Příručka bezpečnostními funkcemi

Důležité bezpečnostní informace

- Výchozí heslo ke správě nastavení přístroje je uvedeno na zadní straně přístroje a označeno jako „**Pwd:**“. Z důvodu ochrany přístroje před neoprávněným přístupem doporučujeme výchozí heslo ihned změnit.
- Při připojování přístroje k externí síti, například k internetu, zajistěte, aby bylo vaše síťové prostředí chráněno samostatnou bránou firewall nebo jinými prostředky, které zabrání úniku informací z důvodu nedostatečných nastavení nebo neoprávněnému přístupu škodlivými třetími stranami.
- Pokud je v okolí signál, bezdrátová místní síť LAN vám umožňuje volně navázat síťové připojení. Pokud ovšem nejsou správně nakonfigurována nastavení zabezpečení, může být signál zachycen nepřátelskými třetími stranami, což může mít za následek:
  - Krádež osobních nebo důvěrných údajů
  - Nevhodné přenášení údajů stranám, které se vydávají za určené osoby
  - Šíření přepsaného obsahu komunikace, která byla zachycena

Související informace

- Síť

Konfigurace certifikátů k zabezpečení zařízení

Musíte nakonfigurovat certifikát pro zabezpečenou správu síťového přístroje pomocí SSL/TLS. Ke konfiguraci certifikátu musíte použít aplikaci Web Based Management.

Přehled funkcí bezpečnostního certifikátu

Váš přístroj podporuje používání více bezpečnostních certifikátů, což umožňuje zabezpečené ověření a komunikaci s přístrojem. S tímto přístrojem lze používat následující funkce bezpečnostních certifikátů:

Podporované funkce, možnosti a nastavení se mohou lišit v závislosti na modelu.

- Komunikace SSL/TLS
- Ověření IEEE 802.1x
- IPsec

Váš přístroj podporuje následující:

- Předinstalovaný certifikát

  V tomto přístroji je předinstalovaný certifikát s automatickým podpisem. Tento certifikát umožňuje používat komunikaci SSL/TLS bez vytvoření nebo nainstalování jiného certifikátu.

Předinstalovaný vlastní certifikát chrání vaši komunikaci do určité úrovně. Pro lepší zabezpečení doporučujeme používat certifikát vydaný důvěryhodnou organizací.

- Certifikát s automatickým podpisem

  Tento tiskový server vydává svůj vlastní certifikát. Pomocí tohoto certifikátu můžete snadno použít komunikaci SSL/TLS bez vytvoření nebo instalování jiného certifikátu od CA.

- Certifikát od certifikačního orgánu (CA)

  Existují dvě metody instalace certifikátu od certifikačního orgánu. Pokud již máte certifikát od certifikačního orgánu nebo chcete použít certifikát od externího důvěryhodného certifikačního orgánu:

  - Při použití požadavku CSR (Požadavek na podepsání certifikátu) z tohoto tiskového serveru.
  - Při importu certifikátu a soukromého klíče.

- Certifikát CA (vydavatel certifikátů)

  Chcete-li použít certifikát CA, který identifikuje vydavatel certifikátu a má vlastní soukromý klíč, musíte importovat certifikát CA od certifikačního úřadu ještě před provedením konfigurace funkcí síťového zabezpečení.

- Pokud chcete používat komunikaci SSL/TLS, doporučujeme obrátit se nejdříve na správce systému.
- Pokud zresetujete tiskový server zpět na výchozí tovární nastavení, nainstalovaný certifikát a soukromý klíč se vymažou. Pokud chcete zachovat stejný certifikát a soukromý klíč i po zresetování tiskového serveru, nejprve je vyexportujte a potom je znovu nainstalujte.

Související informace

- Konfigurace certifikátů k zabezpečení zařízení

Související témata:

- Konfigurace ověřování IEEE 802.1x pro síť pomocí webové správy (webového prohlížeče)

Vytvoření a instalace certifikátu

Při volbě bezpečnostního certifikátu máte dvě možnosti: použít certifikát s automatickým podpisem nebo použít certifikát od certifikačního orgánu (CA).

Možnost 1

Vlastnoručně podepsaný certifikát

1. Vytvořte vlastnoručně podepsaný certifikát pomocí aplikace Web Based Management.
2. Nainstalujte certifikát s automatickým podpisem na počítač.

Možnost 2

Certifikát od certifikačního orgánu (CA)

1. Vytvořte žádost o podpis certifikátu (CSR) pomocí webové správy.
2. Nainstalujte certifikát vydaný certifikačním orgánem (CA) na přístroj Brother pomocí webové správy.
3. Nainstalujte certifikát na počítač.

Související informace

- Konfigurace certifikátů k zabezpečení zařízení

Vytvoření certifikátu s automatickým podpisem

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na tlačítko **Create Self-Signed Certificate (Vytvorit vlastnorucne podepsany certifikat)**.
6. Zadejte **Common Name (Spolecny nazev)** a **Valid Date (Datum platnosti)**.
   - Délka je **Common Name (Spolecny nazev)** menší než 64 bajtů. Zadejte identifikátor, jako je IP adresa, název uzlu nebo název domény, která se má použít při přístupu k tomuto přístroji prostřednictvím komunikace SSL/TLS. Název uzlu se zobrazí ve výchozím nastavení.
   - Pokud použijete protokol IPPS nebo HTTPS a zadáte jiný název v URL, **Common Name (Spolecny nazev)** než který byl použit pro certifikát s automatickým podpisem, zobrazí se varování.
7. Zvolte nastavení z rozevíracího seznamu **Public Key Algorithm (Algoritmus pro verejny klic)**.
8. Zvolte nastavení z rozevíracího seznamu **Digest Algorithm (Algoritmus Digest)**.
9. Klikněte na tlačítko **Submit (Odeslat)**.

Související informace

- Konfigurace certifikátů k zabezpečení zařízení

Vytvoření žádosti o podpis certifikátu (CSR) a provedení instalace certifikátu od certifikačního úřadu (CA)

Pokud již máte certifikát od externího důvěryhodného certifikačního orgánu (CA), můžete si certifikát a soukromý klíč uložit do přístroje a spravovat je prostřednictvím importu a exportu. Jestliže certifikát od externího důvěryhodného certifikačního orgánu nemáte, vytvořte žádost o podpis certifikátu (CSR), odešlete ji certifikačnímu orgánu k autorizaci a vrácený certifikát nainstalujte do přístroje.

- Vytvoření požadavku na podepsání certifikátů (CSR)
- Instalace certifikátu do přístroje

Vytvoření požadavku na podepsání certifikátů (CSR)

Požadavek na podepsání certifikátů (CSR) je požadavek zaslaný certifikační autoritě (CA) pro ověření údajů obsažených v certifikátu.

Před vytvořením CSR doporučujeme na počítač instalovat kořenový certifikát od certifikační autority.

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na tlačítko **Create CSR (Vytvorit CSR)**.
6. Zadejte **Common Name (Spolecny nazev)** (povinné) a přidejte další informace o vaší **Organization (Organizace)** (volitelné).

- Údaje o firmě jsou nutné proto, aby certifikační úřad mohl potvrdit identitu a dosvědčit ji uživateli z vnějšku.
- Délka **Common Name (Spolecny nazev)** musí být menší než 64 bajtů. Zadejte identifikátor, jako je IP adresa, název uzlu nebo název domény, která se má použít při přístupu k tomuto přístroji prostřednictvím komunikace SSL/TLS. Název uzlu se zobrazí ve výchozím nastavení. Je požadováno **Common Name (Spolecny nazev)**.
- Pokud zadáte jiný název v URL, než obecný název, který byl použit pro certifikát, objeví se varování.
- Položky **Organization (Organizace)**, **Organization Unit (Organizacni jednotka)**, **City/Locality (Mesto/oblast)** a **State/Province (Stat/provincie)** musí být menší než 64 bajtů.
- **Country/Region (Zeme/region)** by měl být dvoumístný kód země podle ISO 3166.
- Provádíte-li konfiguraci rozšíření certifikátu X.509v3, vyberte zaškrtávací políčko **Configure extended partition (Konfigurovat rozsireny oddil)** a potom zvolte **Auto (Register IPv4) (Auto (registrace IPv4))** nebo **Manual (Rucne)**.

7. Zvolte nastavení z rozevíracího seznamu **Public Key Algorithm (Algoritmus pro verejny klic)**.
8. Zvolte nastavení z rozevíracího seznamu **Digest Algorithm (Algoritmus Digest)**.
9. Klikněte na tlačítko **Submit (Odeslat)**.

   Na obrazovce se objeví požadavek CSR. Tento požadavek CSR uložte jako soubor nebo jej zkopírujte do online formuláře CSR, poskytnutého certifikační autoritou.
10. Klikněte na **Uložit**.

- Postupujte podle certifikačních zásad, pokud jde o metodu pro odeslání žádosti CSR certifikační autoritě.
- Pokud používáte podnikový kořen certifikačního úřadu Windows Server, doporučujeme při vytváření klientského certifikátu pro zabezpečenou správu jako šablonu certifikátu používat webový server. Pokud vytváříte klientský certifikát pro prostředí IEEE 802.1x s ověřováním EAP-TLS, doporučujeme používat pro šablonu certifikátu Uživatele.

Související informace

- Vytvoření žádosti o podpis certifikátu (CSR) a provedení instalace certifikátu od certifikačního úřadu (CA)

Instalace certifikátu do přístroje

Když obdržíte certifikát od certifikačního orgánu, postupujte podle níže uvedených kroků a nainstalujte jej na tiskový server:

Na váš přístroj lze nainstalovat pouze certifikát vystavený požadavkem o podepsání certifikátu (CSR) vašeho přístroje. Pokud chcete vytvořit jiný požadavek CSR, před vytvořením nového CSR se ujistěte, že je certifikát nainstalován. Další požadavek CSR vytvořte až po instalaci certifikátu do přístroje. V opačném případě bude požadavek CSR vytvořený před instalací nového CSR neplatný.

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na tlačítko **Install Certificate (Nainstalovat certifikat)**.
6. Vyhledejte soubor, který obsahuje certifikát vydaný certifikačním orgánem, a poté klikněte na **Submit (Odeslat)**.

   Certifikát je vytvořen a uložen do paměti přístroje.

Používáte-li komunikaci SSL/TLS, je na vašem počítači rovněž potřeba nainstalovat kořenový certifikát od certifikačního orgánu. Obraťte se na správce sítě.

Související informace

- Vytvoření žádosti o podpis certifikátu (CSR) a provedení instalace certifikátu od certifikačního úřadu (CA)

Import a export certifikátu a soukromého klíče

Certifikát a soukromý klíč můžete na přístroji uložit a spravovat pomocí importu a exportu.

- Import certifikátu a soukromého klíče
- Exportování certifikátu a soukromého klíče

Import certifikátu a soukromého klíče

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na tlačítko **Import Certificate and Private Key (Naimportovat certifikat a osobni klic)**.
6. Vyhledejte a vyberte soubor, který chcete importovat.
7. Je-li soubor šifrován, zadejte heslo a potom klikněte na **Submit (Odeslat)**.

Certifikát a soukromý klíč jsou úspěšně importovány do vašeho přístroje.

Související informace

- Import a export certifikátu a soukromého klíče

Exportování certifikátu a soukromého klíče

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na pole **Export** zobrazené s volbou **Certificate List (Seznam certifikatu)**.
6. Zadejte heslo, pokud chcete soubor zašifrovat.

   Pokud heslo není zadáno, výstup není zašifrován.
7. Zadejte znovu heslo pro potvrzení a klikněte na tlačítko **Submit (Odeslat)**.
8. Klikněte na **Uložit**.

Certifikát a soukromý klíč se exportuje do vašeho počítače.

Do svého počítače také můžete importovat certifikát.

Související informace

- Import a export certifikátu a soukromého klíče

Importování a exportování certifikátu CA

Na přístroji Brother lze importovat, exportovat a ukládat certifikáty CA.

- Importování certifikátu CA
- Exportování certifikátu CA

Importování certifikátu CA

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **CA Certificate (Certifikat CA)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Klikněte na **Import CA Certificate (Importovat certifikat CA)**.
6. Přejděte k souboru, který chcete importovat.
7. Klikněte na tlačítko **Submit (Odeslat)**.

Související informace

- Importování a exportování certifikátu CA

Exportování certifikátu CA

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **CA Certificate (Certifikat CA)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Vyberte certifikát, který chcete exportovat, a klikněte na tlačítko **Export**.
6. Klikněte na tlačítko **Submit (Odeslat)**.

Související informace

- Importování a exportování certifikátu CA

Používání SSL/TLS

- Zabezpečená správa síťového zařízení pomocí SSL/TLS
- Zabezpečený tisk dokumentů pomocí SSL/TLS
- Bezpečné odeslání nebo přijetí e-mailu pomocí SSL/TLS

Zabezpečená správa síťového zařízení pomocí SSL/TLS

- Konfigurace certifikátu pro SSL/TLS a dostupné protokoly
- Přístup k webové správě pomocí SSL/TLS
- Instalace certifikátu s automatickým podpisem pro uživatele systému Windows jako správce
- Konfigurace certifikátů k zabezpečení zařízení

Konfigurace certifikátu pro SSL/TLS a dostupné protokoly

Před používáním komunikace SSL/TLS nakonfigurujte certifikát ve svém přístroji pomocí webové správy.

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

   Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.
4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Network (Sit)** > **Protocol (Protokol)**.

   Pokud levý navigační panel není zobrazen, začněte procházet z ☰.
5. Klikněte na **HTTP Server Settings (Nastaveni serveru HTTP)**.
6. Vyberte certifikát, který chcete konfigurovat z rozevíracího seznamu **Select the Certificate (Vybrat certifikat)**.
7. Klikněte na **Submit (Odeslat)**.
8. Klepnutím na **Yes (Ano)** restartujete tiskový server.

Související informace

- Zabezpečená správa síťového zařízení pomocí SSL/TLS

Související témata:

- Zabezpečený tisk dokumentů pomocí SSL/TLS

Přístup k webové správě pomocí SSL/TLS

Pro zabezpečenou správu síťového přístroje musíte použít nástroje s protokoly zabezpečení.

- Aby bylo možné používat protokol HTTPS, musí být ve vašem přístroji povolen. Protokol HTTPS je povolen ve výchozím nastavení.
- Nastavení protokolu HTTPS můžete změnit na obrazovce webové správy.

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Nyní máte přístup k přístroji prostřednictvím HTTPS.

Související informace

- Zabezpečená správa síťového zařízení pomocí SSL/TLS

Instalace certifikátu s automatickým podpisem pro uživatele systému Windows jako správce

- Následující postup je určený pro prohlížeč Microsoft Edge. Pokud používáte jiný webový prohlížeč, vyhledejte si pokyny k instalaci certifikátů v jeho dokumentaci nebo online nápovědě.
- Certifikát s automatickým podpisem si vytvořte pomocí webové správy.

1. Klikněte pravým tlačítkem na ikonu **Microsoft Edge** a potom klikněte na možnost **Spustit jako správce**.

   Pokud se objeví obrazovka **Řízení uživatelských účtů**, klikněte na **Ano**.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Pokud vaše připojení není soukromé, klikněte na tlačítko **Upřesnit** a poté přejděte na webovou stránku.
4. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

   Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.
5. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Security (Zabezpeceni)** > **Certificate (Certifikat)**.

   Pokud levý navigační panel není zobrazen, začněte procházet z ☰.
6. Klikněte na **Export**.
7. Pokud výstupní soubor chcete šifrovat, zadejte do pole **Enter password (Zadejte heslo)** heslo. Zůstane-li políčko **Enter password (Zadejte heslo)** prázdné, výstupní soubor nebude zašifrován.
8. Zadejte heslo znovu do pole **Retype password (Znovu zadejte heslo)** a klikněte na **Submit (Odeslat)**.
9. Klikněte na stažený soubor, čímž jej otevřete.
10. Když se zobrazí **Průvodce importem certifikátu**, klikněte na **Další**.
11. Klikněte na tlačítko **Další**.
12. Pokud k tomu budete vyzváni, zadejte heslo, a poté klikněte na možnost **Další**.
13. Vyberte možnost **Všechny certifikáty umístit v následujícím úložišti** a poté **Procházet...**.
14. Vyberte možnost **Důvěryhodné kořenové certifikační autority** a poté klikněte na tlačítko **OK**.
15. Klikněte na tlačítko **Další**.
16. Klikněte na tlačítko **Dokončit**.
17. Klikněte na **Ano**, je-li otisk (kryptografický otisk) správné.
18. Klikněte na tlačítko **OK**.

Související informace

- Zabezpečená správa síťového zařízení pomocí SSL/TLS

Zabezpečený tisk dokumentů pomocí SSL/TLS

Tisk dokumentů pomocí IPPS

Chcete-li provést zabezpečený tisk dokumentů s protokolem IPP, použijte protokol IPPS.

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Network (Sit)** > **Protocol (Protokol)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Ujistěte se, že je zaškrtnuto políčko **IPP**.

Není-li políčko **IPP** zaškrtnuto, zvolte políčko **IPP** a poté klikněte na tlačítko **Submit (Odeslat)**.

Restartováním přístroje aktivujte konfiguraci.

Po restartování přístroje se vraťte na jeho webovou stránku, zadejte heslo a na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Network (Sit)** > **Protocol (Protokol)**.

6. Klikněte na tlačítko **HTTP Server Settings (Nastaveni serveru HTTP)**.
7. V oblasti **IPP** zaškrtněte políčko **HTTPS** a poté klikněte na možnost **Submit (Odeslat)**.
8. Restartováním přístroje aktivujte konfiguraci.

Komunikace pomocí IPPS nemůže zabránit neoprávněnému přístupu k tiskovému serveru.

Související informace

- Zabezpečený tisk dokumentů pomocí SSL/TLS

Používání SNMPv3

- Zabezpečená správa síťového přístroje pomocí SNMPv3

Zabezpečená správa síťového přístroje pomocí SNMPv3

Protokol Simple Network Management Protocol verze 3 (SNMPv3) poskytuje ověření uživatele a šifrování dat za účelem zabezpečené správy síťových zařízení.

1. Spusťte webový prohlížeč.
2. Zadejte do adresového řádku prohlížeče „https://obvyklý název“ (kde „obvyklý název“ je obvyklý název, který jste přiřadili k certifikátu, mohlo by se jednat o IP adresu, název uzlu nebo název domény).
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)** > **Network (Sit)** > **Protocol (Protokol)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Ujistěte se, zda je povoleno nastavení **SNMP**, a potom klikněte na **Advanced Settings (Pokrocila nastaveni)**.
6. Proveďte nastavení režimu SNMPv1/v2c.

Možnost	Popis
SNMP v1/v2c read-write access (Cteni/zapis SNMP v1/v2c)	Tiskový server používá verzi 1 a 2c protokolu SNMP. V tomto režimu můžete používat všechny aplikace přístroje. Není to však bezpečné, protože nedojde k ověření uživatele a data nebudou zašifrována.
SNMP v1/v2c read-only access (Přístup SNMP v1/v2c pouze pro čtení)	Tiskový server používá přístup pouze pro čtení prostřednictvím protokolu SNMP verzí 1 a 2c.
Disabled (Zakazano)	Protokol SNMP verze 1 a 2c zakažte. Všechny aplikace, které používají protokol SNMP v1/v2c, budou zakázány. Chcete-li povolit aplikace používající SNMPv1/v2c, použijte režim **SNMP v1/v2c read-only access (Přístup SNMP v1/v2c pouze pro čtení)** nebo **SNMP v1/v2c read-write access (Cteni/zapis SNMP v1/v2c)**.

7. Proveďte nastavení režimu SNMPv3.

Možnost	Popis
Enabled (Povoleno)	Tiskový server používá verzi 3 protokolu SNMP. Aby bylo možné zabezpečeně spravovat tiskový server, použijte režim SNMPv3 a potom nakonfigurujte nastavení.
Disabled (Zakazano)	Protokol SNMP verze 3 zakažte. Všechny aplikace, které používají protokol SNMPv3, budou zakázány. Chcete-li aplikace používající protokol SNMPv3 povolit, použijte režim SNMPv3.

8. Klikněte na **Submit (Odeslat)**.

Pokud přístroj zobrazí volby nastavení protokolu, vyberte požadované volby.

9. Restartováním přístroje aktivujte konfiguraci.

Související informace

- Používání SNMPv3

Používání ověření IEEE 802.1x pro vaši síť

Co je ověřování IEEE 802.1x?

IEEE 802.1x je standard IEEE, který omezuje přístup z neověřených síťových zařízení. Přístroj Brother odesílá požadavek na ověření serveru RADIUS (server ověření) prostřednictvím přístupového bodu nebo rozbočovače. Poté, co byl váš požadavek ověřen serverem RADIUS, bude mít váš přístroj přístup k síti.

Související informace

- Používání ověření IEEE 802.1x pro vaši síť

Konfigurace ověřování IEEE 802.1x pro síť pomocí webové správy (webového prohlížeče)

- Konfigurujete-li váš přístroj pomocí ověřování EAP-TLS, musíte před zahájením konfigurace nainstalovat certifikát klienta vydaný CA. Požádejte správce sítě o certifikát klienta. Pokud jste nainstalovali více certifikátů, doporučujeme si zapsat název certifikátu, který chcete používat.
- Před ověřením certifikátu serveru musíte naimportovat certifikát CA vydaný certifikačním orgánem, který podepsal certifikát serveru. Požádejte vašeho správce sítě, případně poskytovatele internetových služeb (ISP) o potvrzení, zda je nezbytné importovat certifikát CA.

Můžete rovněž nakonfigurovat ověření IEEE 802.1x pomocí průvodce nastavením bezdrátového připojení z ovládacího panelu (Bezdrátová síť).

1. Spusťte webový prohlížeč.
2. Zadejte „https://IP adresa přístroje“ do řádku s adresou prohlížeče (kde místo části „IP adresa přístroje“ zadáte IP adresu svého přístroje).

   Například:

   https://192.168.1.2

   IP adresa vašeho přístroje je uvedena ve Zprávě s konfigurací sítě.
3. Podle potřeby zadejte heslo do pole **Login (Prihlasit)** a potom klikněte na **Login (Prihlasit)**.

Výchozí heslo ke správě nastavení tohoto přístroje je uvedeno na zadní nebo spodní straně přístroje a označeno jako „**Pwd**“. Při prvním přihlášení změňte výchozí heslo podle pokynů na obrazovce.

4. Na levém navigačním panelu klikněte na volbu **Network (Sit)**.

Pokud levý navigační panel není zobrazen, začněte procházet z ☰.

5. Postupujte jedním z následujících způsobů:
   - Pro drátovou síť

     Klikněte na **Wired (Dratova)** > **Wired 802.1x Authentication (Overovani 802.1x (dratove))**.
   - Pro bezdrátovou síť

     Klikněte na **Wireless (Bezdratova)** > **Wireless (Enterprise) (Bezdratove (firemni))**.
6. Konfigurace nastavení ověření IEEE 802.1x.

- Chcete-li povolit ověřování IEEE 802.1x pro drátovou síť, vyberte volbu **Enabled (Aktivováno)** u položky **Wired 802.1x status (Stav dratove site 802.1x)** na stránce **Wired 802.1x Authentication (Overovani 802.1x (dratove))**.
- Pokud používáte ověření **EAP-TLS**, musíte z rozevíracího seznamu **Client Certificate (Certifikat klienta)** zvolit pro ověření nainstalovaný klientský certifikát (zobrazí se název certifikátu).
- Zvolíte-li autentizaci **EAP-FAST**, **PEAP**, **EAP-TTLS** nebo **EAP-TLS**, vyberte metodu ověřování z rozevíracího seznamu **Server Certificate Verification (Overovani certifikatu serveru)**. Certifikát serveru ověřte pomocí certifikátu CA, importovaného do přístroje předem a vydaného certifikačním orgánem, který podepsal certifikát serveru.

Můžete vybrat jednu z následujících metod ověření z rozevíracího seznamu **Server Certificate Verification (Overovani certifikatu serveru)**:

Možnost	Popis
No Verification (Bez overeni)	Certifikát serveru je vždy důvěryhodný. Ověřování se neprovádí.

Možnost	Popis
CA Cert. (Certifikat CA)	Metoda ověření spolehlivosti certifikační autority, která vydala certifikát serveru, pomocí certifikátu CA vydaného certifikační autoritou, která podepsala certifikát serveru.
CA Cert. + ServerID (Certifikat CA + ServerID)	Metoda ověření za účelem kontroly obecného názvu [1] certifikátu serveru, kromě CA spolehlivosti certifikátu serveru.

7. Po dokončení konfigurace klikněte na **Submit (Odeslat)**.

   U drátových sítí: Po konfiguraci připojte přístroj k síti podporované IEEE 802.1x. Po několika minutách vytiskněte Zprávu o konfiguraci sítě, abyste zkontrolovali stav <**Wired IEEE 802.1x**>.

Možnost	Popis
Success	Funkce IEEE 802.1x v drátové síti je povolena a ověření proběhlo úspěšně.
Failed	Funkce IEEE 802.1x v drátové síti je povolena, ověření však neproběhlo úspěšně.
Off	Funkce IEEE 802.1x v drátové síti není k dispozici.

Související informace

- Používání ověření IEEE 802.1x pro vaši síť

Související témata:

- Přehled funkcí bezpečnostního certifikátu
- Konfigurace certifikátů k zabezpečení zařízení

1 Ověření obecného názvu porovnává obecný název certifikátu serveru se znakovým řetězcem nakonfigurovaným pro **Server ID (ID serveru)**. Než začnete používat tuto metodu, obraťte se na správce systému ohledně obecného jména certifikátu serveru a potom kromě spolehlivosti CA certifikátu serveru nakonfigurujte hodnotu **Server ID (ID serveru)**.

Metody ověřování IEEE 802.1x

EAP-FAST

Protokol Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) byl vyvinut společností Cisco Systems, Inc. a používá k ověření uživatelské jméno a heslo a symetrický algoritmus klíče, čímž dosahuje tunelového ověření.

Přístroj Brother podporuje následující metody vnitřního ověření:

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

EAP-MD5 (drátová síť)

EAP-MD5 (Extensible Authentication Protocol-Message digest algorithm 5) využívá k ověření ID uživatele a heslo.

PEAP

Protokol Protected Extensible Authentication Protocol (PEAP) je verzí metody EAP, vytvořené společnostmi Cisco Systems, Inc., Microsoft Corporation a RSA Security. Protokol PEAP vytvoří šifrovaný SSL (Secure Sockets Layer)/TLS (zabezpečení transportní vrstvy) tunel mezi klientem a ověřovacím serverem a zašle uživateli jeho ID a heslo. PEAP poskytuje oboustranné ověření mezi serverem a klientem.

Přístroj Brother podporuje následující metody vnitřního ověření:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) byl vyvinut společnostmi Funk Software a Certicom. EAP-TTLS vytváří mezi klientem a ověřovacím serverem pro zaslání hesla a ID uživatele podobný šifrovaný tunel SSL jako PEAP. EAP-TTLS poskytuje oboustranné ověření mezi serverem a klientem.

Přístroj Brother podporuje následující metody vnitřního ověření:

- 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 ověření digitálního certifikátu klientem i ověřovacím serverem.

Související informace

- Používání ověření IEEE 802.1x pro vaši síť