



DS-900WN DS-800WN

Przewodnik administratora

Zalecane ustawienia przeznaczone do żadanego celu

Ustawienia sieciowe

Ustawienia niezbędne do skanowania

Podstawowe ustawienia zabezpieczeń

Zaawansowane ustawienia bezpieczeństwa

Korzystanie z funkcji Epson Open Platform

Prawa autorskie

Żadnej części tej publikacji nie można powielać, przechowywać w systemach wyszukiwania ani przesyłać w jakiegokolwiek formie lub w jakikolwiek sposób elektronicznie, mechanicznie, przez fotokopiowanie, nagrywanie lub inny sposób bez uprzedniej pisemnej zgody firmy Seiko Epson Corporation. Nie przewiduje się odpowiedzialności z tytułu naruszenia praw patentowych w związku z wykorzystaniem informacji zawartych w niniejszym dokumencie. Firma nie przyjmuje też odpowiedzialności za szkody wynikające z użycia informacji zawartych w niniejszym dokumencie. Informacje w tej publikacji są przeznaczone wyłącznie do użycia wraz z produktami firmy Epson. Firma Epson nie ponosi odpowiedzialności za użycie tych informacji względem innych produktów.

Firma Seiko Epson Corporation ani jej podmioty powiązane nie ponoszą odpowiedzialności wobec kupującego lub podmiotów trzecich z tytułu szkód, strat, kosztów lub wydatków poniesionych przez kupującego lub podmioty trzecie w wyniku wypadku, niewłaściwego użycia lub nadużycia tego produktu lub niezatwierdzonych modyfikacji, napraw lub zmian tego produktu lub (wykluczając Stany Zjednoczone) nieprzestrzegania instrukcji obsługi i konserwacji firmy Seiko Epson Corporation.

Firma Seiko Epson Corporation i jej podmioty powiązane nie ponoszą odpowiedzialności za jakiegokolwiek szkody lub problemy wynikające z użycia wyposażenia opcjonalnego lub materiałów eksploatacyjnych innych niż te oznaczone jako oryginalne produkty firmy Epson lub produkty dopuszczone przez firmę Seiko Epson Corporation.

Firma Seiko Epson Corporation nie ponosi odpowiedzialności za jakiegokolwiek szkody spowodowane zakłóceniami elektromagnetycznymi, które wynikają z użycia kabli interfejsu innych niż te oznaczone jako produkty dopuszczone przez firmę Seiko Epson Corporation.

© 2024 Seiko Epson Corporation

Zawartość tej instrukcji obsługi i dane techniczne tego produktu mogą zostać zmienione bez uprzedniego powiadomienia.

Znaki towarowe

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Uwaga ogólna: wszystkie inne znaki towarowe są własnością odpowiednich właścicieli i używane wyłącznie w celach identyfikacyjnych.

Spis treści

Prawa autorskie

Znaki towarowe

Wprowadzenie

Zawartość tego dokumentu.	8
Korzystanie z tej instrukcji.	8
Oznaczenia i symbole.	8
Opisy zastosowane w niniejszym podręczniku.	8
Odniesienia do systemów operacyjnych.	8

Informacje dotyczące hasła administratora

Informacje dotyczące hasła administratora.	11
Początkowe hasło administratora.	11
Operacje wymagające hasła administratora.	11
Zmiana hasła administratora.	11
Resetowanie hasła administratora.	11

Zalecane ustawienia przeznaczone do żądanego celu

Zalecane ustawienia przeznaczone do żądanego celu.	13
--	----

Ustawienia sieciowe

Łączenie skanera z siecią.	16
Czynności do wykonania przed nawiązaniem połączenia sieciowego.	16
Łączenie drukarki z siecią z poziomu panelu sterowania.	18
Dodawanie lub wymienianie komputera lub urządzeń.	22
Nawiązywanie połączenia ze skanerem połączonym z siecią.	22
Nawiązywanie bezpośredniego połączenia między urządzeniem inteligentnym a skanerem (Wi-Fi Direct).	24
Ponowna konfiguracja połączenia sieciowego.	26
Sprawdzanie stanu połączenia sieciowego.	28
Sprawdzanie stanu połączenia sieciowego za pomocą panelu sterowania.	28
Dane techniczne sieci.	30
Specyfikacje Wi-Fi.	30

Dane techniczne Ethernet.	31
Funkcje sieciowe i obsługa IPv4/IPv6.	32
Protokół bezpieczeństwa.	32
Używanie portów na skanerze.	32
Rozwiązywanie problemów.	34
Nie można połączyć się z siecią.	34

Oprogramowanie do konfigurowania skanera

Aplikacja konfiguracji obsługi skanera (Web Config).	38
Uruchamianie aplikacji Web Config w przeglądarce internetowej.	38
Epson Device Admin.	39
Szablon konfiguracji.	40

Ustawienia niezbędne do skanowania

Rejestrowanie serwera poczty e-mail.	45
Sprawdzanie połączenie serwera e-mail.	46
Tworzenie folderu sieciowego.	48
Udostępnianie kontaktów.	55
Porównanie możliwych konfiguracji kontaktów.	56
Rejestrowanie miejsca docelowego w kontaktach za pomocą aplikacji Web Config.	56
Rejestrowanie miejsc docelowych jako grupy z użyciem Web Config.	58
Tworzenie kopii zapasowej kontaktów i ich importowanie.	59
Eksportowanie i importowanie wielu kontaktów za pomocą narzędzia.	60
Obsługa użytkowników i serwera LDAP.	62
Konfiguracja funkcji AirPrint.	65
Problemy podczas przygotowywania skanowania sieciowego.	66
Wskazówki dotyczące rozwiązywania problemów.	66
Nie można uzyskać dostępu do aplikacji Web Config.	66

Dostosowanie wyświetlacza panelu sterowania

Rejestrowanie Wstępne.	70
Opcje menu Wstępne.	71

Edycja ekranu głównego panelu sterowania.	72
Zmiana ustawień Układ ekranu głównego.	72
Dodaj ikonę.	73
Usuń ikonę.	74
Przenieś ikonę.	75

Podstawowe ustawienia zabezpieczeń

Wprowadzenie do funkcji zabezpieczeń produktu.	77
Ustawienia administratora.	77
Konfigurowanie hasła administratora.	77
Korzystanie z funkcji Zablokuj ustawienie na panelu sterowania.	79
Logowanie na konto administratora z poziomu panelu sterowania.	83
Ograniczanie dostępnych funkcji (Kontrola dostępu).	83
Tworzenie konta użytkownika.	83
Włączanie funkcji Kontrola dostępu.	85
Logowanie do skanera, na którym włączono funkcję Kontrola dostępu.	85
Wyłączanie interfejsu zewnętrznego.	85
Włączanie weryfikacji programu podczas uruchamiania.	86
Wyłączanie skanowania sieciowego z komputera.	86
Włączanie lub wyłączanie funkcji skanowania WSD.	87
Monitorowanie zdalnego skanera.	87
Sprawdzanie informacji o skanerze zdalnym.	87
Otrzymywanie powiadomień e-mail w przypadku występowania zdarzeń.	88
Sterowanie zasilaniem skanera przy użyciu aplikacji Web Config.	89
Przywracanie ustawień domyślnych.	89
Informacje o Epson Remote Services.	90
Rozwiązywanie problemów.	90
Zapomnienie hasła administratora.	90

Zaawansowane ustawienia bezpieczeństwa

Ustawienia zabezpieczeń i zapobieganie niebezpieczeństwom.	92
Ustawienia funkcji zabezpieczeń.	93
Kontrola użycia protokołów.	93
Kontrola dostępu do protokołów.	93
Protokoły, które można włączyć lub wyłączyć.	94
Opcje ustawień protokołów.	94

Używanie certyfikatu cyfrowego.	96
Informacje o certyfikatach cyfrowych.	96
Konfiguracja Certyfikat CA.	97
Aktualizowanie certyfikatu z podpisem własnym.	100
Konfiguracja Certyfikat CA.	101
Komunikacja SSL/TLS ze skanerem.	102
Konfiguracja podstawowych ustawień SSL/TLS	102
Konfigurowanie certyfikatu serwera na potrzeby skanera.	103
Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP.	103
Informacje o IPsec/Filtrowanie IP.	103
Konfigurowanie zasad domyślnych.	103
Konfigurowanie zasad grupowych.	107
Przykłady konfiguracji opcji IPsec/Filtrowanie IP.	114
Konfiguracja certyfikatu dla IPsec/filtrowania IP.	115
Podłączanie skanera do sieci IEEE802.1X.	115
Konfigurowanie sieci IEEE 802.1X.	115
Konfiguracja certyfikatu dla IEEE 802.1X.	117
Rozwiązywanie problemów związanych z zaawansowanymi zabezpieczeniami.	117
Przywracanie ustawień zabezpieczeń.	117
Problemy z korzystaniem z funkcji zabezpieczeń sieciowych.	117
Problemy z używaniem certyfikatu cyfrowego.	119

Korzystanie z funkcji Epson Open Platform

Opis platformy Epson Open Platform.	125
Konfigurowanie platformy Epson Open Platform.	125
Weryfikacja platformy Epson Open Platform.	125

Mocowanie urządzenia uwierzytelniającego

Podłączenie urządzenia uwierzytelniającego.	128
Sprawdzenie działania urządzenia uwierzytelniającego.	128
Potwierdzanie rozpoznania karty uwierzytelniającej.	128
Rozwiązywanie problemów związanych z urządzeniem uwierzytelniającym.	129
Nie można odczytać karty uwierzytelniającej.	129

Konserwacja

Czyszczenie zewnętrznej części skanera.	131
Czyszczenie wnętrza skanera.	131
Wymiana zestawu montażowego rolek.	136
Kody zestawu montażowego rolek.	141
Zerowanie liczby wykonanych skanów po wymianie wałków.	141
Oszczędzanie energii.	142
Przenoszenie skanera.	142
Tworzenie kopii zapasowej ustawień.	143
Eksport ustawień.	143
Importowanie ustawień.	144
Przywr. ust. domyśl.	144
Aktualizacja aplikacji i oprogramowania sprzętowego.	145
Aktualizowanie oprogramowania układowego skanera za pomocą panelu sterowania.	146
Aktualizowanie oprogramowania układowego za pomocą narzędzia Web Config. .	146
Aktualizowanie oprogramowania układowego bez nawiązywania połączenia z Internetem.	147

Wprowadzenie

Zawartość tego dokumentu.	8
Korzystanie z tej instrukcji.	8

Zawartość tego dokumentu

W tym dokumencie przedstawiono następujące informacje dla administratorów skanera.

- Ustawienia sieciowe
- Przygotowywanie funkcji skanowania
- Włączanie i zarządzanie ustawieniami bezpieczeństwa
- Wykonywanie codziennej konserwacji

Aby uzyskać więcej informacji o standardowych metodach obsługi skanera, patrz *Przewodnik użytkownika*.

Korzystanie z tej instrukcji

Oznaczenia i symbole



Przeestroga:

Instrukcje, których należy dokładnie przestrzegać w celu uniknięcia obrażeń ciała.



Ważne:

Instrukcje, których należy przestrzegać w celu uniknięcia uszkodzenia sprzętu.

Uwaga:

Znajdują się tu informacje dodatkowe i referencyjne.

Powiązane informacje

➔ Łączy do części powiązanych.

Opisy zastosowane w niniejszym podręczniku

- Zdjęcia ekranów aplikacji pochodzą z Windows 10 lub macOS High Sierra. Treść wyświetlana na ekranach jest różna, zależnie od modelu i sytuacji.
- Ilustracje zamieszczone w podręczniku mają wyłącznie charakter poglądowy. Chociaż mogą się one różnić nieznacznie od rzeczywistego produktu, sposoby obsługi są identyczne.

Odniesienia do systemów operacyjnych

Windows

W tym podręczniku takie określenia jak „Windows 11”, „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Server 2022”, „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2” i „Windows Server 2008” odnoszą się do następujących systemów operacyjnych. Oprócz tego określenie „Windows” stosowane jest w odniesieniu do wszystkich wersji.

- System operacyjny Microsoft® Windows® 11
- System operacyjny Microsoft® Windows® 10
- System operacyjny Microsoft® Windows® 8.1
- System operacyjny Microsoft® Windows® 8
- System operacyjny Microsoft® Windows® 7
- System operacyjny Microsoft® Windows Server® 2022
- System operacyjny Microsoft® Windows Server® 2019
- System operacyjny Microsoft® Windows Server® 2016
- System operacyjny Microsoft® Windows Server® 2012 R2
- System operacyjny Microsoft® Windows Server® 2012
- System operacyjny Microsoft® Windows Server® 2008 R2
- System operacyjny Microsoft® Windows Server® 2008

Mac OS

W tym podręczniku, nazwa "Mac OS" odnosi się do systemu Mac OS X 10.9 lub wersji nowszej, a także do macOS 11 lub wersji nowszej.

Informacje dotyczące hasła administratora

Informacje dotyczące hasła administratora.	11
Początkowe hasło administratora.	11
Operacje wymagające hasła administratora.	11
Zmiana hasła administratora.	11
Resetowanie hasła administratora.	11

Informacje dotyczące hasła administratora

Urządzenie pozwala na ustawienie hasła administratora, aby zapobiec nieautoryzowanemu dostępowi osób trzecich lub zmianie ustawień urządzenia lub ustawień sieciowych zapisanych na urządzeniu, gdy jest ono połączone z siecią.

Jeśli hasło administratora zostało ustawione, trzeba wprowadzić hasło w przypadku zmiany ustawień w oprogramowaniu konfiguracyjnym, takim jak Web Config.

Na skanerze zostanie ustawione początkowe hasło administratora, ale można je dowolnie zmienić.

Początkowe hasło administratora

Początkowe hasło administratora jest różne w zależności od etykiety na produkcie. Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer. Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź numer seryjny znajdujący się na etykiecie przyklejonej z tyłu produktu.

Zaleca się zmianę początkowego hasła administratora.

Uwaga:

Żadna nazwa użytkownika nie jest ustawiona jako domyślna.

Operacje wymagające hasła administratora

Jeśli zostanie wyświetlony monit o wprowadzenie hasła administratora w trakcie operacji poniżej, wprowadź hasło administratora ustawione na produkcie.

- Podczas logowania do zaawansowanych ustawień aplikacji Web Config
- Podczas obsługi menu na panelu sterowania, które zostało zablokowane przez administratora
- Podczas zmiany ustawień urządzenia w aplikacji
- Podczas aktualizacji oprogramowania sprzętowego do urządzenia
- W przypadku zmiany lub resetowania hasła administratora

Zmiana hasła administratora

Można je zmienić w panelu sterowania produktu lub w aplikacji Web Config.

W przypadku zmiany hasła nowe hasło musi zawierać od 8 do 20 znaków i wyłącznie jednobajtowe znaki i symbole alfanumeryczne.

Resetowanie hasła administratora

Możesz zresetować hasło administratora do ustawienia wstępnego w panelu sterowania produktu lub w aplikacji Web Config.

Jeśli nie pamiętasz hasła i nie możesz zresetować go do ustawień domyślnych, produkt wymaga naprawy. Skontaktuj się z lokalnym sprzedawcą.

Zalecane ustawienia przeznaczone do żądanego celu

Zalecane ustawienia przeznaczone do żądanego celu.13

Zalecane ustawienia przeznaczone do żądanego celu

Poniżej przedstawiono sposób konfigurowania ustawień stosownie do żądanego celu.

Łączenie skanera z siecią

Cel	Wymagane ustawienia
Połączenie skanera z siecią.	Ustaw skaner do skanowania sieciowego. „Łączenie skanera z siecią” na stronie 16
Połączenie skanera z nowym komputerem.	Skonfiguruj ustawienia sieciowe skanera na nowym komputerze. „Dodawanie lub wymienianie komputera lub urządzeń” na stronie 22

Ustawienia skanowania

Cel	Wymagane ustawienia
Wysyłanie zeskanowanych obrazów pocztą e-mail. (Skanowanie do wiadomości e-mail)	1. Skonfiguruj serwer poczty e-mail, który ma być używany. „Rejestrowanie serwera poczty e-mail” na stronie 45 2. Zarejestruj adres e-mail odbiorcy w Kontakty (opcjonalne). Po zarejestrowaniu adresu e-mail nie trzeba będzie go wprowadzać za każdym razem, aby wysłać coś do tego odbiorcy. Wystarczy go wybrać z listy Kontakty. „Udostępnianie kontaktów” na stronie 55
Zapisywanie zeskanowanych obrazów w folderze sieciowym. (Skanowanie do folderu sieciowego/FTP)	1. Utwórz folder sieciowy, w którym mają być zapisywane obrazy. „Tworzenie folderu sieciowego” na stronie 48 2. Zarejestruj ścieżkę do folderu w Kontakty (opcjonalne). Po zarejestrowaniu ścieżki folderu nie trzeba będzie jej wprowadzać za każdym razem, aby wysłać coś do tego odbiorcy. Wystarczy go wybrać z listy Kontakty. „Udostępnianie kontaktów” na stronie 55
Zapisywanie zeskanowanych obrazów w pamięci w chmurze. (Skanowanie do chmury)	Skonfiguruj usługę Epson Connect. Szczegółowe informacje dotyczące konfiguracji można znaleźć w witrynie Epson Connect. Podczas konfigurowania trzeba podać informacje o koncie użytkownika usługi chmury, z którą ma być połączona. https://www.epsonconnect.com/ http://www.epsonconnect.eu (tylko w Europie)

Dostosowanie wyświetlacza panelu sterowania

Cel	Wymagane ustawienia
Zmiana pozycji wyświetlanych na panelu sterowania skanera.	Ustaw Wstępne lub Edytuj Główny . Można zarejestrować ulubione ustawienia skanowania na panelu sterowania i edytować wyświetlane pozycje. „Dostosowanie wyświetlacza panelu sterowania” na stronie 69

Konfigurowanie podstawowych funkcji bezpieczeństwa

Cel	Wymagane ustawienia
Uniemożliwienie osobom innym niż administrator zmiany ustawień skanera.	Ustaw hasło administratora do skanera. „Ustawienia administratora” na stronie 77
Wyłączenie obsługi skanera przez port USB.	Wyłącz interfejs zewnętrzny. „Wyłączanie interfejsu zewnętrznego” na stronie 85

Konfigurowanie zaawansowanych funkcji bezpieczeństwa

Cel	Wymagane ustawienia
Kontrolowanie używanych protokołów.	Włącz lub wyłącz poszczególne protokoły. „Kontrola użycia protokołów” na stronie 93
Szyfrowanie komunikacji.	1. Skonfiguruj certyfikat cyfrowy. „Używanie certyfikatu cyfrowego” na stronie 96 2. Skonfiguruj komunikację SSL/TLS. „Komunikacja SSL/TLS ze skanerem” na stronie 102
Używanie szyfrowanej komunikacji (IPsec). Używanie oprogramowania tylko z określonego komputera (filtrowanie IP).	Skonfiguruj zasady filtrowania ruchu. „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103
Używanie skanera w sieci IEEE802.1X.	Skonfiguruj sieć IEEE802.1X na skanerze. „Podłączanie skanera do sieci IEEE802.1X” na stronie 115

Synchronizowanie skanera z systemem uwierzytelniającym

Uzyskaj klucz produktu z dedykowanej witryny i na skanerze włącz platformę Epson Open Platform.

[„Korzystanie z funkcji Epson Open Platform” na stronie 124](#)

Korzystanie z opcji uwierzytelniania (Epson Print Admin/Epson Print Admin Serverless)

Aby korzystać z tej opcji, należy zakupić klucz licencyjny.

Aby uzyskać więcej informacji, należy skontaktować się ze sprzedawcą.

Uwaga:

Kiedy system jest zsynchronizowany z platformą Epson Open Platform, nie można używać rozwiązania Epson Print Admin Serverless.

Ustawienia sieciowe

Łączenie skanera z siecią.	16
Dodawanie lub wymienianie komputera lub urządzeń.	22
Sprawdzanie stanu połączenia sieciowego.	28
Dane techniczne sieci.	30
Rozwiązywanie problemów.	34

Łączenie skanera z siecią

W tym rozdziale opisano procedurę łączenia skanera z siecią za pomocą panelu sterowania skanera.

Uwaga:

Jeśli skaner i komputer są w tym samym segmencie, można też połączyć się za pomocą programu instalacyjnego.

Aby uruchomić program instalacyjny, przejdź do poniższej witryny, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

<https://epson.sn>

Możliwe jest wyświetlanie instrukcji w aplikacji Instr. filmu internetowego. Uzyskaj dostęp do następującego adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Czynności do wykonania przed nawiązaniem połączenia sieciowego

Aby nawiązać połączenie z siecią, należy sprawdzić informacje o metodzie nawiązywania i ustawienia połączenia.

Gromadzenie informacji o ustawieniach połączenia

Przed nawiązaniem połączenia należy przygotować wymagane informacje o ustawieniach połączenia. Należy wcześniej sprawdzić następujące informacje.

Wymiary	Elementy	Uwaga
Metoda połączenia urządzenia	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Określanie połączenia skanera z siecią. W przypadku przewodowej sieci LAN połączenie jest nawiązywane z przełącznikiem. W przypadku sieci Wi-Fi połączenie jest nawiązywane z siecią (SSID) punktu dostępu.
Informacje o połączeniu z siecią LAN	<input type="checkbox"/> Adres IP <input type="checkbox"/> Maska podsieci <input type="checkbox"/> Brama domyślna	Określanie adresu IP przydzielanego skanerowi. Podczas statycznego przydzielania adresu IP wymagane są wszystkie wartości. W przypadku dynamicznego przydzielania adresu IP za pomocą funkcji DHCP te informacje nie są potrzebne, ponieważ zostaną ustawione automatycznie.
Informacje o połączeniu z siecią Wi-Fi	<input type="checkbox"/> Identyfikator SSID <input type="checkbox"/> Hasło	To jest identyfikator SSID (nazwa sieci) i hasło punktu dostępu, z którym skaner ma być połączony. Jeśli włączono funkcję filtrowania adresów MAC, zarejestruj adres MAC skanera przed zarejestrowaniem skanera. Więcej informacji o obsługiwanych standardach można znaleźć w następującym rozdziale. „Dane techniczne sieci” na stronie 30
Informacje o serwerze DNS	<input type="checkbox"/> Adres IP podstawowego serwera DNS <input type="checkbox"/> Adres IP pomocniczego serwera DNS	Te informacje są wymagane podczas określania serwerów DNS. Pomocniczy serwer DNS jest ustawiany, gdy system ma konfigurację nadmiarową i dostępny jest pomocniczy serwer DNS. W małych organizacjach, w których nie ma serwera DNS, trzeba ustawić adres IP routera.

Wymiary	Elementy	Uwaga
Informacje o serwerze proxy	<input type="checkbox"/> Nazwa serwera proxy	<p>Informacje te należy skonfigurować, jeśli w środowisku sieciowym używany jest serwer proxy do uzyskiwania dostępu do Internetu z Intranetu, a skaner uzyskuje dostęp bezpośrednio do Internetu.</p> <p>W przypadku następujących funkcji skaner nawiązuje bezpośrednie połączenie z Internetem.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Usługi Epson Connect <input type="checkbox"/> Usługi chmury innych firm <input type="checkbox"/> Aktualizacja oprogramowania układowego <input type="checkbox"/> Wysyłanie zeskanowanych obrazów do usługi SharePoint (WebDAV)
Informacje o numerze portu	<input type="checkbox"/> Numer portu do rozgłoszenia	<p>Sprawdź numer portu używany przez skaner i komputer, a następnie w razie potrzeby zezwól na ruch na tym porcie w konfiguracji zapory.</p> <p>Więcej informacji o portach używanych przez skaner można znaleźć w następującym rozdziale.</p> <p>„Używanie portów na skanerze” na stronie 32</p>

Przydzielanie adresu IP

Poniżej przedstawiono następujące rodzaje przydzielania adresu IP.

Statyczny adres IP:

Ręczne przydzielanie wstępnie określonego adresu IP do skanera (hosta).

Informacje potrzebne do połączenia z siecią (maska podsieci, domyślna brama, serwer DNS itd.) trzeba ustawić ręcznie.

Adres IP nie zmienia się nawet po wyłączeniu urządzenia. Takie rozwiązanie jest przydatne do zarządzania urządzeniami w środowisku, w którym nie można zmieniać adresu IP, lub zarządzania urządzeniami za pomocą adresów IP. Zaleca się przydzielenie takiego adresu do skanera, serwera itd., do których wiele komputerów uzyskuje dostęp. Ponadto w przypadku używania funkcji zabezpieczeń, takich jak filtrowanie IPsec/IP, zaleca się przydzielenie statycznego adresu IP, który się nie zmienia.

Automatyczne przydzielanie za pomocą funkcji DHCP (dynamiczny adres IP):

Możliwe jest automatyczne przydzielanie adresu IP do skanera (hosta) za pomocą funkcji DHCP serwera DHCP lub routera.

Informacje potrzebne do połączenia z siecią (maska podsieci, domyślna brama, serwer DNS itd.) są ustawiane automatycznie, więc można łatwo połączyć się z siecią.

Jeśli urządzenie lub router zostaną wyłączone, w zależności od ustawień serwera DHCP adres IP może się zmienić po ponownym połączeniu.

Zaleca się zarządzanie urządzeniami przy użyciu środków innych niż adres IP i komunikacji za pomocą protokołów, które umożliwiają śledzenie zmian adresu IP.

Uwaga:

Jeśli używana jest funkcja rezerwacji adresu IP serwera DHCP, można przydzielić ten sam adres IP do urządzeń w danym okresie.

Serwer DNS i serwer proxy

Serwer DNS przechowuje nazwę hosta, nazwę domeny adresu e-mail itd. powiązane z informacjami o adresie IP.

Komunikacja jest niemożliwa, jeśli inne urządzenie zostanie opisane przy użyciu nazwy hosta, nazwy domeny itd., gdy komputer lub skaner przesyłają dane za pośrednictwem protokołu IP.

Informacje te są wysyłane w zapytaniu do serwera DNS, który zwraca adres IP innego urządzenia. Ten proces jest nazywany rozwiązywaniem nazw.

Dzięki niemu urządzenia, takie jak komputery i skanery, mogą się ze sobą komunikować przy użyciu adresu IP.

Rozwiązywanie nazw jest niezbędne, aby skaner mógł się komunikować, używając funkcji poczty e-mail lub połączenia internetowego.

Jeśli te funkcje mają być używane, należy skonfigurować serwer DNS.

Serwer jest ustawiany automatycznie, jeśli adres IP skanera jest przydzielany przez serwer DHCP lub funkcję DHCP routera.

Serwer proxy jest zwykle zlokalizowany na bramie między siecią lokalną a Internetem oraz pośredniczy w wymianie danych między komputerem, skanerem i Internetem (zdalny serwer). Zdalny serwer komunikuje się tylko z serwerem proxy. W związku z tym nie można uzyskać dostępu do informacji o skanerze, takich jak adres IP i numer portu, co zwiększa bezpieczeństwo.

Jeśli połączenie z Internetem jest nawiązywane za pośrednictwem serwera proxy, należy skonfigurować serwer proxy na skanerze.

Łączenie drukarki z siecią z poziomu panelu sterowania

Połącz skaner z siecią, używając panelu sterowania skanera.

Przydzielanie adresu IP

Skonfiguruj podstawowe opcje, takie jak Adres hosta, Maska podsieci, Domyśl. brama.

W tym rozdziale przedstawiono procedurę konfigurowania statycznego adresu IP.

1. Włącz skaner.
2. Na ekranie głównym panelu sterowania skanera wybierz pozycję **Ustaw..**
3. Wybierz pozycje **Ustawienia sieciowe > Zaawansowane > TCP/IP.**
4. Wybierz ustawienie **Ręczne** dla opcji **Uzyskaj adres IP.**

Jeśli adres IP jest przydzielany automatycznie za pomocą funkcji DHCP routera, należy wybrać pozycję **Auto**. W takim przypadku ustawienia **Adres IP**, **Maska podsieci** i **Domyśl. brama** z kroków od 5 do 6 są również ustawiane automatycznie, dlatego należy przejść do kroku 7.

5. Wprowadź adres IP.

Przyciski ◀ i ▶ powodują przełączanie na następny lub poprzedni segment rozdzielony kropką.

Potwierdź wartości z poprzedniego ekranu.

6. Ustaw opcje **Maska podsieci** i **Domyśl. brama**.

Potwierdź wartości z poprzedniego ekranu.



Ważne:

Jeśli kombinacja ustawień Adres IP, Maska podsieci i Domyśl. brama jest niepoprawna, ustawienie **Uruchom ustawienia** jest nieaktywne i nie można kontynuować ustawiania. Należy sprawdzić, czy wpisy są poprawne.

7. Wprowadź adres IP podstawowego serwera DNS.

Potwierdź wartości z poprzedniego ekranu.

Uwaga:

Po wybraniu opcji **Auto** w ustawieniach przydzielania adresu IP można wybrać ustawienia serwera DNS z obszaru **Ręczne** lub **Auto**. Jeśli nie można automatycznie uzyskać adresu serwera DNS, należy wybrać opcję **Ręczne** i wprowadzić adres serwera DNS. Potem wprowadzić bezpośrednio adres pomocniczego serwera DNS. W przypadku wybrania opcji **Auto** należy przejść do kroku 9.

8. Wprowadź adres IP pomocniczego serwera DNS.

Potwierdź wartości z poprzedniego ekranu.

9. Dotknij pozycji **Uruchom ustawienia**.

Konfigurowanie serwera proxy

Jeśli poniższe informacje są spełnione, należy skonfigurować serwer proxy.

- Serwer proxy jest zaprojektowany z myślą o połączeniu internetowym.
- W przypadku używania funkcji wymagających bezpośredniego połączenia skanera z Internetem, takich jak Epson Connect lub usługa chmury innej firmy.

1. Na ekranie głównym wybierz pozycję **Ustaw..**

Podczas konfigurowania ustawień po ustawieniu adresu IP zostanie wyświetlany ekran **Zaawansowane**. Przejdź do kroku 3.

2. Wybierz pozycję **Ustawienia sieciowe > Zaawansowane**.

3. Wybierz pozycję **Serwer proxy**.

4. Wybierz ustawienie **Użyj** dla opcji **Ustaw. serwera proxy**.

5. Wprowadź adres serwera proxy w formacie IPv4 lub FQDN.

Potwierdź wartości z poprzedniego ekranu.

6. Wprowadź numer portu serwera proxy.


Potwierdź wartości z poprzedniego ekranu.

7. Dotknij pozycji **Uruchom ustawienia**.

Łączenie z siecią Ethernet

Podłącz skaner do sieci, używając kabla sieciowego, a następnie sprawdź, czy połączenie działa prawidłowo.

1. Podłącz skaner do koncentratora (przełącznika sieci lokalnej) kablem sieciowym.

2. Na ekranie głównym wybierz pozycję .
3. Wybierz pozycję **Router**.
4. Upewnij się, czy ustawienia Połączenie i Adres IP są poprawne.
5. Dotknij pozycji **Zamknij**.

Nawiązywanie połączenia z bezprzewodową siecią LAN (Wi-Fi)

Skaner można połączyć z bezprzewodową siecią LAN (Wi-Fi) na kilka sposobów. Wybierz metodę połączenia dopasowaną do środowiska i warunków, w których urządzenie będzie używane.

Jeżeli informacje o routerze bezprzewodowym, takie jak SSID i hasło, są znane, można wprowadzić je ręcznie.

Jeżeli router bezprzewodowy obsługuje funkcję WPS, można skonfigurować ustawienia, naciskając odpowiedni przycisk.

Po podłączeniu skanera do sieci połącz się z nim z urządzenia, które ma być wykorzystane (komputera, urządzenia inteligentnego, tabletu itd.).

Informacje dotyczące korzystania z połączenia Wi-Fi w paśmie 5 GHz

Produkt zwykle wykorzystuje kanał W52 (36) podczas nawiązywania połączenia Wi-Fi Direct (zwykle AP). W związku z tym, że kanał sieci bezprzewodowej (Wi-Fi) jest wybierany automatycznie, używany kanał może się różnić, kiedy w tym samym czasie będzie używane połączenie Wi-Fi Direct. Jeśli kanał się różni, wymiana danych ze skanerem może być wolna. Jeśli w otoczeniu sieciowym nie ma zbyt wielu innych sieci, można połączyć się z siecią pracującą w paśmie 2,4 GHz. W tym paśmie kanały powinny być zgodne.

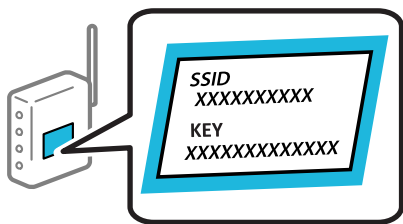
Jeśli sieć bezprzewodowa zostanie ustawiona na pasmo 5 GHz, zaleca się wyłączenie funkcji Wi-Fi Direct.


Konfigurowanie ustawień Wi-Fi przez wprowadzenie identyfikatora SSID i hasła

Sieć Wi-Fi można skonfigurować, wprowadzając informacje niezbędne do połączenia się z routerem bezprzewodowym na panelu sterowania skanera. Aby móc skonfigurować sieć za pomocą tej metody, trzeba znać identyfikator SSID oraz hasło do sieci routera bezprzewodowego.

Uwaga:

W przypadku korzystania z routera bezprzewodowego z ustawieniami domyślnymi identyfikator SSID oraz hasło podane są na etykiecie routera bezprzewodowego. Aby uzyskać identyfikator SSID i hasło, należy skontaktować się z osobą, która skonfigurowała router bezprzewodowy, lub zapoznać się z dokumentacją dostarczoną wraz z routerem bezprzewodowym.



1. Na ekranie głównym dotknij pozycji .
2. Wybierz pozycję **Router**.

3. Dotknij pozycji **Rozpocznij konfigurację**.

Jeśli połączenie sieciowe zostało już skonfigurowane, wyświetlą się szczegóły połączenia. Dotknij pozycji **Zmień na połączenie Wi-Fi**, lub **Zmień ustawienia**, aby zmienić ustawienia.

4. Wybierz pozycję **Kreator konfiguracji Wi-Fi**.

5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby wybrać SSID, wprowadź hasło dla routera bezprzewodowego i rozpocznij konfigurację.

Aby sprawdzić stan połączenia sieciowego skanera po ukończeniu konfiguracji, więcej informacji możesz uzyskać, klikając łącze informacji powiązanych.

Uwaga:

- Jeśli identyfikator SSID jest nieznany, należy sprawdzić, czy nie został on umieszczony na etykiecie routera bezprzewodowego. W przypadku korzystania z routera bezprzewodowego z ustawieniami domyślnymi identyfikator SSID podany jest na etykiecie routera bezprzewodowego. Jeśli nie można znaleźć żadnych informacji, należy zapoznać się z dokumentacją dostarczoną wraz z routerem bezprzewodowym.
- Wielkość liter w hasle ma znaczenie.
- Jeśli hasło jest nieznane, należy sprawdzić, czy nie zostało ono umieszczona na etykiecie routera bezprzewodowego. Hasło na etykiecie może być oznaczone napisem „Network Key”, „Wireless Password” itd. W przypadku korzystania z routera bezprzewodowego z ustawieniami domyślnymi hasło podane jest na etykiecie routera bezprzewodowego.
- Jeśli na liście nie ma identyfikatora SSID, z którym ma być nawiązane połączenie, należy użyć oprogramowania lub aplikacji, aby skonfigurować sieć Wi-Fi z poziomu komputera lub urządzenia inteligentnego, np. smartfona lub tableta. Więcej informacji można uzyskać, wprowadzając w pasku adresu przeglądarki adres „<https://epson.sn>”, aby uzyskać dostęp do witryny, i wprowadzając nazwę produktu, a następnie przechodząc do **Konfiguracja**.

Powiązane informacje

➔ „Sprawdzanie stanu połączenia sieciowego” na stronie 28

Wprowadzanie ustawień Wi-Fi poprzez konfigurację kodu PIN (WPS)

Sieć Wi-Fi można automatycznie skonfigurować, naciskając przycisk na routerze bezprzewodowym. Po spełnieniu poniższych warunków można przeprowadzać konfigurację, korzystając z tej metody.

- Router bezprzewodowy jest zgodny z WPS (Wi-Fi Protected Setup).
- Obecne połączenie Wi-Fi zostało ustanowione przez naciśnięcie przycisku na routerze bezprzewodowym.

Uwaga:

Jeśli nie można znaleźć przycisku lub w przypadku konfiguracji za pomocą oprogramowania, przejrzyj dokumentację dostarczoną wraz z routerem bezprzewodowym.



1. Na ekranie głównym dotknij pozycji

2. Wybierz pozycję **Router**.

3. Dotknij pozycji **Rozpocznij konfigurację**.

Jeśli połączenie sieciowe zostało już skonfigurowane, wyświetlą się szczegóły połączenia. Dotknij pozycji **Zmień na połączenie Wi-Fi**, lub **Zmień ustawienia**, aby zmienić ustawienia.

4. Wybierz pozycję **Ust. Push Button (WPS)**.

5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Aby sprawdzić stan połączenia sieciowego skanera po ukończeniu konfiguracji, więcej informacji możesz uzyskać, klikając łącze informacji powiązanych.

Uwaga:


Jeśli nie uda się nawiązać połączenia, zrestartuj router bezprzewodowy, przesuń go bliżej skanera i spróbuj ponownie.

Powiązane informacje

➔ [„Sprawdzanie stanu połączenia sieciowego” na stronie 28](#)

Wprowadzanie ustawień Wi-Fi przy pomocy konfiguracji kodu PIN (WPS)

Można automatycznie połączyć się z routerem bezprzewodowym, używając kodu PIN. Można użyć tej metody do dokonania konfiguracji, jeśli ruter bezprzewodowy obsługuje WPS (Wi-Fi Protected Setup). Aby wprowadzić kod PIN w routerze bezprzewodowym, użyj komputera.

1. Na ekranie głównym dotknij pozycji .

2. Wybierz pozycję **Router**.

3. Dotknij pozycji **Rozpocznij konfigurację**.

Jeśli połączenie sieciowe zostało już skonfigurowane, wyświetlą się szczegóły połączenia. Dotknij pozycji **Zmień na połączenie Wi-Fi**, lub **Zmień ustawienia**, aby zmienić ustawienia.

4. Wybierz pozycje **Inne > Ust. kodu PIN (WPS)**

5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Aby sprawdzić stan połączenia sieciowego skanera po ukończeniu konfiguracji, więcej informacji możesz uzyskać, klikając łącze informacji powiązanych.

Uwaga:

Należy zapoznać się z dokumentacją dostarczoną wraz z routerem bezprzewodowym, aby uzyskać dalsze informacje na temat wprowadzania kodu PIN.

Powiązane informacje

➔ [„Sprawdzanie stanu połączenia sieciowego” na stronie 28](#)

Dodawanie lub wymienianie komputera lub urządzeń

Nawiązywanie połączenia ze skanerem połączonym z siecią

Jeżeli skaner został już połączony z siecią, można połączyć komputer lub urządzenie inteligentne ze skanerem przez sieć.

Korzystanie ze skanera sieciowego z drugiego komputera

Aby połączyć skaner z komputerem, zalecamy użycie instalatora.

Aby uruchomić program instalacyjny, przejdź do poniższej witryny, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

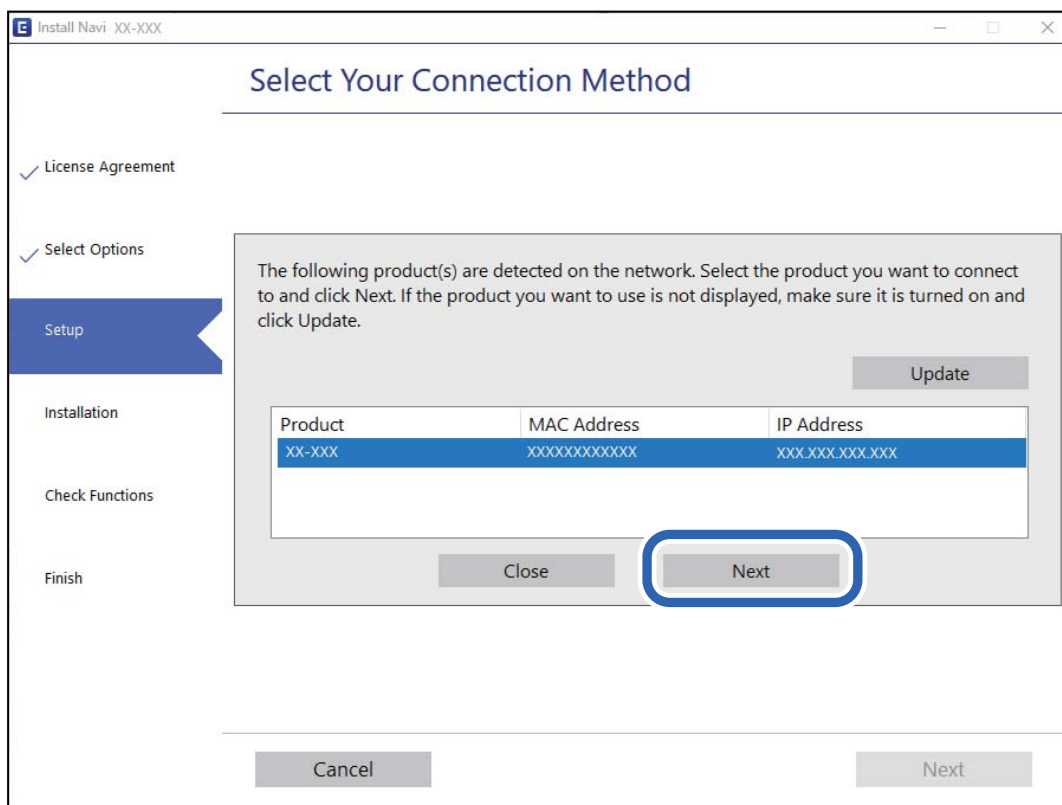
<https://epson.sn>

Możliwe jest wyświetlanie instrukcji w aplikacji Instr. filmu internetowego. Uzyskaj dostęp do następującego adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Wybór skanera

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aż zostanie wyświetlony następujący ekran, wybierz nazwę skanera, z którym połączenie ma być nawiązane, a następnie kliknij przycisk **Dalej**.



Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Korzystanie ze skanera sieciowego z urządzenia inteligentnego

Możliwe jest połączenie urządzenia inteligentnego ze skanerem przy użyciu jednej z następujących metod.

Połączenie przez router bezprzewodowy

Podłącz urządzenie inteligentne do tej samej sieci Wi-Fi (SSID) co skaner.

Przejdź poniżej w celu uzyskania szczegółowych informacji.

„Konfigurowanie ustawień połączenia z urządzeniem inteligentnym” na stronie 27

Połączenie przez Wi-Fi Direct

Podłącz urządzenie inteligentne do skanera bezpośrednio z pominięciem routera bezprzewodowego.

Przejdź poniżej w celu uzyskania szczegółowych informacji.

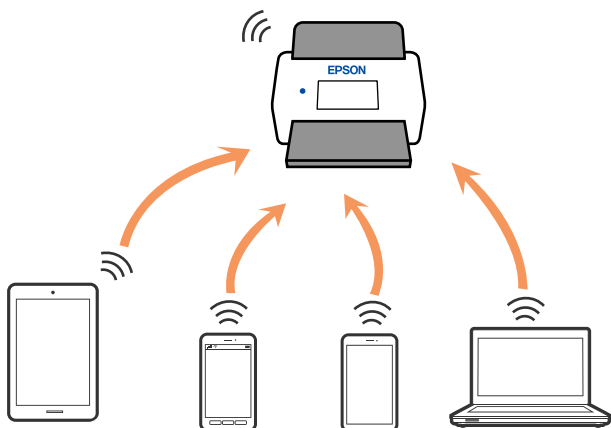
[„Nawiązywanie bezpośredniego połączenia między urządzeniem inteligentnym a skanerem \(Wi-Fi Direct\)” na stronie 24](#)

Nawiązywanie bezpośredniego połączenia między urządzeniem inteligentnym a skanerem (Wi-Fi Direct)

Funkcja Wi-Fi Direct (zwykle AP) pozwala połączyć urządzenie inteligentne bezpośrednio ze skanerem z pominięciem routera bezprzewodowego i skanowanie z urządzenia inteligentnego.

Informacje o aplikacji Wi-Fi Direct


Z tej metody połączenia można skorzystać wtedy, kiedy w domu lub biurze nie jest używana sieć Wi-Fi lub w celu bezpośredniego połączenia skanera i urządzenia inteligentnego. W tym trybie skaner pełni rolę routera bezprzewodowego, do którego można podłączyć urządzenia bez konieczności korzystania ze standardowego routera bezprzewodowego. Jednak trzeba pamiętać, że urządzenia podłączone bezpośrednio do skanera nie mogą się komunikować przez to urządzenie.



Skaner może być połączony równocześnie przez sieć Wi-Fi lub Ethernet i Wi-Fi Direct (zwykle AP). Jednak jeżeli połączenie sieciowe zostanie rozpoczęte w trybie Wi-Fi Direct (zwykle AP), kiedy skaner jest połączony przez Wi-Fi, połączenie Wi-Fi jest czasowo rozłączane.

Nawiązywanie połączenia z urządzeniem inteligentnym przy użyciu Wi-Fi Direct

Metoda ta pozwala na połączenie skanera bezpośrednio z urządzeniami inteligentnymi bez routera bezprzewodowego.

1. Na ekranie głównym wybierz pozycję .
2. Wybierz pozycję **Wi-Fi Direct**.

- Wybierz pozycję **Rozpocznij konfigurację**.
- Na urządzeniu inteligentnym uruchom aplikację Epson Smart Panel.
- Postępuj zgodnie z instrukcjami wyświetlanymi w aplikacji Epson Smart Panel, aby połączyć się ze skanerem.
Po połączeniu urządzenia inteligentnego ze skanerem przejdź do następnego kroku.
- Na panelu sterowania skanera wybierz pozycję **Zakończ**.

Rozłączanie połączenia Wi-Fi Direct (zwykle AP)

Są dostępne dwa sposoby wyłączenia połączenia Wi-Fi Direct (zwykle AP): można wyłączyć wszystkie połączenia z panelu sterowania skanera lub wyłączyć każde połączenie z komputera lub urządzenia inteligentnego.

Jeżeli chcesz wyłączyć wszystkie połączenia wybierz  > **Wi-Fi Direct** > **Rozpocznij konfigurację** > **Zmień** > **Wyłącz Wi-Fi Direct**.



Ważne:

Jeśli połączenie Wi-Fi Direct (zwykle AP) zostanie wyłączone, wszystkie komputery i inteligentne urządzenia połączone ze skanerem przez połączenie Wi-Fi Direct (zwykle AP) zostaną odłączone.

Uwaga:

Aby rozłączyć konkretne urządzenie, odłącz je przez to urządzenie, a nie skaner. Jedną z podanych dalej metod można odłączyć urządzenie od Wi-Fi Direct (zwykle AP).

- Usuń skojarzenie połączenia Wi-Fi z nazwą sieci (SSID) skanera.
- Połącz z siecią o innej nazwie (SSID).

Zmiana ustawień Wi-Fi Direct (zwykle AP), takich jak identyfikator SSID

Po włączeniu połączenia Wi-Fi Direct (zwykle AP) można zmienić jego ustawienia, wybierając pozycję



> **Wi-Fi Direct** > **Rozpocznij konfigurację** > **Zmień**, co spowoduje wyświetlenie następujących ustawień.

Zmień nazwę sieci

Nazwę sieci (SSID) funkcji Wi-Fi Direct (zwykle AP) służącą do nawiązywania połączeń ze skanerem można zmienić na dowolnie wybraną nazwę. Do definiowania nazwy sieci (SSID) można używać znaków ASCII wyświetlanych na klawiaturze programowej na panelu sterowania. Dozwolone są maksymalnie 22 znaki.

Po zmianie nazwy sieci (SSID) wszystkie połączone urządzenia zostaną rozłączone. Aby ponownie nawiązać połączenie z urządzeniem, należy użyć nowej nazwy sieci (SSID).

Zmień hasło

Możliwa jest zmiana hasła Wi-Fi Direct (zwykle AP) służącego do nawiązywania połączenia ze skanerem. Hasło można ustawić, używając klawiatury programowej ze znakami ASCII wyświetlanej na panelu sterowania. Można użyć od 8 do 22 znaków.

Po zmianie hasła wszystkie połączone urządzenia zostaną rozłączone. Aby ponownie połączyć urządzenia, należy użyć nowego hasła.

Zmień zakres częstotliwości

Można zmienić zakres częstotliwości funkcji Wi-Fi Direct używanej do nawiązywania połączenia ze skanerem. Można wybrać zakres 2,4 GHz lub 5 GHz.

Po zmianie zakresu częstotliwości wszystkie połączone urządzenia zostaną rozłączone. Ponownie połącz urządzenie.

Należy pamiętać, że po zmianie na zakres częstotliwości 5 GHz nie można ponownie połączyć urządzeń, które nie obsługują tego zakresu.

W niektórych regionach ustawienie to może nie być widoczne.

Wyłącz Wi-Fi Direct

Można wyłączyć połączenie Wi-Fi Direct (zwykle AP) skanera. Po wyłączeniu wszystkie urządzenia połączone ze skanerem za pośrednictwem połączenia Wi-Fi Direct (zwykle AP) zostaną rozłączone.

Przywr. ust. domyśl.

Można przywrócić wartości domyślne wszystkich ustawień funkcji Wi-Fi Direct (zwykle AP).

Zostaną usunięte informacje o połączeniu Wi-Fi Direct (zwykle AP) z urządzeniem inteligentnym zapisane w pamięci skanera.

Uwaga:

Można też użyć karty **Sieć > Wi-Fi Direct** w aplikacji *Web Config* do konfiguracji następujących ustawień.

- Włączanie lub wyłączenie sieci Wi-Fi Direct (zwykle AP)
 - Zmiana nazwy sieci (SSID)
 - Zmiana hasła
 - Zmiana zakresu częstotliwości
- W niektórych regionach ustawienie to może nie być widoczne.*
- Przywracanie ustawień funkcji Wi-Fi Direct (zwykle AP)

Ponowna konfiguracja połączenia sieciowego

W tym rozdziale opisano konfigurowanie ustawień połączenia sieciowego i zmianę metody połączenia w przypadku zmiany routera bezprzewodowego lub komputera.

Podczas zmiany routera bezprzewodowego

Podczas zmiany routera bezprzewodowego skonfiguruj ustawienia połączenia między komputerem lub urządzeniem inteligentnym a skanerem.

Ustawienia te trzeba zmienić w przypadku zmiany usługodawcy internetowego i tym podobne.

Konfigurowanie ustawień połączenia z komputerem

Aby połączyć skaner z komputerem, zalecamy użycie instalatora.

Aby uruchomić program instalacyjny, przejdź do poniższej witryny, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

<https://epson.sn>

Możliwe jest wyświetlanie instrukcji w aplikacji Instr. filmu internetowego. Uzyskaj dostęp do następującego adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Wybór metody łączenia

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Na ekranie **Wybierz opcję instalacji** wybierz pozycję **Skonfiguruj ponownie połączenie z Drukarka (dla nowego routera sieciowego lub po zmianie USB na sieć, itp.)**, a następnie kliknij przycisk **Dalej**.

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zakończyć konfigurację.

Jeśli nie można nawiązać połączenia, zapoznaj się z następującymi rozdziałami, aby rozwiązać problem.

„Nie można połączyć się z siecią” na stronie 34

Konfigurowanie ustawień połączenia z urządzeniem inteligentnym

Skanera można używać na urządzeniach inteligentnych po połączeniu skanera z tą samą siecią Wi-Fi (SSID), z którą połączone jest urządzenie inteligentne. Aby używać skanera z poziomu urządzenia inteligentnego, uzyskaj dostęp do następującej witryny, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

<https://epson.sn>

Uzyskaj dostęp do witryny z urządzenia inteligentnego, które ma być połączone ze skanerem.

Podczas zmiany komputera

Podczas zmiany komputera skonfiguruj ustawienia połączenia między komputerem a skanerem.

Konfigurowanie ustawień połączenia z komputerem

Aby połączyć skaner z komputerem, zalecamy użycie instalatora.

Aby uruchomić program instalacyjny, przejdź do poniższej witryny, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

<https://epson.sn>

Możliwe jest wyświetlanie instrukcji w aplikacji Instr. filmu internetowego. Uzyskaj dostęp do następującego adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zmiana metody połączenia z komputerem

W tym rozdziale opisano zmianę metody połączenia, gdy komputer i skaner są już połączone.

Zmiana połączenia sieciowego z Ethernet na Wi-Fi

Zmianę połączenia Ethernet na połączenie Wi-Fi można wykonać na panelu sterowania skanera. Procedura zmiany połączenia jest zasadniczo taka sama, jak w przypadku konfiguracji połączenia Wi-Fi.

Powiązane informacje

➔ „Nawiązywanie połączenia z bezprzewodową siecią LAN (Wi-Fi)” na stronie 20

Zmiana połączenia sieciowego z Wi-Fi na Ethernet

Wykonaj poniższe czynności, aby zmienić połączenie Wi-Fi na połączenie Ethernet.

1. Na ekranie głównym wybierz pozycję **Ustaw.**.
2. Wybierz pozycję **Ustawienia sieciowe > Ustawienie sieci LAN**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zmiana połączenia USB na połączenie sieciowe

Korzystanie z instalatora i ponowna konfiguracja w innej metodzie łączenia się.

Przejdź na poniższą stronę internetową, a następnie wprowadź nazwę produktu. Przejdź do obszaru **Konfiguracja**, a następnie rozpocznij konfigurację.

<https://epson.sn>

Wybór zmiany metod łączenia się

Postępuj zgodnie z instrukcjami wyświetlanymi w poszczególnych oknach. Na ekranie **Wybierz opcję instalacji** wybierz pozycję **Skonfiguruj ponownie połączenie z Drukarka (dla nowego routera sieciowego lub po zmianie USB na sieć, itp.)**, a następnie kliknij przycisk **Dalej**.

Wybierz żądane połączenie sieciowe, **Podłącz przez sieć bezprzewodową (Wi-Fi)** lub **Połącz przez przewodową sieć LAN (Ethernet)**, a następnie kliknij przycisk **Dalej**.

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zakończyć konfigurację.

Sprawdzanie stanu połączenia sieciowego

Stan połączenia sieciowego można sprawdzić w następujący sposób.

Sprawdzanie stanu połączenia sieciowego za pomocą panelu sterowania

Stan połączenia sieciowego można sprawdzić przy użyciu ikony sieci lub informacji o sieci wyświetlanych na panelu sterowania skanera.

Sprawdzanie stanu połączenia sieciowego za pomocą ikony sieci

Stan połączenia sieciowego i siłę sygnału radiowego można sprawdzić, korzystając z ikony sieci na ekranie głównym skanera.



	<p>Wyświetlanie stanu połączenia sieciowego. Wybierz ikonę, aby sprawdzić i zmienić bieżące ustawienia. Jest to skrót dla następującego menu.</p>
<p>Ustaw. > Ustawienia sieciowe > Ustawienia Wi-Fi</p>	
	<p>Skaner nie jest połączony z siecią bezprzewodową (Wi-Fi).</p>
	<p>Trwa wyszukiwanie identyfikatora SSID, adres IP nie jest przydzielony lub wystąpił problem z siecią bezprzewodową (Wi-Fi).</p>
	<p>Skaner jest połączony z siecią bezprzewodową (Wi-Fi). Liczba kresek wskazuje siłę sygnału połączenia. Im więcej kresek, tym silniejszy sygnał.</p>
	<p>Skaner nie jest połączony z siecią bezprzewodową (Wi-Fi) w trybie Wi-Fi Direct (zwykle AP).</p>
	<p>Skaner jest połączony z siecią bezprzewodową (Wi-Fi) w trybie Wi-Fi Direct (zwykle AP).</p>
	<p>Skaner nie jest połączony z siecią przewodową (Ethernet) lub sieć nie jest skonfigurowana.</p>
	<p>Skaner jest połączony z siecią przewodową (Ethernet).</p>

Wyświetlanie szczegółowych informacji o sieci na panelu sterowania

Jeśli skaner jest połączony z siecią, można przejrzeć inne informacje powiązane z siecią, wybierając menu sieci, która ma być sprawdzona.

1. Na ekranie głównym wybierz pozycję **Ustaw.**
2. Wybierz pozycję **Ustawienia sieciowe > Stan sieci.**
3. W celu sprawdzenia informacji wybierz menu, które chcesz sprawdzić.
 - Stan sieci LAN/Wi-Fi
Wyświetlenie informacji o sieci (nazwa urządzenia, połączenie, siła sygnału itd.) na potrzeby połączeń Ethernet lub Wi-Fi.
 - Stan usługi Wi-Fi Direct
Wyświetlenie informacji o włączeniu lub wyłączeniu funkcji Wi-Fi Direct, informacji, takich jak SSID, hasło itp. na potrzeby połączeń Wi-Fi Direct.

Stan serwera e-mail

Wyświetlenie informacji o sieci serwera e-mail.

Dane techniczne sieci

Specyfikacje Wi-Fi

W podanej dalej tabeli znajdują się specyfikacje sieci Wi-Fi.

Kraje lub regiony z wyjątkiem poniższych	Tabela A
Irlandia, Wielka Brytania, Austria, Niemcy, Liechtenstein, Szwajcaria, Francja, Belgia, Luksemburg, Holandia, Włochy, Portugalia, Hiszpania, Dania, Finlandia, Norwegia, Szwecja, Islandia, Chorwacja, Cypr, Grecja, Północna Macedonia, Serbia, Słowenia, Malta, Bośnia i Hercegowina, Kosowo, Czarnogóra, Albania, Bułgaria, Czechy, Estonia, Węgry, Łotwa, Litwa, Polska, Rumunia, Słowacja, Izrael, Australia, Nowa Zelandia, Tajwan	Tabela B
Turcja	<p>DS-900WN: Numery seryjne zaczynające się od XDA8: tabela A Numery seryjne zaczynające się od XDA7: tabela B</p> <p>DS-800WN: Numery seryjne zaczynające się od XDA2: tabela A Numery seryjne zaczynające się od XD9Z: tabela B</p>

Tabela A

Standardy	IEEE 802.11b/g/n*1
Zakres częstotliwości	2400–2483,5 MHz
Maksymalna moc przekazywanej transmisji radiowej	20 dBm (EIRP)
Kanały	1/2/3/4/5/6/7/8/9/10/11/12/13
Tryby połączenia	Infrastruktura, Wi-Fi Direct (zwykle AP)*2*3
Protokoły zabezpieczeń*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Dostępne tylko dla HT20.

*2 Brak obsługi w standardzie IEEE 802.11b.

*3 Z infrastruktury i trybów Wi-Fi Direct lub połączenia Ethernet można korzystać jednocześnie.

*4 W trybie Wi-Fi Direct obsługiwane jest tylko WPA2-PSK (AES).

*5 Zgodność z protokołem WPA2 wraz z obsługą WPA/WPA2 Personal.

Tabela B

Standardy	IEEE 802.11a/b/g/n ^{*1} /ac		
Zakresy częstotliwości	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanały	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48) W58 (149/153/157/161/165)
Tryby połączenia	Infrastruktura, Wi-Fi Direct (zwykłe AP) ^{*4, *5}		
Protokoły zabezpieczeń ^{*6}	WEP (64/128bit), WPA2-PSK (AES) ^{*7} , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Dostępne tylko dla HT20.

*2 Niedostępne w Tajwanie.

*3 Dostępność tych kanałów i możliwość korzystania z produktu na zewnątrz za pośrednictwem tych kanałów różni się w zależności od lokalizacji. Więcej informacji znajduje się na stronie <http://support.epson.net/wifi5ghz/>

*4 Brak obsługi w standardzie IEEE 802.11b.

*5 Z infrastruktury i trybów Wi-Fi Direct lub połączenia Ethernet można korzystać jednocześnie.

*6 W trybie Wi-Fi Direct obsługiwane jest tylko WPA2-PSK (AES).

*7 Zgodność z protokołem WPA2 wraz z obsługą WPA/WPA2 Personal.

Dane techniczne Ethernet

Standardy	IEEE802.3i (10BASE-T) ^{*1} IEEE802.3u (100BASE-TX) ^{*1} IEEE802.3ab (1000BASE-T) ^{*1} IEEE802.3az (energooszczędny Ethernet) ^{*2}
Tryb komunikacji	Auto, 10 Mb/s pełny duplex, 10 Mb/s półduplex, 100 Mb/s pełny duplex, 100 Mb/s półduplex
Złącze	RJ-45

*1 Użyć skrętki ekranowanej kategorii 5e lub wyższej, aby zapobiec zakłóceniom radiowym.

*2 Podłączone urządzenie powinno być zgodne ze standardami IEEE802.3az.

Funkcje sieciowe i obsługa IPv4/IPv6

Funkcje	Obsługiwane
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Protokół bezpieczeństwa

IEEE802.1X*	
IPsec/filtrowanie IP	
SSL/TLS	Serwer/klient HTTPS
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Należy użyć urządzenia komunikacyjnego zgodnego ze standardem IEEE802.1X.

Używanie portów na skanerze

Skaner wykorzystuje następujące porty. W razie potrzeby należy poprosić administratora sieci o otwarcie tych portów.

Gdy wysyłający (klient) to skaner

Użycie	Miejsce docelowe (serwer)	Protokół	Numer portu	
Wysyłanie plików (gdy funkcja skanowania do folderu sieciowego jest używana na panelu skanera)	Serwer FTP/FTPS	FTP/FTPS (TCP)	20	
			21	
	Serwer plików	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	Serwer WebDAV	NetBIOS (TCP)	139	
			Protokół HTTP (TCP)	80
Protokół HTTPS (TCP)	443			
Wysyłanie poczty e-mail (gdy funkcja skanowania do poczty e-mail jest używana na panelu skanera)	Serwer SMTP	SMTP (TCP)	25	
		SMTP SSL/TLS (TCP)	465	
		SMTP STARTTLS (TCP)	587	

Użycie	Miejsce docelowe (serwer)	Protokół	Numer portu
Połączenie POP przed SMTP (podczas skanowania do wiadomości e-mail z poziomu skanera)	Serwer POP	POP3 (TCP)	110
W przypadku korzystania z usługi Epson Connect	Serwer Epson Connect	HTTPS	443
		XMPP	5222
Gromadzenie informacji o użytkowniku (użycie kontaktów z pamięci skanera)	Serwer LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Uwierzytelnianie użytkowników podczas gromadzenia informacji o użytkowniku (w przypadku używania kontaktów z pamięci skanera) Uwierzytelnianie użytkowników podczas korzystania z funkcji skanowania do folderu sieciowego (SMB) na skanerze	Serwer KDC	Kerberos	88
Kontrola WSD	Komputer kliencki	WSD (TCP)	5357
Wyszukiwanie komputera podczas skanowania wypychanego z poziomu aplikacji	Komputer kliencki	Wykrywanie w trakcie skanowania wypychanego przez sieć	2968

Gdy wysyłający (klient) to Komputer kliencki

Użycie	Miejsce docelowe (serwer)	Protokół	Numer portu
Wykrywanie skanera z aplikacji, takiej jak EpsonNet Config i sterownik skanera	Skaner	ENPC (UDP)	3289
Gromadzenie i konfigurowanie informacji MIB z aplikacji, takiej jak EpsonNet Config i sterownik skanera	Skaner	SNMP (UDP)	161
Wyszukiwanie skanera WSD	Skaner	WS-Discovery (UDP)	3702
Przesyłanie danych skanowania z aplikacji	Skaner	Skanowanie sieciowe (TCP)	1865
Gromadzenie informacji o zadaniu podczas skanowania wypychanego z poziomu aplikacji	Skaner	Skanowanie wypychane przez sieć	2968
Web Config	Skaner	HTTP (TCP)	80
		HTTPS (TCP)	443

Rozwiązywanie problemów

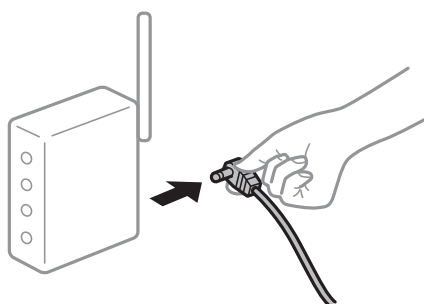
Nie można połączyć się z siecią

Problem może wynikać z jednej z następujących przyczyn.

■ Wystąpił błąd na urządzeniach sieciowych obsługujących połączenie Wi-Fi.

Rozwiązania

Wyłącz urządzenia, które mają być podłączone do sieci. Poczekaj około 10 sekund, a następnie włącz urządzenia w następującej kolejności: router bezprzewodowy, komputer lub urządzenie inteligentne, a następnie skaner. Przenieś skaner i komputer lub urządzenie inteligentne bliżej routera bezprzewodowego, aby ułatwić komunikację radiową, a następnie ponownie spróbuj skonfigurować ustawienia sieci.



■ Urządzenia nie mogą odbierać sygnałów od routera bezprzewodowego, ponieważ są zbyt daleko od niego.

Rozwiązania

Po przeniesieniu komputera lub urządzenia inteligentnego i skanera bliżej routera bezprzewodowego wyłącz router bezprzewodowy, a następnie włącz go ponownie.

■ W przypadku wymiany routera bezprzewodowego ustawienia nie zgadzają się z nowym routerem.

Rozwiązania

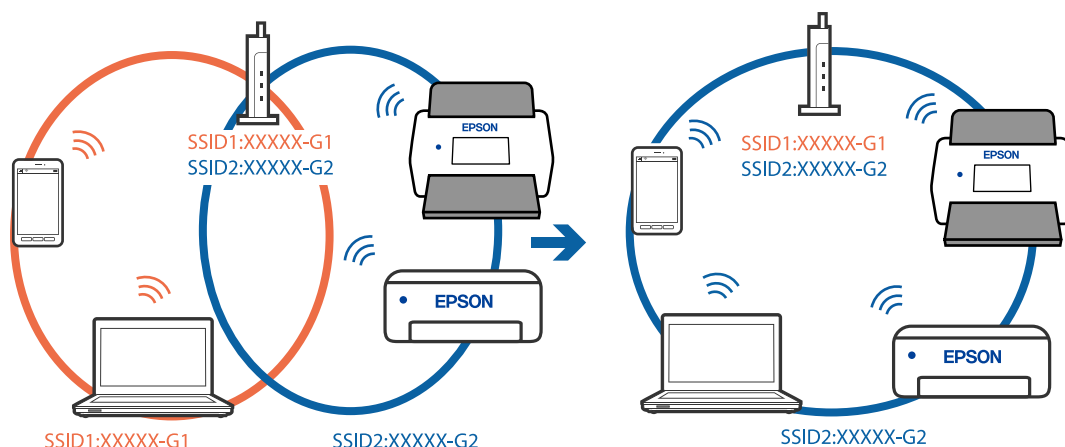
Ponownie skonfiguruj ustawienia połączenia, tak aby pasowały do nowego routera bezprzewodowego.

■ Identyfikatory SSID, z którymi są połączone komputer lub urządzenie inteligentne są różne.

Rozwiązania

W przypadku korzystania z wielu routerów bezprzewodowych jednocześnie lub gdy router bezprzewodowy ma wiele identyfikatorów SSID i urządzenia są połączone z różnymi identyfikatorami SSID, nie można połączyć się z routerem bezprzewodowym.

Podłącz komputer lub urządzenie inteligentne do tego samego identyfikatora SSID co skaner.



Router bezprzewodowy ma funkcję separatora prywatności.

Rozwiązania

Większość routerów bezprzewodowych ma funkcję separatora prywatności blokującą komunikację między połączonymi urządzeniami. Jeżeli nie można połączyć skanera z komputerem lub urządzeniem inteligentnym, nawet gdy znajdują się w tej samej sieci, wyłącz funkcję separatora prywatności na routerze bezprzewodowym. Zapoznaj się z podręcznikiem dostarczonym wraz z routerem bezprzewodowym, aby poznać dalsze szczegóły.

Adres IP jest przydzielony nieprawidłowo.

Rozwiązania

Jeśli adres IP przydzielony skanerowi to 169.254.XXX.XXX, a maska podsieci to 255.255.0.0, oznacza to, że adres IP nie został przydzielony poprawnie.

Na panelu sterowania skanera wybierz pozycję **Ustaw. > Ustawienia sieciowe > Zaawansowane > Ustawienia TCP/IP**, a następnie sprawdź adres IP i maskę podsieci przydzielone skanerowi.

Ponownie uruchom router bezprzewodowy lub zresetuj ustawienia sieciowe skanera.

Wystąpił problem z ustawieniami sieciowymi na tym komputerze.

Rozwiązania

Spróbuj uzyskać dostęp do innej witryny z komputera, aby upewnić się, że ustawienia sieci komputera są poprawne. Jeśli nie można uzyskać dostępu do żadnej witryny, oznacza to problem z komputerem.

Sprawdź połączenie sieciowe komputera. Należy zapoznać się z dokumentacją dostarczoną wraz z komputerem, aby poznać dalsze informacje.

Skaner został połączony przez sieć Ethernet przy użyciu urządzeń obsługujących IEEE 802.3az (Ethernet energooszczędny).

Rozwiązania

W przypadku podłączenia skanera przez Ethernet z użyciem urządzeń obsługujących IEEE 802.3az (Ethernet energooszczędny), mogą pojawić się dalej wymienione problemy, zależnie od stosowanego koncentratora lub routera.

- Połączenie robi się niestabilne, a skaner wielokrotnie łączy się i rozłącza.
- Nie można połączyć się ze skanerem.

- Prędkość komunikacji spada.

Wykonaj poniższe czynności, aby wyłączyć standard IEEE 802.3az na skanerze, a następnie ponownie nawiąź połączenie.

1. Wyciągnij kabel Ethernet podłączony do komputera i skanera.
 2. Wyłącz standard IEEE 802.3az, jeśli jest włączony na komputerze.
Zapoznaj się z dokumentacją dostarczoną wraz z komputerem, aby poznać dalsze informacje.
 3. Połącz komputer ze skanerem bezpośrednio kablem Ethernet.
 4. Na skanerze sprawdź ustawienia sieciowe.
Wybierz pozycje **Ustaw.** > **Ustawienia sieciowe** > **Stan sieci** > **Stan sieci LAN/Wi-Fi**.
 5. Sprawdź adres IP skanera.
 6. Na komputerze uruchom aplikację Web Config.
Uruchom przeglądarkę internetową, a następnie wprowadź adres IP skanera.
[„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)
 7. Wybierz pozycje **Sieć** > **Sieć przewodowa LAN**.
 8. Wybierz ustawienie **Wył.** dla opcji **IEEE 802.3az**.
 9. Kliknij pozycję **Dalej**.
 10. Kliknij pozycję **OK**.
 11. Wyciągnij kabel Ethernet podłączony do komputera i skanera.
 12. Jeśli w kroku 2 na komputerze wyłączono standard IEEE 802.3az, włącz go.
 13. Podłącz do komputera i skanera wtyczki kabla Ethernet odłączone w kroku 1.
- Jeśli problem będzie występował nadal, przyczyna może leżeć po stronie urządzeń innych niż skaner.

■ Skaner jest wyłączony.

Rozwiązania

Upewnij się, czy skaner jest włączony.

Poczekaj, aż lampka stanu przestanie migać. To oznacza gotowość urządzenia do skanowania.

Oprogramowanie do konfigurowania skanera

Aplikacja konfiguracji obsługi skanera (Web Config)	38
Epson Device Admin.	39

Aplikacja konfiguracji obsługi skanera (Web Config)

Web Config jest aplikacją, którą uruchamia się w przeglądarkach internetowych na komputerach lub urządzeniach inteligentnych, np. Microsoft Edge i Safari. Umożliwia ona sprawdzenie stanu skanera lub zmianę usługi sieciowej oraz ustawień skanera. Aby skorzystać z aplikacji Web Config, podłącz skaner i komputer lub urządzenie do tej samej sieci.

Obsługiwane są następujące przeglądarki. Użyj najnowszej wersji.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Uwaga:

Podczas korzystania z urządzenia może zostać wyświetlony monit o wprowadzenie hasła administratora. Patrz podane poniżej sekcje, aby uzyskać szczegółowe informacje dotyczące hasła administratora.

[„Informacje dotyczące hasła administratora” na stronie 11](#)

Powiązane informacje

➔ [„Nie można uzyskać dostępu do aplikacji Web Config” na stronie 66](#)

Uruchamianie aplikacji Web Config w przeglądarce internetowej

Skaner jest wyposażony we wbudowane oprogramowanie o nazwie Web Config. Są to strony, na których można konfigurować ustawienia. Aby uzyskać dostęp do aplikacji Web Config, wystarczy w pasku adresu przeglądarki wprowadzić adres IP skanera połączonego z siecią.

1. Sprawdź adres IP skanera.

Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Ustawienia sieciowe** > **Stan sieci**. Następnie wybierz metodę aktywnego połączenia (**Stan sieci LAN/Wi-Fi** lub **Stan usługi Wi-Fi Direct**), aby potwierdzić adres IP skanera.

Przykładowy adres IP: 192.168.100.201

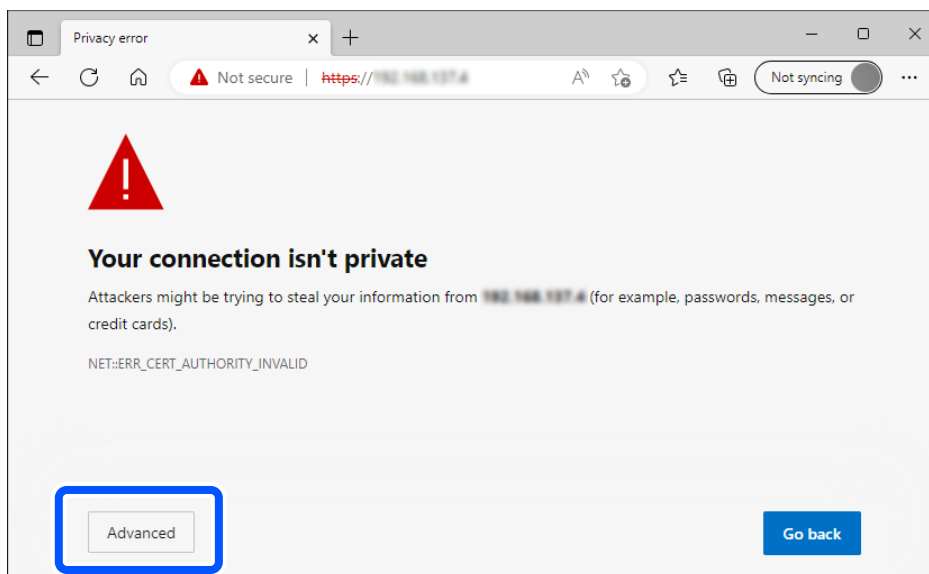
2. Uruchom na komputerze lub urządzeniu inteligentnym przeglądarkę, a następnie w pasku adresu wprowadź adres IP skanera.

Format: http://adres IP skanera/

Przykład: http://192.168.100.201/

Jeśli w przeglądarce zostanie wyświetlone ostrzeżenie, można je zignorować i wyświetlić stronę (aplikację Web Config). Ponieważ skaner wykorzystuje certyfikat z podpisem własnym do uzyskiwania dostępu do protokołu HTTPS, podczas uruchamiania aplikacji Web Config w przeglądarce wyświetlane jest ostrzeżenie. Nie oznacza to problemu i można je zignorować. W zależności od przeglądarki wyświetlenie strony może wymagać kliknięcia pozycji **Ustawienia zaawansowane**.

Przykład: przeglądarka Microsoft Edge



Uwaga:

Jeśli ostrzeżenie nie jest wyświetlane, przejdź do następnego kroku.

W przypadku adresów IPv6 użyj następującego formatu.

Format: `http://[adres IP skanera]/`

Przykład: `http://[2001:db8::1000:1]/`

3. Aby móc zmienić ustawienia skanera, musisz zalogować się na konto z uprawnieniami administratora aplikacji Web Config.

W prawym górnym rogu ekranu kliknij pozycję **zaloguj**. Wprowadź **Nazwa użytkownika** i **Aktualne hasło**, a następnie kliknij przycisk **OK**.

Poniżej przedstawiono wstępne wartości dla informacji administratora Web Config.

·Nazwa użytkownika: brak (puste)

·Hasło: jest uzależnione od etykiety przyklejonej na produkcie.

Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer. Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź numer seryjny znajdujący się na etykiecie przyklejonej z tyłu produktu.

Uwaga:

Jeśli w prawym górnym rogu ekranu wyświetlana jest pozycja **wyloguj**, oznacza to, że zalogowano już na konto administratora.

Po około 20 minutach braku aktywności nastąpi automatyczne wylogowanie.

Epson Device Admin

Epson Device Admin jest wielofunkcyjną aplikacją, która umożliwia zarządzanie urządzeniami w sieci.

Szablony konfiguracji umożliwiają stosowanie ujednoliconych ustawień do wielu skanerów w sieci, co ułatwia instalowanie i zarządzanie wieloma skanerami.

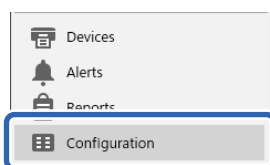
Aplikację Epson Device Admin można pobrać z witryny pomocy technicznej firmy Epson. Więcej informacji o korzystaniu z tej aplikacji można znaleźć w dokumentacji lub pomocy aplikacji Epson Device Admin.

Szablon konfiguracji

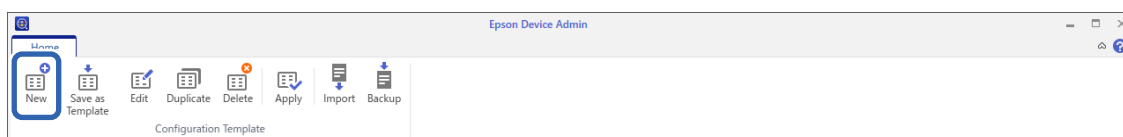
Tworzenie szablonu konfiguracji

Utwórz nowy szablon konfiguracji.

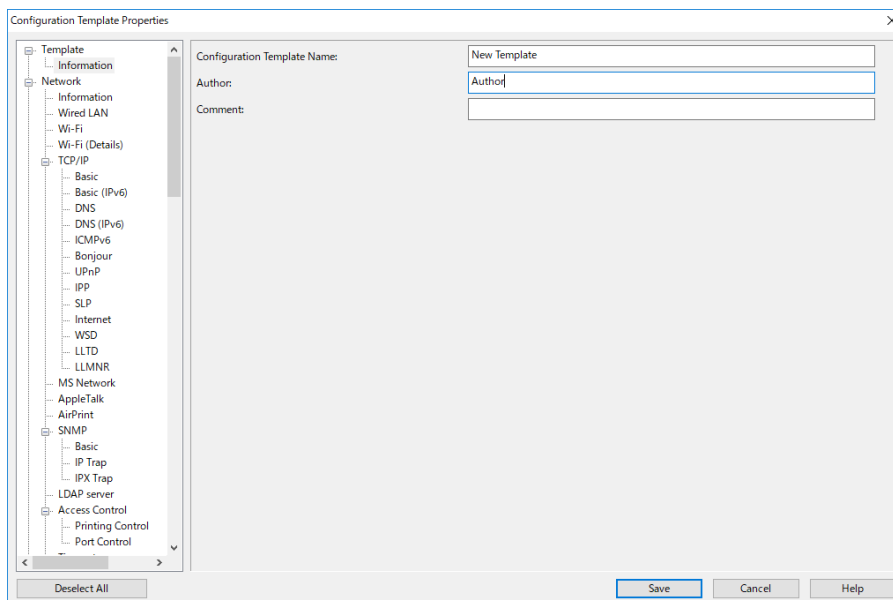
1. Uruchom aplikację Epson Device Admin.
2. Z bocznego menu zadań wybierz pozycję **Konfiguracja**.



3. Wybierz **Nowy** w menu wstążki.



4. Ustaw każdą pozycję.



Pozycja	Objaśnienie
Nazwa szablonu konfiguracji	Nazwa szablonu konfiguracji. Wprowadź maksymalnie 1024 znaki w kodowaniu Unicode (UTF-8).
Autor	Informacje dotyczące autora szablonu. Wprowadź maksymalnie 1024 znaki w kodowaniu Unicode (UTF-8).

Pozycja	Objaśnienie
Komentarz	Można wprowadzić dowolne informacje. Wprowadź maksymalnie 1024 znaki w kodowaniu Unicode (UTF-8).

5. Z lewej strony można wybrać pozycje do ustawienia.

Uwaga:

Klikaj pozycje menu po lewej stronie, aby przełączać się na każdy z ekranów. Ustawiona wartość jest zachowywana po przełączeniu na inny ekran, chyba że użyto opcji *Anuluj*. Po wprowadzeniu wszystkich ustawień kliknij przycisk *Zapisz*.

Zastosowanie szablonu konfiguracji

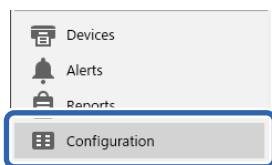
Zapisanych szablonów konfiguracji można używać na tym skanerze. Stosowane są pozycje wybrane w szablonie. Jeśli docelowy skaner nie posiada odpowiedniej funkcji, dana pozycja nie ma zastosowania.

Uwaga:

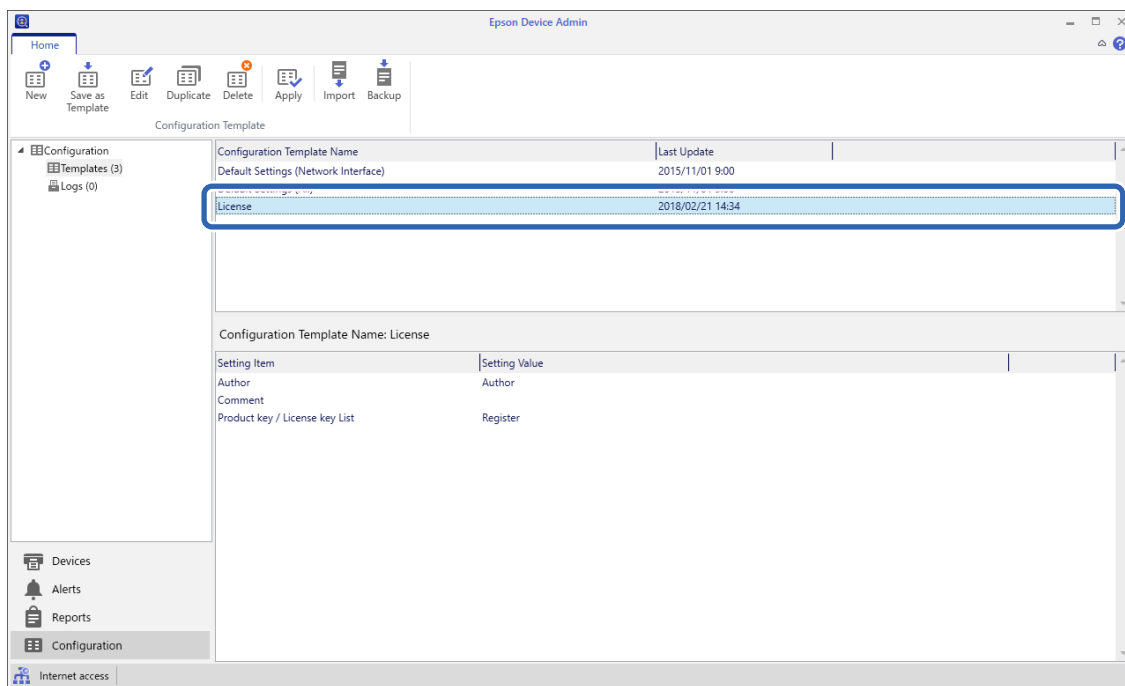
Gdy na skanerze ustawiane jest hasło administratora, skonfiguruj je z wyprzedzeniem.

1. Na wstążce menu w oknie *Lista urządzeń* wybierz pozycje **Opcjonalne > Menedżer haseł**.
2. Wybierz pozycję **Włącz automatyczne zarządzanie hasłami**, a następnie kliknij przycisk **Menedżer haseł**.
3. Wybierz odpowiedni skaner, a następnie kliknij **Edytuj**.
4. Ustaw hasło, a następnie kliknij przycisk **OK**.

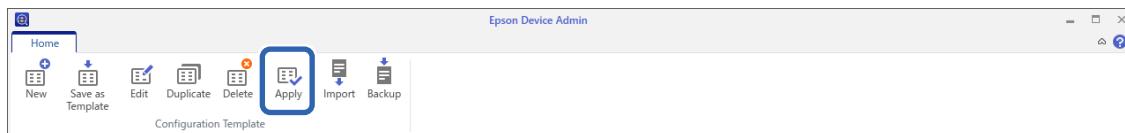
1. Z bocznego menu zadań wybierz pozycję **Konfiguracja**.



2. Wybierz szablon konfiguracji, który chcesz zastosować, w obszarze **Nazwa szablonu konfiguracji**.



3. Kliknij **Zastosuj** w menu wstążki.
Zostanie wyświetlony ekran wyboru urządzenia.

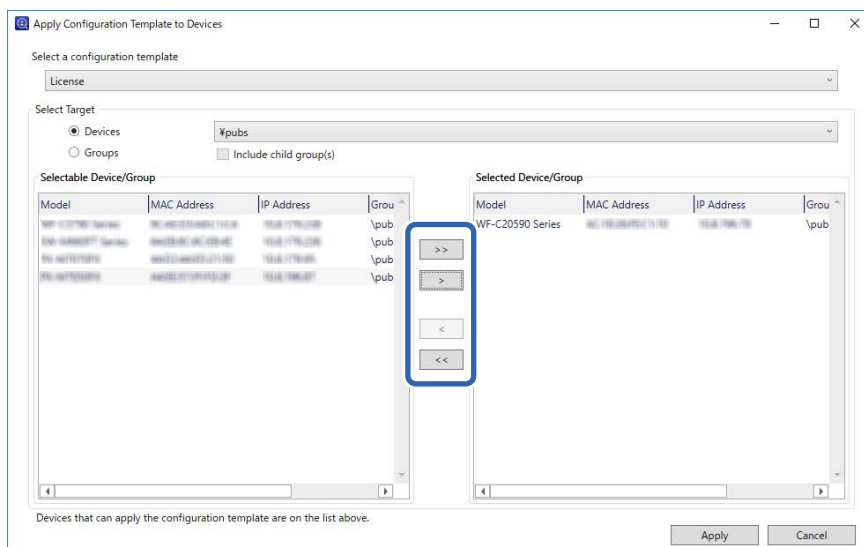


4. Wybierz szablon konfiguracji, który ma być zastosowany.

Uwaga:

- Po wyborze pozycji **Urządzenia** oraz grup zawierających urządzenia z menu rozwijanego wyświetlone zostaną wszystkie urządzenia.
- Grupy zostaną wyświetlone po wybraniu pozycji **Grupy**. Wybierz opcję **Uwzględnij grupę(y) podrzędną**, aby automatycznie wybrać grupy podrzędne w ramach wybranej grupy.

- Przenieś skaner lub grupy, do których ma być zastosowany szablon, do obszaru **Wybrane urządzenie/grupa**.



- Kliknij pozycję **Zastosuj**.

Zostanie wyświetlony ekran potwierdzenia szablonu konfiguracji, który ma być zastosowany.

- Wybierz przycisk **OK**, aby zastosować szablon konfiguracji.

- Po wyświetleniu komunikatu z informacją o zakończeniu procesu kliknij przycisk **OK**.

- Kliknij **Szczegóły** i sprawdź wyświetlane informacje.

Jeśli przy zastosowanych pozycjach wyświetlane jest oznaczenie , operacja zakończyła się powodzeniem.

- Kliknij pozycję **Zamknij**.

Ustawienia niezbędne do skanowania

Rejestrowanie serwera poczty e-mail.	45
Tworzenie folderu sieciowego.	48
Udostępnianie kontaktów.	55
Konfiguracja funkcji AirPrint.	65
Problemy podczas przygotowywania skanowania sieciowego.	66

Rejestrowanie serwera poczty e-mail

Przed konfiguracją serwera e-maili należy sprawdzić następujące elementy.

- Sprawdź, czy skaner jest podłączony do sieci
- Informacje o konfiguracji serwera poczty e-mail

W przypadku korzystania z serwera poczty e-mail w Internecie należy uzyskać informacje o serwerze od dostawcy lub z witryny.

Rejestracja

Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Sieć > Serwer e-mail > Podstawowe**.

„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Ustawienia można też konfigurować na panelu sterowania skanera. Wybierz pozycje **Ustaw. > Ustawienia sieciowe > Zaawansowane > Serwer e-mail > Ustaw. serwera**.

Elementy ustawień serwera e-mail

Pozycja	Ustawienia i objaśnienie	
Sposób uwierzytelniania	Określ metodę uwierzytelniania używaną przez skaner w celu uzyskania dostępu do serwera pocztowego.	
	Wył.	Uwierzytelnianie jest wyłączone w przypadku komunikacji z serwerem pocztowym.
	UWIERZYTELNIANIE SMTP	Serwer pocztowy wymaga obsługi uwierzytelniania SMTP.
	POP przed SMTP	Po zaznaczeniu tej pozycji skonfiguruj serwer POP3.
Konto uwierzytelnione	Jeśli opcja Sposób uwierzytelniania jest ustawiona na UWIERZYTELNIANIE SMTP lub POP przed SMTP , wprowadź nazwę uwierzytelnianego konta. Wprowadź od 0 do 255 znaków ASCII (0x20–0x7E).	
Hasło uwierzytelnione	Jeśli opcja Sposób uwierzytelniania jest ustawiona na UWIERZYTELNIANIE SMTP lub POP przed SMTP , wprowadź hasło uwierzytelnianego konta. Wprowadź od 0 do 20 znaków ASCII (0x20–0x7E).	
Adres email wysyłającego	Ustaw adres e-mail, który będzie używany przez skaner do wysyłania wiadomości e-mail. W tej opcji można użyć istniejącego adresu e-mail. Zaleca się jednak utworzenie dedykowanego adresu e-mail, tak aby ułatwić rozpoznawanie poczty e-mail wysyłanej ze skanera. Wprowadź od 0 do 255 znaków ASCII (0x20–0x7E) z wyjątkiem następujących znaków: : () < > [] ; ¥. Kropka „.” nie może być pierwszym znakiem.	
Adres serwera SMTP	Wprowadź od 0 do 255 znaków: A–Z a–z 0–9. -. Można użyć formatu IPv4 lub FQDN.	
Numer portu serwera SMTP	Podaj liczbę od 1 do 65535.	

Pozycja	Ustawienia i objaśnienie	
Bezpieczne połączenie	Określ bezpieczną metodę połączenia dla serwera e-mail.	
	Brak	Jeśli wybrano opcję POP przed SMTP jako ustawienie Sposób uwierzytelniania , metoda połączenia będzie mieć ustawienie Brak .
	SSL/TLS	Opcja ta jest dostępna, jeśli Sposób uwierzytelniania ma ustawienie Wył. lub UWIERZYTELNIANIE SMTP .
	STARTTLS	Opcja ta jest dostępna, jeśli Sposób uwierzytelniania ma ustawienie Wył. lub UWIERZYTELNIANIE SMTP .
Weryfikacja certyfikatu (wyłącznie w systemie Web Config)	Włączenie tej opcji powoduje zweryfikowanie certyfikatu. Zaleca się ustawienie tej opcji na Włącz , gdy opcja Bezpieczne połączenie ma ustawienie inne niż Brak .	
Adres serwera POP3	Jeśli opcja Sposób uwierzytelniania jest ustawiona na POP przed SMTP , wprowadź adres serwera POP3. Można wprowadzić od 0 do 255 znaków: A–Z a–z 0–9. Można użyć formatu IPv4 lub FQDN.	
Numer portu serwera POP3	Ustaw po wybraniu POP przed SMTP w obszarze Sposób uwierzytelniania . Podaj liczbę od 1 do 65535.	

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Sprawdzanie połączenie serwera e-mail

1. Wybierz menu testowania połączenia.

W przypadku konfiguracji w aplikacji Web Config:

Wybierz pozycje **Sieć > Serwer e-mail > Test połączenia > Start**.

W przypadku konfiguracji z poziomu panelu sterowania:

Wybierz pozycje **Ustaw. > Ustawienia sieciowe > Zaawansowane > Serwer e-mail > Sprawdzanie połączenia**.

Uruchomiony zostanie test połączenia z serwerem e-mail.

2. Sprawdź wyniki testu.

Pomyślne ukończenie testu wskazuje komunikat **Test połączenia zakończony powodzeniem..**

Jeśli zamiast niego wyświetlany jest komunikat o błędzie, postępuj zgodnie z instrukcjami w komunikacie, aby skasować błąd.

„Objaśnienia do testu połączenia z serwerem pocztowym” na stronie 47

Objaśnienia do testu połączenia z serwerem pocztowym

Komunikat	Przyczyna
Błąd komunikacji serwera SMTP. Sprawdź następujące elementy. - Ustawienia sieci	Sytuacje, w których ten komunikat jest wyświetlany <ul style="list-style-type: none"> <input type="checkbox"/> Skaner nie jest połączony z siecią <input type="checkbox"/> Serwer SMTP nie działa <input type="checkbox"/> Połączenie sieciowe zostało rozłączone w trakcie komunikacji <input type="checkbox"/> Odebrano niepełne dane
Błąd komunikacji serwera POP3. Sprawdź następujące elementy. - Ustawienia sieci	Sytuacje, w których ten komunikat jest wyświetlany <ul style="list-style-type: none"> <input type="checkbox"/> Skaner nie jest połączony z siecią <input type="checkbox"/> Serwer POP3 nie działa <input type="checkbox"/> Połączenie sieciowe zostało rozłączone w trakcie komunikacji <input type="checkbox"/> Odebrano niepełne dane
Podczas łączenia z serwerem SMTP wystąpił błąd. Sprawdź następujące elementy. - Adres serwera SMTP - Serwer DNS	Sytuacje, w których ten komunikat jest wyświetlany <ul style="list-style-type: none"> <input type="checkbox"/> Połączenie z serwerem DNS nie powiodło się <input type="checkbox"/> Rozwiązywanie nazwy serwera SMTP nie powiodło się
Podczas łączenia z serwerem POP3 wystąpił błąd. Sprawdź następujące elementy. - Adres serwera POP3 - Serwer DNS	Sytuacje, w których ten komunikat jest wyświetlany <ul style="list-style-type: none"> <input type="checkbox"/> Połączenie z serwerem DNS nie powiodło się <input type="checkbox"/> Rozwiązywanie nazwy serwera POP3 nie powiodło się
Błąd uwierzytelnienia serwera SMTP. Sprawdź następujące elementy. - Metoda uwierzytelniania - Uwierzytelnione konto - Uwierzytelnione hasło	Ten komunikat jest wyświetlany, gdy uwierzytelnianie na serwerze SMTP nie powiedzie się.
Błąd uwierzytelnienia serwera POP3. Sprawdź następujące elementy. - Metoda uwierzytelniania - Uwierzytelnione konto - Uwierzytelnione hasło	Ten komunikat jest wyświetlany, gdy uwierzytelnianie na serwerze POP3 nie powiedzie się.
Nieobsługiwana metoda komunikacji. Sprawdź następujące elementy. - Adres serwera SMTP - Numer portu serwera SMTP.	Ten komunikat jest wyświetlany podczas próby komunikacji przy użyciu nieobsługiwanych protokołów.
Połączenie z serwerem SMTP nie powiodło się. Zmień Bezpieczne połączenie na Brak.	Ten komunikat pojawia się w przypadku niezgodności SMTP między serwerem a klientem lub gdy serwer nie obsługuje zabezpieczonego połączenia SMTP (połączenie SSL).
Połączenie z serwerem SMTP nie powiodło się. Zmień Bezpieczne połączenie na SSL/TLS.	Ten komunikat jest wyświetlany, gdy wystąpi niezgodność SMTP między serwerem a klientem lub gdy serwer wysłał żądania użycia połączenia SSL/TLS w celu ustanowienia bezpiecznego połączenia SMTP.
Połączenie z serwerem SMTP nie powiodło się. Zmień Bezpieczne połączenie na STARTTLS.	Ten komunikat jest wyświetlany, gdy wystąpi niezgodność SMTP między serwerem a klientem lub gdy serwer wysłał żądania użycia połączenia STARTTLS w celu ustanowienia bezpiecznego połączenia SMTP.
Połączenie jest podejrzone. Sprawdź następujące elementy. - Data i godzina	Ten komunikat jest wyświetlany, gdy data i godzina na skanerze są niepoprawne lub certyfikat wygasł.

Komunikat	Przyczyna
Połączenie jest podejrzanе. Sprawdź następujące elementy. - Certyfikat CA	Ten komunikat jest wyświetlany, gdy na skanerze nie ma głównego certyfikatu odpowiadającego serwerowi lub nie zaimportowano certyfikatu Certyfikat CA.
Połączenie nie jest zabezpieczone.	Ten komunikat jest wyświetlany, gdy uzyskany certyfikat jest uszkodzony.
Uwierzytelnienie serwera SMTP nie powiodło się. Zmień metodę uwierzytelnienia na SMTP-AUTH.	Ten komunikat jest wyświetlany, gdy wystąpi niezgodność metody uwierzytelniania między serwerem a klientem. Serwer obsługuje metodę UWIERZYTELNIANIE SMTP.
Uwierzytelnienie serwera SMTP nie powiodło się. Zmień metodę uwierzytelnienia na POP przed SMTP.	Ten komunikat jest wyświetlany, gdy wystąpi niezgodność metody uwierzytelniania między serwerem a klientem. Serwer nie obsługuje metody UWIERZYTELNIANIE SMTP.
Nieprawidłowy adres e-mail nadawcy. Zmień na adres e-mail dla używanej usługi e-mail.	Ten komunikat jest wyświetlany, gdy podany adres e-mail nadawcy jest błędny.
Dostęp do urządzenia można uzyskać dopiero po zakończeniu przetwarzania.	Ten komunikat jest wyświetlany, gdy skaner jest zajęty.

Tworzenie folderu sieciowego

Folder sieciowy tworzy się na komputerze. Używany komputer musi być połączony z tą samą siecią co skaner.


Metoda konfigurowania folderu sieciowego różni się w zależności od środowiska. W tym przykładzie przedstawiono tworzenie folderu sieciowego na pulpicie komputera w następującym środowisku.

- System operacyjny: Windows 10
- Lokalizacja tworzenia folderu udostępnionego: pulpit
- Ścieżka folderu: C:\Users\xxxx\Desktop\scan_folder (na pulpicie utwórz folder sieciowy o nazwie „scan_folder”)

1. Zaloguj się na komputerze, na którym ma być utworzony folder sieciowy. Do zalogowania użyj konta użytkownika z uprawnieniami administratora.

Uwaga:

Jeśli konto użytkownika z uprawnieniami administratora nie jest znane, należy skontaktować się z administratorem komputera.

2. Upewnij się, że nazwa urządzenia (nazwa komputera) nie zawiera znaków dwubajtowych. Kliknij przycisk Start w systemie Windows, a następnie wybierz polecenia  **Ustawienia** > **System** > **Informacje**.

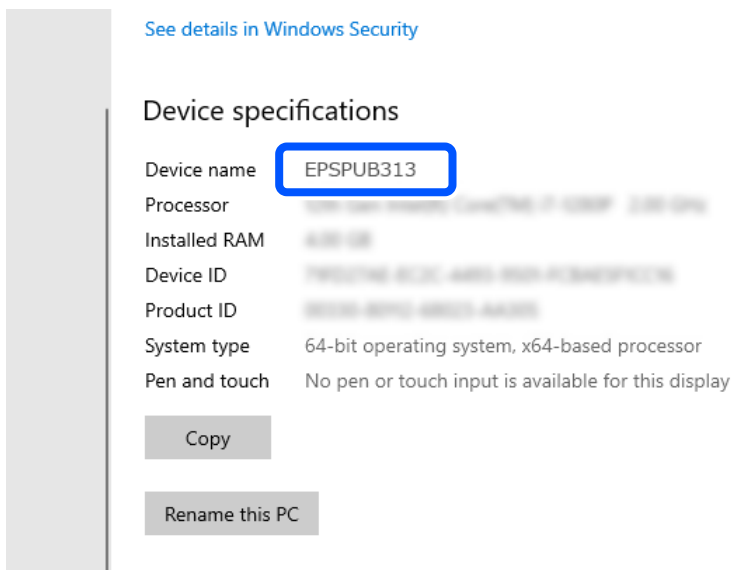
Uwaga:

Jeśli w nazwie urządzenia będą znaki dwubajtowe, zapisanie pliku może się nie udać.

3. Sprawdź, czy ciąg tekstowy wyświetlany w polu **Specyfikacja urządzenia** > **Nazwa urządzenia** nie zawiera żadnych znaków dwubajtowych.

Nazwy urządzenia zawierające tylko znaki jednobajtowe nie powinny powodować problemów. Zamknij ekran.

Przykład: EPSPUB313



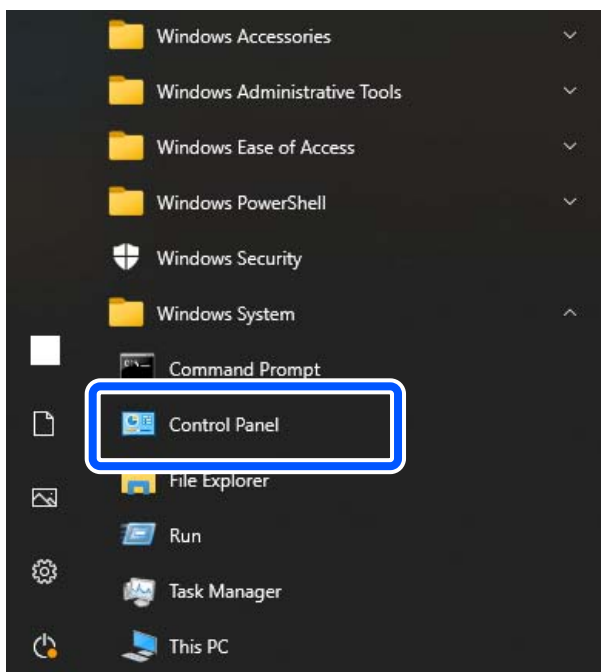
Ważne:

Jeśli nazwa urządzenia zawiera znaki dwubajtowe, należy użyć komputera, którego nazwa nie zawiera znaków dwubajtowych, lub zmienić nazwę danego urządzenia.

Jeśli zachodzi potrzeba zmiany nazwy urządzenia, należy skontaktować się z administratorem. Zmiana nazwy może wpłynąć na możliwość zarządzania komputerem i dostępem do zasobów.

Sprawdź ustawienia komputera.

4. Kliknij przycisk Start w systemie Windows, a następnie wybierz polecenia **System Windows > Panel sterowania**.



5. W oknie Panel sterowania kliknij pozycje **Sieć i Internet > Centrum sieci i udostępniania > Zmień zaawansowane ustawienia udostępniania**.

Zostanie wyświetlony profil sieciowy.

6. Upewnij się, że w bieżącym profilu w obszarze **Udostępnianie plików i drukarek** zaznaczona jest opcja **Włącz udostępnianie plików i drukarek**.

Jeśli opcja jest już zaznaczona, kliknij przycisk **Anuluj** i zamknij okno.

Po zmianie ustawień kliknij przycisk **Zapisz zmiany**, a następnie zamknij okno.

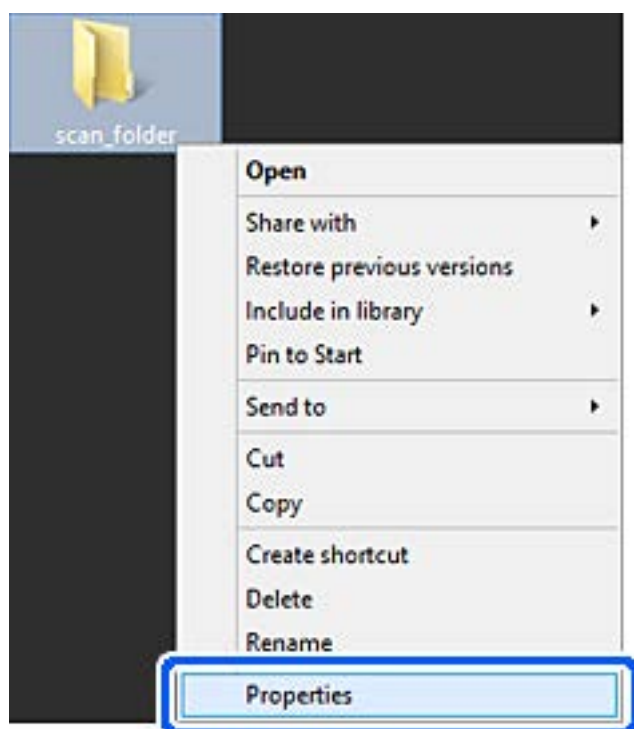
Utwórz folder sieciowy.

7. Utwórz folder na pulpicie i nadaj mu nazwę.

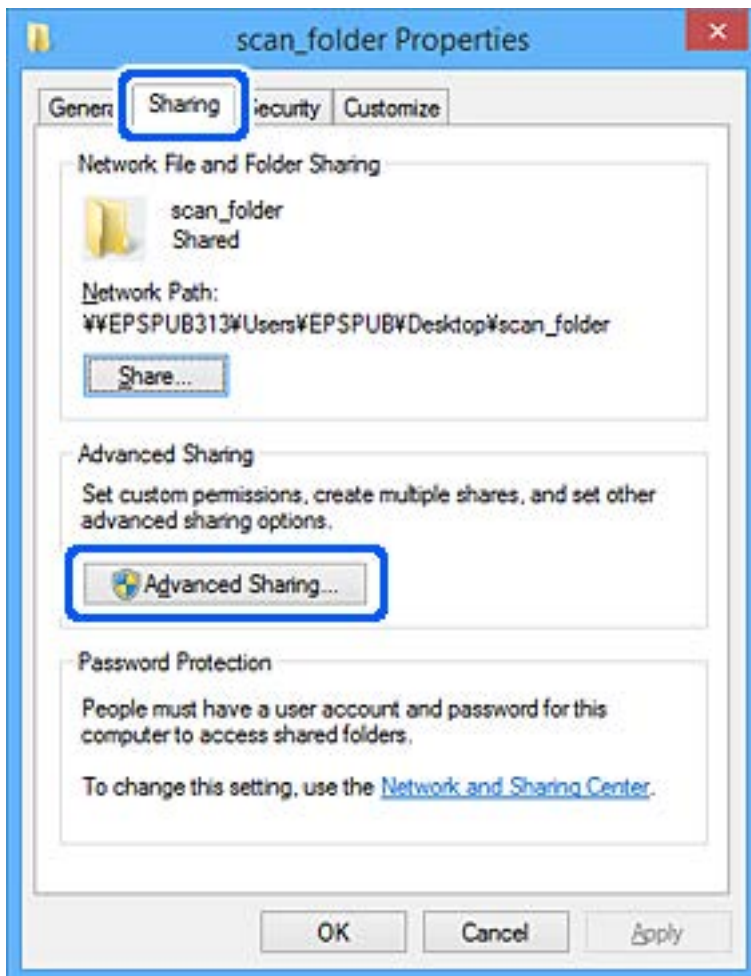
W przypadku nazwy folderu wprowadź od 1 do 12 znaków alfanumerycznych. Jeśli nazwa będzie miała więcej niż 12 znaków, uzyskanie dostępu do folderu może nie być możliwe w zależności od otoczenia sieciowego.

Przykład: scan_folder

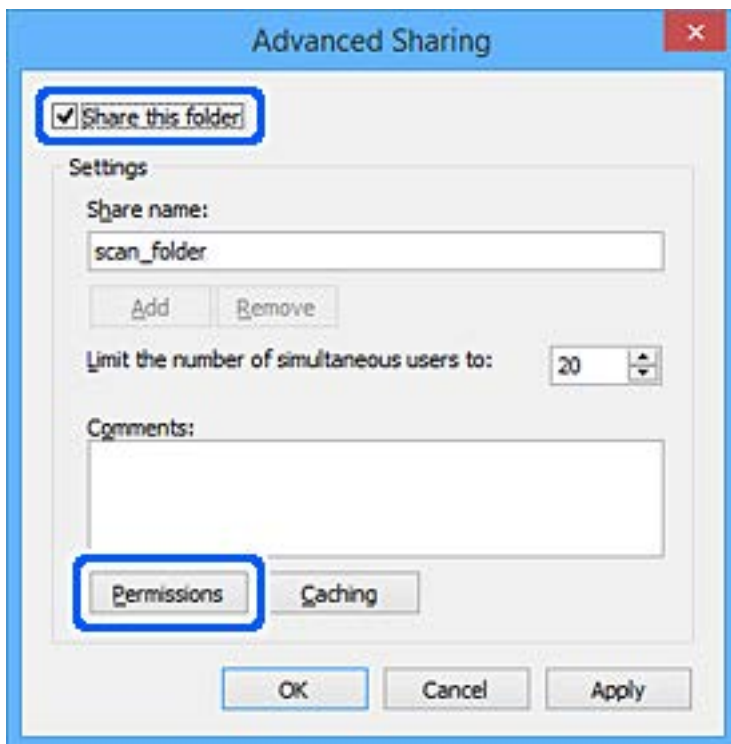
8. Kliknij prawym przyciskiem folder, a następnie wybierz polecenie **Właściwości**.



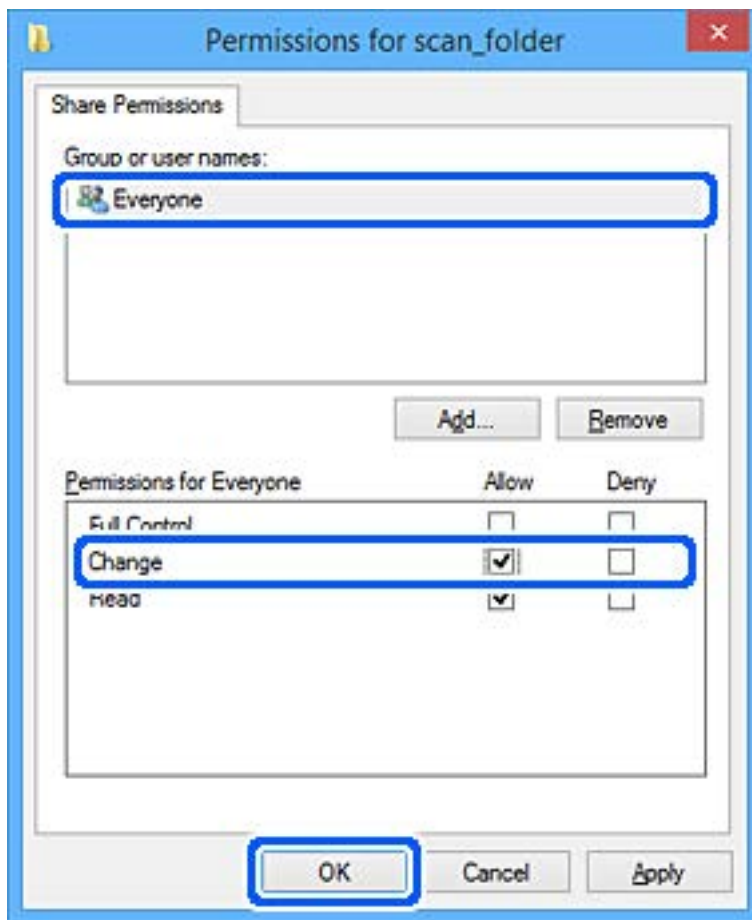
9. Na karcie **Udostępnianie** kliknij przycisk **Udostępnianie zaawansowane**.



10. Wybierz pozycję **Udostępnij ten folder**, a następnie kliknij przycisk **Uprawnienia**.



11. W polu **Nazwy grupy lub użytkownika** wybierz pozycję **Wszyscy**, w kolumnie **Zmiana** wybierz ustawienie **Zezwól**, a następnie kliknij przycisk **OK**.

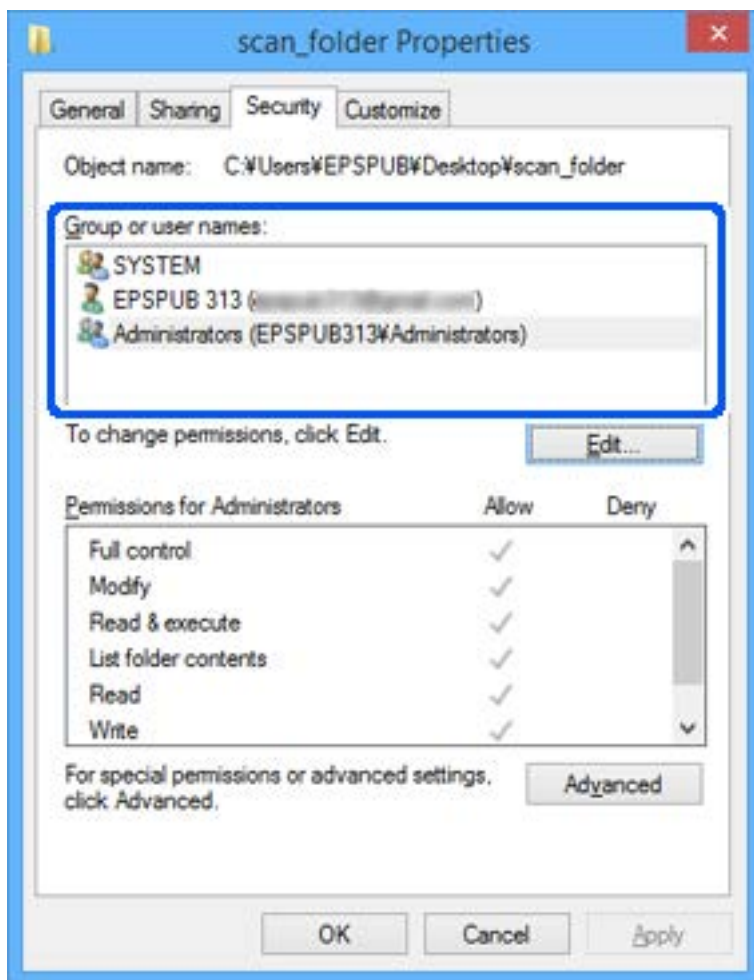


12. Kliknij przycisk **OK**, aby zamknąć okno i wrócić do okna Właściwości.

Uwaga:

Grupy użytkowników lub użytkowników z przyznanym dostępem do folderu sieciowego można sprawdzać na karcie **Zabezpieczenia** > **Nazwy grupy lub użytkownika**.

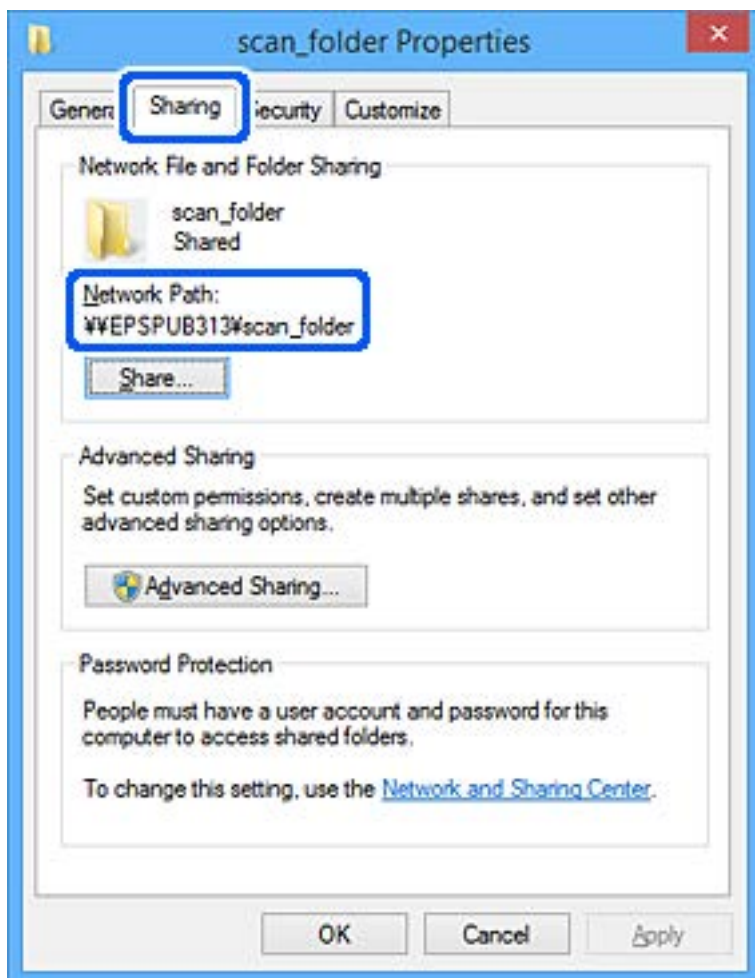
Przykład: dostęp do folderu sieciowego ma użytkownik zalogowany na komputerze, a także grupa Administratorzy.



13. Przejdź do karty **Udostępnianie**.

Zostanie wyświetlona ścieżka sieciowa folderu sieciowego. Jest używana podczas rejestrowania w kontaktach na skanerze. Zapisz ją.

Przykład: \\EPSPUB313\scan_folder



14. Kliknij przycisk **Zamknij** lub **OK**, aby zamknąć okno.

Tworzenie folderu sieciowego zostało ukończone.

Udostępnianie kontaktów

Zarejestrowanie miejsc docelowych na liście kontaktów skanera pozwala na łatwe wprowadzenie miejsca docelowego podczas skanowania.

Na liście kontaktów można zarejestrować następujące rodzaje miejsc docelowych. Łącznie można zarejestrować do 300 pozycji.

Uwaga:

Można także do wprowadzenia miejsca docelowego wykorzystać serwer LDAP (wyszukiwanie LDAP).

E-mail	Miejsce docelowe wiadomości e-mail. Wcześniej trzeba skonfigurować ustawienia serwera poczty e-mail.
Folder sieciowy	Miejsce docelowe danych skanowania. Przedtem należy odpowiednio przygotować folder sieciowy.

Powiązane informacje

➔ „Obsługa użytkowników i serwera LDAP” na stronie 62

Porównanie możliwych konfiguracji kontaktów

Listę kontaktów skanera można skonfigurować za pomocą trzech narzędzi: panelu sterowania skanera oraz narzędzia Web Config i Epson Device Admin. Poniższa tabela objaśnia różnice między możliwościami konfiguracji dostępnymi w przypadku każdego z tych narzędzi.

Funkcje	Web Config*	Epson Device Admin	Panel sterowania skanera
Rejestracja miejsca docelowego	✓	✓	✓
Edycja miejsca docelowego	✓	✓	✓
Dodanie grupy	✓	✓	✓
Edycja grupy	✓	✓	✓
Usunięcie miejsca docelowego lub grupy	✓	✓	✓
Usunięcie wszystkich miejsc docelowych	✓	✓	–
Zaimportowanie pliku	✓	✓	–
Wyeksportowanie pliku	✓	✓	–

* Aby zmieniać ustawienia należy zalogować się jako administrator.

Rejestrowanie miejsca docelowego w kontaktach za pomocą aplikacji Web Config

Uwaga:

Można też rejestrować kontakty z poziomu panelu sterowania skanera.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Skanuj > Kontakty**.
2. Wybierz numer, które ma być zarejestrowany, a następnie kliknij przycisk **Edytuj**.
3. Wprowadź wartości w polach **Nazwa** i **Hasło indeksu**.
4. Wybierz typ miejsca docelowego w opcji **Typ**.

Uwaga:

Nie można zmieniać opcji **Typ** po zakończeniu rejestracji. Aby zmienić typ, należy usunąć miejsce docelowe, a potem zarejestrować je ponownie.

5. Wprowadź wartości poszczególnych pozycji, a następnie kliknij przycisk **Zastosuj**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Elementy ustawień miejsca docelowego

Elementy	Ustawienia i objaśnienie
Ustawienia wspólne	
Nazwa	Umożliwia wprowadzenie nazwy wyświetlanej na liście kontaktów o długości do 30 znaków w formacie Unicode (UTF-16). Jeśli ustawienie nie będzie określone, zostaw puste pole.
Hasło indeksu	Wprowadź nazwę o maksymalnie 30 znakach w kodowaniu Unicode (UTF-16), aby wyszukać kontakty na panelu sterowania skanera. Jeśli ustawienie nie będzie określone, zostaw puste pole.
Typ	Wybór typu adresu, który ma być zarejestrowany.
Przypisz do częst. używan.	Określenie zarejestrowanego adresu jako często używanego adresu. Często używane adresy są wyświetlane na górze ekranu skanowania, co pozwala na określenie miejsca docelowego bez wyświetlania kontaktów.
E-mail	
Adres email	Umożliwia wprowadzenie adresu e-mail o długości od 1 do 255 znaków: A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Folder sieciowy (SMB)	
Zapisz do	\\„Ścieżka do folderu” Umożliwia wprowadzenie lokalizacji folderu docelowego. Ścieżka musi mieć od 1 do 253 znaków w formacie Unicode (UTF-16), nie uwzględniając ciągu „\”. Wprowadź ścieżkę sieciową wyświetloną na ekranie właściwości folderu. Sprawdź następujące informacje dotyczące ustawiania ścieżki sieciowej. „Tworzenie folderu sieciowego” na stronie 48
Nazwa użytkownika	Umożliwia wprowadzenie nazwy użytkownika używanej do uzyskiwania dostępu do folderu sieciowego. Nazwa musi mieć do 30 znaków w formacie Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F).
Hasło	Wprowadź hasło dostępu do folderu sieciowego zawierające od 0 do 20 znaków w formacie Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F).
FTP	
Bezpieczne połączenie	Wybierz protokół FTP lub FTPS w zależności od protokołu transferu plików obsługiwanego przez serwer FTP. Wybierz pozycję FTPS , aby pozwolić skanerowi na komunikację z zabezpieczeniami.
Zapisz do	Wprowadź nazwę serwera zawierającą od 1 do 253 znaków w formacie Unicode (UTF-16), pomijając „ftp://” lub „ftps://”.

Elementy	Ustawienia i objaśnienie
Nazwa użytkownika	Umożliwia wprowadzenie nazwy użytkownika używanej do uzyskiwania dostępu do serwera FTP. Nazwa musi mieć do 30 znaków w formacie Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli serwer zezwala na połączenia anonimowe, podaj nazwę użytkownika typu Anonymous lub FTP. Jeśli ustawienie nie będzie określone, zostaw puste pole.
Hasło	Podaj hasło używane przy logowaniu na serwer FTP. Hasło musi zawierać od 0 do 20 znaków Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określone, zostaw puste pole.
Tryb połączenia	Wybór trybu połączenia z menu. Jeśli między skanerem a serwerem FTP znajduje się zaporę, wybierz opcję Tryb pasywny .
Numer portu	Umożliwia wprowadzenie numeru portu serwera FTP w zakresie od 1 do 65535.
Weryfikacja certyfikatu	Certyfikat serwera FTP jest weryfikowany po włączeniu tej opcji. Opcja jest dostępna, tylko jeśli wybrano ustawienie FTPS dla opcji Bezpieczne połączenie . Aby skonfigurować tę opcję, należy zaimportować Certyfikat CA na skanerze.
SharePoint(WebDAV)*	
Bezpieczne połączenie	Wybierz protokół HTTP lub HTTPS w zależności od protokołu transferu plików obsługiwanego przez serwer. Wybierz pozycję HTTPS , aby pozwolić skanerowi na komunikację z zabezpieczeniami.
Zapisz do	Wprowadź nazwę serwera zawierającą od 1 do 253 znaków w formacie Unicode (UTF-16), pomijając „http://” lub „https://”.
Nazwa użytkownika	Umożliwia wprowadzenie nazwy użytkownika używanej do uzyskiwania dostępu do serwera. Nazwa musi mieć do 30 znaków w formacie Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określone, zostaw puste pole.
Hasło	Wprowadź hasło dostępu do serwera zawierające od 0 do 20 znaków w formacie Unicode (UTF-16). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określone, zostaw puste pole.
Weryfikacja certyfikatu	Certyfikat serwera jest weryfikowany po włączeniu tej opcji. Opcja jest dostępna, tylko jeśli wybrano ustawienie HTTPS dla opcji Bezpieczne połączenie . Aby skonfigurować tę opcję, należy zaimportować Certyfikat CA na skanerze.
Serwer proxy	Wybierz, czy korzystać z serwera proxy.

* SharePoint Online nie jest obsługiwana w przypadku skanowania do folderu sieciowego z panelu sterowania skanera.

Jeśli chcesz zapisać zeskanowany obraz w usłudze SharePoint Online, użyj Document Capture Pro po zainstalowaniu SharePoint Online Connector. Szczegóły zawiera instrukcja do aplikacji Document Capture Pro.

<https://support.epson.net/dcp/>

Rejestrowanie miejsc docelowych jako grupy z użyciem Web Config

Jeśli typ miejsca docelowego jest ustawiony na **E-mail**, można rejestrować miejsca docelowe jako grupy.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycję **Skanuj > Kontakty**.

- Wybierz numer, które ma być zarejestrowany, a następnie kliknij przycisk **Edytuj**.
- Z listy **Typ** wybierz grupę.
- Kliknij pozycję **Wybierz** w obszarze **Kontakty dla Grupa**.
Zostaną wyświetlone dostępne miejsca docelowe.
- Zaznacz miejsca docelowe, które mają być zarejestrowane w grupie, a następnie kliknij przycisk **Wybierz**.
- Wprowadź wartości w polach **Nazwa** i **Hasło indeksu**.
- Określ, czy przydzielić zarejestrowaną grupę do często używanych grup.
Uwaga:
Miejsca docelowe można rejestrować w wielu grupach.
- Kliknij pozycję **Zastosuj**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Tworzenie kopii zapasowej kontaktów i ich importowanie

Używając aplikacji Web Config lub innych narzędzi, można tworzyć kopie zapasowe kontaktów i je importować.

W przypadku aplikacji Web Config można utworzyć kopię zapasową kontaktów, eksportując ustawienia skanera zawierające kontakty. Wyeksportowanego pliku nie można edytować, ponieważ jest to plik binarny.

Podczas importowania ustawień skanera na skanerze kontakty są nadpisywane.

W przypadku aplikacji Epson Device Admin na ekranie właściwości urządzenia można eksportować tylko kontakty. Jeżeli eksport nie obejmuje pozycji związanych z bezpieczeństwem, można edytować wyeksportowane kontakty i zaimportować je, ponieważ są zapisywane w pliku SYLK lub CSV.

Importowanie kontaktów z wykorzystaniem Web Config

Jeśli użytkownik ma skaner, który umożliwia tworzenie kopii zapasowej kontaktów i jest zgodny z tym skanerem, można zarejestrować kontakty, importując plik kopii zapasowej.

Uwaga:

Więcej informacji o tworzeniu kopii zapasowej kontaktów skanera można znaleźć w podręczniku dostarczonym ze skanerem.

Wykonaj następujące czynności, aby zaimportować kontakty na tym skanerze.

- Uruchom aplikację Web Config, wybierz pozycje **Zarządzanie urządzeniem > Wartość ustawienia Eksportuj i Importuj > Importuj**.
- W polu **Plik** wybierz plik kopii zapasowej, wprowadź hasło, a następnie kliknij przycisk **Dalej**.
- Zaznacz pole wyboru **Kontakty**, a następnie kliknij przycisk **Dalej**.

Wykonywanie kopii zapasowych kontaktów przy użyciu Web Config

Usterka skanera może spowodować utratę danych kontaktów. Po każdej zmianie danych zaleca się wykonanie ich kopii zapasowej. Firma Epson nie ponosi odpowiedzialności za utratę danych, za wykonanie kopii zapasowej danych i/lub ustawień lub jej przywrócenie nawet w okresie gwarancji.

Aplikacja Web Config umożliwia wykonanie kopii zapasowej kontaktów przechowywanych na skanerze i zapisanie jej na komputerze.

1. Otwórz aplikację Web Config i wybierz pozycje **Zarządzanie urządzeniem > Wartość ustawienia Eksportuj i Importuj > Eksportuj**.
2. Zaznacz pole wyboru **Kontakty** w kategorii **Skanuj**.
3. Wprowadź hasło, aby zaszyfrować wyeksportowany plik.
Hasło będzie potrzebne do zaimportowania pliku. Pozostaw to pole puste, aby zrezygnować z szyfrowania pliku.
4. Kliknij przycisk **Eksportuj**.

Eksportowanie i importowanie wielu kontaktów za pomocą narzędzia

Narzędzie Epson Device Admin umożliwia utworzenie kopii zapasowej tylko kontaktów i edytowanie wyeksportowanego pliku, a następnie ich jednoczesne zaimportowanie.

Jest to przydatne do tworzenia kopii zapasowej tylko kontaktów lub w przypadku wymiany skanera i konieczności przeniesienia kontaktów ze starego skanera na nowy.

Eksportowanie kontaktów

Informacje o kontaktach można zapisywać w pliku.

Pliki zapisane w formacie SYLK lub csv można edytować w aplikacji arkusza kalkulacyjnego lub edytorze tekstowym. Po usunięciu lub dodaniu informacji można zaimportować wszystkie te kontakty na raz.

Informacje zawierające elementy zabezpieczeń, takie jak hasła i dane osobowe, są zapisywane w pliku binarnym zabezpieczonym hasłem. Nie można edytować tego pliku. Tego pliku można używać jako kopii zapasowej informacji zawierających elementy zabezpieczeń.

1. Uruchom aplikację Epson Device Admin.
2. Z bocznego menu zadań wybierz pozycję **Urządzenia**.
3. Z listy urządzeń wybierz urządzenie, które ma być skonfigurowane.
4. Na karcie wstążki **Ekran główny** kliknij pozycję **Konfiguracja urządzenia**.
Jeśli zostało ustawione hasło administratora, wprowadź hasło i kliknij przycisk **OK**.
5. Kliknij pozycje **Wspólny > Kontakty**.

- Wybierz format eksportu w oknie **Eksportuj** > **Elementy eksportu**.
 - Wszystkie elementy
Eksport zaszyfrowanego pliku binarnego. Wybierz, czy w pliku mają być zapisane elementy zabezpieczeń, takie jak hasła i dane osobowe. Nie można edytować tego pliku. Jeśli zostanie wybrany ten format, trzeba ustawić hasło do pliku. Kliknij przycisk **Konfiguracja** i ustaw hasło o długości od 8 do 63 znaków ASCII. To hasło będzie potrzebne podczas importowania danych z pliku binarnego.
 - Elementy poza informacjami o zabezpieczeniu
Eksport pliku w formacie SYLK lub csv. Tę opcję wybierz, aby móc edytować informacje w wyeksportowanym pliku.
- Kliknij pozycję **Eksportuj**.
- Określ miejsce zapisu, wybierz typ pliku, a następnie kliknij przycisk **Zapisz**.
Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.
- Kliknij pozycję **OK**.
Sprawdź, czy plik został zapisany w wybranym miejscu.

Importowanie kontaktów

Informacje o kontaktach można zaimportować z pliku.

Możliwe jest importowanie plików zapisanych w formacie SYLK lub csv albo plików binarnych zawierających elementy zabezpieczeń.

- Uruchom aplikację Epson Device Admin.
- Z bocznego menu zadań wybierz pozycję **Urządzenia**.
- Z listy urządzeń wybierz urządzenie, które ma być skonfigurowane.
- Na karcie wstążki **Ekran główny** kliknij pozycję **Konfiguracja urządzenia**.
Jeśli zostało ustawione hasło administratora, wprowadź hasło i kliknij przycisk **OK**.
- Kliknij pozycję **Wspólny** > **Kontakty**.
- Kliknij przycisk **Przeglądaj** w obszarze **Importuj**.
- Wybierz plik, który ma być zaimportowany, a następnie kliknij przycisk **Otwórz**.
Po wybraniu pliku binarnego w polu **Hasło** wprowadź hasło ustawione podczas eksportowania pliku.
- Kliknij pozycję **Importuj**.
Zostanie wyświetlony ekran potwierdzenia.
- Kliknij pozycję **OK**.
Zostaną wyświetlone wyniki weryfikacji.
 - Edytuj odczytane informacje
Kliknij, aby edytować informacje osobno.

- Odczytaj więcej pliku

Kliknij, aby zaimportować wiele plików.

10. Kliknij przycisk **Importuj**, a następnie przycisk **OK** na ekranie zakończenia importu.

Wróć do ekranu właściwości urządzenia.

11. Kliknij pozycję **Prześlij**.

12. Na ekranie potwierdzenia kliknij przycisk **OK**.

Ustawienia zostaną wysłane do skanera.

13. Na ekranie zakończenia wysyłania kliknij przycisk **OK**.

Informacje skanera zostaną zaktualizowane.

Otwórz kontakty w aplikacji Web Config lub na panelu sterowania skanera, a następnie sprawdź, czy zostały zaktualizowane.

Obsługa użytkowników i serwera LDAP

Obsługa serwera LDAP umożliwia używanie informacji o adresie zarejestrowanych na serwerze LDAP jako miejsc docelowych wiadomości e-mail.

Konfigurowanie serwera LDAP

Aby móc używać informacji z serwera LDAP, zarejestruj go na skanerze.

1. Otwórz aplikację Web Config i wybierz kartę **Sieć > Serwer LDAP > Podstawowe**.

2. Wprowadź wartości poszczególnych pozycji.

3. Wybierz pozycję **OK**.

Zostaną wyświetlone wybrane ustawienia.

Opcje ustawień serwera LDAP

Elementy	Ustawienia i objaśnienie
Użyj serwera LDAP	Wybierz pozycję Użyj lub Nie należy używać .
Adres serwera LDAP	Wprowadź adres serwera LDAP. Wprowadź od 1 do 255 znaków w formacie IPv4, IPv6 lub FQDN. W przypadku formatu FQDN można używać znaków alfanumerycznych w kodowaniu ASCII (0x20–0x7E) oraz znaku „-” (z wyjątkiem początku i końca adresu).
Numer portu serwera LDAP	Umożliwia wprowadzenie numeru portu serwera LDAP w zakresie od 1 do 65535.
Bezpieczne połączenie	Określ metodę uwierzytelniania używaną przez skaner w celu uzyskania dostępu do serwera LDAP.

Elementy	Ustawienia i objaśnienie
Weryfikacja certyfikatu	Po włączeniu wykonywana jest weryfikacja certyfikatu serwera LDAP. Zalecane jest ustawienie Włącz . Aby skonfigurować tę opcję, należy na skanerze zaimportować Certyfikat CA .
Limit czasu wyszukiwania (sek.)	Określanie czasu trwania wyszukiwania przed wystąpieniem błędu upływu czasu. Dostępne wartości od 5 do 300.
Sposób uwierzytelniania	Wybór jednej z metod uwierzytelniania. Po wybraniu ustawienia Uwierzytelnienie Kerberos wybierz pozycję Ustawienia Kerberos , aby skonfigurować ustawienia Kerberos. Aby móc używać Uwierzytelnienie Kerberos, należy zapewnić następujące środowisko. <ul style="list-style-type: none"> <input type="checkbox"/> Zapewniona komunikacja między skanerem a serwerem DNS. <input type="checkbox"/> Godzina skanera, serwera KDC i serwera uwierzytelniającego (serwera LDAP, serwera SMTP, serwera plików) jest zsynchronizowana. <input type="checkbox"/> Jeśli serwerowi usług zostanie przydzielony adres IP, w pełni kwalifikowana nazwa domeny serwera usług jest rejestrowana w strefie wyszukiwania wstecznego serwera DNS.
Obszar Kerberos, który ma być używany	Jeśli zostanie wybrane ustawienie Uwierzytelnienie Kerberos dla opcji Sposób uwierzytelniania , wybierz obszar Kerberos, który ma być używany.
DN administratora / Nazwa użytkownika	Wprowadź nazwę użytkownika serwera LDAP. Nazwa powinna mieć długość maksymalnie 128 znaków w kodowaniu Unicode (UTF-8). Nie można używać znaków kontrolnych, takich jak 0x00–0x1F oraz 0x7F. To ustawienie nie jest używane, gdy wybrane zostanie ustawienie Uwierzytelnianie użytkownika anonimowego dla opcji Sposób uwierzytelniania . Jeśli ustawienie nie będzie określone, zostaw puste pole.
Hasło	Wprowadź hasło do uwierzytelniania na serwerze LDAP. Hasło powinno mieć długość maksymalnie 128 znaków w kodowaniu Unicode (UTF-8). Nie można używać znaków kontrolnych, takich jak 0x00–0x1F oraz 0x7F. To ustawienie nie jest używane, gdy wybrane zostanie ustawienie Uwierzytelnianie użytkownika anonimowego dla opcji Sposób uwierzytelniania . Jeśli ustawienie nie będzie określone, zostaw puste pole.

Ustawienia serwera Kerberos

Jeśli wybrano ustawienie **Uwierzytelnienie Kerberos** dla opcji **Sposób uwierzytelniania** w obszarze **Serwer LDAP > Podstawowe**, trzeba skonfigurować następujące ustawienia Kerberos w obszarze **Sieć > Ustawienia Kerberos**. Można zarejestrować do 10 ustawień Kerberos.

Elementy	Ustawienia i objaśnienie
Obszar (domena)	Umożliwia wprowadzenie domeny serwera uwierzytelniania Kerberos o długości do 255 znaków w formacie ASCII (0x20–0x7E). Jeśli ustawienie nie będzie rejestrowane, zostaw puste pole.
Adres KDC	Wprowadź adres serwera uwierzytelniania Kerberos. Adres powinien mieć długość do 255 znaków w formacie IPv4, IPv6 lub FQDN. Jeśli ustawienie nie będzie rejestrowane, zostaw puste pole.
Numer portu (Kerberos)	Wprowadź numer portu serwera Kerberos w zakresie od 1 do 65535.

Konfigurowanie ustawień wyszukiwania serwera LDAP

Po skonfigurowaniu ustawień wyszukiwania można użyć adresu e-mail zapisanego na serwerze LDAP.

1. Otwórz aplikację Web Config i wybierz kartę **Sieć > Serwer LDAP > Ustawienia wyszukiwania**.
2. Wprowadź wartości poszczególnych pozycji.
3. Kliknij przycisk **OK**, aby wyświetlić ustawienia.
Zostaną wyświetlone wybrane ustawienia.

Opcje ustawień wyszukiwania serwera LDAP

Elementy	Ustawienia i objaśnienie
Baza wyszukiwania (wyróżniająca się nazwa)	Aby przeprowadzić wyszukiwanie w konkretnej domenie, podaj nazwę domeny serwera LDAP. Wprowadź od 0 do 128 znaków w kodowaniu Unicode (UTF-8). Jeśli wybrany atrybut nie będzie wyszukiwany, pozostaw to pole puste. Przykład katalogu lokalnego serwera: dc=server,dc=local
Liczba pozycji wyszukiwania	Określanie liczby wyników wyszukiwania w zakresie od 5 do 500. Podana liczba wyników wyszukiwania zostanie zapisana i będzie wyświetlana tymczasowo. Wyszukiwanie można wykonać, nawet jeśli liczba wyników wyszukiwania przekracza określoną liczbę i wyświetlany jest komunikat o błędzie.
Atrybut Nazwa użytkownika	Określanie nazwy atrybutu do wyświetlania podczas wyszukiwania nazw użytkowników. Wprowadź od 1 do 255 znaków w kodowaniu Unicode (UTF-8). Pierwszy znak powinien pochodzić ze zbioru a-z lub A-Z. Przykład: cn, uid
Atrybut Wyświetlanie nazwy użytkownika	Określanie nazwy atrybutu wyświetlanego jako nazwa użytkownika. Wprowadź od 0 do 255 znaków w kodowaniu Unicode (UTF-8). Pierwszy znak powinien pochodzić ze zbioru a-z lub A-Z. Przykład: cn, sn
Atrybut Adres e-mail	Określanie nazwy atrybutu do wyświetlania podczas wyszukiwania adresów e-mail. Wprowadź od 1 do 255 znaków: A-Z a-z 0-9 oraz -. Pierwszy znak powinien pochodzić ze zbioru a-z lub A-Z. Przykład: mail
Atrybut arbitralny 1 - Atrybut arbitralny 4	Można określić inne dowolne atrybuty do wyszukiwania. Wprowadź od 0 do 255 znaków w kodowaniu Unicode (UTF-8). Pierwszym znakiem powinna być wielka lub mała litera. Aby nie wyszukiwać według innych atrybutów, pozostaw te pola puste. Przykład: o, ou

Sprawdzanie połączenia z serwerem LDAP

Możliwe jest wykonanie testu połączenia z serwerem LDAP przy użyciu parametrów ustawionych w obszarze **Serwer LDAP > Ustawienia wyszukiwania**.

1. Otwórz aplikację Web Config i wybierz kartę **Sieć > Serwer LDAP > Test połączenia**.

2. Wybierz pozycję **Start**.

Zostanie uruchomiony test połączenia. Po zakończeniu testu wyświetlany jest raport z testu.

Objaśnienia do testu połączenia z serwerem LDAP

Komunikaty	Objaśnienie
Test połączenia zakończony powodzeniem.	Ten komunikat jest wyświetlany, gdy połączenie z serwerem się powiedzie.
Test połączenia zakończony niepowodzeniem. Sprawdź ustawienia.	Ten komunikat jest wyświetlany w przypadku następujących sytuacji: <ul style="list-style-type: none"> <input type="checkbox"/> Adres serwera LDAP lub numer portu są nieprawidłowe. <input type="checkbox"/> Upłynął limit czasu. <input type="checkbox"/> Wybrano ustawienie Nie należy używać dla opcji Użyj serwera LDAP. <input type="checkbox"/> Jeśli wybrano ustawienie Uwierzytelnienie Kerberos dla opcji Sposób uwierzytelniania, ustawienia, takie jak Obszar (domena), Adres KDC i Numer portu (Kerberos) są niepoprawne.
Test połączenia zakończony niepowodzeniem. Sprawdź Data i godzina na produkcie lub serwerze.	Ten komunikat jest wyświetlany, gdy nawiązywanie połączenia zakończy się niepowodzeniem z powodu niezgodności ustawień daty i godziny skanera i serwera LDAP.
Uwierzytelnienie nie powiodło się. Sprawdź ustawienia.	Ten komunikat jest wyświetlany w przypadku następujących sytuacji: <ul style="list-style-type: none"> <input type="checkbox"/> Wartości Nazwa użytkownika i/lub Hasło są niepoprawne. <input type="checkbox"/> Jeśli wybrano ustawienie Uwierzytelnienie Kerberos dla opcji Sposób uwierzytelniania, nie można konfigurować godziny/daty.
Dostęp do urządzenia można uzyskać dopiero po zakończeniu przetwarzania.	Ten komunikat jest wyświetlany, gdy skaner jest zajęty.

Konfiguracja funkcji AirPrint

Uzyskaj dostęp do aplikacji Web Config, wybierz kartę **Sieć**, a następnie wybierz pozycję **Konfiguracja AirPrint**.

Elementy	Objaśnienie
Nazwa usługi Bonjour	Umożliwia wprowadzenie nazwy usługi Bonjour w postaci tekstu ASCII (0x20–0x7E) o długości do 41 znaków.
Lokalizacja Bonjour	Umożliwia wprowadzenie opisu lokalizacji skanera za pomocą tekstu Unicode (UTF-8) o długości do 127 bajtów.
Wide-Area Bonjour	Konfigurowanie, czy używany ma być Wide-Area Bonjour. Jeśli opcja zostanie włączona, skaner trzeba będzie zarejestrować na serwerze DNS, aby móc go wyszukiwać w segmencie sieci.

Elementy	Objaśnienie
Włącz AirPrint	<p>Umożliwia włączenie funkcji Bonjour i AirPrint (usługa skanowania). Ten przycisk jest dostępny tylko, gdy funkcja AirPrint jest wyłączona.</p> <p>Uwaga: <i>Jeśli funkcja AirPrint jest wyłączona, wyłączone zostanie też skanowanie Mopria z komputerów Chromebook, systemu Windows i aplikacji Mopria Scan.</i></p>

Problemy podczas przygotowywania skanowania sieciowego

Wskazówki dotyczące rozwiązywania problemów

Sprawdzenie komunikatu o błędzie

Po wystąpieniu błędu najpierw sprawdź, czy na panelu sterowania skanera lub ekranie sterownika wyświetlane są jakieś komunikaty. Jeśli włączono wysyłanie powiadomień e-mail dla tego typu zdarzenia, można szybko sprawdzić stan urządzenia.

Sprawdzenie stanu połączenia

Możliwe jest sprawdzanie stanu połączenia komputera serwera lub komputera klienckiego za pomocą polecenia, takiego jak ping lub ipconfig.

Test połączenia

Umożliwia sprawdzanie połączenia między skanerem a serwerem pocztowym, wykonywanie testu połączenia z poziomemu skanera. Ponadto można też sprawdzać połączenie z poziomemu komputera klienckiego do serwera.

Inicjowanie ustawień

Jeśli w ustawieniach ani w informacjach o stanie połączenia nie zostaną wykryte błędy, można rozwiązać problemy, wyłączając lub inicjując ustawienia sieciowe skanera, a następnie konfigurując je ponownie.

Nie można uzyskać dostępu do aplikacji Web Config

■ Skaner nie ma przydzielonego adresu IP.

Rozwiązania

Skaner może nie mieć przydzielonego poprawnego adresu IP. Skonfiguruj adres IP za pomocą panelu sterowania skanera. Aby sprawdzić aktualne ustawienie, skorzystaj z panelu sterowania skanera.

■ Przeglądarka internetowa nie obsługuje siły szyfrowania protokołu SSL/TLS.

Rozwiązania

SSL/TLS wykorzystuje parametr Siła szyfrowania. Aplikację Web Config można otwierać w przeglądarkach internetowych, które obsługują szyfrowania wymienione poniżej. Sprawdź, czy używana jest przeglądarka z listy obsługiwanych.

80 bitów: AES256/AES128/3DES

112 bitów: AES256/AES128/3DES

- 128 bitów: AES256/AES128
- 192 bity: AES256
- 256 bitów: AES256

■ **Certyfikat CA wygaś.**

Rozwiązania

Jeśli wystąpi problem z datą ważności certyfikatu, podczas nawiązywania połączenia z aplikacją Web Config za pośrednictwem protokołu SSL/TLS (https) zostanie wyświetlony komunikat „Certyfikat wygasł”. Jeśli komunikat jest wyświetlany przed upływem daty ważności, upewnij się, czy data na skanerze jest ustawiona prawidłowo.

■ **Nazwa publiczna certyfikatu i skanera nie zgadzają się.**

Rozwiązania

Jeżeli nazwa publiczna certyfikatu i skanera nie zgadzają się, podczas uzyskiwania dostępu do aplikacji Web Config za pośrednictwem protokołu SSL/TLS (https) zostanie wyświetlony komunikat „Nazwa certyfikatu zabezpieczeń nie zgadza się...”. Dzieje się tak, ponieważ nie zgadzają się następujące adresy IP.

- Adres IP skanera wprowadzony w nazwie publicznej na potrzeby utworzenia Certyfikat podpisywany samodzielnie lub CSR.
- Adres IP wprowadzony w przeglądarce internetowej podczas uruchamiania aplikacji Web Config

W przypadku Certyfikat podpisywany samodzielnie zaktualizuj certyfikat.

W przypadku Certyfikat CA ponownie uzyskaj certyfikat dla skanera.

■ **W przeglądarce internetowej nie skonfigurowano prawidłowo ustawień serwera proxy adresu lokalnego.**

Rozwiązania

Jeśli skaner ma korzystać z serwera proxy, w przeglądarce internetowej wyłącz łączenie się z adresem lokalnym za pośrednictwem serwera proxy.

- Windows:

Wybierz pozycję **Panel sterowania > Sieć i Internet > Opcje internetowe > Połączenia > Ustawienia sieci LAN > Serwer proxy**, a następnie wyłącz używanie serwera proxy w sieci lokalnej (adresy lokalne).

- Mac OS:

Wybierz **Preferencje systemowe (lub Ustawienia systemu) > Sieć > Zaawansowane > Proxy**, a następnie dodaj adres lokalny do listy **Pomiń ustawienia proxy dla tych komputerów i domen**.

Przykład:

192.168.1.*: Adres lokalny 192.168.1.XXX, maska podsieci 255.255.255.0

192.168.*.*: Adres lokalny 192.168.XXX.XXX, maska podsieci 255.255.0.0

■ **W ustawieniach komputera wyłączony jest DHCP.**

Rozwiązania

Jeżeli na komputerze wyłączone jest automatyczne uzyskiwanie adresu IP przez DHCP, to nie można uzyskać dostępu do Web Config. Włącz DHCP.

Przykład w systemie Windows 10:

Otwórz Panel sterowania, następnie kliknij **Sieć i Internet** > **Centrum sieci i udostępniania** > **Zmień ustawienia karty sieciowej**. Otwórz ekran właściwości połączenia, którego używasz, a następnie otwórz ekran właściwości **Protokół internetowy TCP/IP wersja 4 (TCP/IPv4)** lub **Protokół internetowy TCP/IP wersja 6 (TCP/IPv6)**. Sprawdź czy na wyświetlonym ekranie zaznaczone jest pole **Uzyskaj adres IP automatycznie**.


Dostosowanie wyświetlacza panelu sterowania

Rejestrowanie Wstępne.	70
Edycja ekranu głównego panelu sterowania.	72

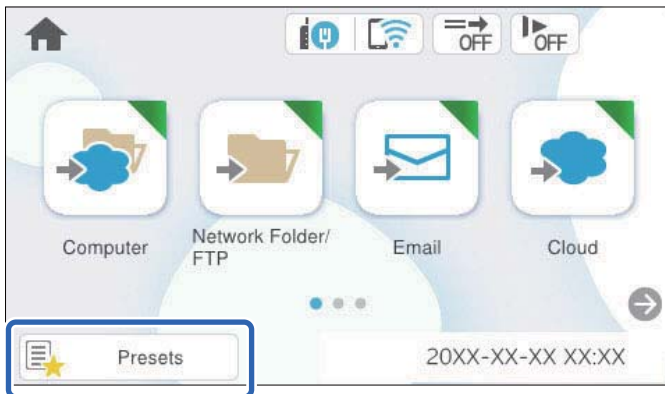
Rejestrowanie Wstępne


Można zarejestrować często używane ustawienia skanowania jako **Wstępne**. Można zarejestrować do 48 ustawień wstępnych.

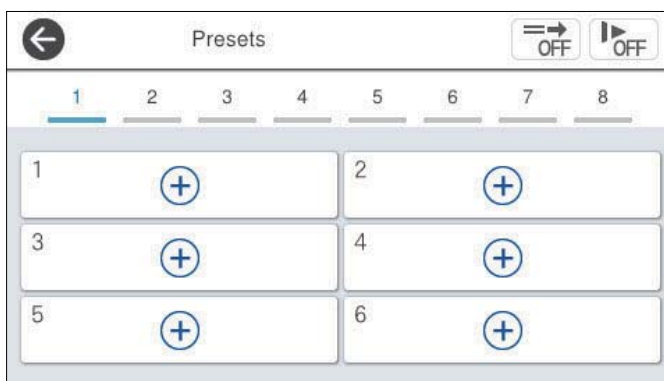
Uwaga:

- Istnieje możliwość zarejestrowania bieżących ustawień przez wybranie  na ekranie rozpoczęcia skanowania.
- Wstępne** można też rejestrować w aplikacji Web Config.
Wybierz pozycję **Skanuj** > **Wstępne**.
- Jeżeli wybierzesz opcję **Skanuj do komputera** przy rejestrowaniu, możesz zarejestrować zadanie utworzone w Document Capture Pro jako **Wstępne**. Funkcja ta jest dostępna tylko dla komputerów połączonych w sieci. Zarejestruj zadanie w Document Capture Pro wcześniej.
- Jeżeli włączona jest funkcja uwierzytelniania, tylko administrator może rejestrować **Wstępne**.

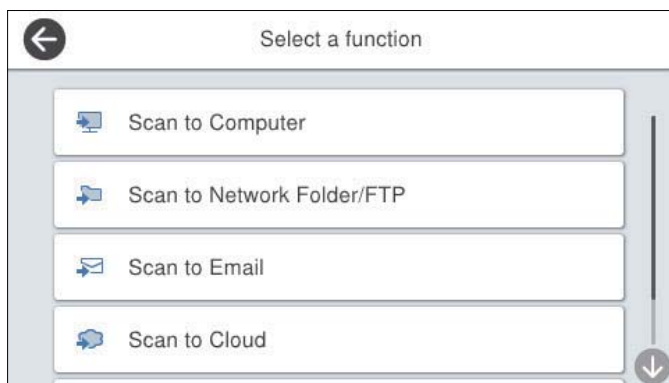
1. Na ekranie głównym panelu sterowania skanera wybierz pozycję **Wstępne**.




2. Wybierz pozycję .



3. Wybierz menu do użycia w celu rejestracji ustawień wstępnych.



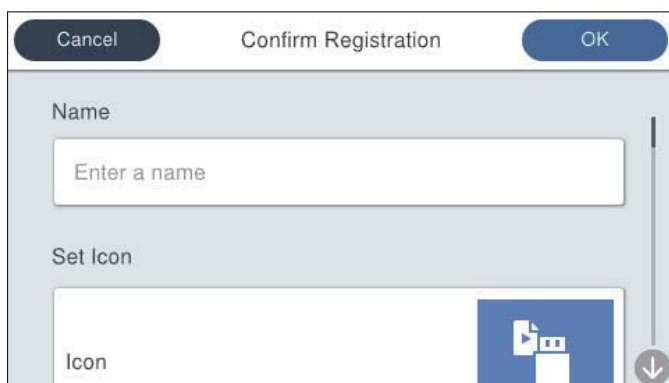
4. Ustaw poszczególne opcje, a następnie wybierz pozycję .

Uwaga:

Gdy wybierzesz opcję **Skanuj do komputera**, wybierz komputer, na którym zainstalowane jest Document Capture Pro, a następnie wybierz zarejestrowane zadanie. Funkcja ta jest dostępna tylko dla komputerów połączonych w sieci.


5. Skonfiguruj ustawienia wstępne.

- Nazwa:** ustawianie nazwy.
- Ustaw Ikona:** ustawianie obrazu i koloru ikony do wyświetlania.
- Ustawienie Szybkie wysyłanie:** natychmiastowe rozpoczęcie skanowania bez potwierdzania po wybraniu ustawień wstępnych.
- Zawartość:** sprawdzanie ustawień skanowania.



6. Wybierz pozycję OK.

Opcje menu Wstępne

Ustawienia zarejestrowane w ustawieniach wstępnych można zmieniać, wybierając pozycję  w każdym ustawieniach wstępnych.

Zmień nazwę:

Zmiana nazwy ustawień wstępnych.

Zmień Ikona:

Zmiana ikony i koloru ustawień wstępnych.

Ustawienie Szybkie wysyłanie:

Natychmiastowe rozpoczęcie skanowania bez potwierdzania po wybraniu ustawień wstępnych.

Zmień pozycję:

Zmiana kolejności wyświetlania ustawień wstępnych.

Usuń:

Usuwanie ustawień wstępnych.

Dodaj lub usuń Ikona na ekranie Ekran główny:

Dodanie lub usunięcie ikony ustawień wstępnych z ekranu głównego.

Potwierdź szczegóły:

Wyświetlanie konfiguracji ustawień wstępnych. Ustawienia wstępne można wczytać, wybierając pozycję **Użyj to ustawienie**.

Edycja ekranu głównego panelu sterowania

Możliwe jest dostosowanie ekranu głównego przez wybranie na panelu sterowania skanera pozycji **Ustaw.** > **Edytuj Główny**.

- Układ:** zmiana metody wyświetlania ikon menu.
[„Zmiana ustawień Układ ekranu głównego” na stronie 72](#)
- Dodaj ikonę:** dodawanie ikon do utworzonych ustawień **Wstępne** lub przywracanie ikon usuniętych z ekranu.
[„Dodaj ikonę” na stronie 73](#)
- Usuń ikonę:** usuwanie ikon z ekranu głównego.
[„Usuń ikonę” na stronie 74](#)
- Przenieś ikonę:** zmiana kolejności wyświetlania ikon.
[„Przenieś ikonę” na stronie 75](#)
- Przywróć wyświetlanie domyślnej ikony:** przywrócenie domyślnych ustawień wyświetlania ekranu głównego.

Zmiana ustawień Układ ekranu głównego

1. Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Układ**.


- Wybierz pozycję **Linia** lub **Macierz**.

Linia:



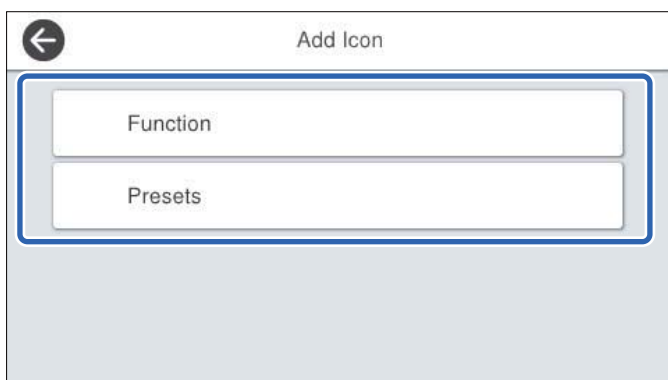
Macierz:



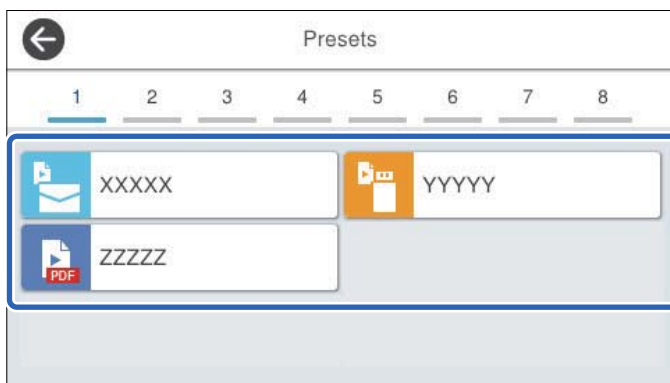
- Wybierz pozycję , aby wrócić i sprawdzić ekran główny.

Dodaj ikonę

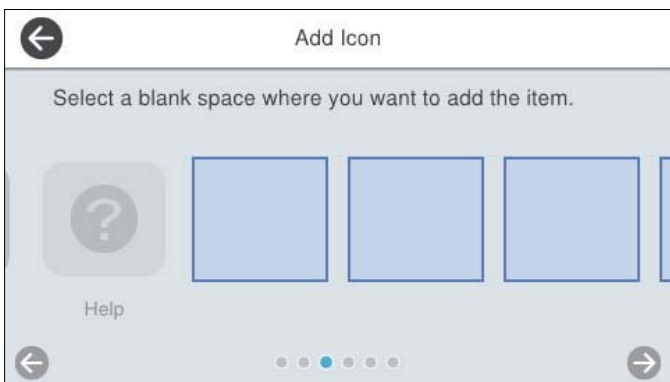
- Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Dodaj ikonę**.
- Wybierz pozycję **Wybór funkcji** lub **Wstępne**.
 - Wybór funkcji: wyświetlanie domyślnych funkcji pokazanych na ekranie głównym.
 - Wstępne: wyświetlanie zarejestrowanych ustawień wstępnych.




- Wybierz pozycję do dodania do ekranu głównego.



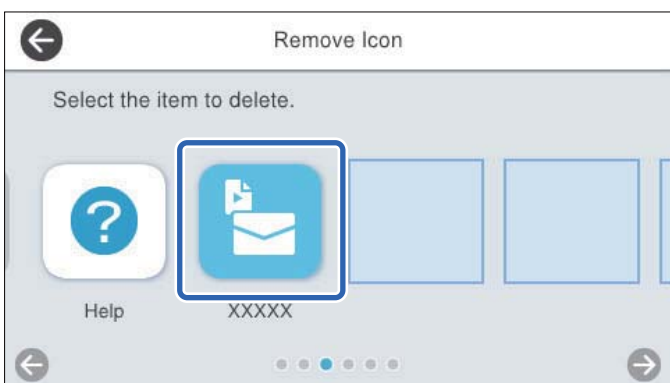
- Wybierz puste miejsce, w którym pozycja ma być dodana.
Aby dodać wiele ikon, powtórz czynności z kroków od 3 do 4.




- Wybierz pozycję , aby wrócić i sprawdzić ekran główny.

Usuń ikonę

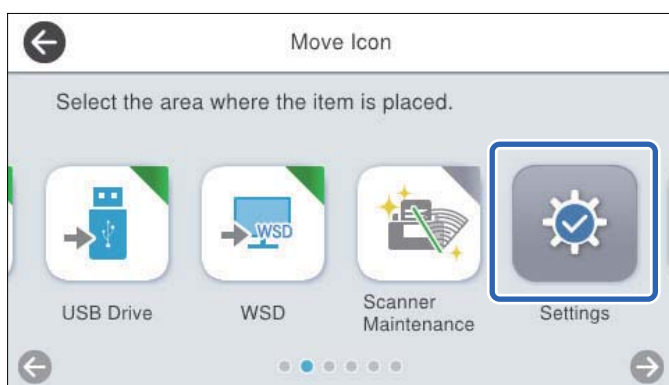
- Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Usuń ikonę.**
- Wybierz ikonę do usunięcia.



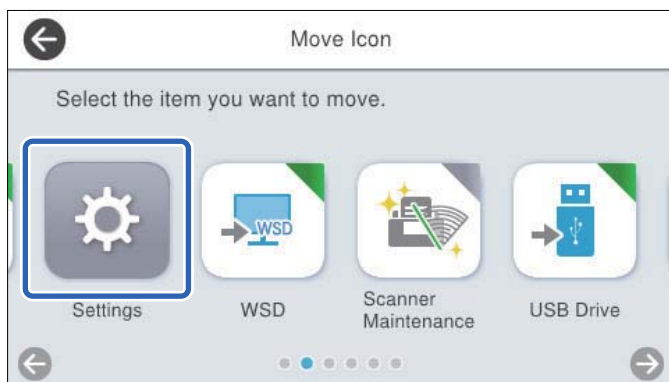
- Wybierz przycisk **Tak**, aby zakończyć.
Aby usunąć wiele ikon, powtórz czynności z kroków od 2 do 3.
- Wybierz pozycję , aby wrócić i sprawdzić ekran główny.


Przenieś ikonę

- Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Przenieś ikonę**.
- Wybierz ikonę do przesunięcia.



- Wybierz ramkę docelową.
Jeśli inna ikona jest już w ramce docelowej, ikony zostaną zamienione.



- Wybierz pozycję , aby wrócić i sprawdzić ekran główny.

Podstawowe ustawienia zabezpieczeń

Wprowadzenie do funkcji zabezpieczeń produktu.	77
Ustawienia administratora.	77
Ograniczanie dostępnych funkcji (Kontrola dostępu).	83
Wyłączanie interfejsu zewnętrznego.	85
Włączanie weryfikacji programu podczas uruchamiania.	86
Wyłączanie skanowania sieciowego z komputera.	86
Włączanie lub wyłączanie funkcji skanowania WSD.	87
Monitorowanie zdalnego skanera.	87
Przywracanie ustawień domyślnych.	89
Informacje o Epson Remote Services.	90
Rozwiązywanie problemów.	90

Wprowadzenie do funkcji zabezpieczeń produktu

W tym rozdziale opisano funkcje zabezpieczeń urządzeń firmy Epson.

Nazwa funkcji	Typ funkcji	Elementy do ustawienia	Czemu zapobiec
Konfigurowanie hasła administratora	Umożliwia zablokowanie ustawień systemowych, takich jak konfigurowanie połączenia sieciowego lub USB.	Administrator musi ustawić hasło do urządzenia. Można ustawić lub zmienić z poziomu aplikacji Web Config i panelu sterowania skanera.	Zapobieganie nieupoważnionemu odczytowi i zmianie informacji przechowywanych na urządzeniu, takich jak identyfikator, hasło, ustawienia sieciowe itd. Ponadto eliminuje szeroką gamę zagrożeń bezpieczeństwa, takich jak ujawnienie informacji dotyczących otoczenia sieciowego lub zasad bezpieczeństwa.
Ustawienia kontroli dostępu	Po zalogowaniu się na urządzeniu przy użyciu wcześniej utworzonego konta użytkownika można używać urządzenia.	Zarejestruj konto dowolnego użytkownika. Można zarejestrować do 10 kont użytkowników.	Ograniczenie funkcji dostępnych dla użytkowników pozwala zapobiegać nieupoważnionemu korzystaniu z urządzenia.
Konfiguracja interfejsu zewnętrznego	Umożliwia kontrolowanie interfejsu używanego do podłączania do urządzenia.	Włącz lub wyłącz połączenie USB z komputerem.	Połączenie USB komputera: zapobieganie nieupoważnionemu używaniu urządzenia przez zablokowanie skanowania bez użycia sieci.

Powiązane informacje

- ➔ [„Konfigurowanie hasła administratora” na stronie 77](#)
- ➔ [„Wyłączanie interfejsu zewnętrznego” na stronie 85](#)

Ustawienia administratora

Konfigurowanie hasła administratora

Ustawiając hasło administratora, można uniemożliwić użytkownikom zmianę ustawień zarządzania systemem. Wartości domyślne są ustawiane w chwili zakupu. W razie potrzeby zmień je.

Uwaga:

Poniżej podano wartości domyślne danych administratora.

Nazwa użytkownika (używana tylko w aplikacji Web Config): brak (puste pole)

Hasło: jest uzależnione od etykiety przyklejonej na produkcie.

Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer. Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź numer seryjny znajdujący się na etykiecie przyklejonej z tyłu produktu.

Hasło administratora można zmienić przy użyciu aplikacji Web Config, panelu sterowania skanera lub Epson Device Admin. W przypadku korzystania z aplikacji Epson Device Admin zapoznaj się z przewodnikiem Epson Device Admin lub pomocą.

Zmiana hasła administratora przy użyciu aplikacji Web Config

Zmień hasło administratora w aplikacji Web Config.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycję **Zabezpieczenie produktu > Zmień Hasło administratora**.
2. Wprowadź niezbędne dane w **Aktualne hasło**, **Nazwa użytkownika**, **Nowe hasło** i **Potwierdź nowe hasło**.
Nowe hasło musi zawierać od 8 do 20 znaków i wyłącznie jednobajtowe znaki i symbole alfanumeryczne.

Uwaga:

Poniżej podano wartości domyślne danych administratora.

Nazwa użytkownika: brak (puste)

Hasło: jest uzależnione od etykiety przyklejonej na produkcie.

Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer. Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź numer seryjny znajdujący się na etykiecie przyklejonej z tyłu produktu.



Ważne:

Konieczne zapamiętaj ustawione hasło administratora. Jeśli zapomnisz hasło, nie będziesz mieć możliwości jego zresetowania i konieczne będzie poproszenie o pomoc personelu serwisowego.

3. Wybierz pozycję **OK**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Zmiana hasła administratora na panelu sterowania skanera

Hasło administratora można zmienić w panelu sterowania skanera.

1. Na panelu sterowania skanera wybierz pozycję **Ustaw..**
2. Wybierz pozycję **Administr. systemu > Ustawienia administratora**.
3. Wybierz pozycję **Hasło administratora > Zmień**.

4. Wprowadź bieżące hasło.

Uwaga:

Początkowe hasło administratora (domyślne) w chwili zakupu jest różne w zależności od etykiety przyklejonej na produkcie. Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer. Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź numer seryjny znajdujący się na etykiecie przyklejonej z tyłu produktu.

5. Wprowadź nowe hasło.

Nowe hasło musi zawierać od 8 do 20 znaków i wyłącznie jednobajtowe znaki i symbole alfanumeryczne.



Ważne:

Koniecznie zapamiętaj ustawione hasło administratora. Jeśli zapomnisz hasło, nie będziesz mieć możliwości jego zresetowania i konieczne będzie poproszenie o pomoc personelu serwisowego.


6. Wprowadź ponownie nowe hasło w celu potwierdzenia.


Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.

Korzystanie z funkcji Zablokuj ustawienie na panelu sterowania

Funkcji Zablokuj ustawienie można używać do blokowania panelu sterowania, aby uniemożliwić użytkownikom zmianę ustawień systemowych.

Konfigurowanie funkcji Zablokuj ustawienie z poziomu panelu sterowania

1. Aby wyłączyć funkcję **Zablokuj ustawienie** po jej włączeniu, w prawym górnym rogu ekranu głównego dotknij pozycji , aby się zalogować jako administrator.

Pozycja  nie jest wyświetlana, gdy funkcja **Zablokuj ustawienie** jest wyłączona. Aby wyłączyć to ustawienie, przejdź do następnego kroku.

2. Wybierz pozycję **Ustaw..**
3. Wybierz pozycję **Administr. systemu > Ustawienia administratora.**
4. Ustaw opcję **Zablokuj ustawienie** na **Wł.** lub **Wył.**

Konfigurowanie funkcji Zablokuj ustawienie za pomocą aplikacji Web Config

1. Wybierz pozycję **Zarządzanie urządzeniem > Panel sterowania.**
2. Wybierz ustawienie **Wł.** lub **Wył.** dla opcji **Blokada panelu.**
3. Kliknij pozycję **OK.**

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Pozycje Zablokuj ustawienie w menu Ustaw.


Poniżej przedstawiono listę pozycji z menu **Ustaw.** na panelu sterowania blokowanych przez funkcję Zablokuj ustawienie.

✓: zablokowane.

-: niezablokowane.

Menu Ustaw.		Zablokuj ustawienie
Ustaw. podstawowe		-
	Jasność LCD	-
	Dźwięki	-
	Timer uśpienia	✓
	Timer wył.	✓
	Włącz zasilanie	✓
	Ust. Data/godzina	✓
	Język/Language	✓/-*
	Klawiatura (ta funkcja jest dostępna w wybranych regionach)	-
	Zak. czasu operacji	✓
	Poł. PC przez USB	✓
Ustawienia skanera		-
	Powoli	-
	Czas zatrz. po wykr. podw. podania	✓
	Funkcja DFDS	-
	Zabezp. papieru	✓
	Wykrywanie zabrudzeń szkła	✓
	Ponaddzw. wykr. podw. załadow.	✓
	Zakończenie czasu opcji Tryb automatycznego podawania	✓
	Potwierdź odbiorcę	✓
Edytuj Główny		✓

Menu Ustaw.		Zablokuj ustawienie
	Układ	✓
	Dodaj ikonę	✓
	Usuń ikonę	✓
	Przenieś ikonę	✓
	Przywróć wyświetlanie domyślnej ikony	✓
Ustawienia użytkownika		✓
	Folder siec./FTP	✓
	E-mail	✓
	Chmura	✓
	Napęd USB	✓
Ustawienia sieciowe		✓
	Ustawienia Wi-Fi	✓
	Ustawienie sieci LAN	✓
	Stan sieci	✓
	Zaawansowane	✓
Ustawienia usługi internetowej		✓
	Usługi Epson Connect	✓
Document Capture Pro		-
	Zmień ustawienia	✓
Menedżer Kontakty		-
	Zarejestruj/Usuń	✓/!*
	Często	-
	Przełóżaj opcje	-
	Opcje wyszukiwania	-
Administr. systemu		✓


Menu Ustaw.		Zablokuj ustawienie
	Menedżer Kontakty	✓
	Ustawienia administratora	✓
	Ograniczenia	✓
	Kontrola dostępu	✓
	Szyfrowanie hasła	✓
	Badania dotyczące klienta	✓
	Ustawienia WSD	✓
	Przywr. ust. domyśl.	✓
	Aktualizacja oprogramowania	✓
Dane urządzenia		-
	Numer seryjny	-
	Bieżąca wersja	-
	Całkowita liczba skanowań	-
	Liczba 1-stronnych skanowań	-
	Liczba 2-stronnych skanowań	-
	Liczba skan. arkusza nośnika	-
	Liczba skanów po wymianie rolki	-
	Liczba skanów po normalne czyszczenie	-
	Stan urządzenia uwierzytelniającego	-
	Informacje o Epson Open Platform	-
	 (Resetuj liczbę skanowań)	✓
Konserwacja skanera		-
	Czyszczenie rolek	-
	Wymiana rolki	-
	Resetuj liczbę skanowań	✓
	Sposób wymiany	-
	Normalne czyszczenie	-
	Resetuj liczbę skanowań	✓
	Jak czyścić	-
	Czyszczenie szyby	-
Ustawienie alarmu wymiany wafła		✓


Menu Ustaw.		Zablokuj ustawienie
	Ustawien alarmu licznika	✓
Ustawienia alarmu okresowego czyszczenia		✓
	Ustawienia alarmu ostrzeżenia	✓
	Ustawien alarmu licznika	✓

* Zezwolenie na wprowadzanie zmian ustawia się w obszarze **Administr. systemu > Ograniczenia**.

Logowanie na konto administratora z poziomu panelu sterowania

Kiedy funkcja **Zablokuj ustawienie** jest włączona, można używać dowolnej z następujących metod do logowania z panelu sterowania skanera.

1. W prawym górnym rogu ekranu dotknij ikony .
2. Kiedy wyświetlony zostanie ekran **Wybierz użytkownika**, wybierz pozycję **Administrator**.
3. Wprowadź hasło, aby się zalogować.
Zostanie wyświetlony komunikat o powodzeniu logowania, a następnie zostanie wyświetlony ekran główny panelu sterowania.

Aby się wylogować, w prawym górnym rogu ekranu dotknij ikony  lub naciśnij przycisk .

Ograniczanie dostępnych funkcji (Kontrola dostępu)

Istnieje możliwość ograniczania dostępu użytkowników do funkcji przez ograniczenie uprawnień kont użytkowników na skanerze.

Kiedy funkcja Kontrola dostępu jest włączona, użytkownik może korzystać z funkcji skanowania, wprowadzając hasło na panelu sterowania skanera w celu zalogowania się. Nie można skanować bez uprzedniego zalogowania.

Skanowanie z poziomu komputera jest możliwe po zarejestrowaniu ustawień Nazwa użytkownika i Hasło w sterowniku skanera (Epson Scan 2). Więcej informacji o konfigurowaniu ustawień można znaleźć w pomocy aplikacji Epson Scan 2 lub dokumencie produktu *Przewodnik użytkownika*.

Tworzenie konta użytkownika

Można utworzyć konto Kontrola dostępu.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz pozycje **Zabezpieczenie produktu > Ustawienia kontroli dostępu > Ustawienia użytkownika**.

2. Kliknij przycisk **Dodaj** obok numeru, który ma być zarejestrowany.



Ważne:

W przypadku korzystania ze skanera z systemem uwierzytelniającym firmy Epson lub innej należy zarejestrować nazwę Nazwa użytkownika w obszarze Ustawienia kontroli dostępu w banku pamięci od 2 do 10.

Oprogramowanie, takie jak system uwierzytelniający, wykorzystuje bank pamięci numer jeden, więc jego nazwa użytkownika nie jest wyświetlana na panelu sterowania skanera.

3. Skonfiguruj poszczególne pozycje.

- Nazwa użytkownika:

Wprowadź nazwę wyświetlaną na liście nazw użytkowników o długości od 1 do 14 znaków. Nazwa powinna zawierać znaki alfanumeryczne.

- Hasło:

Wprowadź hasło o długości do 20 znaków w formacie ASCII (0x20–0x7E). Jeśli hasło ma być zainicjowane, pozostaw to pole puste.

- Zaznacz pole wyboru w celu włączenia lub wyłączenia każdej funkcji.

Wybierz pozycję **Skanuj**, aby zezwolić na korzystanie z funkcji skanowania.

4. Kliknij pozycję **Zastosuj**.

Edytowanie konta użytkownika

Możliwe jest edytowanie zarejestrowanego konta Kontrola dostępu.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz pozycje **Zabezpieczenie produktu > Ustawienia kontroli dostępu > Ustawienia użytkownika**.
2. Kliknij przycisk **Edytuj** obok numeru, który ma być edytowany.
3. Zmień poszczególne opcje.
4. Kliknij przycisk **Zastosuj**.

Usuwanie konta użytkownika

Możliwe jest usuwanie zarejestrowanego konta Kontrola dostępu.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz pozycje **Zabezpieczenie produktu > Ustawienia kontroli dostępu > Ustawienia użytkownika**.
2. Kliknij przycisk **Edytuj** obok numeru, który ma być usunięty.
3. Kliknij przycisk **Usuń**.



Ważne:

*Po kliknięciu przycisku **Usuń** konto użytkownika zostanie usunięte bez wyświetlania komunikatu potwierdzającego. Podczas usuwania konta należy zachować szczególną ostrożność.*

Włączanie funkcji Kontrola dostępu

Kiedy zostanie włączona funkcja Kontrola dostępu, z drukarki będą mogli korzystać wyłącznie zarejestrowani użytkownicy.


Uwaga:

Jeśli funkcja Ustawienia kontroli dostępu jest włączona, trzeba powiadomić użytkownika o jego informacjach uwierzytelniających.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz pozycje **Zabezpieczenie produktu > Ustawienia kontroli dostępu > Podstawowe**.
2. Wybierz pozycję **Włączenie kontroli dostępu**.
Po włączeniu funkcji Ustawienia kontroli dostępu skanowanie z poziomu komputera bez informacji uwierzytelnienia będzie wymagać zaznaczenia opcji **Umożliwia drukowanie i skanowanie bez informacji uwierzytelniania z komputera**.
3. Kliknij pozycję **OK**.

Logowanie do skanera, na którym włączono funkcję Kontrola dostępu

Kiedy funkcja **Kontrola dostępu** jest włączona, można używać dowolnej z następujących metod do logowania z panelu sterowania skanera.

1. W prawym górnym rogu ekranu dotknij ikony .
2. Jeśli wyświetlony zostanie ekran **Wybierz użytkownika**, wybierz użytkownika.
3. Wprowadź hasło, aby się zalogować.

Zostanie wyświetlony komunikat o powodzeniu logowania, a następnie zostanie wyświetlony ekran główny panelu sterowania.

Aby się wylogować, w prawym górnym rogu ekranu dotknij ikony  lub naciśnij przycisk .

Wyłączanie interfejsu zewnętrznego

Można wyłączyć interfejs używany do podłączania urządzenia do skanera. Aby ograniczyć skanowanie inne niż przez sieć, należy skonfigurować ustawienia ograniczeń.

Uwaga:

Ustawienia ograniczeń można też konfigurować na panelu sterowania skanera.

Poł. PC przez USB: **Ustaw.** > **Ustaw. podstawowe** > **Poł. PC przez USB**

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie produktu > Złącze zewnętrzny**.
2. Wybierz ustawienie **Wyłącz** w przypadku funkcji, które mają być ustawione.
Wybierz ustawienie **Włącz**, aby anulować kontrolę.
Poł. PC przez USB

Można ograniczyć wykorzystanie połączenia USB z komputera. Aby to zrobić, należy wybrać **Wyłącz**.

3. Kliknij pozycję **OK**.

4. Sprawdź, czy nie można używać wyłączzonego portu.

Poł. PC przez USB

Jeśli na komputerze zainstalowano sterownik

Podłącz skaner do komputera za pomocą kabla USB, a następnie upewnij się, że skaner nie skanuje.

Jeśli na komputerze nie zainstalowano sterownika

System Windows:

Otwórz Menedżer urządzeń i nie zamykaj go, podłącz skaner do komputera za pomocą kabla USB, a następnie upewnij się, że informacje wyświetlane w oknie Menedżer urządzeń nie zmieniają się.

Mac OS:

Podłącz skaner do komputera za pomocą kabla USB, a następnie upewnij się, że nie można dodać skanera w oknie **Drukarki i skanery**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Włączanie weryfikacji programu podczas uruchamiania

Jeśli zostanie włączona funkcja weryfikacji programu, skaner będzie wykonywać weryfikację podczas uruchamiania w celu sprawdzenia, czy jakieś nieupoważnione osoby nie zmodyfikowały oprogramowania. W razie stwierdzenia jakichkolwiek problemów nie będzie można uruchomić skanera.

Uwaga:

Włączenie tej funkcji powoduje wydłużenie czasu uruchamiania skanera.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zabezpieczenie produktu > Sprawdzanie programu podczas uruchamiania**.

Uwaga:

Ustawienia można też konfigurować na panelu sterowania skanera.

Ustaw. > **Administr. systemu** > **Sprawdz. progr. przy uruch.**

2. Wybierz pozycję **Wł.**, aby włączyć opcję **Sprawdzanie programu podczas uruchamiania**.

3. Kliknij przycisk **OK**.

Wyłączenie skanowania sieciowego z komputera

Aby wyłączyć skanowanie sieciowe za pomocą aplikacji lub Epson Scan 2 z poziomu komputera, skonfiguruj następujące ustawienia w aplikacji Web Config.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Skanuj > Skanowanie sieciowe**.

2. W oknie **Epson Scan 2** usuń zaznaczenie pola wyboru **Włącz skanowanie**.
3. Kliknij przycisk **Dalej**.
Zostanie wyświetlony ekran potwierdzenia ustawień.
4. Kliknij przycisk **OK**.

Włączanie lub wyłączenie funkcji skanowania WSD

Uwaga:

Ustawienia można też konfigurować na panelu sterowania skanera. Wybierz pozycje **Ustaw.** > **Administr. systemu** > **Ustawienia WSD**.

Możliwe jest włączenie lub wyłączenie funkcji skanowania WSD.

Jeśli nie chcesz, aby skaner był skonfigurowany na komputerze jako urządzenie skanujące WSD, wyłącz funkcję WSD.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zabezpieczenie sieci** > **Protokół**.
2. W obszarze **Ustawienia WSD** zmień ustawienie pola wyboru **Włącz WSD**.
3. Kliknij pozycję **Dalej**.
Zostanie wyświetlony ekran potwierdzenia ustawień.
4. Kliknij przycisk **OK**.

Uwaga:

Jeśli na komputerze skaner nadal jest ustawiony jako urządzenie skanujące WSD, wybierz kartę **Skanuj** > **Skanowanie sieciowe**, a następnie usuń zaznaczenie pola wyboru **Włącz skanowanie** w obszarze **AirPrint**.

Jeśli funkcja AirPrint jest wyłączona, wyłączone zostanie też skanowanie Mopria z komputerów Chromebook, systemu Windows i aplikacji Mopria Scan.

Monitorowanie zdalnego skanera

Sprawdzanie informacji o skanerze zdalnym

Na ekranie **Stan** w aplikacji Web Config można sprawdzać następujące informacje o działającym skanerze.

- Status urządzenia
Sprawdzanie stanu, usługi chmury, numeru produktu, adresu MAC itd.
- Stan sieci
Przeglądanie informacji o stanie połączenia sieciowego, adresie IP, adresie serwera DNS itd.
- Stan używania
Sprawdzanie pierwszego dnia skanowania, liczby skanów itd.
- Stan urządzenia
Sprawdzanie stanu każdej funkcji skanera.

Migawka panelu

Wyświetlanie zrzutu ekranu wyświetlanego na panelu sterowania skanera.

Otrzymywanie powiadomień e-mail w przypadku występowania zdarzeń

Informacje o powiadomieniach e-mail

To jest funkcja powiadomień, która — w razie wystąpienia zdarzeń, takich jak zatrzymanie skanowania lub błąd skanera — powoduje wysłanie wiadomości e-mail na określony adres.

Możliwe jest zarejestrowanie do pięciu miejsc docelowych i skonfigurowanie ustawień powiadomień dla każdego miejsca.

Aby móc używać tej funkcji, należy skonfigurować ustawienia serwera pocztowego przed przystąpieniem do konfigurowania powiadomień.

Powiązane informacje

➔ „Rejestrowanie serwera poczty e-mail” na stronie 45

Konfigurowanie powiadomień e-mail

Można skonfigurować powiadomienia e-mail za pomocą aplikacji Web Config.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zarządzanie urządzeniem > Powiadomienie przez e-mail**.
2. Ustaw temat powiadomienia e-mail.
Wybierz zawartość wyświetlaną w temacie, używając dwóch list rozwijanych.
 - Wybrana zawartość zostanie wyświetlona obok pozycji **Temat**.
 - Nie można ustawić tej samej zawartości po lewej i prawej stronie.
 - Jeśli liczba znaków w pozycji **Lokalizacja** przekroczy 32 bajty, znaki przekraczające limit 32 bajtów zostaną pominięte.
3. Wprowadź adres e-mail do wysyłania powiadomień e-mail.
Użyj znaków A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @. Wprowadź od 1 do 255 znaków.
4. Wybierz język powiadomień e-mail.
5. Zaznacz pole obok zdarzenia, dla którego mają być wysyłane powiadomienia.

Liczba **Ustawienia powiadomień** jest połączona z docelowym numerem **Ustawienia adresu e-mail**.

Przykład:

Aby wysłać powiadomienie na adres e-mail ustawiony dla numeru 1 w obszarze **Ustawienia adresu e-mail** po zmianie hasła administratora, zaznacz pole wyboru w kolumnie **1** w wierszu **Zmieniono Hasło administratora**.

6. Kliknij pozycję **OK**.

Sprawdź, czy powiadomienie e-mail zostanie wysłane, powodując takie zdarzenie.

Przykład: Hasło administratora zostało zmienione.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Pozycje wysyłania powiadomień e-mail

Elementy	Ustawienia i objaśnienie
Zmieniono Hasło administratora	Powiadamianie po zmianie hasła administratora.
Błąd skanera	Powiadamianie po wystąpieniu błędu skanera.
Błąd Wi-Fi	Powiadomienie, gdy wystąpił błąd interfejsu sieci bezprzewodowej LAN.

Sterowanie zasilaniem skanera przy użyciu aplikacji Web Config

Jeśli komputer jest w innej lokalizacji niż skaner, można używać aplikacji Web Config, aby wyłączać lub ponownie uruchamiać skaner.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zarządzanie urządzeniem > Zasilanie**.
2. Wybierz pozycję **Wyłącz zasilanie** lub **Uruchom ponownie**.
3. Kliknij przycisk **Wykonaj**.

Przywracanie ustawień domyślnych

Możliwe jest przywrócenie wartości domyślnych ustawień sieciowych lub innych ustawień przechowywanych w pamięci skanera.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zarządzanie urządzeniem > Przywr. ust. domyśl.**

Uwaga:

Ustawienia można też konfigurować na panelu sterowania skanera.

Ustaw. > Administr. systemu > Przywr. ust. domyśl.

2. Wybierz pozycje do przywrócenia.
3. Kliknij pozycję **Wykonaj**.

Na koniec postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Informacje o Epson Remote Services

Epson Remote Services jest usługą, która służy do okresowego gromadzenia informacji o skanerze przez Internet. Można jej używać do prognozowania wymiany lub uzupełnienia materiałów eksploatacyjnych i części zamiennych, a także szybkiego rozwiązywania wszelkich błędów lub problemów.

Aby uzyskać więcej informacji o usłudze Epson Remote Services, należy skontaktować się ze sprzedawcą.

Rozwiązywanie problemów

Zapomnienie hasła administratora

Aby odzyskać dostęp do urządzenia, potrzebna jest pomoc personelu serwisu. Skontaktuj się z lokalnym sprzedawcą.

Uwaga:

Poniżej przedstawiono wstępne wartości dla administratora Web Config.

Nazwa użytkownika: brak (puste)

Hasło: jest uzależnione od etykiety przyklejonej na produkcie.

Jeśli z tyłu jest przyklejona etykieta „PASSWORD”, wprowadź znajdujący się na niej 8-cyfrowy numer.

Jeśli nie ma etykiety „PASSWORD”, w polu hasła administratora wprowadź seryjny numer znajdujący się na etykiecie przyklejonej z tyłu produktu.

W przypadku przywrócenia hasła administratora zostanie ono zresetowane do początkowej wartości w chwili zakupu.

Zaawansowane ustawienia bezpieczeństwa

Ustawienia zabezpieczeń i zapobieganie niebezpieczeństwom.	92
Kontrola użycia protokołów.	93
Używanie certyfikatu cyfrowego.	96
Komunikacja SSL/TLS ze skanerem.	102
Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP.	103
Podłączanie skanera do sieci IEEE802.1X.	115
Rozwiązywanie problemów związanych z zaawansowanymi zabezpieczeniami.	117

Ustawienia zabezpieczeń i zapobieganie niebezpieczeństwom

Jeśli skaner jest połączony z siecią, można uzyskać do niego dostęp z lokalizacji zdalnej. Ponadto wiele osób może współużytkować skaner, co pomaga poprawić wydajność operacyjną i wygodę obsługi. Jednak powoduje to zwiększenie zagrożeń, takich jak nieupoważniony dostęp i użycie oraz manipulowanie danymi. W przypadku użytkownika skanera w środowisku, w którym jest zapewniony dostęp do Internetu, zagrożenia są jeszcze większe.

Na skanerach bez ochrony przez dostępem z zewnątrz możliwe będzie odczytywanie przez Internet kontaktów przechowywanych w pamięci skanera.

Aby uniknąć tego ryzyka, skanery firmy Epson są wyposażone w różne technologie zabezpieczające.

Skaner trzeba skonfigurować odpowiednio do warunków środowiskowych, które zostały opracowane z uwzględnieniem informacji o środowisku klienta.

Nazwa	Typ funkcji	Elementy do ustawienia	Działanie zabezpieczające
Kontrolowanie protokołów	Możliwe jest kontrolowanie protokołów i usług wykorzystywanych do komunikacji między skanerami i komputerami, a także włączenie i wyłączenie funkcji.	Protokół lub usługa, które są stosowane do funkcji dozwolonych lub zabronionych osobno.	Ograniczenie zagrożeń bezpieczeństwa, które mogą wystąpić przez niezamierzone użycie, uniemożliwiając użytkownikom korzystanie z niepotrzebnych funkcji.
Komunikacja SSL/TLS	Przesyłana zawartość jest szyfrowana za pośrednictwem protokołu SSL/TLS podczas uzyskiwania dostępu do serwera Epson przez Internet, np. podczas komunikacji z komputerem za pośrednictwem przeglądarki internetowej, używania programu Epson Connect i aktualizacji oprogramowania układowego.	Administrator musi uzyskać certyfikat podpisany przez zaufany urząd certyfikacji, a następnie zaimportować go na skanerze.	Identyfikacja skanera przez certyfikat podpisany przez urząd certyfikacji zapobiega podszywaniu się i nieupoważnionemu dostępowi. Poza tym komunikacja jest chroniona przy użyciu protokołów SSL/TLS, co zapobiega ujawnianiu zawartości danych zadań skanowania i informacji o konfiguracji urządzenia.
IPsec/filtrowanie IP	Można zezwolić na obsługę i odrzucanie danych z konkretnego klienta lub danych określonego typu. Ponieważ protokół IPsec umożliwia ochronę danych na poziomie pakietu IP (szyfrowanie i uwierzytelnianie), można bezpiecznie przysyłać dane za pośrednictwem niezabezpieczonego protokołu.	Utwórz podstawowe zasady i indywidualne zasady, aby ustawić klienty lub typy danych, które są dozwolone na skanerze.	Ochrona przed nieupoważnionym dostępem, a także manipulacją i przechwyceniem danych przesyłanych do skanera.

Nazwa	Typ funkcji	Elementy do ustawienia	Działanie zabezpieczające
IEEE 802.1X	Pozwala na łączenie się z siecią wyłącznie upoważnionym do tego użytkownikom. Skanera mogą używać tylko użytkownicy z uprawnieniami.	Konfigurowanie uwierzytelniania na serwerze RADIUS (serwer uwierzytelniający).	Ochrona przed nieupoważnionym dostępem i użytkowaniem skanera.

Powiązane informacje

- ➔ [„Kontrola użycia protokołów” na stronie 93](#)
- ➔ [„Komunikacja SSL/TLS ze skanerem” na stronie 102](#)
- ➔ [„Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103](#)
- ➔ [„Podłączanie skanera do sieci IEEE802.1X” na stronie 115](#)

Ustawienia funkcji zabezpieczeń

Zaleca się, aby podczas ustawiania IPsec/filtrowania IP lub IEEE 802.1X uzyskać dostęp do Web Config z użyciem SSL/TLS w celu zakomunikowania informacji o ustawieniach, co ograniczy zagrożenia bezpieczeństwa, takie jak manipulacja czy przechwytywanie.

Przed ustawieniem IPsec/filtrowania IP lub IEEE 802.1X koniecznie skonfiguruj hasło administratora.

Kontrola użycia protokołów

Przy skanowaniu można korzystać z rozmaitych ścieżek i protokołów. Można też używać skanowania sieciowego z nieograniczonej liczby komputerów przyłączonych do sieci.

Powstające przy tym zagrożenia można zredukować, wprowadzając ograniczenia w skanowaniu z pewnych ścieżek lub kontrolując dostęp do funkcji.

Kontrola dostępu do protokołów

Skonfiguruj ustawienia protokołów obsługiwanych przez skaner.

1. Otwórz aplikację Web Config, a następnie wybierz kartę **Zabezpieczenie sieci** tab > **Protokół**.
2. Skonfiguruj poszczególne parametry.
3. Kliknij pozycję **Dalej**.
4. Kliknij pozycję **OK**.

Ustawienia zostaną zastosowane do skanera.

Powiązane informacje

- ➔ [„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)

Protokoły, które można włączyć lub wyłączyć

Protokół	Opis
Ustawienia Bonjour	Określa, czy ma być używany protokół Bonjour. Bonjour jest protokołem używanym do wykrywania urządzeń, skanowania i innych usług.
Ustawienia SLP	Pozwala włączyć lub wyłączyć funkcję SLP. SLP to protokół używany do skanowania inicjowanego na skanerze i wyszukiwania sieci w aplikacji EpsonNet Config.
Ustawienia WSD	Pozwala włączyć lub wyłączyć funkcję WSD. Po jej włączeniu można dodawać urządzenia WSD i skanować za pośrednictwem portu WSD.
Ustawienia LLTD	Pozwala włączyć lub wyłączyć funkcję LLTD. Po jej włączeniu opcja ta jest wyświetlana w mapie sieci systemu Windows.
Ustawienia LLMNR	Pozwala włączyć lub wyłączyć funkcję LLMNR. Po jej włączeniu można używać interpretacji nazw bez pośrednictwa usług NetBIOS, nawet przy braku dostępu do DNS.
Ustawienia SNMPv1/v2c	Określa, czy ma być włączona funkcja SNMPv1/v2c. Służy ona między innymi do konfigurowania i monitorowania urządzeń.
Ustawienia SNMPv3	Określa, czy ma być włączona funkcja SNMPv3. Służy ona między innymi do konfigurowania i monitorowania urządzeń zaszyfrowanych itd.

Opcje ustawień protokołów

Ustawienia Bonjour

Elementy	Wartość i opis
Użyj Bonjour	Zaznacz tę opcję, aby używać protokołu Bonjour do wyszukiwania i obsługi urządzeń.
Nazwa Bonjour	Wyświetla nazwę Bonjour.
Nazwa usługi Bonjour	Wyświetla nazwę usługi Bonjour.
Lokalizacja	Wyświetla nazwę lokalizacji Bonjour.
Wide-Area Bonjour	Włączanie używania Wide-Area Bonjour.

Ustawienia SLP

Elementy	Wartość i opis
Włącz SLP	Zaznacz tę opcję, aby włączyć funkcję SLP. Ta opcja jest używana na potrzeby wyszukiwania sieci w aplikacji EpsonNet Config.

Ustawienia WSD

Elementy	Wartość i opis
Włącz WSD	Zaznacz tę opcję, aby umożliwić dodawanie urządzeń za pomocą WSD oraz skanowanie przez port WSD.

Elementy	Wartość i opis
Limit czasu skanowania (sek.)	Określ limit czasu komunikacji podczas skanowania przez WSD, wprowadzając wartość z zakresu od 3 do 3600 sekund.
Nazwa urządzenia	Wyświetla nazwę urządzenia WSD.
Lokalizacja	Wyświetla nazwę lokalizacji WSD.

Ustawienia LLTD

Elementy	Wartość i opis
Włącz LLTD	Ta opcja włącza protokół LLTD. Skaner jest wyświetlany na mapie sieci Windows.
Nazwa urządzenia	Wyświetla nazwę urządzenia LLTD.

Ustawienia LLMNR

Elementy	Wartość i opis
Włącz LLMNR	Ta opcja włącza protokół LLMNR. Można korzystać z interpretacji nazw bez pośrednictwa usług NetBIOS, nawet przy braku dostępu do DNS.

Ustawienia SNMPv1/v2c

Elementy	Wartość i opis
Włącz SNMPv1/v2c	Ta opcja włącza protokół SNMPv1/v2c.
Upoważnienie dostępu	Określ uprawnienia dostępu, gdy włączony jest protokół SNMPv1/v2c. Wybierz pozycję Należy tylko przeczytać lub Przeczytaj/Pisz .
Nazwa grupy (tylko do odczytu)	Wprowadź od 0 do 32 znaków ASCII (0x20 do 0x7E).
Nazwa grupy (odczyt/zapis)	Wprowadź od 0 do 32 znaków ASCII (0x20 do 0x7E).

Ustawienia SNMPv3

Elementy	Wartość i opis
Włącz SNMPv3	Włączenie protokołu SNMPv3 (zaznaczenie pola).
Nazwa użytkownika	Wprowadzenie od 1 do 32 znaków jednobajtowych.
Ustawienia uwierzytelniania	

Elementy		Wartość i opis
	Algorytm	Wybór algorytmu uwierzytelniania na potrzeby protokołu SNMPv3.
	Hasło	Wprowadzanie hasła uwierzytelniania na potrzeby protokołu SNMPv3. Wprowadź od 8 do 32 znaków ASCII (0x20–0x7E). Jeśli ustawienie nie będzie określone, zostaw puste pole.
	Potwierdź hasło	Wprowadź skonfigurowane hasło w celu potwierdzenia.
Ustawienia szyfrowania		
	Algorytm	Wybór algorytmu szyfrowania na potrzeby protokołu SNMPv3.
	Hasło	Wprowadzanie hasła szyfrowania na potrzeby protokołu SNMPv3. Wprowadź od 8 do 32 znaków ASCII (0x20–0x7E). Jeśli ustawienie nie będzie określone, zostaw puste pole.
	Potwierdź hasło	Wprowadź skonfigurowane hasło w celu potwierdzenia.
Nazwa kontekstowa		Wprowadzenie do 32 znaków w formacie Unicode (UTF-8). Jeśli ustawienie nie będzie określone, zostaw puste pole. Liczba znaków, które można wprowadzić, zależy od języka.

Używanie certyfikatu cyfrowego

Informacje o certyfikatach cyfrowych

Certyfikat CA

To jest certyfikat podpisany przez urząd certyfikacji. Można go uzyskać, wysyłając żądanie do danego urzędu certyfikacji. Ten certyfikat poświadcza istnienie skanera i służy do komunikacji SSL/TLS, która umożliwia bezpieczne przesyłanie danych.

Jeżeli jest używany do komunikacji SSL/TLS, pełni rolę certyfikatu serwera.

W przypadku użycia funkcji filtrowania IPsec/IP lub komunikacji IEEE 802.1X pełni rolę certyfikatu klienta.

Certyfikat urzędu certyfikacji

To jest certyfikat w łańcuchu Certyfikat CA, zwany też pośrednim certyfikatem urzędu certyfikacji. Jest używany przez przeglądarkę internetową do weryfikacji ścieżki certyfikatu skanera w trakcie uzyskiwania dostępu do serwera innej firmy lub aplikacji Web Config.

W przypadku certyfikatu urzędu certyfikacji należy określić, kiedy ścieżka certyfikatu serwera ma być weryfikowana w trakcie uzyskiwania dostępu z poziomu skanera. W przypadku skanera należy ustawić, aby umożliwić certyfikację ścieżki Certyfikat CA na potrzeby połączenia SSL/TLS.

Certyfikat urzędu certyfikacji dla skanera można uzyskać od urzędu certyfikacji, który wystawił dany certyfikat urzędu certyfikacji.

Możliwe jest też uzyskanie certyfikatu urzędu certyfikacji używanego do weryfikacji serwera innej firmy z urzędu certyfikacji, który wystawił Certyfikat CA dla tego serwera.

Certyfikat podpisywany samodzielnie

To jest certyfikat, który jest wystawiany i podpisywany przez sam skaner. Jest zwany również certyfikatem głównym. Nie jest jednak godny zaufania i nie zapobiega podszywaniu się, ponieważ wystawca sam go podpisuje.

Można go używać podczas konfiguracji ustawień zabezpieczeń i podstawowej komunikacji SSL/TLS bez Certyfikat CA.

W przypadku wykorzystywania certyfikatu tego rodzaju na potrzeby komunikacji SSL/TLS w przeglądarce internetowej może zostać wyświetlony komunikat ostrzegawczy, ponieważ certyfikat nie jest zarejestrowany w przeglądarce. Certyfikat podpisywany samodzielnie nie można używać na potrzeby komunikacji innej niż SSL/TLS.

Powiązane informacje

- ➔ „Konfiguracja Certyfikat CA” na stronie 97
- ➔ „Aktualizowanie certyfikatu z podpisem własnym” na stronie 100
- ➔ „Konfiguracja Certyfikat CA” na stronie 101

Konfiguracja Certyfikat CA

Uzyskiwanie certyfikatu podpisanego przez urząd certyfikacji

Aby uzyskać certyfikat podpisany przez urząd certyfikacji, należy utworzyć żądanie CSR (Certificate Signing Request) i przesłać je do wybranego urzędu certyfikacji. Żądanie CSR można utworzyć na komputerze za pomocą aplikacji Web Config.

Aby utworzyć żądanie CSR i uzyskać certyfikat podpisany przez urząd certyfikacji za pomocą aplikacji Web Config, wykonaj następujące czynności. Jeśli żądanie CSR zostanie utworzone za pomocą aplikacji Web Config, certyfikat będzie mieć format PEM/DER.

1. Otwórz aplikację Web Config, a następnie wybierz kartę **Zabezpieczenie sieci**. Następnie wybierz pozycje **SSL/TLS > Certyfikat** lub **IPsec/Filtrowanie IP > Certyfikat klienta** lub **IEEE802.1X > Certyfikat klienta**.

Niezależnie od wybranej pozycji można uzyskać ten sam certyfikat i używać go wspólnie.

2. Kliknij przycisk **Generuj** obok żądania CSR.

Zostanie wyświetlona strona tworzenia żądania CSR.

3. Wprowadź wartości poszczególnych pozycji.

Uwaga:

Dostępne długości kluczy i skróty zależą od danego urzędu certyfikacji. Utwórz żądanie zgodnie z regułami obowiązującymi w danym urzędzie certyfikacji.

4. Kliknij przycisk **OK**.

Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.

5. Wybierz kartę **Zabezpieczenie sieci**. Następnie wybierz pozycje **SSL/TLS > Certyfikat** lub **IPsec/Filtrowanie IP > Certyfikat klienta** lub **IEEE802.1X > Certyfikat klienta**.

6. Kliknij jeden z dostępnych przycisków pobrania żądania **CSR** zgodnie z formatem danego urzędu certyfikacji, aby pobrać żądanie CSR na komputer.



Ważne:

Nie generuj ponownie żądania CSR. W przeciwnym razie zaimportowanie wystawionego Certyfikat CA może nie być możliwe.

7. Pobrane żądanie CSR wyślij do urzędu certyfikacji, aby uzyskać Certyfikat CA.
Należy przestrzegać reguł dotyczących metody i formy przesyłania żądań CSR obowiązujących w danym urzędzie certyfikacji.
8. Otrzymany Certyfikat CA zapisz na komputerze podłączonym do skanera.
Proces uzyskiwania Certyfikat CA zostanie zakończony w chwili zapisania certyfikatu w miejscu docelowym.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Opcje ustawień żądania CSR

Elementy	Ustawienia i objaśnienie
Długość klucza	Wybierz długość klucza.
Popularna nazwa	Można wprowadzić od 1 do 128 znaków. Jeśli jest to adres IP, powinien to być adres statyczny. Można wprowadzić od 1 do 5 adresów IPv4, adresów IPv6, nazw hosta, w pełni kwalifikowanych nazw domen, rozdzielając je przecinkami. Pierwszy element jest przechowywany jako nazwa publiczna, a pozostałe elementy jako aliasy podmiotu certyfikatu. Przykład: Adres IP skanera: 192.0.2.123, nazwa skanera: EPSONA1B2C3 Popularna nazwa: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organizacja/ Jednostka organizacyjna/ Miejscowość/ Stan/Prowincja	Można wprowadzić od 0 do 64 znaków ASCII (0x20–0x7E). Nazwy wyróżniające można rozdzielić przecinkami.
Kraj	Podaj dwucyfrowy kod kraju zgodnie z normą ISO-3166.
Adres email wysyłającego	Można wprowadzić adres e-mail nadawcy dla ustawienia serwera poczty e-mail. Wprowadź ten sam adres e-mail, który jest Adres email wysyłającego dla karty Sieć > Serwer e-mail > Podstawowe .

Importowanie certyfikatu podpisanego przez urząd certyfikacji

Uzyskany Certyfikat CA można zaimportować na skanerze.

**Ważne:**

- Upewnij się, że ustawienia daty i godziny na skanerze są prawidłowe. Certyfikat może być nieprawidłowy.
- W przypadku uzyskania certyfikatu na podstawie żądania CSR utworzonego za pomocą aplikacji Web Config certyfikat można zaimportować tylko raz.

1. Otwórz aplikację Web Config, a następnie wybierz kartę **Zabezpieczenie sieci**. Następnie wybierz pozycje **SSL/TLS > Certyfikat** lub **IPsec/Filtrowanie IP > Certyfikat klienta** lub **IEEE802.1X > Certyfikat klienta**.

2. Kliknij pozycję **Importuj**

Zostanie wyświetlona strona importowania certyfikatu.

3. Wprowadź wartości poszczególnych pozycji. Ustaw opcje **Certyfikat CA 1** i **Certyfikat CA 2** w przypadku weryfikacji ścieżki certyfikatu w przeglądarce internetowej, z której uzyskiwany jest dostęp do skanera.

Wymagane ustawienia mogą się różnić w zależności od sposobu tworzenia żądania CSR oraz formatu pliku certyfikatu. Wartości należy wprowadzać w następujący sposób.

W przypadku certyfikatu w formacie PEM/DER uzyskanego za pomocą aplikacji Web Config

Klucz prywatny: nie konfiguruj, ponieważ skaner ma już klucz prywatny.

Hasło: nie konfiguruj.

Certyfikat CA 1/Certyfikat CA 2: pole opcjonalne

W przypadku certyfikatu w formacie PEM/DER uzyskanego za pomocą komputera

Klucz prywatny: wprowadź wartość.

Hasło: nie konfiguruj.

Certyfikat CA 1/Certyfikat CA 2: pole opcjonalne

W przypadku certyfikatu w formacie PKCS#12 uzyskanego za pomocą komputera

Klucz prywatny: nie konfiguruj.

Hasło: pole opcjonalne

Certyfikat CA 1/Certyfikat CA 2: Nie konfiguruj.

4. Kliknij pozycję **OK**.

Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.

Uwaga:

Kliknij przycisk **Potwierdź**, aby zweryfikować dane certyfikatu.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Elementy ustawień importu certyfikatu z podpisem CA

Elementy	Ustawienia i objaśnienie
Certyfikat serwera lub Certyfikat klienta	Wybierz format certyfikatu. Dla połączenia SSL/TLS wyświetla się Certyfikat serwera. Dla IPsec/filtrowania IP lub IEEE 802.1X wyświetla się Certyfikat klienta.
Klucz prywatny	Jeśli uzyskasz certyfikat w formacie PEM/DER po skorzystaniu z CSR utworzonego z komputera, określ plik prywatnego klucza odpowiadającego certyfikatowi.
Hasło	Jeśli format pliku to Certyfikat z kluczem prywatnym (PKCS#12) , wprowadź hasło szyfrowania prywatnego klucza ustawionego podczas uzyskiwania certyfikatu.
Certyfikat CA 1	Jeśli format certyfikatu to Certyfikat (PEM/DER) , zaimportuj certyfikat urzędu certyfikacyjnego wystawiającego Certyfikat CA wykorzystywany jako certyfikat serwera. W razie potrzeby określ plik.
Certyfikat CA 2	Jeśli format certyfikatu to Certyfikat (PEM/DER) , zaimportuj certyfikat urzędu certyfikacyjnego wystawiającego Certyfikat CA 1. W razie potrzeby określ plik.

Usuwanie certyfikatu podpisanego przez urząd certyfikacji

Zaimportowany certyfikat można usunąć, jeśli ten wygaśnie lub gdy szyfrowanie przesyłanych danych nie będzie już potrzebne.

**Ważne:**

W przypadku uzyskania certyfikatu na podstawie żądania CSR utworzonego za pomocą aplikacji Web Config nie można ponownie zaimportować usuniętego certyfikatu. W takim przypadku należy utworzyć ponownie żądanie CSR i uzyskać nowy certyfikat.

1. Otwórz aplikację Web Config, a następnie wybierz kartę **Zabezpieczenie sieci**. Następnie wybierz pozycje **SSL/TLS > Certyfikat** lub **IPsec/Filtrowanie IP > Certyfikat klienta** lub **IEEE802.1X > Certyfikat klienta**.
2. Kliknij przycisk **Usuń**.
3. W oknie komunikatu potwierdź, że certyfikat ma zostać usunięty.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Aktualizowanie certyfikatu z podpisem własnym

Ponieważ Certyfikat podpisany samodzielnie jest wystawiany przez skaner, można go zaktualizować po wygaśnięciu lub zmianie opisanych treści.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie sieci** tab > **SSL/TLS > Certyfikat**.
2. Kliknij przycisk **Aktualizuj**.

3. Wprowadź nazwę **Popularna nazwa**.

Można wprowadzić do pięciu adresów IPv4, adresów IPv6, nazw hosta, w pełni kwalifikowanych domen o długości od 1 do 128 znaków, rozdzielając je przecinkami. Pierwszy parametr jest przechowywany w nazwie publicznej, a pozostałe są przechowywane w polu aliasu dla podmiotu certyfikatu.

Przykład:

Adres IP skanera: 192.0.2.123, nazwa skanera: EPSONA1B2C3

Nazwa publiczna: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Podaj okres ważności certyfikatu.

5. Kliknij przycisk **Dalej**.

Wyświetlony zostanie komunikat z potwierdzeniem.

6. Kliknij przycisk **OK**.

Ustawienia skanera zostały zaktualizowane.

Uwaga:

Informacje o certyfikacie można sprawdzić, wybierając pozycje **Zabezpieczenie sieci > SSL/TLS > Certyfikat > Certyfikat podpisywany samodzielnie** i klikając przycisk **Potwierdź**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Konfiguracja Certyfikat CA

Po ustawieniu Certyfikat CA można zweryfikować ścieżkę certyfikatu urzędu certyfikacji serwera, do którego dostęp uzyskuje skaner. Pozwala to zapobiegać podszywaniu się.

Certyfikat CA dla drukarki można uzyskać od urzędu certyfikacji, który wystawił dany Certyfikat CA.

Importowanie Certyfikat CA

Certyfikat CA można zaimportować na skanerze.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zabezpieczenie sieci > Certyfikat CA**.
2. Kliknij pozycję **Importuj**.
3. Wskaż Certyfikat CA, który chcesz zaimportować.
4. Kliknij pozycję **OK**.

Po zakończeniu importu nastąpi powrót do ekranu **Certyfikat CA**, gdzie zostanie wyświetlony zaimportowany Certyfikat CA.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Usuwanie Certyfikat CA

Można usunąć zaimportowany Certyfikat CA.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz kartę **Zabezpieczenie sieci > Certyfikat CA**.
2. Kliknij **Usuń** obok Certyfikat CA do usunięcia.
3. W wyświetlonym komunikacie potwierdź chęć usunięcia certyfikatu.
4. Kliknij **Uruchom ponownie sieć**, a następnie upewnij się, że usunięty certyfikat CA nie jest wyszczególniony na zaktualizowanym ekranie.

Powiązane informacje

➔ [„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)

Komunikacja SSL/TLS ze skanerem

Jeśli na skanerze zainstalowano certyfikat serwera i włączono protokół SSL/TLS (Secure Sockets Layer/Transport Layer Security), można szyfrować komunikację między komputerami. Czynności te trzeba wykonać, aby uniemożliwić zdalny dostęp osobom nieupoważnionym.

Konfiguracja podstawowych ustawień SSL/TLS

Jeśli skaner obsługuje funkcję serwera HTTPS, możesz wykorzystać komunikację SSL/TLS do jej zaszyfrowania. Istnieje możliwość konfigurowania skanera i zarządzania nim z wykorzystaniem Web Config przy jednoczesnym zapewnieniu bezpieczeństwa.

Skonfiguruj siłę szyfrowania i funkcję przekierowania

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie sieci > SSL/TLS > Podstawowe**.
2. Wybierz wartość poszczególnych pozycji.
 - Siła szyfrowania
Wybierz poziom siły szyfrowania.
 - Przekieruj HTTP na HTTPS
Przekieruj na HTTPS, kiedy zostanie uzyskany dostęp do HTTP.
3. Kliknij przycisk **Dalej**.
Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.
Skaner został zaktualizowany.

Powiązane informacje

➔ [„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)

Konfigurowanie certyfikatu serwera na potrzeby skanera

1. Otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > SSL/TLS > Certyfikat**.
2. W polu **Certyfikat serwera** wybierz certyfikat, który ma być używany.
 - Certyfikat podpisywany samodzielnie
Zostanie wygenerowany certyfikat z podpisem własnym na potrzeby skanera. Jeśli nie został pobrany certyfikat podpisany przez urząd certyfikacji, wybierz tę opcję.
 - Certyfikat CA
Tutaj można wskazać uzyskany i zaimportowany uprzednio certyfikat podpisany przez urząd certyfikacji.
3. Kliknij pozycję **Dalej**.
Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij pozycję **OK**.
Ustawienia skanera zostały zaktualizowane.

Powiązane informacje

- ➔ [„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)
- ➔ [„Konfiguracja Certyfikat CA” na stronie 97](#)
- ➔ [„Konfiguracja Certyfikat CA” na stronie 101](#)

Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP

Informacje o IPsec/Filtrowanie IP

Ruch można filtrować na podstawie adresów IP, usług i portów, używając funkcji filtrowania IPsec/IP. Połączenie różnych filtrów umożliwia takie skonfigurowanie skanera, aby akceptowane lub blokowane były określone klienty i konkretne rodzaje danych. Ponadto można zwiększyć poziom bezpieczeństwa za pomocą protokołu IPsec.

Uwaga:

Protokół IPsec jest obsługiwany przez komputery z systemem Windows Vista lub nowszym albo systemem Windows Server 2008 lub nowszym.

Konfigurowanie zasad domyślnych

W celu filtrowania ruchu należy skonfigurować zasady domyślne. Takie zasady będą mieć zastosowanie do wszystkich użytkowników i grup nawiązujących połączenia ze skanerem. W celu uzyskania bardziej precyzyjnej kontroli nad użytkownikami i grupami użytkowników należy skonfigurować zasady grupowe.

1. Otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe**.
2. Wprowadź wartości poszczególnych pozycji.

3. Kliknij przycisk **Dalej**.
Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.
Ustawienia skanera zostały zaktualizowane.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Elementy ustawień opcji Zasady domyślne**Zasady domyślne**

Elementy	Ustawienia i objaśnienie
IPsec/Filtrowanie IP	Umożliwia włączenie lub wyłączenie funkcji filtrowania IPsec/IP.

 Kontrola dostępu

Umożliwia skonfigurowanie metody weryfikowania pakietów protokołu IP.

Elementy	Ustawienia i objaśnienie
Zezwól na dostęp	Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IP.
Odmów dostępu	Wybierz tę opcję, aby zablokować przekazywanie skonfigurowanych pakietów protokołu IP.
IPsec	Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IPsec.

Wersja IKE

Wybierz ustawienie **IKEv1** lub **IKEv2** dla opcji **Wersja IKE**. Wybierz jedną z nich odpowiednio do urządzenia, z którym skaner jest połączony.

IKEv1

Po wybraniu ustawienia **IKEv1** dla opcji **Wersja IKE** wyświetlane są następujące pozycje.

Elementy	Ustawienia i objaśnienie
Sposób uwierzytelniania	Aby wybrać opcję Certyfikat , należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji.
Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

IKEv2

Po wybraniu ustawienia **IKEv2** dla opcji **Wersja IKE** wyświetlane są następujące pozycje.

Elementy	Ustawienia i objaśnienie	
Lokalny	Sposób uwierzytelniania	Aby wybrać opcję Certyfikat , należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji.
	Typ ID	Jeśli zostanie wybrane ustawienie Klucz współdzielony dla opcji Sposób uwierzytelniania , wybierz rodzaj identyfikatora skanera.
	ID	Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora. Na początku identyfikatora nie można używać znaków: @, # i =. Wyróżniająca nazwa: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=”. Adres IP: wprowadź adres w formacie IPv4 lub IPv6. FQDN: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.). Adres email: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@”. ID klucza: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E).
	Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
	Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

Elementy		Ustawienia i objaśnienie
Zdalny	Sposób uwierzytelniania	Aby wybrać opcję Certyfikat , należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji.
	Typ ID	Jeśli zostanie wybrane ustawienie Klucz współdzielony dla opcji Sposób uwierzytelniania , wybierz rodzaj identyfikatora urządzenia, które ma być uwierzytelnione.
	ID	Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora. Na początku identyfikatora nie można używać znaków: @, # i =. Wyróżniająca nazwa: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=”. Adres IP: wprowadź adres w formacie IPv4 lub IPv6. FQDN: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.). Adres email: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@”. ID klucza: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E).
	Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
	Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

Hermetyzacja

Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Kontrola dostępu**, skonfiguruj tryb hermetyzacji.

Elementy	Ustawienia i objaśnienie
Tryb transportu	Wybierz tę opcję, jeśli skaner jest używany tylko w jednej sieci LAN. Pakiety protokołu IP w warstwie 4. lub wyższej będą szyfrowane.
Tryb tunelowania	Wybierz tę opcję, jeśli skaner jest używany w sieci obsługującej Internet, np. IPsec-VPN. Szyfrowane będą nagłówki i zawartość pakietów IP. Zdalna brama (Tryb tunelowania): jeśli dla opcji Tryb tunelowania zostanie wybrane ustawienie Hermetyzacja , w tym polu wprowadź adres bramy o długości od 1 do 39 znaków.

Protokół zabezpieczenia

Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Kontrola dostępu**, wybierz jedno z poniższych ustawień.

Elementy	Ustawienia i objaśnienie
ESP	Wybierz tę opcję, aby zapewnić integralność uwierzytelniania i danych, a także włączyć szyfrowanie danych.
AH	Wybierz tę opcję, aby zapewnić integralność uwierzytelniania i danych. Nawet jeśli szyfrowanie danych jest niemożliwe, nadal będzie można korzystać z protokołu IPsec.

Ustawienia algorytmu

Zaleca się wybranie pozycji **Dowolny** dla wszystkich ustawień lub wybranie pozycji innej niż **Dowolny** dla poszczególnych ustawień. Jeśli pozycja **Dowolny** zostanie wybrana dla niektórych ustawień, a pozycja inna niż **Dowolny** zostanie wybrana dla innych ustawień, komunikacja z urządzeniem może nie być możliwa w zależności od innego urządzenia, które ma być uwierzytelnione.

Elementy		Ustawienia i objaśnienie
IKE	Szyfrowanie	Umożliwia wybór algorytmu szyfrowania protokołu IKE. Dostępne pozycje różnią się w zależności od wersji protokołu IKE.
	Uwierzytelnianie	Umożliwia wybór algorytmu uwierzytelniania protokołu IKE.
	Wymiana kluczy	Umożliwia wybór algorytmu wymiany kluczy protokołu IKE. Dostępne pozycje różnią się w zależności od wersji protokołu IKE.
ESP	Szyfrowanie	Umożliwia wybór algorytmu szyfrowania protokołu ESP. Opcja jest dostępna, tylko jeśli wybrano ustawienie ESP dla opcji Protokół zabezpieczenia .
	Uwierzytelnianie	Umożliwia wybór algorytmu uwierzytelniania protokołu ESP. Opcja jest dostępna, tylko jeśli wybrano ustawienie ESP dla opcji Protokół zabezpieczenia .
AH	Uwierzytelnianie	Umożliwia wybór algorytmu szyfrowania protokołu AH. Opcja jest dostępna, tylko jeśli wybrano ustawienie AH dla opcji Protokół zabezpieczenia .

Konfigurowanie zasad grupowych

Zasady grupowe to co najmniej jedna reguła stosowana do użytkownika lub grupy użytkowników. Skaner weryfikuje pakiety protokołu IP pod kątem zgodności ze skonfigurowanymi zasadami. Pakiety protokołu IP są najpierw uwierzytelniane z wykorzystaniem zasad grupowych od 1 do 10, a następnie z wykorzystaniem zasad domyślnych.

1. Otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe**.
2. Kliknij numerowaną kartę, którą chcesz skonfigurować.
3. Wprowadź wartości poszczególnych pozycji.
4. Kliknij przycisk **Dalej**.
Wyświetlony zostanie komunikat z potwierdzeniem.
5. Kliknij przycisk **OK**.
Ustawienia skanera zostały zaktualizowane.

Elementy ustawień opcji Zasady grupy

Elementy	Ustawienia i objaśnienie
Włącz te Zasady grupy	Umożliwia włączenie lub wyłączenie zasad grupowych.

Kontrola dostępu

Umożliwia skonfigurowanie metody weryfikowania pakietów protokołu IP.

Elementy	Ustawienia i objaśnienie
Zezwól na dostęp	Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IP.
Odmów dostępu	Wybierz tę opcję, aby zablokować przekazywanie skonfigurowanych pakietów protokołu IP.
IPsec	Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IPsec.

Adres lokalny (skaner)

Wybierz adres IPv4 lub adres IPv6 dopasowany do otoczenia sieciowego. Jeśli adres IP jest przydzielany automatycznie, można wybrać opcję **Użyj automatycznego uzyskiwania adresu IPv4**.

Uwaga:

Jeśli adres IPv6 jest przydzielany automatycznie, połączenie może być niedostępne. Należy skonfigurować statyczny adres IPv6.

Zdalny adres (Host)

Umożliwia określenie adresu IP urządzenia na potrzeby kontroli dostępu. Adres IP musi mieć do 43 znaków. Jeśli nie zostanie podany żaden adres IP, kontrolowane będą wszystkie adresy.

Uwaga:

Jeśli adres IP jest przydzielany automatycznie (np. przez serwer DHCP), połączenie może być niedostępne. Należy skonfigurować statyczny adres IP.

Metoda wyboru portu

Umożliwia wybranie metody określania portów.

Nazwa usługi

Jeśli dla opcji **Nazwa usługi** zostanie wybrane ustawienie **Metoda wyboru portu**, wybierz jedno z poniższych ustawień.

Protokół transportu

Jeśli dla opcji **Numer portu** zostanie wybrane ustawienie **Metoda wyboru portu**, skonfiguruj tryb hermetyzacji.

Elementy	Ustawienia i objaśnienie
Dowolny protokół	Wybierz tę opcję, aby kontrolować wszystkie typy protokołów.
TCP	Wybierz tę opcję, aby kontrolować dane w trybie emisji pojedynczej.
UDP	Wybierz tę opcję, aby kontrolować dane w trybach rozgłaszania oraz multiemisji.
ICMPv4	Wybierz tę opcję, aby kontrolować komendy ping.

Port lokalny

Jeśli dla opcji **Metoda wyboru portu** zostanie wybrane ustawienie **Numer portu**, a dla opcji **Protokół transportu** — ustawienie **TCP** lub **UDP**, wprowadź numery portów, na których odbierane pakiety mają być kontrolowane. Rozdziel numery portów przecinkami. Można podać maksymalnie 10 numerów portów.

Przykład: 20,80,119,5220

Jeśli nie zostanie podany żaden numer portu, kontrolowane będą wszystkie porty.

Port zdalny

Jeśli dla opcji **Metoda wyboru portu** zostanie wybrane ustawienie **Numer portu**, a dla opcji **Protokół transportu** — ustawienie **TCP** lub **UDP**, wprowadź numery portów, na których wysyłane pakiety mają być kontrolowane. Rozdziel numery portów przecinkami. Można podać maksymalnie 10 numerów portów.

Przykład: 25,80,143,5220

Jeśli nie zostanie podany żaden numer portu, kontrolowane będą wszystkie porty.

Wersja IKE

Wybierz ustawienie **IKEv1** lub **IKEv2** dla opcji **Wersja IKE**. Wybierz jedną z nich odpowiednio do urządzenia, z którym skaner jest połączony.

IKEv1

Po wybraniu ustawienia **IKEv1** dla opcji **Wersja IKE** wyświetlane są następujące pozycje.

Elementy	Ustawienia i objaśnienie
Sposób uwierzytelniania	Jeśli dla opcji IPsec zostanie wybrane ustawienie Kontrola dostępu , wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych.
Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

IKEv2

Po wybraniu ustawienia **IKEv2** dla opcji **Wersja IKE** wyświetlane są następujące pozycje.

Elementy		Ustawienia i objaśnienie
Lokalny	Sposób uwierzytelniania	Jeśli dla opcji IPsec zostanie wybrane ustawienie Kontrola dostępu , wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych.
	Typ ID	Jeśli zostanie wybrane ustawienie Klucz współdzielony dla opcji Sposób uwierzytelniania , wybierz rodzaj identyfikatora skanera.
	ID	Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora. Na początku identyfikatora nie można używać znaków: @, # i =. Wyróżniająca nazwa: wprowadź od 1 do 255 bajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=”. Adres IP: wprowadź adres w formacie IPv4 lub IPv6. FQDN: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.). Adres email: wprowadź od 1 do 255 bajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@”. ID klucza: wprowadź od 1 do 255 bajtowych znaków ASCII (0x20 do 0x7E).
	Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
	Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

Elementy		Ustawienia i objaśnienie
Zdalny	Sposób uwierzytelniania	Jeśli dla opcji IPsec zostanie wybrane ustawienie Kontrola dostępu , wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych.
	Typ ID	Jeśli zostanie wybrane ustawienie Klucz współdzielony dla opcji Sposób uwierzytelniania , wybierz rodzaj identyfikatora urządzenia, które ma być uwierzytelnione.
	ID	Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora. Na początku identyfikatora nie można używać znaków: @, # i =. Wyróżniająca nazwa: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=”. Adres IP: wprowadź adres w formacie IPv4 lub IPv6. FQDN: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.). Adres email: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@”. ID klucza: wprowadź od 1 do 255 jednobajtowych znaków ASCII (0x20 do 0x7E).
	Klucz współdzielony	Jeśli dla opcji Klucz współdzielony zostanie wybrane ustawienie Sposób uwierzytelniania , w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków.
	Potwierdź Klucz współdzielony	Wprowadź skonfigurowany klucz w celu potwierdzenia.

Hermetyzacja

Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Kontrola dostępu**, skonfiguruj tryb hermetyzacji.

Elementy	Ustawienia i objaśnienie
Tryb transportu	Wybierz tę opcję, jeśli skaner jest używany tylko w jednej sieci LAN. Pakiety protokołu IP w warstwie 4. lub wyższej będą szyfrowane.
Tryb tunelowania	Wybierz tę opcję, jeśli skaner jest używany w sieci obsługującej Internet, np. IPsec-VPN. Szyfrowane będą nagłówki i zawartość pakietów IP. Zdalna brama (Tryb tunelowania): jeśli dla opcji Tryb tunelowania zostanie wybrane ustawienie Hermetyzacja , w tym polu wprowadź adres bramy o długości od 1 do 39 znaków.

Protokół zabezpieczenia

Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Kontrola dostępu**, wybierz jedno z poniższych ustawień.

Elementy	Ustawienia i objaśnienie
ESP	Wybierz tę opcję, aby zapewnić integralność uwierzytelniania i danych, a także włączyć szyfrowanie danych.
AH	Wybierz tę opcję, aby zapewnić integralność uwierzytelniania i danych. Nawet jeśli szyfrowanie danych jest niemożliwe, nadal będzie można korzystać z protokołu IPsec.

Ustawienia algorytmu

Zaleca się wybranie pozycji **Dowolny** dla wszystkich ustawień lub wybranie pozycji innej niż **Dowolny** dla poszczególnych ustawień. Jeśli pozycja **Dowolny** zostanie wybrana dla niektórych ustawień, a pozycja inna niż **Dowolny** zostanie wybrana dla innych ustawień, komunikacja z urządzeniem może nie być możliwa w zależności od innego urządzenia, które ma być uwierzytelnione.

Elementy		Ustawienia i objaśnienie
IKE	Szyfrowanie	Umożliwia wybór algorytmu szyfrowania protokołu IKE. Dostępne pozycje różnią się w zależności od wersji protokołu IKE.
	Uwierzytelnianie	Umożliwia wybór algorytmu uwierzytelniania protokołu IKE.
	Wymiana kluczy	Umożliwia wybór algorytmu wymiany kluczy protokołu IKE. Dostępne pozycje różnią się w zależności od wersji protokołu IKE.
ESP	Szyfrowanie	Umożliwia wybór algorytmu szyfrowania protokołu ESP. Opcja jest dostępna, tylko jeśli wybrano ustawienie ESP dla opcji Protokół zabezpieczenia .
	Uwierzytelnianie	Umożliwia wybór algorytmu uwierzytelniania protokołu ESP. Opcja jest dostępna, tylko jeśli wybrano ustawienie ESP dla opcji Protokół zabezpieczenia .
AH	Uwierzytelnianie	Umożliwia wybór algorytmu szyfrowania protokołu AH. Opcja jest dostępna, tylko jeśli wybrano ustawienie AH dla opcji Protokół zabezpieczenia .

Kombinacja ustawienia Adres lokalny (skaner) i Zdalny adres (Host) w Zasady grupy

		Ustawianie Adres lokalny (skaner)		
		IPv4	IPv6* ²	Dowolne adresy* ³
Ustawianie Zdalny adres (Host)	IPv4* ¹	✓	–	✓
	IPv6* ^{1, 2}	–	✓	✓
	Puste	✓	✓	✓

*1 Jeśli dla opcji **Kontrola dostępu** zostanie wybrane ustawienie **IPsec**, nie można określać długości prefiksu.

*2 Jeśli dla opcji **Kontrola dostępu** zostanie wybrane ustawienie **IPsec**, można wybrać łącze lokalne (fe80::), ale zasady grupowe będą wyłączone.

*3 Poza adresami połączeń lokalnych IPv6.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Odwołania nazw usług w zasadach grupowych

Uwaga:

Niedostępne usługi są wyświetlane, ale nie można ich zaznaczać.

Nazwa usługi	Typ protokołu	Numer portu lokalnego	Numer portu zdalnego	Kontrolowane funkcje
Dowolny	–	–	–	Wszystkie usługi
ENPC	UDP	3289	Dowolny port	Wyszukiwanie skanera w aplikacjach, takich jak Epson Device Admin i sterownik skanera
SNMP	UDP	161	Dowolny port	Uzyskiwanie i konfiguracja MIB w aplikacjach, takich jak Epson Device Admin i sterownik skanera Epson
WSD	TCP	Dowolny port	5357	Kontrolowanie WSD
WS-Discovery	UDP	3702	Dowolny port	Wyszukiwanie skanerów WSD
Network Scan	TCP	1865	Dowolny port	Przesyłanie zeskanowanych danych z Document Capture Pro
Network Push Scan	TCP	Dowolny port	2968	Pozyskiwanie informacji o zadaniach skanowania inicjowanego z Document Capture Pro
Network Push Scan Discovery	UDP	2968	Dowolny port	Wyszukiwanie komputera ze skanera
Dane FTP (zdalny)	TCP	Dowolny port	20	Klient FTP (przekazywanie danych skanowania) Jednak może być w ten sposób kontrolowany wyłącznie serwer FTP, który korzysta ze zdalnego portu nr 20.
Kontrola FTP (zdalny)	TCP	Dowolny port	21	Klient FTP (kontrolowanie przekazywania danych skanowania)
CIFS (zdalny)	TCP	Dowolny port	445	Klient CIFS (przekazywanie danych skanowania do folderu)
NetBIOS Name Service (zdalny)	UDP	Dowolny port	137	Klient CIFS (przekazywanie danych skanowania do folderu)
NetBIOS Datagram Service (zdalny)	UDP	Dowolny port	138	
NetBIOS Session Service (zdalny)	TCP	Dowolny port	139	
HTTP (lokalny)	TCP	80	Dowolny port	Serwer HTTP(S) (przesyłanie danych Web Config i WSD)
HTTPS (lokalny)	TCP	443	Dowolny port	
HTTP (zdalny)	TCP	Dowolny port	80	Klient HTTP(S) (aktualizowanie oprogramowania układowego i certyfikatu głównego)
HTTPS (zdalny)	TCP	Dowolny port	443	

Przykłady konfiguracji opcji IPsec/Filtrowanie IP

Wyłącznie odbieranie pakietów protokołu IPsec

Poniższy przykład przedstawia konfigurowanie wyłącznie zasad domyślnych.

Zasady domyślne:

- IPsec/Filtrowanie IP: **Włącz**
- Kontrola dostępu: **IPsec**
- Sposób uwierzytelniania: **Klucz współdzielony**
- Klucz współdzielony: wprowadź maksymalnie 127 znaków.

Zasady grupy: nie konfiguruje.

Pobieranie danych skanowania i ustawień skanera

Ten przykład przedstawia zezwalanie na przesyłanie danych skanowania i konfiguracji skanera z określonych usług.

Zasady domyślne:

- IPsec/Filtrowanie IP: **Włącz**
- Kontrola dostępu: **Odmów dostępu**

Zasady grupy:

- Włącz te Zasady grupy:** zaznacz to pole wyboru.
- Kontrola dostępu: **Zezwól na dostęp**
- Zdalny adres (Host): adres IP klienta
- Metoda wyboru portu: **Nazwa usługi**
- Nazwa usługi: zaznacz pole wyboru **ENPC, SNMP, HTTP (lokalny), HTTPS (lokalny) i Network Scan.**

Uzyskiwanie dostępu wyłącznie z określonego adresu IP

Poniższy przykład umożliwia uzyskanie dostępu do skanera ze ściśle określonego adresu IP.

Zasady domyślne:

- IPsec/Filtrowanie IP: **Włącz**
- Kontrola dostępu: **Odmów dostępu**

Zasady grupy:

- Włącz te Zasady grupy:** zaznacz to pole wyboru.
- Kontrola dostępu: **Zezwól na dostęp**
- Zdalny adres (Host): adres IP klienta administratora

Uwaga:

Klient będzie mógł uzyskać dostęp do skanera i skonfigurować go niezależnie od konfiguracji zasad.

Konfiguracja certyfikatu dla IPsec/filtrowania IP

Skonfiguruj certyfikat klienta dla IPsec/filtrowania IP. Kiedy go ustawisz, możesz wykorzystać certyfikat jako metodę uwierzytelnienia dla IPsec/filtrowania IP. Jeśli chcesz skonfigurować urządzenie certyfikacyjne, przejdź do **Certyfikat CA**.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz kartę **Zabezpieczenie sieci > IPsec/Filtrowanie IP > Certyfikat klienta**.
2. Importuj certyfikat w **Certyfikat klienta**.
Jeśli masz już zaimportowany certyfikat opublikowany przez urządzenie certyfikacyjne, możesz skopiować certyfikat i wykorzystać go w IPsec/filtrowaniu IP. Aby skopiować, wybierz certyfikat z **Kopiuj z**, a następnie kliknij przycisk **Kopiuj**.

Powiązane informacje

- ➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38
- ➔ „Konfiguracja Certyfikat CA” na stronie 97
- ➔ „Konfiguracja Certyfikat CA” na stronie 101

Podłączanie skanera do sieci IEEE802.1X

Konfigurowanie sieci IEEE 802.1X

Po włączeniu funkcji IEEE 802.1X na skanerze można używać go w sieci połączonej z serwerem RADIUS, przełącznikiem sieci lokalnej z funkcją uwierzytelniania lub punktem dostępu.

1. Otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > IEEE802.1X > Podstawowe**.
2. Wprowadź wartości poszczególnych pozycji.
Aby używać skanera w sieci Wi-Fi, kliknij przycisk **Konfiguracja Wi-Fi** i wybierz lub wprowadź identyfikator SSID.
Uwaga:
Można współdzielić ustawienia między połączeniami Ethernet i Wi-Fi.
3. Kliknij przycisk **Dalej**.
Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.
Ustawienia skanera zostały zaktualizowane.

Powiązane informacje

- ➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Pozycje ustawień sieciowych IEEE 802.1X

Elementy	Ustawienia i objaśnienie	
IEEE802.1X (przewodowa sieć LAN)	Umożliwia włączenie lub wyłączenie ustawień strony (IEEE802.1X > Podstawowe) dotyczących uwierzytelniania IEEE802.1X (przewodowa sieć LAN).	
IEEE802.1X (Wi-Fi)	Wyświetlanie stanu połączenia IEEE802.1X (Wi-Fi).	
Metoda połączenia	Wyświetlanie metody połączenia bieżącej sieci.	
Typ EAP	Wybierz opcję określającą metodę uwierzytelniania skanera na serwerze RADIUS.	
	EAP-TLS	Trzeba uzyskać certyfikat podpisany przez urząd certyfikacji i zaimportować go.
	PEAP-TLS	
	PEAP/MSCHAPv2	Trzeba skonfigurować hasło.
EAP-TTLS		
ID użytkownika	Skonfiguruj identyfikator używany do uwierzytelniania na serwerze RADIUS. Wprowadź od 1 do 128 znaków jednobajtowych w formacie ASCII (0x20 do 0x7E).	
Hasło	Skonfiguruj hasło używane do uwierzytelniania skanera. Wprowadź od 1 do 128 znaków jednobajtowych w formacie ASCII (0x20 do 0x7E). Jeśli rolę serwera RADIUS pełni urządzenie z systemem Windows, można wprowadzić do 127 znaków.	
Potwierdź hasło	Wprowadź skonfigurowane hasło w celu potwierdzenia.	
ID serwera	Można podać identyfikator serwera, aby przeprowadzać uwierzytelnianie na konkretnym serwerze RADIUS. Moduł uwierzytelniający sprawdza, czy w polu subject/subjectAltName certyfikatu serwera wysłanego przez serwer RADIUS jest identyfikator serwera. Wprowadź od 0 do 128 znaków jednobajtowych ASCII (0x20 do 0x7E).	
Weryfikacja certyfikatu (przewodowa sieć lokalna)	Aby wykonać funkcję Weryfikacja certyfikatu przy użyciu trybu IEEE802.1X (przewodowa sieć LAN) , wybierz ustawienie Włącz . Jeśli zostanie wybrane ustawienie Enable, zapoznaj się z informacjami powiązanymi i zaimportuj plik Certyfikat CA . Pamiętaj, że funkcja Weryfikacja certyfikatu jest zawsze włączona w trybie IEEE802.1X (Wi-Fi). Zaimportuj plik Certyfikat CA.	
Nazwa użytkownika anonimowego	Jeśli opcja Typ EAP zostanie ustawiona na PEAP-TLS lub PEAP/MSCHAPv2 , można skonfigurować nazwę użytkownika anonimowego zamiast ID użytkownika, która będzie używana w pierwszym etapie uwierzytelniania PEAP. Wprowadź od 0 do 128 znaków jednobajtowych ASCII (0x20 do 0x7E).	
Siła szyfrowania	Dostępne są następujące opcje.	
	Wys.	AES256/3DES
	Średnia	AES256/3DES/AES128/RC4

Powiązane informacje

➔ „Konfiguracja Certyfikat CA” na stronie 101

Konfiguracja certyfikatu dla IEEE 802.1X

Skonfiguruj certyfikat klienta dla IEEE802.1X. Ustawiając go, możesz skorzystać z **EAP-TLS** i **PEAP-TLS** jako metody uwierzytelnienia IEEE 802.1X. Jeśli chcesz skonfigurować certyfikat urzędu certyfikacyjnego, przejdź do **Certyfikat CA**.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz kartę **Zabezpieczenie sieci > IEEE802.1X > Certyfikat klienta**.
2. Wprowadź certyfikat w **Certyfikat klienta**.
Jeśli masz już zaimportowany certyfikat opublikowany przez urząd certyfikacyjny, możesz skopiować i wykorzystać go w IEEE802.1X. Aby skopiować, wybierz certyfikat z **Kopiuj z**, a następnie kliknij przycisk **Kopiuj**.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Rozwiązywanie problemów związanych z zaawansowanymi zabezpieczeniami

Przywracanie ustawień zabezpieczeń

Utworzenie bardzo bezpiecznego środowiska, np. IPsec/Filtrowanie IP, może uniemożliwić komunikację z urządzeniami ze względu na niepoprawne ustawienia albo problem z urządzeniem lub serwerem. W takim przypadku przywróć ustawienia zabezpieczeń, aby ponownie skonfigurować ustawienia urządzenia lub zezwolić na tymczasowe użycie.

Wyłączanie funkcji zabezpieczeń przy użyciu aplikacji Web Config

Funkcję IPsec/Filtrowanie IP można wyłączyć za pomocą aplikacji Web Config.

1. Otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe**.
2. Wyłącz IPsec/Filtrowanie IP.

Problemy z korzystaniem z funkcji zabezpieczeń sieciowych

Zapomniany klucz wstępny

Możliwe jest ponowne konfigurowanie klucza wstępnego.

Aby zmienić klucz, otwórz aplikację Web Config i wybierz kartę **Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe > Zasady domyślne** lub **Zasady grupy**.

Po zmianie klucza wstępnego trzeba skonfigurować klucz wstępny na komputerach.

Powiązane informacje

- ➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38
- ➔ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103

Brak możliwości nawiązania połączenia z wykorzystaniem protokołu IPsec

Określ algorytm, którego skaner lub komputer nie obsługuje.

Skaner obsługuje algorytmy wymienione w poniższej tabeli. Sprawdź ustawienia komputera.

Metoda szyfrowania	Algorytmy
Algorytm szyfrowania protokołu IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algorytm uwierzytelniania protokołu IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algorytm wymiany kluczy protokołu IKE	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
Algorytm szyfrowania protokołu ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algorytm uwierzytelniania protokołu ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algorytm uwierzytelniania protokołu AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Dostępne tylko na potrzeby protokołu IKEv2

Powiązane informacje

- ➔ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103

Nagły brak możliwości nawiązania komunikacji

Adres IP skanera został zmieniony lub nie może być używany.

Jeżeli adres IP przydzielony do adresu lokalnego w Zasady grupy został zmieniony lub nie może być używany, nie można używać komunikacji IPsec. Wyłącz obsługę protokołu IPsec na panelu sterowania skanera.

Jeśli adres IP przydzielony przez serwer DHCP jest nieaktualny, serwer DHCP jest aktualnie ponownie uruchamiany lub adres IPv6 jest nieaktualny lub nie został uzyskany, adres IP zarejestrowany na potrzeby aplikacji Web Config (**Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe > Zasady grupy > Adres lokalny (skaner)**) może nie zostać znaleziony.

Należy używać statycznego adresu IP.

Adres IP komputera został zmieniony lub nie może być używany.

Jeżeli adres IP przydzielony do adresu zdalnego w Zasady grupy został zmieniony lub nie może być używany, nie można używać komunikacji IPsec.

Wyłącz obsługę protokołu IPsec na panelu sterowania skanera.

Jeśli adres IP przydzielony przez serwer DHCP jest nieaktualny, serwer DHCP jest aktualnie ponownie uruchamiany lub adres IPv6 jest nieaktualny lub nie został uzyskany, adres IP zarejestrowany na potrzeby aplikacji Web Config (**Zabezpieczenie sieci > IPsec/Filtrowanie IP > Podstawowe > Zasady grupy > Zdalny adres (Host)**) może nie zostać znaleziony.

Należy używać statycznego adresu IP.

Powiązane informacje

- ➔ [„Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38](#)
- ➔ [„Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103](#)

Brak połączenia po skonfigurowaniu filtrowania IPsec/IP

Ustawienia funkcji filtrowania IPsec/IP są nieprawidłowe.

Wyłącz filtrowanie IPsec/IP na panelu sterowania skanera. Podłącz skaner do komputera i ponownie skonfiguruj filtrowanie IPsec/IP.

Powiązane informacje

- ➔ [„Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 103](#)

Nie można uzyskać dostępu do urządzenia po skonfigurowaniu funkcji IEEE 802.1X

Ustawienia połączenia IEEE 802.1X są niepoprawne.

Wyłącz łączność IEEE 802.1X i Wi-Fi z poziomu panelu sterowania skanera. Połącz skaner i komputer, a następnie ponownie skonfiguruj połączenie IEEE 802.1X.

Powiązane informacje

- ➔ [„Konfigurowanie sieci IEEE 802.1X” na stronie 115](#)

Problemy z używaniem certyfikatu cyfrowego

Nie można zaimportować Certyfikat CA

Certyfikat CA i informacje dotyczące żądania CSR nie zgadzają się.

Jeśli Certyfikat CA oraz żądanie CSR nie zawierają tych samych informacji, import żądania CSR będzie niemożliwy. Sprawdź następujące rzeczy:

- Czy próbujesz zaimportować certyfikat na urządzenie o niezgodnych danych?
Sprawdź informacje zawarte w żądaniu CSR, po czym zaimportuj certyfikat na urządzenie o tych samych danych.
- Czy po wysłaniu żądania CSR do urzędu certyfikacji plik żądania CSR zapisany na skanerze został nadpisany?
Uzyskaj certyfikat z urzędu certyfikacji ponownie przy użyciu aktualnego żądania CSR.

Certyfikat CA ma wielkość przekraczającą 5 KB.

Zaimportowanie Certyfikat CA o wielkości przekraczającej 5 KB jest niemożliwe.

Hasło do importu certyfikatu jest nieprawidłowe.

Wprowadź prawidłowe hasło. Jeśli nie pamiętasz hasła, zaimportowanie certyfikatu będzie niemożliwe. Ponownie uzyskaj Certyfikat CA.

Powiązane informacje

➔ [„Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 98](#)

Brak możliwości aktualizacji certyfikatu z podpisem własnym

Nie wprowadzono Popularna nazwa.

Popularna nazwa musi zostać podana.

W Popularna nazwa wprowadzono nieobsługiwane znaki.

Wprowadź nazwę hosta lub nazwę w formacie IPv4, IPv6 lub FQDN zawierającą od 1 do 128 znaków w kodowaniu ASCII (0x20–0x7E).

Nazwa publiczna zawiera przecinek lub spację.

Użycie przecinka powoduje podzielenie nazwy **Popularna nazwa** w miejscu jego użycia. Jeśli przed lub po przecinku wstawiona zostanie spacja, wystąpi błąd.

Powiązane informacje

➔ [„Aktualizowanie certyfikatu z podpisem własnym” na stronie 100](#)

Brak możliwości utworzenia żądania CSR

Nie wprowadzono Popularna nazwa.

Popularna nazwa musi zostać podana.

W polach Popularna nazwa, Organizacja, Jednostka organizacyjna, Miejscowość i Stan/Prowincja wprowadzono nieobsługiwane znaki.

Wprowadź nazwę hosta lub nazwę w formacie IPv4, IPv6 lub FQDN w kodowaniu ASCII (0x20–0x7E).

Popularna nazwa zawiera przecinek lub spację.

Użycie przecinka powoduje podzielenie nazwy **Popularna nazwa** w miejscu jego użycia. Jeśli przed lub po przecinku wstawiona zostanie spacja, wystąpi błąd.

Powiązane informacje

➔ [„Uzyskiwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 97](#)

Wyświetlane jest ostrzeżenie dotyczące certyfikatu cyfrowego

Komunikat	Przyczyna i sposób rozwiązania problemu
Wprowadź Certyfikat serwera.	<p>Przyczyna: Nie wybrano pliku do zaimportowania.</p> <p>Rozwiązanie: Wybierz plik i kliknij przycisk Importuj.</p>
Certyfikat CA 1 nie został wprowadzony.	<p>Przyczyna: Nie podano pierwszego certyfikatu urzędu certyfikacji. Podano wyłącznie drugi certyfikat urzędu certyfikacji.</p> <p>Rozwiązanie: Najpierw należy zaimportować pierwszy certyfikat urzędu certyfikacji.</p>
Poniżej nieprawidłowa wartość.	<p>Przyczyna: Ścieżka dostępu do pliku i/lub hasło zawierają nieobsługiwane znaki.</p> <p>Rozwiązanie: Upewnij się, że wszystkie pozycje zostały podane prawidłowo.</p>
Nieprawidłowa data i godzina.	<p>Przyczyna: Nie ustawiono daty i godziny na skanerze.</p> <p>Rozwiązanie: Ustaw datę i godzinę za pomocą aplikacji Web Config lub EpsonNet Config.</p>
Nieprawidłowe hasło.	<p>Przyczyna: Podane hasło jest niezgodne z hasłem ustawionym dla certyfikatu urzędu certyfikacji.</p> <p>Rozwiązanie: Podaj prawidłowe hasło.</p>

Komunikat	Przyczyna i sposób rozwiązania problemu
Nieprawidłowy plik.	<p>Przyczyna:</p> <p>Importowany plik certyfikatu nie jest plikiem w formacie X509.</p> <p>Rozwiązanie:</p> <p>Upewnij się, że wybrano prawidłowy plik certyfikatu wysłany przez zaufany urząd certyfikacji.</p>
	<p>Przyczyna:</p> <p>Zaimportowany plik jest zbyt duży. Maksymalny dopuszczalny rozmiar pliku to 5 KB.</p> <p>Rozwiązanie:</p> <p>Jeśli wybrano prawidłowy plik, zachodzi podejrzenie uszkodzenia lub sfalszowania certyfikatu.</p>
	<p>Przyczyna:</p> <p>Łańcuch zawarty w certyfikacie jest nieprawidłowy.</p> <p>Rozwiązanie:</p> <p>Więcej informacji na temat certyfikatu zawiera serwis WWW urzędu certyfikacji.</p>
Nie można użyć certyfikatu Certyfikat serwera, który zawiera więcej niż trzy certyfikaty Certyfikat CA.	<p>Przyczyna:</p> <p>Plik certyfikatu w formacie PKCS#12 zawiera więcej niż 3 certyfikaty urzędów certyfikacji.</p> <p>Rozwiązanie:</p> <p>Należy skonwertować certyfikaty z formatu PKCS#12 do formatu PEM i zaimportować je oddzielnie. Nie można importować plików certyfikatów w formacie PKCS#12 zawierających więcej niż 2 certyfikaty urzędów certyfikacji.</p>
Certyfikat utracił ważność. Sprawdź, czy certyfikat jest ważny lub sprawdź ustawienie Data i godzina w produkcie.	<p>Przyczyna:</p> <p>Certyfikat jest nieaktualny.</p> <p>Rozwiązanie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Jeśli certyfikat jest nieaktualny, pobierz i zaimportuj nowy certyfikat. <input type="checkbox"/> Jeśli certyfikat jest aktualny, sprawdź, czy ustawienia daty i godziny na skanerze są prawidłowe.
Wymagany jest Klucz prywatny.	<p>Przyczyna:</p> <p>Z certyfikatem nie jest powiązany klucz prywatny.</p> <p>Rozwiązanie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PEM/DER, należy wskazać plik klucza prywatnego. <input type="checkbox"/> Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PKCS#12, należy utworzyć plik z kluczem prywatnym.
	<p>Przyczyna:</p> <p>Ponownie zaimportowano certyfikat w formacie PEM/DER uzyskany na podstawie żądania CSR za pomocą aplikacji Web Config.</p> <p>Rozwiązanie:</p> <p>Jeśli na podstawie żądania CSR w aplikacji Web Config został pobrany certyfikat w formacie PEM/DER, certyfikat ten można zaimportować tylko raz.</p>

Komunikat	Przyczyna i sposób rozwiązania problemu
Konfiguracja nie powiodła się.	<p>Przyczyna:</p> <p>Nie można zakończyć konfiguracji, ponieważ nie udało się nawiązać komunikacji między skanerem a komputerem lub pliku nie można odczytać z powodu innego błędu.</p> <p>Rozwiązanie:</p> <p>Sprawdź podany plik oraz połączenie między drukarką a komputerem, po czym zaimportuj plik ponownie.</p>

Powiązane informacje

➔ [„Informacje o certyfikatach cyfrowych” na stronie 96](#)

Plik z certyfikatem podpisanym przez urząd certyfikacji został omyłkowo usunięty

Nie ma kopii zapasowej certyfikatu podpisanego przez urząd certyfikacji.

Jeśli dostępny jest plik kopii zapasowej, zaimportuj certyfikat ponownie.

W przypadku uzyskania certyfikatu na podstawie żądania CSR utworzonego za pomocą aplikacji Web Config nie można ponownie zaimportować usuniętego certyfikatu. Utwórz żądanie CSR i uzyskaj nowy certyfikat.

Powiązane informacje

➔ [„Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 98](#)

➔ [„Usuwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 100](#)

Korzystanie z funkcji Epson Open Platform

Opis platformy Epson Open Platform.125

Konfigurowanie platformy Epson Open Platform. 125

Weryfikacja platformy Epson Open Platform. 125

Opis platformy Epson Open Platform

Epson Open Platform jest platformą umożliwiającą używanie systemów uwierzytelniających do uwierzytelniania użytkowników na tym skanerze.

Platforma współpracuje z oprogramowaniem Epson Print Admin (system uwierzytelniający firmy Epson) lub systemem uwierzytelniającym innej firmy. Można pobierać dzienniki na poziomie urządzenia i użytkownika, konfigurować urządzenia dostępne dla użytkowników i grup, a także ograniczać dostępne funkcje i nie tylko.

Podłączając urządzenie uwierzytelniające, można też wykonywać uwierzytelnianie użytkowników za pomocą kart identyfikacyjnych.

Konfigurowanie platformy Epson Open Platform

Włącz funkcję Epson Open Platform, aby móc używać urządzenia z poziomu systemu uwierzytelniania.

1. Uzyskaj klucz produktu z dedykowanej witryny.
Więcej informacji o uzyskiwaniu klucza produktu można znaleźć w podręczniku Epson Open Platform.
2. Otwórz aplikację Web Config, a następnie wybierz pozycje **Epson Open Platform > Klucz produktu lub Klucz licencyjny**.
3. Sprawdź każdą pozycję i ustaw ją.
 - Numer seryjny
Zostanie wyświetlony numer seryjny urządzenia.
 - Wersja Epson Open Platform
Wybierz wersję platformy Epson Open Platform. Odpowiednia wersja zależy od systemu uwierzytelniania.
 - Klucz produktu lub Klucz licencyjny
Wprowadź uzyskany klucz produktu.
4. Kliknij pozycję **Dalej**.
Zostanie wyświetlony ekran potwierdzenia ustawień.
5. Kliknij przycisk **OK**.
Ustawienia zostały zastosowane do skanera.

Uwaga:

Kiedy system jest zsynchronizowany z platformą Epson Open Platform, nie można używać rozwiązania Epson Print Admin Serverless.

Weryfikacja platformy Epson Open Platform

Można sprawdzić poprawność działania platformy Epson Open Platform przy użyciu dowolnej z następujących metod.

Web Config

Klucz produktu został wprowadzony na karcie **Epson Open Platform > Klucz produktu lub Klucz licencyjny > Klucz produktu lub Klucz licencyjny**, a karta **Epson Open Platform > System uwierzytelniania** jest wyświetlana w menu po lewej stronie.

Panel sterowania skanera

Sprawdź, czy klucz produktu jest wyświetlany w obszarze **Ustaw. > Dane urządzenia > Informacje o Epson Open Platform**.

Mocowanie urządzenia uwierzytelniającego

Podłączenie urządzenia uwierzytelniającego.	128
Sprawdzenie działania urządzenia uwierzytelniającego.	128
Potwierdzanie rozpoznania karty uwierzytelniającej.	128
Rozwiązywanie problemów związanych z urządzeniem uwierzytelniającym.	129

Podłączenie urządzenia uwierzytelniającego

Uwaga:

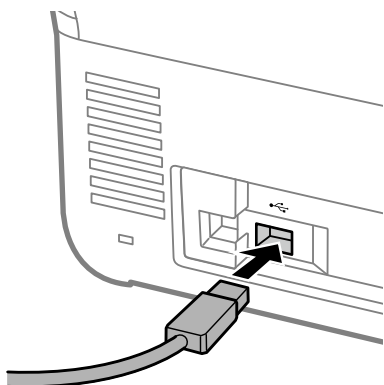
Urządzenia uwierzytelniającego używa się podczas korzystania z systemu uwierzytelniającego.



Ważne:

W przypadku podłączania urządzenia uwierzytelniającego do wielu skanerów należy używać produktu o takim samym numerze modelu.

Kabel USB od czytnika kart podłącz do portu do podłączenia zewnętrznego interfejsu kablem USB na skanerze.



Sprawdzenie działania urządzenia uwierzytelniającego

Stan połączenia i rozpoznawanie karty uwierzytelniającej do urządzenia uwierzytelniającego można sprawdzić z poziomu panelu sterowania skanera.

Informacje będą wyświetlane, jeśli zostaną wybrane pozycje **Ustaw.** > **Dane urządzenia** > **Stan urządzenia uwierzytelniającego.**

Potwierdzanie rozpoznania karty uwierzytelniającej

Można sprawdzić, czy karty uwierzytelniające są rozpoznawane, używając w tym celu aplikacji Web Config.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Zarządzanie urządzeniem** > **Czytnik kart.**
2. Przytrzymaj kartę nad czytnikiem kart uwierzytelniających.
3. Kliknij pozycję **Sprawdź.**
Zostaną wyświetlone wyniki.

Rozwiązywanie problemów związanych z urządzeniem uwierzytelniającym

Nie można odczytać karty uwierzytelniającej

Zastosuj się do poniższych rozwiązań.

- Sprawdź, czy urządzenie uwierzytelniające jest prawidłowo podłączone do skanera.
Podłącz urządzenie uwierzytelniające do portu do podłączenia zewnętrznego interfejsu kablem USB z tyłu skanera.
- Sprawdź, czy urządzenie uwierzytelniające i karta uwierzytelniająca mają certyfikat.
Skontaktuj się z dostawcą w celu uzyskania informacji o obsługiwanych urządzeniach i kartach uwierzytelniających.

Konserwacja

Czyszczenie zewnętrznej części skanera.	131
Czyszczenie wnętrza skanera.	131
Wymiana zestawu montażowego rolek.	136
Zerowanie liczby wykonanych skanów po wymianie wałków.	141
Oszczędzanie energii.	142
Przenoszenie skanera.	142
Tworzenie kopii zapasowej ustawień.	143
Przywr. ust. domyśl.	144
Aktualizacja aplikacji i oprogramowania sprzętowego.	145


Czyszczenie zewnętrznej części skanera

Wszelkie plamy na obudowie zewnętrznej wycierać suchą ściereczką lub szmatką zwilżoną wodą z dodatkiem łagodnego środka myjącego.



Ważne:

- Do czyszczenia skanera nigdy nie należy używać alkoholu, rozcieńczalnika ani żadnego rozpuszczalnika powodującego korozję. Używanie takich substancji może spowodować deformację lub odbarwienie urządzenia.
- Nie dopuścić, żeby do środka dostała się woda. Mogłoby to doprowadzić do wadliwego działania urządzenia.
- Nigdy nie należy otwierać obudowy skanera.

1. Naciśnij przycisk , aby wyłączyć skaner.
2. Odłącz zasilacz AC od skanera.
3. Oczyść obudowę zewnętrzną szmatką zwilżoną łagodnym detergentem i wodą.

Uwaga:

Przetrzeć ekran dotykowy miękką, suchą szmatką.

Czyszczenie wnętrza skanera

Po pewnym czasie użytkowania skanera można zauważyć, że na rolkach lub szklanej części wewnątrz urządzenia gromadzi się kurz z papieru i pomieszczenia, który może spowodować problemy z podawaniem papieru lub jakością zeskanowanych obrazów. Czyścić wnętrze skanera co 5,000 skanów.


Bieżącą liczbę skanów można sprawdzić na panelu sterowania lub w aplikacji Epson Scan 2 Utility.

Jeżeli na powierzchni są zabrudzenia trudne do usunięcia, należy użyć oryginalnego zestawu czyszczącego firmy Epson. Aby usunąć plamy, na szmatkę nałożyć małą ilość środka czyszczącego.

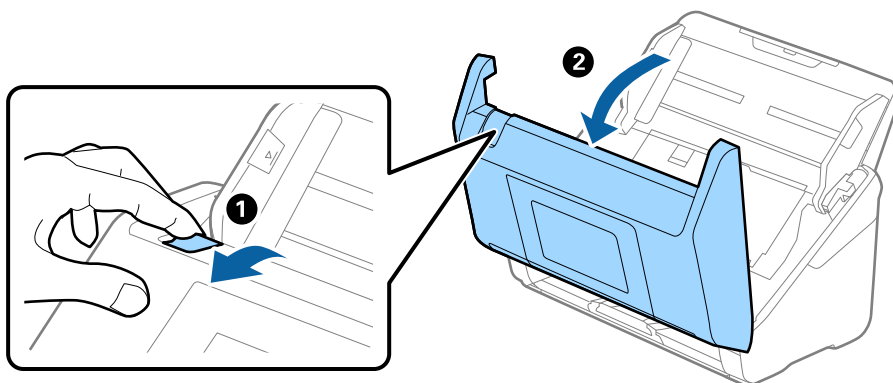


Ważne:

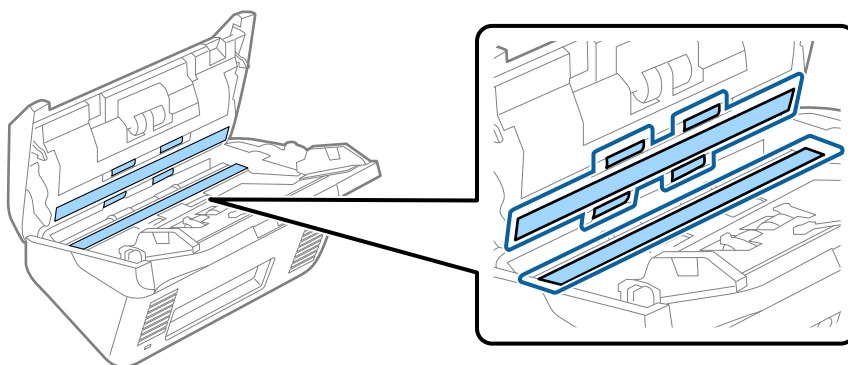
- Do czyszczenia skanera nigdy nie należy używać alkoholu, rozcieńczalnika ani żadnego rozpuszczalnika powodującego korozję. Używanie takich substancji może spowodować deformację lub odbarwienie urządzenia.
- Pod żadnym pozorem nie spryskiwać skanera jakimkolwiek płynem lub smarem. Może to doprowadzić do uszkodzenia urządzenia i obwodów, a następnie jego nieprawidłowego funkcjonowania.
- Nigdy nie należy otwierać obudowy skanera.

1. Naciśnij przycisk , aby wyłączyć skaner.
2. Odłącz zasilacz AC od skanera.

3. Pociągnij dźwignię i otwórz pokrywę skanera.



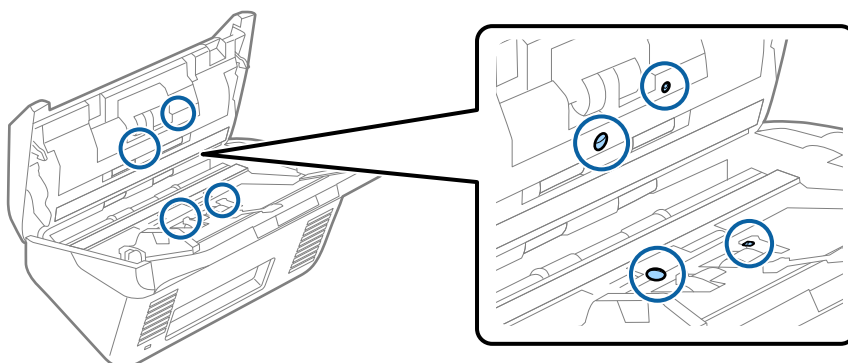
4. Wytrzyj wszelkie plamy na rolce z tworzywa (cztery miejsca) i szybie skanera na dole wewnątrz pokrywy skanera. Przetrzyj miękką i wilgotną szmatką niezostawiającą kłaczek z niewielkim dodatkiem środka czyszczącego lub wody.



Ważne:

- Nie należy przykładać zbyt dużej siły do szyby skanera.
- Nie używać szczotki ani twardego narzędzia. Jakikolwiek zarysowania na szybie mogą pogorszyć jakość skanów.
- Nie należy rozpylać środków do czyszczenia bezpośrednio na szybę skanera.

5. Wszelkie plamy na czujnikach wycierać bawełnianym wacikiem.



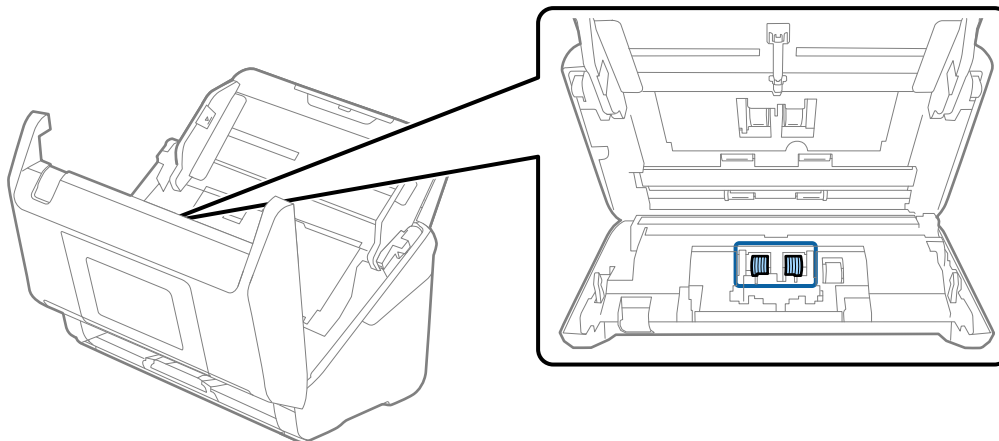


Ważne:

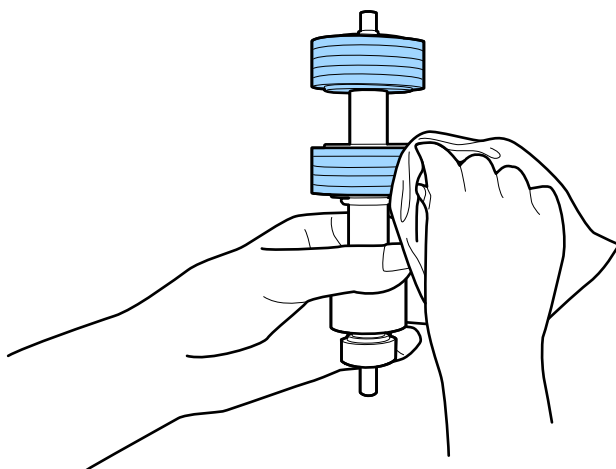
Wacika nie nasączać cieczeniami np. płynem czyszczącym.

6. Zdjąć pokrywę, a następnie wyjąć rolkę rozdzielającą.

Więcej szczegółów znajduje się w części „Wymiana zestawu montażowego rolki”.



7. Przetrzyj wałek rozdzielający. Przetrzyj miękką i wilgotną szmatką niezostawiającą kłaczek z niewielkim dodatkiem środka czyszczącego lub wody.

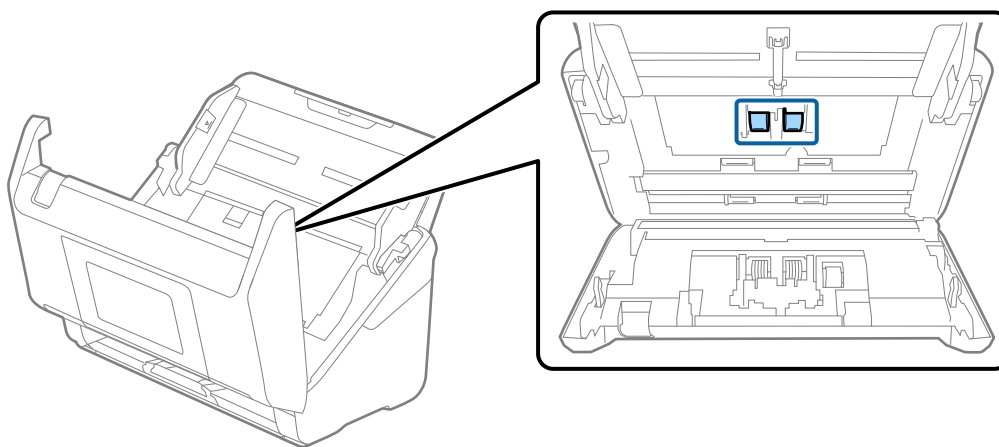


Ważne:

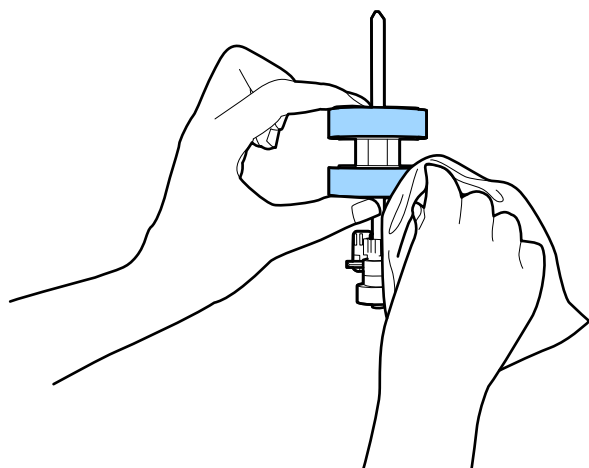
Do czyszczenia rolki używać tylko oryginalnego zestawu czyszczącego firmy Epson lub miękkiej, wilgotnej szmatki. Sucha szmatka może spowodować uszkodzenie powierzchni rolki.

8. Zdjąć pokrywę, a następnie wyjąć rolkę podającą.

Więcej szczegółów znajduje się w części „Wymiana zestawu montażowego rolki”.



9. Przetrzyj wałek odbierający. Przetrzyj miękką i wilgotną szmatką niezostawiającą kłaczek z niewielkim dodatkiem środka czyszczącego lub wody.

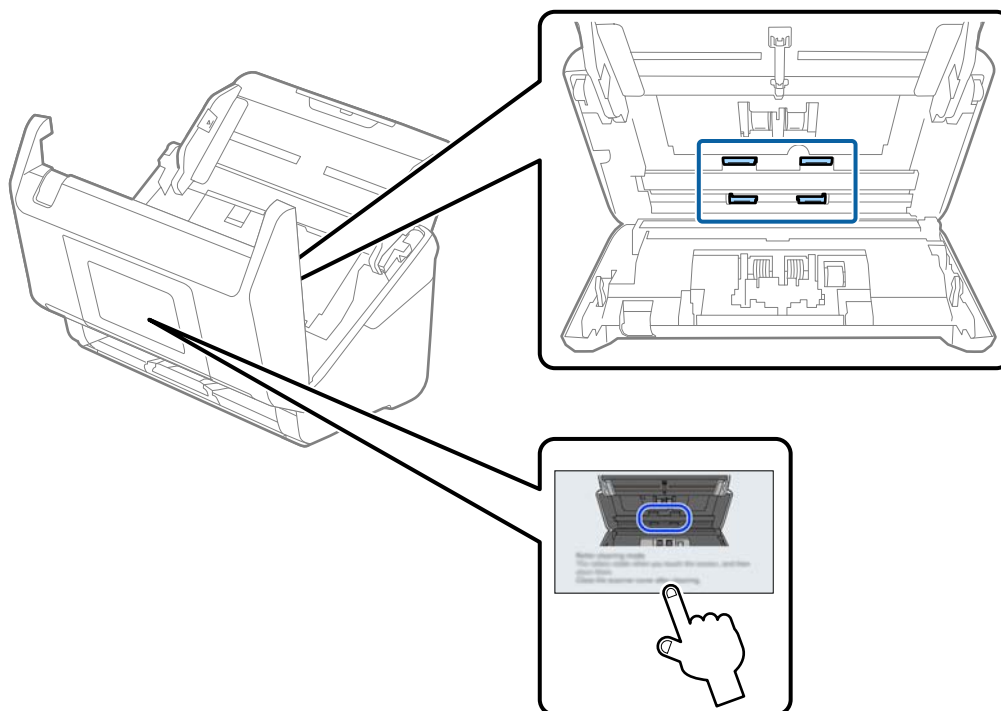


Ważne:

Do czyszczenia rolki używać tylko oryginalnego zestawu czyszczącego firmy Epson lub miękkiej, wilgotnej szmatki. Sucha szmatka może spowodować uszkodzenie powierzchni rolki.

10. Zamknij pokrywę skanera.
11. Podłącz wtyczkę zasilacza AC do gniazda elektrycznego, a następnie włącz skaner.
12. Na ekranie głównym wybierz pozycję **Konserwacja skanera**.
13. Na ekranie **Konserwacja skanera** wybrać pozycję **Czyszczenie rolek**.
14. Pociągnąć dźwignię, aby otworzyć pokrywę skanera.
Skaner zostanie przełączony w tryb czyszczenia rolek.

15. Powoli obracać rolki na dole, dotykając dowolnego miejsca ekranu LCD. Przetrzeć powierzchnię rolek, używając oryginalnego zestawu czyszczącego firmy Epson lub miękkiej szmatki zwilżonej wodą. Powtarzać, aż rolki będą czyste.



Przeostroga:

Podczas obracania rolek zachować ostrożność, aby nie pochwycić nimi dłoni ani włosów. Mogłoby to doprowadzić to obrażeń ciała.

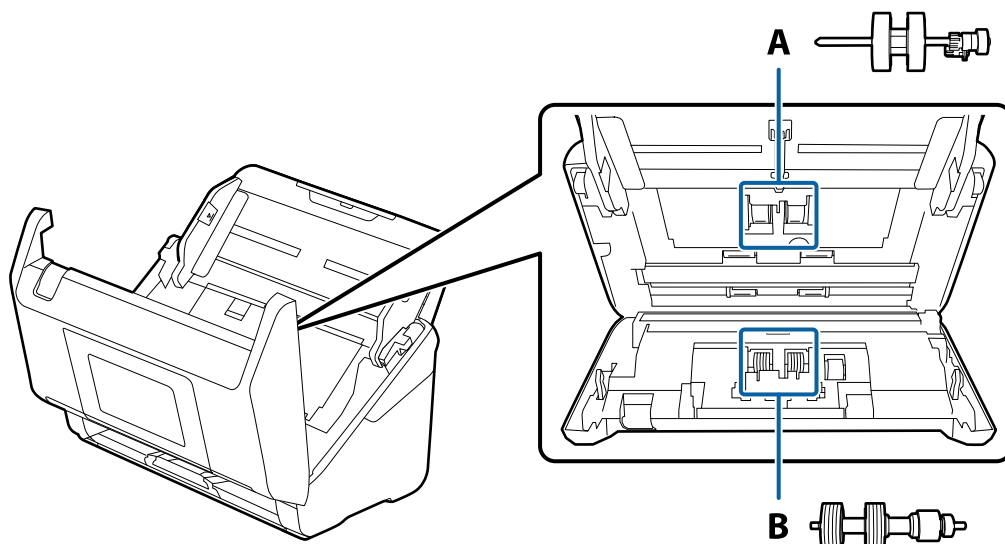
16. Zamknij pokrywę skanera.
Tryb czyszczenia rolek zostanie wyłączony.

Powiązane informacje


➔ „Wymiana zestawu montażowego rolek” na stronie 136

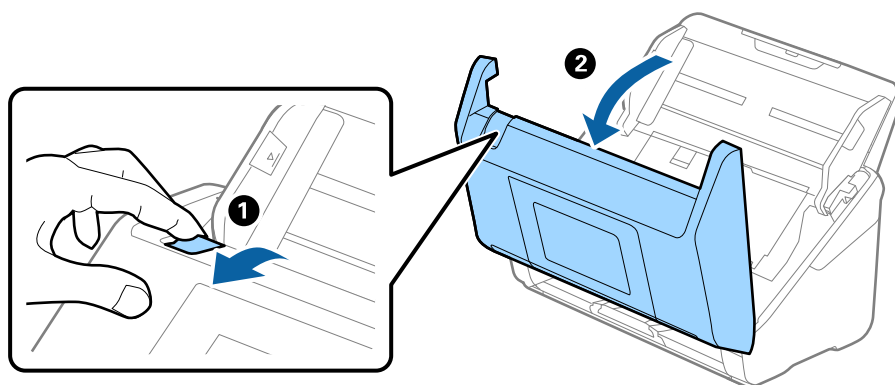
Wymiana zestawu montażowego rolek

Zestaw montażowy rolek (wałek odbierający i wałek rozdzielający) należy wymienić po tym, jak liczba skanów przekroczy wartość określoną dla cyklu eksploatacji rolek. Po wyświetleniu na panelu sterowania lub na ekranie komputera komunikatu o konieczności ich wymiany wykonać podane niżej czynności.

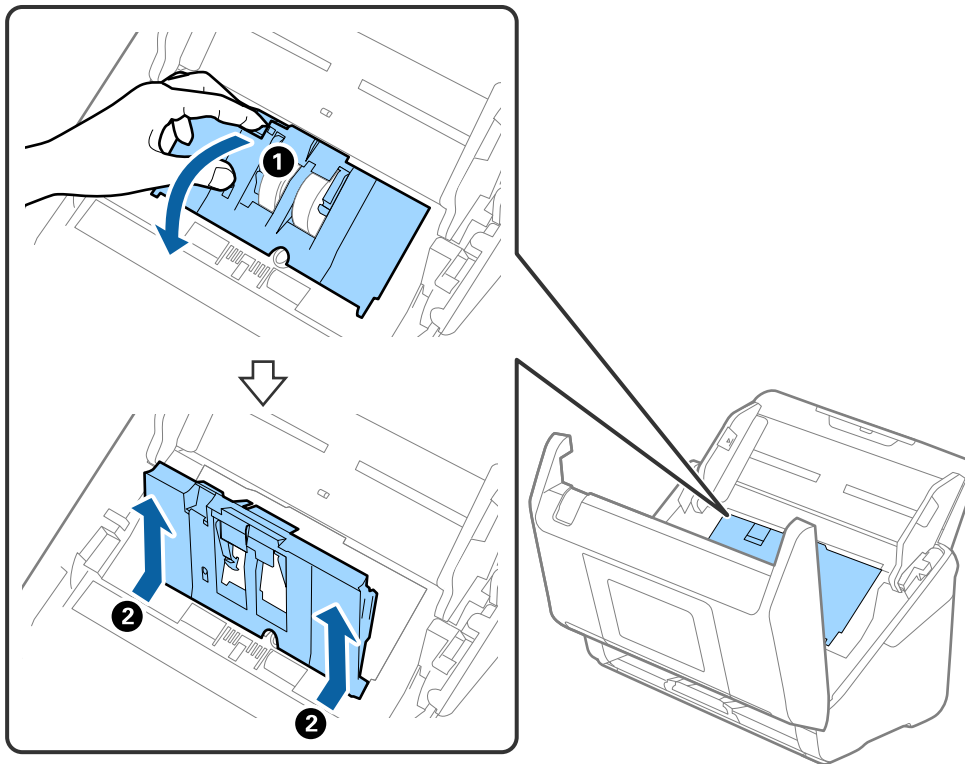


A: wałek odbierający, B: wałek rozdzielający

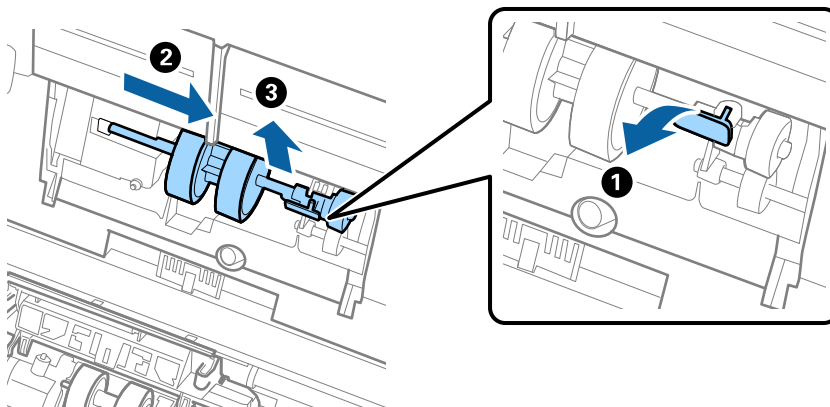
1. Naciśnij przycisk , aby wyłączyć skanera.
2. Odłącz zasilacz AC od skanera.
3. Pociągnij dźwignię i otwórz pokrywę skanera.



4. Otwórz pokrywę rolki podającej, a następnie wysuń ją i wyjmij.



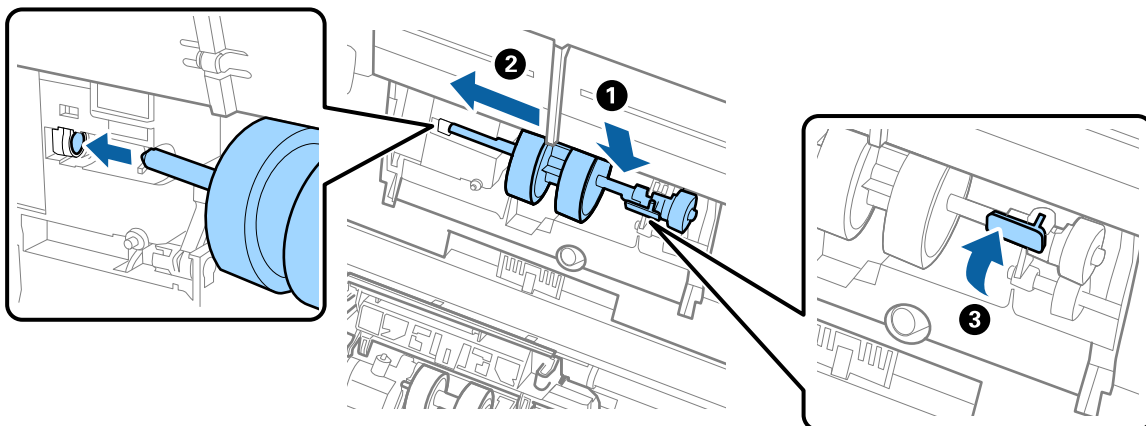
5. Pociągnij w dół osprzęt osi rolki, a następnie wysuń i wyjmij zainstalowane rolki podające.



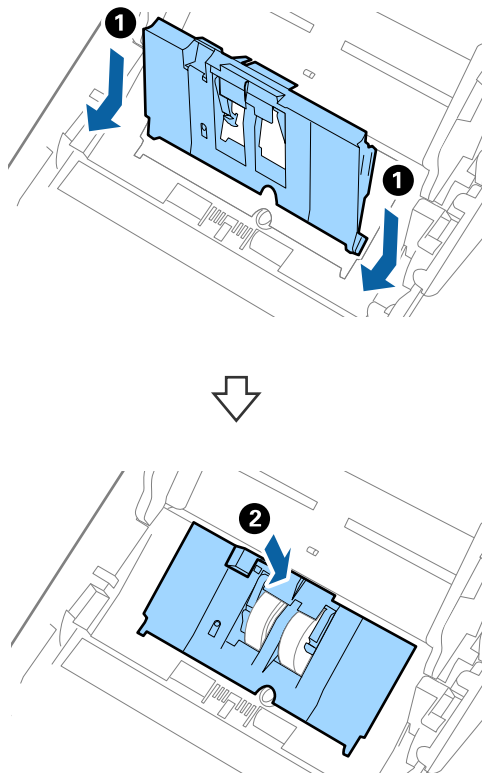
Ważne:

Nie używać dużej siły w celu wysunięcia rolki podającej. Mogłoby to uszkodzić wnętrze skanera.

6. Przytrzymując osprzęt, przesun w lewą stronę nowy wałek odbierający i umieść go w otworze skanera. Dociśnij osprzęt w celu jego zabezpieczenia.

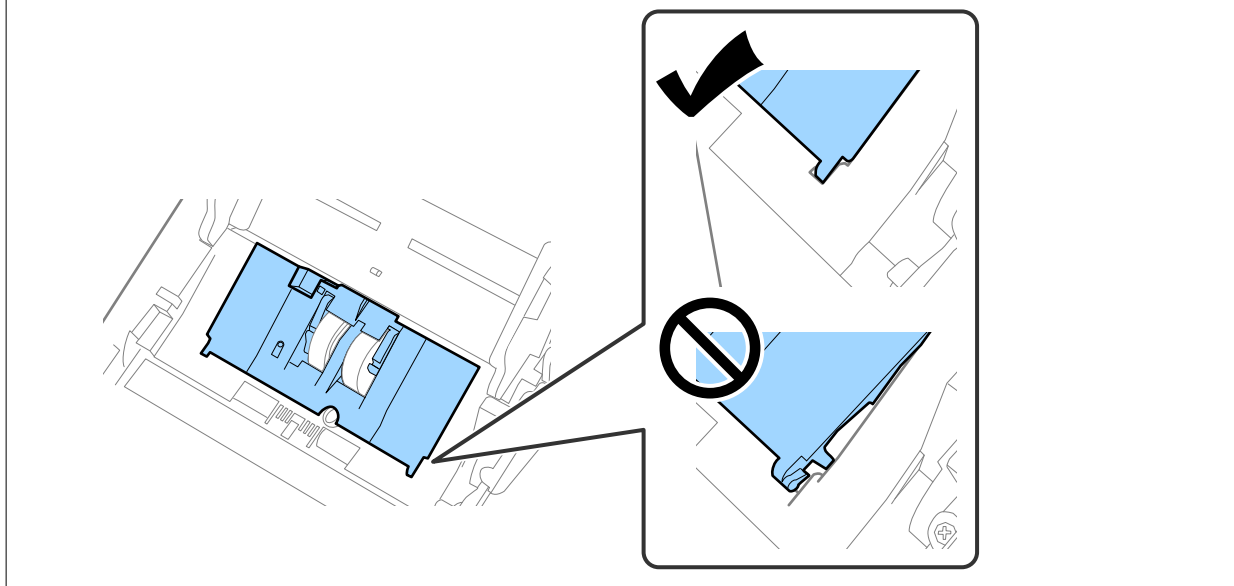


7. Umieść krawędź pokrywy rolki podającej w szczelinie i wsun ją. Dokładnie zamknij pokrywę.

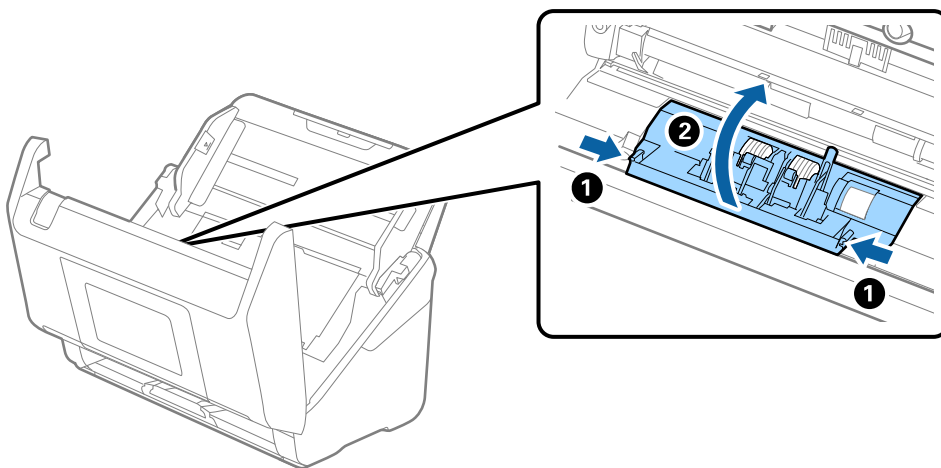


! **Ważne:**

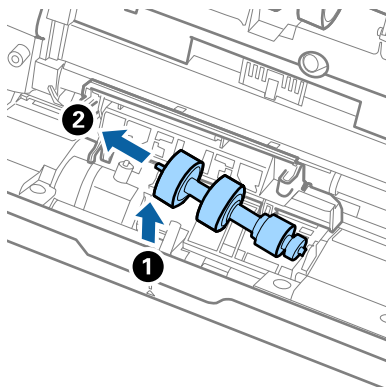
- Upewnij się, czy pokrywa rolki odbierającej jest zamknięta.
- Jeżeli pokrywa trudno się domyka, sprawdź poprawność zainstalowania rolek podających.
- Nie instaluj pokrywy, kiedy jest podniesiona.



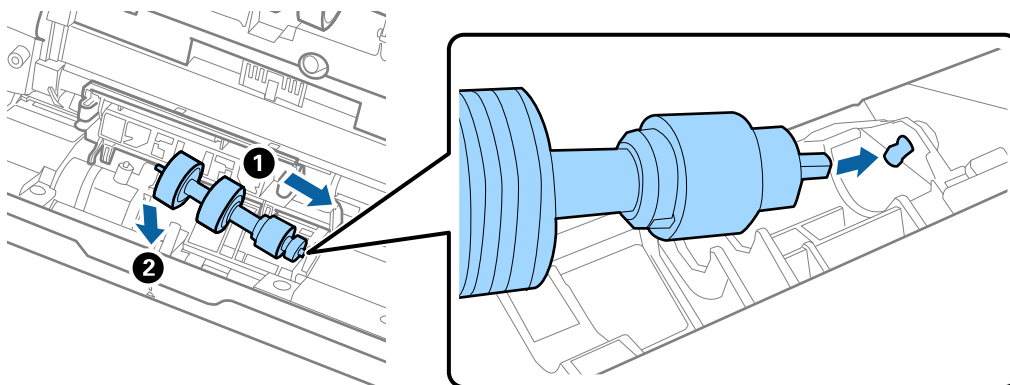
8. Popchnij zaczepy na obu końcach pokrywy wałka rozdzielającego w celu jego otwarcia.



9. Podnieś lewą stronę wałka rozdzielającego, a następnie wysuń i wyjmij zainstalowane wałki rozdzielające.



10. Umieść oś nowej rolki rozdzielającej w otworze po prawej stronie, a następnie opuść rolkę.



11. Zamknij pokrywę rolki rozdzielającej.



Ważne:

Jeżeli pokrywa trudno się domyka, sprawdzić poprawność zainstalowania rolek rozdzielających.

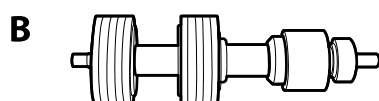
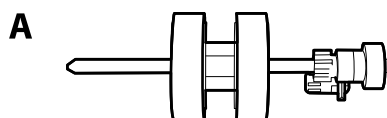
12. Zamknąć pokrywę skanera.
13. Podłączyć wtyczkę zasilacza AC do gniazda elektrycznego, a następnie włączyć skaner.
14. Wyzeruj liczbę skanów na panelu sterowania.

Uwaga:

Zutylizuj wałek odbierający i wałek rozdzielający zgodnie z lokalnie obowiązującymi zasadami i przepisami. Nie wolno ich remontować.

Kody zestawu montażowego rolek

Części (rolkę podającą i rolkę rozdzielającą) powinno się wymienić, kiedy liczba skanów przekroczy liczbę określoną w zasadach konserwacji. Bieżącą liczbę skanów można sprawdzić na panelu sterowania lub w aplikacji Epson Scan 2 Utility.



A: rolka podająca, B: rolka rozdzielająca

Nazwa części	Kody	Cykl eksploatacji
Zestaw montażowy rolek 2	B12B819711 B12B819721 (tylko Indie)	200,000*

* Liczbę tę osiągnięto kolejno w trakcie skanowania z użyciem oryginalnego papieru testowego firmy Epson i służy ona jako wskazówka w odniesieniu do cyklu wymiany. Cykl wymiany może różnić się w zależności od typów papieru np. takiego, który wytwarza dużo kurzu lub papieru z chropowatą powierzchnią, który może skrócić cykl eksploatacji.

Zerowanie liczby wykonanych skanów po wymianie wałków

Po wymianie zestawu montażowego rolki należy wyzerować liczbę skanów z poziomu panelu sterowania lub aplikacji Epson Scan 2 Utility.

W tym rozdziale opisano zerowanie za pomocą panelu sterowania.

1. Na ekranie głównym dotknij pozycji **Konserwacja skanera**.
2. Dotknij pozycji **Wymiana rolki**.
3. Dotknij pozycji **Resetuj liczbę skanowań**.
4. Wybierz przycisk **Liczba skanów po wymianie rolki**, a następnie dotknij przycisku **Tak**.

Uwaga:

Aby wyzerować z poziomu aplikacji Epson Scan 2 Utility, uruchom aplikację Epson Scan 2 Utility, kliknij kartę **Licznik**, a następnie w obszarze **Zestaw montażowy** kliknij pozycję **Resetuj**.

Powiązane informacje

➔ [„Wymiana zestawu montażowego rolek” na stronie 136](#)

Oszczędzanie energii

Kiedy skaner nie wykonuje żadnych czynności, można oszczędzać energię poprzez skorzystanie z trybu wstrzymania lub automatycznego wyłączenia. Można ustawić okres czasu, po którym skaner przejdzie w tryb wstrzymania lub wyłączy się automatycznie. Jakikolwiek zwiększenie będzie miało wpływ na wydajność energetyczną produktu. Przed dokonaniem zmian w ustawieniu weź pod uwagę kwestie środowiskowe.


1. Na ekranie głównym wybierz pozycję **Ustaw.**
2. Wybierz pozycję **Ustaw. podstawowe**.
3. Wybierz **Timer uśpienia** lub **Ustaw. wyłączenia**, a następnie skonfiguruj ustawienia.

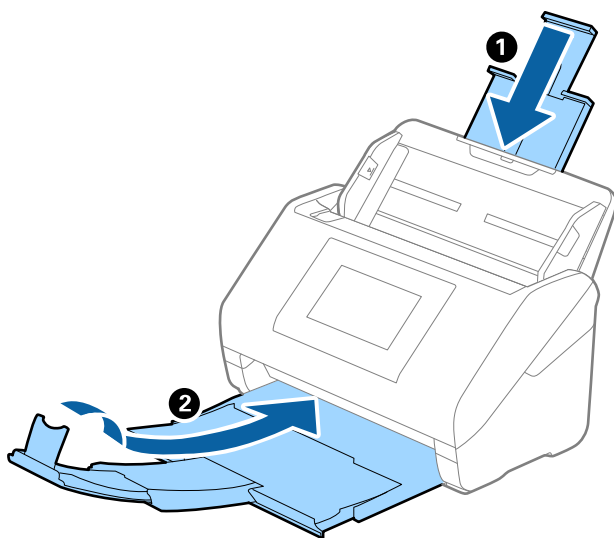
Uwaga:

Dostępne funkcje mogą się różnić w zależności od miejsca zakupu.

Przenoszenie skanera

Na potrzeby przewiezienia skanera podczas przeprowadzki lub do naprawy zapakować go, wykonując niżej podane czynności.

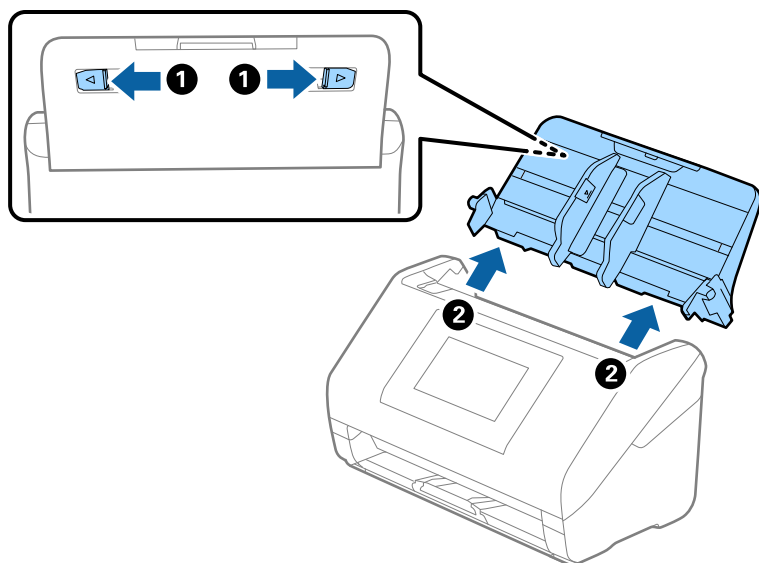
1. Nacisnąć przycisk  w celu wyłączenia skanera.
2. Odłączyć zasilacz AC.
3. Odłączyć kable i zdjąć urządzenia.
Zdjąć opcjonalną lub dostarczoną Paper Alignment Plate, jeśli jest zamocowana.
4. Zamknąć przedłużenie podajnika wejściowego i podajnik wyjściowy.



Ważne:

Sprawdzić, czy zasobnik wyjściowy jest właściwie zamknięty, ponieważ w przeciwnym razie może ulec uszkodzeniu podczas transportu.

5. Zdjąć podajnik wejściowy.



6. Obłóżyć skaner materiałami pakunkowymi, z którymi został dostarczony, a następnie umieścić urządzenie w oryginalnym lub wytrzymałym pudle.

Tworzenie kopii zapasowej ustawień

Można wyeksportować zestaw wartości ustawień z aplikacji Web Config do pliku. Funkcji tej można używać do tworzenia kopii zapasowej kontaktów, wartości ustawień, w przypadku wymiany skanera itd.

Wyeksportowanego pliku nie można edytować, ponieważ jest to plik binarny.

Eksport ustawień

Możliwe jest eksportowanie ustawień skanera.

1. Otwórz aplikację Web Config i wybierz pozycję **Zarządzanie urządzeniem > Wartość ustawienia Eksportuj i Importuj > Eksportuj**.

2. Wybierz ustawienia, które chcesz wyeksportować.

Wybierz ustawienia, które chcesz wyeksportować. Po wybraniu kategorii nadrzędnej podkategorie zostają również wybrane. Nie można jednak wybrać podkategorii powodujących błędy powielenia w obrębie tej samej sieci (jak adresy IP itp.).

3. Wprowadź hasło, aby zaszyfrować wyeksportowany plik.

Hasło będzie potrzebne do zaimportowania pliku. Pozostawić to pole puste, aby zrezygnować z szyfrowania pliku.

4. Kliknij przycisk **Eksportuj**.



Ważne:

Aby wyeksportować ustawienia sieciowe skanera, jak nazwa urządzenia i adres IPv6, zaznacz opcję **Włącz wybór indywidualnych ustawień urządzenia** i wybierz dodatkowe pozycje. Wybranych wartości należy używać tylko w przypadku skanera zastępczego.

Powiązane informacje

- ➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Importowanie ustawień

Plik wyeksportowany z aplikacji Web Config można zaimportować na skanerze.



Ważne:

Podczas importowania wartości zawierających poszczególne informacje, takie jak nazwa skanera lub adres IP, sprawdź, czy w tej samej sieci nie ma takiego samego adresu IP.

1. Uzyskaj dostęp do aplikacji Web Config, a następnie wybierz pozycje **Zarządzanie urządzeniem > Wartość ustawienia Eksportuj i Importuj > Importuj**.
2. Wybierz wyeksportowany plik, a następnie wprowadź hasło szyfrowania.
3. Kliknij przycisk **Dalej**.
4. Wybierz ustawienia, które mają być importowane, a następnie kliknij przycisk **Dalej**.
5. Kliknij przycisk **OK**.

Ustawienia zostały zastosowane do skanera.

Powiązane informacje

- ➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Przywr. ust. domyśl.

Na panelu sterowania wybierz pozycje **Ustaw. > Administr. systemu > Przywr. ust. domyśl.**, a następnie wybierz pozycje, które mają być przywrócone do wartości domyślnych.

- Ustawienia sieciowe: przywracanie wartości domyślnych ustawień sieciowych.
- Wszystkie poza ustawieniami sieciowymi: przywracanie wartości domyślnych ustawień innych niż ustawienia sieciowe.
- Wszystkie ustawienia: przywracanie wartości domyślnych wszystkich ustawień.



Ważne:

Jeśli zostanie wybrane ustawienie **Wszystkie ustawienia**, wszystkie dane ustawień zarejestrowane w skanerze, w tym kontakty, zostaną usunięte. Usuniętych ustawień nie można przywrócić.

Uwaga:

Ustawienia można też konfigurować w aplikacji Web Config.

Karta **Zarządzanie urządzeniem** > **Przywr. ust. domyśl.**

Aktualizacja aplikacji i oprogramowania sprzętowego

Aktualizując aplikacje i oprogramowanie sprzętowe, można rozwiązać pewne problemy, poprawić działanie programów albo dodać funkcje. Użytkownik powinien upewnić się, że korzysta z najnowszych wersji aplikacji i oprogramowania sprzętowego.



Ważne:

Podczas aktualizacji oprogramowania nie należy wyłączać komputera ani skanera.

Uwaga:

Jeśli skaner można połączyć z Internetem, oprogramowanie układowe można zaktualizować za pośrednictwem aplikacji Web Config. Wybierz pozycję **Zarządzanie urządzeniem** > **Aktualizacja oprogramowania sprzętowego**, zapoznaj się z wyświetlonym komunikatem, a następnie kliknij przycisk **Start**.

1. Użytkownik powinien upewnić się, że skaner i komputer są połączone i że komputer jest podłączony do Internetu.
2. Uruchomić aplikację EPSON Software Updater i zaktualizować aplikacje lub oprogramowanie sprzętowe.

Uwaga:

Nie są obsługiwane systemy operacyjne Windows Server.

Windows 11

Kliknąć przycisk Start, a następnie wybrać polecenia **Wszystkie aplikacje** > **Epson Software** > **EPSON Software Updater**.

Windows 10

Kliknąć przycisk Start, a następnie wybrać polecenia **Epson Software** > **EPSON Software Updater**.

Windows 8.1/Windows 8

Wprowadzić nazwę aplikacji w panelu wyszukiwania, po czym wybrać wyświetloną ikonę.

Windows 7

Kliknąć przycisk Start, a następnie wybrać polecenia **Wszystkie programy** lub **Programy** > **Epson Software** > **EPSON Software Updater**.

Mac OS

Wybrać polecenia **Finder** > **Idź** > **Aplikacje** > **Epson Software** > **EPSON Software Updater**.

Uwaga:

Jeżeli na liście aplikacji nie możesz znaleźć aplikacji, którą chcesz zaktualizować, nie będzie można jej zaktualizować za pomocą programu EPSON Software Updater. Sprawdź na lokalnym portalu Epson, czy są dostępne najnowsze wersje aplikacji.

<http://www.epson.com>

Aktualizowanie oprogramowania układowego skanera za pomocą panelu sterowania


Jeśli skaner ma połączenie z Internetem, oprogramowanie układowe skanera można zaktualizować przy użyciu panelu sterowania. Można również ustawić skaner tak, aby włączyć regularne sprawdzanie dostępności aktualizacji oprogramowania układowego i powiadamianie o dostępności takich aktualizacji.

1. Na ekranie głównym wybierz pozycję **Ustaw.**
2. Wybrać pozycje **Administr. systemu > Aktualizacja oprogramowania > Aktualizuj.**

Uwaga:

Wybierz pozycje **Powiadomienie > Wł.**, aby włączyć na skanerze regularne sprawdzanie dostępności aktualizacji oprogramowania układowego.

3. Zapoznaj się z komunikatem wyświetlanym na ekranie i rozpocznij wyszukiwanie dostępnych aktualizacji.
4. Jeżeli na ekranie LCD wyświetli się komunikat informujący o dostępności aktualizacji oprogramowania układowego, zastosuj się do instrukcji na ekranie, aby rozpocząć aktualizację.

 **Ważne:**

- Nie wolno wyłączać ani odłączać skanera od źródła zasilania do momentu zakończenia aktualizacji, gdyż w przeciwnym razie skaner może ulec awarii.
- Jeżeli aktualizacja oprogramowania układowego nie zostanie zakończona lub nie zostanie przeprowadzona pomyślnie, skaner nie uruchomi się normalnie i przy następnym włączeniu na ekranie będzie wyświetlany komunikat „Recovery Mode”. W takiej sytuacji trzeba ponownie zaktualizować oprogramowanie układowe przy pomocy komputera. Podłącz skaner do komputera przy użyciu przewodu USB. Gdy na skanerze wyświetlany jest komunikat „Recovery Mode”, nie można zaktualizować oprogramowania układowego za pośrednictwem połączenia sieciowego. Na komputerze otwórz lokalną witrynę internetową firmy Epson, a następnie pobierz najnowszą wersję oprogramowania układowego skanera. W instrukcjach w witrynie internetowej opisane zostały następane kroki.

Aktualizowanie oprogramowania układowego za pomocą narzędzia Web Config

Jeśli skaner można połączyć z Internetem, oprogramowanie układowe można zaktualizować za pośrednictwem aplikacji Web Config.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zarządzanie urządzeniem > Aktualizacja oprogramowania sprzętowego.**
2. Kliknij **Start**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zostanie wyświetlone potwierdzenie aktualizacji oprogramowania układowego, a także informacje o oprogramowaniu układowym, jeśli jest dostępna aktualizacja.

Uwaga:

Oprogramowanie układowe można też zaktualizować za pomocą programu Epson Device Admin. Informacje o oprogramowaniu układowym można sprawdzić na liście urządzenia. Jest to przydatne, jeżeli trzeba zaktualizować wiele urządzeń. Więcej informacji można znaleźć w dokumentacji lub pomocy narzędzia Epson Device Admin.

Powiązane informacje

➔ „Uruchamianie aplikacji Web Config w przeglądarce internetowej” na stronie 38

Aktualizowanie oprogramowania układowego bez nawiązywania połączenia z Internetem

Można pobrać oprogramowanie układowe urządzenia z witryny firmy Epson, zapisać je na komputerze, a następnie połączyć komputer z urządzeniem za pomocą kabla USB, aby zaktualizować oprogramowanie układowe. If you cannot update over the network, try this method.

Uwaga:

Przed przystąpieniem do aktualizacji upewnij się, czy sterownik skanera Epson Scan 2 jest zainstalowany na komputerze. Jeżeli aplikacja Epson Scan 2 nie jest zainstalowana, zainstaluj ją ponownie.

1. Sprawdź dostępność najnowszych aktualizacji oprogramowania układowego w witrynie firmy Epson.
<http://www.epson.com>
 - Jeśli dostępne jest oprogramowanie układowe dla posiadanego skanera, pobierz je i przejdź do następnego kroku.
 - Jeśli informacji o oprogramowaniu układowym nie ma w witrynie, oznacza to, że używana jest już najnowsza wersja.
2. Połącz komputer z pobranym oprogramowaniem układowym ze skanerem za pomocą kabla USB.
3. Kliknij dwukrotnie pobrany plik .exe.
Zostanie uruchomiony tryb Epson Firmware Updater.
4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.