Przewodnik po funkcjach zabezpieczeń

Spis Treści

Wprowadzenie

Definicje oznaczeń

W tym Podręczniku Użytkownika stosowane są następujące symbole i konwencje:

WAŻNE	WAŻNE wskazuje na potencjalnie niebezpieczną sytuację która, jeśli się jej nie uniknie, może spowodować uszkodzenie własności lub utratę funkcjonalności produktu.
INFORMACJA	INFORMACJA określają środowisko pracy, warunki instalacji lub specjalne warunki eksploatacji.
	Ikony podpowiedzi oznaczają przydatne wskazówki i dodatkowe informacje.
Pogrubienie	Pogrubieniem oznaczone są przyciski na panelu sterowania urządzenia lub na ekranie komputera.
Kursywa	Italicized emphasizes ważny punkt lub wskazuje powiązany temat.

Powiązane informacje

- Wprowadzenie

Znaki handlowe

Adobe® i Reader® są zastrzeżonymi znakami handlowymi lub znakami handlowymi firmy Adobe Systems Incorporated Stanach Zjednoczonych i/lub innych krajach.

Każda firma, której nazwa oprogramowania jest wymieniona w tym podręczniku, posiada umowę License oprogramowania dotyczącą programów będących jej własnością.

Wszelkie nazwy handlowe lub nazwy produktów widoczne na produktach Brother, a także w powiązanych dokumentach lub innych materiałach, to znaki handlowe lub zarejestrowane znaki handlowe firm będących ich właścicielami.

Powiązane informacje

- Wprowadzenie

Prawa autorskie

Powiązane informacje

- Wprowadzenie

Przed użyciem funkcji zabezpieczeń sieci

W urządzeniu zastosowano niektóre z najnowocześniejszych obecnie protokołów zabezpieczeń sieciowych i szyfrowania. Te funkcje sieciowe można zintegrować z ogólnym planem zabezpieczeń sieciowych, aby ułatwić ochronę danych i zapobiegać próbom nieautoryzowanego dostępu do urządzenia.

Zalecamy wyłączenie protokołów FTP i TFTP. Uzyskiwanie dostępu do urządzenia za pośrednictwem tych protokołów nie jest bezpieczne.

Powiązane informacje

- Wprowadzenie
  - Wyłączanie niepotrzebnych protokołów

Wyłączanie niepotrzebnych protokołów

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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Sieć** > **Protokół**.

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

5. Usuń zaznaczenia pól wyboru niepotrzebnych protokołów, aby je wyłączyć.
6. Kliknij przycisk **Prześlij**.
7. Uruchom ponownie urządzenie Brother, aby aktywować konfigurację.

Powiązane informacje

- Przed użyciem funkcji zabezpieczeń sieci

Bezpieczeństwo sieci

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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

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

5. Kliknij przycisk **Utwórz certyfikat z własnym podpisem**.
6. Wprowadź informacje w polach **Nazwa pospolita** i **Data ważności**.
   - Długość tekstu w polu **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 **Nazwa pospolita** zostanie wyświetlone okno ostrzeżenia.
7. Wybierz ustawienie z listy rozwijanej **Algorytm klucza publicznego**.
8. Wybierz ustawienie z listy rozwijanej **Algorytm skrótu**.
9. Kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

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

5. Kliknij przycisk **Utwórz CSR**.
6. Wpisz **Nazwa pospolita** (wymagane) i dodaj inne informacje o **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 **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 **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 **Organizacja**, **Jednostka organizacyjna**, **Miasto/miejscowość** i **Województwo/stan** musi być mniejsza niż 64 bajty.
- Pozycję **Kraj/region** powinien stanowić dwuliterowy kod kraju według normy ISO 3166.
- W przypadku konfigurowania rozszerzenia certyfikatu X.509v3 zaznacz pole wyboru **Skonfiguruj partycję rozszerzoną**, a następnie wybierz opcję **Auto (rejestr. IPv4)** lub **Ręczne**.

7. Wybierz ustawienie z listy rozwijanej **Algorytm klucza publicznego**.
8. Wybierz ustawienie z listy rozwijanej **Algorytm skrótu**.
9. Kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij przycisk **Zainstaluj certyfikat**.
6. Wyszukaj plik zawierający certyfikat wystawiony przez urząd certyfikacji, a następnie kliknij **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

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

5. Kliknij przycisk **Importuj certyfikat i klucz prywatny**.
6. Przejdź do pliku, który ma zostać zaimportowany.
7. Jeżeli plik jest zaszyfrowany, wprowadź hasło, a następnie kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

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

5. Kliknij przycisk **Eksportuj** widoczny z **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 **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat CA**.

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

5. Kliknij **Importuj certyfikat urzędu certyfikacji**.
6. Znajdź plik, który chcesz importować.
7. Kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat CA**.

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

5. Wybierz certyfikat, który ma zostać wyeksportowany, a następnie kliknij przycisk **Eksportuj**.
6. Kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Sieć** > **Protokół**.

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

5. Kliknij **Ustawienia serwera HTTP**.
6. Wybierz certyfikat, który chcesz skonfigurować, z listy rozwijanej **Wybierz certyfikat**.
7. Kliknij **Prześlij**.
8. Kliknij **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 **Zaloguj**, a następnie kliknij **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Certyfikat**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
6. Kliknij **Eksportuj**.
7. Aby zaszyfrować wydrukowany plik, wpisz hasło w polu **Wprowadź hasło**. Jeśli pole **Wprowadź hasło** jest puste, plik wyjściowy nie zostanie zaszyfrowany.
8. Wprowadź ponownie hasło w polu **Wpisz hasło pon.**, a następnie kliknij przycisk **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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Sieć** > **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 **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 **Sieć** > **Sieć** > **Protokół**.

6. Kliknij przycisk **Ustawienia serwera HTTP**.
7. Zaznacz pole wyboru **HTTPS(Port 443)** w obszarze **IPP**, a następnie kliknij **Prześlij**.
8. Uruchom ponownie urządzenie, aby aktywować konfigurację.

Komunikacja za pośrednictwem protokołu IPPS nie zapobiega nieautoryzowanemu 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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Sieć** > **Protokół**.

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

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

Opcja	Opis
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 tylko do odczytu	Serwer drukowania korzysta z wersji 1 i 2c protokołu SNMP funkcji dostępu w trybie tylko do odczytu.
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 tylko do odczytu** lub **SNMP v1/v2c — dostęp do odczytu i zapisu**.

7. Skonfiguruj ustawienia trybu SNMPv3.

Opcja	Opis
Włączone	Serwer drukowania korzysta z wersji 3 protokołu SNMP. Aby bezpiecznie zarządzać serwerem druku, użyj trybu SNMPv3.
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 **Prześlij**.

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

9. Uruchom ponownie urządzenie, aby aktywować konfigurację.

Powiązane informacje

- Używanie protokołu SNMPv3

Używanie IPsec

Wprowadzenie do protokołu IPsec

IPsec (Internet Protocol Security) to protokół zabezpieczeń, który wykorzystuje opcjonalną funkcję protokołu internetowego, aby zapobiegać manipulacji danymi oraz zapewnić poufność danych transmitowanych jako pakiety IP. Funkcja IPsec szyfruje dane przesyłane za pośrednictwem sieci, na przykład dane drukowania wysyłane z komputerów do drukarki. Ze względu na to, że dane są szyfrowane w warstwie sieciowej, aplikacje wykorzystujące protokół wyższego poziomu korzystają z funkcji IPsec nawet wtedy, gdy użytkownik nie wie, że jest używana.

IPsec obsługuje następujące funkcje:

- Transmisje IPsec

  Zgodnie z warunkami ustawień IPsec, komputer podłączony do sieci wysyła dane i odbiera dane z określonego urządzenia za pośrednictwem protokołu IPsec. Gdy urządzenia rozpoczynają komunikację za pośrednictwem protokołu IPsec, najpierw następuje wymiana kluczy z wykorzystaniem technologii IKE, a następnie za pomocą kluczy transmitowane są zaszyfrowane dane.

  Ponadto IPsec ma dwa tryby robocze: tryb transportowy oraz trybu tunelowy. Tryb transportowy używany jest głównie do komunikacji między urządzeniami, a tryb tunelu jest używany w środowiskach, takich jak sieci VPN (Virtual Private Network).

  W przypadku transmisji IPsec niezbędne są następujące warunki:
  - Komputer, który może komunikować się za pomocą protokołu IPsec, jest podłączony do sieci.
  - Urządzenie jest skonfigurowane do komunikacji IPsec.
  - Komputer podłączony do urządzenia jest skonfigurowany do połączeń IPsec.

- Ustawienia IPsec

  Ustawienia, które są niezbędne do połączeń za pomocą protokołu IPsec. Ustawienia te można skonfigurować za pomocą funkcji Zarządzanie przez interfejs webowy.

  Aby skonfigurować ustawienia protokołu IPsec, należy użyć przeglądarki na komputerze podłączonym do sieci.

Powiązane informacje

- Używanie IPsec

Konfigurowanie protokołu IPsec przy użyciu funkcji Zarządzanie przez interfejs webowy

Warunki połączenia IPsec obejmują dwa **Szablon** typy: **Adres** i **IPsec**. Możliwe jest skonfigurowanie maksymalnie 10 warunków połączenia.

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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **IPsec**.

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

Opcja	Opis
Stan	Włącz lub wyłącz IPsec.
Tryb negocjacji	Wybierz **Tryb negocjacji** dla opcji IKE Phase 1. IKE to protokół używany do wymiany kluczy szyfrujących w celu przeprowadzenia zaszyfrowanej komunikacji za pośrednictwem protokołu IPsec. W trybie **Główne** szybkość przetwarzania jest niska, ale poziom zabezpieczeń jest wysoki. W trybie **Agresywne** prędkość przetwarzania jest wyższa niż w trybie **Główne**, ale bezpieczeństwo jest niższe.
Cały ruch inny niż IPsec	Wybierz działanie, jakie ma zostać wykonane, dla pakietów innych niż IPsec. Podczas korzystania z usług sieciowych należy wybrać ustawienie **Zezwalaj** w opcji **Cały ruch inny niż IPsec**. Jeśli wybrane zostanie ustawienie **Odrzuć**, nie będzie można użyć usług sieciowych.
Pomijanie emisji/multiemisji	Wybierz **Włączone** lub **Wyłączone**.
Pomijanie protokołu	Zaznacz pola wyboru dla opcji, które mają zostać użyte.
Reguły	Zaznacz pole wyboru **Włączone**, aby aktywować szablon. Po wybraniu wielu pól wyboru pola wyboru o niższych numerach mają priorytet w przypadku, gdy ustawienia dla wybranych pól wyboru kolidują ze sobą. Kliknij odpowiednią listę rozwijaną, aby wybrać **Szablon adresu**, który jest używany dla warunków połączenia IPsec. Aby dodać opcję **Szablon adresu**, kliknij **Dodaj szablon**. Kliknij odpowiednią listę rozwijaną, aby wybrać **Szablon IPsec**, który jest używany dla warunków połączenia IPsec. Aby dodać opcję **Szablon IPsec**, kliknij **Dodaj szablon**.

6. Kliknij **Prześlij**.

   Jeśli urządzenie musi zostać uruchomione ponownie w celu aktywowania nowych ustawień, wyświetlony zostanie ekran potwierdzenia ponownego uruchomienia.

Jeśli w tabeli **Reguły** we włączonym szablonie pozycja jest pusta, wyświetlony zostanie komunikat o błędzie. Potwierdź wybory i kliknij **Prześlij** ponownie.

Powiązane informacje

- Używanie IPsec

Powiązane tematy:

- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Konfigurowanie szablonu adresu protokołu IPsec z użyciem funkcji Zarządzanie 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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Szablon adresu IPsec**.

   Jeśli lewy pasek nawigacyjny nie jest widoczny, rozpocznij nawigację od ☰.
5. Kliknij przycisk **Usuń**, aby usunąć **Szablon adresu**. Gdy **Szablon adresu** jest używany, nie można go usunąć.
6. Kliknij **Szablon adresu**, który chcesz utworzyć. Zostanie wyświetlony **Szablon adresu IPsec**.
7. Skonfiguruj ustawienia.

Opcja	Opis
Nazwa szablonu	Wpisz nazwę szablonu (do 16 znaków).
Lokalny adres IP	• **Adres IP** Podaj adres IP. Wybierz **Wszystkie adresy IPv4**, **Wszystkie adresy IPv6**, **WSZYSTKIE adresy IPv6 połączenia lokalnego** lub **Niestand.** z listy rozwijanej. Jeśli wybrano **Niestand.** z listy rozwijanej, wpisz adres IP (IPv4 lub IPv6) w polu tekstowym. • **Zakres adresów IP** Wpisz początkowy i końcowy adres IP dla zakresu adresów IP w polach tekstowych. Jeśli początkowy i końcowy adres IP nie jest zgodny ze standardem IPv4 lub IPv6 lub jeśli końcowy adres IP jest mniejszy niż adres początkowy, wygenerowany zostanie błąd. • **Adres IP/prefiks** Podaj adres IP w notacji CIDR. Na przykład: 192.168.1.1/24 Ponieważ prefiks podany jest w postaci 24-bitowej maski podsieci (255.255.255.0) dla adresu 192.168.1.1, ważne są adresy 192.168.1.###.
Zdalny adres IP	• **Dowolny** Jeśli wybrana zostanie opcja **Dowolny**, włączone będą wszystkie adresy IP. • **Adres IP** Wpisz określony adres IP (IPv4 lub IPv6) w polu tekstowym. • **Zakres adresów IP** Wpisz pierwszy i ostatni adres IP z zakresu adresów IP. Jeśli pierwszy i ostatni adres IP nie jest zgodny ze standardem IPv4 lub IPv6 lub jeśli ostatni adres IP jest mniejszy niż adres pierwszy, wygenerowany zostanie błąd.

Opcja	Opis
	• **Adres IP/prefiks** Podaj adres IP w notacji CIDR. Na przykład: 192.168.1.1/24 Ponieważ prefiks podany jest w postaci 24-bitowej maski podsieci (255.255.255.0) dla adresu 192.168.1.1, ważne są adresy 192.168.1.###.

8. Kliknij przycisk **Prześlij**.

Gdy zmienisz ustawienia aktualnie używanego szablonu, zrestartuj urządzenie, aby aktywować konfigurację.

Powiązane informacje

- Używanie IPsec

Konfigurowanie szablonu protokołu IPsec przy użyciu funkcji Zarządzanie 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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Bezpieczeństwo** > **Szablon IPsec**.

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

5. Kliknij przycisk **Usuń**, aby usunąć **Szablon IPsec**. Gdy **Szablon IPsec** jest używany, nie można go usunąć.
6. Kliknij **Szablon IPsec**, który chcesz utworzyć. Wyświetlony zostanie ekran **Szablon IPsec**. Pola konfiguracji różnią się w zależności od wybranych ustawień **Użyj predef. szablonu** i **Wymiana kluczy internetowych (IKE)**.
7. W polu **Nazwa szablonu** wpisz nazwę szablony (maksymalnie 16 znaków).
8. Jeśli wybrano **Niestand.** z listy rozwijanej **Użyj predef. szablonu**, należy wybrać opcje **Wymiana kluczy internetowych (IKE)**, a następnie zmienić ustawienia w razie potrzeby.
9. Kliknij przycisk **Prześlij**.

Powiązane informacje

- Używanie IPsec
  - Ustawienia IKEv1 dla szablonu protokołu IPsec
  - Ustawienia IKEv2 dla szablonu protokołu IPsec
  - Ustawienia ręczne dla szablonu protokołu IPsec

Ustawienia IKEv1 dla szablonu protokołu IPsec

Opcja	Opis
Nazwa szablonu	Wpisz nazwę szablonu (do 16 znaków).
Użyj predef. szablonu	Wybierz **Niestand.**, **IKEv1 — wysoka ochrona** lub **IKEv1 — średnia ochrona**. Elementy ustawień różnią się w zależności od wybranego szablonu.
Wymiana kluczy internetowych (IKE)	IKE to protokół komunikacyjny używany do wymiany kluczy szyfrujących w celu przeprowadzenia zaszyfrowanej komunikacji za pośrednictwem protokołu IPsec. W celu przeprowadzenia szyfrowania komunikacji tylko w tym momencie, ustalany jest algorytm szyfrowania niezbędny dla protokołu IPsec i udostępniane są klucze szyfrowania. W przypadku IKE, klucze szyfrowania są przesyłane za pomocą metody wymiany kluczy Diffie-Hellman i przeprowadzana jest szyfrowana komunikacja, ograniczona wyłącznie do IKE. Jeśli została wybrana opcja **Niestand.** w **Użyj predef. szablonu**, zaznacz **IKEv1**.
Typ uwierzytelniania	• **Grupa Diffiego-Hellmana** Ta metoda wymiany kluczy pozwala na bezpiecznie przesyłane tajnych kluczy za pośrednictwem niezabezpieczonej sieci. Metoda wymiany kluczy Diffie-Hellman wykorzystuje problem logarytmu dyskretnego, a nie tajny klucz, do wysyłania i odbierania otwartych informacji wygenerowanych za pomocą liczb losowych i tajnego klucza. Wybierz **Grupa1**, **Grupa2**, **Grupa5** lub **Grupa14**. • **Szyfrowanie** Wybierz **DES**, **3DES**, **AES-CBC 128** lub **AES-CBC 256**. • **Skrót** Wybierz **MD5**, **SHA1**, **SHA256**, **SHA384** lub **SHA512**. • **Okres istnienia skojarzeń zabezpieczeń** Podaj okres ważności IKE SA. Wpisz czas (w sekundach) oraz liczbę kilobajtów (KB).
Zabezpieczenia hermetyzacji	• **Protokół** Wybierz **ESP**, **AH** lub **AH+ESP**. - ESP to protokół wykorzystywany do przeprowadzania zaszyfrowanej komunikacji za pomocą protokołu IPsec. ESP szyfruje ładunek (treść komunikacji) i dodaje informacje dodatkowe. Pakiet IP składa się z nagłówka i zaszyfrowanego ładunku danych, który następuje po nagłówku. Oprócz zaszyfrowanych danych, pakiet IP zawiera również informacje dotyczące metody szyfrowania i klucza szyfrowania, dane uwierzytelniające i inne. - AH jest częścią protokołu IPsec, która dokonuje uwierzytelnienia nadawcy i uniemożliwia manipulowanie danymi (zapewnia kompletność danych). W pakiecie IP, dane umieszczone są tuż po nagłówku. Ponadto, pakiety zawierają wartości skrótów (hash), które są obliczane za pomocą równania na podstawie przekazanych treści, tajnego klucza i innych, w celu zapobiegania fałszowaniu nadawcy i manipulowania danymi. W odróżnieniu od ESP, przekazywane treści nie są zaszyfrowane, a dane są wysyłane i odbierane jako zwykły tekst. • **Szyfrowanie (Niedostępne dla opcji AH).** Wybierz **DES**, **3DES**, **AES-CBC 128** lub **AES-CBC 256**.

Opcja	Opis
	• **Skrót** Wybierz **Brak**, **MD5**, **SHA1**, **SHA256**, **SHA384** lub **SHA512**. **Brak** można wybrać tylko wtedy, gdy opcja **ESP** jest wybrana dla ustawienia **Protokół**. • **Okres istnienia skojarzeń zabezpieczeń** Określ czas życia IKE SA. Wpisz czas (w sekundach) i liczbę kilobajtów (kb). • **Tryb hermetyzacji** Wybierz opcję **Transport** lub **Tunel**. • **Adres IP routera zdalnego** Wpisz adres IP (IPv4 lub IPv6) dla zdalnego routera. Wprowadź te informacje tylko wtedy, gdy wybrany jest tryb **Tunel**. SA (Security Association) to metoda szyfrowanej komunikacji korzystającej z protokołu IPsec lub IPv6, która wymienia i dzieli się informacjami, takimi jak metoda i klucz szyfrowania, w celu ustanowienia bezpiecznego kanału komunikacji przed rozpoczęciem komunikacji. SA może również odnosić się do wirtualnego szyfrowanego kanału komunikacji, który został ustanowiony. SA wykorzystywane do protokołu IPsec określa metodę szyfrowania, prowadzi wymianę kluczy, oraz dokonuje uwierzytelnienia obustronnego zgodnie ze standardową procedurą IKE (Internet Key Exchange). Dodatkowo, metoda SA jest regularnie aktualizowana.
Doskonałe utajnienie przekazywania (PFS)	PFS nie określa kluczy na podstawie poprzednich kluczy, które były używane do szyfrowania wiadomości. Ponadto, jeżeli klucz użyty do szyfrowania wiadomości został wyprowadzony z klucza nadrzędnego, ten klucz nadrzędny nie zostanie wykorzystany do wyprowadzenia innych kluczy. Z tego względu nawet jeśli bezpieczeństwo klucza zostanie naruszone, szkody będą ograniczone jedynie do wiadomości, które zostały zaszyfrowane przy użyciu tego klucza. Wybierz **Włączone** lub **Wyłączone**.
Metoda uwierz.	Wybierz metodę uwierzytelniania. Wybierz **Klucz wstępny** lub **Certyfikaty**.
Klucz wstępny	Podczas szyfrowania komunikacji klucz szyfrowania jest wymieniany i udostępniany przed użyciem innego kanału. Jeśli wybrano **Klucz wstępny** dla **Metoda uwierz.**, wpisz **Klucz wstępny** (do 32 znaków). • **Lokalne/Typ ID/ID** Wybierz typ identyfikatora nadawcy, a następnie wpisz identyfikator. Wybierz **Adres IPv4**, **Adres IPv6**, **Nazwa FQDN**, **Adres e-mail** lub **Certyfikat** dla typu. Jeśli wybrano **Certyfikat**, wpisz nazwę wspólną certyfikatu w polu **ID**. • **Zdalny/Typ ID/ID** Wybierz typ identyfikatora odbiorcy, a następnie wpisz identyfikator. Wybierz **Adres IPv4**, **Adres IPv6**, **Nazwa FQDN**, **Adres e-mail** lub **Certyfikat** dla typu. Jeśli wybrano **Certyfikat**, wpisz nazwę wspólną certyfikatu w polu **ID**.
Certyfikat	Jeśli wybrano opcję **Certyfikaty** dla **Metoda uwierz.**, wybierz certyfikat.

Opcja	Opis
	Można wybrać tylko te certyfikaty, które zostały utworzone za pomocą strony **Certyfikat** ekranu konfiguracji zabezpieczeń funkcji Zarządzanie przez interfejs webowy.

Powiązane informacje

- Konfigurowanie szablonu protokołu IPsec przy użyciu funkcji Zarządzanie przez interfejs webowy

Ustawienia IKEv2 dla szablonu protokołu IPsec

Opcja	Opis
Nazwa szablonu	Wpisz nazwę szablonu (do 16 znaków).
Użyj predef. szablonu	Wybierz **Niestand.**, **IKEv2 — wysoka ochrona** lub **IKEv2 — średnia ochrona**. Elementy ustawień różnią się w zależności od wybranego szablonu.
Wymiana kluczy internetowych (IKE)	IKE to protokół komunikacyjny używany do wymiany kluczy szyfrujących w celu przeprowadzenia zaszyfrowanej komunikacji za pośrednictwem protokołu IPsec. W celu przeprowadzenia szyfrowania komunikacji tylko w tym momencie, ustalany jest algorytm szyfrowania niezbędny dla protokołu IPsec i udostępniane są klucze szyfrowania. W przypadku IKE, klucze szyfrowania są przesyłane za pomocą metody wymiany kluczy Diffie-Hellman i przeprowadzana jest szyfrowana komunikacja, ograniczona wyłącznie do IKE. Jeśli została wybrana opcja **Niestand.** w **Użyj predef. szablonu**, zaznacz **IKEv2**.
Typ uwierzytelniania	• **Grupa Diffiego-Hellmana** Ta metoda wymiany kluczy pozwala na bezpiecznie przesyłane tajnych kluczy za pośrednictwem niezabezpieczonej sieci. Metoda wymiany kluczy Diffie-Hellman wykorzystuje problem logarytmu dyskretnego, a nie tajny klucz, do wysyłania i odbierania otwartych informacji wygenerowanych za pomocą liczb losowych i tajnego klucza. Wybierz **Grupa1**, **Grupa2**, **Grupa5** lub **Grupa14**. • **Szyfrowanie** Wybierz **DES**, **3DES**, **AES-CBC 128** lub **AES-CBC 256**. • **Skrót** Wybierz **MD5**, **SHA1**, **SHA256**, **SHA384** lub **SHA512**. • **Okres istnienia skojarzeń zabezpieczeń** Podaj okres ważności IKE SA. Wpisz czas (w sekundach) oraz liczbę kilobajtów (KB).
Zabezpieczenia hermetyzacji	• **Protokół** Wybierz **ESP**. ESP to protokół wykorzystywany do przeprowadzania zaszyfrowanej komunikacji za pomocą protokołu IPsec. ESP szyfruje ładunek (treść komunikacji) i dodaje informacje dodatkowe. Pakiet IP składa się z nagłówka i zaszyfrowanego ładunku danych, który następuje po nagłówku. Oprócz zaszyfrowanych danych, pakiet IP zawiera również informacje dotyczące metody szyfrowania i klucza szyfrowania, dane uwierzytelniające i inne. • **Szyfrowanie** Wybierz opcję **DES**, **3DES**, **AES-CBC 128** lub **AES-CBC 256**. • **Skrót** Wybierz **MD5**, **SHA1**, **SHA256**, **SHA384**, lub **SHA512**. • **Okres istnienia skojarzeń zabezpieczeń** Określ czas życia IKE SA. Wpisz czas (w sekundach) i liczbę kilobajtów (kb). • **Tryb hermetyzacji** Wybierz opcję **Transport** lub **Tunel**.

Opcja	Opis
	• **Adres IP routera zdalnego** Wpisz adres IP (IPv4 lub IPv6) dla zdalnego routera. Wprowadź te informacje tylko wtedy, gdy wybrany jest tryb **Tunel**. SA (Security Association) to metoda szyfrowanej komunikacji korzystającej z protokołu IPsec lub IPv6, która wymienia i dzieli się informacjami, takimi jak metoda i klucz szyfrowania, w celu ustanowienia bezpiecznego kanału komunikacji przed rozpoczęciem komunikacji. SA może również odnosić się do wirtualnego szyfrowanego kanału komunikacji, który został ustanowiony. SA wykorzystywane do protokołu IPsec określa metodę szyfrowania, prowadzi wymianę kluczy, oraz dokonuje uwierzytelnienia obustronnego zgodnie ze standardową procedurą IKE (Internet Key Exchange). Dodatkowo, metoda SA jest regularnie aktualizowana.
Doskonałe utajnienie przekazywania (PFS)	PFS nie określa kluczy na podstawie poprzednich kluczy, które były używane do szyfrowania wiadomości. Ponadto, jeżeli klucz użyty do szyfrowania wiadomości został wyprowadzony z klucza nadrzędnego, ten klucz nadrzędny nie zostanie wykorzystany do wyprowadzenia innych kluczy. Z tego względu nawet jeśli bezpieczeństwo klucza zostanie naruszone, szkody będą ograniczone jedynie do wiadomości, które zostały zaszyfrowane przy użyciu tego klucza. Wybierz **Włączone** lub **Wyłączone**.
Metoda uwierz.	Wybierz metodę uwierzytelniania. Wybierz **Klucz wstępny**, **Certyfikaty**, **EAP - MD5** lub **EAP - MS-CHAPv2**. EAP to protokół uwierzytelniania stanowiący rozszerzenie PPP. W przypadku użycia EAP z IEEE 802.1x inny klucz jest używany do uwierzytelniania użytkowników i podczas każdej sesji. Poniższe ustawienia są konieczne tylko wtedy, gdy wybrano opcję **EAP - MD5** lub **EAP - MS-CHAPv2** w **Metoda uwierz.**: • **Tryb** Wybierz **Tryb serwera** lub **Tryb klienta**. • **Certyfikat** Wybierz certyfikat. • **Nazwa użytk.** Wpisz nazwę użytkownika (do 32 znaków). • **Hasło** Wpisz hasło (do 32 znaków). Hasło należy wprowadzić dwukrotnie w celu potwierdzenia.
Klucz wstępny	Podczas szyfrowania komunikacji klucz szyfrowania jest wymieniany i udostępniany przed użyciem innego kanału. Jeśli wybrano **Klucz wstępny** dla **Metoda uwierz.**, wpisz **Klucz wstępny** (do 32 znaków). • **Lokalne/Typ ID/ID** Wybierz typ identyfikatora nadawcy, a następnie wpisz identyfikator. Wybierz **Adres IPv4**, **Adres IPv6**, **Nazwa FQDN**, **Adres e-mail** lub **Certyfikat** dla typu. Jeśli wybrano **Certyfikat**, wpisz nazwę wspólną certyfikatu w polu **ID**. • **Zdalny/Typ ID/ID** Wybierz typ identyfikatora odbiorcy, a następnie wpisz identyfikator.

Opcja	Opis
	Wybierz **Adres IPv4**, **Adres IPv6**, **Nazwa FQDN**, **Adres e-mail** lub **Certyfikat** dla typu. Jeśli wybrano **Certyfikat**, wpisz nazwę wspólną certyfikatu w polu **ID**.
Certyfikat	Jeśli wybrano opcję **Certyfikaty** dla **Metoda uwierz.**, wybierz certyfikat. Można wybrać tylko te certyfikaty, które zostały utworzone za pomocą strony **Certyfikat** ekranu konfiguracji zabezpieczeń funkcji Zarządzanie przez interfejs webowy.

Powiązane informacje

- Konfigurowanie szablonu protokołu IPsec przy użyciu funkcji Zarządzanie przez interfejs webowy

Ustawienia ręczne dla szablonu protokołu IPsec

Opcja	Opis
Nazwa szablonu	Wpisz nazwę szablonu (do 16 znaków).
Użyj predef. szablonu	Wybierz **Niestand.**.
Wymiana kluczy internetowych (IKE)	IKE to protokół komunikacyjny używany do wymiany kluczy szyfrujących w celu przeprowadzenia zaszyfrowanej komunikacji za pośrednictwem protokołu IPsec. W celu przeprowadzenia szyfrowania komunikacji tylko w tym momencie, ustalany jest algorytm szyfrowania niezbędny dla protokołu IPsec i udostępniane są klucze szyfrowania. W przypadku IKE, klucze szyfrowania są przesyłane za pomocą metody wymiany kluczy Diffie-Hellman i przeprowadzana jest szyfrowana komunikacja, ograniczona wyłącznie do IKE. Wybierz **Ręczne**.
Klucz uwierzytelniania (ESP, AH)	Wpisz wartości **Wej./Wyj.**. Te ustawienia są niezbędne, gdy ustawienie **Niestand.** jest wybrane dla opcji **Użyj predef. szablonu**, ustawienie **Ręczne** jest wybrane dla opcji **Wymiana kluczy internetowych (IKE)**, i ustawienie inne niż **Brak** jest wybrane dla opcji **Skrót** w sekcji **Zabezpieczenia hermetyzacji**. Liczba znaków, które można ustawić, zależy od ustawień wybranych w opcji **Skrót** w sekcji **Zabezpieczenia hermetyzacji**. Jeżeli długość podanego klucza uwierzytelniania różni się od wybranego algorytmu hash, wystąpi błąd. • **MD5**: 128 bitów (16 bajtów) • **SHA1**: 160 bitów (20 bajtów) • **SHA256**: 256 bitów (32 bajty) • **SHA384**: 384 bitów (48 bajtów) • **SHA512**: 512 bitów (64 bajty) Podając klucz w kodzie ASCII, znaki należy zawrzeć w podwójnych cudzysłowach (").
Klucz kodu (ESP)	Wpisz wartości **Wej./Wyj.**. Ustawienia te są niezbędne, gdy ustawienie **Niestand.** wybrane jest dla opcji **Użyj predef. szablonu**, ustawienie **Ręczne** jest wybrane dla opcji **Wymiana kluczy internetowych (IKE)** oraz ustawienie **ESP** jest wybrane dla opcji **Protokół** w sekcji **Zabezpieczenia hermetyzacji**. Liczba znaków, które można ustawić, zależy od ustawień wybranych w opcji **Szyfrowanie** w sekcji **Zabezpieczenia hermetyzacji**. Jeżeli długość podanego klucza kodu różni się od wybranego algorytmu szyfrowania, wystąpi błąd. • **DES**: 64 bity (8 bajtów) • **3DES**: 192 bity (24 bajty) • **AES-CBC 128**: 128 bitów (16 bajtów) • **AES-CBC 256**: 256 bitów (32 bajty) Podając klucz w kodzie ASCII, znaki należy zawrzeć w podwójnych cudzysłowach (").
SPI	Te parametry są używane do identyfikacji informacji zabezpieczających. Ogólnie host posiada wiele SA (Security Associations) dla różnych typów komunikacji IPsec. Dlatego niezbędne jest określenie odpowiedniego SA po odebraniu pakietu IPsec. Parametr SPI,

Opcja	Opis
	identyfikujący SA, dołączony jest w nagłówku AH (Authentication Header) i ESP (Encapsulating Security Payload). Te ustawienia są niezbędne, gdy wybrano opcję **Niestand.** w **Użyj predef. szablonu**, i **Ręczne** w **Wymiana kluczy internetowych (IKE)**. Wprowadź wartości **Wej./Wyj.**. (3–10 znaków)
Zabezpieczenia hermetyzacji	• **Protokół** Wybierz **ESP** lub **AH**. - ESP to protokół wykorzystywany do przeprowadzania zaszyfrowanej komunikacji za pomocą protokołu IPsec. ESP szyfruje ładunek (treść komunikacji) i dodaje informacje dodatkowe. Pakiet IP składa się z nagłówka i zaszyfrowanego ładunku danych, który następuje po nagłówku. Oprócz zaszyfrowanych danych, pakiet IP zawiera również informacje dotyczące metody szyfrowania i klucza szyfrowania, dane uwierzytelniające i inne. - AH jest częścią protokołu IPsec, która dokonuje uwierzytelnienia nadawcy i uniemożliwia manipulowanie danymi (zapewnia kompletność danych). W pakiecie IP, dane umieszczone są tuż po nagłówku. Ponadto, pakiety zawierają wartości skrótów (hash), które są obliczane za pomocą równania na podstawie przekazanych treści, tajnego klucza i innych, w celu zapobiegania fałszowaniu nadawcy i manipulowania danymi. W odróżnieniu od ESP, przekazywane treści nie są zaszyfrowane, a dane są wysyłane i odbierane jako zwykły tekst. • **Szyfrowanie (Niedostępne dla opcji AH).** Wybierz **DES**, **3DES**, **AES-CBC 128** lub **AES-CBC 256**. • **Skrót** Wybierz **Brak**, **MD5**, **SHA1**, **SHA256**, **SHA384** lub **SHA512**. **Brak** można wybrać tylko wtedy, gdy opcja **ESP** jest wybrana dla ustawienia **Protokół**. • **Okres istnienia skojarzeń zabezpieczeń** Określ czas życia IKE SA. Wpisz czas (w sekundach) i liczbę kilobajtów (kb). • **Tryb hermetyzacji** Wybierz opcję **Transport** lub **Tunel**. • **Adres IP routera zdalnego** Wpisz adres IP (IPv4 lub IPv6) dla zdalnego routera. Wprowadź te informacje tylko wtedy, gdy wybrany jest tryb **Tunel**. SA (Security Association) to metoda szyfrowanej komunikacji korzystającej z protokołu IPsec lub IPv6, która wymienia i dzieli się informacjami, takimi jak metoda i klucz szyfrowania, w celu ustanowienia bezpiecznego kanału komunikacji przed rozpoczęciem komunikacji. SA może również odnosić się do wirtualnego szyfrowanego kanału komunikacji, który został ustanowiony. SA wykorzystywane do protokołu IPsec określa metodę szyfrowania, prowadzi wymianę kluczy, oraz dokonuje uwierzytelnienia obustronnego zgodnie ze standardową procedurą IKE (Internet Key Exchange). Dodatkowo, metoda SA jest regularnie aktualizowana.

Powiązane informacje

- Konfigurowanie szablonu protokołu IPsec przy użyciu funkcji Zarządzanie przez interfejs webowy

Stosowanie uwierzytelniania metodą IEEE 802.1x w sieci

Czym jest uwierzytelnianie IEEE 802.1x?

IEEE 802.1x to standard IEEE, który ogranicza dostęp z nieautoryzowanych 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 **Zaloguj**, a następnie kliknij **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 **Sieć**.

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

5. Wykonaj jedną z następujących czynności:
   - Sieć przewodowa

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

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

- Aby włączyć uwierzytelnianie IEEE 802.1x dla sieci przewodowej, wybierz ustawienie **Włączone** dla **Stan sieci przew. 802.1x** na stronie **Uwierzytelnianie 802.1x (przewod.)**.
- W przypadku używania uwierzytelniania **EAP-TLS** należy wybrać z listy rozwijanej **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 **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 **Weryfikacja cert. serwera** wybierz jedną z następujących metod weryfikacji:

Opcja	Opis
Bez weryfikacji	Certyfikatowi serwera można zawsze ufać. Weryfikacja nie jest przeprowadzana.
Cert. urzędu cert.	Metoda weryfikacji urzędu certyfikacji, który wydał certyfikat serwera, przy użyciu certyfikatu CA wydanego przez urząd certyfikacji, który zatwierdził certyfikat serwera.
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 **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.
Wył.	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 **ID serwera**. Przed użyciem tej metody skontaktuj się z administratorem systemu w sprawie nazwy zwykłej certyfikatu serwera, a następnie skonfiguruj ustawienie **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 przez tunelowanie 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

Uwierzytelnianie użytkownika

Użycie uwierzytelniania Active Directory

Wprowadzenie do uwierzytelniania Active Directory

Uwierzytelnianie Active Directory ogranicza korzystanie z urządzenia. Jeśli włączone jest uwierzytelnianie Active Directory, panel sterowania urządzenia zostanie zablokowany. Nie można zmienić ustawień urządzenia do momentu wprowadzenia przez użytkownika identyfikatora użytkownika i hasła.

Uwierzytelnianie Active Directory oferuje następujące funkcje:

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

- Przechowywanie danych przychodzących drukowania
- Przechowywanie danych przychodzących faksów
- Pozyskuje adres e-mail z serwera Active Directory na podstawie ID użytkownika podczas wysyłania zeskanowanych danych do serwera poczty e-mail.

  Aby użyć tej funkcji, wybierz opcję **Wł.** w ustawieniu **Pobierz adres e-mail** i metodę uwierzytelnienia **LDAP + kerberos** lub **LDAP + NTLMv2**. Twój adres e-mail będzie ustawiony jako nadawca, gdy urządzenie będzie przesyłać zeskanowane dane na serwer poczty e-mail, lub jako odbiorca, gdy będziesz wysyłać zeskanowane dane na swój adres e-mail.

Gdy uwierzytelnianie Active Directory jest włączone, urządzenie zapisuje dane wszystkich przychodzących faksów. Po zalogowaniu się urządzenie wydrukuje zapisane dane faksów.

Ustawienie uwierzytelniania Active Directory można zmienić za pomocą funkcji Zarządzanie przez interfejs webowy.

Powiązane informacje

- Użycie uwierzytelniania Active Directory

Konfigurowanie uwierzytelniania Active Directory za pomocą funkcji Zarządzanie przez interfejs webowy

Funkcja uwierzytelniania Active Directory obsługuje uwierzytelnianie Kerberos oraz NTLMv2. Należy skonfigurować protokół SNTP (serwer czasu sieciowego) i konfigurację serwera DNS w celu korzystania z uwierzytelniania.

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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Funkcja ograniczania użytkowników** lub **Zarządzanie ograniczeniami**.

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

5. Wybierz opcję **Uwierzytelnianie w usłudze Active Directory**.
6. Kliknij przycisk **Prześlij**.
7. Kliknij **Uwierzytelnianie w usłudze Active Directory**.
8. Skonfiguruj następujące ustawienia:

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

Opcja	Opis
Dane Faksu RX w pamięci masowej	Wybierz tę opcję, aby zapisać dane przychodzącego faksu. Można wydrukować wszystkie dane przychodzącego faksu po zalogowaniu się do urządzenia.
Zapamiętaj ID użytkownika	Wybierz tę opcję, aby zapisać swój identyfikator użytkownika.
Adres serwera Active Directory	Wpisz adres IP lub nazwę serwera Active Directory (na przykład: ad.przyklad.com).
Nazwa domeny Active Directory	Wpisz nazwę domeny aktywnego katalogu.
Protokół i metoda uwierzytelniania	Wybierz protokół i metodę uwierzytelniania.
SSL/TLS	Wybierz opcję **SSL/TLS**.
Port serwera LDAP	Wpisz numer portu, aby podłączyć serwer Active Directory za pośrednictwem protokołu LDAP (dostępnego tylko dla metody lub uwierzytelniania **LDAP + kerberos** lub **LDAP + NTLMv2**).

Opcja	Opis
Katalog główny wyszukiwania LDAP	Wpisz element główny wyszukiwania LDAP (dostępne tylko dla metody uwierzytelniania **LDAP + kerberos** lub **LDAP + NTLMv2**).
Pobierz adres e-mail	Wybierz tę opcję, aby uzyskać adres e-mail zalogowanego użytkownika z serwera Active Directory. (dostępne tylko dla metody uwierzytelnienia **LDAP + kerberos** lub **LDAP + NTLMv2**)
Pobierz katalog główny użytkownika	Wybierz tę opcję, aby wskazać swój główny katalog jako miejsce docelowe Skanowania do sieci. (dostępne tylko dla metody uwierzytelnienia **LDAP + kerberos** lub **LDAP + NTLMv2**)

9. Kliknij przycisk **Prześlij**.

Powiązane informacje

- Użycie uwierzytelniania Active Directory

Logowanie w celu zmiany ustawień urządzenia za pomocą panelu sterowania urządzenia (uwierzytelnienie Active Directory)

Gdy usługa uwierzytelnienia Active Directory jest włączona, panel sterowania urządzenia zostanie zablokowany do momentu wprowadzenia identyfikatora użytkownika i hasła w panelu sterowania urządzenia.

1. Na panelu sterowania urządzenia wprowadź identyfikator użytkownika i hasło, aby się zalogować.
2. Po pomyślnym uwierzytelnieniu panel sterowania urządzenia zostanie odblokowany.

Powiązane informacje

- Użycie uwierzytelniania Active Directory

Użyj uwierzytelniania LDAP

Wprowadzenie do uwierzytelnienia LDAP

Funkcja Uwierzytelniania LDAP ogranicza korzystanie z urządzenia. Jeśli włączone jest uwierzytelnianie LDAP, panel sterowania urządzenia zostanie zablokowany. Nie można zmienić ustawień urządzenia do momentu wprowadzenia przez użytkownika identyfikatora użytkownika i hasła.

Uwierzytelnianie LDAP oferuje następujące funkcje:

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

- Przechowywanie danych przychodzących drukowania
- Przechowywanie danych przychodzących faksów
- Pozyskiwanie adresu e-mail z serwera LDAP w oparciu o identyfikator użytkownika podczas przesyłania danych zeskanowanych na serwer poczty e-mail.

  Aby użyć tej funkcji, wybierz opcję **Wł.** w ustawieniu **Pobierz adres e-mail**. Twój adres e-mail będzie ustawiony jako nadawca, gdy urządzenie będzie przesyłać zeskanowane dane na serwer poczty e-mail, lub jako odbiorca, gdy będziesz wysyłać zeskanowane dane na swój adres e-mail.

Gdy uwierzytelnianie LDAP jest włączone, urządzenie zapisuje dane wszystkich przychodzących faksów. Po zalogowaniu się urządzenie wydrukuje zapisane dane faksów.

Ustawienie uwierzytelniania LDAP można zmienić za pomocą funkcji Zarządzanie przez interfejs webowy.

Powiązane informacje

- Użyj uwierzytelniania LDAP

Konfiguracja uwierzytelnienia LDAP za pomocą funkcji Zarządzanie 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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Funkcja ograniczania użytkowników** lub **Zarządzanie ograniczeniami**.

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

5. Wybierz **Uwierzytelnianie LDAP**.
6. Kliknij przycisk **Prześlij**.
7. Kliknij menu **Uwierzytelnianie LDAP**.
8. Skonfiguruj następujące ustawienia:

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

Opcja	Opis
Dane Faksu RX w pamięci masowej	Wybierz tę opcję, aby zapisać dane przychodzącego faksu. Można wydrukować wszystkie dane przychodzącego faksu po zalogowaniu się do urządzenia.
Zapamiętaj ID użytkownika	Wybierz tę opcję, aby zapisać swój identyfikator użytkownika.
Adres serwera LDAP	Wpisz adres IP lub nazwę serwera LDAP (na przykład: ldap.przyklad.com).
SSL/TLS	Wybierz opcję **SSL/TLS**, aby korzystać z LDAP przez SSL/TLS.
Port serwera LDAP	Wpisz numer portu serwera LDAP.
Katalog główny wyszukiwania LDAP	Wpisz katalog główny wyszukiwania LDAP.
Atrybut nazwy (Klucz wyszukiwania)	Wpisz atrybut, którego chcesz używać jako klucza wyszukiwania.
Pobierz adres e-mail	Wybierz tę opcję, aby uzyskać adres e-mail zalogowanego użytkownika z serwera LDAP.
Pobierz katalog główny użytkownika	Wybierz tę opcję, aby wskazać swój główny katalog jako miejsce docelowe Skanowania do sieci.

9. Kliknij przycisk **Prześlij**.

Powiązane informacje

- Użyj uwierzytelniania LDAP

Logowanie w celu zmiany ustawień urządzenia za pomocą panelu sterowania urządzenia (Uwierzytelnianie LDAP)

Gdy uwierzytelnianie LDAP jest włączone, panel sterowania urządzenia zostanie zablokowany do momentu wprowadzenia identyfikatora użytkownika i hasła w panelu sterowania urządzenia.

1. Na panelu sterowania urządzenia wprowadź identyfikator użytkownika i hasło, aby się zalogować.
2. Po pomyślnym uwierzytelnieniu panel sterowania urządzenia zostanie odblokowany.

Powiązane informacje

- Użyj uwierzytelniania LDAP

Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Opcja Secure Function Lock 3.0 (Blokada funkcji 3.0) zwiększa bezpieczeństwo dzięki ograniczeniu dostępu do funkcji urządzenia.

Przed użyciem opcji Secure Function Lock 3.0

Za pomocą opcji Secure Function Lock (Blokada funkcji) można konfigurować hasła, ustawiać określone limity stron użytkowników i przyznawać dostęp do niektórych lub wszystkich funkcji wymienionych poniżej.

Następujące ustawienia opcji Secure Function Lock 3.0 można konfigurować i zmieniać przy użyciu funkcji Zarządzanie przez interfejs webowy:

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

- **Drukuj**
- **Kopiuj**
- **Skanuj**
- **Faks**
- **Nośnik**
- **Web Connect**
- **Aplikacje**
- **Limity stron**
- **Liczniki stron**
- **ID karty (ID NFC)**

Modele z ekranem dotykowym LCD:

Gdy włączona jest funkcja Secure Function Lock, urządzenie automatycznie przechodzi w tryb publiczny, a niektóre funkcje urządzenia zostają ograniczone wyłącznie do autoryzowanych użytkowników. Aby uzyskać dostęp do zastrzeżonych funkcji urządzenia, naciśnij , wybierz nazwę użytkownika i wprowadź hasło.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Konfigurowanie opcji Secure Function Lock 3.0 przy użyciu funkcji Zarządzanie 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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Funkcja ograniczania użytkowników** lub **Zarządzanie ograniczeniami**.

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

5. Wybierz **Bezpieczna blokada funkcji**.
6. Kliknij przycisk **Prześlij**.
7. Kliknij menu **Funkcje ograniczone**.
8. Skonfiguruj ustawienia zarządzania ograniczeniami dla użytkowników lub grup.
9. Kliknij przycisk **Prześlij**.
10. Kliknij menu **Lista użytkowników**.
11. Skonfiguruj listę użytkowników.
12. Kliknij przycisk **Prześlij**.

Ustawienia blokady listy użytkowników można także zmienić w menu **Bezpieczna blokada funkcji**.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Skanowanie przy użyciu opcji Secure Function Lock 3.0

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

Ograniczenia ustawienia skanowania (dla administratorów)

Opcja Secure Function Lock 3.0 (Blokada funkcji 3.0) umożliwia administratorowi ograniczenie grupy użytkowników, którym wolno skanować. Kiedy funkcja skanowania przez użytkowników publicznych jest wyłączona, skanować będą mogli tylko ci użytkownicy, którzy mają zaznaczone pole wyboru odpowiadające opcji **Skanuj**.

Korzystanie z funkcji skanowania (dla użytkowników z ograniczeniami)

- Aby skanować za pomocą panelu sterowania urządzenia:

  Aby uzyskać dostęp do trybu skanowania, użytkownik z ograniczeniami musi wprowadzić swoje hasło na panelu sterowania urządzenia.
- Aby skanować z komputera:

  Przed rozpoczęciem skanowania ze swojego komputera użytkownik z ograniczeniami musi wprowadzić swoje hasło na panelu sterowania urządzenia. Jeśli hasło nie zostanie wprowadzone na panelu sterowania urządzenia, na komputerze użytkownika zostanie wyświetlony komunikat o błędzie.

Jeśli urządzenie obsługuje uwierzytelnianie przy użyciu karty elektronicznej, użytkownicy z ograniczeniami mogą także uzyskać dostęp do trybu skanowania, dotykając symbolu NFC na panelu sterowania urządzenia swoją kartą elektroniczną.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Konfigurowanie trybu publicznego opcji Secure Function Lock 3.0

Na ekranie opcji Secure Function Lock (Blokada funkcji) można skonfigurować tryb publiczny, który ogranicza dostęp do funkcji przez użytkowników publicznych. Użytkownicy publiczni nie muszą wprowadzać hasła, aby korzystać z funkcji udostępnionych za pomocą ustawień trybu publicznego.

Tryb publiczny obejmuje zadania drukowania wysyłane za pośrednictwem Brother iPrint&Scan i Brother Mobile Connect.

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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Funkcja ograniczania użytkowników** lub **Zarządzanie ograniczeniami**.

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

5. Wybierz opcję **Bezpieczna blokada funkcji**.
6. Kliknij przycisk **Prześlij**.
7. Kliknij menu **Funkcje ograniczone**.
8. Zaznacz pole wyboru w wierszu **Tryb publiczny**, aby zezwolić na użycie wymienionej funkcji, ewentualnie usuń zaznaczenie pola, aby ograniczyć możliwość jej użycia.
9. Kliknij przycisk **Prześlij**.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Konfigurowanie osobistych ustawień ekranu głównego za pomocą funkcji Zarządzanie przez interfejs webowy

Jako administrator możesz określić, które karty mogą wyświetlać na swoich osobistych ekranach głównych użytkownicy. Karty te zapewniają szybki dostęp do ulubionych skrótów użytkowników, które mogą przypisywać do kart swoich osobistych ekranów głównych z poziomu panelu sterowania urządzenia.

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

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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Funkcja ograniczania użytkowników** lub **Zarządzanie ograniczeniami**.

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

5. Wybierz **Bezpieczna blokada funkcji**.
6. W polu **Ustawienia kart** wybierz **Osobiste** dla nazw kart, których chcesz używać jako swoje osobiste ekrany główne.
7. Kliknij przycisk **Prześlij**.
8. Kliknij menu **Funkcje ograniczone**.
9. Skonfiguruj ustawienia zarządzania ograniczeniami dla użytkowników lub grup.
10. Kliknij przycisk **Prześlij**.
11. Kliknij menu **Lista użytkowników**.
12. Skonfiguruj listę użytkowników.
13. Wybierz **Lista użytkowników/ograniczone funkcje** z listy rozwijanej dla każdego użytkownika.
14. Wybierz nazwę karty z listy rozwijanej **Ekran główny** dla każdego użytkownika.
15. Kliknij przycisk **Prześlij**.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Dodatkowe funkcje opcji Secure Function Lock 3.0

Na ekranie opcji Secure Function Lock można skonfigurować następujące funkcje:

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

Reset wszyst. liczników

Kliknij opcję **Reset wszyst. liczników** w kolumnie **Liczniki stron**, aby zresetować licznik stron.

Eksportuj do pliku CSV

Kliknij **Eksportuj do pliku CSV**, aby eksportować bieżący i ostatni licznik stron wraz z informacjami **Lista użytkowników/ograniczone funkcje** do pliku CSV.

ID karty (ID NFC)

Kliknij menu **Lista użytkowników**, a następnie wpisz identyfikator karty użytkownika w polu **ID karty (ID NFC)**. Można użyć swojej karty elektronicznej do uwierzytelniania.

Wyjście

Jeśli w urządzeniu zainstalowany jest moduł sortera, wybierz z listy rozwijanej tacę wyjściową dla każdego użytkownika.

Ostatni rekord licznika

Kliknij opcję **Ostatni rekord licznika**, aby urządzenie zachowało informacje o liczbie stron po zresetowaniu licznika.

Autom. resetowanie licznika

Kliknij opcję **Autom. resetowanie licznika**, aby skonfigurować odstęp czasu między resetowaniami licznika stron. Można wybrać interwał dzienny, tygodniowy lub miesięczny.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Zarejestruj nową kartę IC przez panel sterowania urządzenia

W urządzeniu można rejestrować karty mikroprocesorowe (karty IC).

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

1. Dotknij zarejestrowaną kartą ze zintegrowanym układem scalonym (kartą elektroniczną) symbolu NFC (Near Field Communication — komunikacja bliskiego zasięgu) na panelu sterowania urządzenia.
2. Naciśnij swój identyfikator użytkownika na wyświetlaczu LCD.
3. Naciśnij przycisk Register Card (Zarejestruj kartę).
4. Dotknij nową kartą elektroniczną symbolu NFC.

   Numer nowej karty elektronicznej zostanie zarejestrowany w urządzeniu.
5. Naciśnij przycisk OK.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Zarejestruj zewnętrzny czytnik kart IC

Po podłączeniu zewnętrznego czytnika kart IC (Integrated Circuit) zarejestruj go przy użyciu funkcji Zarządzanie przez interfejs webowy. To urządzenie obsługuje zewnętrzne czytniki kart IC z obsługą sterowników klasy HID.

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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Zewnętrzny czytnik kart**.

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

5. Wprowadź wymagane informacje, a następnie kliknij **Prześlij**.
6. Uruchom ponownie urządzenie Brother, aby aktywować konfigurację.
7. Podłącz czytnik kart do urządzenia.
8. Dotknij kartą czytnik kart podczas korzystania z funkcji uwierzytelniania kartą.

Powiązane informacje

- Użycie opcji Secure Function Lock 3.0 (Blokada funkcji 3.0)

Bezpieczne wysyłanie i odbieranie wiadomości e-mail

Konfiguracja wysyłania i odbierania wiadomości e-mail przy użyciu funkcji Zarządzanie przez interfejs webowy

- Funkcja odbierania wiadomości e-mail jest dostępna tylko w niektórych modelach.
- Do konfigurowania bezpiecznego wysyłania wiadomości e-mail z uwierzytelnianiem użytkownika lub wysyłania i odbierania wiadomości e-mail z użyciem protokołu SSL/TLS zalecamy używanie funkcji Zarządzanie przez interfejs webowy (tylko obsługiwane modele).

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 **Zaloguj**, a następnie kliknij **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 **Sieć** > **Sieć** > **Protokół**.

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

5. W polu **Klient POP3/IMAP4/SMTP** kliknij opcję **Ustawienia zaawansowane**, a następnie upewnij się, że dla opcji **Klient POP3/IMAP4/SMTP** zostało wybrane ustawienie **Włączone**.

- Obsługa konkretnych protokołów zależy od urządzenia.
- Jeśli zostanie wyświetlony ekran wyboru **Metoda uwierz.**, wybierz metodę uwierzytelniania, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

6. Skonfiguruj ustawienia **Klient POP3/IMAP4/SMTP**.
   - Potwierdź poprawność konfiguracji poczty e-mail, wysyłając testową wiadomość e-mail.
   - Jeśli ustawienia serwera POP3/IMAP4/SMTP nie są znane, skontaktuj się z administratorem sieci lub dostawcą usług internetowych (ISP).
7. Po zakończeniu kliknij **Prześlij**.

   Zostanie wyświetlone okno dialogowe **Test konfig. wysyłania/odbierania wiad. e-mail**.
8. Wykonaj instrukcje wyświetlane w oknie dialogowym, aby przetestować bieżące ustawienia.

Powiązane informacje

- Bezpieczne wysyłanie i odbieranie wiadomości e-mail

Powiązane tematy:

- Bezpieczne wysyłanie i odbieranie wiadomości e-mail z użyciem protokołu SSL/TLS

Wysyłanie wiadomości e-mail z uwierzytelnianiem użytkownika

Urządzenie wysyła wiadomości e-mail za pośrednictwem serwera e-mail, które wymaga uwierzytelnienia użytkownika. Ta metoda uniemożliwia dostęp nieautoryzowanym użytkowników do serwera poczty e-mail.

Korzystając z funkcji uwierzytelniania użytkownika, można wysyłać powiadomienia i raporty pocztą e-mail oraz faksy internetowe (funkcja dostępna tylko w niektórych modelach).

- Obsługa konkretnych protokołów zależy od urządzenia.
- Zalecamy używanie funkcji Zarządzanie przez interfejs webowy do konfigurowania metody uwierzytelniania SMTP.

Ustawienia serwera poczty e-mail

Należy skonfigurować w urządzeniu tę samą metodę uwierzytelniania SMTP, która jest stosowana na serwerze poczty e-mail. Aby uzyskać szczegółowe informacje dotyczące ustawień serwera poczty e-mail, skontaktuj się z administratorem sieci lub dostawcą usług internetowych (Internet Service Provider, ISP).

Aby włączyć uwierzytelnianie serwera SMTP przy użyciu funkcji zarządzanie przez interfejs webowy, wybierz metodę uwierzytelniania **Metoda uwierz. serwera** na ekranie **Klient POP3/IMAP4/SMTP**.

Powiązane informacje

- Bezpieczne wysyłanie i odbieranie wiadomości e-mail

Bezpieczne wysyłanie i odbieranie wiadomości e-mail z użyciem protokołu SSL/TLS

To urządzenie obsługuje protokoły komunikacyjne SSL/TLS. Aby użyć serwera poczty e-mail korzystającego z protokołu SSL/TLS, należy skonfigurować następujące ustawienia.

- Funkcja odbierania wiadomości e-mail jest dostępna tylko w niektórych modelach.
- Do konfigurowania protokołów SSL/TLS zalecamy używanie funkcji Zarządzanie przez interfejs webowy.

Weryfikowanie certyfikatu serwera

Jeśli w obszarze **SSL/TLS** została wybrana opcja **SSL** lub **TLS**, wówczas pole wyboru **Zweryfikuj certyfikat serwera** zostanie zaznaczone automatycznie.

- 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.
- Jeśli weryfikacja certyfikatu serwera nie jest potrzebna, usuń zaznaczenie pola wyboru **Zweryfikuj certyfikat serwera**.

Numer portu

Jeśli zostanie wybrana opcja **SSL** lub **TLS**, wartość **Port** zostanie zmieniona na odpowiednią dla danego protokołu. Aby zmienić numer portu ręcznie, wybierz opcję **SSL/TLS**, a następnie wpisz numer portu.

Należy skonfigurować w urządzeniu tę samą metodę komunikacji, która jest stosowana na serwerze poczty e-mail. Aby uzyskać szczegółowe informacje dotyczące ustawień serwera poczty e-mail, skontaktuj się z administratorem sieci lub dostawcą usług internetowych (ISP).

W większości przypadków zabezpieczone usługi pocztowe wymagają następujących ustawień:

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

SMTP	**Port**	587
	Metoda uwierz. serwera	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Powiązane informacje

- Bezpieczne wysyłanie i odbieranie wiadomości e-mail

Powiązane tematy:

- Konfiguracja wysyłania i odbierania wiadomości e-mail przy użyciu funkcji Zarządzanie przez interfejs webowy
- Konfiguracja certyfikatów bezpieczeństwa urządzenia

Zapisywanie dziennika druku w sieci

- Zapisz dziennik drukowania w Przeglądzie sieci
- Konfigurowanie funkcji zapisywania dziennika druku w sieci za pomocą funkcji Zarządzanie przez interfejs webowy
- Użycie ustawienia funkcji wykrywania błędów dla funkcji zapisywania dziennika druku w sieci
- Korzystanie z funkcji zapisywania dziennika druku w sieci z zastosowaniem funkcji Secure Function Lock 3.0

Zapisz dziennik drukowania w Przeglądzie sieci

Funkcja zapisywania dziennika druku w sieci umożliwia zapisanie pliku z dziennikiem druku urządzenia na serwerze sieciowym przy użyciu protokołu CIFS (Common Internet File System). Dla każdego zadania można zapisać identyfikator, typ zadania drukowania, nazwę zadania, nazwę użytkownika, datę, czas oraz liczbę drukowanych stron. CIFS to protokół pracujący w oparciu o protokół TCP/IP, który umożliwia komputerom w sieci współdzielenie plików w sieci intranet lub w Internecie.

W dzienniku druku zapisywane są następujące funkcje druku:

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

- Zadania drukowania z komputera
- Drukowanie bezpośrednie z użyciem USB
- Kopiowanie
- Odebrany faks
- Druk Web Connect

- Funkcja zapisywania dziennika druku w sieci obsługuje uwierzytelnianie Kerberos oraz NTLMv2. W celu uwierzytelniania konieczne jest skonfigurowanie protokołu SNTP (serwera czasu sieciowego) lub prawidłowe ustawienie daty, czasu i strefy czasowej na panelu sterowania.
- Przy zapisywaniu pliku na serwerze typ pliku można ustawić na TXT lub CSV.

Powiązane informacje

- Zapisywanie dziennika druku w sieci

Konfigurowanie funkcji zapisywania dziennika druku w sieci za pomocą funkcji Zarządzanie 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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Przechowuj dziennik drukowania w sieci**.

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

5. W polu **Dziennik drukowania** kliknij **Wł.**.
6. Skonfiguruj następujące ustawienia:

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

Opcja	Opis
Ścieżka folderu sieciowego	Wpisz folder docelowy na serwerze CIFS, na którym ma zostać zapisany dziennik druku (np. \\NazwaKomputera\FolderUdostępniony).
Nazwa pliku	Wpisz nazwę pliku, której chcesz używać dla dziennika druku (do 32 znaków).
Typ pliku	Wybierz opcję **TXT** lub **CSV** typu pliku dziennika druku.
Źródło czasu dla dziennika	Wybierz źródło czasu dla dziennika drukowania.
Metoda uwierzyt.	Wybierz metodę uwierzytelniania wymaganą w celu uzyskania dostępu do serwera CIFS: **Autom.**, **Kerberos** lub **NTLMv2**. Kerberos to protokół uwierzytelniania, umożliwiający serwerom sieciowym sprawdzanie tożsamości urządzeń lub użytkowników poprzez jedno logowanie. NTLMv2 to metoda uwierzytelniania używana w systemach Windows do logowania na serwery. • **Autom.**: Jeżeli zostanie wybrana opcja **Autom.**, do metody uwierzytelniania zostanie wykorzystany protokół NTLMv2. • **Kerberos**: Wybierz opcję **Kerberos**, aby używać wyłącznie uwierzytelniania Kerberos. • **NTLMv2**: Wybierz opcję **NTLMv2**, aby używać wyłącznie uwierzytelniania NTLMv2. • W celu stosowania uwierzytelniania **Kerberos** i **NTLMv2** konieczne jest również skonfigurowanie ustawień **Data i godzina** lub protokołu SNTP (serwera czasu sieciowego) i serwera DNS. • Ustawienia daty i godziny można również konfigurować za pomocą panelu sterowania urządzenia.

Opcja	Opis
Nazwa użytkow.	Wpisz nazwę użytkownika dla uwierzytelniania (do 96 znaków). Jeśli nazwa użytkownika jest częścią domeny, wprowadź ją w jednym z następujących formatów: użytkownik@domena lub domena\użytkownik.
Hasło	Wpisz hasło dla uwierzytelniania (do 32 znaków).
Adres serwera Kerberos (jeśli jest potrzebne)	Wpisz adres hosta KDC (ang. Key Distribution Center) (np. kerberos.przyklad.com, maks. 64 znaki) lub adres IP (np. 192.168.56.189).
Ustawienie wykrywania błędów	Wybierz, jaka operacja ma być wykonywana, gdy nie można zapisać dziennika druku na serwerze z powodu błędu sieci.

7. W polu **Stan połączenia** potwierdź stan ostatniego logowania.

Możesz również potwierdzić stan błędu na wyświetlaczu LCD urządzenia.

8. Kliknij przycisk **Prześlij**, aby wyświetlić stronę **Testuj dziennik drukowania w sieci**.

   Aby przetestować ustawienia, kliknij przycisk **Tak**, a następnie przejdź do kolejnego kroku.

   Aby pominąć test, kliknij **Nie**. Ustawienia zostaną wysłane automatycznie.
9. Urządzenie przetestuje ustawienia.
10. Jeśli ustawienia zostaną zaakceptowane, na ekranie wyświetlony zostanie komunikat **Test OK**.

    Jeśli wyświetlony zostanie komunikat **Błąd testu** należy sprawdzić wszystkie ustawienia, a następnie kliknąć **Prześlij** w celu ponownego wyświetlenia strony testu.

Powiązane informacje

- Zapisywanie dziennika druku w sieci

Użycie ustawienia funkcji wykrywania błędów dla funkcji zapisywania dziennika druku w sieci

Użycie funkcji wykrywania błędów w celu określenia, jaka operacja ma być wykonywana, gdy nie można zapisać dziennika druku na serwerze z powodu błędu sieci.

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 **Zaloguj**, a następnie kliknij **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 **Administrator** > **Przechowuj dziennik drukowania w sieci**.

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

5. W sekcji **Ustawienie wykrywania błędów** wybierz opcję **Anuluj drukowanie** lub **Ignoruj dziennik i drukuj**.

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

Opcja	Opis
Anuluj drukowanie	W przypadku wyboru opcji **Anuluj drukowanie** zadania druku będą anulowane, gdy nie będzie można zapisać dziennika druku na serwerze. Nawet w przypadku wybrania opcji **Anuluj drukowanie**, urządzenie będzie drukowało odbierane faksy.

Ignoruj dziennik i drukuj	W przypadku wybrania opcji **Ignoruj dziennik i drukuj** urządzenie wydrukuje dokumentację, nawet jeśli nie będzie można zapisać dziennika druku na serwerze.
	Po przywróceniu działania funkcji zapisywania dziennika druku jest on zapisywany w następujący sposób:
	`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. Jeśli nie można zapisać dziennika druku na końcu zadania drukowania, liczba wydrukowanych stron nie zostanie zarejestrowana.
	b. Jeśli nie można zapisać dziennika druku na początku i na końcu zadania drukowania, dziennik druku dla tego zadania nie zostanie zarejestrowany. Po przywróceniu funkcji błąd zostanie umieszczony w dzienniku druku.

6. Kliknij przycisk **Prześlij**, aby wyświetlić stronę **Testuj dziennik drukowania w sieci**.

   Aby przetestować ustawienia, kliknij przycisk **Tak**, a następnie przejdź do kolejnego kroku.

   Aby pominąć test, kliknij **Nie**. Ustawienia zostaną wysłane automatycznie.

7. Urządzenie przetestuje ustawienia.
8. Jeśli ustawienia zostaną zaakceptowane, na ekranie wyświetlony zostanie komunikat **Test OK**.

   Jeśli wyświetlony zostanie komunikat **Błąd testu** należy sprawdzić wszystkie ustawienia, a następnie kliknąć **Prześlij** w celu ponownego wyświetlenia strony testu.

Powiązane informacje

- Zapisywanie dziennika druku w sieci

Korzystanie z funkcji zapisywania dziennika druku w sieci z zastosowaniem funkcji Secure Function Lock 3.0

Gdy funkcja Secure Function Lock (Blokada funkcji) 3.0 jest aktywna, nazwy zarejestrowanych użytkowników dla kopiowania, odbierania faksów, druku Web Connect i druku bezpośredniego przez USB będą zapisywane w raporcie zapisywania dziennika druku w sieci. Gdy włączone jest uwierzytelnianie Active Directory, nazwa użytkownika jest rejestrowana w raporcie zapisywania dziennika druku w sieci:

Dostępne funkcje, opcje i ustawienia mogą się różnić w zależności 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
```

Powiązane informacje

- Zapisywanie dziennika druku w sieci

brother

Brother Earth

www.brotherearth.com

POL
Wersja 0