Przewodnik po funkcjach zabezpieczeń

Ważne informacje dotyczące bezpieczeństwa

- Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się na spodzie urządzenia i jest oznaczone napisem „**Pwd:**”. Zalecamy niezwłoczną zmianę domyślnego hasła w celu ochrony urządzenia przed nieupoważnionym dostępem.
- Podczas podłączania urządzenia do sieci zewnętrznej, np. do Internetu, upewnij się, że środowisko sieciowe jest chronione osobną zaporą lub innymi środkami, aby zapobiec wyciekowi informacji z powodu nieodpowiednich ustawień lub nieupoważnionego dostępu ze strony innych podmiotów o złych zamiarach.
- Jeśli w okolicy jest dostępny sygnał, bezprzewodowa sieć LAN umożliwia swobodne wykonywanie połączeń LAN. Jednak jeśli ustawienia bezpieczeństwa nie zostaną prawidłowo skonfigurowane, sygnał może zostać przechwycony przez inne podmioty o złych zamiarach, co może doprowadzić do:
  - kradzieży danych osobowych lub informacji poufnych,
  - niewłaściwego przekazywania informacji do podmiotów podszywających się pod określone osoby,
  - rozpowszechniania transkrypcji przechwyconych rozmów.

Powiązane informacje

- Sieć

Konfiguracja certyfikatów bezpieczeństwa urządzenia

Aby możliwe było bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS, należy skonfigurować certyfikat. Do skonfigurowania certyfikatu należy użyć funkcji Zarządzanie przez interfejs webowy.

Przegląd funkcji certyfikatów zabezpieczających

Urządzenie umożliwia korzystanie z wielu certyfikatów zabezpieczających, co umożliwia bezpieczne zarządzanie, uwierzytelnianie i komunikację z urządzeniem. Urządzenie umożliwia korzystanie z następujących funkcji certyfikatu zabezpieczającego:

Dostępne funkcje, opcje i ustawienia mogą się różnić w zależności od modelu.

- Komunikacja z użyciem protokołu SSL/TLS
- Uwierzytelnianie IEEE 802.1x
- IPsec

Twoje urządzenie obsługuje:

- Wstępnie zainstalowany certyfikat

  Urządzenie dysponuje wstępnie zainstalowanym samopodpisanym certyfikatem. Ten certyfikat umożliwia użycie protokołu SSL/TLS w komunikacji bez potrzeby tworzenia lub instalowania innego certyfikatu.

Wstępnie zainstalowany samopodpisany certyfikat stanowi do pewnego stopnia zabezpieczenie komunikacji. Aby zapewnić wyższy stopień bezpieczeństwa, zalecamy stosowanie certyfikatu wydanego przez zaufaną organizację.

- Certyfikat samopodpisany

  Ten serwer wydruku wystawia swój własny certyfikat. Ten certyfikat umożliwia użycie protokołu SSL/TLS w komunikacji bez potrzeby tworzenia lub instalowania innego certyfikatu z ośrodka certyfikacji.
- Certyfikat z ośrodka certyfikacji (CA)

  Istnieją dwie metody instalowania certyfikatu pochodzącego z CA. W przypadku posiadania certyfikatu pochodzącego z ośrodka certyfikacji lub w celu użycia certyfikatu pochodzącego z zewnętrznego, zaufanego ośrodka certyfikacji:
  - Użycie żądania podpisania certyfikatu (CSR) z tego serwera wydruku.
  - Importowanie certyfikatu i klucza prywatnego.
- Certyfikat ośrodka certyfikacji (CA)

  Aby użyć certyfikatu CA, który identyfikuje ośrodek certyfikacji i posiadany przez niego klucz prywatny, należy przed skonfigurowaniem funkcji zabezpieczeń w sieci zaimportować certyfikat CA z ośrodka certyfikacji.

- Jeśli planowane jest użycie protokołu SSL/TLS w komunikacji, zalecamy w pierwszej kolejności skontaktowanie się z administratorem systemu.
- Przywrócenie fabrycznych ustawień domyślnych serwera wydruku powoduje usunięcie zainstalowanego certyfikatu i klucza prywatnego. Aby zachować ten sam certyfikat i klucz prywatny po zresetowaniu serwera wydruku, należy je wyeksportować przed zresetowaniem, a następnie ponownie zainstalować.

Powiązane informacje

- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Powiązane tematy:

- Konfigurowanie uwierzytelniania IEEE 802.1x dla sieci przy użyciu funkcji zarządzania przez interfejs webowy (przeglądarkę internetową)

Jak utworzyć i zainstalować certyfikat

Przy wyborze certyfikatu zabezpieczeń dostępne są dwie opcje: można użyć samodzielnie podpisanego certyfikatu lub certyfikatu wystawionego przez urząd certyfikacji.

Opcja 1

Certyfikat podpisany samodzielnie

1. Utwórz samodzielnie podpisany certyfikat przy użyciu funkcji Zarządzanie przez interfejs webowy.
2. Zainstaluj samodzielnie podpisany certyfikat na komputerze.

Opcja 2

Certyfikat wydany przez urząd certyfikacji

1. Utwórz żądanie podpisania certyfikatu (CSR) za pomocą narzędzia Zarządzanie przez interfejs webowy.
2. Zainstaluj certyfikat wydany przez urząd certyfikacji (CA) w urządzeniu Brother przy użyciu funkcji Zarządzanie przez interfejs webowy.
3. Zainstaluj certyfikat na komputerze.

Powiązane informacje

- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Tworzenie certyfikatu podpisanego samodzielnie

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.

5. Kliknij przycisk **Create Self-Signed Certificate (Utwórz certyfikat z własnym podpisem)**.
6. Wprowadź informacje w polach **Common Name (Nazwa pospolita)** i **Valid Date (Data ważności)**.
   - Długość tekstu w polu **Common Name (Nazwa pospolita)** jest mniejsza niż 64 bajty. Wprowadź identyfikator, taki jak adres IP, nazwa węzła lub nazwa domeny, używany w celu uzyskania dostępu do urządzenia za pośrednictwem komunikacji z wykorzystaniem protokołu SSL/TLS. Domyślnie wyświetlana jest nazwa węzła.
   - W przypadku korzystania z komunikacji z wykorzystaniem protokołu IPPS lub HTTPS i wprowadzenia w polu adresu URL innej nazwy niż w używanej przez samodzielnie podpisany certyfikat w polu **Common Name (Nazwa pospolita)** zostanie wyświetlone okno ostrzeżenia.
7. Wybierz ustawienie z listy rozwijanej **Public Key Algorithm (Algorytm klucza publicznego)**.
8. Wybierz ustawienie z listy rozwijanej **Digest Algorithm (Algorytm skrótu)**.
9. Kliknij przycisk **Submit (Prześlij)**.

Powiązane informacje

- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Tworzenie żądania podpisania certyfikatu (Certificate Signing Request, CSR) i instalacja certyfikatu z urzędu certyfikacji (CA)

Jeśli posiadasz już certyfikat z zaufanego, zewnętrznego urzędu certyfikacji (CA), możesz zapisać certyfikat i klucz prywatny na urządzeniu i zarządzać nimi poprzez importowanie i eksportowanie. Jeżeli nie posiadasz certyfikatu z zaufanego zewnętrznego urzędu certyfikacji, utwórz żądanie podpisania certyfikatu (CSR), wyślij je do urzędu certyfikacji w celu uwierzytelnienia, a następnie zainstaluj odesłany certyfikat w urządzeniu.

- Tworzenie żądania podpisania certyfikatu (Certificate Signing Request, CSR)
- Instalowanie certyfikatu w urządzeniu

Tworzenie żądania podpisania certyfikatu (Certificate Signing Request, CSR)

Żądanie podpisania certyfikatu (Certificate Signing Request, CSR) to żądanie wysyłane do urzędu certyfikacji w celu uwierzytelnienia poświadczeń zawartych w certyfikacie.

Przed utworzeniem żądania CSR zalecamy zainstalowanie na komputerze certyfikatu głównego z urzędu certyfikacji.

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij przycisk **Create CSR (Utwórz CSR)**.
6. Wpisz **Common Name (Nazwa pospolita)** (wymagane) i dodaj inne informacje o **Organization (Organizacja)** (opcjonalne).

   - Wymagane jest podanie szczegółowych informacji na temat firmy, aby urząd certyfikacji mógł potwierdzić tożsamość użytkownika i poświadczyć jej prawdziwość przed podmiotem zewnętrznym.
   - Długość tekstu w polu **Common Name (Nazwa pospolita)** musi być mniejsza niż 64 bajty. Wprowadź identyfikator, taki jak adres IP, nazwa węzła lub nazwa domeny, używany w celu uzyskania dostępu do urządzenia za pośrednictwem komunikacji z wykorzystaniem protokołu SSL/TLS. Domyślnie wyświetlana jest nazwa węzła. Podanie informacji w polu **Common Name (Nazwa pospolita)** jest wymagane.
   - Wprowadzenie w polu adresu URL nazwy innej niż nazwa zwykła używana przez certyfikat spowoduje wyświetlenie okno wyskakującego z ostrzeżeniem.
   - Długość tekstu w polach **Organization (Organizacja)**, **Organization Unit (Jednostka organizacyjna)**, **City/Locality (Miasto/miejscowość)** i **State/Province (Województwo/stan)** musi być mniejsza niż 64 bajty.
   - Pozycję **Country/Region (Kraj/region)** powinien stanowić dwuliterowy kod kraju według normy ISO 3166.
   - W przypadku konfigurowania rozszerzenia certyfikatu X.509v3 zaznacz pole wyboru **Configure extended partition (Skonfiguruj partycję rozszerzoną)**, a następnie wybierz opcję **Auto (Register IPv4) (Auto (rejestr. IPv4))** lub **Manual (Ręczne)**.
7. Wybierz ustawienie z listy rozwijanej **Public Key Algorithm (Algorytm klucza publicznego)**.
8. Wybierz ustawienie z listy rozwijanej **Digest Algorithm (Algorytm skrótu)**.
9. Kliknij przycisk **Submit (Prześlij)**.

   CSR wyświetla się na ekranie. Zapisz CSR jako plik lub przeklej do formularza CSR online zapewnionego przez urząd certyfikacji.

10. Kliknij **Zapisz**.

- Należy postępować według zasad urzędu certyfikacji dotyczących przesyłania do niego informacji o uwierzytelnianiu po stronie klienta.
- W przypadku korzystania z opcji Główny urząd certyfikacji przedsiębiorstwa w systemie Windows Server podczas tworzenia certyfikatu klienckiego w celu bezpiecznego zarządzania zalecamy użycie serwera stron internetowych. W przypadku tworzenia certyfikatu klienckiego dla środowiska IEEE 802.1x z uwierzytelnianiem EAP-TLS zalecamy użycie użytkownika jako szablonu certyfikatu.

Powiązane informacje

- Tworzenie żądania podpisania certyfikatu (Certificate Signing Request, CSR) i instalacja certyfikatu z urzędu certyfikacji (CA)

Instalowanie certyfikatu w urządzeniu

Wykonaj poniższe kroki, aby zainstalować certyfikat na serwerze wydruku po otrzymaniu go z urzędu certyfikacji:

W urządzeniu można zainstalować tylko certyfikat wydany wraz z żądaniem podpisania certyfikatu (CSR) dla tego urządzenia. Aby utworzyć nowe żądanie CSR, należy się najpierw upewnić, że dany certyfikat jest zainstalowany. Utwórz kolejne żądanie CSR tylko po zainstalowaniu certyfikatu w urządzeniu, w przeciwnym razie żądanie CSR złożone przed zainstalowaniem nowego CSR będzie nieważne.

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij przycisk **Install Certificate (Zainstaluj certyfikat)**.
6. Wyszukaj plik zawierający certyfikat wystawiony przez urząd certyfikacji, a następnie kliknij **Submit (Prześlij)**.

   Certyfikat zostaje utworzony i zapisany w pamięci urządzenia.

Aby korzystać z komunikacji z zastosowaniem protokołu SSL/TLS, należy zainstalować na komputerze certyfikat główny z urzędu certyfikacji. Skontaktuj się z administratorem sieci.

Powiązane informacje

- Tworzenie żądania podpisania certyfikatu (Certificate Signing Request, CSR) i instalacja certyfikatu z urzędu certyfikacji (CA)

Importowanie i eksportowanie certyfikatu oraz klucza prywatnego

Zapisz certyfikat i prywatny klucz w urządzeniu i zarządzaj nimi poprzez importowanie i eksportowanie.

- Importowanie certyfikatu i klucza prywatnego
- Eksportowanie certyfikatu i klucza prywatnego

Importowanie certyfikatu i klucza prywatnego

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ≡.
5. Kliknij przycisk **Import Certificate and Private Key (Importuj certyfikat i klucz prywatny)**.
6. Przejdź do pliku, który ma zostać zaimportowany.
7. Jeżeli plik jest zaszyfrowany, wprowadź hasło, a następnie kliknij przycisk **Submit (Prześlij)**.

Certyfikat i klucz prywatny zostaną importowane do urządzenia.

Powiązane informacje

- Importowanie i eksportowanie certyfikatu oraz klucza prywatnego

Eksportowanie certyfikatu i klucza prywatnego

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij przycisk **Export (Eksportuj)** widoczny z **Certificate List (Lista certyfikatów)**.
6. Wprowadź hasło, jeżeli chcesz zaszyfrować plik.

   W przypadku niewpisania hasła plik nie zostanie zaszyfrowany.
7. Wprowadź ponownie hasło w celu potwierdzenia i kliknij przycisk **Submit (Prześlij)**.
8. Kliknij **Zapisz**.

Certyfikat i klucz prywatny zostały wyeksportowane na komputer.

Możesz również zaimportować certyfikat na swój komputer.

Powiązane informacje

- Importowanie i eksportowanie certyfikatu oraz klucza prywatnego

Importowanie i eksportowanie certyfikatu CA

Urządzenie Brother umożliwia importowanie, eksportowanie i zapisywanie certyfikatów CA.

- Importowanie certyfikatu CA
- Eksportowanie certyfikatu CA

Importowanie certyfikatu CA

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **CA Certificate (Certyfikat CA)**.

Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ≡.

5. Kliknij **Import CA Certificate (Importuj certyfikat urzędu certyfikacji)**.
6. Znajdź plik, który chcesz importować.
7. Kliknij przycisk **Submit (Prześlij)**.

Powiązane informacje

- Importowanie i eksportowanie certyfikatu CA

Eksportowanie certyfikatu CA

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **CA Certificate (Certyfikat CA)**.

Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.

5. Wybierz certyfikat, który ma zostać wyeksportowany, a następnie kliknij przycisk **Export (Eksportuj)**.
6. Kliknij przycisk **Submit (Prześlij)**.

Powiązane informacje

- Importowanie i eksportowanie certyfikatu CA

Używanie protokołu SSL/TLS

- Bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS
- Bezpieczne drukowanie dokumentów przy użyciu protokołu SSL/TLS
- Bezpieczne wysyłanie i odbieranie wiadomości e-mail z użyciem protokołu SSL/TLS

Bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS

Konfiguracja certyfikatu dla SSL/TLS i dostępnych protokołów

Skonfiguruj certyfikat urządzenia, używając funkcji Zarządzania przez interfejs webowy przed rozpoczęciem korzystania z komunikacji przez protokoły SSL/TLS.

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Network (Sieć)** > **Protocol (Protokół)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij **HTTP Server Settings (Ustawienia serwera HTTP)**.
6. Wybierz certyfikat, który chcesz skonfigurować, z listy rozwijanej **Select the Certificate (Wybierz certyfikat)**.
7. Kliknij **Submit (Prześlij)**.
8. Kliknij **Yes (Tak)**, aby uruchomić ponownie serwer druku.

Powiązane informacje

- Bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS

Powiązane tematy:

- Bezpieczne drukowanie dokumentów przy użyciu protokołu SSL/TLS

Dostęp do funkcji Zarządzanie przez interfejs webowy przez protokół SSL/TLS

W celu bezpiecznego zarządzania urządzeniem sieciowym należy używać programów narzędziowych do zarządzania razem z protokołami zabezpieczeń.

- Aby użyć protokołu HTTPS, w urządzeniu musi być włączona funkcja HTTPS. Domyślnie włączony jest protokół HTTPS.
- Można zmienić ustawienia protokołu HTTPS na ekranie Zarządzania przez interfejs webowy.

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Teraz można uzyskać dostęp do urządzenia za pomocą protokołu HTTPS.

Powiązane informacje

- Bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS

Instalowanie samodzielnie podpisanego certyfikatu dla użytkowników systemu Windows z uprawnieniami Administratora

- Poniższe kroki dotyczą programu Microsoft Edge. W przypadku korzystania z innej przeglądarki internetowej instrukcje dotyczące instalowania certyfikatów znajdują się w dokumentacji lub pomocy online przeglądarki.
- Upewnij się, że samodzielnie podpisany certyfikat został utworzony za pomocą funkcji Zarządzanie przez interfejs webowy.

1. Kliknij prawym przyciskiem myszy ikonę **Microsoft Edge**, a następnie kliknij **Uruchom jako administrator**.

   Jeśli wyświetlony zostanie ekran **Kontrola konta użytkownika**, kliknij **Tak**.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli połączenie nie jest prywatne, kliknij przycisk **Zaawansowane**, a następnie przejdź do witryny internetowej.
4. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
5. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Security (Bezpieczeństwo)** > **Certificate (Certyfikat)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
6. Kliknij **Export (Eksportuj)**.
7. Aby zaszyfrować wydrukowany plik, wpisz hasło w polu **Enter password (Wprowadź hasło)**. Jeśli pole **Enter password (Wprowadź hasło)** jest puste, plik wyjściowy nie zostanie zaszyfrowany.
8. Wprowadź ponownie hasło w polu **Retype password (Wpisz hasło pon.)**, a następnie kliknij przycisk **Submit (Prześlij)**.
9. Kliknij pobrany plik, aby go otworzyć.
10. Po wyświetleniu okna **Kreator importu certyfikatów** kliknij przycisk **Dalej**.
11. Kliknij przycisk **Dalej**.
12. W razie potrzeby wpisz hasło i kliknij **Dalej**.
13. Wybierz **Umieść wszystkie certyfikaty w następującym magazynie**, a następnie kliknij **Przeglądaj...**.
14. Wybierz **Zaufane główne urzędy certyfikacji**, a następnie kliknij przycisk **OK**.
15. Kliknij przycisk **Dalej**.
16. Kliknij przycisk **Zakończ**.
17. Kliknij przycisk **Tak**, jeżeli odcisk palca jest prawidłowy.
18. Kliknij przycisk **OK**.

Powiązane informacje

- Bezpieczne zarządzanie urządzeniem sieciowym przy użyciu protokołu SSL/TLS

Bezpieczne drukowanie dokumentów przy użyciu protokołu SSL/TLS

- Drukowanie dokumentów za pomocą IPP
- Konfiguracja certyfikatu dla SSL/TLS i dostępnych protokołów
- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Drukowanie dokumentów za pomocą IPP

W celu bezpiecznego wydrukowania dokumentów za pomocą protokołu IPP użyj protokołu IPPS.

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

   Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Network (Sieć)** > **Protocol (Protokół)**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Potwierdź, że zaznaczone jest pole wyboru **IPP**.

   Jeśli pole wyboru **IPP** nie jest zaznaczone, zaznacz pole wyboru **IPP**, a następnie kliknij **Submit (Prześlij)**.

   Uruchom ponownie urządzenie, aby aktywować konfigurację.

   Po ponownym uruchomieniu urządzenia wróć na stronę internetową urządzenia, wpisz hasło, a następnie na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Network (Sieć)** > **Protocol (Protokół)**.
6. Kliknij przycisk **HTTP Server Settings (Ustawienia serwera HTTP)**.
7. Zaznacz pole wyboru **HTTPS** w obszarze **IPP**, a następnie kliknij **Submit (Prześlij)**.
8. Uruchom ponownie urządzenie, aby aktywować konfigurację.

Komunikacja za pośrednictwem protokołu IPPS nie zapobiega nieuprawnionemu dostępowi do serwera druku.

Powiązane informacje

- Bezpieczne drukowanie dokumentów przy użyciu protokołu SSL/TLS

Używanie protokołu SNMPv3

- Bezpieczne zarządzanie urządzeniem sieciowym za pomocą SNMPv3

Bezpieczne zarządzanie urządzeniem sieciowym za pomocą SNMPv3

Protokół SNMPv3 (ang. Simple Network Management Protocol version 3) zapewnia uwierzytelnianie użytkowników i szyfrowanie danych umożliwiające bezpieczne zarządzanie urządzeniami sieciowymi.

1. Uruchom przeglądarkę internetową.
2. Wpisz w pasku adresowym przeglądarki „https://Nazwa własna” (gdzie „Nazwa własna” oznacza nazwę własną przypisaną do certyfikatu; może to być adres IP, nazwa węzła lub nazwa domeny).
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)** > **Network (Sieć)** > **Protocol (Protokół)**.

Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.

5. Sprawdź, czy włączone jest ustawienie **SNMP**, a następnie kliknij przycisk **Advanced Settings (Ustawienia zaawansowane)**.
6. Skonfiguruj ustawienia trybu SNMPv1/v2c.

Opcja	Opis
SNMP v1/v2c read-write access (SNMP v1/v2c — dostęp do odczytu i zapisu)	Serwer drukowania korzysta z wersji 1 i 2c protokołu SNMP. Korzystając z tego trybu, można używać wszystkich aplikacji urządzenia. Nie jest to jednak bezpieczne, ponieważ nie uwierzytelnia on użytkownika, a dane nie są szyfrowane.
SNMP v1/v2c read-only access (SNMP v1/v2c tylko do odczytu)	Serwer drukowania korzysta z wersji 1 i 2c protokołu SNMP funkcji dostępu w trybie tylko do odczytu.
Disabled (Wyłączone)	Wyłącz wersję 1 i 2c protokołu SNMP. Wszystkie aplikacje korzystające z SNMPv1/v2c zostaną ograniczone. Aby umożliwić działanie aplikacji korzystających z protokoły SNMPv1/v2c, należy użyć trybu **SNMP v1/v2c read-only access (SNMP v1/v2c tylko do odczytu)** lub **SNMP v1/v2c read-write access (SNMP v1/v2c — dostęp do odczytu i zapisu)**.

7. Skonfiguruj ustawienia trybu SNMPv3.

Opcja	Opis
Enabled (Włączone)	Serwer drukowania korzysta z wersji 3 protokołu SNMP. Aby bezpiecznie zarządzać serwerem drukowania, użyj protokołu trybu SNMPv3, a następnie skonfiguruj ustawienia.
Disabled (Wyłączone)	Wyłącz wersję 3 protokołu SNMP. Wszystkie aplikacje korzystające z SNMPv3 zostaną ograniczone. Aby umożliwić działanie aplikacji korzystających z protokołu SNMPv3, należy użyć trybu SNMPv3.

8. Kliknij **Submit (Prześlij)**.

Jeśli na urządzeniu wyświetlone zostaną opcje ustawień protokołu, wybierz żądane opcje.

9. Uruchom ponownie urządzenie, aby aktywować konfigurację.

Powiązane informacje

- Używanie protokołu SNMPv3

Stosowanie uwierzytelniania metodą IEEE 802.1x w sieci

Czym jest uwierzytelnianie IEEE 802.1x?

IEEE 802.1x to standard IEEE, który ogranicza dostęp z nieuprawnionych urządzeń sieciowych. Urządzenie Brother wysyła żądanie uwierzytelniania do serwera RADIUS (serwer uwierzytelniania) za pośrednictwem punktu dostępowego lub koncentratora. Po zweryfikowaniu żądania przez serwer RADIUS urządzenie może uzyskać dostęp do sieci.

Powiązane informacje

- Stosowanie uwierzytelniania metodą IEEE 802.1x w sieci

Konfigurowanie uwierzytelniania IEEE 802.1x dla sieci przy użyciu funkcji zarządzania przez interfejs webowy (przeglądarkę internetową)

- W przypadku konfiguracji urządzenia z wykorzystaniem uwierzytelniania EAP-TLS należy przed rozpoczęciem konfiguracji zainstalować certyfikat klienta wydany przez odpowiednią instytucję certyfikacyjną. Aby uzyskać certyfikat klienta, skontaktuj się z administratorem sieci. Jeśli został zainstalowany więcej niż jeden certyfikat, zalecamy zapisanie nazwy certyfikatu, który ma być używany.
- Przed zweryfikowaniem certyfikatu serwera należy zaimportować certyfikat CA wystawiony przez ośrodek certyfikacji, który podpisał certyfikat serwera. Skontaktuj się z administratorem sieci lub dostawcą usług internetowych (ISP), aby potwierdzić konieczność zaimportowania certyfikatu CA.

Można także zsynchronizować uwierzytelnianie IEEE 802.1x przy użyciu Kreatora bezprzewodowej konfiguracji z poziomu panelu sterowania (sieć bezprzewodowa).

1. Uruchom przeglądarkę internetową.
2. Wprowadź „https://adres IP urządzenia” w polu adresu przeglądarki (gdzie „adres IP urządzenia” jest adresem IP urządzenia).

   Na przykład:

   https://192.168.1.2

   Adres IP urządzenia można znaleźć w Raporcie konfiguracji sieci.
3. Jeśli jest to wymagane, wprowadź hasło w polu **Login (Zaloguj)**, a następnie kliknij **Login (Zaloguj)**.

Domyślne hasło do zarządzania ustawieniami tego urządzenia znajduje się z tyłu lub na spodzie urządzenia i jest oznaczone napisem „**Pwd**”. Po zalogowaniu się po raz pierwszy zmień domyślne hasło, postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

4. Na lewym pasku nawigacyjnym kliknij **Network (Sieć)**.

Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.

5. Wykonaj jedną z następujących czynności:
   - Sieć przewodowa

     Kliknij **Wired (Przewodowa)** > **Wired 802.1x Authentication (Uwierzytelnianie 802.1x (przewod.))**.
   - Sieć bezprzewodowa

     Kliknij **Wireless (Bezprzewodowa)** > **Wireless (Enterprise) (Bezprzewodowa (firmowa))**.
6. Konfiguruj ustawienia uwierzytelnienia IEEE 802.1x.

- Aby włączyć uwierzytelnianie IEEE 802.1x dla sieci przewodowej, wybierz ustawienie **Enabled (Włączone)** dla **Wired 802.1x status (Stan sieci przew. 802.1x)** na stronie **Wired 802.1x Authentication (Uwierzytelnianie 802.1x (przewod.))**.
- W przypadku używania uwierzytelniania **EAP-TLS** należy wybrać z listy rozwijanej **Client Certificate (Certyfikat klienta)** zainstalowany certyfikat kliencki (wyświetlany z nazwą certyfikatu) w celu weryfikacji.
- Jeśli wybierzesz uwierzytelnienie **EAP-FAST**, **PEAP**, **EAP-TTLS** lub **EAP-TLS**, wybierz metodę weryfikacji z listy rozwijanej **Server Certificate Verification (Weryfikacja cert. serwera)**. Zweryfikuj certyfikat serwera przy użyciu certyfikatu CA zaimportowanego wcześniej do urządzenia, wydanego przez urząd certyfikacji, który zatwierdził certyfikat serwera.

Z listy rozwijanej **Server Certificate Verification (Weryfikacja cert. serwera)** wybierz jedną z następujących metod weryfikacji:

Opcja	Opis
No Verification (Bez weryfikacji)	Certyfikatowi serwera można zawsze ufać. Weryfikacja nie jest przeprowadzana.
CA Cert. (Cert. urzędu cert.)	Metoda weryfikacji urzędu certyfikacji, który wydał certyfikat serwera, przy użyciu certyfikatu CA wydanego przez urząd certyfikacji, który zatwierdził certyfikat serwera.
CA Cert. + ServerID (Cert. urzędu cert. + ServerID)	Metoda weryfikacji wartości nazwy zwykłej [1] wartość certyfikatu serwera, oprócz sprawdzania urzędu certyfikacji, który wydał certyfikat serwera.

7. Po zakończeniu konfiguracji kliknij **Submit (Prześlij)**.

   W przypadku sieci przewodowej: Po skonfigurowaniu podłącz urządzenie do sieci obsługującej standard IEEE 802.1x. Po kilku minutach wydrukuj Raport konfiguracji sieci w celu sprawdzenia stanu <**Wired IEEE 802.1x**>.

Opcja	Opis
Success	Funkcja przewodowa IEEE 802.1x jest włączona i uwierzytelnianie się powiodło.
Failed	Funkcja przewodowa IEEE 802.1x jest włączona, ale uwierzytelnianie się nie powiodło.
Off	Funkcja przewodowa IEEE 802.1x nie jest dostępna.

Powiązane informacje

- Stosowanie uwierzytelniania metodą IEEE 802.1x w sieci

Powiązane tematy:

- Przegląd funkcji certyfikatów zabezpieczających
- Konfiguracja certyfikatów bezpieczeństwa urządzenia

1 Weryfikacja nazwy zwykłej polega na porównaniu nazwy zwykłej certyfikatu serwera z ciągiem znaków ustawionym dla opcji **Server ID (ID serwera)**. Przed użyciem tej metody skontaktuj się z administratorem systemu w sprawie nazwy zwykłej certyfikatu serwera, a następnie skonfiguruj ustawienie **Server ID (ID serwera)**.

Metody uwierzytelniania IEEE 802.1x

EAP-FAST

Protokół Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) został opracowany przez firmę Cisco Systems, Inc., do uwierzytelniania wykorzystuje ID oraz hasło, a do uwierzytelniania tunelowego wykorzystuje algorytmy kluczy symetrycznych.

Urządzenie Brother obsługuje następujące wewnętrzne metody uwierzytelniania:

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

EAP-MD5 (sieć przewodowa)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) korzysta z ID użytkownika i hasła dla uwierzytelniania typu wyzwanie-odpowiedź.

PEAP

Protected Extensible Authentication Protocol (PEAP) to wersja metody EAP stworzona przez Cisco Systems, Inc., Microsoft Corporation i RSA Security. PEAP tworzy zaszyfrowany tunel Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) pomiędzy klientem i serwerem uwierzytelniania, w celu wysyłania ID i hasła. PEAP oferuje uwierzytelnianie wzajemne pomiędzy serwerem a klientem.

Urządzenie Brother obsługuje następujące wewnętrzne metody uwierzytelniania:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) został opracowany przez firmy Funk Software i Certicom. EAP-TTLS tworzy podobny szyfrowany tunel SSL do PEAP, pomiędzy klientem a serwerem uwierzytelniania, w celu wysłania ID użytkownika i hasła. EAP-TTLS oferuje wzajemne uwierzytelnianie pomiędzy serwerem a klientem.

Urządzenie Brother obsługuje następujące wewnętrzne metody uwierzytelniania:

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

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) wymaga uwierzytelniania certyfikatem cyfrowym zarówno po stronie klienta, jak i serwera uwierzytelniania.

Powiązane informacje

- Stosowanie uwierzytelniania metodą IEEE 802.1x w sieci