAP-FAST**, **PEAP**, **EAP-TTLS** vagy **EAP-TLS** hitelesítést választja, az ellenőrzési módszert a **Server Certificate Verification (Kiszolgálói tanúsítvány ellenőrzése)** legördülő listából választhatja ki. A kiszolgálói tanúsítványt a tanúsítványt aláíró hitelesítésszolgáltató által kiadott CA-tanúsítvány használatával ellenőrizheti, amelyet előzőleg importálni kell a készüléken.

   A **Server Certificate Verification (Kiszolgálói tanúsítvány ellenőrzése)** legördülő listából a következő ellenőrzési módszerek egyikét válassza ki:

Beállítás	Leírás
No Verification (Nincs ellenőrzés)	A kiszolgálói tanúsítvány mindig megbízható. A készülék nem hajtja végre az ellenőrzést.
CA Cert. (CA-tanúsítvány)	A kiszolgálói tanúsítvány CA megbízhatóságának ellenőrzésére használt módszer, a kiszolgálói tanúsítványt aláíró hitelesítésszolgáltató által kiadott CA-tanúsítvány felhasználásával.
CA Cert. + ServerID (CA-tanúsítvány + kiszolgáló azonosítója)	A kiszolgálói tanúsítvány közös nevének ellenőrzésére használt módszer [1], a kiszolgálói tanúsítvány CA megbízhatósága mellett.

7. A konfiguráció befejezését követően kattintson a **Submit (Küldés)** lehetőségre.

   Vezetékes hálózatok esetén: A beállítás után csatlakoztassa a készülékét az IEEE 802.1x hitelesítést támogató hálózatra. Néhány perc múlva nyomtassa ki a Hálózati konfiguráció jelentést, és ellenőrizze a <**Wired IEEE 802.1x**> állapotát.

Beállítás	Leírás
Success	A vezetékes IEEE 802.1x funkció engedélyezve van, és a hitelesítés sikeres volt.
Failed	A vezetékes IEEE 802.1x funkció engedélyezve van, azonban a hitelesítés sikertelen volt.
Off	A vezetékes IEEE 802.1x funkció nem áll rendelkezésre.

Kapcsolódó tájékoztatás

- IEEE 802.1x hitelesítés használata a hálózaton

Kapcsolódó témák:

- Biztonsági tanúsítvány jellemzőinek áttekintése
- Tanúsítványok konfigurálása az eszközbiztonság számára

1 A közös név ellenőrzése a kiszolgálói tanúsítvány közös nevét veti össze a **Server ID (Kiszolgáló azonosítója)** elemhez beállított karakterlánccal. Mielőtt ezt a módszert használná, kérdezze meg a rendszeradminisztrátort a kiszolgálói tanúsítvány közös nevéről, majd konfigurálja a kiszolgálói tanúsítvány **Server ID (Kiszolgáló azonosítója)**.

IEEE 802.1x hitelesítési módszerek

EAP-FAST

Az Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) protokollt a Cisco Systems, Inc. fejlesztette ki, amely egy felhasználói azonosítót és egy jelszót használ a hitelesítésre, valamint szimmetrikus kulcsalgoritmusok segítségével hozza létre a tunneled hitelesítési folyamatot.

A Brother készüléke a következő belső hitelesítési módszereket támogatja:

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

EAP-MD5 (vezetékes hálózat)

Az Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) módszer egy felhasználói azonosítót és jelszót használ a kihívás és válaszvárás alapú hitelesítéshez.

PEAP

A Protected Extensible Authentication Protocol (PEAP) az EAP-módszer egyik, a Cisco Systems, Inc., a Microsoft Corporation és RSA Security által fejlesztett változata. A PEAP titkosított SSL (Secure Sockets Layer, Biztonságos adatcsomagolási réteg)/TLS (Átviteli réteg biztonsága) alagutat hoz létre az ügyfél és a hitelesítő kiszolgáló között a felhasználói azonosító és a jelszó elküldéséhez. A PEAP kölcsönös hitelesítést tesz lehetővé a kiszolgáló és az ügyfél között.

A Brother készüléke a következő belső hitelesítési módszereket támogatja:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Az EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) protokollt a Funk Software és a Certicom fejlesztette ki. Az EAP-TTLS a PEAP módszerhez hasonló titkosított SSL alagutat hoz létre egy ügyfél és egy hitelesítési kiszolgáló között a felhasználói azonosító és jelszó átküldésére. Az EAP-TTLS kölcsönös hitelesítést tesz lehetővé a kiszolgáló és az ügyfél között.

A Brother készüléke a következő belső hitelesítési módszereket támogatja:

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

EAP-TLS

Az EAP-TLS (Extensible Authentication Protocol Transport Layer Security) protokoll digitális tanúsítványon alapuló hitelesítést igényel mind az ügyfél-, mind a hitelesítő kiszolgáló oldalán.

Kapcsolódó tájékoztatás

- IEEE 802.1x hitelesítés használata a hálózaton

Felhasználói hitelesítés

- Active Directory hitelesítés használata
- LDAP-hitelesítés használata
- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

Active Directory hitelesítés használata

- Az Active Directory hitelesítés bemutatása
- Az Active Directory hitelesítés konfigurálása a Web alapú kezelővel
- Bejelentkezés készülék beállításainak a módosításához a készülék kezelőpanelén (Active Directory hitelesítés)

Az Active Directory hitelesítés bemutatása

Az Active Directory hitelesítés korlátozza a készülék használatát. Ha az Active Directory hitelesítés engedélyezett, a készülék vezérlőpultja zárolt állapotra vált.A készülék beállításait csak akkor módosíthatja, ha megadott egy felhasználói azonosítót és jelszót.

Az Active Directory hitelesítés a következő funkciókat kínálja:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

- Bejövő nyomtatási adatok tárolása
- Bejövő faxadatok tárolása
- A felhasználói azonosítója alapján szerzi be az e-mail címet az Active Directory kiszolgálóról, amikor a beolvasott adatokat egy e-mail kiszolgálónak küldi el.

  A funkció használatához válassza ki a **On (Bekapcsolva)** opciót a **Get Mail Address (E-mail cím lekérése)** beállításhoz és a **LDAP + kerberos** vagy **LDAP + NTLMv2** hitelesítési módszert. Az e-mail-címe feladóként jelenik meg, amikor a készülék szkennelt adatokat küld egy e-mail kiszolgáló felé, vagy címzettként, amennyiben a szkennelt adatokat saját e-mail-címére kívánja küldeni.

Ha az Active Directory hitelesítés engedélyezve van, készüléke minden bejövő faxadatot tárol. A bejelentkezést követően a készülék kinyomtatja a tárolt faxadatokat.

Az Active Directory hitelesítés beállításait a Web alapú kezelés segítségével módosíthatja.

Kapcsolódó tájékoztatás

- Active Directory hitelesítés használata

Az Active Directory hitelesítés konfigurálása a Web alapú kezelővel

Az Active Directory hitelesítés támogatja a Kerberos-hitelesítést és az NTLMv2-hitelesítést. A hitelesítéshez konfigurálnia kell az SNTP protokollt (hálózati időkiszolgáló) és a DNS kiszolgáló konfigurációt.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. A bal oldali navigációs sávban kattintson erre: **Administrator (Rendszergazda)** > **User Restriction Function (Felhasználókorlátozási funkció)** vagy erre: **Restriction Management (Korlátozáskezelés)**.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Válassza a **Active Directory Authentication (Active Directory hitelesítés)** lehetőséget.
6. Kattintson a **Submit (Küldés)** gombra.
7. Kattintson a **Active Directory Authentication (Active Directory hitelesítés)** gombra.
8. Konfigurálja a következő beállításokat:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

Beállítás	Leírás
Storage Fax RX Data (Fogadott faxadatok tárolása)	A lehetőség kiválasztásával tárolhatja a bejövő faxadatokat. A készülékre való bejelentkezést követően az összes bejövő faxadatot kinyomtathatja.
Remember User ID (Felhasználói azonosító megjegyzése)	Az opció kiválasztása esetén elmentheti a felhasználóazonosítót.
Active Directory Server Address (Active Directory kiszolgáló címe)	Írja be az Active Directory-kiszolgáló IP-címét vagy kiszolgálónevét (például: ad.example.com).
Active Directory Domain Name (Active Directory tartománynéve)	Írja be az Active Directory tartománynevét.
Protocol & Authentication Method (Protokoll és hitelesítési módszer)	elölje ki a protokollt és a azonosítási módot.
SSL/TLS	Válassza az **SSL/TLS** lehetőséget.
LDAP Server Port (LDAP-kiszolgáló portja)	Írja be az Active Directory kiszolgálóhoz LDAP-n keresztül történő csatlakozáshoz használandó portszámot (csak a(z) **LDAP + kerberos** vagy **LDAP + NTLMv2** vagy hitelesítési módszer esetén).

Beállítás	Leírás
LDAP Search Root (LDAP-keresés gyökere)	Írja be az LDAP-keresés gyökerét (csak az **LDAP + kerberos** vagy **LDAP + NTLMv2** vagy hitelesítési módszer esetén érhető el).
Get Mail Address (E-mail cím lekérése)	Az opció kiválasztása esetén a készülék lekéri a bejelentkezett felhasználó e-mail-címét az Active Directory kiszolgálótól. (kizárólag a(z) **LDAP + kerberos** vagy **LDAP + NTLMv2** hitelesítési módszer esetén támogatott)
Get User's Home Directory (Felhasználó alapkönyvtárának beolvasása)	Az opció kiválasztása esetén az Ön kezdőkönyvtárát állítja be a készülék célként hálózatra történő szkenneléshez. (kizárólag a(z) **LDAP + kerberos** vagy **LDAP + NTLMv2** hitelesítési módszer esetén támogatott)

9. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- Active Directory hitelesítés használata

Bejelentkezés készülék beállításainak a módosításához a készülék kezelőpanelén (Active Directory hitelesítés)

Ha az Active Directory hitelesítés engedélyezve van, a készülék kezelőpanele zárolt állapotban marad, amíg meg nem adja felhasználói azonosítóját és jelszavát a kezelőpanelen.

1. A készülék kezelőpanelén adja meg a belépéshez szükséges felhasználói azonosítót és a jelszót.
2. Sikeres hitelesítés esetén a készülék kezelőpanelének zárolása megszűnik.

Kapcsolódó tájékoztatás

- Active Directory hitelesítés használata

LDAP-hitelesítés használata

- Bevezetés LDAP hitelesítéshez
- Az LDAP hitelesítés konfigurálása a Web alapú kezelővel
- A készülék beállításainak a készülék kezelőpanelén keresztül történő módosításához bejelentkezés szükséges (LDAP-hitelesítés)

Bevezetés LDAP hitelesítéshez

Az LDAP-hitelesítés korlátozza a készülék használatát. Ha az LDAP hitelesítés engedélyezett, a készülék vezérlőpultja zárolt állapotra vált. A készülék beállításait csak akkor módosíthatja, ha megadott egy felhasználói azonosítót és jelszót.

Az LDAP hitelesítés a következő funkciókat kínálja:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

- Bejövő nyomtatási adatok tárolása
- Bejövő faxadatok tárolása
- Lekéri az e-mail-címet az LDAP-kiszolgálótól a felhasználóazonosító alapján, amikor szkennelt adatokat továbbít egy e-mail kiszolgáló felé.

  Ennek a funkciónak a használatához válassza ki a **On (Bekapcsolva)** opciót a **Get Mail Address (E-mail cím lekérése)** beállításhoz. Az e-mail-címe feladóként jelenik meg, amikor a készülék szkennelt adatokat küld egy e-mail kiszolgáló felé, vagy címzettként, amennyiben a szkennelt adatokat saját e-mail-címére kívánja küldeni.

Ha az LDAP-hitelesítés engedélyezve van, készüléke minden bejövő faxadatot tárol. A bejelentkezést követően a készülék kinyomtatja a tárolt faxadatokat.

Az LDAP hitelesítés beállításait a Web alapú kezelés segítségével módosíthatja.

Kapcsolódó tájékoztatás

- LDAP-hitelesítés használata

Az LDAP hitelesítés konfigurálása a Web alapú kezelővel

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. A bal oldali navigációs sávban kattintson erre: **Administrator (Rendszergazda)** > **User Restriction Function (Felhasználókorlátozási funkció)** vagy erre: **Restriction Management (Korlátozáskezelés)**.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.

5. Jelölje ki a(z) **LDAP Authentication (LDAP-hitelesítés)** elemet.
6. Kattintson a **Submit (Küldés)** gombra.
7. Kattintson a **LDAP Authentication (LDAP-hitelesítés)** menüre.
8. Konfigurálja a következő beállításokat:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

Beállítás	Leírás
Storage Fax RX Data (Fogadott faxadatok tárolása)	A lehetőség kiválasztásával tárolhatja a bejövő faxadatokat. A készülékre való bejelentkezést követően az összes bejövő faxadatot kinyomtathatja.
Remember User ID (Felhasználói azonosító megjegyzése)	Az opció kiválasztása esetén elmentheti a felhasználóazonosítót.
LDAP Server Address (LDAP-kiszolgálócím)	Írja be az LDAP-kiszolgáló IP-címét vagy a kiszolgáló nevét (például: ldap.example.com).
SSL/TLS	Válassza az **SSL/TLS** lehetőséget az LDAP SSL/TLS-en keresztüli használatát.
LDAP Server Port (LDAP-kiszolgáló portja)	Írja be az LDAP-kiszolgáló portszámát.
LDAP Search Root (LDAP-keresés gyökere)	Írja be az LDAP-keresés gyökérkönyvtárát.
Attribute of Name (Search Key) (Név (keresési kulcs) attribútuma)	Írja be a keresési kulcsként használni kívánt attribútumot.
Get Mail Address (E-mail cím lekérése)	Az opció kiválasztása esetén a készülék lekéri a bejelentkezett felhasználó e-mail-címét az LDAP-kiszolgálótól.
Get User's Home Directory (Felhasználó alapkönyvtárának beolvasása)	Az opció kiválasztása esetén az Ön kezdőkönyvtárát állítja be a készülék célként hálózatra történő szkenneléshez.

9. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- LDAP-hitelesítés használata

A készülék beállításainak a készülék kezelőpanelén keresztül történő módosításához bejelentkezés szükséges (LDAP-hitelesítés)

Ha az Active Directory engedélyezve van, a készülék kezelőpanelje zárolt állapotban marad, amíg meg nem adja felhasználói azonosítóját, tartománynevét és jelszavát a kezelőpanelen.

1. A készülék kezelőpanelén adja meg a belépéshez szükséges felhasználói azonosítót és a jelszót.
2. Sikeres hitelesítés esetén a készülék kezelőpanelének zárolása megszűnik.

Kapcsolódó tájékoztatás

- LDAP-hitelesítés használata

A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

A Secure Function Lock (Biztonságos funkciózár) 3.0 szolgáltatás növeli a biztonságot a készüléken elérhető funkciók korlátozásával.

A Secure Function Lock 3.0 használata előtt

A Secure Function Lock használatával jelszavakat állíthat be, felhasználói oldalakat korlátozhat és az itt felsorolt funkciók egy részéhez vagy az összeshez is engedélyezheti a hozzáférést.

A Secure Function Lock 3.0 (Biztonságos funkciózár) következő beállításait konfigurálhatja és módosíthatja a Web alapú kezelés segítségével:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

- **Print (Nyomtatás)**
- **Copy (Másolás)**
- **Scan (Szkennelés)**
- **Fax**
- **Media (Média)**
- **Web Connect (Webes csatlakozás)**
- **Apps (Alkalmazások)**
- **Page Limits (Lapfelhasználás korlátozása)**
- **Page Counters (Oldalszámlálók)**
- **Card ID (NFC ID) (Kártyaazonosító (NFC azonosító))**

Érintőképernyős LCD-kijelzővel rendelkező modellek:

Ha a Secure Function Lock (Biztonságos funkciózár) be van kapcsolva, a készülék automatikusan belép a nyilvános módba, és a készülék néhány funkciója korlátozódik csak a authorized felhasználók számára.

Ahhoz, hogy hozzáférhessen a korlátozott készülékfunkciókhoz, nyomja meg a gombot, válassza ki a felhasználónevét, majd adja meg a jelszavát.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

A Secure Function Lock 3.0 konfigurálása a Web alapú kezelővel

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. A bal oldali navigációs sávban kattintson erre: **Administrator (Rendszergazda)** > **User Restriction Function (Felhasználókorlátozási funkció)** vagy erre: **Restriction Management (Korlátozáskezelés)**.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Jelölje ki a(z) **Secure Function Lock (Biztonságos funkciózár)** elemet.
6. Kattintson a **Submit (Küldés)** gombra.
7. Kattintson a **Restricted Functions (Korlátozott funkciók)** menüre.
8. Konfigurálja a beállításokat a korlátozások felhasználónkénti vagy csoportonkénti kezeléséhez.
9. Kattintson a **Submit (Küldés)** gombra.
10. Kattintson a **User List (Felhasználólista)** menüre.
11. Konfigurálja a Felhasználói listát.
12. Kattintson a **Submit (Küldés)** gombra.

A **Secure Function Lock (Biztonságos funkciózár)** menüben is módosíthatók a felhasználói lista alapú funkciózár beállításai.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

Szkennelés a Secure Function Lock 3.0 használatával

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

Szkennelési korlátozások beállítása (rendszergazdák esetében)

A Secure Function Lock (Biztonságos funkciózár) 3.0 lehetővé teszi a rendszergazdák számára, hogy egyes felhasználók szkenneléshez való hozzáférését korlátozzák. Ha a Szkennelés funkció a nyilvános felhasználók számára Ki van kapcsolva, akkor csak azok a felhasználók tudnak szkennelni, akiknél a **Scan (Beolvasás)** jelölőnégyzet be van jelölve.

A Szkennelés funkció használata (korlátozott felhasználók esetében)

- Szkennelés a készülék kezelőpanelének használatával:

  A korlátozott felhasználóknak meg kell adniuk a jelszavukat a készülék kezelőpaneljén, hogy beléphessenek a Szkennelés üzemmódba.
- Szkennelés számítógépről:

  A korlátozott felhasználóknak meg kell adniuk a jelszavukat a készülék kezelőpaneljén, hogy szkennelni tudjanak a számítógépükről. Ha nem adják meg a jelszót a készülék kezelőpaneljén, egy hibaüzenet jelenik meg a felhasználó számítógépén.

Ha a készülék támogatja az IC kártya alapú hitelesítést, akkor a korlátozott felhasználók úgy is elérhetik a Szkennelés üzemmódot, hogy regisztrált IC kártyájukat hozzáérintik a készülék kezelőpaneljén levő NFC szimbólumhoz.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

Nyilvános mód konfigurálása a Secure Function Lock 3.0 szolgáltatáshoz

Használja a Secure Function Lock (Biztonságos funkciózár) képernyőt a Nyilvános mód beállításához, amely korlátozza a nyilvános felhasználók számára elérhető funkciókat. A nyilvános felhasználóknak nem kell majd jelszót beírniuk ahhoz, hogy a Nyilvános módnál beállított funkciókat elérjék.

A Nyilvános mód a Brother iPrint&Scan és a Brother Mobile Connect szolgáltatásokon keresztül küldött nyomtatási feladatokat foglalja magában.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. A bal oldali navigációs sávban kattintson erre: **Administrator (Rendszergazda)** > **User Restriction Function (Felhasználókorlátozási funkció)** vagy erre: **Restriction Management (Korlátozáskezelés)**.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Válassza a **Secure Function Lock (Biztonságos funkciózár)** lehetőséget.
6. Kattintson a **Submit (Küldés)** gombra.
7. Kattintson a **Restricted Functions (Korlátozott funkciók)** menüre.
8. A **Public Mode (Nyilvános mód)** sorban jelölje be a jelölőnégyzetet, ha engedélyez egy funkciót, és szüntesse meg a bejelölést, ha korlátozni akarja a funkciót.
9. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

A személyes főképernyő beállításainak konfigurálása web alapú kezelő használatával

Rendszergazdaként lehetősége van megadni, hogy a felhasználók milyen füleket lássanak a személyes főképernyőjükön. Az ilyen fülek gyors hozzáférést biztosítanak a felhasználóknak a favorite parancsikonjaikhoz, amelyeket készülék vezérlőpanelén rendelhetnek hozzá a személyes főképernyőjükhöz.

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. A bal oldali navigációs sávban kattintson erre: **Administrator (Rendszergazda)** > **User Restriction Function (Felhasználókorlátozási funkció)** vagy erre: **Restriction Management (Korlátozáskezelés)**.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ☰ lehetőségből kezdje.
5. Jelölje ki a(z) **Secure Function Lock (Biztonságos funkciózár)** elemet.
6. A **Tab Settings (Fülbeállítások)** mezőben válassza a **Personal (Személyes)** lehetőséget a személyes főképernyőn használt fülek neveinek a kiválasztásához.
7. Kattintson a **Submit (Küldés)** gombra.
8. Kattintson a **Restricted Functions (Korlátozott funkciók)** menüre.
9. Konfigurálja a beállításokat a korlátozások felhasználónkénti vagy csoportonkénti kezeléséhez.
10. Kattintson a **Submit (Küldés)** gombra.
11. Kattintson a **User List (Felhasználólista)** menüre.
12. Konfigurálja a Felhasználói listát.
13. Válassza ki a **User List / Restricted Functions (Felhasználólista / korlátozott funkciók)** beállításokat az egyes felhasználók számára a legördülő listából.
14. Válassza ki a fülnevet a **Home Screen (Kezdőképernyő)** legördülő listából az egyes felhasználók számára.
15. Kattintson a **Submit (Küldés)** gombra.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

A Secure Function Lock 3.0 további funkciói

Konfigurálja a következő tulajdonságokat a Secure Function Lock képernyőn:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

All Counter Reset (Minden számláló nullázása)

Kattintson az **All Counter Reset (Minden számláló nullázása)** lehetőségre a **Page Counters (Oldalszámlálók)** oszlopban az oldalszámláló alaphelyzetbe állításához.

Export to CSV file (Exportálás CSV fájlba)

Kattintson a(z) **Export to CSV file (Exportálás CSV fájlba)** lehetőségre a jelenlegi és az utolsó oldalszámláló, valamint a(z) **User List / Restricted Functions (Felhasználólista / korlátozott funkciók)** információk CSV-fájlként történő exportálásához.

Card ID (NFC ID) (Kártyaazonosító (NFC azonosító))

Kattintson a **User List (Felhasználólista)** menüre, majd írjon be egy felhasználói kártyaazonosítót a **Card ID (NFC ID) (Kártyaazonosító (NFC azonosító))** mezőbe. IC kártyáját használhatja hitelesítésre.

Output (Kimenet)

Amikor a Postafiók egység fel van szerelve a készülékre, a legördülő listából válasszon kimeneti tálcát az egyes felhasználók számára.

Last Counter Record (Utolsó számlálóérték)

Kattintson a **Last Counter Record (Utolsó számlálóérték)** lehetőségre, ha azt szeretné, hogy a készülék megtartsa az oldalszámot a számláló nullázása után.

Counter Auto Reset (Számláló automatikus nullázása)

Kattintson a(z) **Counter Auto Reset (Számláló automatikus nullázása)** lehetőségre az oldalszámláló visszaállításai közötti időintervallum konfigurálásához. Adjon meg egy napi, heti vagy havi intervallumot.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

Új IC kártya regisztrálása a készülék vezérlőpaneljével

A készüléken integrált áramköri lapot tartalmazó kártya (IC-kártya) is regisztrálható.

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

1. Érintse meg a készülék vezérlőpaneljén lévő Near-Field Communication (NFC) szimbólumot egy regisztrált integrált áramköri lapot tartalmazó Integrated Circuit (IC) kártyával.
2. Érintse meg a felhasználói azonosítóját az LCD képernyőn.
3. Nyomja meg a Kártya regisztrálása gombot.
4. Érintse az NFC szimbólumhoz az új IC kártyát.

   Az új IC kártya számát ezzel regisztrálta a készülékben.
5. Nyomja meg az OK gombot.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

Regisztráljon egy külső IC kártyaolvasót

Külső IC (integrált áramkör) kártyaolvasó csatlakoztatásakor használja a Web alapú kezelést a kártyaolvasó regisztrálásához. A készülék HIT osztályú illesztőprogram segítségével támogatja a külső IC kártyaolvasókat.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Administrator (Rendszergazda)** > **External Card Reader (Külső kártya-olvasó)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. Adja meg a szükséges információkat, majd kattintson a(z) **Submit (Küldés)** gombra.
6. Indítsa újra Brother készülékét a konfiguráció aktiválásához.
7. Csatlakoztassa a kártyaolvasót a készülékhez.
8. Érintse a kártyát a kártyaolvasóhoz a kártya alapú hitelesítés használatakor.

Kapcsolódó tájékoztatás

- A Secure Function Lock (Biztonságos funkciózár) 3.0 használata

E-mail biztonságos küldése és fogadása

- E-mail küldés és fogadás konfigurálása Web alapú kezelés használatával
- E-mail küldése felhasználói hitelesítéssel
- E-mail biztonságos küldése vagy fogadása SSL/TLS használatával

E-mail küldés és fogadás konfigurálása Web alapú kezelés használatával

- Az e-mail fogadása funkció csak bizonyos modellek esetében érhető el.
- A Web alapú kezelés használatát javasoljuk felhasználói hitelesítéssel történő biztonságos e-mail küldés bekonfigurálásához, vagy küldje és fogadja e-mailjeit SSL/TLS használatával (csak a támogatott modellek esetében).

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

   A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.
4. Kattintson a bal oldali navigációs sáv **Network (Hálózat)** > **Network (Hálózat)** > **Protocol (Protokoll)** gombjára.

   Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.
5. A **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP kliens)** mezőben kattintson a(z) **Advanced Settings (Speciális beállítások)** gombra, és győződjön meg arról, hogy a **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP kliens)** állapota **Enabled (Engedélyezve)**.

   - A rendelkezésre álló protokollok a készüléktől függően eltérőek lehetnek.
   - Ha a(z) **Authentication Method (Hitelesítési módszer)** kiválasztására szolgáló képernyő megjelenik, válassza ki a hitelesítési módszerét, majd kövesse a képernyőn megjelenő utasításokat.
6. Konfigurálja a **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP kliens)** beállításokat.
   - A konfigurálás után egy tesztlevél elküldésével ellenőrizze, hogy az e-mail beállítások helyesek-e.
   - Ha nem ismeri a POP3/IMAP4/SMTP-kiszolgáló beállításait, forduljon a hálózati rendszergazdához vagy az internetszolgáltatóhoz (ISP).
7. Ha befejezte, kattintson a(z) **Submit (Küldés)** gombra.

   Megjelenik a(z) **Test Send/Receive E-mail Configuration (E-mail küldési/fogadási beállítások tesztelése)** párbeszédpanel.
8. A jelenlegi beállítások ellenőrzéséhez kövesse a párbeszédpanel utasításait.

Kapcsolódó tájékoztatás

- E-mail biztonságos küldése és fogadása

Kapcsolódó témák:

- E-mail biztonságos küldése vagy fogadása SSL/TLS használatával

E-mail küldése felhasználói hitelesítéssel

A készüléke az e-maileket felhasználói hitelesítést igénylő e-mail kiszolgálón keresztül küldi. Ez a módszer meggátolja a unauthorized felhasználók hozzáférését az e-mail-kiszolgálóhoz.

A felhasználói hitelesítést használhatja e-mail értesítés, e-mail jelentések és I-Fax küldése céljára is (csak bizonyos modellek esetén érhető el).

- A rendelkezésre álló protokollok a készüléktől függően eltérőek lehetnek.
- Az SMTP-hitelesítés beállításához ajánlott a Web alapú kezelés használata.

E-mail szerver beállításai

A készülék SMTP hitelesítési módszerét úgy kell beállítani, hogy egyezzen az e-mail kiszolgálója által használt módszerrel. Az e-mail kiszolgáló beállítására vonatkozó részletekért vegye fel a kapcsolatot a hálózati rendszergazdával vagy az internetszolgáltatóval.

Ha engedélyezni kívánja az SMTP-kiszolgáló Web alapú kezelés használatával történő hitelesítését, akkor válassza ki a hitelesítési módszerét a(z) **Server Authentication Method (Kiszolgáló hitelesítési módszere)** alatt a(z) **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP kliens)** képernyőn.

Kapcsolódó tájékoztatás

- E-mail biztonságos küldése és fogadása

E-mail biztonságos küldése vagy fogadása SSL/TLS használatával

Készüléke támogatja az SSL/TLS kommunikációs módszerek használatát. SSL/TLS kommunikációt használó e-mail kiszolgáló alkalmazásához el kell végeznie az alábbi beállításokat.

- Az e-mail fogadása funkció csak bizonyos modellek esetében érhető el.
- Az SSL/TLS konfigurálásához a Web alapú kezelést ajánljuk.

Szervertanúsítvány ellenőrzése

Ha az **SSL/TLS** területen az **SSL** vagy a **TLS** lehetőséget választja, a készülék automatikusan bejelöli a **Verify Server Certificate (Kiszolgálói tanúsítvány ellenőrzése)** jelölőnégyzetet.

- A szerver tanúsítványának ellenőrzése előtt először importálnia kell a CA tanúsítványt attól a CA-tól, amelyik aláírta a szerver tanúsítványát. Érdeklődjön a hálózati rendszergazdánál vagy az internetszolgáltatójánál (ISP) arról, hogy a CA tanúsítvány importálása szükséges-e.
- Ha nem kell ellenőriznie a szerver tanúsítványát, vegye ki a bejelölést a **Verify Server Certificate (Kiszolgálói tanúsítvány ellenőrzése)** jelölőnégyzetből.

Port száma

Ha a(z) **SSL** vagy **TLS** lehetőséget választja, a **Port** érték megváltozik, hogy egyezzen a protokollal. A portszám kézi módosításához adja meg a portszámot az **SSL/TLS** beállítások kiválasztása után.

A készülék kommunikációs módszerét úgy kell beállítani, hogy egyezzen az e-mail kiszolgálója által használt módszerrel. Az e-mail szerver beállítására vonatkozó részletekért vegye fel a kapcsolatot a hálózati rendszergazdával vagy az internetszolgáltatóval.

A legtöbb esetben a biztonságos webmail szolgáltatások a következő beállításokat igénylik:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

SMTP	**Port**	587
	Server Authentication Method (Kiszolgáló hitelesítési módszere)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Kapcsolódó tájékoztatás

- E-mail biztonságos küldése és fogadása

Kapcsolódó témák:

- E-mail küldés és fogadás konfigurálása Web alapú kezelés használatával
- Tanúsítványok konfigurálása az eszközbiztonság számára

Nyomtatási napló tárolása a hálózaton

Nyomtatási napló tárolása a hálózati áttekintéshez

A nyomtatási napló hálózati tárolása funkció esetén a Common Internet File System (CIFS) protokoll használatával egy hálózati kiszolgálóra mentheti készüléke nyomtatási naplóját. Rögzítheti az egyes nyomtatási feladatok azonosítóját, típusát, nevét, felhasználónevét, dátumát, idejét és a nyomtatott oldalak számát. A CIFS egy protokoll, amely TCP/IP-n keresztül teszi lehetővé a hálózatban levő számítógépeken a fájlok megosztását az intraneten vagy interneten keresztül.

A nyomtatási napló a következő nyomtatási funkciókat rögzíti:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

- Nyomtatási feladatok a számítógépről
- Közvetlen nyomtatás USB-ről
- Másolás
- Fogadott fax
- Web Connect nyomtatás

- A nyomtatási napló hálózati tárolása funkció támogatja a Kerberos és az NTLMv2 hitelesítést. A hitelesítéshez konfigurálnia kell az SNTP protokollt (hálózati időkiszolgáló), vagy megfelelően be kell állítania a dátumot, az időt és az időzónát a kezelőpanelen.
- A fájlok kiszolgálón való tárolásakor a fájltípust TXT vagy CSV értékre kell beállítani.

Kapcsolódó tájékoztatás

- Nyomtatási napló tárolása a hálózaton

A nyomtatási napló hálózati tárolása funkció beállításainak konfigurálása a Web alapú kezelő használatával

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. Kattintson a bal oldali navigációs sáv **Administrator (Rendszergazda)** > **Store Print Log to Network (Nyomtatási napló tárolása a hálózaton)** gombjára.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. A **Print Log (Nyomtatási napló)** mezőben kattintson az **On (Bekapcsolva)** lehetőségre.
6. Konfigurálja a következő beállításokat:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

Beállítás	Leírás
Network Folder Path (Hálózati mappa elérési útja)	Írja be annak a mappának a nevét Például: amelyben a CIFS-kiszolgáló tárolni fogja a nyomtatási naplót (például: \\ComputerName\SharedFolder).
File Name (Fájlnév)	Írja be a nyomtatási naplóhoz használni kívánt fájlnevet (legfeljebb 32 karakter).
File Type (Fájltípus)	Válassza ki a **TXT** vagy a **CSV** opciót a nyomtatási napló fájltípusához.
Time Source for Log (Napló időforrása)	Válassza ki az időforrást a nyomtatási naplóhoz.
Auth. Method (Hitelesítési módszer)	Válassza ki a CIFS-kiszolgáló eléréséhez szükséges hitelesítési módszert az **Auto (Automatikus)**, **Kerberos** vagy **NTLMv2** módszerek közül. A Kerberos egy olyan hitelesítési protokoll, amely egyszeri bejelentkezéssel teszi lehetővé az eszközök vagy személyek számára a személyazonosságuk biztonságos igazolását a hálózati kiszolgálóknak. A Windows az NTLMv2 hitelesítési módszert használja a kiszolgálókra való bejelentkezéshez. • **Auto (Automatikus)**: Ha az **Auto (Automatikus)** lehetőséget választja, az NTLMv2 lesz hitelesítési módszerként használva. • **Kerberos**: Válassza a **Kerberos** opciót, ha csak Kerberos-hitelesítést kíván használni. • **NTLMv2**: Válassza az **NTLMv2** opciót, ha csak NTLMv2-hitelesítést kíván használni.

Beállítás	Leírás
	• A **Kerberos** és **NTLMv2** hitelesítéshez konfigurálnia kell a **Date&Time (Dátum és idő)** beállításokat vagy az SNTP protokollt (hálózati időkiszolgálót) és a DNS kiszolgálót. • A dátum és idő konfigurálását a készülék kezelőpaneljéről is elvégezheti.
Username (Felhasználónév)	Írja be a hitelesítéshez használni kívánt felhasználónevet (legfeljebb 96 karakter). Ha a felhasználónév egy tartomány része, a következő stílusok valamelyike szerint adja meg a felhasználónevet: felhasználó@tartomány vagy tartomány\felhasználó.
Password (Jelszó)	Írja be a hitelesítéshez használni kívánt jelszót (legfeljebb 32 karakter).
Kerberos Server Address (Kerberos-kiszolgáló címe) (ha szükséges)	Írja be a kulcsszolgáltató (KDC) állomáscímét (például: kerberos.példa.hu; legfeljebb 64 karakter) vagy az IP-címet (például: 192.168.56.189).
Error Detection Setting (Hibaészlelési beállítás)	Válassza ki, hogy mit tegyen a készülék, ha hálózati hiba miatt meghiúsul a nyomtatási napló kiszolgálón való tárolása.

7. A **Connection Status (Kapcsolat állapota)** mezőben ellenőrizze az utolsó napló állapotát.

A készülék LCD-kijelzőjén a hibaállapotot is ellenőrizheti.

8. A **Submit (Küldés)** oldal megjelenítéséhez kattintson a **Test Print Log to Network (Tesztoldal nyomtatása napló a hálózaton)** gombra.

   A beállítások teszteléséhez kattintson a **Yes (Igen)** gombra, majd folytassa a következő lépéssel.

   A teszt kihagyásához kattintson a **No (Nem)** gombra. A beállításokat a rendszer automatikusan elküldi.
9. A készülék teszteli a beállításokat.
10. Ha a beállításokat a rendszer elfogadja, a képernyőn a **Test OK (Sikeres teszt)** üzenet jelenik meg.

    Ha a **Test Error (Hiba a teszt során)** üzenet jelenik meg, ellenőrizze a beállításokat, majd kattintson a **Submit (Küldés)** gombra a tesztoldal újbóli megjelenítéséhez.

Kapcsolódó tájékoztatás

- Nyomtatási napló tárolása a hálózaton

A nyomtatási napló tárolása a hálózaton funkció hibaészlelési beállításainak használata

A hibaészlelési beállítások használatával határozza meg, mit tegyen a készülék, ha hálózati hiba miatt meghiúsul a nyomtatási napló tárolása a kiszolgálón.

1. Indítsa el a webböngészőt.
2. Írja be a „https://készülék IP-címe” címet a böngésző címsorába (ahol a „készülék IP-címe” a készülékének az IP-címe).

   Például:

   https://192.168.1.2

   A készülék IP-címe megtalálható a Hálózati konfigurációs jelentésben.
3. Szükség esetén írja be a jelszót a **Login (Bejelentkezés)** mezőbe, majd kattintson a **Login (Bejelentkezés)** lehetőségre.

A készülék beállításainak elvégzéséhez szükséges jelszó a készülék hátulján vagy alján található a „**Pwd**” kifejezés mellett. Módosítsa az alapértelmezett jelszót a képernyőn megjelenő utasításokat követve, amikor először bejelentkezik.

4. Kattintson a bal oldali navigációs sáv **Administrator (Rendszergazda)** > **Store Print Log to Network (Nyomtatási napló tárolása a hálózaton)** gombjára.

Ha a bal oldali navigációs sáv nem látható, akkor a navigációt a ≡ lehetőségből kezdje.

5. Az **Error Detection Setting (Hibaészlelési beállítás)** szakaszban válassza a **Cancel Print (Nyomtatás megszakítása)** vagy az **Ignore Log & Print (Napló figyelmen kívül hagyása és nyomtatás)** opciót.

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

Beállítás	Leírás
Cancel Print (Nyomtatás megszakítása)	Ha a **Cancel Print (Nyomtatás megszakítása)** lehetőséget választja, akkor a készülék canceled a nyomtatási feladatokat, ha a nyomtatási napló nem tárolható a kiszolgálón. A faxokat még akkor is kinyomtatja a készülék, ha a **Cancel Print (Nyomtatás megszakítása)** opciót választja.

Ignore Log & Print (Napló figyelmen kívül hagyása és nyomtatás)	Ha az **Ignore Log & Print (Napló figyelmen kívül hagyása és nyomtatás)** opciót választja, akkor a készülék akkor is nyomtatja a dokumentumot, ha a nyomtatási napló nem tárolható a kiszolgálón.
	Amikor a nyomtatási napló újra tárolható a kiszolgálón, a nyomtatási napló rögzítése a következő módon történik:
	`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. Ha a nyomtatás végén nem tárolható a nyomtatási napló, akkor a nyomtatott oldalak számát nem rögzíti a rendszer.

Beállítás	Leírás
	b. Ha a nyomtatás elején és végén sem tárolható a napló, akkor a készülék nem rögzíti a naplót. A funkció helyreállása után a hiba szerepelni fog a nyomtatási naplóban.

6. A **Submit (Küldés)** oldal megjelenítéséhez kattintson a **Test Print Log to Network (Tesztoldal nyomtatása napló a hálózaton)** gombra.

   A beállítások teszteléséhez kattintson a **Yes (Igen)** gombra, majd folytassa a következő lépéssel.

   A teszt kihagyásához kattintson a **No (Nem)** gombra. A beállításokat a rendszer automatikusan elküldi.
7. A készülék teszteli a beállításokat.
8. Ha a beállításokat a rendszer elfogadja, a képernyőn a **Test OK (Sikeres teszt)** üzenet jelenik meg.

   Ha a **Test Error (Hiba a teszt során)** üzenet jelenik meg, ellenőrizze a beállításokat, majd kattintson a **Submit (Küldés)** gombra a tesztoldal újbóli megjelenítéséhez.

Kapcsolódó tájékoztatás

- Nyomtatási napló tárolása a hálózaton

A nyomtatási napló hálózati tárolása funkció használata a Secure Function Lock 3.0 szolgáltatással

Ha a Secure Function Lock 3.0 (Biztonságos funkciózár) szolgáltatás aktív, akkor a nyomtatási napló hálózati tárolásának jelentése rögzíti a másolás, faxfogadás, Web Connect nyomtatás és USB közvetlen nyomtatás funkciók regisztrált felhasználóit. Ha az Active Directory hitelesítés engedélyezve van, a „nyomtatási napló tárolása a hálózaton” jelentés rögzíti a bejelentkezett felhasználónevet:

A támogatott funkciók, opciók és beállítások a modelltől függően eltérhetnek.

```
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
```

Kapcsolódó tájékoztatás

- Nyomtatási napló tárolása a hálózaton

brother

Brother Earth

www.brotherearth.com

HUN
0 verzió