EPSON
EXCEED YOUR VISION

DS-790WN

Przewodnik administratora

NPD6726-00 PL

Prawa autorskie

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

Znaki towarowe

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION i ich logo są zarejestrowanymi znakami towarowymi lub znakami towarowymi firmy Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa i PaSoRi są zastrzeżonymi znakami towarowymi firmy Sony Corporation.
- ❏ MIFARE jest zastrzeżonym znakiem towarowym firmy NXP Semiconductor Corporation.
- ❏ Uwaga ogólna: inne nazwy produktów użyte w niniejszym dokumencie służą wyłącznie celom identyfikacyjnym i mogą być znakami towarowymi należącymi do ich właścicieli. Firma Epson nie rości sobie żadnych praw do tych znaków.

Spis treści

Podstawowe ustawienia zabezpieczeń

Zaawansowane ustawienia bezpieczeństwa

Ustawienia uwierzytelniania

Konserwacja

Wprowadzenie

Zawartość tego dokumentu

W tym dokumencie przedstawiono następujące informacje dla administratorów skanera.

❏ Ustawienia sieciowe

❏ Przygotowywanie funkcji skanowania

❏ Włączanie i zarządzanie ustawieniami bezpieczeństwa

❏ Włączanie i zarządzanie Ustawienia uwierzytelniania

❏ Wykonywanie codziennej konserwacji

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

Uwaga:
W tym dokumencie opisano opcję Ustawienia uwierzytelniania, która umożliwia uwierzytelnianie użytkowników bez użycia serwera. Poza opcjami Ustawienia uwierzytelniania przedstawionymi w tym podręczniku można też stworzyć system uwierzytelniania wykorzystujący serwer uwierzytelniania. Użyj Document Capture Pro Server Authentication Edition (nazwa skrócona to Document Capture Pro Server AE), aby postawić taki system.

Więcej informacji można uzyskać, kontaktując się z lokalnym biurem firmy Epson.

Korzystanie z tej instrukcji

Oznaczenia i symbole

> ⚠ ***Przestroga:***
> *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

➡ Łącza 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

Użyte w niniejszej instrukcji nazwy „Windows 10", „Windows 8.1", „Windows 8", „Windows 7", „Windows Server 2019", „Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012" oraz „Windows Server 2008 R2" oznaczają odpowiednie systemy operacyjne. Dodatkowo „Windows" odnosi się do wszystkich wersji, a „Windows Server" odnosi się do wersji „Windows Server 2019", „Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012" i „Windows Server 2008 R2".

- ❏ 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® 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

Mac OS

W tej instrukcji obsługi termin „Mac OS" odnosi się do systemów macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan i OS X Yosemite.

Zalecane ustawienia przeznaczone do żądanego celu

Zalecane ustawienia przeznaczone do żądanego celu

Poniżej przedstawiono sposób konfigurowania ustawień stosownie do żądanego celu.

Łączenie skanera z siecią

Przeznaczenie	Wymagane ustawienia
Połączenie skanera z siecią.	Ustaw skaner do skanowania sieciowego. „Łączenie skanera z siecią" na stronie 14
Połączenie skanera z nowym komputerem.	Skonfiguruj ustawienia sieciowe skanera na nowym komputerze. „Dodawanie lub wymienianie komputera lub urządzeń" na stronie 20

Ustawienia skanowania

Przeznaczenie	Wymagane ustawienia
Wysyłanie zeskanowanych obrazów pocztą e-mail. (Skanowanie do wiadomości e-mail)	1. Skonfiguruj serwer poczty e-mail, który ma być używany. „Konfigurowanie serwera pocztowego" na stronie 42 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 63
Zapisywanie zeskanowanych obrazów w folderze sieciowym. (Skanowanie do folderu sieciowego/FTP)	1. Utwórz folder sieciowy, w którym mają być zapisywane obrazy. „Konfigurowanie folderu udostępnionego sieci" na stronie 45 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 63
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

Przeznaczenie	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 77

Konfigurowanie podstawowych funkcji bezpieczeństwa

Przeznaczenie	Wymagane ustawienia
Uniemożliwienie osobom innym niż administrator zmiany ustawień skanera.	Ustaw hasło administratora do skanera. „Ustawienia administratora" na stronie 86
Wyłączenie obsługi skanera przez port USB.	Wyłącz interfejs zewnętrzny. „Wyłączanie interfejsu zewnętrznego" na stronie 92

Konfigurowanie zaawansowanych funkcji bezpieczeństwa

Przeznaczenie	Wymagane ustawienia
Kontrolowanie używanych protokołów.	Włącz lub wyłącz poszczególne protokoły. „Kontrola użycia protokołów" na stronie 98
Szyfrowanie komunikacji.	1. Skonfiguruj certyfikat cyfrowy. „Używanie certyfikatu cyfrowego" na stronie 101 2. Skonfiguruj komunikację SSL/TLS. „Komunikacja SSL/TLS ze skanerem" na stronie 107
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 108
Używanie skanera w sieci IEEE802.1X.	Skonfiguruj sieć IEEE802.1X na skanerze. „Podłączanie skanera do sieci IEEE802.1X" na stronie 120

Konfigurowanie funkcji uwierzytelniania przez skaner

Przeznaczenie	Wymagane ustawienia
Włączanie opcji Ustawienia uwierzytelniania.	Więcej informacji o opcjach Ustawienia uwierzytelniania i Sposób uwierzytelniania można znaleźć w następującym rozdziale. „Informacje o opcji Ustawienia uwierzytelniania" na stronie 130 „Informacje o aplikacji Sposób uwierzytelniania" na stronie 131

Korzystanie z systemu uwierzytelniania serwera

Aplikacja Document Capture Pro Server Authentication Edition (skrót to Document Capture Pro Server AE) umożliwia stworzenie systemu uwierzytelniania, który wykorzystuje serwer do uwierzytelniania użytkowników.

Więcej informacji można uzyskać, kontaktując się z lokalnym biurem firmy Epson.

Ustawienia sieciowe

Łączenie skanera z siecią

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

Uwaga:
Jeżeli skaner i komputer są w tym samym segmencie sieci, można również je połączyć za pomocą programu instalacyjnego.

❏ *Konfigurowanie ze strony internetowej*

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

http://epson.sn

❏ *Konfigurowanie za pomocą dysku oprogramowania (tylko modele dostarczone z dyskiem z oprogramowaniem i użytkownicy komputerów Windows z napędami dysków).*

Umieść dysk oprogramowania w komputerze, a następnie postępuj zgodnie z instrukcjami na ekranie.

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	❏ Ethernet ❏ 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	❏ Adres IP ❏ Maska podsieci ❏ 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	❏ Identyfikator SSID ❏ 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 28

Wymiary	Elementy	Uwaga
Informacje o serwerze DNS	❏ Adres IP podstawowego serwera DNS ❏ 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.
Informacje o serwerze proxy	❏ Nazwa serwera proxy	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. W przypadku następujących funkcji skaner nawiązuje bezpośrednie połączenie z Internetem. ❏ Usługi Epson Connect ❏ Usługi chmury innych firm ❏ Aktualizacja oprogramowania układowego ❏ Wysyłanie zeskanowanych obrazów do usługi SharePoint (WebDAV)
Informacje o numerze portu	❏ Numer portu do rozgłoszenia	Sprawdź numer portu używany przez skaner i komputer, a następnie w razie potrzeby zezwól na ruch na tym porcie w konfiguracji zapory. Więcej informacji o portach używanych przez skaner można znaleźć w następującym rozdziale. „Używanie portów na skanerze” na stronie 30

Przydzielanie adresu IP

Poniżej przedstawiono następujące rodzaje przydzielania adresu IP.

Statyczny adres IP:

Ręczne przydzielania 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 pozycje **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 ruterze bezprzewodowym, takie jak SSID i hasło, są znane, można wprowadzić je ręcznie.

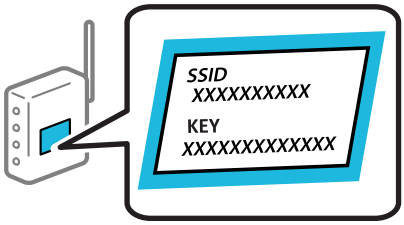
Jeżeli router bezprzewodowy obsługuje funkcję WPS, można skonfigurować ustawienia, naciskając odpowiedni przycisk.

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

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 haśle 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.*

Powiązane informacje

➡ „Sprawdzanie stanu połączenia sieciowego” na stronie 26

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 26

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 ruterze 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 26

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. Może on zostać uruchomiony po wykonaniu jednej z poniższych czynności.

❏ Konfiguracja ze strony internetowej

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

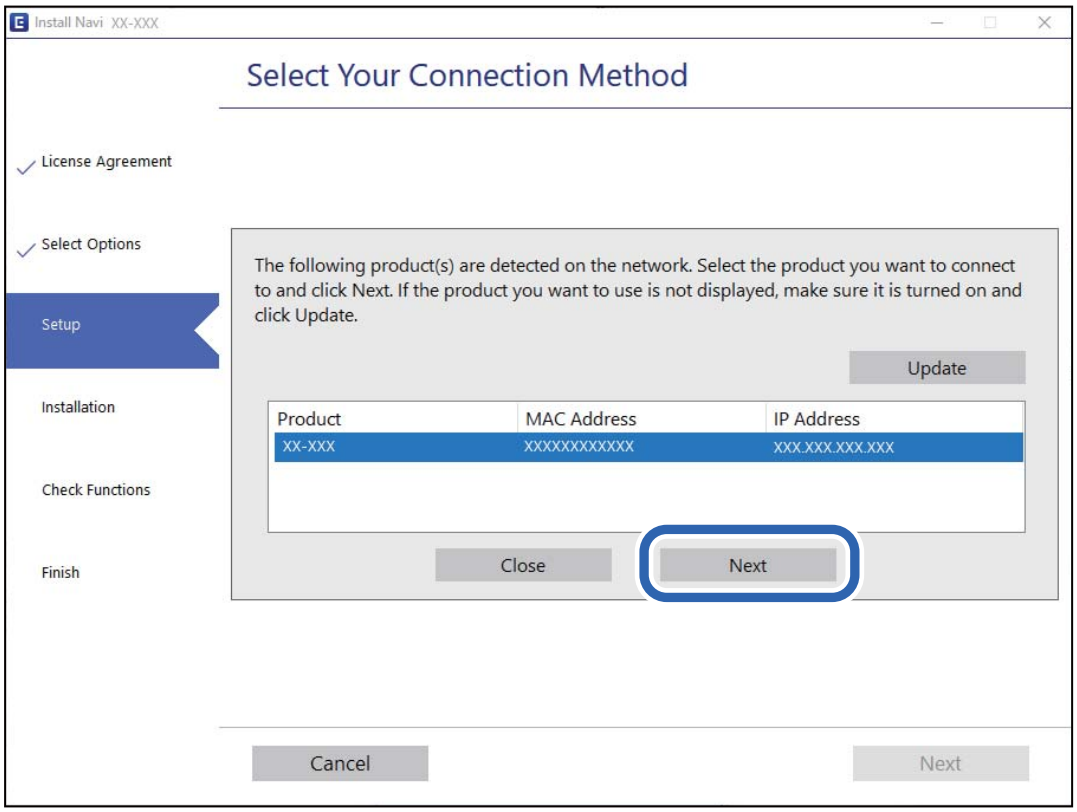
http://epson.sn

❏ Konfigurowanie za pomocą dysku oprogramowania (tylko modele dostarczone z dyskiem z oprogramowaniem i użytkownicy komputerów Windows z napędami dysków).

Umieść dysk oprogramowania w komputerze, a następnie postępuj zgodnie z instrukcjami na ekranie.

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 25

Połączenie przez Wi-Fi Direct

Podłącz urządzenie inteligentne do skanera bezpośrednio z pominięciem routera bezprzewodowego.

Przejdź poniżej w celu uzyskania szczegółowych informacji.

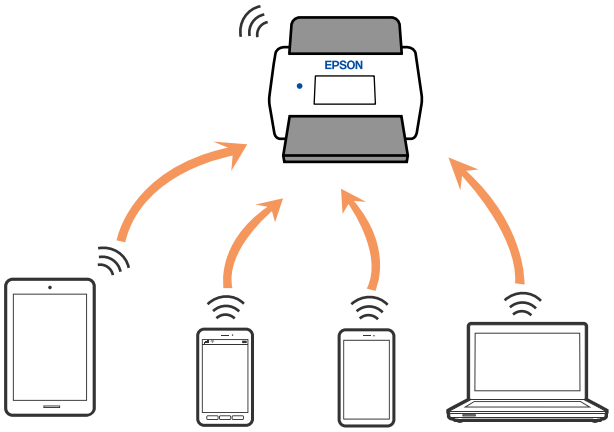
„Nawiązywanie bezpośredniego połączenia między urządzeniem inteligentnym a skanerem (Wi-Fi Direct)” na stronie 22

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

Funkcja Wi-Fi Direct (zwykłe 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 podłączenia 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 (zwykłe AP). Jednak jeżeli połączenie sieciowe zostanie rozpoczęte w trybie Wi-Fi Direct (zwykłe 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**.

3. Wybierz pozycję **Rozpocznij konfigurację**.
4. Na urządzeniu inteligentnym uruchom aplikację Epson Smart Panel.
5. 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.
6. Na panelu sterowania skanera wybierz pozycję **Zakończ**.

Rozłączanie połączenia Wi-Fi Direct (zwykłe AP)

Są dostępne dwa sposoby wyłączania połączenia Wi-Fi Direct (zwykłe 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 (zwykłe AP) zostanie wyłączone, wszystkie komputery i inteligentne urządzenia połączone ze skanerem przez połączenie Wi-Fi Direct (zwykłe 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 (zwykłe AP).

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

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

Po włączeniu połączenia Wi-Fi Direct (zwykłe AP) można zmienić jego ustawienia, wybierając pozycje  > **Wi-Fi Direct** > **Rozpocznij konfigurację** > **Zmień**, co spowoduje wyświetlenie następujących ustawień.

Zmień nazwę sieci

Nazwę sieci (SSID) funkcji Wi-Fi Direct (zwykłe 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 (zwykłe AP) służącego do nawiązywania połączenia ze skanerem. Hasło można ustawić, używając klawiatury programowanej 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 (zwykłe AP) skanera. Po wyłączeniu wszystkie urządzenia połączone ze skanerem za pośrednictwem połączenia Wi-Fi Direct (zwykłe AP) zostaną rozłączone.

Przywr. ust. domyśl.

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

Zostaną usunięte informacje o połączeniu Wi-Fi Direct (zwykłe 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 wyłączanie sieci Wi-Fi Direct (zwykłe 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 (zwykłe 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. Może on zostać uruchomiony po wykonaniu jednej z poniższych czynności.

❏ Konfiguracja ze strony internetowej

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

http://epson.sn

❏ Konfigurowanie za pomocą dysku oprogramowania (tylko modele dostarczone z dyskiem z oprogramowaniem i użytkownicy komputerów Windows z napędami dysków).

Umieść dysk oprogramowania w komputerze, a następnie postępuj zgodnie z instrukcjami na ekranie.

Wybór metod łączenia

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Na ekranie **Wybierz operację** 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 32

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.

http://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. Może on zostać uruchomiony wykonując poniższą czynność.

❏ Konfiguracja ze strony internetowej

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

http://epson.sn

❏ Konfigurowanie za pomocą dysku oprogramowania (tylko modele dostarczone z dyskiem z oprogramowaniem i użytkownicy komputerów Windows z napędami dysków).

Umieść dysk oprogramowania w komputerze, a następnie postępuj zgodnie z instrukcjami na ekranie.

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 18

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 pozycje **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.

❏ Konfiguracja ze strony internetowej

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

http://epson.sn

❏ Konfigurowanie za pomocą dysku oprogramowania (tylko modele dostarczone z dyskiem z oprogramowaniem i użytkownicy komputerów Windows z napędami dysków).

Umieść dysk oprogramowania w komputerze, a następnie postępuj zgodnie z instrukcjami na ekranie.

Wybór zmiany metod łączenia się

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Na ekranie **Wybierz operację** 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.

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

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 pozycje **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

Parametry Wi-Fi znajdują się w poniższej tabeli.

Kraje lub regiony z wyjątkiem poniższych	Tabela A
Australia Nowa Zelandia Tajwan Korea Południowa	Tabela B

Tabela A

Standardy	IEEE 802.11b/g/n*1
Zakres częstotliwości	2,4 GHz
Maksymalna moc przekazywanej transmisji radiowej	2400–2483,5 MHz: 20 dBm (EIRP)
Kanały	1/2/3/4/5/6/7/8/9/10/11/12/13
Tryby połączenia	Infrastruktura, Wi-Fi Direct (zwykłe 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 Wi-Fi Direct obsługuje 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)
	Technologia 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 dupleks, 10 Mb/s półdupleks, 100 Mb/s pełny dupleks, 100 Mb/s półdupleks
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 IPv4/IPv6

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

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
		NetBIOS (TCP)	139
	Serwer WebDAV	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

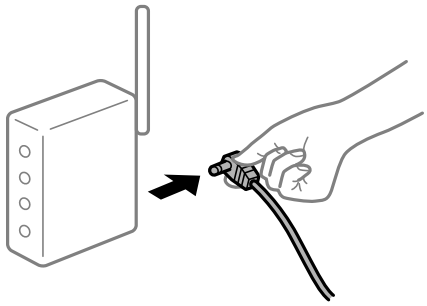
Nie można połączyć się z siecią

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

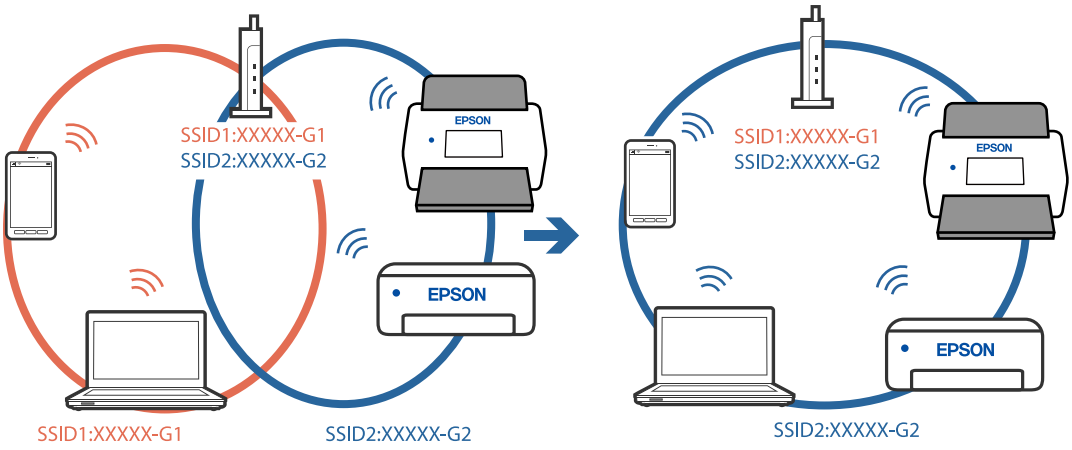
Ponownie skonfiguruj ustawienia połączenia, tak aby pasowały do nowego routera bezprzewodowego.

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 ruterem 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 pozycje **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 nawiąż 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 konfiguracyjnej w przeglądarce” na stronie 36
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

Web Config

Web Config jest aplikacją działającą na komputerze w przeglądarkach internetowych, takich jak Internet Explorer i Safari. Umożliwia ona sprawdzenie stanu skanera lub zmianę usługi sieciowej oraz ustawień skanera. Ponieważ dostęp do skanerów i ich obsługa odbywa się bezpośrednio przez sieć, nadaje się do konfigurowania jednego skanera naraz. Aby korzystać z aplikacji Web Config, połącz komputer z tą samą siecią, co skaner.

Obsługiwane są następujące przeglądarki.

Microsoft Edge, Windows Internet Explorer 8 lub wersja nowsza, Firefox*, Chrome*, Safari*

* Użyj najnowszej wersji.

Uruchamianie aplikacji konfiguracyjnej w przeglądarce

1. Sprawdź adres IP skanera.

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

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

   Format:

   IPv4: http://adres IP skanera/

   IPv6: http://[adres IP skanera]/

   Przykłady:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Uwaga:
   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.

3. Zaloguj się na konto administratora, aby zmienić ustawienia skanera.

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

   Uwaga:
   - ❏ *Poniżej przedstawiono wstępne wartości dla informacji administratora Web Config.*
     - *· Nazwa użytkownika: brak (puste)*
     - *· Hasło: numer seryjny skanera*

     Aby znaleźć numer seryjny należy sprawdzić etykietę z tyłu skanera.
   - ❏ *Jeśli w prawym górnym rogu ekranu wyświetlana jest pozycja **Wylogowanie administratora**, oznacza to, że zalogowano już na konto administratora.*

Uruchomienie Web Config w Windows

Po podłączeniu komputera do skanera przy użyciu WSD wykonaj podane poniżej czynności w celu uruchomienia aplikacji Web Config.

1. Na komputerze otwórz listę skanerów.
   - ❏ Windows 10

     Kliknij przycisk Start i wybierz kolejno pozycje **System Windows** > **Panel sterowania** > **Sprzęt i dźwięk** > **Wyświetl urządzenia i drukarki**.
   - ❏ Windows 8.1/Windows 8

     Wybierz **Pulpit** > **Ustawienia** > **Panel sterowania** > **Sprzęt i dźwięk** (lub **Sprzęt**) > **Wyświetl urządzenia i drukarki**.
   - ❏ Windows 7

     Kliknij przycisk Start i wybierz kolejno **Panel sterowania** > **Wyświetl urządzenia i drukarki** w menu **Sprzęt i dźwięk**.
2. Kliknij skaner prawym przyciskiem myszy, a następnie wybierz polecenie **Właściwości**.
3. Wybierz kartę **Usługa internetowa** i kliknij URL.

   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.

   Uwaga:
   - ❏ *Poniżej przedstawiono wstępne wartości dla informacji administratora Web Config.*

     · Nazwa użytkownika: brak (puste)

     · Hasło: numer seryjny skanera

     Aby znaleźć numer seryjny należy sprawdzić etykietę z tyłu skanera.
   - ❏ *Jeśli w prawym górnym rogu ekranu wyświetlana jest pozycja **Wylogowanie administratora**, oznacza to, że zalogowano już na konto administratora.*

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.

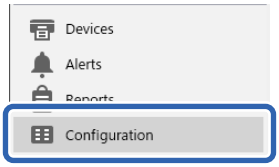
Szablon konfiguracji

Tworzenie szablonu konfiguracji

Utwórz nowy szablon konfiguracji.

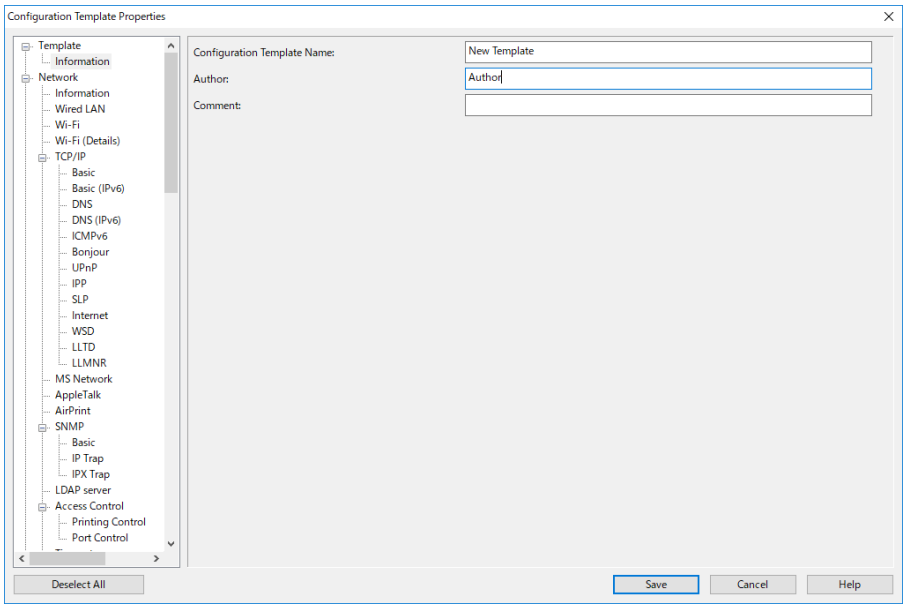
1. Uruchom aplikację Epson Device Admin.

2. Z bocznego menu zadań wybierz pozycję **Configuration**.



3. Wybierz **New** w menu wstążki.

4. Ustaw każdą pozycję.



Pozycja	Objaśnienie
Configuration Template Name	Nazwa szablonu konfiguracji. Wprowadź maksymalnie 1024 znaki w kodowaniu Unicode (UTF-8).
Author	Informacje dotyczące autora szablonu. Wprowadź maksymalnie 1024 znaki w kodowaniu Unicode (UTF-8).
Comment	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 **Save**.*

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.

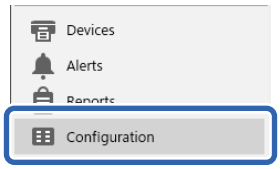
*1. Na wstążce menu w oknie Lista urządzeń wybierz pozycje **Options** > **Password manager**.*

*2. Wybierz pozycję **Enable automatic password management**, a następnie kliknij przycisk **Password manager**.*

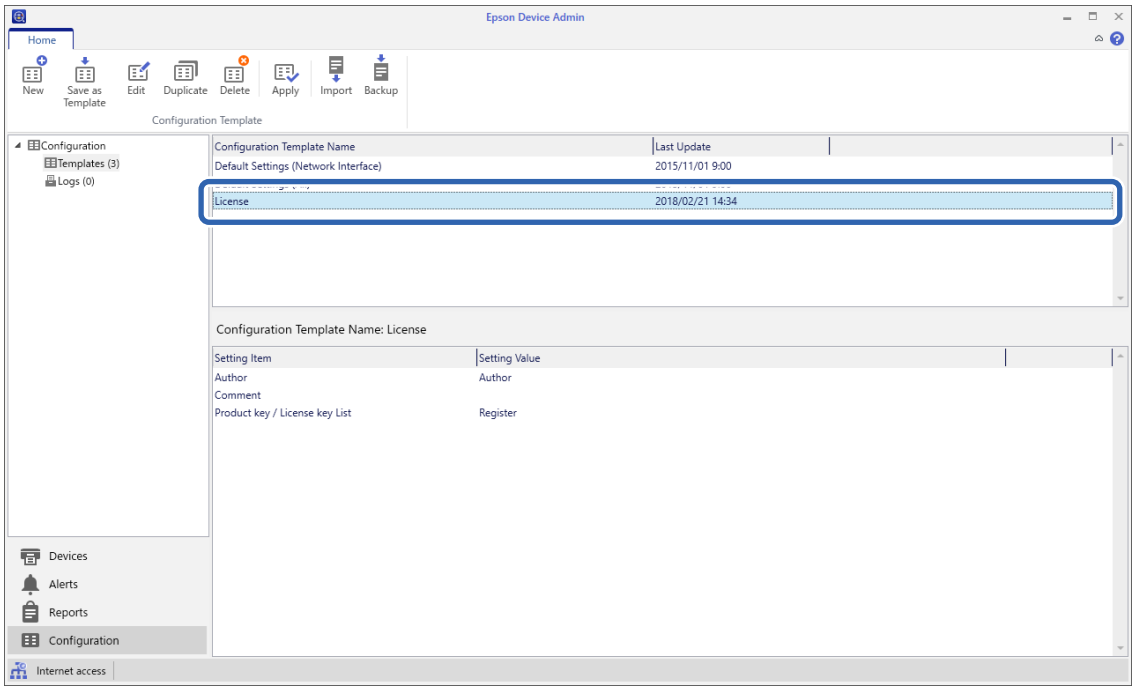
*3. Wybierz odpowiedni skaner, a następnie kliknij **Edit**.*

*4. Ustaw hasło, a następnie kliknij przycisk **OK**.*

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



2. Wybierz szablon konfiguracji, który chcesz zastosować, w obszarze **Configuration Template Name**.



3. Kliknij **Apply** w menu wstążki.

   Zostanie wyświetlony ekran wyboru urządzenia.

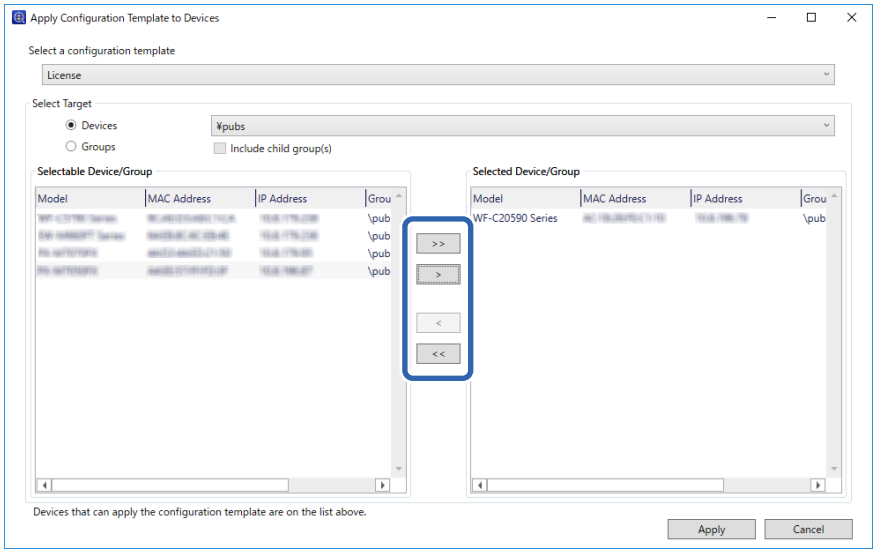
4. Wybierz szablon konfiguracji, który ma być zastosowany.

   Uwaga:

   ❏ *Po wyborze pozycji **Devices** oraz grup zawierających urządzenia z menu rozwijanego wyświetlone zostaną wszystkie urządzenia.*

   ❏ *Grupy zostaną wyświetlone po wybraniu pozycji **Groups**. Wybierz opcję **Include child group(s)**, aby automatycznie wybrać grupy podrzędne w ramach wybranej grupy.*

5. Przenieś skaner lub grupy, do których ma być zastosowany szablon, do obszaru **Selected Device/Group**.



6. Kliknij pozycję **Apply**.

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

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

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

9. Kliknij **Details** i sprawdź wyświetlane informacje.

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

10. Kliknij pozycję **Close**.

Ustawienia niezbędne do skanowania

Konfigurowanie serwera pocztowego

Serwer pocztowy można konfigurować za pomocą aplikacji Web Config.

Jeśli na skanerze zostanie włączone wysyłanie wiadomości e-mail przez skonfigurowanie serwera pocztowego, możliwe jest wykonywanie następujących czynności.

❏ Przesyłanie skanów za pośrednictwem poczty e-mail

❏ Odbieranie powiadomień e-mail od skanera

Przed przystąpieniem do konfigurowania należy sprawdzić następujące zagadnienia.

❏ Skaner jest połączony z siecią z dostępem do serwera pocztowego.

❏ Konfiguracja poczty e-mail na komputerze wykorzystującym ten sam serwer pocztowy, co skaner.

Uwaga:

❏ *W przypadku korzystania z serwera pocztowego w Internecie należy sprawdzić informacje od dostawcy lub witryny.*

❏ *Możliwe jest też skonfigurowanie serwera pocztowego z poziomu panelu sterowania. Wybierz pozycje wymienione poniżej.*

Ustaw.* > *Ustawienia sieciowe* > *Zaawansowane* > *Serwer e-mail* > *Ustaw. serwera

1. Otwórz aplikację Web Config i wybierz kartę **Sieć** > **Serwer e-mail** > **Podstawowe**.
2. Wprowadź wartości poszczególnych pozycji.
3. Wybierz pozycję **OK**.

   Zostaną wyświetlone wybrane ustawienia.

Powiązane informacje

➡ „Uruchamianie aplikacji konfiguracyjnej w przeglądarce” na stronie 36

Opcje ustawień serwera pocztowego

Elementy	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 musi obsługiwać uwierzytelnianie SMTP.
	POP przed SMTP	W przypadku wybrania tej metody należy skonfigurować serwer POP3.
Konto uwierzytelnione	Jeśli dla opcji **Sposób uwierzytelniania** zostanie wybrane ustawienie **UWIERZYTELNIANIE SMTP** lub **POP przed SMTP**, wprowadź nazwę uwierzytelnianego konta o długości od 0 do 255 znaków ASCII (0x20–0x7E).	
Hasło uwierzytelnione	Jeśli dla opcji **Sposób uwierzytelniania** zostanie wybrane ustawienie **UWIERZYTELNIANIE SMTP** lub **POP przed SMTP**, wprowadź hasło uwierzytelniania o długości od 0 do 20 znaków ASCII (0x20–0x7E).	

Elementy	Ustawienia i objaśnienie	
Adres email wysyłającego	Wprowadź adres e-mail nadawcy. 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.	
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	Włączenie tej opcji powoduje zweryfikowanie certyfikatu. Zalecane jest ustawienie **Włącz**.	
Adres serwera POP3	Jeśli dla opcji **Sposób uwierzytelniania** zostanie wybrane ustawienie **POP przed SMTP**, wprowadź adres serwera POP3 o długości od 0 do 255 znaków A–Z a–z 0–9 . -. Można użyć formatu IPv4 lub FQDN.	
Numer portu serwera POP3	Jeśli dla opcji **Sposób uwierzytelniania** zostanie wybrane ustawienie **POP przed SMTP**, wprowadź liczbę z zakresu od 1 do 65535.	

Sprawdzanie połączenia z serwerem pocztowym

Połączenie z serwerem pocztowym można sprawdzić, wykonując test połączenia.

1. Otwórz aplikację Web Config i wybierz kartę **Sieć** > **Serwer e-mail** > **Test połączenia**.
2. Wybierz pozycję **Start**.

   Uruchomiony zostanie test połączenia z serwerem e-mail. Po zakończeniu testu wyświetlany jest raport z testu.

   Uwaga:
   Połączenie z serwerem pocztowym można też sprawdzać z poziomu panelu sterowania. Wybierz pozycje wymienione poniżej.

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

Objaśnienia do testu połączenia z serwerem pocztowym

Komunikaty	Przyczyna
Test połączenia zakończony powodzeniem.	Ten komunikat jest wyświetlany, gdy połączenie z serwerem się powiedzie.

Komunikaty	Przyczyna
Błąd komunikacji serwera SMTP. Sprawdź następujące elementy. - Ustawienia sieci	Sytuacje, w których ten komunikat jest wyświetlany ❏ Skaner nie jest połączony z siecią ❏ Serwer SMTP nie działa ❏ Połączenie sieciowe zostało rozłączone w trakcie komunikacji ❏ Odebrano niepełne dane
Błąd komunikacji serwera POP3. Sprawdź następujące elementy. - Ustawienia sieci	Sytuacje, w których ten komunikat jest wyświetlany ❏ Skaner nie jest połączony z siecią ❏ Serwer POP3 nie działa ❏ Połączenie sieciowe zostało rozłączone w trakcie komunikacji ❏ 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 ❏ Połączenie z serwerem DNS nie powiodło się ❏ 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 ❏ Połączenie z serwerem DNS nie powiodło się ❏ 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 jest wyświetlany, gdy wystąpi niezgodność SMTP między serwerem a klientem lub serwer nie obsługuje bezpiecznego 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 wysyła 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 wysyła żądania użycia połączenia STARTTLS w celu ustanowienia bezpiecznego połączenia SMTP.
Połączenie jest podejrzane. Sprawdź następujące elementy. - Data i godzina	Ten komunikat jest wyświetlany, gdy data i godzina na skanerze są niepoprawne lub certyfikat wygasł.
Połączenie jest podejrzane. Sprawdź następujące elementy. - Certyfikat CA	Ten komunikat jest wyświetlany, gdy na skanerze nie ma głównego certyfikatu odpowiadającego serwerowi lub nie zaimportowano certyfikatu Certyfikat CA.

Komunikaty	Przyczyna
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.

Konfigurowanie folderu udostępnionego sieci

Wprowadź ustawienie dla udostępnionego foldera sieciowego, aby zapisać zeskanowany obraz.

Podczas zapisywania pliku w folderze skaner loguje się jako użytkownik komputera, na którym folder ten stworzono.

Tworzenie folderu udostępnionego

Powiązane informacje

➡ „Czynności do wykonania przed utworzenie folderu udostępnionego” na stronie 45

➡ „Sprawdzanie profilu sieciowego” na stronie 46

➡ „Lokalizacja tworzenia folderu udostępnionego i przykład zabezpieczeń” na stronie 46

➡ „Dodawanie grupy lub użytkownika z uprawnieniami dostępu” na stronie 59

Czynności do wykonania przed utworzenie folderu udostępnionego

Przed utworzeniem folderu udostępnionego należy sprawdzić następujące zagadnienia.

❏ Skaner jest połączony z siecią z dostępem do komputera, na którym utworzony zostanie folder udostępniony.

❏ W nazwie komputera, na którym utworzony zostanie folder udostępniony, nie ma znaku wielobajtowego.

Ważne:

Jeżeli w nazwie komputera jest znak wielobajtowy, zapisanie pliku do folderu udostępnionego może się nie powieść.

W takim przypadku należy zmienić na komputer, którego nazwa nie zawiera znaku wielobajtowego, lub zmienić nazwę tego komputera.

Przed przystąpieniem do zmiany nazwy komputera należy skontaktować się z administratorem, ponieważ może to wpływać na niektóre ustawienia, takie jak zarządzanie komputerem, dostęp do zasobów itd.

Sprawdzanie profilu sieciowego

Na komputerze, na którym ma być utworzony folder udostępniony, sprawdź, czy włączone jest udostępnianie folderów.

1. Na komputerze, na którym ma być utworzony folder udostępniony, zaloguj się na konto z uprawnieniami administratora.
2. Wybierz pozycje **Panel kontrolny** > **Sieć Internet** > **Sieć i centrum udostępniania**.
3. Kliknij polecenie **Zmień zaawansowane ustawienia udostępniania**, a następnie na liście profili sieciowych przycisk obok profilu z oznaczeniem **(bieżący profil)**.
4. Sprawdź, czy 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.

Lokalizacja tworzenia folderu udostępnionego i przykład zabezpieczeń

W zależności od lokalizacji miejsca utworzenia folderu udostępniania bezpieczeństwo i wygoda użytkowania mogą się różnić.

Aby móc używać folderu udostępnionego ze skanerów lub innych komputerów, należy przyznać następujące uprawnienia do odczytu i zmiany folderu.

❏ Karta **Udostępnianie** > **Udostępnianie zaawansowane** > **Uprawnienia**

Umożliwia kontrolowanie sieciowych uprawnień dostępu do folderu udostępnionego.

❏ Uprawnienia dostępu na karcie **Zabezpieczenia**

Umożliwia kontrolowanie dostępu sieciowego i lokalnego do folderu udostępnionego.

Jeśli dostęp do folderu udostępnionego utworzonego na pulpicie zostanie przyznanym wszystkim użytkownikom (**Wszyscy**), wszyscy użytkownicy z dostępem do komputera będą mogli z niego korzystać.

Jednak użytkownik bez uprawnień nie będzie mógł uzyskać dostępu, ponieważ pulpit (folder) jest w folderze użytkownika, a jego ustawienia zabezpieczeń są dziedziczone przez ten folder udostępniony. Użytkownik, któremu na karcie **Zabezpieczenia** zostaną przyznane uprawnienia dostępu (użytkownik zalogowany i administrator w tym przypadku), mogą obsługiwać ten folder.

Więcej informacji o tworzeniu w poprawnej lokalizacji można znaleźć poniżej.

Ten przykład dotyczy tworzenia folderu „scan_folder”.

Powiązane informacje

➡ „Przykład konfiguracji serwera plików” na stronie 46

➡ „Przykład konfiguracji komputera osobistego” na stronie 53

Przykład konfiguracji serwera plików

W tym rozdziale opisano tworzenie folderu udostępnionego w katalogu głównym dysku komputera udostępnionego, np. serwerze plików, w następujących warunkach.

Użytkownicy z kontrolą dostępu, np. osoby z komputerami w tej samej domenie, co komputer, na którym utworzono folder udostępniony, mogą uzyskać dostęp do folderu udostępnionego.

Konfigurację tę należy ustawić, zezwalając dowolnemu użytkownikowi na odczyt i zapis w folderze udostępnionym na komputerze, np. serwerze plików i komputerze udostępnionym.

❏ Miejsce tworzenia folderu udostępnionego: katalog główny dysku

❏ Ścieżka folderu: C:\scan_folder

❏ Uprawnienia dostępu przez sieć (uprawnienia udostępniania): wszyscy

❏ Uprawnienia dostępu w systemie plików (zabezpieczenia): użytkownicy uwierzytelnieni

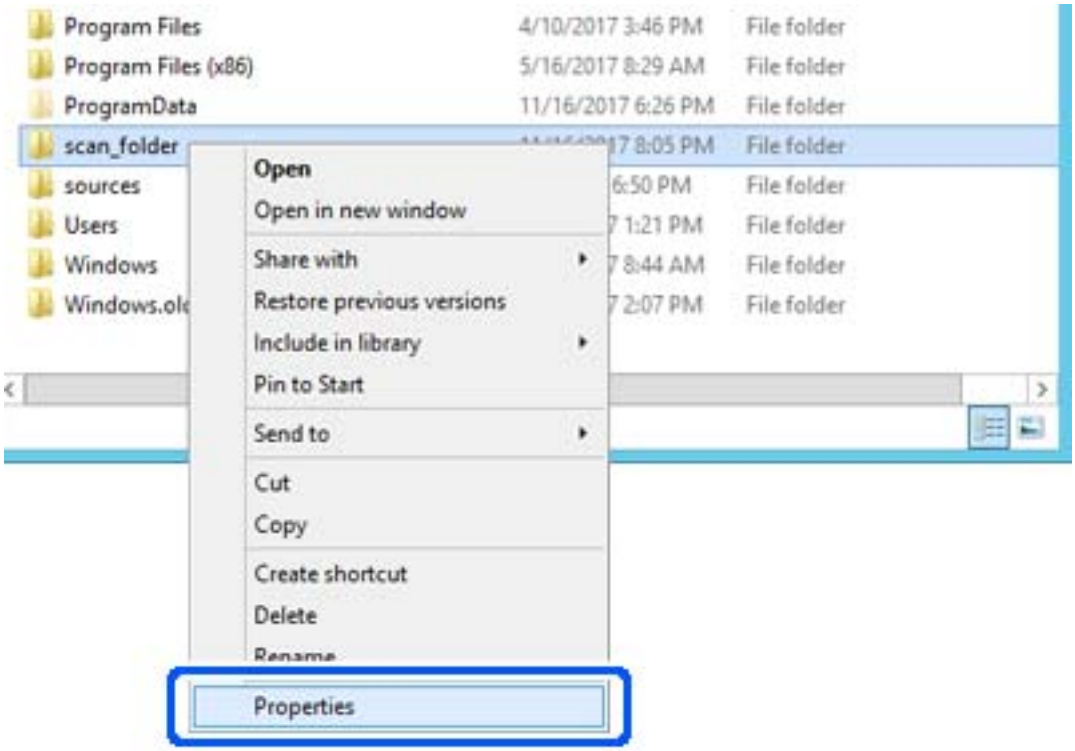
1. Na komputerze, na którym ma być utworzony folder udostępniony, zaloguj się na konto z uprawnieniami administratora.

2. Uruchom program Eksplorator.

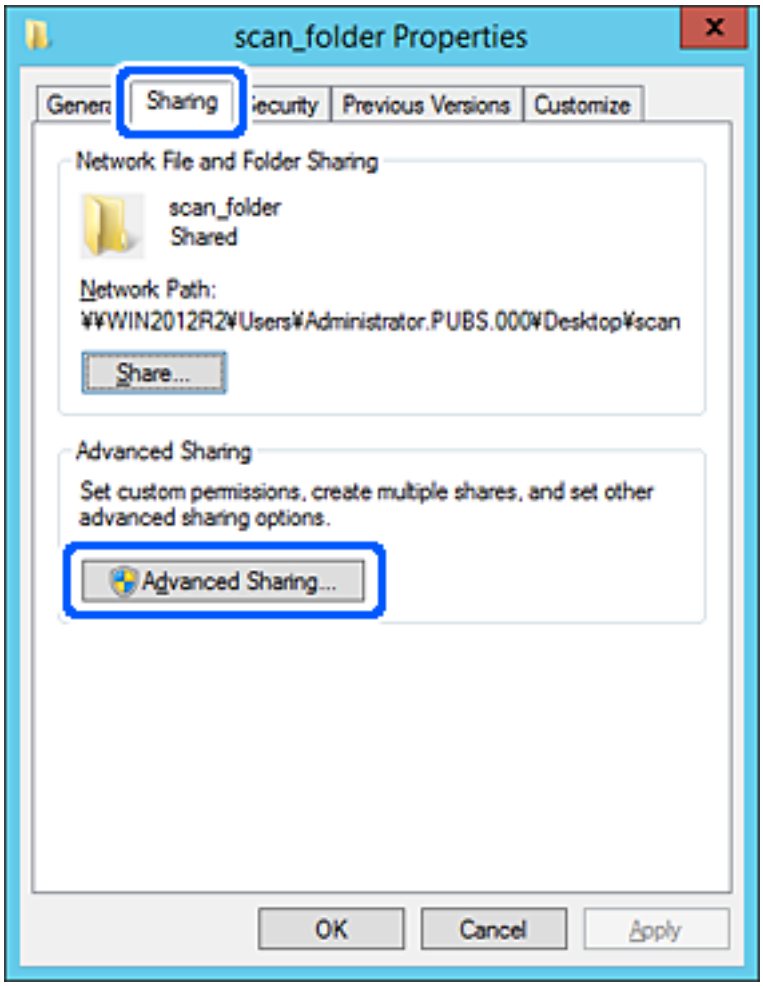
3. Utwórz folder w katalogu głównym dysku i nadaj mu nazwę „scan_folder”.

   W przypadku nazwy folderu można wprowadzić ciąg o długości od 1 do 12 znaków alfanumerycznych. Jeśli limit znaków nazwy folderu zostanie przekroczony, uzyskanie dostępu do folderu może nie być możliwe w zależności od środowiska.

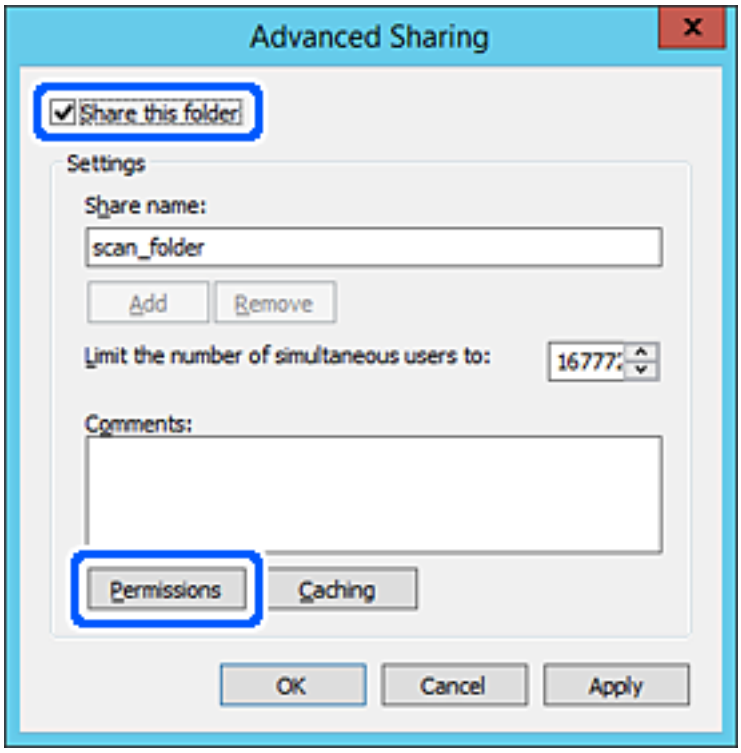
4. Kliknij prawym przyciskiem folder, a następnie wybierz polecenie **Właściwości**.



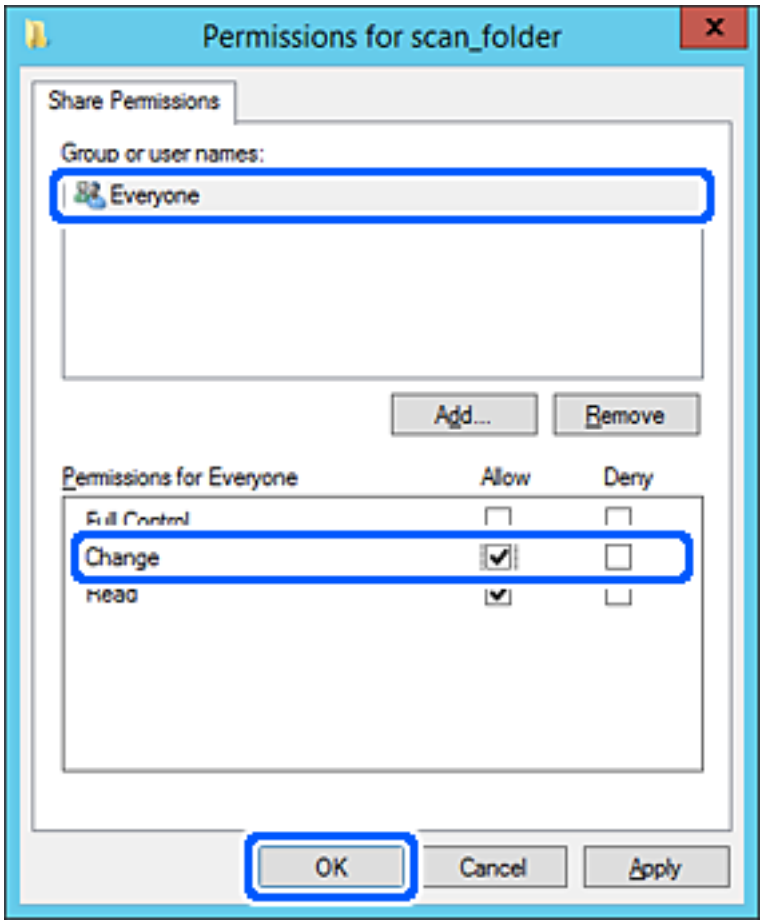
5. Na karcie **Udostępnianie** kliknij przycisk **Udostępnianie zaawansowane**.



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

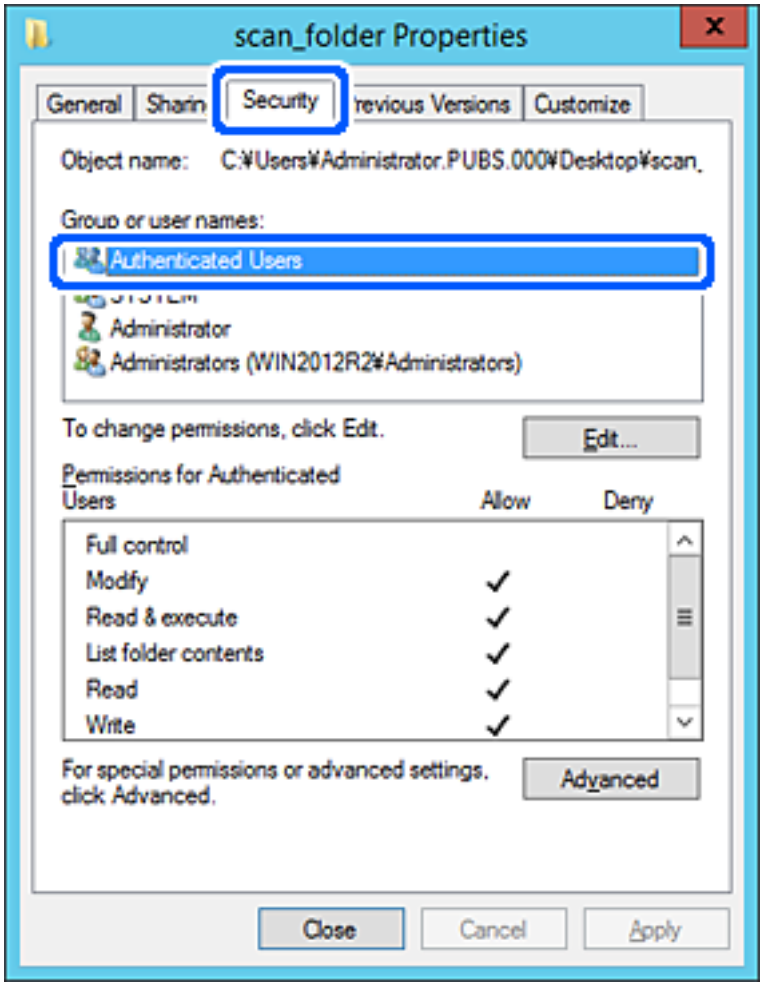


7. W polu **Nazwy grupy lub użytkownika** wybierz pozycję **Wszyscy**, w kolumnie **Zmiana** wybierz ustawienie **Zezwól**, a następnie kliknij przycisk **OK**.



8. Kliknij pozycję **OK**.

9. Przejdź do karty **Zabezpieczenia**, a następnie w polu **Nazwy grupy lub użytkownika** wybierz pozycję **Użytkownicy uwierzytelnieni**.

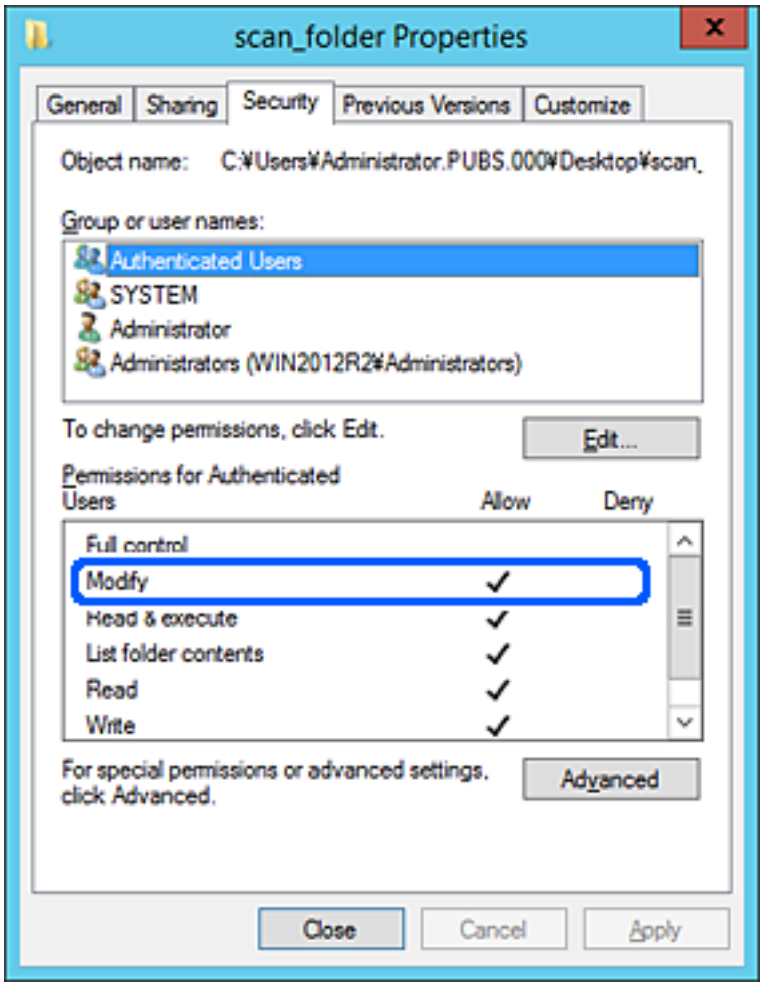


„Użytkownicy uwierzytelnieni” to specjalna grupa, która wywiera wpływ na wszystkich użytkowników, którzy logują się w domenie lub na komputerze. Ta grupa jest wyświetlana tylko, w katalogu głównym zostanie utworzony folder.

Jeśli nie zostanie wyświetlony, można go dodać, klikając przycisk **Edytuj**. Więcej informacji można znaleźć w części Informacje pokrewne.

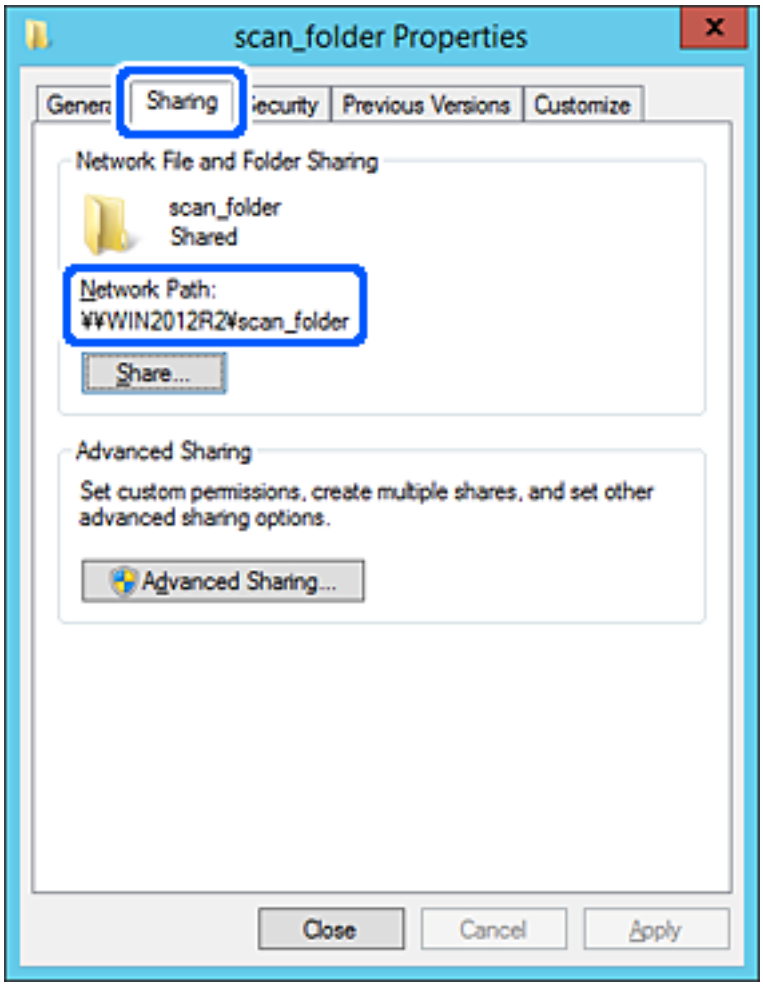
10. Upewnij się, że w obszarze **Uprawnienia użytkowników uwierzytelnionych** w kolumnie **Modyfikacja** wybrano ustawienie **Zezwól**.

    W przeciwnym razie wybierz pozycję **Użytkownicy uwierzytelnieni**, kliknij przycisk **Edytuj**, w obszarze **Uprawnienia uwierzytelnionych użytkowników** w kolumnie **Modyfikacja** wybierz ustawienie **Zezwól**, a następnie kliknij przycisk **OK**.



11. Przejdź do karty **Udostępnianie**.

    Zostanie wyświetlona ścieżka sieciowa folderu udostępnionego. Jest używana podczas rejestracji kontaktów skanera. Zapisz ją.



12. Kliknij przycisk **OK** lub **Zamknij**, aby zamknąć ekran.

    Sprawdź, czy plik można zapisać lub odczytać w folderze udostępnionym z poziomu komputerów w tej samej domenie.

Powiązane informacje

➡ „Dodawanie grupy lub użytkownika z uprawnieniami dostępu” na stronie 59

➡ „Rejestrowanie miejsca docelowego w kontaktach za pomocą aplikacji Web Config” na stronie 64

Przykład konfiguracji komputera osobistego

W tym przykładzie przedstawiono tworzenie folderu udostępnionego na pulpicie użytkownika aktualnie zalogowanego na komputerze.

Użytkownik, który zaloguje się na komputerze i ma uprawnienia administratora, może uzyskać dostęp do folderu na pulpicie i folderu dokumentów w folderze użytkownika.

Konfigurację tę należy wykonać, aby NIE zezwolić innym użytkownikom na odczyt i zapis w folderze udostępnionym na komputerze osobistym.

- ❏ Miejsce tworzenia folderu udostępnionego: pulpit
- ❏ Ścieżka folderu: C:\Users\xxxx\Desktop\scan_folder
- ❏ Uprawnienia dostępu przez sieć (uprawnienia udostępniania): wszyscy
- ❏ Uprawnienia dostępu w systemie plików (zabezpieczenia): bez dodawania lub z dodawaniem nazw użytkowników/grup, aby zezwolić na dostęp

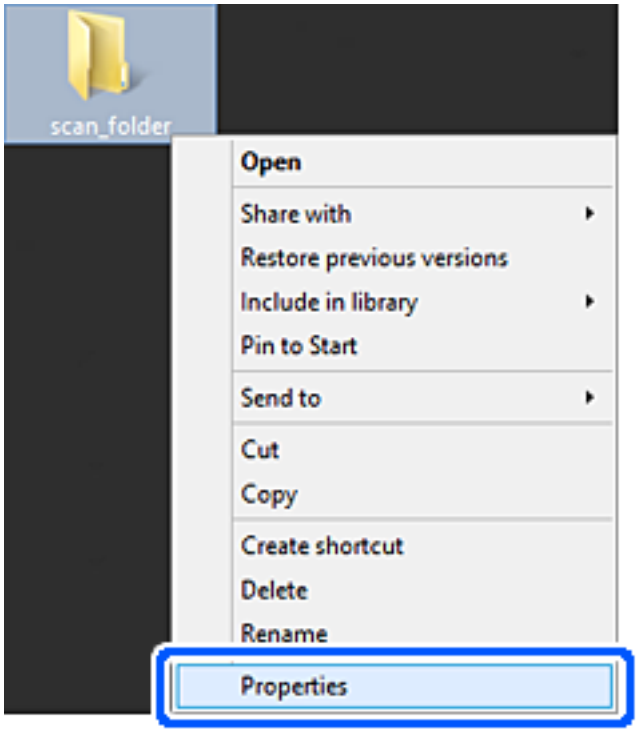
1. Na komputerze, na którym ma być utworzony folder udostępniony, zaloguj się na konto z uprawnieniami administratora.

2. Uruchom program Eksplorator.

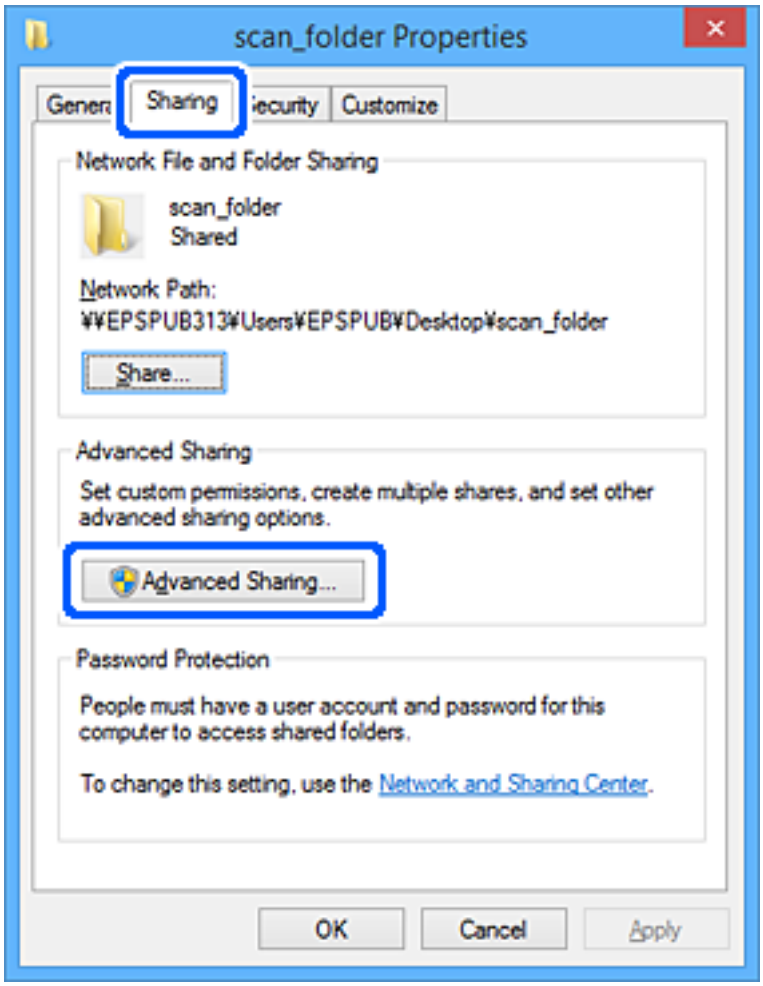
3. Utwórz folder na pulpicie i nadaj mu nazwę „scan_folder”.

   W przypadku nazwy folderu można wprowadzić ciąg o długości od 1 do 12 znaków alfanumerycznych. Jeśli limit znaków nazwy folderu zostanie przekroczony, uzyskanie dostępu do folderu może nie być możliwe w zależności od środowiska.

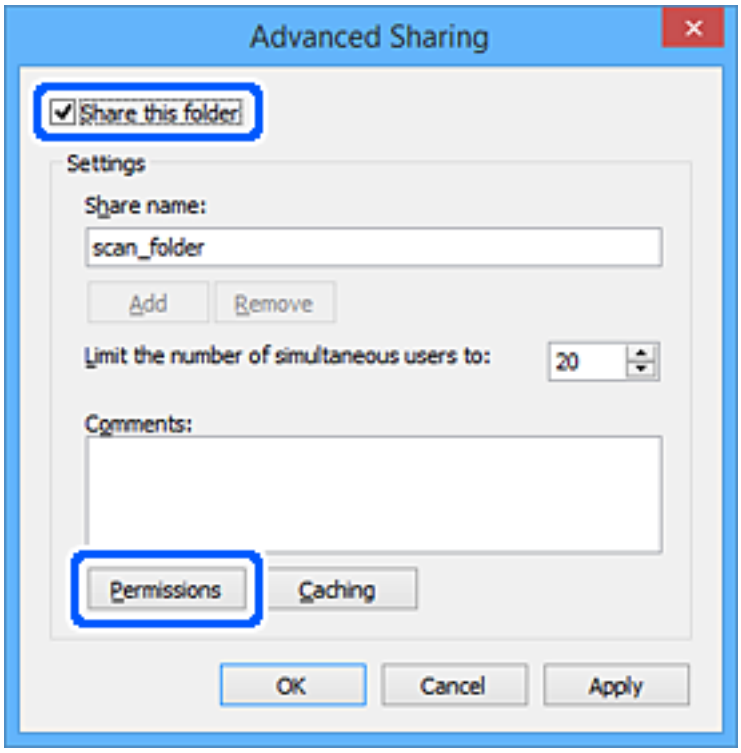
4. Kliknij prawym przyciskiem folder, a następnie wybierz polecenie **Właściwości**.



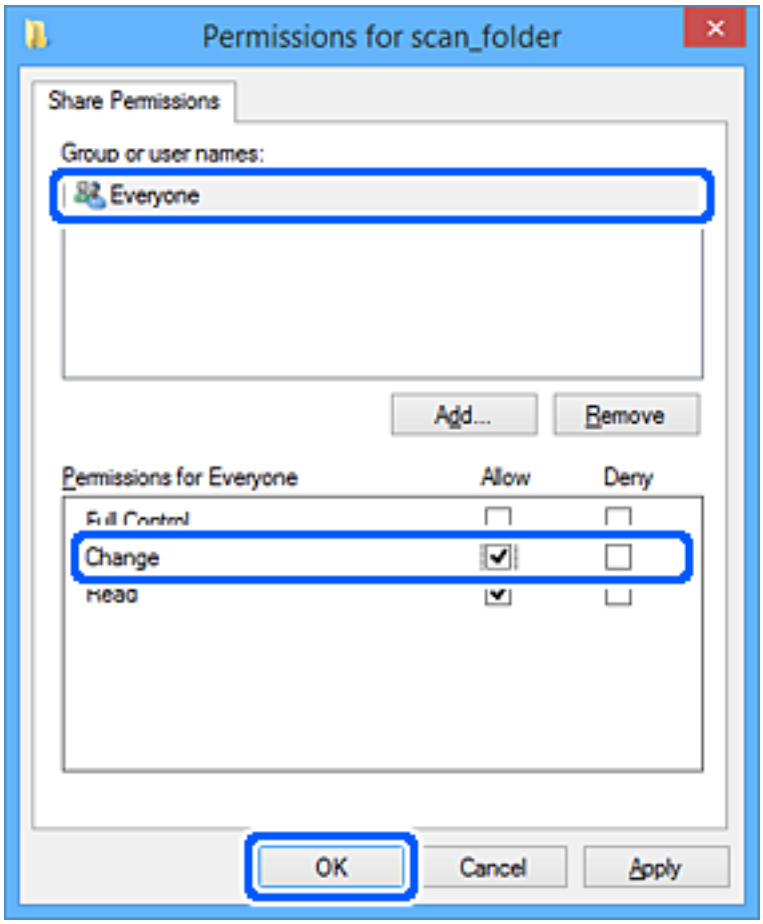
5. Na karcie **Udostępnianie** kliknij przycisk **Udostępnianie zaawansowane**.



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



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



8. Kliknij pozycję **OK**.

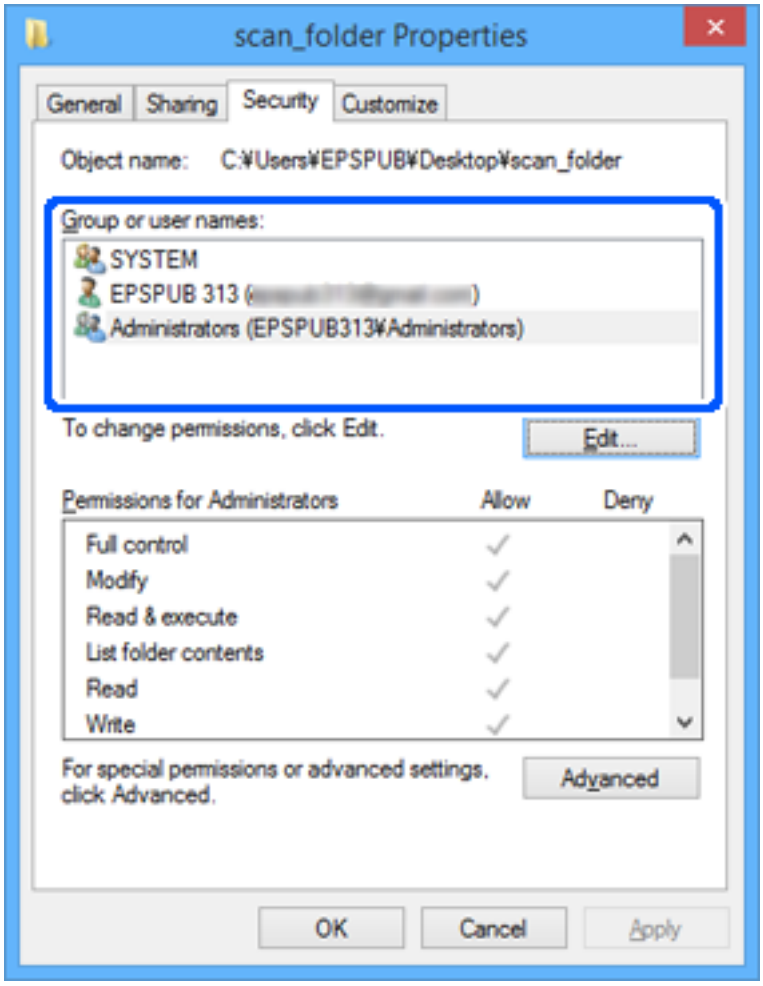
9. Przejdź do karty **Zabezpieczenia**.

10. Sprawdź, czy grupa lub użytkownik są wyświetlane w polu **Nazwy grupy lub użytkownika**.

    Grupa lub użytkownik wyświetlani w tym polu mogą uzyskiwać dostęp do folderu udostępnionego.

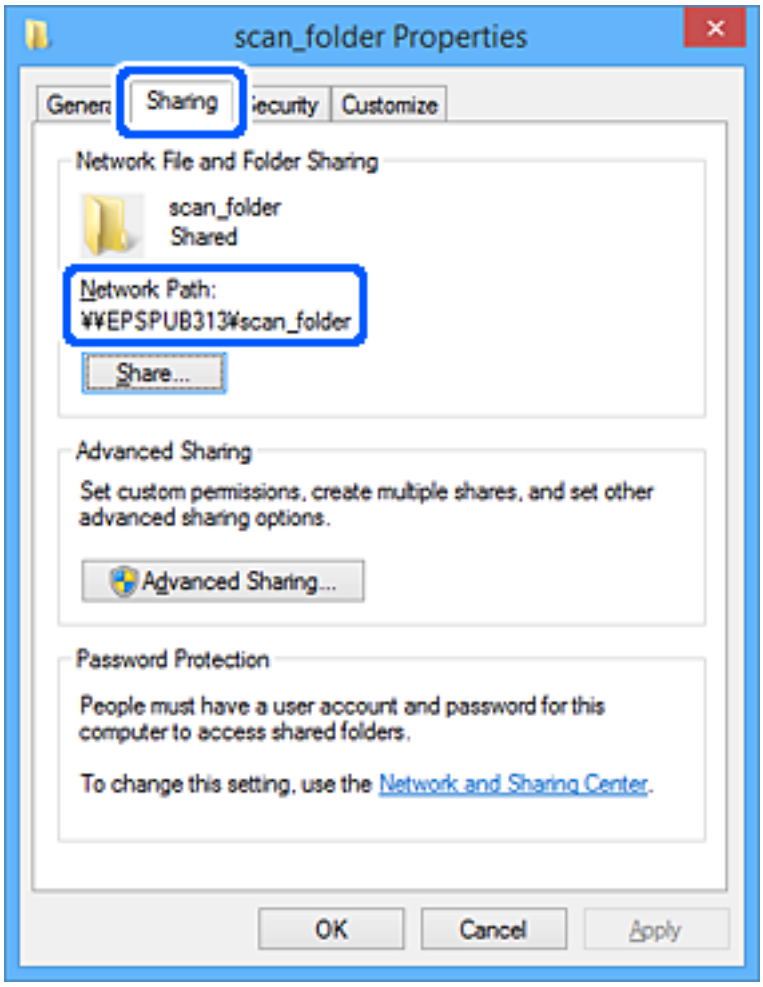
    W takim przypadku użytkownik, który zaloguj się na tym komputerze z uprawnieniami administratora, może uzyskać dostęp do tego folderu udostępnionego.

Dodaj uprawnienia dostępu w razie potrzeby. Można go dodać, klikając przycisk **Edytuj**. Więcej informacji można znaleźć w części Informacje pokrewne.



11. Przejdź do karty **Udostępnianie**.

    Zostanie wyświetlona ścieżka sieciowa folderu udostępnionego. Jest używana podczas rejestracji kontaktów skanera. Zapisz ją.



12. Kliknij przycisk **OK** lub **Zamknij**, aby zamknąć ekran.

    Sprawdź, czy plik można zapisać lub odczytać w folderze udostępnionym na komputerach użytkowników lub grup z uprawnieniem dostępu.

Powiązane informacje

➡ „Dodawanie grupy lub użytkownika z uprawnieniami dostępu” na stronie 59

➡ „Rejestrowanie miejsca docelowego w kontaktach za pomocą aplikacji Web Config” na stronie 64

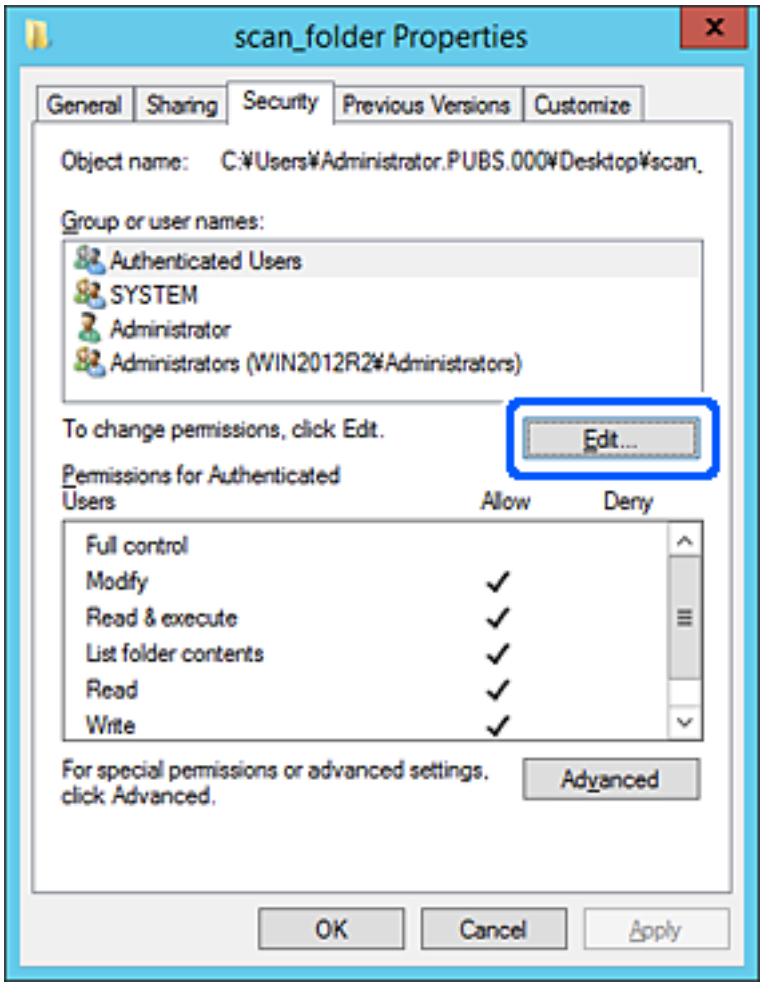
Dodawanie grupy lub użytkownika z uprawnieniami dostępu

Można dodać grupę lub użytkownika z uprawnieniami dostępu.

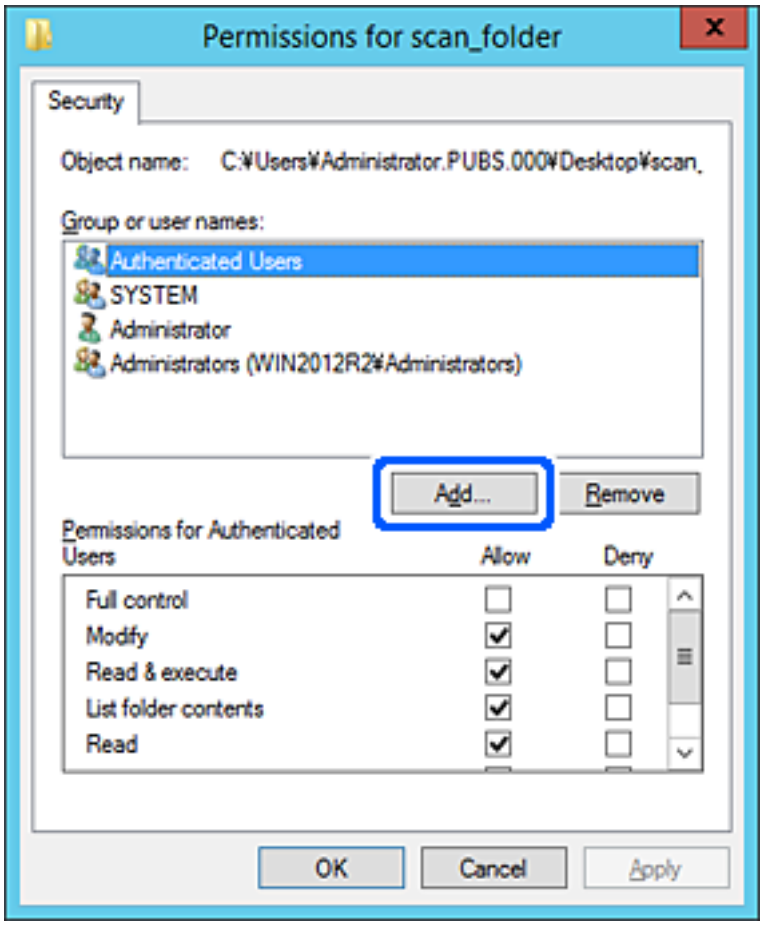
1. Kliknij folder prawym przyciskiem myszy i wybierz polecenie **Właściwości**.

2. Przejdź do karty **Zabezpieczenia**.

3. Kliknij przycisk **Edytuj**.



4. W obszarze **Nazwy grupy lub użytkownika** kliknij przycisk **Dodaj**.

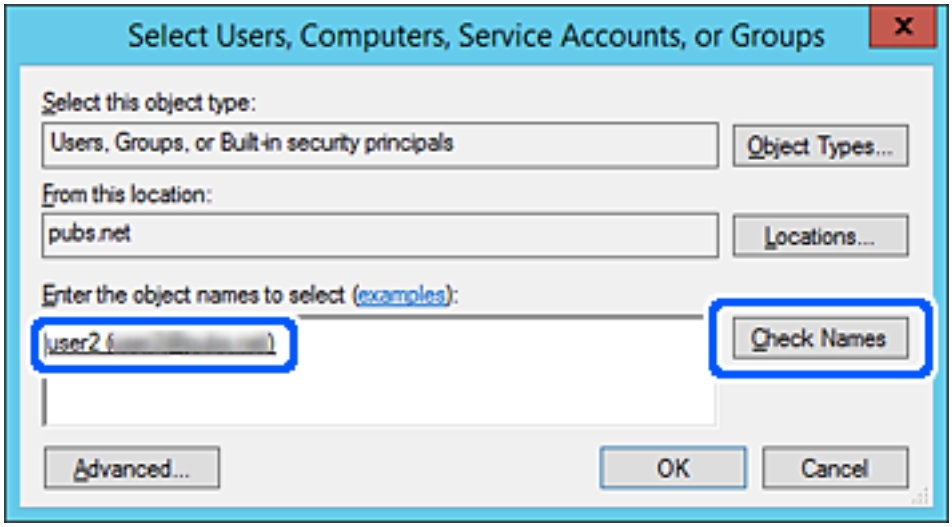


5. Wprowadź nazwę grupy lub użytkownika, której ma być przyznany dostęp, a następnie kliknij przycisk **Sprawdź nazwy**.

   Do nazwy zostanie dodane podkreślenie.

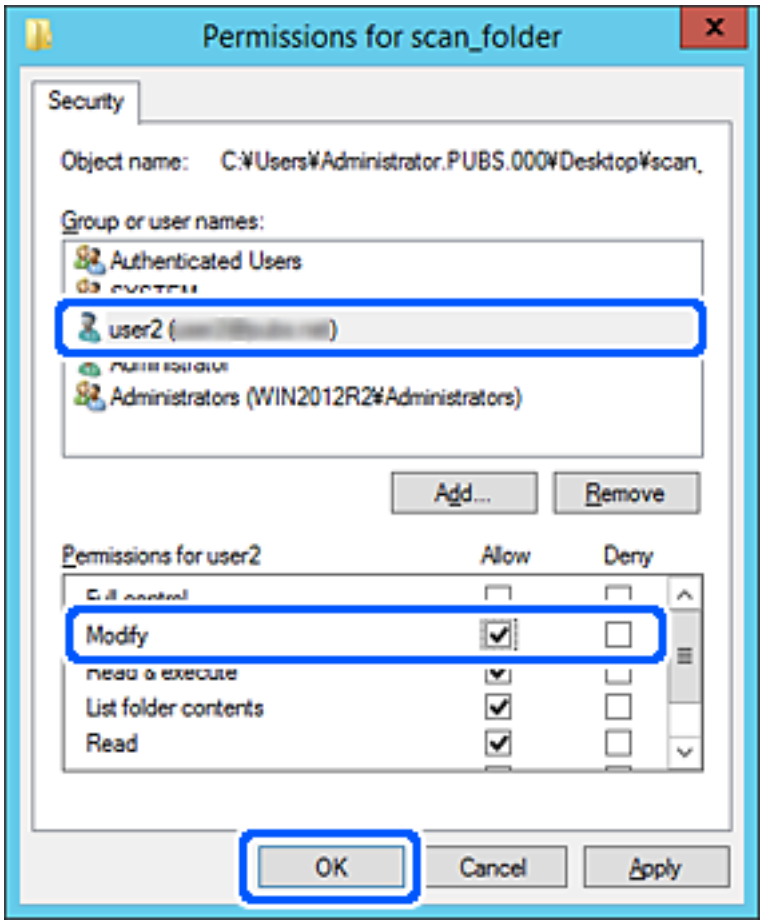
Uwaga:
Jeżeli pełna nazwa grupy lub użytkownika nie jest znana, wprowadź część nazwy, a następnie kliknij przycisk ***Sprawdź nazwy****. Zostaną wyświetlone nazwy grup lub nazwy użytkowników pasujące do części nazwy, a następnie można wybrać pełną nazwę z listy.*

Jeżeli pasuje tylko jedna nazwa, w polu ***Wybieranie: Użytkownicy lub Grupy*** *zostanie wyświetlona pełna nazwa z podkreśleniem.*



6. Kliknij przycisk **OK**.

7. Na ekranie Uprawnienia wybierz nazwę użytkownika wprowadzonego w polu **Nazwy grupy lub użytkownika**, wybierz uprawnienie dostępu w kolumnie **Zmiana**, a następnie kliknij przycisk **OK**.



8. Kliknij przycisk **OK** lub **Zamknij**, aby zamknąć ekran.

   Sprawdź, czy plik można zapisać lub odczytać w folderze udostępnionym na komputerach użytkowników lub grup z uprawnieniem dostępu.

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 70

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 konfiguracyjnej w przeglądarce” na stronie 36

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-8). Jeśli ustawienie nie będzie określane, zostaw puste pole.
Hasło indeksu	Wprowadź nazwę o maksymalnie 30 znakach w kodowaniu Unicode (UTF-8), aby wyszukać kontakty na panelu sterowania skanera. Jeśli ustawienie nie będzie określane, 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-8), nie uwzględniając ciągu „\\”. Wprowadź ścieżkę sieciową wyświetloną na ekranie właściwości folderu. Sprawdź następujące informacje dotyczące ustawiania ścieżki sieciowej. „Przykład konfiguracji komputera osobistego” na stronie 53
Nazwa użytkownika	Umożliwia wprowadzenie nazwy użytkownika używanej do uzyskiwania dostępu do folderu sieciowego. Nazwa musi mieć do 30 znaków w formacie Unicode (UTF-8). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F).
Hasło	Umożliwia wprowadzenie hasła używanego do uzyskiwania dostępu do folderu sieciowego. Hasło musi mieć do 20 znaków w formacie Unicode (UTF-8). 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	Wprowadzanie nazwy serwera. Nazwa powinna mieć długość od 1 do 253 znaków w formacie ASCII (0x20–0x7E), bez przedrostka „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-8). 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 określane, zostaw puste pole.
Hasło	Umożliwia wprowadzenie hasła używanego do uzyskiwania dostępu do serwera FTP. Hasło musi mieć do 20 znaków w formacie Unicode (UTF-8). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określane, zostaw puste pole.
Tryb połączenia	Wybór trybu połączenia z menu. Jeśli między skanerem a serwerem FTP znajduje się zapora, 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	Wprowadzanie nazwy serwera. Nazwa powinna mieć długość od 1 do 253 znaków w formacie ASCII (0x20–0x7E), bez przedrostka „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-8). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określane, zostaw puste pole.
Hasło	Umożliwia wprowadzenie hasła używanego do uzyskiwania dostępu do serwera. Hasło musi mieć do 20 znaków w formacie Unicode (UTF-8). Należy jednak unikać stosowania znaków sterujących (0x00 do 0x1F, 0x7F). Jeśli ustawienie nie będzie określane, 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.

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 pozycje **Skanuj** > **Kontakty**.
2. Wybierz numer, które ma być zarejestrowany, a następnie kliknij przycisk **Edytuj**.
3. Z listy **Typ** wybierz grupę.

4. Kliknij pozycję **Wybierz** w obszarze **Kontakty dla Grupa**.

   Zostaną wyświetlone dostępne miejsca docelowe.

5. Zaznacz miejsca docelowe, które mają być zarejestrowane w grupie, a następnie kliknij przycisk **Wybierz**.

6. Wprowadź wartości w polach **Nazwa** i **Hasło indeksu**.

7. Określ, czy przydzielić zarejestrowaną grupę do często używanych grup.

   Uwaga:
   Miejsca docelowe można rejestrować w wielu grupach.

8. Kliknij pozycję **Zastosuj**.

Powiązane informacje

➡ „Uruchamianie aplikacji konfiguracyjnej w przeglądarce” na stronie 36

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.

1. Uruchom aplikację Web Config, wybierz pozycje **Zarządzanie urządzeniem** > **Wartość ustawienia Eksportuj i Importuj** > **Importuj**.

2. W polu **Plik** wybierz plik kopii zapasowej, wprowadź hasło, a następnie kliknij przycisk **Dalej**.

3. 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 przywracanie 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 **Devices**.
3. Z listy urządzeń wybierz urządzenie, które ma być skonfigurowane.
4. Na karcie wstążki **Home** kliknij pozycję **Device Configuration**.

   Jeśli zostało ustawione hasło administratora, wprowadź hasło i kliknij przycisk **OK**.
5. Kliknij pozycje **Common** > **Contacts**.

6. Wybierz format eksportu w oknie **Export** > **Export items**.

   ❏ All Items

   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 **Configuration** i ustaw hasło o długości od 8 do 63 znaków ASCII. To hasło będzie potrzebne podczas importowania danych z pliku binarnego.

   ❏ Items except Security Information

   Eksport pliku w formacie SYLK lub csv. Tę opcje wybierz, aby móc edytować informacje w wyeksportowanym pliku.

7. Kliknij pozycję **Export**.

8. Określ miejsce zapisu, wybierz typ pliku, a następnie kliknij przycisk **Save**.

   Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.

9. 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.

1. Uruchom aplikację Epson Device Admin.

2. Z bocznego menu zadań wybierz pozycję **Devices**.

3. Z listy urządzeń wybierz urządzenie, które ma być skonfigurowane.

4. Na karcie wstążki **Home** kliknij pozycję **Device Configuration**.

   Jeśli zostało ustawione hasło administratora, wprowadź hasło i kliknij przycisk **OK**.

5. Kliknij pozycje **Common** > **Contacts**.

6. Kliknij przycisk **Browse** w obszarze **Import**.

7. Wybierz plik, który ma być zaimportowany, a następnie kliknij przycisk **Open**.

   Po wybraniu pliku binarnego w polu **Password** wprowadź hasło ustawione podczas eksportowania pliku.

8. Kliknij pozycję **Import**.

   Zostanie wyświetlony ekran potwierdzenia.

9. Kliknij pozycję **OK**.

   Zostaną wyświetlone wyniki weryfikacji.

❏ Edit the information read

Kliknij, aby edytować informacje osobno.

❏ Read more file

Kliknij, aby zaimportować wiele plików.

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

    Wróć do ekranu właściwości urządzenia.

11. Kliknij pozycję **Transmit**.

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.

Elementy	Ustawienia i objaśnienie
Bezpieczne połączenie	Określ metodę uwierzytelniania używaną przez skaner w celu uzyskania dostępu do serwera LDAP.
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. ❏ Zapewniona komunikacja między skanerem a serwerem DNS. ❏ Godzina skanera, serwera KDC i serwera uwierzytelniającego (serwera LDAP, serwera SMTP, serwera plików) jest zsynchronizowana. ❏ 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 określane, 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 określane, 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.

Elementy	Ustawienia i objaśnienie
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 niepowodzenie. Sprawdź ustawienia.	Ten komunikat jest wyświetlany w przypadku następujących sytuacji: ❏ Adres serwera LDAP lub numer portu są nieprawidłowe. ❏ Upłynął limit czasu. ❏ Wybrano ustawienie **Nie należy używać** dla opcji **Użyj serwera LDAP**. ❏ 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 niepowodzenie. 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: ❏ Wartości **Nazwa użytkownika** i/lub **Hasło** są niepoprawne. ❏ 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.

Korzystanie z aplikacji Document Capture Pro Server

Używając programu Document Capture Pro Server, można zarządzać metodą sortowania, formatem zapisu i miejscami docelowymi przekazywania wyników skanowania uruchamianego z panelu sterowania skanera. Na panelu sterowania skanera można przywoływać i wykonywać zadania zarejestrowane wcześniej na serwerze.

Zainstaluj go na komputerze serwera.

Więcej informacji o programie Document Capture Pro Server można uzyskać od lokalnego przedstawiciela firmy Epson.

Konfigurowanie trybu serwera

Aby móc używać programu Document Capture Pro Server, należy wykonać następujące czynności.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Skanuj** > **Document Capture Pro**.
2. Wybierz ustawienie **Tryb serwera** dla opcji **Tryb**.
3. Wprowadź adres serwera z zainstalowanym programem Document Capture Pro Server w polu **Adres serwera**.

   Wprowadź od 2 do 255 znaków w formacie IPv4, IPv6, nazwy hosta lub FQDN. W przypadku formatu FQDN można używać znaków alfanumerycznych w kodowaniu ASCII (0x20–0x7E) oraz znaku „-” (z wyjątkiem początku i końca adresu).
4. Kliknij pozycję **OK**.

   Zostanie ponownie nawiązane połączenie z siecią i usługa będzie aktywna.

Konfigurowanie 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 rozległa sieć Bonjour. Jeżeli opcja zostanie włączona, skaner trzeba będzie zarejestrować na serwerze DNS, aby móc go wyszukiwać w segmencie sieci.
Włącz AirPrint	Funkcje Bonjour i AirPrint (usługa skanowania) są włączone.

Problemy podczas przygotowywania skanowania sieciowego

Wskazówki dotyczące rozwiązywania problemów

❏ Sprawdzanie 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.

❏ Sprawdzanie 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 poziomu skanera. Ponadto można też sprawdzać połączenie z poziomu 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 wygasł.

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 pozycję **Preferencje systemowe** > **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

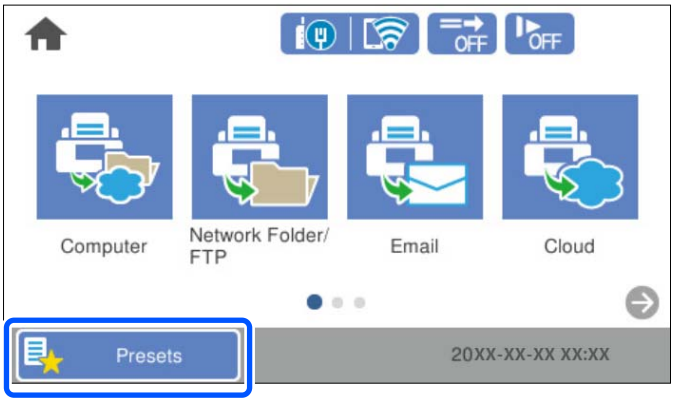
Można zarejestrować często używane ustawienia skanowania jako **Wstępne**. Można zarejestrować do 48 ustawień wstępnych.

Uwaga:

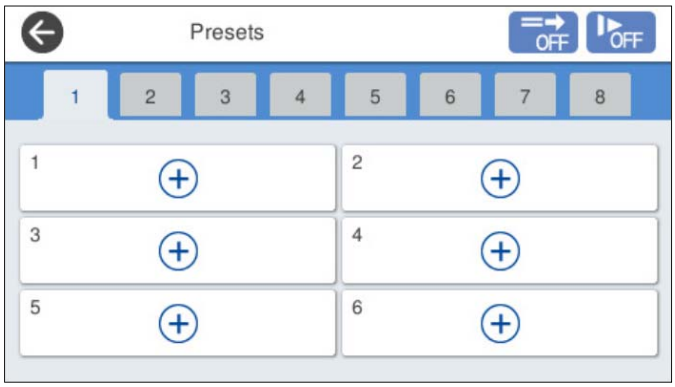
- *Istnieje możliwość zarejestrowania bieżących ustawień przez wybranie* ☆ *na ekranie rozpoczęcia skanowania.*
- ***Wstępne** można też rejestrować w aplikacji Web Config.*

  *Wybierz pozycje **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**.*

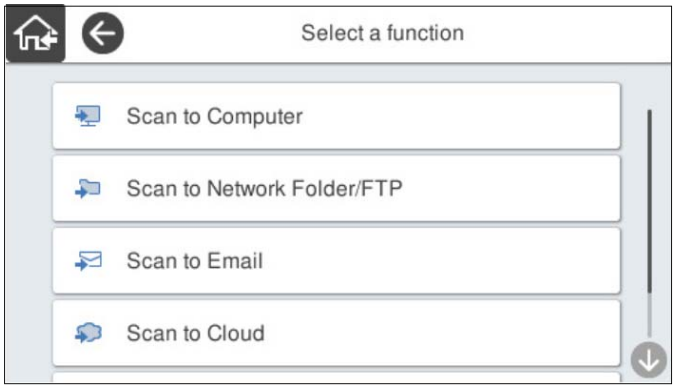
1. Na ekranie głównym panelu sterowania skanera wybierz pozycję **Wstępne**.



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.

  Gdy używane jest Document Capture Pro Server, to nawet jeżeli oprogramowanie jest ustawione na tryb potwierdzania zawartość zadania przed skanowaniem, aplikacja **Ustawienie Szybkie wysyłanie** w ustawieniach wstępnych skanera ma nad tym priorytet.
- ❏ **Zawartość**: sprawdzanie ustawień skanowania.

6. Wybierz pozycję **OK**.

Opcje menu Wstępne

Ustawienia zarejestrowane w ustawieniach wstępnych można zmieniać, wybierając pozycję > w każdych 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 80
- ❏ Dodaj ikonę: dodawanie ikon do utworzonych ustawień **Wstępne** lub przywracanie ikon usuniętych z ekranu.
  „Dodaj ikonę” na stronie 81
- ❏ Usuń ikonę: usuwanie ikon z ekranu głównego.
  „Usuń ikonę” na stronie 82
- ❏ Przenieś ikonę: zmiana kolejności wyświetlania ikon.
  „Przenieś ikonę” na stronie 83
- ❏ Przywróć wyświetlanie domyślnej ikony: przywrócenie domyślnych ustawień wyświetlania ekranu głównego.
- ❏ Tapeta: zmiana koloru tapety na ekranie głównym.

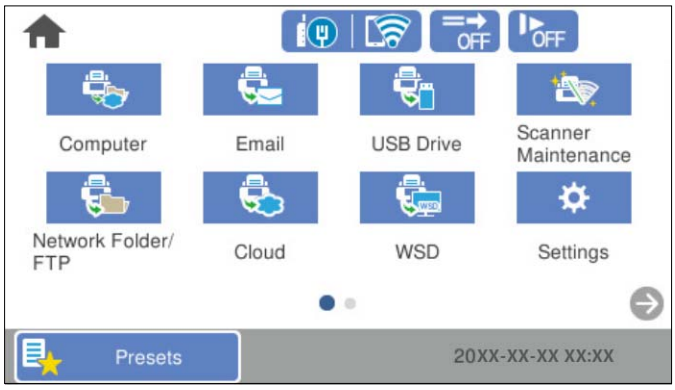
Zmiana ustawień Układ ekranu głównego

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

2. Wybierz pozycję **Linia** lub **Macierz**.

   Linia:

   Macierz:



3. Wybierz pozycję , aby wrócić i sprawdź ekran główny.

Dodaj ikonę

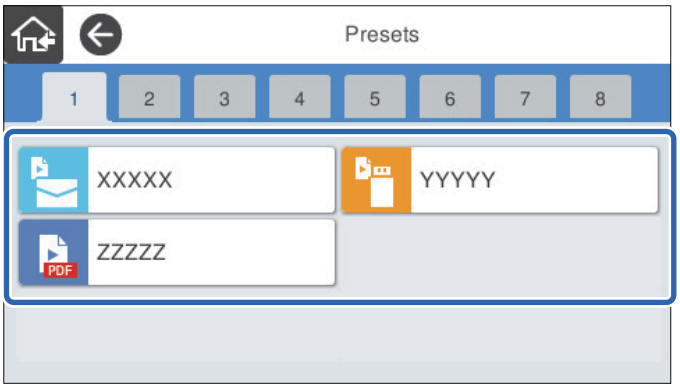
1. Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Dodaj ikonę**.

2. Wybierz pozycję **Wybór funkcji** lub **Wstępne**.

   ❏ Wybór funkcji: wyświetlanie domyślnych funkcji pokazanych na ekranie głównym.

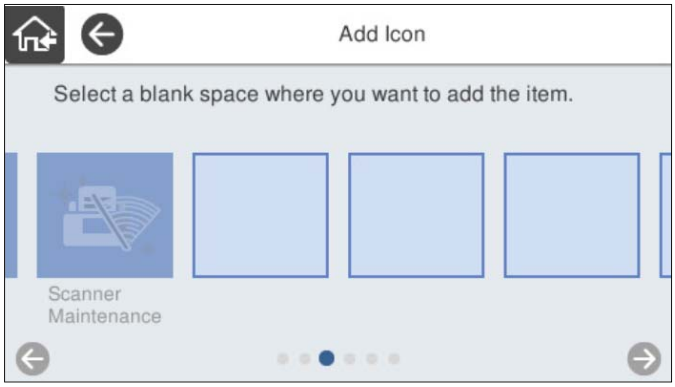
❏ Wstępne: wyświetlanie zarejestrowanych ustawień wstępnych.

3. Wybierz pozycję do dodania do ekranu głównego.



4. Wybierz puste miejsce, w którym pozycja ma być dodana.

   Aby dodać wiele ikon, powtórz czynności z kroków od 3 do 4.

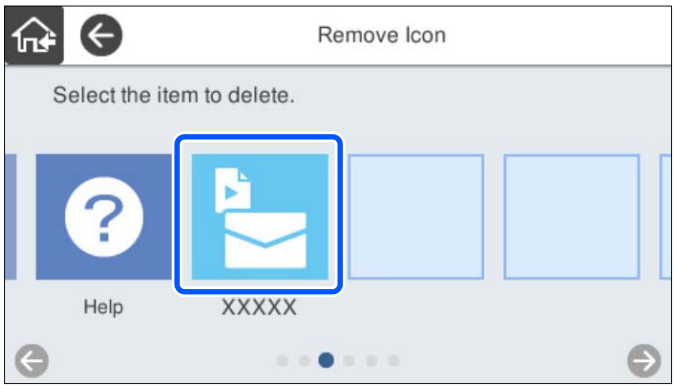


5. Wybierz pozycję , aby wrócić i sprawdź ekran główny.

Usuń ikonę

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

2. Wybierz ikonę do usunięcia.



3. Wybierz przycisk **Tak**, aby zakończyć.

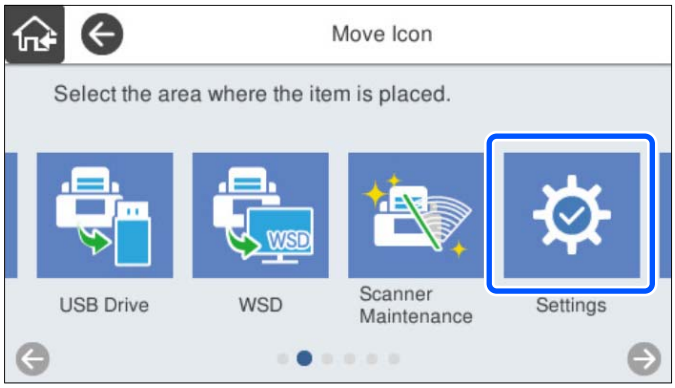
   Aby usunąć wiele ikon, powtórz czynności z kroków od 2 do 3.

4. Wybierz pozycję , aby wrócić i sprawdź ekran główny.

Przenieś ikonę

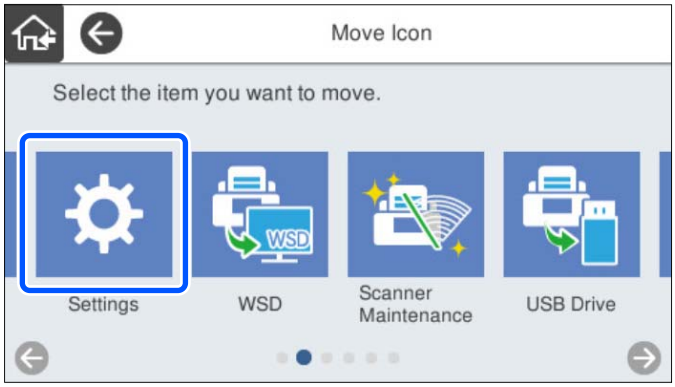
1. Na panelu sterowania skanera wybierz pozycje **Ustaw.** > **Edytuj Główny** > **Przenieś ikonę**.

2. Wybierz ikonę do przesunięcia.



3. Wybierz ramkę docelową.

   Jeśli inna ikona jest już w ramce docelowej, ikony zostaną zamienione.



4. Wybierz pozycję , aby wrócić i sprawdź ekran główny.

Podstawowe ustawienia zabezpieczeń

Wprowadzenie do funkcji zabezpieczeń produktu

W tym rozdziale opisano funkcje zabezpieczeń urządzeń firmy Epson.

Nazwa funkcji	Typ funkcji	Elementy do ustawienia	Działanie zabezpieczające
Konfiguracja 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.
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 86

➡ „Wyłączanie interfejsu zewnętrznego” na stronie 92

Ustawienia administratora

Konfigurowanie hasła administratora

Ustawiając hasło administratora, można uniemożliwić użytkownikom zmianę ustawień zarządzania systemem. Domyślne wartości są ustawiane w momencie zakupu. Zmień je w razie potrzeby.

Uwaga:
Poniżej przedstawiono domyślne wartości informacji o administratorze.

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

❏ *Hasło: numer seryjny skanera*

Aby znaleźć numer seryjny, należy sprawdzić etykietę z tyłu skanera.

Hasło administratora można ustawić i zmienić je przy użyciu aplikacji Web Config lub Epson Device Admin albo z panelu sterowania skanera. Korzystając z aplikacji Epson Device Admin, sprawdź przewodnik lub pomoc aplikacji Epson Device Admin.

Zmiana hasła administratora za pomocą aplikacji Web Config

Hasło administratora można zmienić w aplikacji Web Config.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie produktu** > **Zmień Hasło administratora**.

2. Wprowadź niezbędne informacje w polach **Aktualne hasło**, **Nazwa użytkownika**, **Nowe hasło** i **Potwierdź nowe hasło**.

   Wprowadź przynajmniej jeden znak w polu nowego hasła.

   Uwaga:
   Poniżej przedstawiono domyślne wartości informacji o administratorze.

   ❏ *Nazwa użytkownika: brak (puste)*

   ❏ *Hasło: numer seryjny skanera*

   Aby znaleźć numer seryjny, należy sprawdzić etykietę z tyłu skanera.

   > ***Ważne:***
   > *Zapamiętaj wprowadzone hasło administratora. W razie zapomnienia hasła nie będzie można go zresetować i trzeba będzie poprosić o pomoc pracowników serwisu.*

3. Wybierz pozycję **OK**.

Powiązane informacje

➡ „Uruchamianie aplikacji konfiguracyjnej w przeglądarce” na stronie 36

Zmiana hasła administratora na panelu sterowania

Możliwa jest zmiana hasła administratora z poziomu panelu sterowania skanera.

1. Na panelu sterowania skanera wybierz pozycję **Ustaw.**.

2. Wybierz pozycje **Administr. systemu** > **Ustawienia administratora**.

3. Wybierz pozycje **Hasło administratora** > **Zmień**.

4. Wprowadź bieżące hasło.

   Uwaga:
   Fabrycznie (wartość domyślna) hasło administratora jest ustawione na numer seryjny skanera.

   Aby znaleźć numer seryjny, należy sprawdzić etykietę z tyłu skanera.

5. Wprowadź nowe hasło.

   Wprowadź przynajmniej jeden znak.

> ***Ważne:***
> *Zapamiętaj wprowadzone hasło administratora. W razie zapomnienia hasła nie będzie można go zresetować i trzeba będzie poprosić o pomoc pracowników serwisu.*

6. Wprowadź nowe hasło ponownie, aby je potwierdzić.

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.

Uwaga:
Po włączeniu na skanerze opcji Ustawienia uwierzytelniania włączana jest również funkcja Zablokuj ustawienie panelu sterowania. Panelu sterowania nie można odblokować, gdy opcja Ustawienia uwierzytelniania jest włączona.

Funkcja Zablokuj ustawienie pozostaje włączona, nawet po wyłączeniu opcji Ustawienia uwierzytelniania. Aby ją wyłączyć, należy skonfigurować ustawienia z poziomu panelu sterowania lub aplikacji Web Config.

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 włączyć to ustawienie, przejdź do następnego kroku.

2. Wybierz pozycję **Ustaw.**.

3. Wybierz pozycje **Administr. systemu** > **Ustawienia administratora**.

4. Ustaw opcję **Zablokuj ustawienie** na **Wł.** lub **Wył.**.

Konfigurowanie funkcji Zablokuj ustawienie za pomocą aplikacji Web Config

1. Wybierz pozycje **Zarządzanie urządzeniem** > **Panel sterowania**.

2. Wybierz ustawienie **Wł.** lub **Wył.** dla opcji **Blokada panelu**.

3. Kliknij pozycję **OK**.

Powiązane informacje

➡ „Uruchamianie aplikacji konfiguracyjnej w przeglądarce” na stronie 36

Pozycje funkcji 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.	✓
	Ust. Data/godzina	✓
	Język/Language	✓/-*
	Klawiatura (Ta funkcja jest dostępna w wybranych regionach).	-
	Zak. czasu operacji	✓
	Poł. PC przez USB	✓
	Włącz zasilanie	✓
Ustawienia skanera		-
	Powoli	-
	Czas zatrz. po wykr. podw. podania	✓
	Funkcja DFDS	-
	Zabezp. papieru	✓
	Wykrywanie zabrudzeń szkła	✓
	Ponaddźw. 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	✓
	Tapeta	✓
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	-
	Przeglądaj opcje	-
	Opcje wyszukiwania	-
Administr. systemu		✓

Menu Ustaw.			**Zablokuj ustawienie**
	Menedżer Kontakty		✓
	Ustawienia administratora		✓
	Ograniczenia		✓
	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		-
	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 wałka			✓
	Ustawien alarmu licznika		✓
Ustawienia alarmu okresowego czyszczenia			✓

Menu Ustaw.		Zablokuj ustawienie
	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

Aby zalogować się na konto administratora z poziomu panelu sterowania skanera, można użyć jednej z następujących metod.

1. W prawym górnym rogu ekranu dotknij ikony  .
   - ❏ Jeśli opcja Ustawienia uwierzytelniania jest włączona, ikona jest wyświetlana na ekranie **Witamy** (ekran gotowości do uwierzytelniania).
   - ❏ Jeśli opcja Ustawienia uwierzytelniania jest wyłączona, ikona jest wyświetlana na ekranie głównym.
2. Dotknij pozycji **Tak** po wyświetleniu ekranu z monitem o potwierdzenie.
3. Wpisz hasło administratora.

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

Aby się wylogować, w prawym górnym rogu ekranu głównego dotknij pozycji  .

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 maja 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 wyłączonego 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 Menadżer urządzeń nie zmienią 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 konfiguracyjnej w przeglądarce” na stronie 36

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

➡ „Konfigurowanie serwera pocztowego” na stronie 42

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 konfiguracyjnej w przeglądarce” na stronie 36

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.

Rozwiązywanie problemów

Zapomnienie hasła administratora

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

Uwaga:
Poniżej przedstawiono wstępne wartości dla administratora Web Config.

❏ *Nazwa użytkownika: brak (puste)*

❏ *Hasło: numer seryjny skanera*

Aby znaleźć numer seryjny należy sprawdzić etykietę z tyłu skanera. Jeżeli przywróci się ustawienia fabryczne dla hasła administratora, zostanie ono zresetowane do wstępnej wartości.

Zaawansowane ustawienia bezpieczeństwa

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 użytkowania 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 przesyłać 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 98
- „Komunikacja SSL/TLS ze skanerem” na stronie 107
- „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 108
- „Podłączanie skanera do sieci IEEE802.1X” na stronie 120

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 konfiguracyjnej w przeglądarce” na stronie 36

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 określane, 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 określane, 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 określane, 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 102
➡ „Aktualizowanie certyfikatu z podpisem własnym” na stronie 105
➡ „Konfiguracja Certyfikat CA” na stronie 106

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

Aktualizowanie certyfikatu z podpisem własnym

Ponieważ Certyfikat podpisywany 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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36
➡ „Konfiguracja Certyfikat CA” na stronie 102
➡ „Konfiguracja Certyfikat CA” na stronie 106

Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP

Informacje o IPsec/Filtrowanie IP

Ruch można filtrować na postawie 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 konfiguracyjnej w przeglądarce” na stronie 36

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 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	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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguruj.

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 urząd certyfikacyjny, 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 urząd certyfikacyjny, 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 konfiguracyjnej w przeglądarce” na stronie 36
➡ „Konfiguracja Certyfikat CA” na stronie 102
➡ „Konfiguracja Certyfikat CA” na stronie 106

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 konfiguracyjnej w przeglądarce” na stronie 36

Opcje ustawień dla sieci IEEE 802.1X

Elementy	Ustawienia i objaśnienie	
IEEE802.1X (przewodowa sieć LAN)	Można włączać lub wyłączać ustawienia na stronie (**IEEE802.1X** > **Podstawowe**) dla sieci IEEE802.1X (przewodowa sieć LAN).	
IEEE802.1X (Wi-Fi)	Wyświetlany jest stan połączenia IEEE802.1X (Wi-Fi).	
Metoda połączenia	Wyświetlana jest metoda połączenia bieżącej sieci.	
Typ EAP	Wybierz metodę uwierzytelniania skanera na serwerze RADIUS.	
	EAP-TLS	Konieczne jest uzyskanie i zaimportowanie certyfikatu podpisanego przez urząd certyfikacji.
	PEAP-TLS	
	PEAP/MSCHAPv2	Konieczne jest skonfigurowanie hasła.
	EAP-TTLS	
ID użytkownika	Określ identyfikator, który będzie służył do uwierzytelniania na serwerze RADIUS. Wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E).	
Hasło	Określ hasło do uwierzytelniania skanera. Wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Jeśli serwer Windows pełni rolę serwera RADIUS, 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 jednobajtowych znaków ASCII (0x20 do 0x7E).	
Weryfikacja certyfikatu	Można włączyć weryfikację certyfikatu bez względu na metodę uwierzytelniania. Zaimportuj certyfikat w oknie **Certyfikat CA**.	
Nazwa użytkownika anonimowego	Jeśli dla opcji **Typ EAP** zostanie wybrane ustawienie **PEAP-TLS** lub **PEAP/MSCHAPv2**, zamiast identyfikatora użytkownika na potrzeby pierwszej fazy uwierzytelniania PEAP można wybrać nazwę anonimową. Wprowadź od 0 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E).	
Siła szyfrowania	Dostępne są następujące opcje.	
	Wys.	AES256/3DES
	Średnia	AES256/3DES/AES128/RC4

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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

➡ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 108

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 108

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 konfiguracyjnej w przeglądarce” na stronie 36

➡ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 108

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 108

Nie można uzyskać dostępu do skanera 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.

Połącz skaner i komputer, a następnie ponownie skonfiguruj połączenie IEEE 802.1X.

Powiązane informacje

➡ „Konfigurowanie sieci IEEE 802.1X” na stronie 120

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 103

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 105

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 102

Wyświetlane jest ostrzeżenie dotyczące certyfikatu cyfrowego

Komunikat	Przyczyna i sposób rozwiązania problemu
Wprowadź Certyfikat serwera.	**Przyczyna:** Nie wybrano pliku do zaimportowania. **Rozwiązanie:** Wybierz plik i kliknij przycisk **Importuj**.
Certyfikat CA 1 nie został wprowadzony.	**Przyczyna:** Nie podano pierwszego certyfikatu urzędu certyfikacji. Podano wyłącznie drugi certyfikat urzędu certyfikacji. **Rozwiązanie:** Najpierw należy zaimportować pierwszy certyfikat urzędu certyfikacji.
Poniżej nieprawidłowa wartość.	**Przyczyna:** Ścieżka dostępu do pliku i/lub hasło zawierają nieobsługiwane znaki. **Rozwiązanie:** Upewnij się, że wszystkie pozycje zostały podane prawidłowo.
Nieprawidłowa data i godzina.	**Przyczyna:** Nie ustawiono daty i godziny na skanerze. **Rozwiązanie:** Ustaw datę i godzinę za pomocą aplikacji Web Config lub EpsonNet Config.
Nieprawidłowe hasło.	**Przyczyna:** Podane hasło jest niezgodne z hasłem ustawionym dla certyfikatu urzędu certyfikacji. **Rozwiązanie:** Podaj prawidłowe hasło.
Nieprawidłowy plik.	**Przyczyna:** Importowany plik certyfikatu nie jest plikiem w formacie X509. **Rozwiązanie:** Upewnij się, że wybrano prawidłowy plik certyfikatu wysłany przez zaufany urząd certyfikacji.
	Przyczyna: Zaimportowany plik jest zbyt duży. Maksymalny dopuszczalny rozmiar pliku to 5 KB. **Rozwiązanie:** Jeśli wybrano prawidłowy plik, zachodzi podejrzenie uszkodzenia lub sfałszowania certyfikatu.
	Przyczyna: Łańcuch zawarty w certyfikacie jest nieprawidłowy. **Rozwiązanie:** Więcej informacji na temat certyfikatu zawiera serwis WWW urzędu certyfikacji.

Komunikat	Przyczyna i sposób rozwiązania problemu
Nie można użyć certyfikatu Certyfikat serwera, który zawiera więcej niż trzy certyfikaty Certyfikat CA.	**Przyczyna:** Plik certyfikatu w formacie PKCS#12 zawiera więcej niż 3 certyfikaty urzędów certyfikacji. **Rozwiązanie:** 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.
Certyfikat utracił ważność. Sprawdź, czy certyfikat jest ważny lub sprawdź ustawienie Data i godzina w produkcie.	**Przyczyna:** Certyfikat jest nieaktualny. **Rozwiązanie:** ❏ Jeśli certyfikat jest nieaktualny, pobierz i zaimportuj nowy certyfikat. ❏ Jeśli certyfikat jest aktualny, sprawdź, czy ustawienia daty i godziny na skanerze są prawidłowe.
Wymagany jest Klucz prywatny.	**Przyczyna:** Z certyfikatem nie jest powiązany klucz prywatny. **Rozwiązanie:** ❏ Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PEM/DER, należy wskazać plik klucza prywatnego. ❏ Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PKCS#12, należy utworzyć plik z kluczem prywatnym.
	Przyczyna: Ponownie zaimportowano certyfikat w formacie PEM/DER uzyskany na podstawie żądania CSR za pomocą aplikacji Web Config. **Rozwiązanie:** Jeśli na podstawie żądania CSR w aplikacji Web Config został pobrany certyfikat w formacie PEM/DER, certyfikat ten można zaimportować tylko raz.
Konfiguracja nie powiodła się.	**Przyczyna:** Nie można zakończyć konfiguracji, ponieważ nie udało się nawiązać komunikacji między skanerem a komputerem lub pliku nie można odczytać z powodu innego błędu. **Rozwiązanie:** Sprawdź podany plik oraz połączenie między drukarką a komputerem, po czym zaimportuj plik ponownie.

Powiązane informacje

➡ „Informacje o certyfikatach cyfrowych” na stronie 101

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.

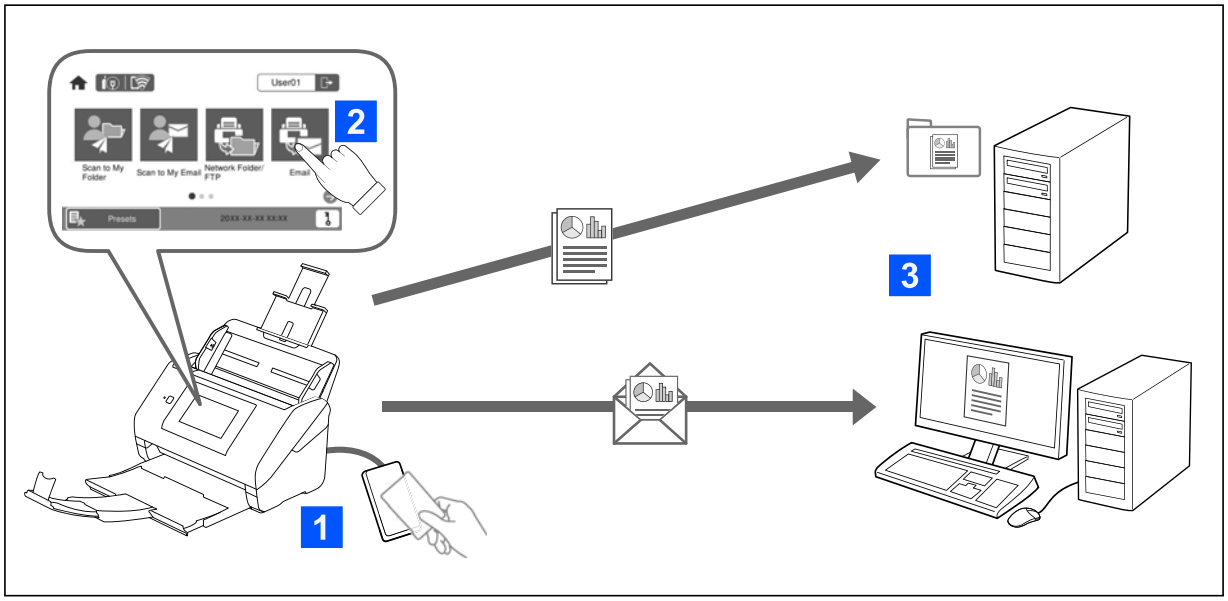
Powiązane informacje

➡ „Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 103

➡ „Usuwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 105

Ustawienia uwierzytelniania

Informacje o opcji Ustawienia uwierzytelniania



Jeśli opcja Ustawienia uwierzytelniania jest włączona, rozpoczęcie skanowania wymaga uwierzytelnienia użytkownika. Możliwe jest ustawienie metod skanowania, które mogą być używane przez każdego użytkownika, i zapobiegać wykonywaniu niezamierzonych operacji.

Można określić adres e-mail uwierzytelnionego użytkownika jako miejsce docelowe skanowania (Skanuj do Moja poczta) lub zapisywać dane każdego użytkownika w jego folderze osobistym (Skanuj do Mój folder). Dostępne są też inne metody skanowania.

Uwaga:

❏ *Nie można skanować z komputera ani urządzenia inteligentnego, gdy włączona jest opcja Ustawienia uwierzytelniania.*

❏ *Poza opcjami Ustawienia uwierzytelniania przedstawionymi w tym podręczniku można też stworzyć system uwierzytelniania wykorzystujący serwer uwierzytelniania. Użyj Document Capture Pro Server Authentication Edition (nazwa skrócona to Document Capture Pro Server AE), aby postawić taki system. Więcej informacji można uzyskać, kontaktując się z lokalnym biurem firmy Epson.*

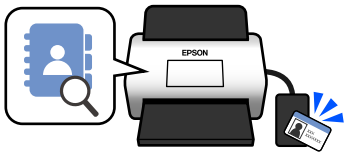
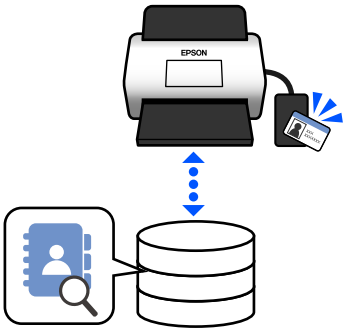
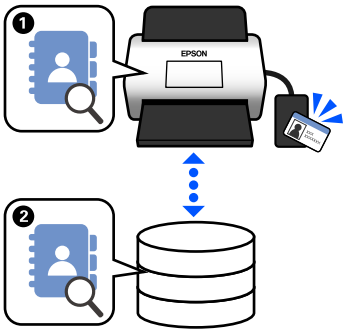
Funkcje dostępne dla Ustawienia uwierzytelniania

Funkcja skanowania na panelu sterowania	Ustawienia uwierzytelniania	
	Po włączeniu	Po wyłączeniu
Skanuj do Mój folder Umożliwia zapisywanie obrazów do folderu przypisanego do uwierzytelnionego użytkownika.	✓	-
Skanuj do Moja poczta Umożliwia wysyłanie obrazów na adres e-mail uwierzytelnionego użytkownika.	✓	-
Skan. do foldera siec./FTP Umożliwia zapisywanie obrazów w folderze sieciowym.	✓	✓

Funkcja skanowania na panelu sterowania	Ustawienia uwierzytelniania	
	Po włączeniu	Po wyłączeniu
Skanuj do komputera Umożliwia zapisywanie obrazów na podłączonym komputerze przy użyciu zadań utworzonych w aplikacji Document Capture Pro (Windows)/Document Capture (Mac OS). * Jeśli opcja Ustawienia uwierzytelniania jest włączona, można używać tylko zadań zarejestrowanych w **Wstępne**.	✓*	✓
Skanuj do e-mail Umożliwia wysyłanie obrazów na ustawiony adres e-mail.	✓	✓
Skanuj do chmury Umożliwia wysyłanie obrazów do ustawionej usługi chmury.	✓	✓
Skanuj do Napęd USB Umożliwia zapisywanie obrazów na dysku USB podłączonym do skanera. To ustawienie jest dostępne tylko, gdy do skanera nie jest podłączone urządzenie uwierzytelniające.	✓	✓
Skanuj do WSD Umożliwia zapisywanie obrazów na podłączonym komputerze przy użyciu funkcji WSD.	-	✓
Wstępne Można zarejestrować do 48 ustawień wstępnych funkcji skanowania. Można przydzielić do pięciu ustawień Wstępne do użytkowników zarejestrowanych w Lokalna DB. Przydzielone ustawienia Wstępne są dostępne tylko dla danego użytkownika. Ustawienia Wstępne, które nie zostały przydzielone do żadnego użytkownika, mogą być używane przez wszystkich użytkowników.	✓	✓

Informacje o aplikacji Sposób uwierzytelniania

Ten skaner udostępnia uwierzytelnianie za pomocą następujących metod bez potrzeby wdrażania serwera uwierzytelniania.

	Lokalna DB	LDAP	Lokalna DB i LDAP
Lokalizacja informacji o użytkowniku	**Pamięć skanera** Ta metoda uwierzytelniania umożliwia sprawdzanie informacji o użytkowniku zarejestrowanych na skanerze i porównanie ich z użytkownikiem, który korzysta z funkcji skanowania.	**Serwer LDAP*** Ta metoda uwierzytelnia umożliwia sprawdzanie informacji o użytkowniku na serwerze LDAP zsynchronizowanym ze skanerem. W pamięci podręcznej skanera może być tymczasowo przechowywanych do 300 pozycji informacji o użytkowniku z serwera LDAP, więc uwierzytelnianie może być wykonywane z tej pamięci, jeśli serwer LDAP będzie niedostępny. * Serwer dostarczający usługę katalogową, który może komunikować się z użyciem protokołu LDAP.	**Pamięć skanera i serwer LDAP** Najpierw sprawdzane są informacje o użytkowniku zarejestrowane na skanerze (❶), i w razie braku dopasowania, sprawdzane są informacje z serwera LDAP (❷).
			
Liczba zarejestrowanych użytkowników	50 (pamięć skanera)	Nieograniczone (serwer LDAP)	50 (pamięć skanera) Nieograniczone (serwer LDAP)
Pamięć podręczna skanera	-	300	Maks. 300 (50 banków pamięci podręcznej jest współdzielonych z ustawieniami Ustawienia użytkownika z Lokalna DB)
Metody logowania	Możliwe jest używanie dowolnych z poniższych metod. ❏ Przytrzymanie karty uwierzytelniającej lub wprowadzenie **ID użytkownika** i **Hasło** ❏ Przytrzymanie karty uwierzytelniającej lub wprowadzenie **Numer identyfikacyjny** ❏ Wprowadzenie **ID użytkownika** i **Hasło** ❏ Wprowadzenie **ID użytkownika** ❏ Wprowadzenie **Numer identyfikacyjny**		
Ograniczenia funkcji „Skanuj do”	Ustawiane indywidualnie dla każdego użytkownika	Takie same ustawienia dla wszystkich użytkowników LDAP	Użytkownicy Lokalna DB: ustawiane indywidualnie Użytkownicy LDAP: takie same ustawienia dla wszystkich użytkowników

	Lokalna DB	LDAP	Lokalna DB i LDAP
Przydzielanie Wstępne do użytkowników	Do pięciu na użytkownika	- (Nie można ustawiać indywidualnie)	Użytkownicy Lokalna DB: do pięciu na użytkownika Użytkownicy LDAP: -

Oprogramowanie do konfigurowania

Ustawienia konfiguruje się za pomocą aplikacji Web Config lub Epson Device Admin.

❏ W przypadku korzystania z aplikacji Web Config możliwe jest skonfigurowanie skanera wyłącznie za pomocą przeglądarki internetowej.

„Web Config” na stronie 36

❏ W przypadku korzystania z aplikacji Epson Device Admin można konfigurować wiele skanerów naraz za pomocą szablonu konfiguracji.

„Epson Device Admin” na stronie 37

Aktualizowanie oprogramowania układowego skanera

Przed włączeniem opcji Ustawienia uwierzytelniania należy zaktualizować oprogramowanie układowe skanera do najnowszej wersji. Zawczasu skaner należy połączyć z Internetem.

Ważne:

Podczas aktualizacji oprogramowania nie należy wyłączać komputera ani skanera.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Zarządzanie urządzeniem** > **Aktualizacja oprogramowania sprzętowego**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zaktualizować oprogramowanie układowe.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Na ekranie listy urządzeń wybierz pozycje **Home** > **Firmware** > **Update**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zaktualizować oprogramowanie układowe.

Uwaga:

Jeśli zainstalowana jest najnowsza wersja oprogramowania układowego, nie trzeba wykonywać aktualizacji.

Podłączanie i konfigurowanie urządzenia uwierzytelniającego

Aby podłączyć urządzenie uwierzytelniające, takie jak czytnik kart IC, i używać go, najpierw trzeba skonfigurować urządzenie. Nie jest to konieczne w przypadku braku urządzenia uwierzytelniającego.

Powiązane informacje

➡ „Podłączenie urządzenia uwierzytelniającego” na stronie 136
➡ „Ustawienia urządzenia uwierzytelniającego” na stronie 137

Lista zgodnych czytników kart

Producent nie gwarantuje, że czytniki wymienione na tej liście będą współpracować z urządzeniem.

Tak: obsługiwane (informacje identyfikacyjne można odczytywać za pomocą standardowych ustawień czytnika kart)

Nie: niezgodne

Producent	Model	Numer modelu	Karta uwierzytelniająca							Tryb
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Tak	Tak*1	Tak*1	Tak*1	Nie	Nie	Nie	Klawiatura
RF IDEAS	pcProx	RDR-7081BKU	Tak*1	Nie	Tak	Tak	Nie	Nie	Nie	Klawiatura
RF IDEAS	pcProx	RDR-7581AKU	Tak	Nie	Tak*1	Tak*1	Nie	Nie	Nie	Klawiatura
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nie	Nie	Tak	Tak	Nie	Nie	Nie	Klawiatura
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Tak	Nie	Tak	Tak	Tak	Tak	Tak	Klawiatura
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura

Producent	Model	Numer modelu	Karta uwierzytelniająca							Tryb
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ELATEC	TWN4 MultiTech 2 BLE-PI	T4LK-FB4BLZ-PI	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura
ELATEC	TWN4 Slim	T4QC-FC3B7	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Tak	Tak	Tak	Tak	Tak	Nie	Tak	Klawiatura[*1]
ACS	ACR122U	ACR122U	Nie	Nie	Tak[*2]	Tak[*2]	Tak	Nie	Tak[*2]	PC/SC
ACS	ACR1252	ACR1252	Nie	Nie	Tak[*2]	Tak[*2]	Tak	Tak	Tak[*2]	PC/SC
Sony	PaSoRi	RC-S330/S	Nie	Nie	Tak[*2]	Tak[*2]	Tak[*2]	Tak[*2]	Tak[*2]	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Nie	Nie	Tak[*2]	Tak[*2]	Tak[*2]	Tak[*2]	Tak[*2]	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura
DMZ	Leitor RFID Multi-125	DMZ087	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Klawiatura
DMZ	Leitor RFID Mifare	DMZ088	Nie	Nie	Tak	Tak	Nie	Nie	Nie	Klawiatura
DMZ	Biometric & RFID Reader	DMZ073	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Klawiatura

Producent	Model	Numer modelu	Karta uwierzytelniająca							Tryb
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
inepro	SCR708	SCR708	Tak*1	Tak*1	Tak*1	Tak*1	Tak*1	Tak*1	Tak*1	Klawiatura
Y Soft	YU03088 001	MU0388	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Nie	Nie	Tak	Tak	Nie	Nie	Tak	Klawiatura
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nie	Nie	Tak	Tak	Nie	Nie	Tak	Klawiatura
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Klawiatura
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Tak*1	Tak*1	Tak*1	Tak*1	Nie	Nie	Nie	Klawiatura
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Tak	Tak	Tak	Tak	Tak	Tak	Nie	Klawiatura

*1 Należy zmienić ustawienia czytnika kart za pomocą oprogramowania dostarczonego przez producenta czytnika kart.

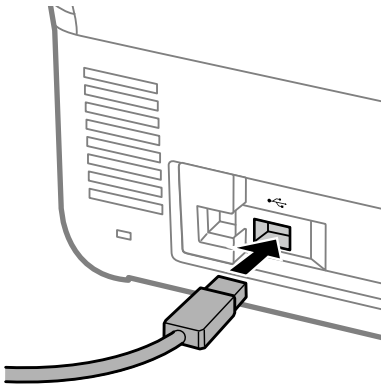
*2 Aby do uwierzytelniania używać danych z konkretnego obszaru karty innego niż standardowy identyfikator karty przez konfigurację ustawień produktu, należy skontaktować się z partnerem firmy Epson lub lokalnym przedstawicielem w celu uzyskania dodatkowych informacji dotyczących konfiguracji urządzenia.

Podłączenie urządzenia 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**.

Ustawienia urządzenia uwierzytelniającego

Ustaw format odczytu informacji uwierzytelniających pobieranych z karty uwierzytelniających.

Dostępne są poniższe metody odczytu dla urządzenia uwierzytelniającego.

❏ Odczyt określonego obszaru karty uwierzytelniającej, takiego jak numer pracownika lub identyfikator osobisty.

❏ Użycie informacji o karcie uwierzytelniającej z wyłączeniem UID (informacje o karcie uwierzytelniającej, takie jak numer seryjny).

Można użyć narzędzia do wygenerowania parametrów operacyjnych. Aby uzyskać szczegółowe informacje, skontaktuj się z dostawcą.

Uwaga:
Używanie kart uwierzytelnienia od różnych producentów:

Podczas korzystania z informacji o karcie UID (informacje identyfikacyjne karty, takie jak numer seryjny) można wprowadzać różne typy kart uwierzytelnienia. Nie można tego łączyć podczas korzystania z innych informacji karty.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Zarządzanie urządzeniem** > **Czytnik kart**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **Card Reader** z poziomu szablonu konfiguracji.

Pozycja	Objaśnienie
Vendor ID	Służy do ustawiania ID dostawcy urządzenia uwierzytelniającego ograniczającego użycie urządzenia w zakresie od 0000 do FFFF, używając 4 znaków alfanumerycznych. Ustawienie 0000 oznacza brak limitu.

Pozycja	Objaśnienie
Product ID	Służy do ustawiania ID produktu urządzenia uwierzytelniającego ograniczającego użycie urządzenia w zakresie od 0000 do FFFF, używając 4 znaków alfanumerycznych. Ustawienie 0000 oznacza brak limitu.
Parametr operacyjny	Służy do ustawiania parametru operacyjnego urządzenia uwierzytelniającego w zakresie od 0 do 8192 znaków. Dostępne są znaki A–Z, a–z, 0–9, +, /, =, spacji oraz nowego wiersza.
Czytnik kart	Służy do wyboru formatu konwersji dla urządzenia uwierzytelniającego. Można sprawdzać szczegóły formatu. Patrz łącze dostępne w opisie elementu.
Zapisz format ID karty uwierzytelniania	Służy do wyboru formatu konwersji informacji uwierzytelniających z karty ID. Można sprawdzać szczegóły formatu. Patrz łącze dostępne w opisie elementu.
Ustaw zakres ID karty	Służy do włączania określania pozycji odczytu.
Pozycja startowa tekstu	Służy do określania pozycji początkowej odczytu informacji identyfikacyjnych. Można określić wartość od 1 do 4096.
Liczba znaków	Służy do określania liczby znaków do odczytania od pozycji początkowej informacji identyfikacyjnych. Można określić wartość od 1 do 4096.

Rejestrowanie i ustawianie informacji

Konfigurowanie

Wprowadź niezbędne ustawienia w zależności od używanego ustawienia Sposób uwierzytelniania i metody skanowania.

Ważne:

Przed rozpoczęciem konfiguracji sprawdź, czy ustawienia godziny skanera są prawidłowe.

Jeśli ustawienie godziny jest nieprawidłowe, wyświetlany jest komunikat o błędzie „Licencja wygasła”, co może uniemożliwić skonfigurowanie skanera. Dodatkowo, aby korzystać z funkcji zabezpieczeń, takich jak komunikacja SSL/TLS czy też IPsec, konieczne jest prawidłowe ustawienie czasu. Procedura ustawiania czasu jest następująca.

❏ *Web Config: karta* ***Zarządzanie urządzeniem*** *>* ***Data i godzina*** *>* ***Data i godzina****.*

❏ *Panel sterowania skanera:* ***Ustaw.*** *>* ***Ustaw. podstawowe*** *>* ***Ust. Data/godzina****.*

Ustawienia	Lokalna DB	LDAP	Lokalna DB i LDAP
Włączanie uwierzytelniania Aby móc konfigurować ustawienia uwierzytelniania, trzeba włączyć uwierzytelnianie. „Włączanie uwierzytelniania” na stronie 139	✓	✓	✓
Ustawienia uwierzytelniania Możliwe jest skonfigurowanie opcji Sposób uwierzytelniania i sposobu uwierzytelniania użytkownika. „Ustawienia uwierzytelniania” na stronie 140	✓	✓	✓

Ustawienia	Lokalna DB	LDAP	Lokalna DB i LDAP
Rejestrowanie Ustawienia użytkownika Służy do rejestrowania ustawień każdego użytkownika. Można też dokonać zbiorczej rejestracji użytkowników, korzystając z pliku CSV. „Rejestrowanie Ustawienia użytkownika" na stronie 141	✓	–	✓
Synchronizowanie z Serwer LDAP Służy do konfigurowania ustawień synchronizowania z serwerem LDAP. „Synchronizowanie z Serwer LDAP" na stronie 148	–	✓	✓
Konfigurowanie Serwer e-mail Służy do konfigurowania ustawień serwera poczty e-mail. Ustawienia te konfiguruje się podczas korzystania z funkcji wymagających serwera poczty e-mail, takich jak Skanuj do Moja poczta. „Konfigurowanie serwera poczty e-mail" na stronie 152	✓	✓	✓
Konfigurowanie funkcji Skanuj do Mój folder Służy do ustawiania folderów miejsc docelowych. Ustawienia te konfiguruje się podczas korzystania z funkcji Skanuj do Mój folder. „Konfigurowanie funkcji Skanuj do Mój folder" na stronie 153	✓	✓	✓
Dostosuj funkcje One-touch Ustawienia te konfiguruje się podczas zmiany pozycji wyświetlanych na panelu sterowania skanera. Można wyświetlić tylko niezbędne ikony na panelu sterowania lub zmienić ich kolejność. „Dostosuj funkcje One-touch" na stronie 155	✓	✓	✓

Włączanie uwierzytelniania

Aby móc konfigurować ustawienia uwierzytelniania, trzeba włączyć uwierzytelnianie.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycję **Wł. (urządzenie/Serwer LDAP)** z obszaru **Zabezpieczenie produktu** > **Podstawowe** > **Uwierzytelnianie**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

W szablonie konfiguracji wybierz pozycję **Wł. (urządzenie/Serwer LDAP)** z **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Uwaga:
Po włączeniu na skanerze opcji Ustawienia uwierzytelniania włączana jest również funkcja Zablokuj ustawienie panelu sterowania. Panelu sterowania nie można odblokować, gdy opcja Ustawienia uwierzytelniania jest włączona.

Funkcja Zablokuj ustawienie pozostaje włączona, nawet po wyłączeniu opcji Ustawienia uwierzytelniania. Aby ją wyłączyć, należy skonfigurować ustawienia z poziomu panelu sterowania lub aplikacji Web Config.

Powiązane informacje

➡ „Konfigurowanie funkcji Zablokuj ustawienie z poziomu panelu sterowania” na stronie 88

➡ „Konfigurowanie funkcji Zablokuj ustawienie za pomocą aplikacji Web Config” na stronie 88

Ustawienia uwierzytelniania

Możliwe jest skonfigurowanie opcji Sposób uwierzytelniania i sposobu uwierzytelniania użytkownika.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Zabezpieczenie produktu** > **Ustawienia uwierzytelniania**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **Authentication Settings** z poziomu szablonu konfiguracji.

Pozycja	Objaśnienie
Sposób uwierzytelniania	Służy do wyboru ustawienia Sposób uwierzytelniania. ❏ Lokalna DB Uwierzytelnianie przy użyciu ustawień Ustawienia użytkownika zarejestrowanych na skanerze. Konieczna jest rejestracja użytkownika na skanerze. ❏ LDAP Uwierzytelnianie z wykorzystaniem informacji o użytkowniku przechowywanych na serwerze LDAP zsynchronizowanym ze skanerem. Wcześniej trzeba skonfigurować ustawienia serwera LDAP. ❏ Lokalna DB i LDAP Uwierzytelnianie z wykorzystaniem informacji o użytkowniku zarejestrowanych na skanerze lub przechowywanych na serwerze LDAP zsynchronizowanym ze skanerem. Trzeba zarejestrować użytkownika na skanerze i skonfigurować serwer LDAP.
Sposób uwierzytelniania użytkownika	Służy do wyboru metody uwierzytelniania użytkownika. ❏ Karta lub ID użytkownika i hasło Korzystanie z karty ID do uwierzytelniania użytkowników. W celu uwierzytelniania można również korzystać z ID użytkownika i hasła. ❏ ID użytkownika i hasło Korzystanie z ID użytkownika i hasła do uwierzytelniania użytkowników. Po wybraniu tej funkcji do uwierzytelniania nie można używać karty uwierzytelniającej. ❏ ID użytkownika Korzystanie wyłącznie z ID użytkownika do uwierzytelniania użytkowników. Nie ma potrzeby ustawiania hasła. ❏ Karta lub Numer identyfikacyjny Korzystanie z karty ID do uwierzytelniania użytkowników. Można również korzystać z opcji Numer identyfikacyjny. ❏ Numer identyfikacyjny Korzystanie wyłącznie z numeru ID do uwierzytelniania użytkowników.

Pozycja	Objaśnienie
Zezwól użytkownikom na rejestrowanie kart uwierzytelniających	Włącz tę opcję, aby umożliwić użytkownikom rejestrowanie kart uwierzytelniających w systemie. Jeśli w obszarze **Sposób uwierzytelniania** zostanie wybrane ustawienie **LDAP**, nie można ustawić tej opcji. Więcej informacji o sposobie rejestrowania kart uwierzytelniających przez użytkowników można znaleźć w rozdziale „Rejestrowanie karty uwierzytelniającej" w dokumencie *Przewodnik użytkownika*.
Minimalna ilość cyfr dla pola Numer identyfikacyjny	Służy do wyboru minimalnej liczby cyfr numeru ID.
Umieszczanie w pamięci cache dla uwierzytelnionych użytkowników LDAP	Podczas korzystania z uwierzytelniania serwera LDAP można ustawić, czy informacje o użytkowniku mają być też zapisywane w pamięci podręcznej.
Użyj informacji o użytkowniku w uwierzytelnianiu SMTP	Jeśli do uwierzytelniania używane są ID użytkownika i hasła, można ustawić, czy do uwierzytelniania SMTP mają być wykorzystane informacje o użytkowniku. Ten system wykorzystuje ID i hasło zalogowanego użytkownika.
Ograniczenia dla uwierzytelnionych użytkowników LDAP	W przypadku korzystania z serwera LDAP można określić funkcje, z których użytkownik może korzystać.

Rejestrowanie Ustawienia użytkownika

Możliwe jest rejestrowanie Ustawienia użytkownika używanych do uwierzytelniania użytkowników. Do rejestrowania można używać dowolnej z następujących metod.

❏ Rejestrowanie pojedynczych ustawień Ustawienia użytkownika (Web Config)

❏ Rejestrowanie wielu ustawień Ustawienia użytkownika partiami za pomocą pliku CSV (Web Config)

❏ Rejestrowanie ustawień User Settings partiami na wielu skanerach za pomocą szablonu konfiguracji (Epson Device Admin)

Powiązane informacje

➡ „Rejestrowanie indywidualne Ustawienia użytkownika (Web Config)" na stronie 141

➡ „Rejestrowanie wielu ustawień Ustawienia użytkownika za pomocą pliku CSV (Web Config)" na stronie 143

➡ „Rejestrowanie ustawień User Settings partiami na wielu skanerach (Epson Device Admin)" na stronie 146

Rejestrowanie indywidualne Ustawienia użytkownika (Web Config)

Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie produktu** > **Ustawienia użytkownika** > **Dodaj**, a następnie przejdź do Ustawienia użytkownika.

Pozycja	Objaśnienie
ID użytkownika	Służy do wprowadzania ID użytkownika używanego do uwierzytelniania o długości od 1 do 83 bajtów w kodowaniu Unicode (UTF-8). Ponieważ w ID użytkownika nie mają znaczenia wielkie i małe litery, można się zalogować z wykorzystaniem wielkich i małych liter.
Wyświetlanie nazwy użytkownika	Służy do wprowadzania wyświetlanej na panelu sterowania skanera nazwy użytkownika o długości maksymalnie 32 znaków w kodowaniu Unicode (UTF-16). Można pozostawić to pole puste.
Hasło	Służy do wprowadzania hasła do uwierzytelniania o długości maksymalnie 32 znaków w kodowaniu ASCII. Wielkość liter w haśle ma znaczenie. Pozostaw to pole puste w przypadku ustawienia opcji **Sposób uwierzytelniania użytkownika** na **ID użytkownika**.
ID karty uwierzytelniania	Służy do wprowadzania ID karty uwierzytelniającej o długości do 116 znaków w kodowaniu ASCII. Można pozostawić to pole puste. W przypadku przyznania zezwolenia za pomocą opcji **Zezwól użytkownikom na rejestrowanie kart uwierzytelniających** w obszarze **Ustawienia uwierzytelniania** odzwierciedlony zostanie rezultat zarejestrowany przez użytkowników.
Numer identyfikacyjny	Ta pozycja jest wyświetlana, gdy opcja **Ustawienia uwierzytelniania** > **Sposób uwierzytelniania użytkownika** jest ustawiona na **Karta lub Numer identyfikacyjny** lub **Numer identyfikacyjny**. Wprowadź numer wypadający między numerem ustawionym w opcji **Ustawienia uwierzytelniania** > **Minimalna ilość cyfr dla pola Numer identyfikacyjny** oraz o długości maksymalnie ośmiu cyfr.
Generuj automatycznie	Ta pozycja jest wyświetlana, gdy opcja **Ustawienia uwierzytelniania** > **Sposób uwierzytelniania użytkownika** jest ustawiona na **Karta lub Numer identyfikacyjny** lub **Numer identyfikacyjny**. Kliknij, aby automatycznie wygenerować numer ID o takiej samej liczbie cyfr, co wybrana w opcji **Minimalna ilość cyfr dla pola Numer identyfikacyjny**.
Dział	Służy do wprowadzania nazwy działu służącej do identyfikowania użytkownika o długości do 40 znaków w kodowaniu Unicode (UTF-16). Można pozostawić to pole puste.
Adres email	Służy do wprowadzania adresu e-mail o długości do 200 znaków w kodowaniu ASCII. Będzie on używany jako obiekt docelowy funkcji **Skanuj do Moja poczta**. Można pozostawić to pole puste.
Skanuj do Mój folder	Miejsca docelowe zapisu można ustawić osobno, jeśli opcja **Skanuj do Mój folder** > **Typ ustawienia** jest ustawiona na **Indywidualne**. Więcej informacji o pozycjach ustawień można znaleźć w następującym rozdziale. „Konfigurowanie funkcji Skanuj do Mój folder” na stronie 153
Ograniczenia	Możliwe jest ograniczenie funkcji wszystkich użytkowników. Wybierz funkcję, której używanie ma być dozwolone.

Pozycja	Objaśnienie
Wstępne	Dla wybranego użytkownika z ustawień Wstępne zapisanych na skanerze, można ustawić do pięciu wstępnych ustawień dostępnych wyłącznie dla niego. ❏ Ustawienia Wstępne przydzielone do użytkownika mogą być używane wyłącznie przez niego. Ustawienia Wstępne, które nie zostały przydzielone do żadnego użytkownika, mogą być używane przez wszystkich użytkowników. ❏ Jeśli użytkownik ma tylko jedne ustawienia Wstępne, są one automatycznie wczytywane po uwierzytelnieniu. Jeśli dostępnych jest wiele ustawień Wstępne, zostanie wyświetlona lista ustawień Wstępne. ❏ Nie można tworzyć ani wyświetlać ustawień Wstępne, które wykorzystują funkcje zablokowane przez opcję **Ograniczenia**.

Rejestrowanie wielu ustawień Ustawienia użytkownika za pomocą pliku CSV (Web Config)

Możliwe jest wprowadzenie ustawień każdego użytkownika w pliku CSV i zarejestrowanie ich partiami.

Tworzenie pliku CSV

Możliwe jest utworzenie pliku CSV w celu zaimportowania Ustawienia użytkownika.

Uwaga:
Po wcześniejszym skonfigurowaniu ustawień Ustawienia użytkownika, a następnie wyeksportowaniu ich do pliku sformatowanego (plik CSV), można używać ich do szybszego wprowadzania ustawień.

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie produktu** > **Ustawienia użytkownika**.

2. Kliknij pozycję **Eksportuj**.

3. Wybierz format pliku w obszarze **Format pliku**.

   Wyboru należy dokonać w oparciu o poniższe informacje.

Pozycja	Objaśnienie
CSV UTF-16 (rozdzielany tabulatorem)	Wybierz w przypadku edycji pliku za pomocą programu Microsoft Excel. Każdy parametr ujęto w „[ ]" (nawiasach kwadratowych). Wprowadź parametry w „[ ]". W przypadku aktualizowania pliku zalecamy jego nadpisanie. Jeśli zapisywany jest nowy plik, należy wybrać tekst Unicode (*.txt) jako format pliku.
CSV UTF-8 (rozdzielany przecinkiem)	Wybierz w przypadku edycji pliku za pomocą edytora tekstów lub makra bez użycia programu Microsoft Excel.
CSV UTF-8 (rozdzielany średnikiem)	

4. Kliknij pozycję **Eksportuj**.

5. Edytuj i zapisz ten plik CSV w aplikacji arkusza kalkulacyjnego, takiej jak Microsoft Excel, lub w edytorze tekstów.

> ***Ważne:***
> *Podczas edycji pliku nie zmieniaj kodowania ani informacji nagłówkowych.*

Pozycje ustawień pliku CSV

Pozycja	Ustawienia i objaśnienie
UserID	Służy do wprowadzania ID użytkownika używanego do uwierzytelniania o długości od 1 do 83 bajtów w kodowaniu Unicode.
UserName	Służy do wprowadzania wyświetlanej na panelu sterowania skanera nazwy użytkownika o długości maksymalnie 32 znaków w kodowaniu Unicode. Można pozostawić to pole puste.
Password	Służy do wprowadzania hasła do uwierzytelniania o długości maksymalnie 32 znaków w kodowaniu ASCII. Podczas importowania jest ono ustawiane jak hasło zamiast **EncPassword**. Pozostaw to pole puste w przypadku ustawienia opcji **Sposób uwierzytelniania użytkownika** na **ID użytkownika**. Podczas eksportowania to pole jest zawsze pozostawiane puste.
AuthenticationCardID	Służy do ustawiania wyniku odczytu karty uwierzytelniającej. W przypadku przyznania zezwolenia za pomocą opcji **Zezwól użytkownikom na rejestrowanie kart uwierzytelniających** w obszarze **Ustawienia uwierzytelniania** odzwierciedlony zostanie rezultat zarejestrowany przez użytkowników. Wprowadź maksymalnie 116 znaków w kodowaniu ASCII. Można pozostawić to pole puste.
IDNumber	Ta pozycja jest wyświetlana, gdy opcja **Ustawienia uwierzytelniania** > **Sposób uwierzytelniania użytkownika** jest ustawiona na **Karta lub Numer identyfikacyjny** lub **Numer identyfikacyjny**. Wprowadź numer wypadający między numerem ustawionym w opcji **Ustawienia uwierzytelniania** > **Minimalna ilość cyfr dla pola Numer identyfikacyjny** oraz o długości maksymalnie ośmiu cyfr. Nie można duplikować numeru ID. Jeśli zostanie on zduplikowany, podczas importowania pliku pojawi się alert z informacją o błędzie. Po pozostawieniu jako puste automatycznie przypisywany jest numer.
Department	Służy do wprowadzania arbitralnej nazwy działu używanej do rozróżniania użytkowników. Wprowadź maksymalnie 40 znaków w kodowaniu Unicode. Można pozostawić to pole puste.
MailAddress	Służy do ustawiania adresu e-mail użytkowników. Będzie on używany jako obiekt docelowy funkcji **Skanuj do Moja poczta**. Można używać A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Wprowadź do 200 znaków. Na początku ciągu nie można używać znaku „,” (przecinek). Można pozostawić to pole puste.
FolderProtocol	Służy do ustawiania typu funkcji Skanuj do Mój folder. Folder sieciowy/FTP (SMB): 0, FTP: 1

Pozycja	Ustawienia i objaśnienie
FolderPath	Służy do ustawiania miejsca docelowego zapisu funkcji Skanuj do Mój folder.
FolderUserName	Służy do ustawiania nazwy użytkownika dla funkcji Skanuj do Mój folder.
FolderPassword	Służy do ustawiania hasła do uwierzytelnienia folderu docelowego funkcji Skanuj do Mój folder o długości do 32 znaków ASCII. Podczas importowania jest ono ustawiane jak hasło zamiast **EncPassword**. Podczas eksportowania to pole jest zawsze pozostawiane puste.
FtpPassive	Służy do ustawiania trybu połączenia serwera FTP, jeśli opcja **Typ** jest ustawiona na **FTP** dla funkcji Skanuj do Mój folder. Tryb aktywny: 0, tryb pasywny: 1
FtpPort	Służy do ustawiania numeru portu do wysyłania danych skanowania na serwer FTP z zakresu od 0 do 65535, jeśli opcja **Typ** jest ustawiona na **FTP** dla funkcji Skanuj do Mój folder.
ScanToMemory	Służy do ustawiania ograniczeń funkcji Skanuj do Napęd USB. Niedozwolone: 0, dozwolone: 1
ScanToMail	Służy do ustawiania ograniczeń funkcji Skanowanie do wiadomości e-mail. Funkcję **Skanuj do Moja poczta** można ustawić, tylko jeśli opcja **Skanowanie do wiadomości e-mail** jest włączona. Niedozwolone: 0, dozwolone: 1
ScanToFolder	Służy do ustawiania ograniczeń funkcji Skanowanie do folderu sieciowego/FTP. Funkcję **Skanuj do Mój folder** można ustawić, tylko jeśli opcja **Skanowanie do folderu sieciowego/FTP** jest włączona. Niedozwolone: 0, dozwolone: 1
ScanToCloud	Służy do ustawiania ograniczeń funkcji Skanowanie do chmury. Niedozwolone: 0, dozwolone: 1
ScanToComputer	Służy do ustawiania ograniczeń funkcji Skanuj do komputera. Niedozwolone: 0, dozwolone: 1
PresetIndex	Służy do ustawiania Wstępne, które mają być powiązane z użytkownikiem. Skonfigurować można do pięciu, oddzielonych przecinkami numerów rejestracji Wstępne.
EncPassword	Podczas eksportowania ustawień użytkownika parametr ustawiony dla opcji **Password** jest szyfrowany, a następnie wartość ta jest kodowana za pomocą szyfru BASE64 i podawana jako wartość wyjściowa. W przypadku importowania z nowym hasłem ustawionym dla opcji **Password** wartość ta jest ignorowana. Jeśli pole **Password** jest puste, wartość ta jest wykorzystywana i hasło pozostaje takie samo, jak przed eksportowaniem.

Pozycja	Ustawienia i objaśnienie
EncFolderPassword	Podczas eksportowania parametr ustawiany dla opcji **FolderPassword** jest szyfrowany, a następnie wartość ta jest kodowana za pomocą BASE64 i podawana jako wartość wyjściowa. W przypadku importowania z nowym hasłem ustawionym dla opcji **FolderPassword** wartość ta jest ignorowana. Jeśli pole **FolderPassword** jest puste, wartość ta jest wykorzystywana i hasło pozostaje takie samo, jak przed eksportowaniem.

Importowanie pliku CSV

1. Uzyskaj dostęp do aplikacji Web Config i wybierz pozycje **Zabezpieczenie produktu** > **Ustawienia użytkownika**.
2. Kliknij pozycję **Importuj**.
3. Wybierz plik do zaimportowania.
4. Kliknij pozycję **Importuj**.
5. Po sprawdzeniu wyświetlanych informacji kliknij przycisk **OK**.

Rejestrowanie ustawień User Settings partiami na wielu skanerach (Epson Device Admin)

Ustawienia User Settings używane w Lokalna DB można rejestrować partiami, używając serwera LDAP lub pliku CSV/ENE.

Uwaga:
*ENE to format pliku binarnego dostarczany przez firmę Epson, który służy do szyfrowania i zapisywania danych **Contacts**, takich jak dane osobowe i Ustawienia użytkownika. Można go wyeksportować z poziomu aplikacji Epson Device Admin oraz ustawić hasło. Jest to przydatne, aby importować Ustawienia użytkownika z pliku kopii zapasowej.*

Importowanie z pliku CSV/ENE

1. Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **User Settings** z poziomu szablonu konfiguracji.
2. Kliknij pozycję **Import**.
3. Wybierz ustawienie **CSV or ENE File** w opcji **Import Source**.
4. Kliknij pozycję **Browse**.

   Zostanie wyświetlony ekran wyboru pliku.
5. Wybierz plik do zaimportowania, aby go otworzyć.

6. Wybierz metodę importu.

   ❏ Overwrite and Add: nadpisywanie, jeśli istnieje użytkownik o takim samym ID; dodanie nowego użytkownika, jeśli nie ma takiego ID.

   ❏ Replace All: zastąpienie wszystkiego ustawieniami użytkownika, które mają być zaimportowane.

7. Kliknij pozycję **Import**.

   Zostanie wyświetlony ekran potwierdzenia ustawień.

8. Kliknij pozycję **OK**.

   Zostaną wyświetlone wyniki weryfikacji.

   Uwaga:
   ❏ *Jeśli liczba importowanych ustawień użytkownika przekracza dopuszczalną liczbę importowanych ustawień, zostanie wyświetlony monit o usunięcie niektórych ustawień użytkownika. Należy usunąć nadmiarowe ustawienia użytkownika przed przystąpieniem do importowania.*

   ❏ *Zaznaczyć ustawienia użytkownika do usunięcia przed zaimportowaniem, a następnie kliknąć przycisk* ***Delete****.*

9. Kliknij pozycję **Import**.

   Ustawienia użytkownika są importowane do szablonu konfiguracji.

Importowanie z serwera LDAP

1. Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **User Settings** z poziomu szablonu konfiguracji.

2. Kliknij pozycję **Import**.

3. Wybierz ustawienie **LDAP** w opcji **Import Source**.

4. Kliknij pozycję **Settings**.

   Zostaną wyświetlone ustawienia **LDAP Server**.

   Uwaga:
   Te ustawienia serwera LDAP służą do importowania ustawień użytkownika z serwera LDAP. Zaimportowane (skopiowane) ustawienia użytkownika są używane do uwierzytelniania użytkowników przez skaner.

   Jeśli natomiast zostanie wybrana metoda uwierzytelniania ***LDAP*** *lub* ***Local DB and LDAP****, użytkownicy są uwierzytelniani przez serwer LDAP.*

5. Skonfiguruj poszczególne pozycje.

   Podczas importowania ustawień użytkownika z serwera LDAP, oprócz ustawień LDAP, można konfigurować następujące ustawienia.

   W przypadku pozostałych pozycji patrz część Informacje pokrewne.

Pozycja		Objaśnienie
LDAP Server Settings	LDAP Server Type	Służy do wyboru rodzaju serwera LDAP.

Pozycja			Objaśnienie
Search Settings	Search Filter		Służy do ustawiania tekstu używanego w filtrze wyszukiwania LDAP. Wybierz pozycję **Custom**, aby edytować tekst wyszukiwania.
	Options	Type	Służy do ustawiania typu miejsca docelowego zapisywania funkcji **Scan To My Folder**.
		Connection Mode	Jeśli opcja **Type** jest ustawiona na **FTP**, można ustawić tryb połączenia FTP.
		Port Number	Jeśli opcja **Type** jest ustawiona na **FTP**, można ustawić numer używanego portu.

6. Wykonaj wymagany test połączenia, klikając przycisk **Connection Test**.

   Zostanie pobranych 10 ustawień użytkownika z serwera LDAP i wyświetlonych na ekranie.

7. Kliknij pozycję **OK**.

8. Wybierz metodę importu.

   ❏ Overwrite and Add: nadpisywanie, jeśli istnieje użytkownik o takim samym ID; dodanie nowego użytkownika, jeśli nie ma takiego ID.

   ❏ Replace All: zastąpienie wszystkiego ustawieniami użytkownika, które mają być zaimportowane.

9. Kliknij pozycję **Import**.

   Zostanie wyświetlony ekran potwierdzenia ustawień.

10. Kliknij pozycję **OK**.

    Zostaną wyświetlone wyniki weryfikacji.

11. Kliknij pozycję **Import**.

    Ustawienia użytkownika są importowane do szablonu konfiguracji.

Powiązane informacje

➡ „Konfigurowanie serwera LDAP” na stronie 149

➡ „Konfigurowanie ustawień wyszukiwania serwera LDAP” na stronie 151

Synchronizowanie z Serwer LDAP

Umożliwia skonfigurowanie ustawień Serwer LDAP na skanerze.

W razie potrzeby trzeba skonfigurować ustawienia serwera podstawowego i pomocniczego.

Uwaga:
*Ustawienia **Serwer LDAP** są współdzielone z **Kontakty**.*

Dostępne usługi

Obsługiwane są następujące usługi katalogowe.

Nazwa usługi	Wersja
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Konfigurowanie serwera LDAP

Aby móc używać serwera LDAP, należy najpierw go skonfigurować.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Sieć** > **Serwer LDAP** > **Podstawowe (Serwer podstawowy)** lub **Podstawowe (Serwer pomocniczy)**.

Jeśli opcja **Sposób uwierzytelniania** zostanie ustawiona na **Uwierzytelnienie Kerberos**, wybierz pozycje **Sieć** > **Ustawienia Kerberos**, aby skonfigurować ustawienia serwera Kerberos.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Network** > **LDAP server** > **Server Settings (Primary Server)** lub **Server Settings (Secondary Server)** z poziomu szablonu konfiguracji.

Jeśli opcja **Sposób uwierzytelniania** zostanie ustawiona na **Uwierzytelnienie Kerberos**, wybierz pozycje **Network — Security** > **Ustawienia Kerberos**, aby skonfigurować ustawienia serwera Kerberos.

Pozycja	Ustawienia i objaśnienie
Użyj serwera LDAP	Wybierz pozycję **Użyj** lub **Nie należy używać**.
Adres serwera LDAP	Umożliwia wprowadzenie adresu serwera LDAP. Wprowadź od 1 do 255 znaków w formacie IPv4, IPv6 lub FQDN. W przypadku formatu FQDN można używać znaków alfanumerycznych ASCII (0x20–0x7E) oraz dywizu, jednak nie można go używać na początku i końcu adresu.
Numer portu serwera LDAP (Port number)	Umożliwia wprowadzenie numeru portu serwera LDAP w zakresie od 1 do 65535.
Bezpieczne połączenie	Określanie metody uwierzytelniania używanej przez skaner w celu uzyskania dostępu do serwera LDAP.
Weryfikacja certyfikatu	Certyfikat serwera LDAP jest uwierzytelniany po włączeniu tej opcji. Zaleca się ustawienie tej opcji na **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 s.

Pozycja	Ustawienia i objaśnienie
Sposób uwierzytelniania	Umożliwia wybór metody uwierzytelnienia. Jeśli zostanie wybrana metoda **Uwierzytelnienie Kerberos**, skonfiguruj wcześniej ustawienia serwera Kerberos. Aby móc używać funkcji Uwierzytelnienie Kerberos, należy zapewnić następujące środowisko. ❏ Zapewniona komunikacja między skanerem a serwerem DNS. ❏ Godzina skanera, serwera KDC i serwera uwierzytelniającego (serwera LDAP, serwera SMTP, serwera plików) są zsynchronizowane. ❏ 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	Umożliwia wprowadzenie nazwy 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 używane, zostaw puste pole.
Hasło	Umożliwia wprowadzenie hasła 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 używane, zostaw puste pole.

Ustawienia serwera Kerberos

Jeśli opcja **Sposób uwierzytelniania** jest ustawiona na **Uwierzytelnienie Kerberos**, trzeba skonfigurować ustawienia serwera Kerberos. Można zarejestrować do 10 ustawień Kerberos.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Sieć** > **Ustawienia Kerberos**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Network** > **Security** > **Ustawienia Kerberos** z poziomu szablonu konfiguracji.

Pozycja	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

Możliwe jest konfigurowanie atrybutów wyszukiwania ustawień użytkownika.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Sieć** > **Serwer LDAP** > **Ustawienia wyszukiwania (Uwierzytelnianie)**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** z poziomu szablonu konfiguracji.

Pozycja	Ustawienia i objaśnienie
Search Base (Distinguished Name)	Określanie pozycji początkowej wyszukiwania informacji o użytkowniku na serwerze 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
User ID Attribute	Określanie nazwy atrybutu do wyświetlania podczas wyszukiwania numeru ID. Wprowadź od 1 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Przykład: cn, uid
User name Display Attribute	Określanie nazwy atrybutu wyświetlanego jako nazwa użytkownika. Wprowadź od 0 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Możesz pozostawić to pole puste. Przykład: cn, name
Authentication Card ID Attribute	Określanie nazwy atrybutu wyświetlanego jako ID karty uwierzytelniającej. Wprowadź od 0 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Możesz pozostawić to pole puste. Przykład: cn, sn
ID Number Attribute	Określanie nazwy atrybutu do wyświetlania podczas wyszukiwania numeru ID. Wprowadź od 1 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Przykład: cn, id
Department Attribute	Określanie nazwy atrybutu wyświetlanego jako nazwa działu. Wprowadź od 0 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Możesz pozostawić to pole puste. Przykład: ou, ou-cl
Email Address Attribute	Określanie nazwy atrybutu do wyświetlania podczas wyszukiwania adresów e-mail. Wprowadź od 1 do 255 znaków w kodowaniu ASCII. Pierwszy znak powinien pochodzić ze zbioru a–z lub A–Z. Przykład: mail
Save To Attribute	Określanie nazwy atrybutu wskazującego miejsce docelowe funkcji Scan To My Folder. Wprowadź od 0 do 255 znaków w kodowaniu ASCII. Przykład: homeDirectory

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 niepowodzenie. Sprawdź ustawienia.	Ten komunikat jest wyświetlany w przypadku następujących sytuacji: ❏ Adres serwera LDAP lub numer portu są nieprawidłowe. ❏ Upłynął limit czasu. ❏ Wybrano ustawienie **Nie należy używać** dla opcji **Użyj serwera LDAP**. ❏ 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 niepowodzenie. 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: ❏ Wartości **Nazwa użytkownika** i/lub **Hasło** są niepoprawne. ❏ 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.

Konfigurowanie serwera poczty e-mail

W przypadku korzystania z funkcji **Skanuj do Moja poczta** trzeba skonfigurować serwer e-mail.

Uwaga:
*Funkcję **Skanuj do Moja poczta** można ustawić, tylko jeśli opcja **Skanowanie do wiadomości e-mail** jest włączona.*

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Sieć** > **Serwer e-mail** > **Podstawowe**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Common** > **Email Server** > **Mail Server Settings** z poziomu szablonu konfiguracji.

Pozycja	Ustawienia i objaśnienie	
Sposób uwierzytelniania	Określanie metody uwierzytelniania używanej 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	Wprowadzanie adresu e-mail nadawcy. 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	Wprowadzanie numeru portu w zakresie od 1 do 65535.	
Bezpieczne połączenie	Określanie bezpiecznej metody połączenia 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	Włączenie tej opcji powoduje uwierzytelnienie certyfikatu. Zaleca się ustawienie tej opcji na **Włącz**.	
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	Jeśli opcja **Sposób uwierzytelniania** jest ustawiona na **POP przed SMTP**, wprowadź numer portu. Wprowadź numer w zakresie od 1 do 65535.	

Konfigurowanie funkcji Skanuj do Mój folder

Możliwe jest zapisywanie zeskanowanych obrazów w folderze przypisanym do każdego użytkownika. Istnieją następujące opcje ustawiania dedykowanego folderu.

Uwaga:
*Funkcję **Scan To My Folder** można ustawić, tylko jeśli opcja **Skanowanie do folderu sieciowego/FTP** jest włączona.*

Ustawienie zapisu	Sposób uwierzytelniania	Lokalizacja ustawienia ścieżki folderu
Wybierz jeden folder sieciowy dla wszystkich opcji Ustawienia uwierzytelniania, aby automatycznie tworzyć folder osobisty w tym wybranym folderze. Tworzonym folderom są nadawane nazwy składające się z ID użytkownika.	❏ Lokalna DB ❏ LDAP ❏ Lokalna DB i LDAP	Skaner (ustawienia Skanuj do Mój folder)
Przypisanie innych folderów sieciowych indywidualnie do każdego użytkownika.	Lokalna DB	Skaner (Ustawienia użytkownika)
	LDAP	Atrybuty LDAP
	Lokalna DB i LDAP	Skaner (Ustawienia użytkownika) lub atrybuty LDAP

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Zabezpieczenie produktu** > **Skanowanie do folderu sieciowego/FTP**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **Skanowanie do folderu sieciowego/FTP** > **Scan to My Folder** z poziomu szablonu konfiguracji.

Pozycja		Objaśnienie
Zapisz do ustawienia	Typ ustawienia	❏ **Udostępnione**: Automatyczne tworzenie foldera o nazwie ID użytkownika poniżej ścieżki do foldera lub adresu URL określonego w **Zapisz do** i zapisywanie w tym folderze zeskanowanych obrazów. ❏ **Indywidualne**: Ustawianie miejsca docelowego zapisu wyników skanowania dla każdego użytkownika. Użytkowników Lokalna DB można ustawić w ustawieniach użytkownika. Użytkownicy LDAP używają lokalizacji zapisu pobieranej z atrybutów wyszukiwania serwera LDAP.
	Typ	Wybór protokołu transmisji zgodnie z miejscem docelowym skanowania. Folder sieciowy: **Folder sieciowy (SMB)** Serwer FTP: **FTP**
	Zapisz do	Określanie ścieżki lub adresu URL dotyczących ścieżki wyjściowej. Wprowadź maksymalnie 160 znaków w kodowaniu Unicode (UTF-16).
	Tryb połączenia	Konfiguruje się, jeśli opcja **Typ** jest ustawiona na **FTP**. Wybierz tryb połączenia z serwerem FTP.
	Numer portu	Konfiguruje się, jeśli opcja **Typ** jest ustawiona na **FTP**. Wpisz numer portu do przesyłania danych skanowania na serwer FTP, z zakresu od 0 do 65535.

Pozycja		Objaśnienie
Ustawienia uwierzytelniania	Typ ustawienia	Konfiguruje się, jeśli opcja **Typ ustawienia** jest ustawiona na **Indywidualne** w obszarze **Zapisz do ustawienia**. Ustaw wartości „Nazwa użytkownika" i „Hasło" używane do uzyskiwania dostępu do folderu. ❏ **Udostępnione**: Używanie wspólnych wartości **Nazwa użytkownika** i **Hasło** dla wszystkich użytkowników. ❏ **Indywidualne**: W przypadku użytkowników Lokalna DB opcje **Nazwa użytkownika** i **Hasło** ustawia się osobno w **Ustawienia użytkownika**. Użytkowników LDAP nie można konfigurować osobno. Wartości **Nazwa użytkownika** i **Hasło** ustawione w tej pozycji używane są jako partia.
	Nazwa użytkownika	Wprowadzanie nazwy użytkownika używanej do uzyskania dostępu do folderu docelowego danych skanowania. Wprowadź maksymalnie 30 znaków w kodowaniu Unicode (UTF-16). Ustawia się w przypadku korzystania z funkcji **Udostępnione** lub serwera LDAP.
	Hasło	Wprowadzanie hasła odpowiadającego **Nazwa użytkownika**. Wprowadź maksymalnie 20 znaków w kodowaniu Unicode (UTF-16). Ustawia się w przypadku korzystania z funkcji **Udostępnione** lub serwera LDAP.

Ograniczenie zmiany lokalizacji docelowej dla funkcji Skanowanie do folderu sieciowego/FTP

Pozycja	Objaśnienie
Zabrania ręcznego wprowadzania miejsca przeznaczenia	Gdy opcja ta jest włączona, użytkownik nie może zmienić domyślnej lokalizacji docelowej.

Dostosuj funkcje One-touch

Można wyświetlić tylko niezbędne ikony poprzez edycję układu ikony wyświetlonego na ekranie głównym dla panelu sterowania.

Konfigurowanie z poziomu aplikacji Web Config:

Wybierz pozycje **Zabezpieczenie produktu** > **Dostosuj funkcje One-touch**.

Konfigurowanie z poziomu aplikacji Epson Device Admin:

Wybierz pozycje **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** z poziomu szablonu konfiguracji.

Uwaga:
W następujących przypadkach ikony dla określonych funkcji są wyświetlane na ekranie głównym.

❏ *Po wybraniu funkcji, które nie są dozwolone z powodu ustawienia **Ograniczenia**.*

❏ *Gdy nie jest zarejestrowany adres e-mail dla zalogowanego użytkownika. (Skanuj do Moja poczta)*

❏ *Gdy nie jest ustawiony folder docelowy. (Skanuj do Mój folder)*

Pozycja	Objaśnienie
Maksymalna liczba funkcji na ekran	Służy do wyboru układu ikon wyświetlanych na panelu sterowania. Zmiany obrazu zgodnie z wybranym układem.
Ekran(y)	Służy do wyboru liczby stron.
Numer	Służy do wyboru funkcji, które mają być wyświetlane na każdej numerowanej pozycji.

Tworzenie raportów Job History za pomocą aplikacji Epson Device Admin

Możesz utworzyć raport Job History dla każdej grupy i każdego użytkownika, korzystając z aplikacji Epson Device Admin. Możliwe jest zapisanie do 3000 wpisów z historii użycia skanera. Raport można utworzyć poprzez wskazanie okresu czasu lub ustawienie regularnego harmonogramu.

Aby zapisać Job History w postaci raportu, z menu wstążki na ekranie Lista urządzeń wybierz pozycję **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices**.

Więcej informacji o tworzeniu raportu użytkownika można znaleźć w dokumentacji Epson Device Admin.

Pozycje uwzględniane w raporcie

W raporcie użytkownika można umieścić następujące pozycje.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Logowanie na konto administratora z poziomu panelu sterowania

Aby zalogować się na konto administratora z poziomu panelu sterowania skanera, można użyć jednej z następujących metod.

1. W prawym górnym rogu ekranu dotknij ikony  .
   - ❏ Jeśli opcja Ustawienia uwierzytelniania jest włączona, ikona jest wyświetlana na ekranie **Witamy** (ekran gotowości do uwierzytelniania).
   - ❏ Jeśli opcja Ustawienia uwierzytelniania jest wyłączona, ikona jest wyświetlana na ekranie głównym.
2. Dotknij pozycji **Tak** po wyświetleniu ekranu z monitem o potwierdzenie.
3. Wpisz hasło administratora.

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

Aby się wylogować, w prawym górnym rogu ekranu głównego dotknij pozycji  .

Wyłączanie Ustawienia uwierzytelniania

Funkcję Ustawienia uwierzytelniania można wyłączyć za pomocą aplikacji Web Config.

Uwaga:
Ustawienia Ustawienia użytkownika zarejestrowane na skanerze zostaną zapisane, nawet jeśli opcja Ustawienia uwierzytelniania jest wyłączona. Można usunąć je, przywracając ustawienia domyślne skanera.

1. Uzyskaj dostęp do aplikacji Web Config.
2. Wybierz pozycje **Zabezpieczenie produktu** > **Podstawowe** > **Uwierzytelnianie**.
3. Wybierz pozycję **Wył.**.
4. Kliknij pozycję **Dalej**.
5. Kliknij pozycję **OK**.

Uwaga:
Funkcja Zablokuj ustawienie pozostaje włączona, nawet po wyłączeniu opcji Ustawienia uwierzytelniania. Aby ją wyłączyć, należy skonfigurować ustawienia z poziomu panelu sterowania lub aplikacji Web Config.

Powiązane informacje

➡ „Konfigurowanie funkcji Zablokuj ustawienie z poziomu panelu sterowania” na stronie 88
➡ „Konfigurowanie funkcji Zablokuj ustawienie za pomocą aplikacji Web Config” na stronie 88

Usuwanie informacji Ustawienia uwierzytelniania (Przywr. ust. domyśl.)

Aby usunąć wszystkie informacje Ustawienia uwierzytelniania (Czytnik kart, Sposób uwierzytelniania, Ustawienia użytkownika itd.), przywróć wartości domyślne wszystkich ustawień skanera.

Na panelu sterowania wybierz pozycje **Ustaw.** > **Administr. systemu** > **Przywr. ust. domyśl.** > **Wszystkie ustawienia**.

Ważne:
Usunięte zostaną również wszystkie kontakty i inne ustawienia sieciowe. Usuniętych ustawień nie można przywrócić.

Rozwiązywanie problemów

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 są obsługiwane.

Konserwacja

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.

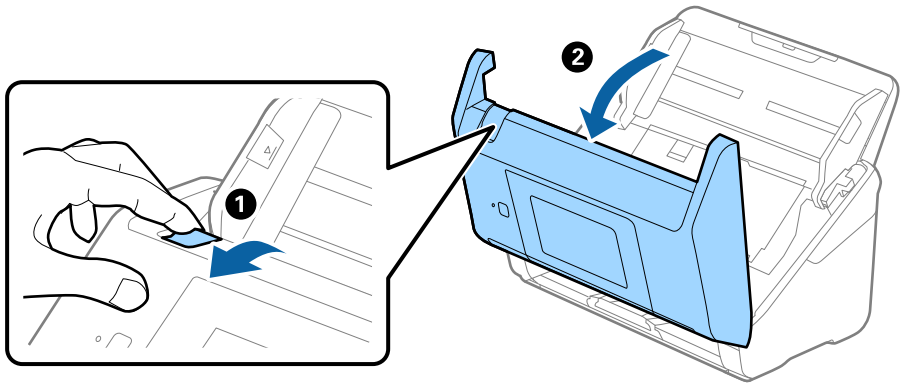
Jeżeli na powierzchni są zabrudzenia trudne do usunięcia, należy użyć oryginalnego zestawu czyszczącego firmy Epson. Aby usunąć plamy, na szmatkę nałożyć małą ilość środka czyszczącego.

Ważne:

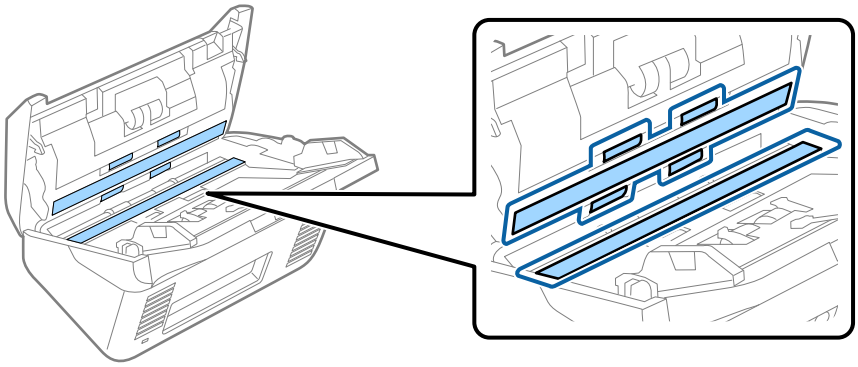
- ❏ *Do czyszczenia skanera nigdy nie należy używać alkoholu, rozcieńczalnika ani żadnego rozpuszczalnika powodującego korozję. Używanie takich substancji może spowodować deformację lub odbarwienie urządzenia.*
- ❏ *Pod żadnym pozorem nie spryskiwać skanera jakimkolwiek płynem lub smarem. Może to doprowadzić 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.

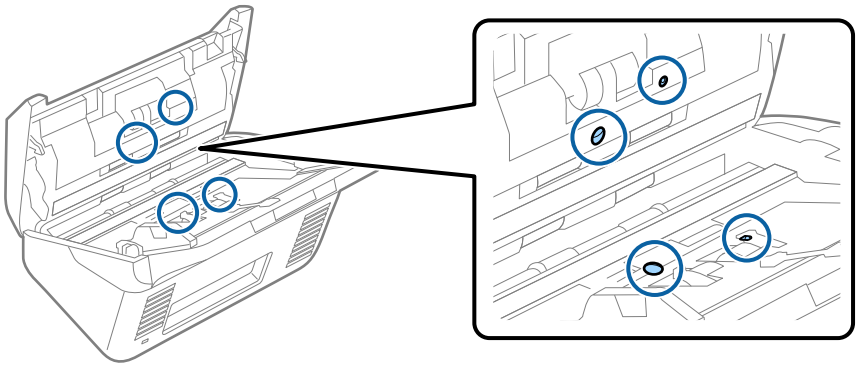


4. Za pomocą miękkiej szmatki lub oryginalnego zestawu czyszczącego firmy Epson wytrzyj wszelkie plamy na plastikowej rolce i szybie skanera na dole wewnątrz pokrywy skanera.



> ***Ważne:***
>
> - *Nie należy przykładać zbyt dużej siły do szyby skanera.*
> - *Nie używaj szczotki ani twardego narzędzia. Jakiekolwiek zarysowania na szybie mogą pogorszyć jakość skanów.*
> - *Nie należy rozpylać środków do czyszczenia bezpośrednio na szybę skanera.*

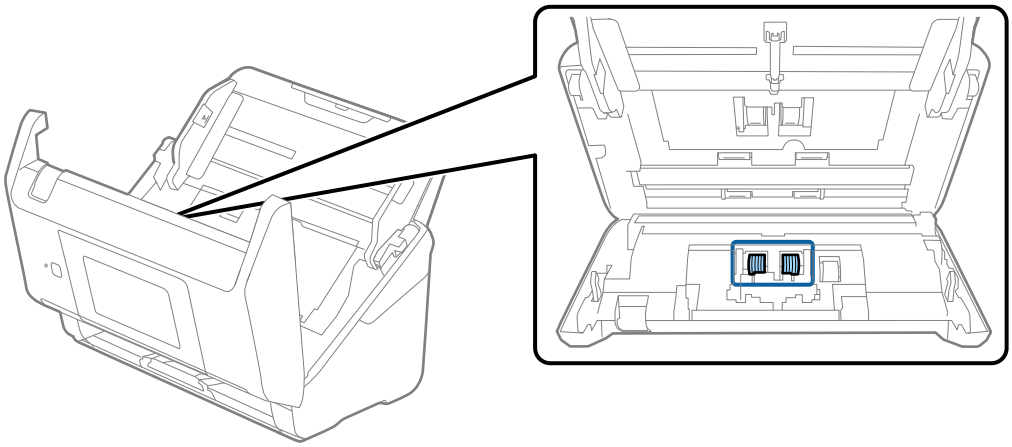
5. Wszelkie plamy na czujnikach wycieraj bawełnianym wacikiem.



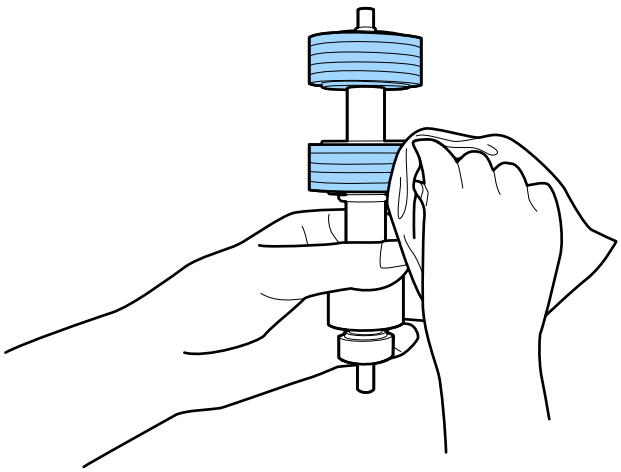
> ***Ważne:***
> *Wacika nie nasączaj cieczami, np. płynem czyszczącym.*

6. Zdejmij pokrywę, a następnie wyjmij rolkę rozdzielającą.

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



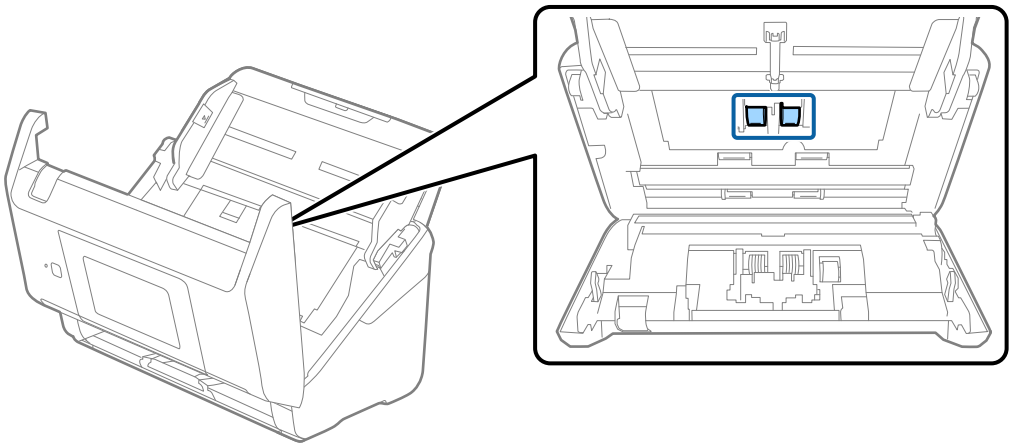
7. Zetrzeć pył lub kurz z rolki rozdzielającej, używając oryginalnego zestawu czyszczącego firmy Epson lub miękkiej, wilgotnej szmatki.



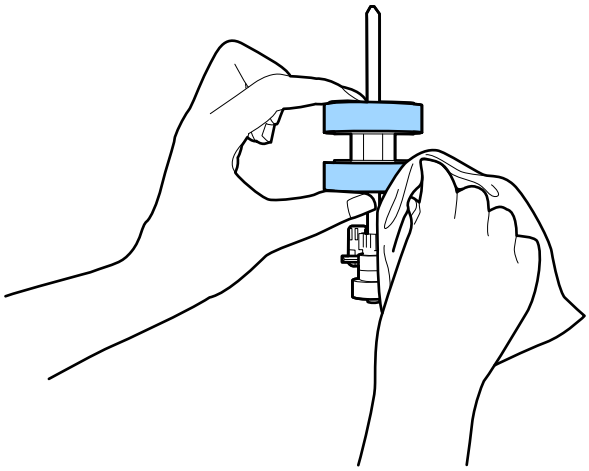
> ***Ważne:***
> *Do czyszczenia rolki używać tylko oryginalnego zestawu czyszczącego firmy Epson lub miękkiej, wilgotnej szmatki. Sucha szmatka może spowodować uszkodzenie powierzchni rolki.*

8. Zdjąć pokrywę, a następnie wyjąć rolkę podającą.

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



9. Zetrzeć pył lub kurz z rolki podającej, używając oryginalnego zestawu czyszczącego firmy Epson lub miękkiej, wilgotnej szmatki.



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

10. Zamknąć pokrywę skanera.

11. Podłącz wtyczkę zasilacza AC do gniazda elektrycznego, a następnie włącz skaner.

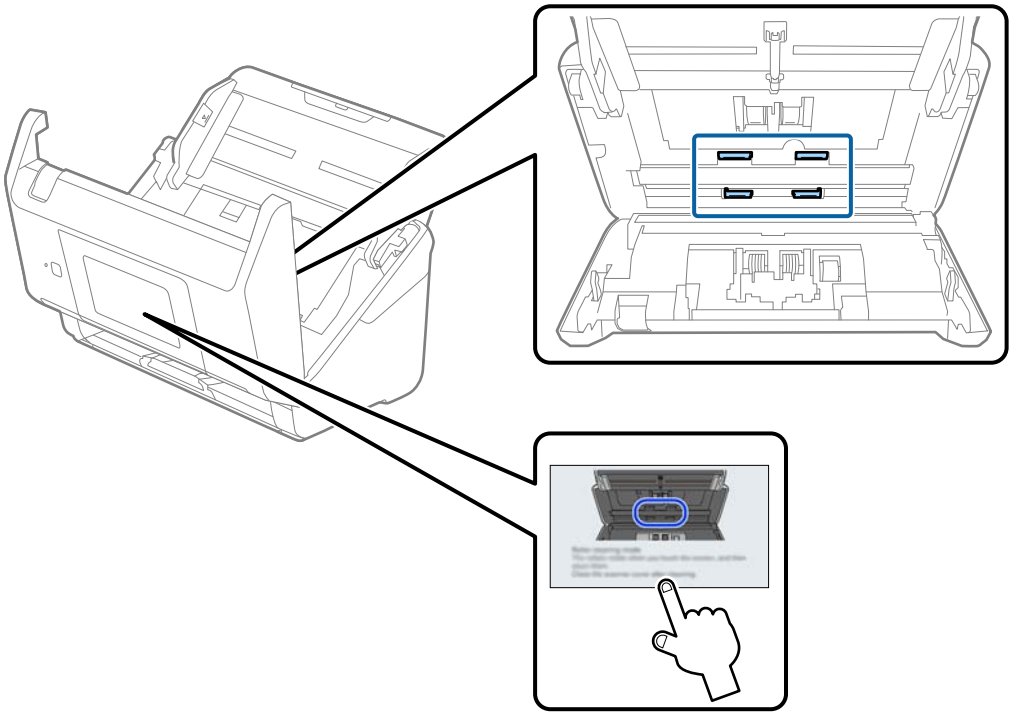
12. Na ekranie głównym wybrać pozycję **Konserwacja skanera**.

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.



> ***Przestroga:***
>
> *Podczas obracania rolek zachować ostrożność, aby nie pochwycić nimi dłoni ani włosów. Mogłoby to doprowadzić do obrażeń ciała.*

16. Zamknąć pokrywę skanera.

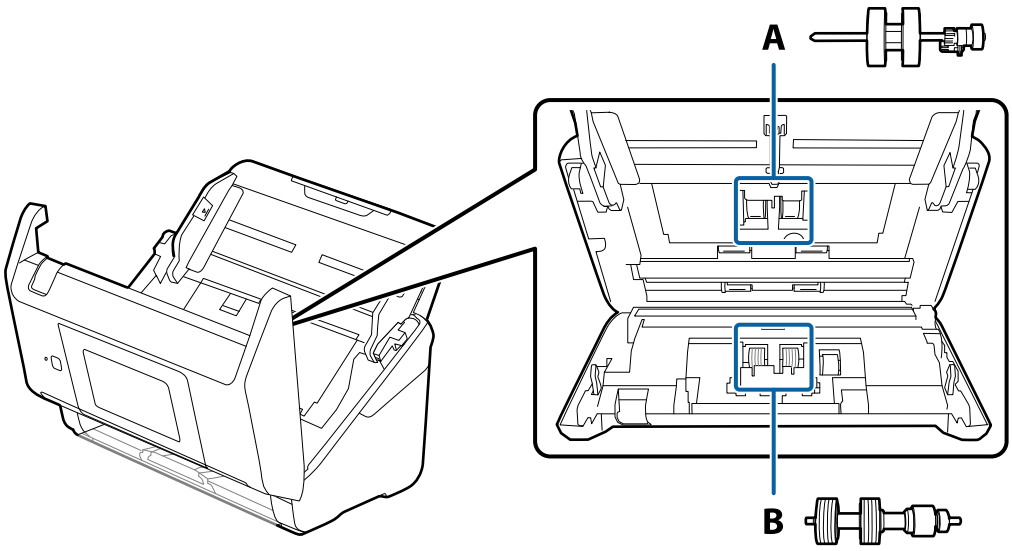
    Tryb czyszczenia rolek zostanie wyłączony.

Powiązane informacje

➡ „Wymiana zestawu montażowego rolek” na stronie 165

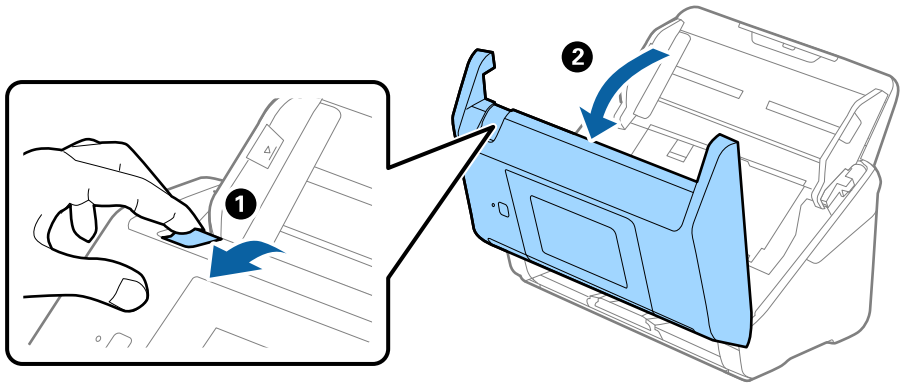
Wymiana zestawu montażowego rolek

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.

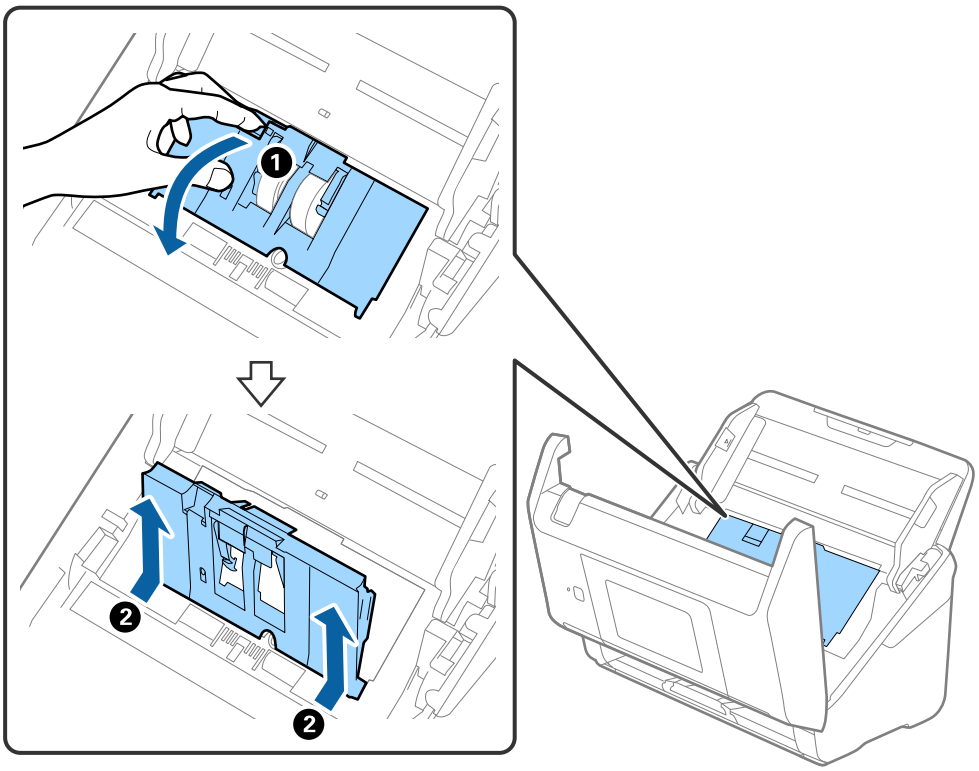


A: wałek odbierający, B: wałek rozdzielający

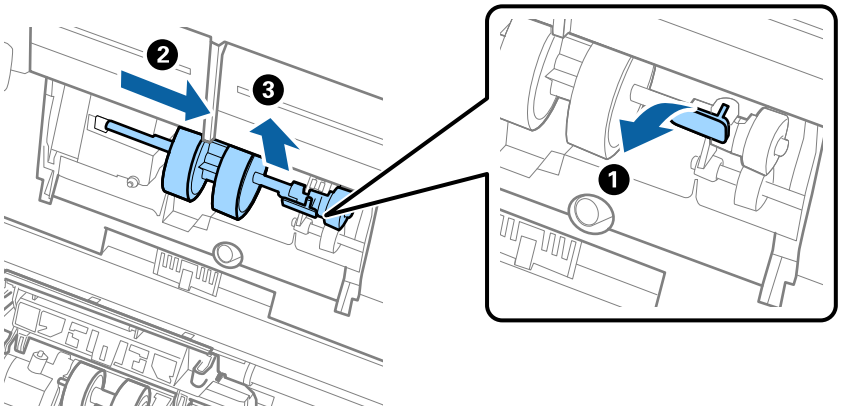
1. Naciśnij przycisk ⏻, aby wyłączyć skaner.
2. Odłącz zasilacz AC od skanera.
3. Pociągnij dźwignię i otwórz pokrywę skanera.



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



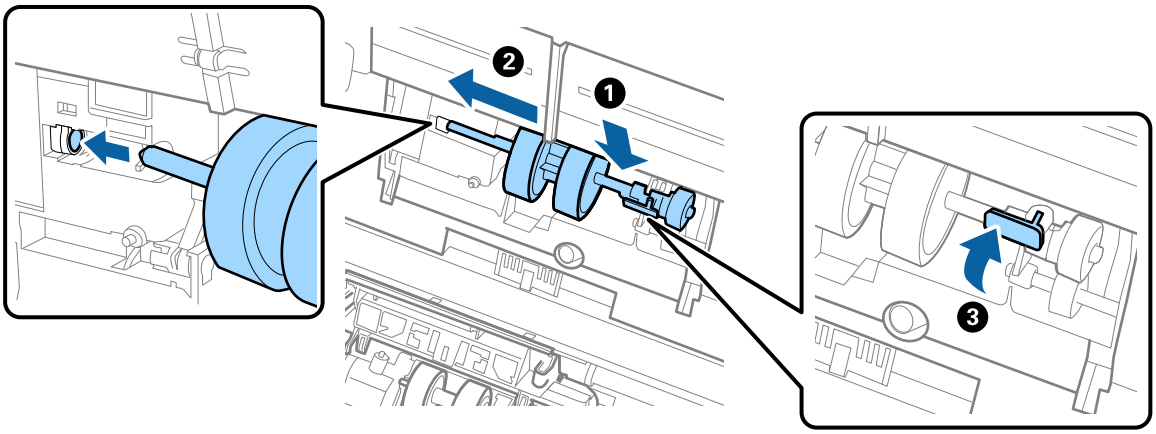
5. Pociągnij w dół osprzęt osi rolki, a następnie wysuń i wyjmij zainstalowane rolki podające.



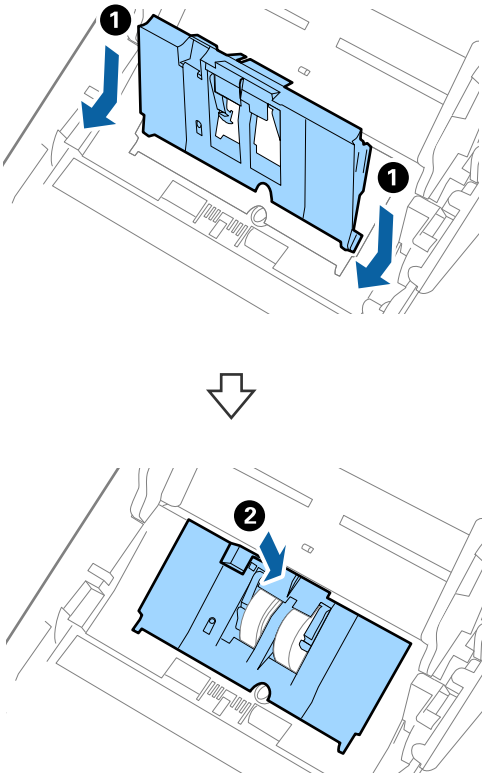
Ważne:

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

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

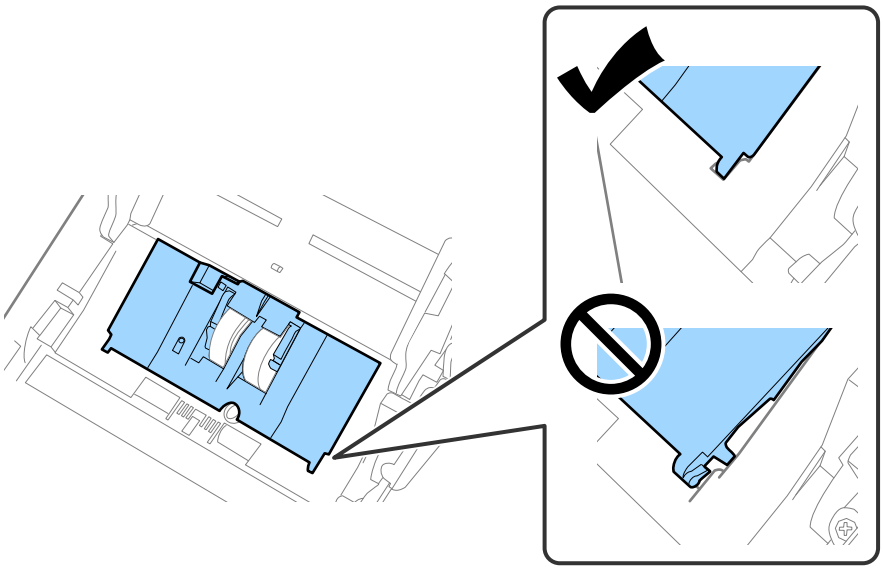


7. Umieść krawędź pokrywy rolki podającej w szczelinie i wsuń ją. Dokładnie zamknij pokrywę.

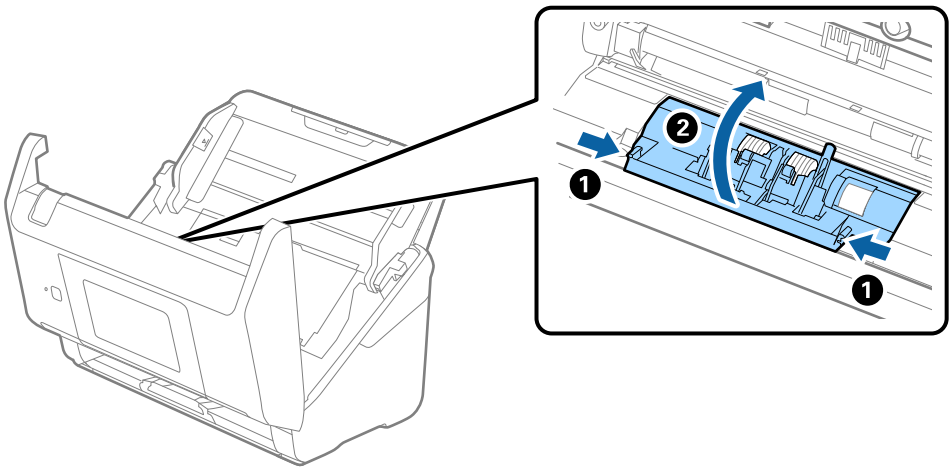


Ważne:

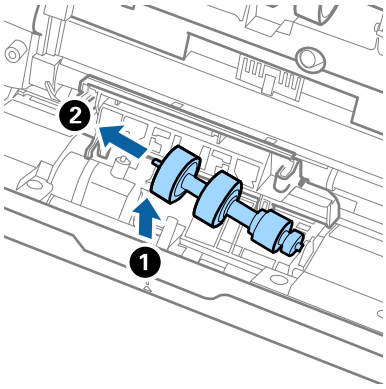
- ❏ *Upewnij się, czy pokrywa rolki odbierającej jest zamknięta.*
- ❏ *Jeżeli pokrywa trudno się domyka, sprawdź poprawność zainstalowania rolek podających.*
- ❏ *Nie instaluj pokrywy, kiedy jest podniesiona.*



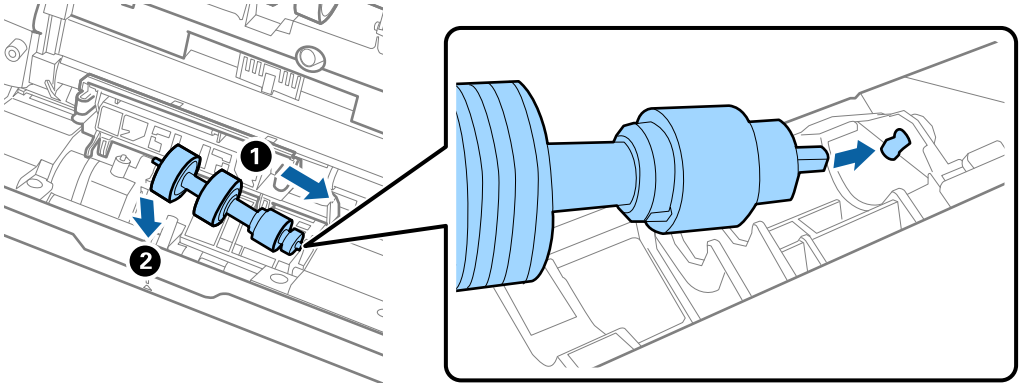
8. Popchnij zaczepy na obu końcach pokrywy wałka rozdzielającego w celu jego otwarcia.



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. Podłącz wtyczkę zasilacza AC do gniazda elektrycznego, a następnie włącz skaner.

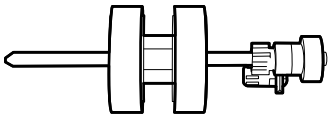
14. Wyzeruj liczbę skanów na panelu sterowania.

Uwaga:
Zutylizuj wałek odbierający i wałek rozdzielający zgodnie z lokalnie obowiązującymi zasadami i przepisami. Nie wolno ich rozmontowywać.

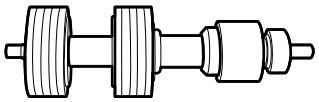
Kody zestawu montażowego wałka

Części (wałek odbierający i wałek rozdzielający) 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



B



A: wałek odbierający, B: wałek rozdzielający

Nazwa części	Kody	Cykl eksploatacji
Zestaw montażowy wałka	B12B819671 B12B819681 (tylko Indie)	200,000*

* Liczbę tą 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

Umożliwia zerowanie liczby skanowań po wymianie zestawu montażowego rolki.

1. Na ekranie głównym wybierz pozycje **Ustaw.** > **Dane urządzenia** > **Resetuj liczbę skanowań** > **Liczba skanów po wymianie rolki**.

2. Dotknij pozycji **Tak**.

Powiązane informacje

➡ „Wymiana zestawu montażowego rolek” na stronie 165

Oszczędzanie energii

Kiedy skaner nie wykonuje żadnych czynności, można oszczędzać energię przez skorzystanie z trybu wstrzymania lub automatycznego wyłączenia. Można ustawić okres czasu, po którym skaner przejdzie w tryb wstrzymania lub wyłączy się automatycznie. Jakiekolwiek zwiększenie będzie miało wpływ na wydajność energetyczną produktu. Przed wprowadzeniem jakichkolwiek zmian weź pod uwagę wpływ na środowisko.

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

2. Wybierz pozycję **Ustaw. podstawowe**.

3. Wybierz **Ustaw. wyłączania**, a następnie skonfiguruj odpowiednie ustawienia.

   Uwaga:
   Dostępne funkcje mogą się różnić w zależności od miejsca zakupu.

Przenoszenie skanera

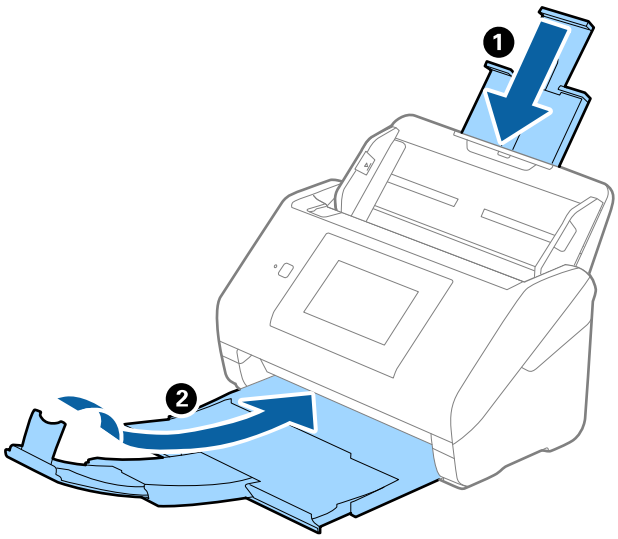
Na potrzeby przewiezienia skanera podczas przeprowadzki lub do naprawy zapakować go, wykonując niżej podane czynności.

1. Nacisnąć przycisk ⏻ w celu wyłączenia skanera.

2. Odłączyć zasilacz.

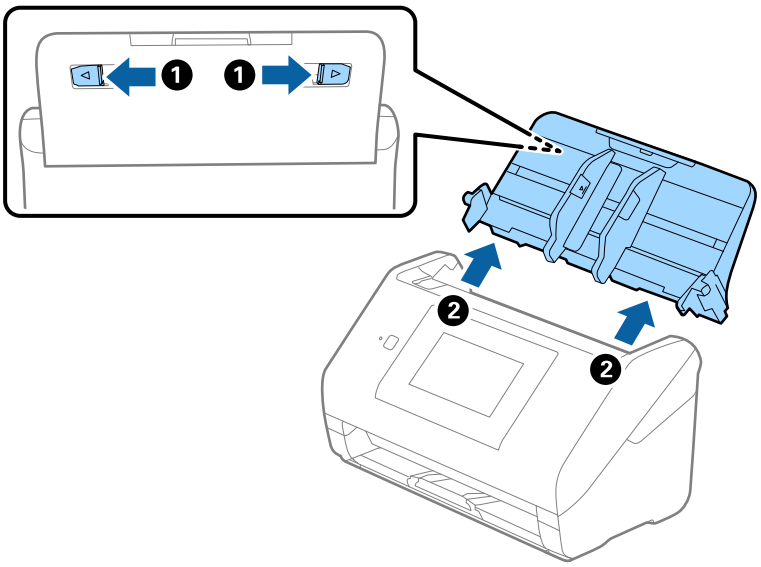
3. Odłączyć kable i zdjąć urządzenia.

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. Obłożyć 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 pozycje **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 konfiguracyjnej w przeglądarce” na stronie 36

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 konfiguracyjnej w przeglądarce” na stronie 36

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:

*Jeżeli wybrana i uruchomiona zostanie opcja **Wszystkie ustawienia**, wszystkie dane ustawień zarejestrowane w skanerze, w tym kontakty i ustawienia uwierzytelniania użytkowników, zostaną usunięte. Usuniętych ustawień nie można przywrócić.*

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 pozycje **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. Uruchom aplikację EPSON Software Updater i zaktualizuj aplikacje lub oprogramowanie sprzętowe.

   Uwaga:
   Nie są obsługiwane systemy operacyjne Windows Server.

   ❏ Windows 10

   Kliknij przycisk Start, a następnie wybierz polecenia **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Wprowadź nazwę aplikacji w panelu wyszukiwania, po czym wybierz wyświetloną ikonę.

   ❏ Windows 7

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

   ❏ Mac OS

   Wybierz polecenia **Finder** > **Przejdź** > **Programy** > **Epson Software** > **EPSON Software Updater**.

Uwaga:
Jeżeli na liście aplikacji nie ma aplikacji, która ma być zaktualizowana, 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 następne 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 konfiguracyjnej w przeglądarce” na stronie 36

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. Jeżeli nie można zaktualizować oprogramowania przez sieć, wypróbuj tę metodę.

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.