Príručka bezpečnostných funkcií

Obsah

Úvod

Definície poznámok

V tejto Príručke používateľa sú použité nasledujúce symboly a pravidlá:

DÔLEŽITÉ	DÔLEŽITÉ označuje potenciálne nebezpečnú situáciu, ktorá v prípade, že jej nezabránite, môže mať za následok poškodenie majetku alebo stratu funkčnosti produktu.
POZNÁMKA	POZNÁMKA stanovuje prevádzkové prostredie, podmienky pre inštaláciu alebo špeciálne podmienky používania.
	Ikony tipov označujú užitočné rady a doplňujúce informácie.
Tučné	Tučným písmom sú označené tlačidlá na ovládacom paneli zariadenia alebo na obrazovke počítača.
Kurzíva	Italicized sú emphasizes dôležité body alebo odkazy na súvisiacu tému.

Súvisiace informácie

- Úvod

Obchodné známky

Adobe® a Reader® sú registrované obchodné známky alebo obchodné známky spoločnosti Adobe Systems Incorporated v USA alebo ďalších krajinách.

Každá spoločnosť, ktorej názov softvéru je uvedený v tejto príručke, má License zmluvu na softvér týkajúcu sa programov v jej vlastníctve.

Všetky obchodné názvy a názvy produktov, ktorých súčasťou sú názvy spoločností, uvádzané na produktoch značky Brother, súvisiacich dokumentoch a na akýchkoľvek iných materiáloch, sú obchodné známky alebo registrované obchodné známky týchto príslušných spoločností.

Súvisiace informácie

- Úvod

Copyright

Súvisiace informácie

- Úvod

Pred použitím funkcií zabezpečenia siete

Zariadenie podporuje niektoré z najnovších sieťových protokolov na zabezpečenie a šifrovanie, ktoré sú dnes dostupné. Tieto sieťové funkcie môžete integrovať do celkového plánu zabezpečenia siete, aby pomáhali chrániť vaše údaje a zabraňovali unauthorized prístupu k zariadeniu.

Odporúčame deaktivovať protokoly FTP a TFTP. Pristupovanie k zariadeniu pomocou týchto protokolov nie je bezpečné.

Súvisiace informácie

- Úvod
  - Zakázanie nepotrebných protokolov

Zakázanie nepotrebných protokolov

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Zrušením začiarknutia políčok akýchkoľvek nepotrebných protokolov tieto protokoly zakážte.
6. Kliknite na položky **Submit (Odoslať)**.
7. Reštartovaním zariadenia Brother aktivujte konfiguráciu.

Súvisiace informácie

- Pred použitím funkcií zabezpečenia siete

Zabezpečenie siete

- Konfigurovanie certifikátov zabezpečenia zariadenia
- Použitie SSL/TLS
- Použitie SNMPv3
- Použitie IPsec
- Použitie overenia IEEE 802.1x vašej siete

Konfigurovanie certifikátov zabezpečenia zariadenia

Ak chcete sieťové zariadenie bezpečne spravovať pomocou protokolu SSL/TLS, musíte nakonfigurovať certifikát. Na konfigurovanie certifikátu musíte použiť aplikáciu Web Based Management.

- Prehľad funkcií certifikátu zabezpečenia
- Vytvorenie a inštalácia certifikátu
- Vytvorenie certifikátu s vlastným podpisom
- Vytvorenie požiadavky na podpis certifikátu (CSR) a inštalácia certifikátu od certifikačnej autority (CA)
- Importovanie a exportovanie certifikátu a súkromného kľúča
- Importovanie a exportovanie certifikátu certifikačnej autority

Prehľad funkcií certifikátu zabezpečenia

Vaše zariadenie podporuje použitie viacerých certifikátov zabezpečenia, ktoré umožňujú bezpečné overenie a komunikáciu so zariadením. V zariadení môžete použiť tieto funkcie certifikátov zabezpečenia:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

- Komunikácia SSL/TLS
- Overenie IEEE 802.1x
- IPsec

Vaše zariadenie podporuje nasledujúce:

- Predinštalovaný certifikát

  Zariadenie obsahuje predinštalovaný certifikát s vlastným podpisom. Tento certifikát umožňuje používať komunikáciu SSL/TLS bez vytvárania alebo inštalácie iného certifikátu.

Predinštalovaný certifikát s vlastným podpisom chráni do určitej miery vašu komunikáciu. V záujme lepšieho zabezpečenia odporúčame používať certifikát vydaný dôveryhodnou organization.

- Certifikát s vlastným podpisom

  Tento tlačový server vydáva vlastný certifikát. Pomocou tohto certifikátu môžete jednoducho používať komunikáciu SSL/TLS bez vytvárania alebo inštalácie iného certifikátu od certifikačnej autority.
- Certifikát certifikačnej autority (CA)

  Existujú dva spôsoby inštalácie certifikátu certifikačnej autority. Ak už máte certifikát od certifikačnej autority alebo chcete používať certifikát od externej dôveryhodnej certifikačnej autority:

  - Keď používate žiadosť o podpísanie certifikátu (CSR) od tohto tlačového servera.
  - Keď importujete certifikát a súkromný kľúč.
- Certifikát certifikačnej autority (CA)

  Ak chcete používať certifikát certifikačnej autority, ktorý identifikuje certifikačnú autoritu a vlastní jej súkromný kľúč, musíte daný certifikát certifikačnej autority importovať z certifikačnej autority ešte pred konfiguráciou funkcií zabezpečenia siete.

- Ak budete používať komunikáciu SSL/TLS, odporúčame najprv kontaktovať správcu systému.
- Keď obnovíte predvolené výrobné nastavenia tlačového servera, nainštalovaný certifikát a súkromný kľúč sa odstránia. Ak chcete ponechať rovnaký certifikát a súkromný kľúč aj po resetovaní tlačového servera, pred resetovaním ich exportujte a potom ich preinštalujte.

Súvisiace informácie

- Konfigurovanie certifikátov zabezpečenia zariadenia

Súvisiace témy:

- Konfigurácia overenia IEEE 802.1x pre vašu sieť pomocou ovládania cez webové rozhranie (webový prehliadač)

Vytvorenie a inštalácia certifikátu

Pri výbere bezpečnostného certifikátu máte dve možnosti: použiť certifikát s vlastným podpisom alebo certifikát od certifikačnej autority.

Možnosť 1

Certifikát s vlastným podpisom

1. Vytvorte certifikát s vlastným podpisom pomocou nástroja Web Based Management (Ovládanie cez webové rozhranie).
2. Nainštalujte certifikát s vlastným podpisom do počítača.

Možnosť 2

Certifikát od certifikačnej autority

1. Vytvorte požiadavku o podpísanie certifikátu (CSR) pomocou ovládania cez webové rozhranie.
2. Nainštalujte certifikát, vydaný certifikačnou autoritou, do vášho zariadenia Brother pomocou ovládania cez webové rozhranie.
3. Nainštalujte certifikát do počítača.

Súvisiace informácie

- Konfigurovanie certifikátov zabezpečenia zariadenia

Vytvorenie certifikátu s vlastným podpisom

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknite na položku **Create Self-Signed Certificate (Vytvoriť certifikát s vlastným podpisom)**.
6. Zadajte **Common Name (Spoločný názov)** a **Valid Date (Platný dátum)**.
   - Dĺžka položky **Common Name (Spoločný názov)** je menej, než 64 bajtov. Zadajte identifikátor, ako napríklad adresu IP, názov uzla alebo názov domény, ktorý sa má používať pri pristupovaní na toto zariadenie prostredníctvom komunikácie SSL/TLS. Predvolené je zobrazovanie názvu uzla.
   - Ak použijete protokol IPPS alebo HTTPS a v URL zadáte iný názov než **Common Name (Spoločný názov)**, ktorý bol použitý pre certifikát s vlastným podpisom, zobrazí sa varovanie.
7. Z rozbaľovacieho zoznamu **Public Key Algorithm (Algoritmus verejného kľúča)** vyberte vaše nastavenie.
8. Z rozbaľovacieho zoznamu **Digest Algorithm (Algoritmus Digest)** vyberte vaše nastavenie.
9. Kliknite na položku **Submit (Odoslať)**.

Súvisiace informácie

- Konfigurovanie certifikátov zabezpečenia zariadenia

Vytvorenie požiadavky na podpis certifikátu (CSR) a inštalácia certifikátu od certifikačnej autority (CA)

Ak už máte certifikát od dôveryhodnej externej certifikačnej autority (CA), certifikát a súkromný kľúč môžete uložiť do zariadenia a spravovať ich prostredníctvom importu a exportu. Ak nemáte certifikát od dôveryhodnej externej certifikačnej autority, vytvorte požiadavku o podpísanie certifikátu (CSR), pošlite ju CA na overenie a poskytnutý certifikát nainštalujte na zariadení.

- Vytvorte žiadosť o podpísanie certifikátu (CSR)
- Inštalácia certifikátu na zariadení

Vytvorte žiadosť o podpísanie certifikátu (CSR)

Žiadosť o podpísanie certifikátu (CSR) je žiadosť odoslaná certifikačnej autorite (CA), aby overila poverenia obsiahnuté v rámci certifikátu.

Odporúčame, aby pred vytvorením CSR nainštalovali do vášho počítača koreňový certifikát od certifikačnej autority.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

   Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.
4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

   Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.
5. Kliknite na položku **Create CSR (Vytvoriť CSR)**.
6. Zadajte (požadované) **Common Name (Spoločný názov)** a pridajte ďalšie (voliteľné) informácie o vašom **Organization (Organizácia)**.

   - Vyžadujú sa podrobnosti o vašej spoločnosti, aby certifikačná autorita mohla potvrdiť vašu identitu a overiť ju pre externú osobu.
   - Dĺžka položky **Common Name (Spoločný názov)** musí byť menej než 64 bajtov. Zadajte identifikátor, ako napríklad adresu IP, názov uzla alebo názov domény, ktorý sa má používať pri pristupovaní na toto zariadenie prostredníctvom komunikácie SSL/TLS. Predvolené je zobrazovanie názvu uzla. Údaj **Common Name (Spoločný názov)** je povinný.
   - Ak v URL zadáte iný názov než Spoločné meno, ktoré bolo použité pre certifikát, zobrazí sa varovanie.
   - Dĺžka položiek **Organization (Organizácia)**, **Organization Unit (Organizačná jednotka)**, **City/Locality (Mesto/lokalita)** a **State/Province (Kraj)** musí byť menej než 64 bajtov.
   - Položka **Country/Region (Krajina/oblasť)** by mala byť vo formáte dvojznakového kódu krajiny podľa štandardu ISO 3166.
   - Ak konfigurujte rozšírenie certifikátu X.509v3, zvoľte políčko na označenie **Configure extended partition (Konfigurovať rozšírenú oblasť)** a potom zvoľte **Auto (Register IPv4) (Automaticky (registrácia IPv4))** alebo **Manual (Manuálne)**.
7. Z rozbaľovacieho zoznamu **Public Key Algorithm (Algoritmus verejného kľúča)** vyberte vaše nastavenie.
8. Z rozbaľovacieho zoznamu **Digest Algorithm (Algoritmus Digest)** vyberte vaše nastavenie.
9. Kliknite na položku **Submit (Odoslať)**.

   Na displeji sa zobrazí žiadosť o podpísanie certifikátu. Žiadosť o podpísanie certifikátu uložte ako súbor alebo kópiu a vložte ho do on-line formuláru žiadosti o podpísanie certifikátu poskytovaného certifikačnou autoritou.
10. Kliknite na **Uložiť**.

- Pri voľbe metódy odoslania žiadosti o podpísanie certifikátu vašej certifikačnej autorite sa riaďte pravidlami vašej certifikačnej autority.
- Ak používate koreňovú certifikačnú autoritu podnikovej siete operačného systému Windows Server, odporúčame vám na bezpečnú tvorbu certifikátu klienta používať ako šablónu certifikátu Webový server. Ak vytvárate certifikát klienta pre prostredie IEEE 802.1x s overením EAP-TLS, ako šablónu certifikátu odporúčame používať Používateľa.

Súvisiace informácie

- Vytvorenie požiadavky na podpis certifikátu (CSR) a inštalácia certifikátu od certifikačnej autority (CA)

Inštalácia certifikátu na zariadení

Keď získate certifikát od certifikačnej autority (CA), nainštalujte ho na tlačový server podľa nasledujúcich pokynov:

Nainštalovať môžete iba certifikát vydaný na základe požiadavky na podpísanie certifikátu (CSR) z tohto zariadenia. Ak chcete vytvoriť novú požiadavku CSR, pred jej vytvorením sa presvedčte, či je nainštalovaný certifikát. Ďalšiu CSR vytvorte až po nainštalovaní certifikátu do vášho zariadenia; v opačnom prípade bude CSR, ktorú ste vytvorili pred inštaláciou, neplatná.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Kliknite na položku **Install Certificate (Inštalovať certifikát)**.
6. Prejdite na súbor, ktorý obsahuje certifikát vydaný certifikačnou autoritou a potom kliknite na **Submit (Odoslať)**.

   Certifikát sa vytvoril a uložil sa do pamäte vášho zariadenia.

Aby ste mohli používať komunikáciu SSL/TLS, v počítači musí byť nainštalovaný koreňový certifikát od certifikačnej autority. Kontaktujte správcu siete.

Súvisiace informácie

- Vytvorenie požiadavky na podpis certifikátu (CSR) a inštalácia certifikátu od certifikačnej autority (CA)

Importovanie a exportovanie certifikátu a súkromného kľúča

Certifikát a súkromný kľúč môžete uložiť do zariadenia a spravovať ich prostredníctvom importu a exportu.

- Importovanie certifikátu a súkromného kľúča
- Exportovanie certifikátu a súkromného kľúča

Importovanie certifikátu a súkromného kľúča

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknite na položku **Import Certificate and Private Key (Importovať certifikát a súkromný kľúč)**.
6. Prechádzaním vyberte súbor, ktorý chcete importovať.
7. Ak je súbor zašifrovaný, zadajte heslo, a potom kliknite na **Submit (Odoslať)**.

Certifikát a súkromný kľúč sú naimportované do vášho zariadenia.

Súvisiace informácie

- Importovanie a exportovanie certifikátu a súkromného kľúča

Exportovanie certifikátu a súkromného kľúča

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknite na položku **Export (Exportovať)** zobrazenú s položkou **Certificate List (Zoznam certifikátov)**.
6. Ak chcete súbor zašifrovať, zadajte heslo.

   Ak heslo ponecháte prázdne, výstup nebude zašifrovaný.
7. Znova zadajte heslo na potvrdenie a potom kliknite na **Submit (Odoslať)**.
8. Kliknite na **Uložiť**.

Certifikát a súkromný kľúč sa exportujú do vášho počítača.

Certifikát môžete do počítača aj importovať.

Súvisiace informácie

- Importovanie a exportovanie certifikátu a súkromného kľúča

Importovanie a exportovanie certifikátu certifikačnej autority

Certifikáty certifikačnej autority v zariadení Brother môžete importovať, exportovať a uložiť.

- Importovanie certifikátu certifikačnej autority
- Exportovanie certifikátu certifikačnej autority

Importovanie certifikátu certifikačnej autority

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **CA Certificate (Certifikát certifikačného orgánu)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknite na **Import CA Certificate (Importovať certifikát certifikačného orgánu)**.
6. Vyhľadajte súbor, ktorý chcete importovať.
7. Kliknite na položky **Submit (Odoslať)**.

Súvisiace informácie

- Importovanie a exportovanie certifikátu certifikačnej autority

Exportovanie certifikátu certifikačnej autority

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **CA Certificate (Certifikát certifikačného orgánu)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Vyberte certifikát, ktorý chcete exportovať a kliknite na položku **Export (Exportovať)**.
6. Kliknite na položku **Submit (Odoslať)**.

Súvisiace informácie

- Importovanie a exportovanie certifikátu certifikačnej autority

Použitie SSL/TLS

- Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SSL/TLS
- Bezpečná tlač dokumentov s použitím protokolu SSL/TLS
- Zabezpečené odosielanie alebo príjem e-mailov pomocou protokolu SSL/TLS

Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SSL/TLS

- Konfigurovanie certifikátu pre protokol SSL/TLS a dostupné protokoly
- Prístup k ovládaniu cez webové rozhranie pomocou protokolu SSL/TLS
- Inštalácia certifikátu s vlastným podpisom pre používateľov systému Windows ako správcov
- Konfigurovanie certifikátov zabezpečenia zariadenia

Konfigurovanie certifikátu pre protokol SSL/TLS a dostupné protokoly

Pred použitím komunikácie SSL/TLS nakonfigurujte vo vašom zariadení certifikát prostredníctvom ovládania cez webové rozhranie.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknite na **HTTP Server Settings (Nastavenia servera HTTP)**.
6. Z rozbaľovacieho zoznamu **Select the Certificate (Zvoľte certifikát)** vyberte certifikát, ktorý chcete konfigurovať.
7. Kliknite na **Submit (Odoslať)**.
8. Kliknutím na **Yes (Áno)** reštartujte váš tlačový server.

Súvisiace informácie

- Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SSL/TLS

Súvisiace témy:

- Bezpečná tlač dokumentov s použitím protokolu SSL/TLS

Prístup k ovládaniu cez webové rozhranie pomocou protokolu SSL/TLS

Na bezpečné spravovanie sieťového zariadenia musíte používať pomôcky na správu s bezpečnostnými protokolmi.

- Na používanie protokolu HTTPS musí byť na vašom zariadení povolené HTTPS. Pri predvolenom nastavení je protokol HTTPS povolený.
- Nastavenia protokolu HTTPS môžete zmeniť na obrazovke ovládania cez webové rozhranie.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

   Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.
4. Teraz môžete k zariadeniu pristupovať pomocou protokolu HTTPS.

Súvisiace informácie

- Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SSL/TLS

Inštalácia certifikátu s vlastným podpisom pre používateľov systému Windows ako správcov

- Nasledujúce kroky sú určené pre prehliadač Microsoft Edge. Ak používate iný webový prehliadač, pokyny na inštaláciu certifikátov nájdete v dokumentácii webového prehliadača alebo v jeho online pomocníkovi.
- Uistite sa, že ste si vytvorili certifikát s vlastným podpisom pomocou ovládania cez webové rozhranie.

1. Pravým tlačidlom myši kliknite na ikonu **Microsoft Edge** a potom kliknite na položku **Spustiť ako správca**.

   Keď sa zobrazí obrazovka **Kontrola používateľských kont**, kliknite na **Áno**.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Ak vaše pripojenie nie je súkromné, kliknite na tlačidlo **Rozšírené** a potom pokračujte na webovú stránku.
4. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

   Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.
5. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **Certificate (Certifikát)** na ľavom navigačnom paneli.

   Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.
6. Kliknite na **Export (Exportovať)**.
7. Ak chcete zašifrovať výstupný súbor, zadajte heslo do poľa **Enter Password (Zadajte heslo)**. Ak je pole **Enter Password (Zadajte heslo)** prázdne, výstupný súbor nebude zašifrovaný.
8. Opäť napíšte do poľa **Retype Password (Znova zadajte heslo)** svoje heslo a kliknite na **Submit (Odoslať)**.
9. Kliknutím na prevzatý súbor ho otvorte.
10. Keď sa objaví okno **Sprievodca importom certifikátov**, kliknite na **Ďalej**.
11. Kliknite na položku **Ďalej**.
12. Prípadne zadajte heslo a potom kliknite na tlačidlo **Ďalej**.
13. Zvoľte **Umiestniť všetky certifikáty v nasledovnom priestore**, a potom kliknite na **Prehľadávať...**.
14. Zvoľte **Dôveryhodné koreňové certifikačné autority** a potom kliknite na **OK**.
15. Kliknite na položku **Ďalej**.
16. Kliknite na položku **Dokončiť**.
17. Ak je údaj odtlačok správny, kliknite na **Áno**.
18. Kliknite na položku **OK**.

Súvisiace informácie

- Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SSL/TLS

Bezpečná tlač dokumentov s použitím protokolu SSL/TLS

- Tlač dokumentov pomocou protokolu IPPS
- Konfigurovanie certifikátu pre protokol SSL/TLS a dostupné protokoly
- Konfigurovanie certifikátov zabezpečenia zariadenia

Tlač dokumentov pomocou protokolu IPPS

Na bezpečnú tlač dokumentov s protokolom IPP použite protokol IPPS.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Skontrolujte, či je začiarknuté políčko **IPP**.

Ak políčko **IPP** nie je začiarknuté, začiarknite políčko **IPP** a potom kliknite na tlačidlo **Submit (Odoslať)**.

Reštartovaním zariadenia aktivujete konfiguráciu.

Po reštartovaní zariadenia sa vráťte na webovú stránku zariadenia, zadajte heslo a v ľavom navigačnom paneli kliknite na položku **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)**.

6. Kliknite na položku **HTTP Server Settings (Nastavenia servera HTTP)**.
7. Začiarknite políčko **HTTPS(Port 443) (HTTPS (Port 443))** v oblasti **IPP** a potom kliknite na tlačidlo **Submit (Odoslať)**.
8. Reštartovaním zariadenia aktivujete konfiguráciu.

Použitie protokolu IPPS pri komunikácii nezabráni unauthorized prístupu k tlačovému serveru.

Súvisiace informácie

- Bezpečná tlač dokumentov s použitím protokolu SSL/TLS

Použitie SNMPv3

- Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SNMPv3

Zabezpečené spravovanie sieťového zariadenia pomocou protokolu SNMPv3

Jednoduchý protokol správy siete verzie 3 (SNMPv3) umožňuje overovanie používateľov a šifrovanie údajov na zabezpečenú správu sieťových zariadení.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://Bezny nazov“ (kde „Bezny nazov“ je bežný názov, ktorý ste priradili certifikátu – môže to byť vaša adresa IP, názov uzla alebo názov domény).
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Uistite sa, že je povolené nastavenie **SNMP** a potom kliknite na **Advanced Settings (Rozšírené nastavenie)**.
6. Konfigurácia nastavení režimu SNMPv1/v2c.

Možnosť	Popis
SNMP v1/v2c read-write access (SNMP v1/v2c – prístup na čítanie/zápis)	Tlačový server využíva verziu 1 a verziu 2c protokolu SNMP. V tomto režime môžete používať všetky aplikácie svojho zariadenia. Tento režim však nie je bezpečný, pretože sa v ňom neoveruje používateľ a nešifrujú sa dáta.
SNMP v1/v2c read-only access (Pri SNMP v1/v2c prístup len na čítanie)	Tlačový server využíva pre verzie 1 a verzie 2c protokolu SNMP prístup len na čítanie.
Disabled (Deaktivované)	Zakázanie verzie 1 a verzie 2c protokolu SNMP. Obmedzia sa všetky aplikácie, ktoré používajú SNMPv1/v2c. Ak chcete povoliť používanie aplikácií využívajúcich protokoly SNMPv1/v2c, používajte režim **SNMP v1/v2c read-only access (Pri SNMP v1/v2c prístup len na čítanie)** alebo **SNMP v1/v2c read-write access (SNMP v1/v2c – prístup na čítanie/zápis)**.

7. Konfigurácia nastavení režimu SNMPv3.

Možnosť	Popis
Enabled (Zapnuté)	Tlačový server využíva protokol SNMP verzie 3. Ak chcete spravovať tlačový server zabezpečeným spôsobom, používajte režim SNMPv3.
Disabled (Deaktivované)	Zakázanie verzie 3 protokolu SNMP. Obmedzia sa všetky aplikácie, ktoré používajú SNMPv3. Ak chcete povoliť používanie aplikácií využívajúcich režim SNMPv3, používajte režim SNMPv3.

8. Kliknite na **Submit (Odoslať)**.

Ak zariadenie zobrazí možnosti nastavenia protokolu, vyberte požadované možnosti.

9. Reštartovaním zariadenia aktivujete konfiguráciu.

Súvisiace informácie

- Použitie SNMPv3

Použitie IPsec

Úvod do zabezpečenia IPsec

IPsec (Internet Protocol Security) je bezpečnostný protokol, ktorý používa voliteľnú funkciu internetového protokolu, aby sa zabránilo manipulácii a zaistila sa dôvernosť údajov prenášaných ako IP pakety. IPsec šifruje dáta prenášané cez sieť, ako sú napríklad tlačové údaje odosielané z počítačov do tlačiarne. Pretože dáta sú šifrované v sieťovej vrstve, aplikácie, ktoré používajú protokol vyššej úrovne používajú zabezpečenie IPsec aj vtedy, keď používateľ nevie o jeho použití.

Protokol IPsec podporuje nasledovné funkcie:

- Prenosy IPsec

  V závislosti od podmienok nastavení protokolu IPsec počítač pripojený do siete odosiela/prijíma údaje do/z určeného zariadenia použitím protokolu IPsec. Keď zariadenia začnú komunikovať prostredníctvom protokolu IPsec, najskôr sa vymenia kľúče pomocou protokolu IKE (Internet Key Exchange), a potom sa použitím daných kľúčov prenesú šifrované údaje.

  Okrem toho má protokol IPsec dva prevádzkové režimy: Režim prenosu a Tunelový režim. Režim prenosu sa používa hlavne na komunikáciu medzi zariadeniami a Tunelový režim sa používa v prostrediach ako napríklad virtuálna súkromná sieť (VPN).

Na prenosy použitím protokolu IPsec je potrebné, aby boli splnené nasledujúce podmienky:

- Počítač, ktorý umožňuje komunikáciu s použitím zabezpečenia IPsec je pripojený do siete.
- Vaše zariadenie je konfigurované na komunikáciu použitím protokolu IPsec.
- Počítač pripojený k vášmu zariadeniu je konfigurovaný na pripojenie použitím protokolu IPsec.

- Nastavenia IPsec

  Nastavenia, ktoré sú potrebné na pripojenie s použitím zabezpečenia IPsec. Tieto nastavenia je možné konfigurovať prostredníctvom služby Web Based Management (Ovládanie cez webové rozhranie).

Aby ste mohli konfigurovať nastavenia IPsec, musíte použiť prehliadač na počítači, ktorý je pripojený do siete.

Súvisiace informácie

- Použitie IPsec

Konfigurovanie IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

Podmienky pripojenia IPsec obsahujú dva typy **Template (Šablóna)**: **Address (Adresa)** a **IPsec**. Konfigurovať je možné maximálne 10 podmienok pripojenia.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **IPsec** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Nakonfigurujte nastavenia.

Možnosť	Popis
Status (Stav)	Povolenie alebo zakázanie IPsec.
Negotiation Mode (Režim vyjednávania)	Zvoľte **Negotiation Mode (Režim vyjednávania)** pre IKE, fáza 1. IKE je protokol, ktorý sa používa na výmenu šifrovacích kľúčov, aby sa mohla uskutočniť šifrovaná komunikácia s použitím zabezpečenia IPsec. V režime **Main (Hlavný)** je rýchlosť spracovania nízka, no zabezpečenie je vysoké. V režime **Aggressive (Agresívny)** je rýchlosť spracovania vyššia než v režime **Main (Hlavný)**, no zabezpečenie je nižšie.
All Non-IPsec Traffic (Všetky prenosy okrem IPsec)	Zvoľte úkon, ktorý sa má vykonať v prípade paketov bez zabezpečenia IPsec. Keď sa používajú webové služby, musíte pre položku **Allow (Povoliť)** zvoliť možnosť **All Non-IPsec Traffic (Všetky prenosy okrem IPsec)**. Ak ste zvolili možnosť **Drop (Pustiť)**, webové služby nie je možné použiť.
Broadcast/Multicast Bypass (Obchádzanie rozosielania/ multicastingu)	Vyberte **Enabled (Zapnuté)** alebo **Disabled (Deaktivované)**.
Protocol Bypass (Obchádzanie protokolu)	Zvoľte políčka na označenie pre požadovanú voľbu alebo voľby.
Rules (Pravidlá)	Začiarknutím políčka na označenie **Enabled (Zapnuté)** aktivujte šablónu. Keď začiarknete viacero políčok na označenie a nastavenia pre začiarknuté políčka sú v konflikte, políčka na označenie s nižšími číslami budú mať prioritu. Kliknutím na zodpovedajúci rozbaľovací zoznam zvoľte položku **Address Template (Šablóna adresy)**, ktorá je použitá pre podmienky pripojenia IPsec. Ak chcete pridať položku **Address Template (Šablóna adresy)**, kliknite na **Add Template (Pridať šablónu)**.

Možnosť	Popis
	Kliknutím na zodpovedajúci rozbaľovací zoznam zvoľte položku **IPsec Template (Šablóna IPsec)**, ktorá je použitá pre podmienky pripojenia IPsec. Ak chcete pridať položku **IPsec Template (Šablóna IPsec)**, kliknite na **Add Template (Pridať šablónu)**.

6. Kliknite na **Submit (Odoslať)**.

   Ak sa kvôli aktivácii nových nastavení musí zariadenie reštartovať, zobrazí sa obrazovka pre potvrdenie reštartovania.

   Ak sa v šablóne, ktorú ste povolili v tabuľke **Rules (Pravidlá)** nachádza prázdna položka, zobrazí sa hlásenie o chybe. Skontrolujte vybrané položky a znova kliknite na **Submit (Odoslať)**.

Súvisiace informácie

- Použitie IPsec

Súvisiace témy:

- Konfigurovanie certifikátov zabezpečenia zariadenia

Konfigurovanie šablóny adresy zabezpečenia IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **IPsec Address Template (Šablóna adresy IPsec)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Kliknutím na tlačidlo **Delete (Vymazať)** odstráňte **Address Template (Šablóna adresy)**. Keď sa **Address Template (Šablóna adresy)** používa, nedá sa odstrániť.
6. Kliknite na položku **Address Template (Šablóna adresy)**, ktorú chcete odstrániť. Zobrazí sa položka **IPsec Address Template (Šablóna adresy IPsec)**.
7. Nakonfigurujte nastavenia.

Možnosť	Popis
Template Name (Názov šablóny)	Zadanie názvu šablóny (maximálne 16 znakov).
Local IP Address (Miestna IP adresa)	• **IP Address (Adresa IP)** Určenie adresy IP. V rozbaľovacom zozname zvoľte možnosť **ALL IPv4 Address (VŠETKY IPv4 adresy)**, **ALL IPv6 Address (VŠETKY IPv6 adresy)**, **All Link Local IPv6 (Všetky lokálne IPv6 adresy pre linku)** alebo **Custom (Vlastné)**. Ak v rozbaľovacom zozname zvolíte možnosť **Custom (Vlastné)**, do textového poľa zadajte adresu IP (IPv4 alebo IPv6). • **IP Address Range (Rozsah IP adries)** Do textových polí zadajte začiatočnú a koncovú adresu IP rozsahu adries IP. Ak začiatočná a koncová adresa IP nie sú standardized pre IPv4 alebo IPv6, alebo ak je koncová adresa IP menšia než začiatočná adresa, dôjde k chybe. • **IP Address / Prefix (IP adresa/predpona)** Určenie adresy IP pomocou zápisu CIDR. Napríklad: 192.168.1.1/24 Pretože predpona je určená vo forme 24-bitovej masky podsiete (255.255.255.0) pre adresu 192.168.1.1, adresy 192.168.1.### sú platné.
Remote IP Address (Vzdialená IP adresa)	• **Any (Akákoľvek)** Ak zvolíte možnosť **Any (Akákoľvek)**, povolia sa všetky adresy IP. • **IP Address (Adresa IP)** Do textového poľa zadajte určenú adresu IP (IPv4 alebo IPv6). • **IP Address Range (Rozsah IP adries)**

Možnosť	Popis
	Zadajte prvú a poslednú adresu IP pre rozsah adries IP. Ak prvá a posledná adresa IP nie sú standardized pre IPv4 alebo IPv6, alebo ak je posledná adresa IP menšia než prvá adresa, dôjde k chybe. • **IP Address / Prefix (IP adresa/predpona)** Určenie adresy IP pomocou zápisu CIDR. Napríklad: 192.168.1.1/24 Pretože predpona je určená vo forme 24-bitovej masky podsiete (255.255.255.0) pre adresu 192.168.1.1, adresy 192.168.1.### sú platné.

8. Kliknite na položku **Submit (Odoslať)**.

Ak zmeníte nastavenia aktuálne používanej šablóny, reštartujte zariadenie, aby sa konfigurácia mohla aktivovať.

Súvisiace informácie

- Použitie IPsec

Konfigurovanie šablóny IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

   Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.
4. Kliknite na **Network (Sieť)** > **Security (Zabezpečenie)** > **IPsec Template (Šablóna IPsec)** na ľavom navigačnom paneli.

   Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.
5. Kliknutím na tlačidlo **Delete (Vymazať)** odstráňte **IPsec Template (Šablóna IPsec)**. Keď sa **IPsec Template (Šablóna IPsec)** používa, nedá sa odstrániť.
6. Kliknite na položku **IPsec Template (Šablóna IPsec)**, ktorú chcete vytvoriť. Zobrazí sa obrazovka **IPsec Template (Šablóna IPsec)**. Polia konfigurácie sa odlišujú na základe nastavení **Use Prefixed Template (Použiť vopred oznámenú šablónu)** a **Internet Key Exchange (IKE)**, ktoré zvolíte.
7. Do poľa **Template Name (Názov šablóny)** zadajte názov pre šablónu (maximálne 16 znakov).
8. Ak vyberiete **Custom (Vlastné)** v rozbaľovacom zozname **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, vyberte možnosti **Internet Key Exchange (IKE)** a potom zmeňte nastavenia, ak je to potrebné.
9. Kliknite na položku **Submit (Odoslať)**.

Súvisiace informácie

- Použitie IPsec
  - Nastavenia IKEv1 pre šablónu IPsec
  - Nastavenia IKEv2 pre šablónu IPsec
  - Manuálne nastavenia pre šablónu IPsec

Nastavenia IKEv1 pre šablónu IPsec

Možnosť	Popis
Template Name (Názov šablóny)	Zadanie názvu šablóny (maximálne 16 znakov).
Use Prefixed Template (Použiť vopred oznámenú šablónu)	Zvoľte **Custom (Vlastné)**, **IKEv1 High Security (IKEv1 Vysoké zabezpečenie)** alebo **IKEv1 Medium Security (IKEv1 stredné zabezpečenie)**. Položky nastavenia sa odlišujú v závislosti od zvolenej šablóny.
Internet Key Exchange (IKE)	IKE je komunikačný protokol, ktorý sa používa na výmenu šifrovacích kľúčov, aby sa mohla uskutočniť šifrovaná komunikácia s použitím zabezpečenia IPsec. Aby sa šifrovaná komunikácia uskutočnila len pre daný raz, určí sa šifrovací algoritmus, ktorý je potrebný pre zabezpečenie IPsec a zdieľajú sa šifrovacie kľúče. Pre protokol IKE sa šifrovacie kľúče vymenia s použitím metódy výmeny kľúčov Diffie-Hellman, a uskutoční sa šifrovaná komunikácia, ktorá je obmedzená na protokol IKE. Ak je zvolená možnosť **Custom (Vlastné)** v položke **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, zvoľte **IKEv1**. .
Authentication Type (Typ overenia)	• **Diffie_Hellman_Group** Táto metóda výmeny kľúčov umožňuje bezpečnú výmenu tajných kľúčov cez nechránenú sieť. Metóda výmeny kľúčov Diffie-Hellman využíva problém diskrétneho logaritmu, nie tajný kľúč, na odosielanie a prijímanie otvorených informácií, ktoré sa vygenerovali s použitím náhodného čísla a daného tajného kľúča. Zvoľte **Group1 (Skupina 1)**, **Group2 (Skupina 2)**, **Group5 (Skupina 5)** alebo **Group14 (Skupina 14)**. • **Encryption (Šifrovanie)** Zvoľte **DES**, **3DES**, **AES-CBC 128** alebo **AES-CBC 256**. • **Hash** Zvoľte **MD5**, **SHA1**, **SHA256**, **SHA384** alebo **SHA512**. • **SA Lifetime (Životnosť SA)** Určenie životnosti bezpečnostnej asociácie protokolu IKE. Zadajte čas (sekundy) a počet kilobajtov (KByte).
Encapsulating Security (Zabezpečenie zapuzdrením)	• **Protocol (Protokol)** Zvoľte **ESP**, **AH** alebo **AH+ESP**. - ESP je protokol na uskutočňovanie šifrovanej komunikácie s použitím zabezpečenia IPsec. ESP šifruje údajovú časť (komunikovaný obsah, tzv. payload) a pridáva dodatočné informácie. Paket protokolu IP obsahuje hlavičku a šifrovanú údajovú časť, ktorá nasleduje za hlavičkou. Okrem šifrovaných dát obsahuje paket protokolu IP aj informácie ohľadne metódy šifrovania a šifrovací kľúč, overovacie údaje a podobne. - AH je súčasťou protokolu IPsec, ktorá overuje odosielateľa a zabraňuje manipulácii (zaručuje úplnosť dát). V pakete protokolu IP sa dáta vkladajú hneď za hlavičku. Okrem toho pakety obsahujú hodnoty hash, ktoré sa vypočítavajú s použitím rovnice z komunikovaného obsahu, tajného kľúča atď., aby sa tak zabránilo falšovaniu odosielateľa a manipulácii s dátami. Na rozdiel od ESP nie je komunikovaný obsah šifrovaný a dáta sa odosielajú a prijímajú ako obyčajný text. • **Encryption (Šifrovanie) (Nie je k dispozícii pre možnosť AH.)** Zvoľte **DES**, **3DES**, **AES-CBC 128** alebo **AES-CBC 256**.

Možnosť	Popis
	• **Hash** Zvoľte **None (Žiadny)**, **MD5**, **SHA1**, **SHA256**, **SHA384** alebo **SHA512**. **None (Žiadny)** je možné zvoliť, len keď je zvolená možnosť **ESP** v položke **Protocol (Protokol)**. • **SA Lifetime (Životnosť SA)** Určite životnosť bezpečnostnej asociácie IKE. Zadajte čas (sekundy) a počet kilobajtov (KByte). • **Encapsulation Mode (Režim zapuzdrenia)** Vyberte možnosť **Transport (Transport)** alebo **Tunnel (Tunel)**. • **Remote Router IP-Address (IP adresa vzdialeného smerovača)** Zadajte adresu IP (IPv4 alebo IPv6) vzdialeného smerovača. Tieto informácie zadajte, len keď je zvolený režim **Tunnel (Tunel)**. SA (bezpečnostná asociácia) je metóda šifrovanej komunikácie používajúca protokol IPsec alebo IPv6, ktorá vymieňa a zdieľa informácie, ako napríklad metódu šifrovania a šifrovací kľúč, aby sa tak pred začatím komunikácie vytvoril zabezpečený komunikačný kanál. SA tiež môže označovať virtuálny zašifrovaný komunikačný kanál, ktorý bol vytvorený. SA použitá pre protokol IPsec vytvára metódu šifrovania, vymieňa kľúče a vykonáva vzájomné overovanie na základe štandardnej procedúry IKE (Internet Key Exchange). Okrem toho sa SA pravidelne aktualizuje.
Perfect Forward Secrecy (PFS) (Technológia Perfect Forward Secrecy)	PFS neodvodzuje kľúče z predchádzajúcich kľúčov, ktoré sa použili na šifrovanie správ. Okrem toho, ak bol kľúč, ktorý sa použil na šifrovanie správy, odvodený z nadradeného kľúča, daný nadradený kľúč sa nepoužije na odvodenie ďalších kľúčov. Preto, aj keby bol kľúč odhalený, škoda bude obmedzená len na správy, ktoré boli šifrované pomocou daného kľúča. Vyberte **Enabled (Zapnuté)** alebo **Disabled (Deaktivované)**.
Authentication Method (Metóda overenia)	Vyberte metódu overenia. Vyberte **Pre-Shared Key (Predbežne zdieľaný kľúč)** alebo **Certificates (Certifikáty)**.
Pre-Shared Key (Predbežne zdieľaný kľúč)	Pri šifrovaní komunikácie sa šifrovací kľúč vopred vymení a zdieľa použitím iného kanála. Ak ste pre **Authentication Method (Metóda overenia)** zvolili **Pre-Shared Key (Predbežne zdieľaný kľúč)**, zadajte **Pre-Shared Key (Predbežne zdieľaný kľúč)** (maximálne 32 znakov). • **Local/ID Type/ID (Miestne/typ ID/ID)** Zvoľte typ ID odosielateľa a potom zadajte ID. Pre typ zvoľte **IPv4 Address (Adresa IPv4)**, **IPv6 Address (Adresa IPv6)**, **FQDN**, **E-mail Address (E-mailová adresa)** alebo **Certificate (Certifikát)**. Ak je zvolená možnosť **Certificate (Certifikát)**, v poli **ID** zadajte spoločné meno certifikátu. • **Remote/ID Type/ID (Diaľkové/typ ID/ID)** Zvoľte typ ID prijímateľa a potom zadajte ID. Pre typ zvoľte **IPv4 Address (Adresa IPv4)**, **IPv6 Address (Adresa IPv6)**, **FQDN**, **E-mail Address (E-mailová adresa)** alebo **Certificate (Certifikát)**. Ak je zvolená možnosť **Certificate (Certifikát)**, v poli **ID** zadajte spoločné meno certifikátu.
Certificate (Certifikát)	Ak ste pre **Authentication Method (Metóda overenia)** zvolili **Certificates (Certifikáty)**, vyberte certifikát.

Možnosť	Popis
	Môžete zvoliť len certifikáty, ktoré boli vytvorené s použitím stránky **Certificate (Certifikát)** na obrazovke konfigurácie zabezpečenia ovládania cez webové rozhranie.

Súvisiace informácie

- Konfigurovanie šablóny IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

Nastavenia IKEv2 pre šablónu IPsec

Možnosť	Popis
Template Name (Názov šablóny)	Zadanie názvu šablóny (maximálne 16 znakov).
Use Prefixed Template (Použiť vopred oznámenú šablónu)	Zvoľte **Custom (Vlastné)**, **IKEv2 High Security (IKEv2 Vysoké zabezpečenie)** alebo **IKEv2 Medium Security (IKEv2 stredné zabezpečenie)**. Položky nastavenia sa odlišujú v závislosti od zvolenej šablóny.
Internet Key Exchange (IKE)	IKE je komunikačný protokol, ktorý sa používa na výmenu šifrovacích kľúčov, aby sa mohla uskutočniť šifrovaná komunikácia s použitím zabezpečenia IPsec. Aby sa šifrovaná komunikácia uskutočnila len pre daný raz, určí sa šifrovací algoritmus, ktorý je potrebný pre zabezpečenie IPsec a zdieľajú sa šifrovacie kľúče. Pre protokol IKE sa šifrovacie kľúče vymenia s použitím metódy výmeny kľúčov Diffie-Hellman, a uskutoční sa šifrovaná komunikácia, ktorá je obmedzená na protokol IKE. Ak je zvolená možnosť **Custom (Vlastné)** v položke **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, zvoľte **IKEv2**.
Authentication Type (Typ overenia)	• **Diffie_Hellman_Group** Táto metóda výmeny kľúčov umožňuje bezpečnú výmenu tajných kľúčov cez nechránenú sieť. Metóda výmeny kľúčov Diffie-Hellman využíva problém diskrétneho logaritmu, nie tajný kľúč, na odosielanie a prijímanie otvorených informácií, ktoré sa vygenerovali s použitím náhodného čísla a daného tajného kľúča. Zvoľte **Group1 (Skupina 1)**, **Group2 (Skupina 2)**, **Group5 (Skupina 5)** alebo **Group14 (Skupina 14)**. • **Encryption (Šifrovanie)** Zvoľte **DES**, **3DES**, **AES-CBC 128** alebo **AES-CBC 256**. • **Hash** Zvoľte **MD5**, **SHA1**, **SHA256**, **SHA384** alebo **SHA512**. • **SA Lifetime (Životnosť SA)** Určenie životnosti bezpečnostnej asociácie protokolu IKE. Zadajte čas (sekundy) a počet kilobajtov (KByte).
Encapsulating Security (Zabezpečenie zapuzdrením)	• **Protocol (Protokol)** Vyberte **ESP**. ESP je protokol na uskutočňovanie šifrovanej komunikácie s použitím zabezpečenia IPsec. ESP šifruje údajovú časť (komunikovaný obsah, tzv. payload) a pridáva dodatočné informácie. Paket protokolu IP obsahuje hlavičku a šifrovanú údajovú časť, ktorá nasleduje za hlavičkou. Okrem šifrovaných dát obsahuje paket protokolu IP aj informácie ohľadne metódy šifrovania a šifrovací kľúč, overovacie údaje a podobne. • **Encryption (Šifrovanie)** Zvoľte **DES**, **3DES**, **AES-CBC 128** alebo **AES-CBC 256**. • **Hash** Vyberte **MD5**, **SHA1**, **SHA256**, **SHA384** alebo **SHA512**. • **SA Lifetime (Životnosť SA)** Určite životnosť bezpečnostnej asociácie IKE. Zadajte čas (sekundy) a počet kilobajtov (KByte). • **Encapsulation Mode (Režim zapuzdrenia)** Vyberte možnosť **Transport (Transport)** alebo **Tunnel (Tunel)**.

Možnosť	Popis
	• **Remote Router IP-Address (IP adresa vzdialeného smerovača)** Zadajte adresu IP (IPv4 alebo IPv6) vzdialeného smerovača. Tieto informácie zadajte, len keď je zvolený režim **Tunnel (Tunel)**. SA (bezpečnostná asociácia) je metóda šifrovanej komunikácie používajúca protokol IPsec alebo IPv6, ktorá vymieňa a zdieľa informácie, ako napríklad metódu šifrovania a šifrovací kľúč, aby sa tak pred začatím komunikácie vytvoril zabezpečený komunikačný kanál. SA tiež môže označovať virtuálny zašifrovaný komunikačný kanál, ktorý bol vytvorený. SA použitá pre protokol IPsec vytvára metódu šifrovania, vymieňa kľúče a vykonáva vzájomné overovanie na základe štandardnej procedúry IKE (Internet Key Exchange). Okrem toho sa SA pravidelne aktualizuje.
Perfect Forward Secrecy (PFS) (Technológia Perfect Forward Secrecy)	PFS neodvodzuje kľúče z predchádzajúcich kľúčov, ktoré sa použili na šifrovanie správ. Okrem toho, ak bol kľúč, ktorý sa použil na šifrovanie správy, odvodený z nadradeného kľúča, daný nadradený kľúč sa nepoužije na odvodenie ďalších kľúčov. Preto, aj keby bol kľúč odhalený, škoda bude obmedzená len na správy, ktoré boli šifrované pomocou daného kľúča. Vyberte **Enabled (Zapnuté)** alebo **Disabled (Deaktivované)**.
Authentication Method (Metóda overenia)	Vyberte metódu overenia. Zvoľte **Pre-Shared Key (Predbežne zdieľaný kľúč)**, **Certificates (Certifikáty)**, **EAP - MD5** alebo **EAP - MS-CHAPv2**. EAP je overovací protokol, ktorý je rozšírením protokolu PPP. Keď sa protokol EAP použije so štandardom IEEE802.1x, na overenie používateľa sa počas každej relácie použije iný kľúč. Nasledovné nastavenia sú potrebné, len keď je vo funkcii **Authentication Method (Metóda overenia)** zvolená možnosť **EAP - MD5** alebo **EAP - MS-CHAPv2**: • **Mode (Režim)** Vyberte **Server-Mode (Režim servera)** alebo **Client-Mode (Režim klienta)**. • **Certificate (Certifikát)** Výber certifikátu. • **User Name (Meno používateľa)** Zadanie mena používateľa (maximálne 32 znakov). • **Password (Heslo)** Zadanie hesla (maximálne 32 znakov). Heslo sa musí kvôli potvrdeniu zadať dvakrát.
Pre-Shared Key (Predbežne zdieľaný kľúč)	Pri šifrovaní komunikácie sa šifrovací kľúč vopred vymení a zdieľa použitím iného kanála. Ak ste pre **Authentication Method (Metóda overenia)** zvolili **Pre-Shared Key (Predbežne zdieľaný kľúč)**, zadajte **Pre-Shared Key (Predbežne zdieľaný kľúč)** (maximálne 32 znakov). • **Local/ID Type/ID (Miestne/typ ID/ID)** Zvoľte typ ID odosielateľa a potom zadajte ID. Pre typ zvoľte **IPv4 Address (Adresa IPv4)**, **IPv6 Address (Adresa IPv6)**, **FQDN**, **E-mail Address (E-mailová adresa)** alebo **Certificate (Certifikát)**. Ak je zvolená možnosť **Certificate (Certifikát)**, v poli **ID** zadajte spoločné meno certifikátu. • **Remote/ID Type/ID (Diaľkové/typ ID/ID)** Zvoľte typ ID prijímateľa a potom zadajte ID.

Možnosť	Popis
	Pre typ zvoľte **IPv4 Address (Adresa IPv4)**, **IPv6 Address (Adresa IPv6)**, **FQDN**, **E-mail Address (E-mailová adresa)** alebo **Certificate (Certifikát)**. Ak je zvolená možnosť **Certificate (Certifikát)**, v poli **ID** zadajte spoločné meno certifikátu.
Certificate (Certifikát)	Ak ste pre **Authentication Method (Metóda overenia)** zvolili **Certificates (Certifikáty)**, vyberte certifikát. Môžete zvoliť len certifikáty, ktoré boli vytvorené s použitím stránky **Certificate (Certifikát)** na obrazovke konfigurácie zabezpečenia ovládania cez webové rozhranie.

Súvisiace informácie

- Konfigurovanie šablóny IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

Manuálne nastavenia pre šablónu IPsec

Možnosť	Popis
Template Name (Názov šablóny)	Zadanie názvu šablóny (maximálne 16 znakov).
Use Prefixed Template (Použiť vopred oznámenú šablónu)	Vyberte **Custom (Vlastné)**.
Internet Key Exchange (IKE)	IKE je komunikačný protokol, ktorý sa používa na výmenu šifrovacích kľúčov, aby sa mohla uskutočniť šifrovaná komunikácia s použitím zabezpečenia IPsec. Aby sa šifrovaná komunikácia uskutočnila len pre daný raz, určí sa šifrovací algoritmus, ktorý je potrebný pre zabezpečenie IPsec a zdieľajú sa šifrovacie kľúče. Pre protokol IKE sa šifrovacie kľúče vymenia s použitím metódy výmeny kľúčov Diffie-Hellman, a uskutoční sa šifrovaná komunikácia, ktorá je obmedzená na protokol IKE. Vyberte **Manual (Manuálne)**.
Authentication Key (ESP, AH) (Overovací kľúč (ESP, AH))	Zadajte hodnoty **In/Out (Vstup/výstup)**. Tieto nastavenia sú nevyhnutné, keď je zvolená možnosť **Custom (Vlastné)** pre položku **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, možnosť **Manual (Manuálne)** je zvolená pre položku **Internet Key Exchange (IKE)**, a pre položku **Hash** pre časť **Encapsulating Security (Zabezpečenie zapuzdrením)** je zvolené iné nastavenie než **None (Žiadny)**. Počet znakov, ktoré môžete nastaviť, sa odlišuje v závislosti od nastavenia, ktoré zvolíte pre položku **Hash** v časti **Encapsulating Security (Zabezpečenie zapuzdrením)**. Ak je dĺžka určeného overovacieho kľúča iná než zvolený hashovací algoritmus, dôjde k chybe. • **MD5**: 128 bitov (16 bajtov) • **SHA1**: 160 bitov (20 bajtov) • **SHA256**: 256 bitov (32 bajtov) • **SHA384**: 384 bitov (48 bajtov) • **SHA512**: 512 bitov (64 bajtov) Keď kľúč určíte v kóde ASCII, ohraničte znaky dvojitými úvodzovkami (").
Code key (ESP) (Kódový kľúč (ESP))	Zadajte hodnoty **In/Out (Vstup/výstup)**. Tieto nastavenia sú nevyhnutné, keď je zvolená hodnota **Custom (Vlastné)** pre položku **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, **Manual (Manuálne)** pre položku **Internet Key Exchange (IKE)** a **ESP** pre položku **Protocol (Protokol)** v časti **Encapsulating Security (Zabezpečenie zapuzdrením)**.

Možnosť	Popis
	Počet znakov, ktoré môžete nastaviť, sa odlišuje v závislosti od nastavenia, ktoré zvolíte pre položku **Encryption (Šifrovanie)** v časti **Encapsulating Security (Zabezpečenie zapuzdrením)**. Ak je dĺžka určeného kódového kľúča iná než vybraný šifrovací algoritmus, dôjde k chybe. • **DES**: 64 bitov (8 bajtov) • **3DES**: 192 bitov (24 bajtov) • **AES-CBC 128**: 128 bitov (16 bajtov) • **AES-CBC 256**: 256 bitov (32 bajtov) Keď kľúč určíte v kóde ASCII, ohraničte znaky dvojitými úvodzovkami (").
SPI	Tieto parametre sa používajú na identifikáciu bezpečnostných informácií. Vo všeobecnosti má hostiteľ viacero bezpečnostných asociácií (SA) pre rôzne typy komunikácie IPsec. Preto je nevyhnutné identifikovať vhodné bezpečnostné asociácie, keď sa prijme paket IPsec. Parameter SPI, ktorý identifikuje bezpečnostnú asociáciu je zahrnutý v hlavičke AH (Authentication Header) a hlavičke ESP (Encapsulating Security Payload). Tieto nastavenia sú nevyhnutné, keď je zvolená možnosť **Custom (Vlastné)** pre položku **Use Prefixed Template (Použiť vopred oznámenú šablónu)**, a možnosť **Manual (Manuálne)** je zvolená pre položku **Internet Key Exchange (IKE)**. Zadajte hodnoty **In/Out (Vstup/výstup)**. (3 až 10 znakov)
Encapsulating Security (Zabezpečenie zapuzdrením)	• **Protocol (Protokol)** Vyberte **ESP** alebo **AH**. - ESP je protokol na uskutočňovanie šifrovanej komunikácie s použitím zabezpečenia IPsec. ESP šifruje údajovú časť (komunikovaný obsah, tzv. payload) a pridáva dodatočné informácie. Paket protokolu IP obsahuje hlavičku a šifrovanú údajovú časť, ktorá nasleduje za hlavičkou. Okrem šifrovaných dát obsahuje paket protokolu IP aj informácie ohľadne metódy šifrovania a šifrovací kľúč, overovacie údaje a podobne. - AH je súčasťou protokolu IPsec, ktorá overuje odosielateľa a zabraňuje manipulácii s dátami (zaručuje úplnosť dát). V pakete protokolu IP sa dáta vkladajú hneď za hlavičku. Okrem toho pakety obsahujú hodnoty hash, ktoré sa vypočítavajú s použitím rovnice z komunikovaného obsahu, tajného kľúča atď., aby sa tak zabránilo falšovaniu odosielateľa a manipulácii s dátami. Na rozdiel od ESP nie je komunikovaný obsah šifrovaný a dáta sa odosielajú a prijímajú ako obyčajný (plain) text. • **Encryption (Šifrovanie) (Nie je k dispozícii pre možnosť AH.)** Zvoľte **DES**, **3DES**, **AES-CBC 128** alebo **AES-CBC 256**. • **Hash** Zvoľte **None (Žiadny)**, **MD5**, **SHA1**, **SHA256**, **SHA384** alebo **SHA512**. **None (Žiadny)** je možné zvoliť, len keď je zvolená možnosť **ESP** v položke **Protocol (Protokol)**. • **SA Lifetime (Životnosť SA)** Určite životnosť bezpečnostnej asociácie IKE. Zadajte čas (sekundy) a počet kilobajtov (KByte). • **Encapsulation Mode (Režim zapuzdrenia)** Vyberte možnosť **Transport (Transport)** alebo **Tunnel (Tunel)**.

Možnosť	Popis
	• **Remote Router IP-Address (IP adresa vzdialeného smerovača)** Zadajte adresu IP (IPv4 alebo IPv6) vzdialeného smerovača. Tieto informácie zadajte, len keď je zvolený režim **Tunnel (Tunel)**. SA (bezpečnostná asociácia) je metóda šifrovanej komunikácie používajúca protokol IPsec alebo IPv6, ktorá vymieňa a zdieľa informácie, ako napríklad metódu šifrovania a šifrovací kľúč, aby sa tak pred začatím komunikácie vytvoril zabezpečený komunikačný kanál. SA tiež môže označovať virtuálny zašifrovaný komunikačný kanál, ktorý bol vytvorený. SA použitá pre protokol IPsec vytvára metódu šifrovania, vymieňa kľúče a vykonáva vzájomné overovanie na základe štandardnej procedúry IKE (Internet Key Exchange). Okrem toho sa SA pravidelne aktualizuje.

Súvisiace informácie

- Konfigurovanie šablóny IPsec pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

Použitie overenia IEEE 802.1x vašej siete

- Čo je overovanie IEEE 802.1x?
- Konfigurácia overenia IEEE 802.1x pre vašu sieť pomocou ovládania cez webové rozhranie (webový prehliadač)
- Metódy overenia IEEE 802.1x

Čo je overovanie IEEE 802.1x?

IEEE 802.1x je štandard IEEE, ktorý obmedzuje prístup zo sieťových zariadení, ktoré unauthorized. Vaše zariadenie Brother odosiela požiadavku na overenie serveru RADIUS (overovací server) cez váš prístupový bod alebo rozbočovač. Po overení vašej požiadavky serverom RADIUS môže vaše zariadenie pristupovať do siete.

Súvisiace informácie

- Použitie overenia IEEE 802.1x vašej siete

Konfigurácia overenia IEEE 802.1x pre vašu sieť pomocou ovládania cez webové rozhranie (webový prehliadač)

- Ak konfigurujete zariadenie pomocou overenia EAP-TLS, pred spustením samotného konfigurovania je potrebné nainštalovať certifikát klienta vydaný certifikačnou autoritou. Informácie o certifikáte klienta vám poskytne správca siete. Ak ste nainštalovali viac ako jeden certifikát, odporúčame poznačiť si názov certifikátu, ktorý chcete používať.
- Pred overením certifikátu servera je potrebné importovať certifikát certifikačnej autority vydaný certifikačnou autoritou, ktorá podpísala certifikát servera. U správcu siete alebo poskytovateľa internetových služieb (ISP) overte, či je importovanie certifikátu certifikačnej autority potrebné.

Overenie IEEE 802.1x môžete nakonfigurovať aj pomocou Sprievodcu nastavením bezdrôtovej siete z ovládacieho panela (bezdrôtová sieť).

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Network (Sieť)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Vykonajte jednu z nasledujúcich činností:
   - Pre káblovú sieť

     Kliknite na **Wired (Káblové)** > **Wired 802.1x Authentication (Overovanie káblovej komunikácie 802.1x)**.
   - Pre bezdrôtovú sieť

     Kliknite na **Wireless (Bezdrôtové)** > **Wireless (Enterprise) (Bezdrôtové (podnikové))**.
6. Nakonfigurujte nastavenia overovania IEEE 802.1x.

- Ak chcete aktivovať overovania cez IEEE 802.1x pre káblové siete, zvoľte **Enabled (Zapnuté)** v položke **Wired 802.1x status (Stav káblovej siete 802.1x)** na stránke **Wired 802.1x Authentication (Overovanie káblovej komunikácie 802.1x)**.
- Ak používate **EAP-TLS** overovanie, v rozbaľovacom zozname **Client Certificate (Certifikát klienta)** musíte zvoliť certifikát klienta, ktorý bol nainštalovaný za účelom overovania (zobrazuje sa s názvom certifikátu).
- Ak zvolíte overovanie **EAP-FAST**, **PEAP**, **EAP-TTLS** alebo **EAP-TLS**, zvoľte metódu overenia v rozbaľovacom zozname **Server Certificate Verification (Overenie serverového certifikátu)**. Certifikát servera overte pomocou certifikátu certifikačnej autority, vopred importovaného do zariadenia, ktorý vydala certifikačná autorita, ktorá zároveň podpísala aj certifikát servera.

V rozbaľovacom zozname **Server Certificate Verification (Overenie serverového certifikátu)** zvoľte jednu z nasledujúcich metód overenia:

Možnosť	Popis
No Verification (Bez overenia)	Certifikát servera je vždy dôveryhodný. Overenie sa nevykonáva.
CA Cert. (Certifikát CA)	Metóda overenia na kontrolu spoľahlivosti certifikátu servera voči certifikačnej autorite, s použitím certifikátu certifikačnej autority, vydaným certifikačnou autoritou, ktorá podpísala certifikát servera.
CA Cert. + ServerID (Certifikát CA + ID servera)	Metóda overenia na kontrolu spoločného mena [1] certifikátu servera, ako doplnok spoľahlivosti certifikátu servera voči certifikačnej autorite.

7. Po dokončení konfigurácie kliknite na položku **Submit (Odoslať)**.

   V prípade káblových sietí: Po dokončení konfigurácie pripojte vaše zariadenie do siete, ktorá podporuje protokol IEEE 802.1x. Po niekoľkých minútach vytlačte Správu o konfigurácii siete a skontrolujte stav <**Wired IEEE 802.1x**>.

Možnosť	Popis
Success	Funkcia IEEE 802.1x v káblovej sieti je povolená a overenie prebehlo úspešne.
Failed	Funkcia IEEE 802.1x v káblovej sieti je povolená; overenie však zlyhalo.
Off	Funkcia IEEE 802.1x v káblovej sieti nie je dostupná.

Súvisiace informácie

- Použitie overenia IEEE 802.1x vašej siete

Súvisiace témy:

- Prehľad funkcií certifikátu zabezpečenia
- Konfigurovanie certifikátov zabezpečenia zariadenia

1 Overovanie spoločného mena porovnáva spoločné meno certifikátu servera s reťazcom znakov konfigurovaným pre **Server ID (ID servera)**. Skôr ako túto metódu použijete, zistite si u vášho správcu systému spoločné meno certifikátu servera, a potom nakonfigurujte **Server ID (ID servera)**.

Metódy overenia IEEE 802.1x

EAP-FAST

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (Rozšíriteľný overovací protokol – flexibilné overovanie cez zabezpečený tunel)) vyvinula spoločnosť Cisco Systems, Inc. a tento protokol používa na overovanie ID používateľa a heslo, a algoritmy so symetrickými kľúčmi na dosiahnutie tunneled procesu overovania.

Vaše zariadenie Brother podporuje nasledujúce metódy vnútorného overenia:

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

EAP-MD5 (Káblová sieť)

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) využíva ID používateľa a heslo na overenie typu výzva-odpoveď.

PEAP

PEAP (Protected Extensible Authentication Protocol) je verzia metódy EAP vyvinutá spoločnosťami Cisco Systems, Inc., Microsoft Corporation a RSA Security. PEAP vytvára zašifrovaný tunel SSL (Secure Sockets Layer)/TLS (Transport Layer Security) medzi klientom a overovacím serverom pre odosielanie ID používateľa a hesla. PEAP poskytuje vzájomné overenie medzi serverom a klientom.

Vaše zariadenie Brother podporuje nasledujúce metódy vnútorného overenia:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) vyvinuli spoločnosti Funk Software a Certicom. EAP-TTLS vytvára zašifrovaný SSL tunel podobný ako pri protokole PEAP, medzi klientom a overovacím serverom, na odosielanie ID používateľa a hesla. EAP-TTLS poskytuje vzájomné overenie medzi serverom a klientom.

Vaše zariadenie Brother podporuje nasledujúce metódy vnútorného overenia:

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

EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) vyžaduje overenie digitálnym osvedčením na strane klienta aj overovacieho servera.

Súvisiace informácie

- Použitie overenia IEEE 802.1x vašej siete

Overenie používateľa

- Použitie overovania Active Directory
- Použitie funkcie overovania LDAP
- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Použitie overovania Active Directory

Úvod do overovania Active Directory

Overovanie Active Directory obmedzuje používanie vášho zariadenia. Keď je overovanie Active Directory povolené, ovládací panel zariadenia bude uzamknutý. Nebudete môcť zmeniť nastavenia zariadenia, kým nezadáte ID používateľa a heslo.

Overovanie Active Directory ponúka nasledovné funkcie:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

- Ukladanie údajov prichádzajúcej tlače
- Ukladanie údajov prichádzajúcich faxov
- Načítanie e-mailovej adresy zo servera Active Directory počas odosielania naskenovaných údajov na e-mailový server, na základe vášho ID používateľa.

  Ak chcete túto funkciu použiť, vyberte možnosť **On (Zapnutý)** pre nastavenie **Get Mail Address (Získať poštovú adresu)** a metódu overenia **LDAP + kerberos** alebo **LDAP + NTLMv2**. Keď zariadenie zasiela naskenované údaje na e-mailový server, vaša e-mailová adresa bude nastavená ako odosielateľ alebo ako príjemca, ak chcete odoslať naskenované údaje na vašu e-mailovú adresu.

Keď je overovanie Active Directory povolené, zariadenie ukladá všetky údaje prichádzajúcich faxov. Keď sa prihlásite, zariadenie vytlačí údaje uložených faxov.

Nastavenia overovania Active Directory môžete zmeniť pomocou aplikácie Ovládanie cez webové rozhranie.

Súvisiace informácie

- Použitie overovania Active Directory

Konfigurovanie overovania Active Directory pomocou ovládania cez webové rozhranie

Overovanie Active Directory podporuje overovanie Kerberos a NTLMv2. Protokol SNTP (sieťový časový server) a konfiguráciu servera DNS je potrebné konfigurovať pre overovanie.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **User Restriction Function (Funkcia používateľských obmedzení)** alebo **Restriction Management (Správa obmedzení)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Vyberte položku **Active Directory Authentication (Overenie Active Directory)**.
6. Kliknite na položky **Submit (Odoslať)**.
7. Kliknite na **Active Directory Authentication (Overenie Active Directory)**.
8. Nakonfigurujte nasledujúce nastavenia:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

Možnosť	Popis
Storage Fax RX Data (Ukladanie prijatých faxových údajov)	Túto možnosť zvoľte pre ukladanie údajov prichádzajúcich faxov. Po prihlásení sa do zariadenia môžete vytlačiť všetky údaje prichádzajúcich faxov.
Remember User ID (Zapamätať si ID používateľa)	Vyberte túto možnosť, ak chcete uložiť vaše ID používateľa.
Active Directory Server Address (Adresa servera Active Directory)	Zadajte adresu IP alebo názov servera (napríklad: ad.priklad.com) servera Active Directory.
Active Directory Domain Name (Názov domény Active Directory)	Zadanie názvu domény Active Directory.
Protocol & Authentication Method (Protokol a metóda overenia)	Vyberte protokol a metódu overenia.
SSL/TLS	Zvoľte možnosť **SSL/TLS**.
LDAP Server Port (Port servera LDAP)	Zadajte číslo portu na pripojenie servera Active Directory prostredníctvom LDAP (dostupné len pre metódu overenia **LDAP + kerberos** alebo **LDAP + NTLMv2**).

Možnosť	Popis
LDAP Search Root (Koreňový adresár vyhľadávania LDAP)	Zadajte koreňový adresár vyhľadávania servera LDAP (dostupné len pre metódu overenia **LDAP + kerberos** alebo **LDAP + NTLMv2**).
Get Mail Address (Získať poštovú adresu)	Túto možnosť zvoľte na získanie e-mailovej adresy prihláseného používateľa zo servera Active Directory. (dostupné len pre metódu overenia **LDAP + kerberos** alebo **LDAP + NTLMv2**)
Get User's Home Directory (Získať domovský adresár používateľa)	Túto možnosť zvoľte na získanie domovského adresára, ako cieľového umiestnenia pre funkciu Skenovať na sieť. (dostupné len pre metódu overenia **LDAP + kerberos** alebo **LDAP + NTLMv2**)

9. Kliknite na položky **Submit (Odoslať)**.

Súvisiace informácie

- Použitie overovania Active Directory

Prihláste sa, aby ste mohli zmeniť nastavenia zariadenia prostredníctvom ovládacieho panela zariadenia (overovanie Active Directory)

Keď je povolené overenie Active Directory, ovládací panel zariadenia bude uzamknutý, kým na ovládacom paneli zariadenia nezadáte ID používateľa a heslo.

1. Na ovládacom paneli zariadenia zadajte vaše ID používateľa a heslo a prihláste sa.
2. Keď je overenie úspešné, ovládací panel zariadenia sa odomkne.

Súvisiace informácie

- Použitie overovania Active Directory

Použitie funkcie overovania LDAP

- Úvod do overovania LDAP
- Konfigurovanie overovania LDAP pomocou ovládania cez webové rozhranie
- Prihláste sa, aby ste mohli zmeniť nastavenia zariadenia prostredníctvom ovládacieho panela zariadenia (overenie LDAP)

Úvod do overovania LDAP

Funkcia overovania LDAP obmedzuje používanie vášho zariadenia. Keď je overovanie LDAP povolené, ovládací panel zariadenia bude uzamknutý. Nebudete môcť zmeniť nastavenia zariadenia, kým nezadáte ID používateľa a heslo.

Overovanie LDAP ponúka nasledovné funkcie:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

- Ukladanie údajov prichádzajúcej tlače
- Ukladanie údajov prichádzajúcich faxov
- Pri odosielaní naskenovaných údajov na e-mailový server získa zo servera LDAP e-mailovú adresu na základe ID používateľa.

  Ak chcete túto funkciu použiť, vyberte možnosť **On (Zapnutý)** pre nastavenie **Get Mail Address (Získať poštovú adresu)**. Keď zariadenie zasiela naskenované údaje na e-mailový server, vaša e-mailová adresa bude nastavená ako odosielateľ alebo ako príjemca, ak chcete odoslať naskenované údaje na vašu e-mailovú adresu.

Keď je overovanie LDAP povolené, zariadenie ukladá všetky údaje prichádzajúcich faxov. Keď sa prihlásite, zariadenie vytlačí údaje uložených faxov.

Nastavenia overovania LDAP môžete zmeniť pomocou aplikácie Ovládanie cez webové rozhranie.

Súvisiace informácie

- Použitie funkcie overovania LDAP

Konfigurovanie overovania LDAP pomocou ovládania cez webové rozhranie

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **User Restriction Function (Funkcia používateľských obmedzení)** alebo **Restriction Management (Správa obmedzení)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Vyberte **LDAP Authentication (Overovanie LDAP)**.
6. Kliknite na položky **Submit (Odoslať)**.
7. Kliknite na ponuku **LDAP Authentication (Overovanie LDAP)**.
8. Nakonfigurujte nasledujúce nastavenia:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

Možnosť	Popis
Storage Fax RX Data (Ukladanie prijatých faxových údajov)	Túto možnosť zvoľte pre ukladanie údajov prichádzajúcich faxov. Po prihlásení sa do zariadenia môžete vytlačiť všetky údaje prichádzajúcich faxov.
Remember User ID (Zapamätať si ID používateľa)	Vyberte túto možnosť, ak chcete uložiť vaše ID používateľa.
LDAP Server Address (Adresa servera LDAP)	Zadajte adresu IP alebo názvu servera (napríklad: ldap.príklad.com) servera LDAP.
SSL/TLS	Zvoľte možnosť **SSL/TLS** na použitie servera LDAP prostredníctvom SSL/TLS.
LDAP Server Port (Port servera LDAP)	Zadanie čísla portu servera LDAP.
LDAP Search Root (Koreňový adresár vyhľadávania LDAP)	Zadajte koreňový adresár vyhľadávania servera LDAP.
Attribute of Name (Search Key) (Atribút názvu (kľúč vyhľadávania))	Zadanie atribútu, ktorý chcete použiť ako kľúč vyhľadávania.
Get Mail Address (Získať poštovú adresu)	Túto možnosť zvoľte na získanie e-mailovej adresy prihláseného používateľa zo servera LDAP.
Get User's Home Directory (Získať domovský adresár používateľa)	Túto možnosť zvoľte na získanie domovského adresára, ako cieľového umiestnenia pre funkciu Skenovať na sieť.

9. Kliknite na položky **Submit (Odoslať)**.

Súvisiace informácie

- Použitie funkcie overovania LDAP

Prihláste sa, aby ste mohli zmeniť nastavenia zariadenia prostredníctvom ovládacieho panela zariadenia (overenie LDAP)

Keď je povolené overenie LDAP, ovládací panel zariadenia bude uzamknutý, kým na ovládacom paneli zariadenia nezadáte ID používateľa a heslo.

1. Na ovládacom paneli zariadenia zadajte vaše ID používateľa a heslo a prihláste sa.
2. Keď je overenie úspešné, ovládací panel zariadenia sa odomkne.

Súvisiace informácie

- Použitie funkcie overovania LDAP

Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Funkcia Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0) zvyšuje zabezpečenie obmedzením funkcií dostupných vo vašom zariadení.

Pred použitím funkcie Secure Function Lock 3.0

Funkciu Secure Function Lock môžete používať na konfigurovanie hesiel, nastavenie limitov počtu strán pre konkrétnych používateľov a udelenie prístupu k niektorým alebo všetkým funkciám uvedeným v tomto zozname.

Pomocou Ovládania cez webové rozhranie môžete nakonfigurovať a zmeniť nasledujúce nastavenia funkcie Secure Function Lock (Zabezpečené uzamknutie funkcií) 3.0:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

- **Print (Tlačiť)**
- **Copy (Kopírovať)**
- **Scan (Skenovať)**
- **Fax**
- **Media (Médium)**
- **Web Connect**
- **Apps (Aplikácie)**
- **Page Limits (Limit strán)**
- **Page Counters (Počítadlo strán)**
- **Card ID (NFC ID) (ID karty (NFC ID))**

Modely s dotykovým displejom LCD:

Keď je zapnutá funkcia Secure Function Lock (Zabezpečené uzamknutie funkcií), zariadenie automaticky prejde do verejného režimu a niektoré funkcie zariadenia sa obmedzia len na authorized používateľov. Ak chcete získať prístup k vyhradeným funkciám zariadenia, stlačte možnosť , zvoľte svoje používateľské meno a zadajte heslo.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Konfigurovanie funkcie Secure Function Lock 3.0 pomocou aplikácie Web Based Management (Ovládanie cez webové rozhranie)

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **User Restriction Function (Funkcia používateľských obmedzení)** alebo **Restriction Management (Správa obmedzení)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. Vyberte **Secure Function Lock (Zabezpečené uzamknutie funkcií)**.
6. Kliknite na položky **Submit (Odoslať)**.
7. Kliknite na ponuku **Restricted Functions (Obmedzené funkcie)**.
8. Nakonfigurujte nastavenia, aby ste mohli spravovať obmedzenia používateľov alebo skupín.
9. Kliknite na položky **Submit (Odoslať)**.
10. Kliknite na ponuku **User List (Zoznam používateľov)**.
11. Nakonfigurujte zoznam používateľov.
12. Kliknite na položky **Submit (Odoslať)**.

V ponuke **Secure Function Lock (Zabezpečené uzamknutie funkcií)** môžete zmeniť aj nastavenia uzamknutia zoznamu používateľov.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Skenovanie pomocou funkcie Secure Function Lock 3.0

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

Nastavenie obmedzení skenovania (pre správcov)

Funkcia Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0) umožňuje správcovi obmedziť používateľov, ktorí môžu skenovať. Ak je v nastavení pre verejných používateľov funkcia Skenovanie nastavená na možnosť Vypnúť, skenovať budú môcť iba používatelia so začiarknutým políčkom na označenie **Scan (Skenovať)**.

Používanie funkcie skenovania (pre obmedzených používateľov)

- Skenovanie s použitím ovládacieho panela zariadenia:

  Obmedzení používatelia musia na ovládacom paneli zariadenia zadať svoje heslá, aby mohli získať prístup k režimu skenovania.
- Skenovanie z počítača:

  Obmedzení používatelia musia pred skenovaním z počítača zadať svoje heslá na ovládacom paneli zariadenia. Ak sa na ovládacom paneli zariadenia nezadá heslo, v počítači používateľa sa zobrazí chybové hlásenie.

Ak zariadenie podporuje overenie IC karty, používatelia s obmedzenými oprávneniami sa do režimu skenovania môžu dostať tak, že priložia registrované IC karty na symbol NFC na ovládacom paneli zariadenia.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Konfigurovanie verejného režimu pre funkciu Secure Function Lock 3.0

Pomocou obrazovky funkcie Secure Function Lock (Zabezpečené uzamknutie funkcií) môžete nastaviť verejný režim, ktorý obmedzuje funkcie dostupné pre verejných používateľov. Verejní používatelia nebudú musieť zadať heslo na získanie prístupu k funkciám sprístupneným prostredníctvom nastavení verejného režimu.

Verejný režim obsahuje tlačové úlohy odoslané cez Brother iPrint&Scan a Brother Mobile Connect.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **User Restriction Function (Funkcia používateľských obmedzení)** alebo **Restriction Management (Správa obmedzení)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Vyberte položku **Secure Function Lock (Zabezpečené uzamknutie funkcií)**.
6. Kliknite na položky **Submit (Odoslať)**.
7. Kliknite na ponuku **Restricted Functions (Obmedzené funkcie)**.
8. V riadku **Public Mode (Verejný režim)** povoľte uvedenú funkciu začiarknutím políčka na označenie alebo ju zakážte zrušením začiarknutia políčka na označenie.
9. Kliknite na položky **Submit (Odoslať)**.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Konfigurácia nastavení osobnej domovskej obrazovky pomocou ovládania cez webové rozhranie

Z pozície správcu môžete stanoviť, ktoré karty si používatelia môžu zobraziť na svojej osobnej domovskej obrazovke. Tieto karty poskytujú rýchly prístup k favorite skratkám používateľov, ktorí si ich môžu priradiť ku kartám svojej domovskej obrazovky z ovládacieho panela zariadenia.

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **User Restriction Function (Funkcia používateľských obmedzení)** alebo **Restriction Management (Správa obmedzení)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Vyberte **Secure Function Lock (Zabezpečené uzamknutie funkcií)**.
6. V poli **Tab Settings (Nastavenia kariet)** vyberte **Personal (Osobné)** pri názvoch kariet, ktoré chcete použiť na svojej osobnej domovskej obrazovke.
7. Kliknite na položky **Submit (Odoslať)**.
8. Kliknite na ponuku **Restricted Functions (Obmedzené funkcie)**.
9. Nakonfigurujte nastavenia, aby ste mohli spravovať obmedzenia používateľov alebo skupín.
10. Kliknite na položky **Submit (Odoslať)**.
11. Kliknite na ponuku **User List (Zoznam používateľov)**.
12. Nakonfigurujte zoznam používateľov.
13. V rozbaľovacom zozname zvoľte pre každého používateľa **User List / Restricted Functions (Zoznam používateľov/obmedzené funkcie)**.
14. V rozbaľovacom zozname **Home Screen (Domovska obrazovka)** zvoľte názov karty pre každého používateľa.
15. Kliknite na položky **Submit (Odoslať)**.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Ďalšie funkcie Secure Function Lock 3.0

Na obrazovke funkcie Secure Function Lock nakonfigurujte nasledujúce funkcie:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

All Counter Reset (Vynulovanie všetkých počítadiel)

Kliknutím na položku **All Counter Reset (Vynulovanie všetkých počítadiel)** v stĺpci **Page Counters (Počítadlo strán)** vynulujete počítadlo strán.

Export to CSV file (Exportovať do súboru CSV)

Kliknutím na **Export to CSV file (Exportovať do súboru CSV)**vyexportujte aktuálne a posledné počítadlo strán vrátane informácií **User List / Restricted Functions (Zoznam používateľov/obmedzené funkcie)** vo formáte súboru CSV.

Card ID (NFC ID) (ID karty (NFC ID))

Kliknite na ponuku **User List (Zoznam používateľov)** a potom do poľa **Card ID (NFC ID) (ID karty (NFC ID))** zadajte ID karty používateľa. Na overenie môžete použiť svoju IC kartu.

Output (Výstup)

Ak je na zariadení nainštalovaná výstupná schránka, z rozbaľovacieho zoznamu vyberte výstupný zásobník pre každého používateľa.

Last Counter Record (Posledný záznam počítadla)

Kliknite na položku **Last Counter Record (Posledný záznam počítadla)**, ak chcete, aby si zariadenie po vynulovaní počítadla zachovalo počet strán.

Counter Auto Reset (Automatické vynulovanie počítadla)

Kliknite na položku **Counter Auto Reset (Automatické vynulovanie počítadla)**, ak chcete nakonfigurovať časový interval medzi vynulovaniami počítadla strán. Vyberte denný, týždenný alebo mesačný interval.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Registrácia novej IC karty pomocou ovládacieho panela zariadenia

Karty integrovaných obvodov (karty IC) môžete zaregistrovať v zariadení.

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

1. Dotknite sa symbolu Near-Field Communication (NFC) na ovládacom paneli zariadenia zaregistrovanou IC kartou (Integrated Circuit Card).
2. Stlačte položku ID používateľa na LCD.
3. Stlačte tlačidlo registrácie karty.
4. Dotknite sa novou IC kartou symbolu NFC.

   Číslo novej IC karty sa potom zaregistruje v zariadení.
5. Stlačte tlačidlo OK.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Registrácia externej čítačky IC kariet

Keď pripojíte externú čítačku IC kariet (Integrated Circuit), použite aplikáciu Web Based Management (Ovládanie cez webové rozhranie) na zaregistrovanie čítačky kariet. Vaše zariadenie podporuje externé čítačky IC kariet podporované ovládačom triedy HID.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **External Card Reader (Externá čítačka kariet)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.

5. Zadajte potrebné informácie a následne kliknite na možnosť **Submit (Odoslať)**.
6. Reštartovaním zariadenia Brother aktivujte konfiguráciu.
7. K zariadeniu pripojte čítačku kariet.
8. Pri používaní overenia karty priložte kartu k čítačke kariet.

Súvisiace informácie

- Použitie funkcie Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií 3.0)

Zabezpečené odosielanie alebo príjem e-mailov

- Konfigurovanie odosielania alebo príjmu e-mailov pomocou aplikácie Ovládanie cez webové rozhranie
- Odoslanie e-mailu s overením používateľa
- Zabezpečené odosielanie alebo príjem e-mailov pomocou protokolu SSL/TLS

Konfigurovanie odosielania alebo príjmu e-mailov pomocou aplikácie Ovládanie cez webové rozhranie

- Prijímanie e-mailov je dostupné len pre určité modely.
- Na konfigurovanie zabezpečeného odosielania e-mailov s overením používateľa alebo odosielania a prijímania e-mailov pomocou protokolu SSL/TLS odporúčame používať ovládanie cez webové rozhranie (len podporované modely).

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

   Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.
4. Kliknite na **Network (Sieť)** > **Network (Sieť)** > **Protocol (Protokol)** na ľavom navigačnom paneli.

   Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ≡.
5. V poli **POP3/IMAP4/SMTP Client (Klient POP3/IMAP4/SMTP)** kliknite na **Advanced Settings (Rozšírené nastavenie)** a uistite sa, že stav položky **POP3/IMAP4/SMTP Client (Klient POP3/IMAP4/SMTP)** je **Enabled (Zapnuté)**.

   - Dostupné protokoly sa môžu líšiť v závislosti od vášho zariadenia.
   - Ak sa zobrazí obrazovka výberu **Authentication Method (Metóda overenia)**, vyberte svoju metódu overenia a postupujte podľa pokynov na displeji.
6. Nakonfigurujte nastavenia **POP3/IMAP4/SMTP Client (Klient POP3/IMAP4/SMTP)**.
   - Po konfigurovaní môžete skontrolujte správnosť nastavení e-mailu odoslaním skúšobného e-mailu.
   - Ak nepoznáte nastavenia servera POP3/IMAP4/SMTP, obráťte sa na správcu siete alebo poskytovateľa internetových služieb (ISP).
7. Po dokončení kliknite na **Submit (Odoslať)**.

   Zobrazí sa dialógové okno **Test Send/Receive E-mail Configuration (Test odoslania/prijatia e-mailovej konfigurácie)**.
8. Podľa pokynov v dialógovom okne otestujte aktuálne nastavenia.

Súvisiace informácie

- Zabezpečené odosielanie alebo príjem e-mailov

Súvisiace témy:

- Zabezpečené odosielanie alebo príjem e-mailov pomocou protokolu SSL/TLS

Odoslanie e-mailu s overením používateľa

Vaše zariadenie odosiela e-mailové správy cez e-mailový server, ktorý vyžaduje overenie používateľa. Táto metóda zabraňuje unauthorized používateľom pristupovať na e-mailový server.

Pomocou overenia používateľa môžete odosielať e-mailové notifikácie, e-mailové správy a I-Fax (dostupné len pre niektoré modely).

- Dostupné protokoly sa môžu líšiť v závislosti od vášho zariadenia.
- Na konfigurovanie overenia SMTP odporúčame používať ovládanie cez webové rozhranie.

Nastavenia e-mailového servera

Metódu overenia SMTP pre zariadenie musíte nakonfigurovať tak, aby sa zhodovala s metódou používanou vaším emailovým serverom. Podrobné informácie o nastaveniach emailového servera vám poskytne správca siete alebo poskytovateľ internetových služieb (ISP).

Ak chcete povoliť overovanie servera SMTP pomocou ovládania cez webové rozhranie, vyberte svoju metódu overenia v časti **Server Authentication Method (Spôsob overenia servera)** na obrazovke **POP3/IMAP4/SMTP Client (Klient POP3/IMAP4/SMTP)**.

Súvisiace informácie

- Zabezpečené odosielanie alebo príjem e-mailov

Zabezpečené odosielanie alebo príjem e-mailov pomocou protokolu SSL/TLS

Vaše zariadenie podporuje metódy komunikácie SSL/TLS. Ak chcete používať e-mailový server, ktorý používa komunikáciu SSL/TLS, musíte nakonfigurovať nasledujúce nastavenia.

- Prijímanie e-mailov je dostupné len pre určité modely.
- Na konfigurovanie protokolu SSL/TLS odporúčame používať ovládanie cez webové rozhranie.

Overenie certifikátu servera

Ak v položke **SSL/TLS** vyberiete možnosť **SSL** alebo **TLS**, automaticky sa začiarkne políčko na označenie **Verify Server Certificate (Overiť certifikát servera)**.

- Pred overením certifikátu servera je potrebné importovať certifikát certifikačnej autority vydaný certifikačnou autoritou, ktorá podpísala certifikát servera. U správcu siete alebo poskytovateľa internetových služieb (ISP) overte, či je importovanie certifikátu certifikačnej autority nevyhnutné.
- Ak nie je potrebné overiť certifikát servera, zrušte začiarknutie políčka na označenie **Verify Server Certificate (Overiť certifikát servera)**.

Číslo portu

Ak zvolíte možnosť **SSL** alebo **TLS**, hodnota **Port** sa zmení tak, aby zodpovedala protokolu. Ak chcete zmeniť číslo portu manuálne, po výbere nastavení **SSL/TLS** zadajte číslo portu.

Metódu komunikácie pre zariadenie musíte nakonfigurovať tak, aby sa zhodovala s metódou používanou vaším e-mailovým serverom. Podrobné informácie o nastaveniach e-mailového servera vám poskytne správca siete alebo poskytovateľ internetových služieb (ISP).

Vo väčšine prípadov si služby zabezpečeného webového e-mailu vyžadujú nasledujúce nastavenia:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

SMTP	**Port**	587
	Server Authentication Method (Spôsob overenia servera)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Súvisiace informácie

- Zabezpečené odosielanie alebo príjem e-mailov

Súvisiace témy:

- Konfigurovanie odosielania alebo príjmu e-mailov pomocou aplikácie Ovládanie cez webové rozhranie
- Konfigurovanie certifikátov zabezpečenia zariadenia

Ukladanie denníka tlače na sieti

- Prehľad uloženia tlačového denníka v sieti
- Konfigurovanie nastavení ukladania tlačového denníka na sieti pomocou služby Web Based Management (Ovládanie cez webové rozhranie)
- Použitie nastavenia zisťovania chýb funkcie ukladania tlačového denníka na sieti
- Používanie funkcie ukladania tlačového denníka na sieti s funkciou Secure Function Lock 3.0

Prehľad uloženia tlačového denníka v sieti

Funkcia uloženia tlačového denníka na sieti umožňuje uložiť súbor tlačového denníka z vášho zariadenia na sieťový server s použitím protokolu CIFS (Common Internet File System). Pre každú tlačovú úlohu môžete zaznamenať identifikáciu, typ tlačovej úlohy, názov úlohy, meno používateľa, dátum, čas a počet vytlačených strán. CIFS je protokol, ktorý beží nad TCP/IP a umožňuje počítačom v sieti zdieľať súbory cez intranet alebo internet.

Do tlačového denníka sa zaznamenávajú nasledujúce tlačové funkcie:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

- Tlačové úlohy z vášho počítača
- Tlač cez rozhranie USB Direct
- Kopírovanie
- Prijatý fax
- Tlač Web Connect

- Funkcia uloženia tlačového denníka na sieti podporuje overovanie Kerberos a overovanie NTLMv2. Pre správne fungovanie overovania musíte nakonfigurovať SNTP protokol (sieťový časový server), alebo správne nastaviť dátum, čas a časové pásmo na ovládacom paneli.
- Pri ukladaní súboru na server môžete nastaviť typ súboru na TXT alebo CSV.

Súvisiace informácie

- Ukladanie denníka tlače na sieti

Konfigurovanie nastavení ukladania tlačového denníka na sieti pomocou služby Web Based Management (Ovládanie cez webové rozhranie)

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **Store Print Log to Network (Uložiť denník tlače na sieť)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. V poli **Print Log (Záznam tlače)** kliknite na **On (Zapnutý)**.
6. Nakonfigurujte nasledujúce nastavenia:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

Možnosť	Popis
Network Folder Path (Cesta k sieťovému priečinku)	Zadajte cieľový priečinok na CIFS serveri, kde sa bude ukladať váš tlačový denník (napríklad: \\NázovPočítača\ZdieľanýPriečinok).
File Name (Názov súboru)	Zadajte názov súboru (v dĺžke maximálne 32 znakov), ktorý chcete používať ako tlačový denník.
File Type (Typ súboru)	Pre typ súboru tlačového denníka zvoľte možnosť **TXT** alebo **CSV**.
Time Source for Log (Časový zdroj pre denník)	Vyberte zdroj času pre tlačový denník.
Auth. Method (Metóda overenia)	Zvoľte metódu overenia, ktorá je potrebná pre prístup k CIFS serveru: **Auto (Automaticky)**, **Kerberos**, alebo **NTLMv2**. Kerberos je overovací protokol, ktorý umožňuje zariadeniam alebo osobám bezpečne overiť svoju identitu voči sieťovým serverom prostredníctvom jediného prihlásenia. NTLMv2 je metóda overenia, ktorú používa operačný systém Windows na prihlasovanie k serverom. • **Auto (Automaticky)**: ak vyberiete **Auto (Automaticky)**, v metóde overenia sa použije NTLMv2. • **Kerberos**: Na overenie len prostredníctvom protokolu Kerberos zvoľte možnosť **Kerberos**. • **NTLMv2**: Na overenie len prostredníctvom protokolu NTLMv2 zvoľte možnosť **NTLMv2**.

Možnosť	Popis
	• Pre overovanie s použitím protokolov **Kerberos** a **NTLMv2** musíte nakonfigurovať aj nastavenia **Date&Time (Dátum a čas)** alebo SNTP protokol (sieťový časový server) a DNS server. • Nastavenia dátumu a času môžete konfigurovať aj prostredníctvom ovládacieho panela zariadenia.
Username (Meno používateľa)	Zadajte meno používateľa pre overenie (s dĺžkou maximálne 96 znakov). Ak je meno používateľa súčasťou domény, meno používateľa zadajte jedným z nasledujúcich spôsobov: používateľ@doména alebo doména \používateľ.
Password (Heslo)	Zadajte heslo pre overenie (s dĺžkou maximálne 32 znakov).
Kerberos Server Address (Adresa servera Kerberos) (ak je potrebné)	Zadajte hostiteľskú adresu kľúčového distribučného centra (KDC) (napríklad: kerberos.priklad.com; maximálne 64 znakov) alebo adresu IP (napríklad: 192.168.56.189).
Error Detection Setting (Nastavenie zisťovania chýb)	Zvoľte úkon, ktorý sa má vykonať v prípade, že tlačový denník nie je možné uložiť na server z dôvodu chyby siete.

7. V poli **Connection Status (Stav pripojenia)** skontrolujte posledný zaznamenaný stav.

Stav chyby môžete skontrolovať aj na displeji LCD zariadenia.

8. Kliknutím na **Submit (Odoslať)** zobrazte stránku **Test Print Log to Network (Denník skúšobnej tlače na sieť)**.

   Ak chcete otestovať nastavenia, kliknite na **Yes (Áno)** a potom prejdite na ďalší krok.

   Ak chcete preskočiť test, kliknite na **No (Nie)**. Vaše nastavenia sa automaticky odošlú.

9. Zariadenie otestuje vaše nastavenia.
10. V prípade prijatia vašich nastavení sa na obrazovke zobrazí hlásenie **Test OK**.

    Ak sa zobrazí **Test Error (Test – chyba)**, skontrolujte všetky nastavenia a potom kliknutím na **Submit (Odoslať)** znova zobrazte skúšobnú stranu.

Súvisiace informácie

- Ukladanie denníka tlače na sieti

Použitie nastavenia zisťovania chýb funkcie ukladania tlačového denníka na sieti

Nastavenia zisťovania chýb použite na určenie úkonu, ktorý sa vykoná, keď tlačový denník nie je možné uložiť na serveri v dôsledku chyby siete.

1. Spustite webový prehľadávač.
2. Do panela s adresou v prehľadávači napíšte „https://adresa IP zariadenia“ (kde „adresa IP zariadenia“ je adresa IP vášho zariadenia).

   Napríklad:

   https://192.168.1.2

   Adresu IP zariadenia nájdete v prehľade konfigurácie siete.
3. Heslo v prípade potreby zadajte do poľa **Login (Prihlásenie)** a potom kliknite na tlačidlo **Login (Prihlásenie)**.

Predvolené heslo na spravovanie nastavení tohto zariadenia sa nachádza na jeho zadnej alebo spodnej časti a je označené nápisom „**Pwd**“. Predvolené heslo zmeňte pomocou pokynov na displeji pri prvom prihlásení.

4. Kliknite na **Administrator (Správca)** > **Store Print Log to Network (Uložiť denník tlače na sieť)** na ľavom navigačnom paneli.

Ak ľavý navigačný panel nie je viditeľný, začnite navigáciu z ☰.

5. V časti **Error Detection Setting (Nastavenie zisťovania chýb)** zvoľte možnosť **Cancel Print (Zrušiť tlač)** alebo **Ignore Log & Print (Ignorovať denník a tlačiť)**.

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

Možnosť	Popis
Cancel Print (Zrušiť tlač)	Ak zvolíte možnosť **Cancel Print (Zrušiť tlač)** a tlačový denník nie je možné uložiť na server, tlačové úlohy sa canceled. Aj keď zvolíte možnosť **Cancel Print (Zrušiť tlač)**, vaše zariadenie vytlačí prijatý fax.

Ignore Log & Print (Ignorovať denník a tlačiť)	Ak zvolíte možnosť **Ignore Log & Print (Ignorovať denník a tlačiť)**, zariadenie dokumentáciu vytlačí aj vtedy, ak tlačový denník nie je možné uložiť na server.
	Po obnovení funkcie uloženia tlačového denníka na sieti sa údaje do denníka zaznamenávajú nasledovne:
	`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. Ak tlačový denník nie je možné uložiť na konci tlače, nezaznamená sa počet vytlačených strán.
	b. Ak denník nie je možné uložiť na začiatku a konci tlačovej úlohy, tlačový denník danej tlačovej úlohy sa nezaznamená. Po obnovení funkcie sa chyba objaví v tlačovom denníku.

6. Kliknutím na **Submit (Odoslať)** zobrazte stránku **Test Print Log to Network (Denník skúšobnej tlače na sieť)**.

   Ak chcete otestovať nastavenia, kliknite na **Yes (Áno)** a potom prejdite na ďalší krok.

   Ak chcete preskočiť test, kliknite na **No (Nie)**. Vaše nastavenia sa automaticky odošlú.
7. Zariadenie otestuje vaše nastavenia.
8. V prípade prijatia vašich nastavení sa na obrazovke zobrazí hlásenie **Test OK**.

   Ak sa zobrazí **Test Error (Test – chyba)**, skontrolujte všetky nastavenia a potom kliknutím na **Submit (Odoslať)** znova zobrazte skúšobnú stranu.

Súvisiace informácie

- Ukladanie denníka tlače na sieti

Používanie funkcie ukladania tlačového denníka na sieti s funkciou Secure Function Lock 3.0

Keď je funkcia Secure Function Lock 3.0 (Zabezpečené uzamknutie funkcií) aktívna, do tlačového denníka ukladaného na sieti sa ukladajú mená používateľov, ktorí sú registrovaní pre používanie funkcií kopírovanie, Fax príjem, tlač Web Connect a priama tlač z USB. Keď je povolené overovanie Active Directory, do tlačového denníka ukladaného v sieti sa ukladajú mená používateľov:

Podporované funkcie, možnosti a nastavenia sa môžu líšiť v závislosti od modelu.

```
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
```

Súvisiace informácie

- Ukladanie denníka tlače na sieti

brother

Brother Earth

www.brotherearth.com

SVK
Verzia 0