EPSON
EXCEED YOUR VISION

# Przewodnik administratora

NPD5668-00 PL

# Spis treści

**Spis treści**

# Prawa autorskie

# Znaki towarowe

- ❏ EPSON® to zastrzeżony znak towarowy, a EPSON EXCEED YOUR VISION lub EXCEED YOUR VISION to znak towarowy Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ 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.

# Informacje o instrukcji

## Oznaczenia i symbole

> ***Przestroga:***
> *Instrukcje, których należy przestrzegać w celu uniknięcia uszczerbku na zdrowiu.*

> ***Ważne:***
> *Instrukcje, których należy przestrzegać w celu uniknięcia uszkodzenia urządzenia.*

***Uwaga:***
*Przydatne porady oraz informacje o ograniczeniach skanera.*

### Powiązane informacje

➡ Kliknięcie tej ikony spowoduje przejście do informacji powiązanych z bieżącym tematem.

## Objaśnienia stosowane w niniejszym podręczniku

❏ Zrzuty ekranowe sterownika skanera oraz ekrany narzędzia Epson Scan 2 (sterownik skanera) pochodzą z systemu Windows 10 lub OS X El Capitan. Materiały prezentowane na tych ekranach różnią się w zależności od modelu i sytuacji.

❏ Ilustracje prezentowane w tym podręczniku są wyłącznie przykładowe. Mogą co prawda występować niewielkie różnice w zależności od konkretnego modelu, jednak zasada obsługi pozostaje taka sama.

❏ Niektóre pozycje menu wyświetlane na ekranie LCD mogą się różnić w zależności od konkretnego modelu i ustawień.

## Odniesienia do systemów operacyjnych

### Windows

W tej instrukcji obsługi hasła, takie jak „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Vista”, „Windows XP”, Windows Server 2016, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2”, „Windows Server 2008”, „Windows Server 2003 R2” oraz „Windows Server 2003” odnoszą się do niżej wymienionych systemów operacyjnych. Oprócz tego określenie „Windows” stosowane jest w odniesieniu do wszystkich wersji.

❏ 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 Vista®

- ❏ System operacyjny Microsoft® Windows® XP
- ❏ System operacyjny Microsoft® Windows® XP Professional x64 Edition
- ❏ System operacyjny Microsoft® Windows Server® 2016
- ❏ System operacyjny Microsoft® Windows Server® 2012 R2
- ❏ System operacyjny Microsoft® Windows Server® 2012
- ❏ System operacyjny Microsoft® Windows Server® 2008 R2
- ❏ System operacyjny Microsoft® Windows Server® 2008
- ❏ System operacyjny Microsoft® Windows Server® 2003 R2
- ❏ System operacyjny Microsoft® Windows Server® 2003

### Mac OS

W tej instrukcji obsługi termin „Mac OS” stosowany jest w odniesieniu do systemów macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x i Mac OS X v10.6.8.

# Wprowadzenie

## Budowa podręcznika

Ten podręcznik jest przeznaczony dla administratora urządzenia odpowiedzialnego za podłączanie drukarki lub skanera do sieci. W podręczniku przestawiono informacje dotyczące sposobu konfigurowania używania funkcji.

Więcej informacji o użyciu funkcji można znaleźć w dokumencie *Przewodnik użytkownika*.

#### Przygotowanie

W tym rozdziale opisano zadnia administratora, sposób konfiguracji urządzeń i zarządzanie oprogramowaniem.

#### Połączenie

W tym rozdziale opisano łączenie urządzenia z siecią lub linią telefoniczną. Przedstawiono też informacje o środowisku sieciowym, np. użycie portów urządzenia, informacje o serwerach DNS i proxy.

#### Ustawienia funkcji

W tym rozdziale opisano ustawienia poszczególnych funkcji urządzenia.

#### Podstawowe ustawienia zabezpieczeń

W tym rozdziale objaśniono ustawienia poszczególnych funkcji, takich jak drukowanie, skanowanie i faksy.

#### Ustawienia obsługi i zarządzania

W tym rozdziale przedstawiono operacje wykonywane po skonfigurowaniu urządzeń, np. sprawdzanie informacji i czynności konserwacyjne.

#### Rozwiązywanie problemów

W tym rozdziale opisano inicjowanie ustawień i rozwiązywanie problemów związanych z siecią.

#### Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

W tym rozdziale przedstawiono metody konfiguracji w celu poprawy bezpieczeństwa urządzenia, np. użycie certyfikatu urzędu certyfikacji, komunikacja SSL/TLS oraz funkcja IPsec/Filtrowanie IP.

Niektóre funkcje opisane w tym rozdziale są dostępne tylko na wybranych modelach urządzeń.

## Definicje terminów użytych w tym podręczniku

W tym podręczniku używane są następujące terminy.

#### Administrator

Osoba odpowiedzialna za instalowanie i konfigurowanie urządzenia lub sieci w biurze lub firmie. W przypadku małych firm osoba ta może być odpowiedzialna za zarówno urządzenie, jak i sieć. W dużych firmach administratorzy mają uprawnienia do zarządzania siecią lub urządzeniami w grupie działów, a administratorzy sieci są odpowiedzialni za ustawienia komunikacji w całej organizacji, np. Internet.

### Administrator sieci

Osoba odpowiedzialna za kontrolowanie środowiska sieciowego. Do jej obowiązków należą konfiguracja routera, serwera proxy, serwera DNS i serwera poczty w celu kontroli danych przesyłanych przez Internet lub sieć.

### Użytkownik

Osoba używająca urządzeń, takich jak drukarki lub skanery.

### Narzędzie Web Config (strony internetowe urządzenia)

Serwer WWW wbudowany w urządzenie. Nazywa się Web Config. Można sprawdzać i zmieniać stan urządzenia za pośrednictwem przeglądarki.

### Narzędzie

Ogólny termin oznaczający oprogramowanie do konfigurowania lub zarządzania urządzeniem, np. Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, itd.

### Skanowanie w trybie wypychania

Ogólny termin oznaczający skanowanie z panelu sterowania urządzenia.

### ASCII (American Standard Code for Information Interchange)

Jeden ze standardów kodowania znaków. Zdefiniowanych jest 128 znaków, w tym litery alfabetu (a–z, A–Z), cyfry arabskie (0–9), symbole, znaki puste i znaki sterujące. Kiedy termin „ASCII" jest używany w tym podręczniku, oznacza to znaki o kodzie 0x20–0x7E (liczby szesnastkowe) wymienione poniżej, bez uwzględniania znaków sterujących.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SP* | ! | " | # | $ | % | & | ' | ( | ) | * | + | , | - | . | / |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? |
| @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ |
| ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| p | q | r | s | t | u | v | w | x | y | z | { | \| | } | ~ | |

* Znak spacji.

### Unicode (UTF-8)

Międzynarodowy standard kodowania znaków. Kiedy termin „UTF-8" jest używany w tym podręczniku, oznacza to kodowanie znaków w formacie UTF-8.

# Przygotowanie

W tym rozdziale opisano rolę administratora i przygotowanie urządzenia przed przystąpieniem do konfiguracji.

## Schemat ustawień skanera i zarządzania

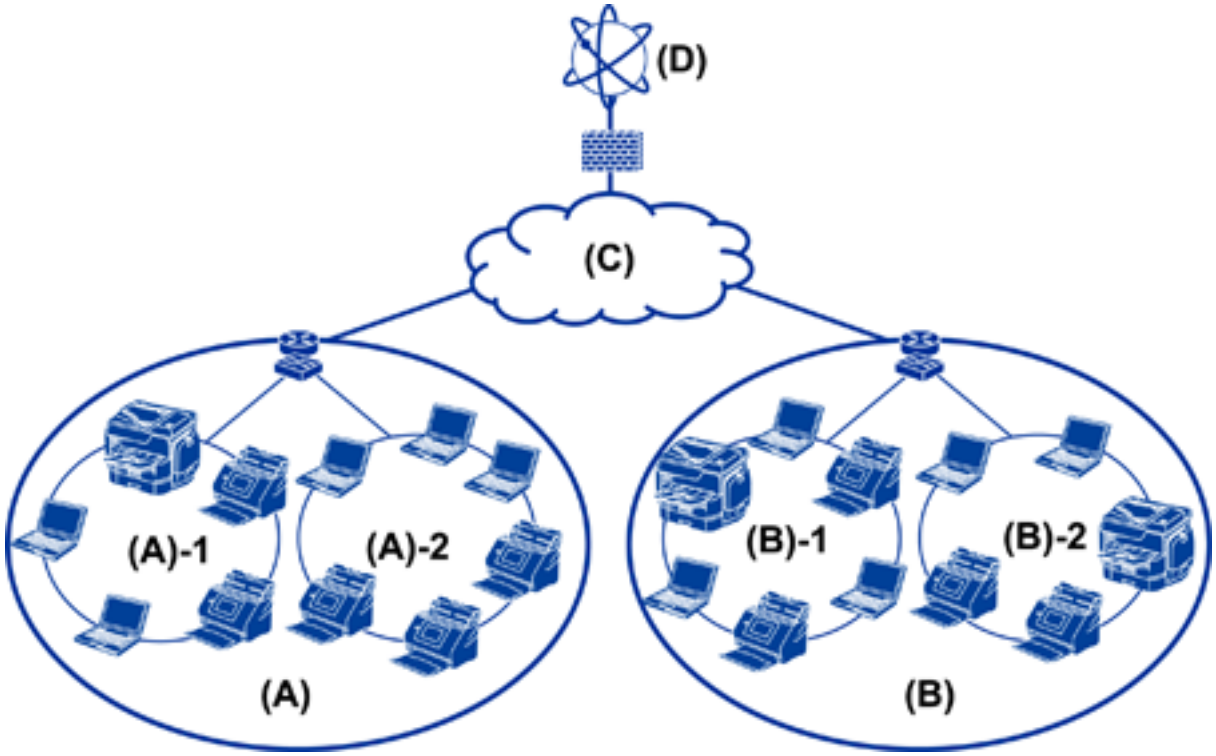
Administrator konfiguruje ustawienia połączenia sieciowego, wykonuje czynności wstępnej konfiguracji i konserwacji skanera, tak aby użytkownicy mogli ich używać.

1. Przygotowywanie
   - ❏ Gromadzenie informacji o ustawieniach połączenia
   - ❏ Wybór metody połączenia
2. Nawiązywanie połączenia
   - ❏ Połączenie sieciowe z poziomu panelu sterowania skanera
3. Konfigurowanie funkcji
   - ❏ Ustawienia sterownika skanera
   - ❏ Inne ustawienia zaawansowane
4. Ustawienia zabezpieczeń
   - ❏ Ustawienia administratora
   - ❏ SSL/TLS
   - ❏ Kontrola protokołu
   - ❏ Zaawansowane ustawienia zabezpieczeń (opcja)
5. Obsługa i zarządzanie
   - ❏ Sprawdzanie stanu urządzenia
   - ❏ Obsługa nagłych wydarzeń
   - ❏ Tworzenie kopii zapasowej ustawień urządzenia

**Powiązane informacje**

➡ „Przygotowanie” na stronie 10
➡ „Połączenie” na stronie 15
➡ „Ustawienia funkcji” na stronie 22
➡ „Podstawowe ustawienia zabezpieczeń” na stronie 32
➡ „Ustawienia obsługi i zarządzania” na stronie 40

# Przykład środowiska sieciowego




(A): Biuro 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Biuro 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

## Wprowadzenie do ustawień połączenia skanera

Dostępne są dwa typy połączeń, które zależą od sposobu używania skanera. Oba służą do podłączania skanera do sieci z komputerem za pośrednictwem koncentratora.

❏ Połączenie serwer / klient (skaner wykorzystujący serwer Windows, zarządzanie zadaniami)

❏ Połączenia równy z równym (bezpośrednie połączenie z komputerem klienckim)

### Powiązane informacje

➡ „Połączenie serwer / klient” na stronie 12

➡ „Połączenie równy z równym” na stronie 12

## Połączenie serwer / klient

Oprogramowanie Document Capture Pro Server zainstalowane na serwerze pozwala na scentralizowanie zarządzania skanerami i zadaniami. Jest ono przydatne we wdrożeniach obejmujących wiele skanerów wykorzystywanych do skanowania dużej liczby dokumentów w konkretnym formacie.

### Powiązane informacje

➡ „Definicje terminów użytych w tym podręczniku” na stronie 8

## Połączenie równy z równym

Pojedynczy skaner można obsługiwać, wykorzystując zainstalowany na komputerze klienckim sterownik skanera, taki jak Epson Scan 2. Instalując na komputerze klienckim oprogramowanie Document Capture Pro (Document Capture), można uruchamiać zadania na poszczególnych komputerach klienckich skanera.

### Powiązane informacje

➡ „Definicje terminów użytych w tym podręczniku” na stronie 8

# Przygotowanie połączenia z siecią

## Gromadzenie informacji o ustawieniach połączenia

Aby móc skonfigurować połączenie, trzeba znać adres IP, adres bramy itd. Uzyskaj następujące informacje.

| Wymiary | Elementy | Uwaga |
|---|---|---|
| Metoda połączenia urządzenia | ❏ Ethernet | W przypadku połączenia Ethernet należy użyć skrętki ekranowanej kategorii 5e lub wyższej. |
| Informacje o połączeniu z siecią lokalną | ❏ Adres IP<br>❏ Maska podsieci<br>❏ Brama domyślna | W przypadku automatycznego ustawiania adresu IP za pomocą funkcji DHCP routera te informacje nie są wymagane. |
| Informacje o serwerze DNS | ❏ Adres IP podstawowego serwera DNS<br>❏ Adres IP pomocniczego serwera DNS | W przypadku korzystania ze statycznego adresu IP skonfiguruj serwer DNS.<br>Skonfiguruj w przypadku przydzielania automatycznego za pomocą funkcji DHCP oraz w razie niepowodzenia automatycznego przydzielenia serwera DNS. |
| Informacje o serwerze proxy | ❏ Nazwa serwera proxy<br>❏ Numer portu | Skonfiguruj w przypadku używania serwera proxy do nawiązywania połączenia z Internetem i w razie korzystania z usługi Epson Connect lub funkcji automatycznej aktualizacji oprogramowania układowego. |

# Dane techniczne skanera

Więcej informacji o standardach obsługiwanych przez skaner lub trybach połączeń można znaleźć w dokumencie *Przewodnik użytkownika*.

# Używanie numeru portu

Więcej informacji o numerze portu używanego przez skaner można znaleźć w rozdziale „Załącznik”.

### Powiązane informacje

➡ „Używanie portów na skanerze” na stronie 60

# Rodzaje przydzielania adresów IP

Adres IP można przydzielać do skanera na dwa sposoby.

### Statyczny adres IP:

Można przydzielić wstępnie określony unikatowy adres IP do skanera.

Adres IP nie zmienia się, nawet po wyłączeniu skanera lub routera, co pozwala na zarządzanie urządzeniem przy użyciu adresu IP.

Ten typ przydaje się w sieciach, gdzie jest wiele skanerów, np. duże biura lub szkoły.

### Automatyczne przydzielanie za pośrednictwem funkcji DHCP:

Poprawny adres IP jest automatycznie przydzielany po nawiązaniu połączenia skanera i routera obsługującego funkcję DHCP.

Jeśli potrzebna jest zmiana adresu IP dla konkretnego urządzenia, należy zarezerwować ten adres i przydzielić go do urządzenia.

# Serwer DNS i serwer proxy

W przypadku korzystania z usługi połączenia internetowego można skonfigurować serwer DNS. Jeżeli serwer nie zostanie skonfigurowany, trzeba będzie określić adres IP serwera, ponieważ rozwiązywanie nazw może się nie powieść.

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.

Można uniemożliwić dostęp do konkretnego adresu URL, używając funkcji filtrowania, ponieważ serwer proxy może sprawdzać zawartość przesyłanych danych.

# Metoda konfiguracji połączenia sieciowego

Aby skonfigurować ustawienia połączenia skanera, takie jak adres IP, maska podsieci i brama domyślna, wykonaj następujące czynności.

### Przy użyciu panelu sterowania:

Skonfiguruj ustawienia z poziomu panelu sterowania poszczególnych skanerów. Podłącz skaner do sieci po skonfigurowaniu jego ustawień połączenia.

### Przy użyciu instalatora:

W przypadku korzystania z instalatora ustawienia sieci skanera i komputera klienckiego są konfigurowane automatycznie. Konfigurację może przeprowadzić nawet niedoświadczony użytkownik, postępując zgodnie z instrukcjami wyświetlanymi przez instalator.

### Używanie narzędzia:

Należy użyć narzędzia na komputerze administratora. Możliwe jest wykrywanie skanerów w sieci, a następnie konfigurowanie ich osobno lub zbiorczo po utworzeniu pliku konfiguracyjnego SYLK. Aby można było skonfigurować wiele skanerów naraz, muszą być podłączone fizycznie za pomocą kabla Ethernet. Ta metoda jest zalecana w przypadku budowania sieci Ethernet.

### Powiązane informacje

➡ „Zmiana sieci z poziomu panelu sterowania” na stronie 15

➡ „Nawiązywanie połączenia z siecią za pomocą instalatora” na stronie 19

➡ „Przydzielanie adresu IP za pomocą programu EpsonNet Config” na stronie 56

# Połączenie

W tym rozdziale przedstawiono środowisko lub procedurę łączenia skanera z siecią.

## Nawiązywanie połączenia z siecią

### Zmiana sieci z poziomu panelu sterowania

Połącz skaner z siecią, używając panelu sterowania skanera.

Więcej informacji o obsłudze panelu sterowania skanera można znaleźć w dokumencie *Przewodnik użytkownika*.

### Przydzielanie adresu IP

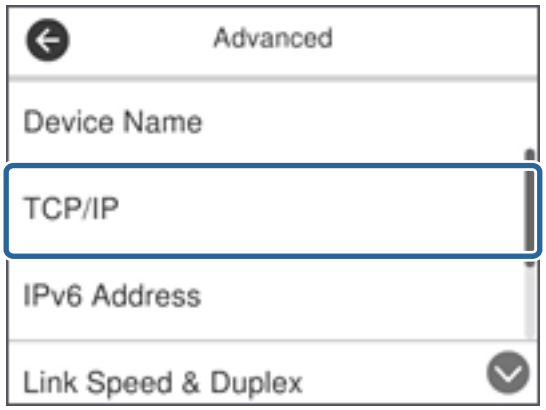
Skonfiguruj podstawowe opcje, takie jak Adres IP, Maska podsieci i Domyśl. brama.

1. Włącz skaner.
2. Na panelu sterowania skanera przesuń ekran w lewo, a następnie dotknij pozycji **Ustaw.**.

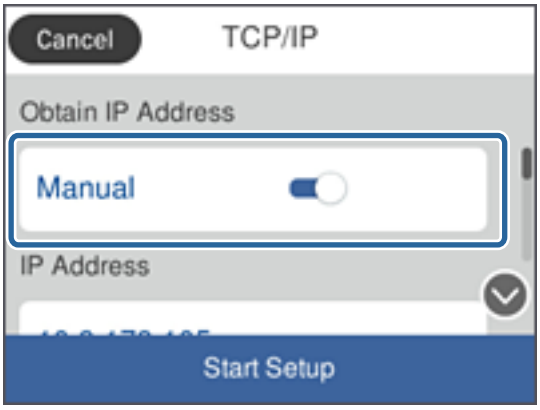

3. Dotknij pozycji **Ustawienia sieciowe** > **Zmień ustawienia**.

   Jeśli pozycja nie jest wyświetlana, przesuń ekran w górę, aby ją wyświetlić.

4. Dotknij pozycji **TCP/IP**.

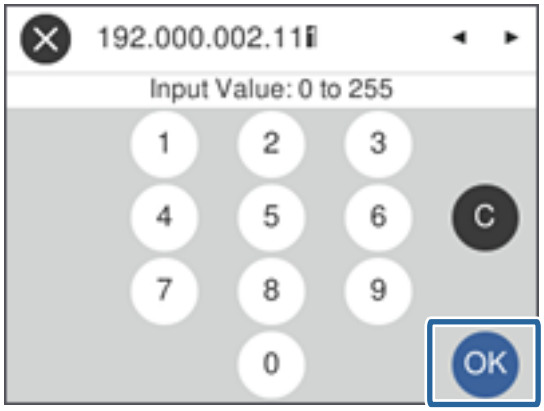



5. Wybierz opcję **Ręczne** w polu **Uzyskaj adres IP**.




***Uwaga:***
*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 6 do 7 są również ustawiane automatycznie, dlatego należy przejść do kroku 8.*

6. Dotknij pola **Adres IP**, wprowadź adres IP, używając klawiatury ekranowej, a następnie dotknij przycisku **OK**.




Potwierdź wartości z poprzedniego ekranu.

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

   Potwierdź wartości z poprzedniego ekranu.

   ***Uwaga:***
   *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.*

8. Dotknij pola **Podstawowy DNS** w obszarze **Serwer DNS**, wprowadź adres IP podstawowego serwera DNS za pomocą klawiatury ekranowej, a następnie dotknij przycisku **OK**.

   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 10.*

9. Dotknij pola **Dodatkowy DNS**, wprowadź adres IP pomocniczego serwera DNS za pomocą klawiatury ekranowej, a następnie dotknij przycisku **OK**.

   Potwierdź wartości z poprzedniego ekranu.

10. Dotknij pozycji **Uruchom ustawienia**.

11. Na ekranie potwierdzenia dotknij pozycji **Zamknij**.

    Ekran zostanie zamknięty automatycznie, jeśli przycisk nie zostanie dotknięty **Zamknij** przez określony czas.

## Łączenie z siecią Ethernet

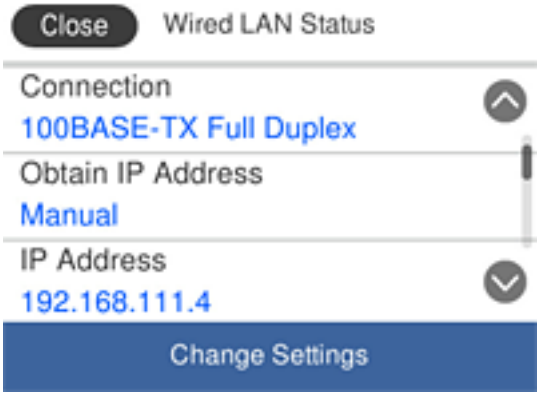
Podłącz skaner do sieci, używając kabla Ethernet, a następnie sprawdź, czy połączenie działa prawidłowo.

1. Podłącz skaner do koncentratora (przełącznika L2) kablem Ethernet.

   Ikona na ekranie głównym zmieni się w ikonę  .

2. Na ekranie głównym dotknij ikony  .

3. Przesuń ekran w górę, a następnie upewnij się, że stan połączenia i adres IP są poprawne.




## Konfigurowanie serwera proxy

Serwera proxy nie można skonfigurować z poziomu panelu sterowania. Można to zrobić za pomocą narzędzia Web Config.

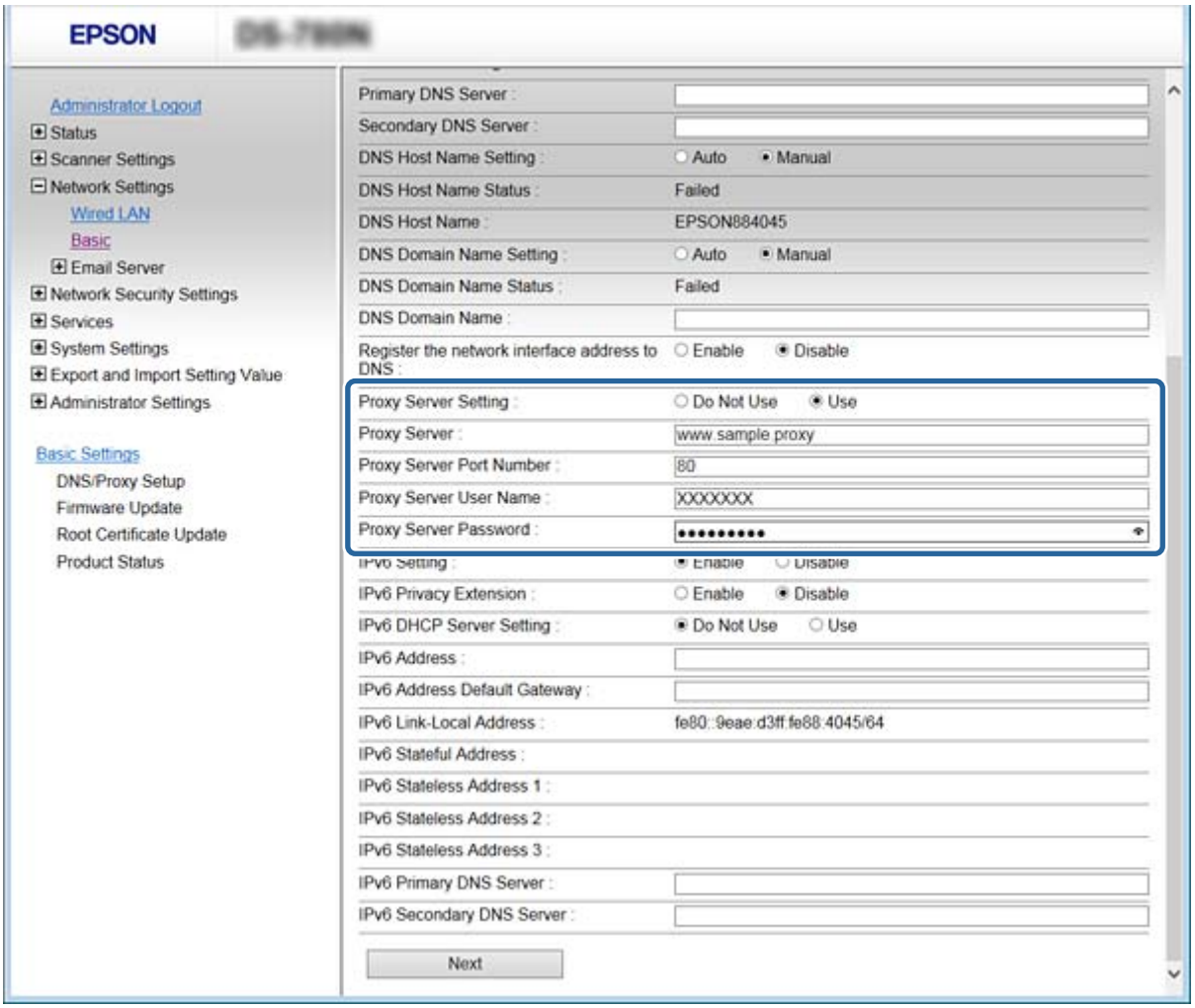
1. Otwórz narzędzie Web Config i wybierz pozycje **Network Settings** > **Basic**.

2. Wybierz opcję **Use** dla ustawienia **Proxy Server Setting**.

3. W polu **Serwer proxy** określ adres serwera proxy w formacie IPv4 lub FQDN, a następnie w polu **Proxy Server Port Number** wprowadź numer portu.

   W przypadku serwerów proxy wymagających uwierzytelniania wprowadź nazwę użytkownika i hasło do uwierzytelniania na serwerze proxy.

4. Kliknij przycisk **Next**.




5. Potwierdź ustawienia i kliknij przycisk **Ustawienia**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Nawiązywanie połączenia z siecią za pomocą instalatora

Zaleca się użycie instalatora do konfigurowania połączenia skanera z komputerem. Instalator można uruchomić, postępując zgodnie z jedną z następujących metod.

❏ Konfigurowanie z poziomu witryny

Przejdź do poniższej witryny, a następnie wprowadź nazwę modelu danego urządzenia. Przejdź do karty **Konfiguracja**, a następnie rozpocznij konfigurację.

http://epson.sn

❏ Konfigurowanie za pomocą dysku z oprogramowaniem (tylko modele, z którymi dostarczono dysk, i użytkownicy z komputerami wyposażonymi w napędy dysków)

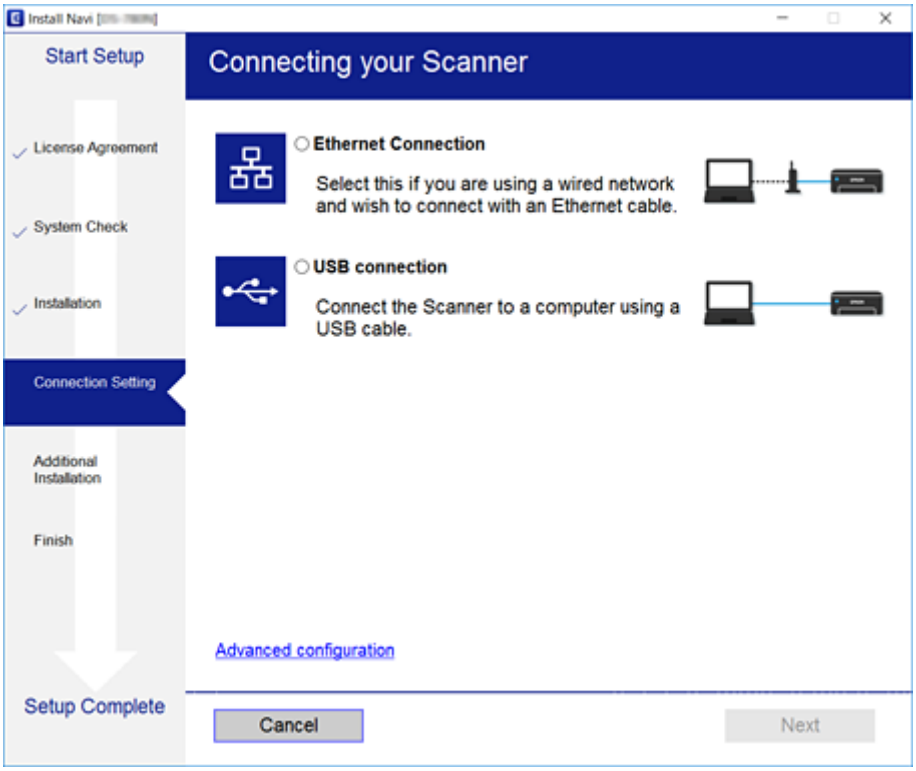
Włóż do komputera dysk z oprogramowaniem, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

### Wybór metody połączenia

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aż zostanie wyświetlony następujący ekran, po czym wybierz metodę połączenia skanera z komputerem.

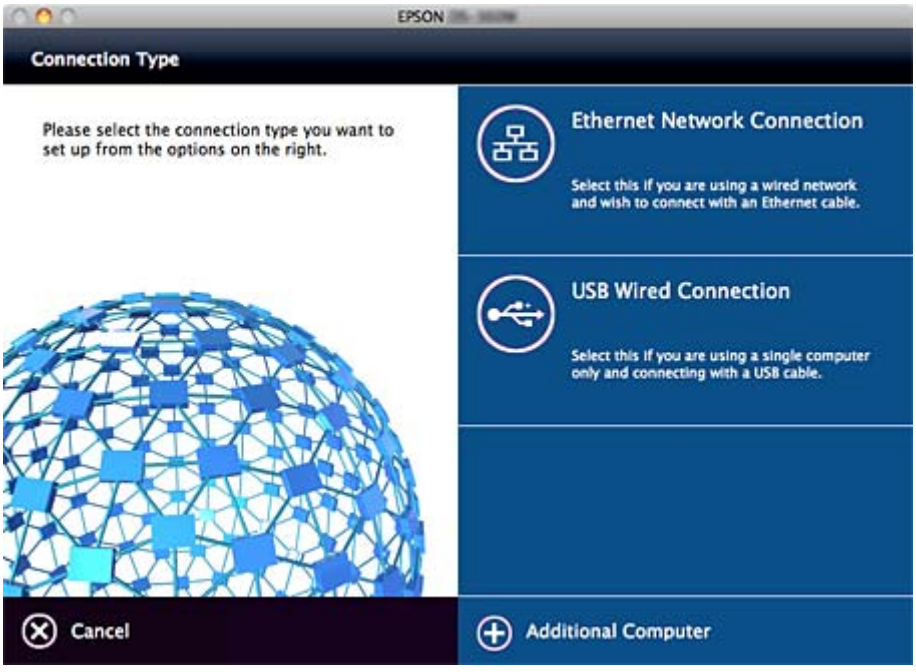
❏ Windows

Wybierz typ połączenia i kliknij przycisk **Dalej**.




❏ Mac OS

Wybierz typ połączenia.



**Połączenie**

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Niezbędne oprogramowanie zostanie zainstalowane.

# Ustawienia funkcji

W tym rozdziale opisano początkowe ustawienia, które trzeba skonfigurować, aby móc używać poszczególnych funkcji urządzenia.

# Oprogramowanie do konfigurowania ustawień

W tym rozdziale opisano procedurę konfigurowania ustawień z poziomu komputera administratora za pomocą narzędzia Web Config.

## Web Config (strony internetowe urządzenia)

### Informacje o Web Config

Web Config jest aplikacją uruchamianą w przeglądarce internetowej. Służy ona do konfigurowania ustawień skanera.

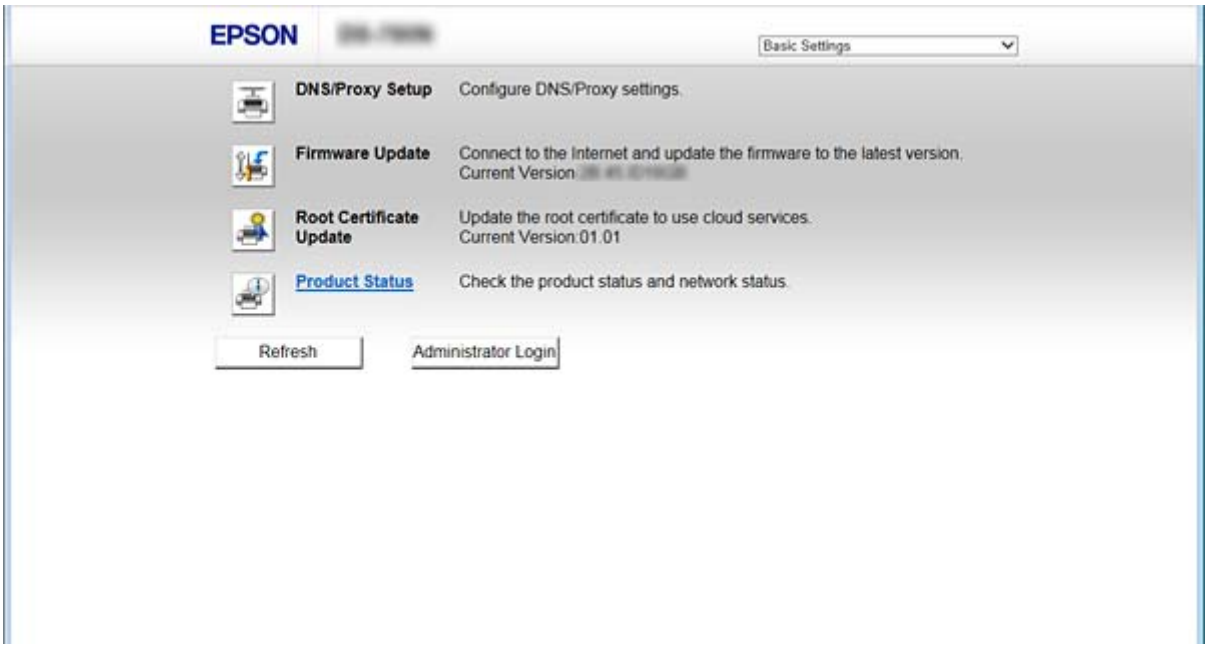
Aby uzyskać dostęp do aplikacji Web Config, należy najpierw przydzielić skanerowi adres IP.

***Uwaga:***
*Aby zablokować stronę z ustawieniami, należy skonfigurować na skanerze hasło administratora.*

Dostępne są dwie strony ustawień (przedstawione poniżej).

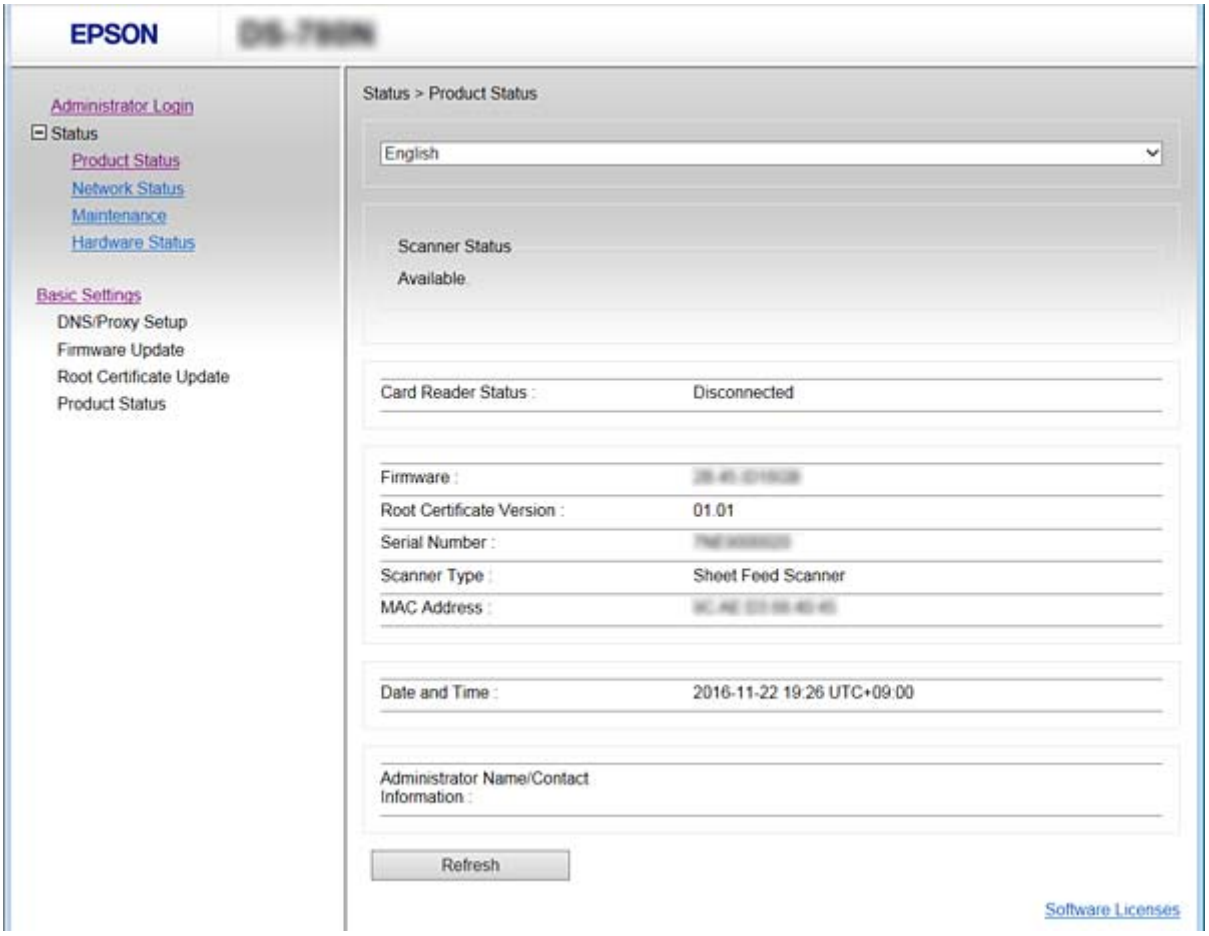
❏ **Basic Settings**

Służy do konfiguracji podstawowych ustawień skanera.



❏ **Advanced Settings**

Służy do konfiguracji zaawansowanych ustawień skanera. Ta strona jest przeznaczona głównie dla administratorów.




## Uzyskiwanie dostępu do aplikacji Web Config

W celu uzyskania dostępu do aplikacji należy wpisać w przeglądarce internetowej adres IP skanera. Obsługa języka JavaScript musi być włączona. Podczas uzyskiwania dostępu do aplikacji Web Config przy użyciu protokołu HTTPS w przeglądarce wyświetlany jest komunikat ostrzegawczy, ponieważ używany jest zapisany na skanerze certyfikat z podpisem własnym.

❏ Dostęp przez HTTPS

IPv4: https://<adres IP skanera> (bez < >)

IPv6: https://[adres IP skanera]/ (z [ ])

❏ Dostęp przez HTTP

IPv4: http://<adres IP skanera> (bez < >)

IPv6: http://[adres IP skanera]/ (z [ ])

***Uwaga:***

❏ *Przykłady*

*IPv4:*

*https://192.0.2.111/*

*http://192.0.2.111/*

*IPv6:*

*https://[2001:db8::1000:1]/*

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

❏ *Jeśli nazwa skanera została zarejestrowana na serwerze DNS, w miejsce adresu IP można użyć nazwy skanera.*

**Powiązane informacje**

➡ „Komunikacja SSL/TLS ze skanerem” na stronie 63

➡ „Informacje o certyfikatach cyfrowych” na stronie 63

# Korzystanie z funkcji skanowania

W zależności od sposobu używania skanera zainstaluj następujące oprogramowanie i skonfiguruj w nim ustawienia.

❏ **Skanowanie z komputera**

- ❏ Sprawdź poprawność konfiguracji usługi skanowania sieciowego za pomocą narzędzia Web Config (poprawne w momencie wysyłki z fabryki).
- ❏ Zainstaluj oprogramowanie Epson Scan 2 na komputerze i ustaw adres IP.
- ❏ W przypadku skanowania przy użyciu zadań zainstaluj oprogramowanie Document Capture Pro (Document Capture) i skonfiguruj ustawienia zadań.

❏ **Skanowanie z poziomu panelu sterowania**

- ❏ W przypadku korzystania z oprogramowania Document Capture Pro lub Document Capture Pro Server:

  Zainstaluj oprogramowanie Document Capture Pro lub Document Capture Pro Server.

  Skonfiguruj oprogramowanie DCP (tryb serwera, tryb klienta).
- ❏ W przypadku korzystania z protokołu WSD:

  Sprawdź poprawność konfiguracji protokołu WSD w narzędziu Web Config lub na panelu sterowania (poprawne w momencie wysyłki z fabryki).

  Skonfiguruj dodatkowe ustawienia urządzenia (komputer z systemem Windows).

## Skanowanie z poziomu komputera

Aby skanować przez sieć z poziomu komputera, zainstaluj oprogramowanie i upewnij się, że usługa skanowania sieciowego jest włączona.

**Powiązane informacje**

➡ „Oprogramowanie do zainstalowania” na stronie 25

➡ „Włączanie skanowania sieciowego” na stronie 25

## Oprogramowanie do zainstalowania

❏ Epson Scan 2

To jest sterownik skanera. W przypadku korzystania z urządzenia z poziomu komputera trzeba zainstalować sterownik na każdym komputerze klienckim. Jeśli zainstalowano program Document Capture Pro/Document Capture, można wykonywać operacje przydzielone do przycisków urządzenia.

Za pomocą oprogramowania EpsonNet SetupManager można rozpowszechniać sterowniki drukarki w postaci pakietów.

❏ Document Capture Pro (Windows) / Document Capture (Mac OS)

Zainstaluj na komputerze klienckim. Zadania zarejestrowane na komputerze z zainstalowanym oprogramowaniem Document Capture Pro / Document Capture można wywoływać i wykonywać z poziomu komputera i panelu sterowania skanera.

Można też skanować z komputera przez sieć. Do skanowania niezbędne jest oprogramowanie Epson Scan 2.

### Powiązane informacje

➡ „EpsonNet SetupManager” na stronie 56

## Ustawianie adresu IP skanera w oprogramowaniu Epson Scan 2

Określając adres IP skanera, będzie można używać skanera w sieci.

1. Uruchom narzędzie **Epson Scan 2 Utility**, wybierając pozycje **Start** > **Wszystkie programy** > **EPSON** > **Epson Scan 2**.

   Jeśli zarejestrowany jest już inny skaner, przejdź do kroku 2.

   W przeciwnym razie przejdź do kroku 4.

2. Kliknij przycisk ▼ w obszarze **Skaner**.

3. Kliknij przycisk **Ustawienia**.

4. Kliknij przycisk **Włącz edytowanie**, a następnie przycisk **Dodaj**.

5. Z listy **Model** wybierz nazwę modelu skanera.

6. Z listy **Adres** w obszarze **Wyszukaj sieć** wybierz adres IP skanera.

   Kliknij przycisk  , a potem  , aby odświeżyć listę. Jeśli nie można znaleźć adresu IP skanera, zaznacz opcję **Wprowadź adres** i ręcznie wprowadź adres IP.

7. Kliknij przycisk **Dodaj**.

8. Kliknij przycisk **OK**.

## Włączanie skanowania sieciowego

Można aktywować usługę skanowania sieciowego, która pozwala skanować z komputera klienckiego przez sieć. Domyślnie funkcja jest włączona.

1. Otwórz narzędzie Web Config i wybierz pozycje **Services** > **Network Scan**.
2. Upewnij się, że opcja **Enable scanning** w obszarze **EPSON Scan** jest zaznaczona.

   Jeśli jest zaznaczona, nie trzeba wykonywać kolejnych czynności. Zamknij narzędzie Web Config.

   W przeciwnym razie zaznacz ją i przejdź do następnego kroku.
3. Kliknij przycisk **Next**.
4. Kliknij przycisk **OK**.

   Zostanie ponownie nawiązane połączenie z siecią i usługa będzie aktywna.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Skanowanie przy użyciu panelu sterowania

Funkcja skanowania do folderu i skanowania do poczty e-mail z poziomu panelu sterowania skanera, a także przesyłanie zeskanowanych danych do poczty, folderów itd. są realizowane przez wykonanie zadania z poziomu komputera.

Podczas przesyłania zeskanowanych danych trzeba utworzyć zadanie w oprogramowaniu Document Capture Pro Server lub Document Capture Pro.

Więcej informacji o tych ustawieniach i tworzeniu zadań można znaleźć w dokumentacji albo pomocy oprogramowania Document Capture Pro Server lub Document Capture Pro.

### Powiązane informacje

➡ „Ustawienia oprogramowania Document Capture Pro Server / Document Capture Pro” na stronie 27

➡ „Ustawienia serwerów i folderów” na stronie 27

## Oprogramowanie do zainstalowania na komputerze

❏ **Document Capture Pro Server**

To jest wersja oprogramowania Document Capture Pro przeznaczona na serwery. Zainstaluj ją na serwerze z systemem Windows. Na serwerze można zarządzać wieloma urządzeniami i zadaniami. Zadania można wykonywać jednocześnie na wielu skanerach.

Używając certyfikowanej wersji oprogramowania Document Capture Pro Server, można zarządzać zadaniami i historią skanowania połączonymi z użytkownikami i grupami.

Więcej informacji na temat oprogramowania Document Capture Pro Server można uzyskać, kontaktując się z lokalnym oddziałem firmy Epson.

❏ **Document Capture Pro (Windows) / Document Capture (Mac OS)**

Podobnie do skanowania na komputerze można wywoływać zadania zarejestrowane na komputerze z poziomu panelu sterowania i wykonywać je. Nie można uruchamiać zadań z komputera jednocześnie na wielu skanerach.

## Ustawienia oprogramowania Document Capture Pro Server / Document Capture Pro

Ustawienia funkcji skanowania można skonfigurować na panelu sterowania skanera.

1. Otwórz narzędzie Web Config i wybierz pozycje **Services** > **Document Capture Pro**.
2. Naciśnij przycisk **Tryb działania**.
   - ❏ Server Mode:

     Wybierz tę opcję w przypadku korzystania z oprogramowania Document Capture Pro Server lub Document Capture Pro tylko do zadań, które zostały przydzielone do konkretnego komputera.
   - ❏ Client Mode:

     Wybierz tę opcję w przypadku wyboru ustawień zadania w oprogramowaniu Document Capture Pro (Document Capture) zainstalowanym na każdym komputerze klienckim w sieci bez określania konkretnego komputera.
3. Odpowiednio do wybranego trybu skonfiguruj następujące ustawienia.
   - ❏ Server Mode:

     W polu **Server Address** określ serwer, na którym zainstalowano oprogramowanie Document Capture Pro Server. Wprowadź od 2 do 252 znaków w formacie IPv4, IPv6, nazwy hosta lub FQDN. W formacie FQDN można używać liter US – ASCII, cyfr, znaków alfabetu i dywizów (ale nie na początku i końcu).
   - ❏ Client Mode:

     Określ wartość ustawienia **Group Settings**, aby używać grupy skanerów zdefiniowanej w oprogramowaniu Document Capture Pro (Document Capture).
4. Kliknij przycisk **Ustawienia**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Ustawienia serwerów i folderów

Oprogramowanie Document Capture Pro i Document Capture Pro Server umożliwia zapisywanie zeskanowanych danych na serwerze lub komputerze klienckim, a następnie użycie funkcji transferu do wykonania funkcji skanowania do folderu oraz skanowania do poczty e-mail.

Aby móc transferować do komputera lub usługi chmury z komputera, na którym zainstalowano oprogramowanie Document Capture Pro lub Document Capture Pro Server, trzeba mieć upoważnienie i odpowiednie informacje.

Informacje o używanej funkcji należy przygotować, zapoznając się z poniższymi informacjami.

Ustawienia tych funkcji można skonfigurować za pomocą oprogramowania Document Capture Pro lub Document Capture Pro Server. Więcej informacji o tych ustawieniach można znaleźć w dokumentacji albo pomocy oprogramowania Document Capture Pro Server lub Document Capture Pro.

| Nazwa | Ustawienia | Wymagania |
|---|---|---|
| Skan. do foldera siec. (SMB) | Tworzenie i konfigurowanie udostępniania folderu zapisu | Konto użytkownika z uprawnieniami administratora na komputerze, na którym tworzony jest folder zapisu. |
| | Miejsce docelowe funkcji Skan. do foldera siec. (SMB) | Nazwa użytkownika i hasło do logowania na komputerze, na którym jest folder zapisu, a także uprawnienia do aktualizowania zawartości folderu zapisu. |
| Skan. do foldera siec. (FTP) | Konfigurowanie logowania na serwerze FTP | Dane logowania na serwerze FTP i uprawnienia do aktualizowania zawartości folderu zapisu. |
| Skanuj do e-mail | Konfigurowanie serwera poczty e-mail | Informacje o konfiguracji serwera poczty e-mail |
| Skanuj do Document Capture Pro (używanie narzędzia Document Capture Pro Server) | Konfigurowanie logowania w usługach chmury | Środowisko z połączeniem internetowym<br>Rejestrowanie konta w usługach chmury |

### Używanie skanowania WSD (tylko system Windows)

Jeżeli na komputerze jest zainstalowany system Windows Vista lub nowszy, można używać funkcji skanowania WSD.

Jeśli można używać protokołu WSD, na panelu sterowania skanera jest wyświetlane menu **Komputer (WSD)**.

1. Otwórz narzędzie Web Config i wybierz pozycje **Services** > **Protocol**.
2. Sprawdź, czy opcja **Enable WSD** jest zaznaczona na ekranie **WSD Settings**.

   Jeśli jest zaznaczona, nie trzeba wykonywać kolejnych czynności i można zamknąć narzędzie Web Config.

   W przeciwnym razie zaznacz tę opcję i przejdź do następnego kroku.
3. Kliknij przycisk **Next**.
4. Sprawdź ustawienia i kliknij przycisk **Ustawienia**.

# Konfigurowanie ustawień systemowych

## Konfigurowanie ustawień na panelu sterowania

### Ustawianie jasności ekranu

Można ustawić jasność ekranu LCD.

1. Na ekranie głównym dotknij pozycji **Ustaw.**.

2. Dotknij pozycji **Ustawienia wspólne** > **Jasność LCD**.
3. Dotknij pozycji  lub  , aby dostosować jasność.
   Można wybrać wartość z zakresu 1 do 9.
4. Dotknij pozycji **OK**.

## Konfigurowanie dźwięku

Możliwe jest skonfigurowanie dźwięków emitowanych podczas obsługi panelu sterowania oraz dźwięków błędów.

1. Na ekranie głównym dotknij pozycji **Ustaw.**.
2. Dotknij pozycji **Ustawienia wspólne** > **Dźwięk**.
3. W miarę potrzeby skonfiguruj następujące pozycje.
   - ❏ Dźwięk podczas obsługi
     Ustaw głośność dźwięków emitowanych podczas obsługi panelu sterowania.
   - ❏ Dźwięk błędu
     Ustaw głośność dźwięku błędów.
4. Dotknij pozycji **OK**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Wykrywanie podawania dwóch oryginałów

Możliwe jest włączenie funkcji wykrywania podawania dwóch arkuszy dokumentu do skanowania i zatrzymanie skanowania, gdy zostanie podanych wiele arkuszy.

Aby skanować oryginały, w przypadku których zwykle dochodzi do podawania wielu oryginałów, np. kopert lub papieru z naklejkami, wyłącz tę funkcję.

***Uwaga:***
*Można ją też ustawić za pomocą narzędzia Web Config lub Epson Scan 2.*

1. Na ekranie głównym dotknij pozycji **Ustaw.**.
2. Dotknij pozycji **Zewnętrzne Ustawienia skanowania** > **Ponaddźw. wykr. podw. załadow.**.
3. Dotknij pozycji **Ponaddźw. wykr. podw. załadow.**, aby włączyć ustawienie lub je wyłączyć.
4. Dotknij pozycji **Zamknij**.

## Konfigurowanie trybu niskiej prędkości

Aby zapobiec zacięciom papieru podczas skanowania cienkich dokumentów, takich jak karteczki, można włączyć skanowanie z niską prędkością.

1. Na ekranie głównym dotknij pozycji **Ustaw.**.
2. Dotknij pozycji **Zewnętrzne Ustawienia skanowania** > **Powoli**.
3. Dotknij pozycji **Powoli**, aby włączyć ustawienie lub je wyłączyć.
4. Dotknij pozycji **Zamknij**.

# Konfigurowanie ustawień za pomocą narzędzia Web Config

## Ustawienia oszczędzania energii w trakcie bezczynności

Można skonfigurować ustawienia oszczędzania energii w przypadku bezczynności skanera. Czas należy dopasować do własnego środowiska pracy.

***Uwaga:***
*Ustawienia oszczędzania energii można też konfigurować na panelu sterowania skanera.*

1. Otwórz narzędzie Web Config i wybierz pozycje **System Settings** > **Power Saving**.
2. W polu **Sleep Timer** wprowadź żądany czas braku aktywności, po którym urządzenie będzie przełączane w tryb oszczędzania energii.

   Maksymalnie można ustawić 240 minut z dokładnością do jednej minuty.
3. Ustaw czas wyłączenia w polu **Power Off Timer**.
4. Kliknij przycisk **OK**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Konfigurowanie panelu sterowania

Można skonfigurować działanie panelu sterowania skanera. Procedura jest następująca.

1. Otwórz narzędzie Web Config i wybierz pozycje **System Settings** > **Control Panel**.
2. W miarę potrzeby skonfiguruj następujące pozycje.

   ❏ Language

   Wybierz język wyświetlania panelu sterowania.

❏ Panel Lock

Jeśli zostanie wybrane ustawienie **ON**, do wykonania operacji wymagających uprawnień administratora trzeba będzie podać hasło administratora. Jeśli hasło administratora nie jest ustawione, funkcja blokady panelu jest wyłączona.

❏ Operation Timeout

Jeśli zostanie wybrane ustawienie **ON**, po zalogowaniu na konto administratora nastąpi automatyczne wylogowanie, gdy żadna czynność nie zostanie wykonana przez pewien czas.

Można ustawić okres od 10 sekund do 240 minut.

3. Kliknij przycisk **OK**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Konfigurowanie ograniczeń interfejsu zewnętrznego

Można ograniczyć połączenia USB z komputerem. Ustawienie można włączyć, aby ograniczyć skanowanie inne niż przez sieć.

1. Otwórz narzędzie Web Config i wybierz pozycje **System Settings** > **External Interface**.
2. Wybierz opcję **Enable** lub **Disable**.

   Aby ograniczyć, wybierz opcję **Disable**.
3. Dotknij pozycji **OK**.

## Synchronizowanie daty i godziny z serwerem czasu

Jeśli używany jest certyfikat wystawiony przez urząd certyfikacji, można zapobiegać problemom z godziną.

1. Otwórz narzędzie Web Config i wybierz pozycje **System Settings** > **Date and Time** > **Time Server**.
2. Wybierz opcję **Use** w polu **Use Time Server**.
3. Wprowadź adres serwera czasu w polu **Time Server Address**.

   Można użyć formatu IPv4, IPv6 lub FQDN. Wprowadź do 252 znaków. Jeśli opcja nie zostanie określona, trzeba zostawić ją pustą.
4. Wprowadź nazwę **Update Interval (min)**.

   Maksymalnie można ustawić 10 800 minut z dokładnością do jednej minuty.
5. Kliknij przycisk **OK**.

   ***Uwaga:***
   *Stan połączenia z serwerem czasu można sprawdzić na ekranie **Time Server Status**.*

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

# Podstawowe ustawienia zabezpieczeń

W tym rozdziale opisano podstawowe ustawienia zabezpieczeń, które nie wymagają specjalnego środowiska.

## Opis podstawowych funkcji zabezpieczeń

W tym rozdziale opisano podstawowe funkcje zabezpieczeń urządzeń firmy Epson.

| Nazwa funkcji | Typ funkcji | Konfigurowane opcje | Działania zapobiegawcze |
|---|---|---|---|
| Konfigurowanie hasła administratora | Blokowanie ustawień powiązanych z systemem, takich jak ustawienia sieci i połączenia USB, tak aby mogły być zmieniane wyłącznie przez administratora. | Administrator ustawia hasło do urządzenia.<br>Konfigurację lub aktualizację można wykonać z poziomu narzędzia Web Config, panelu sterowania, programu Epson Device Admin i EpsonNet Config. | Zapobieganie nieupoważnionemu odczytowi i zmianie informacji przechowywanych na urządzeniu, takich jak identyfikator, hasło, ustawienia sieciowe i kontakty. Ponadto ograniczenie różnorodnych zagrożeń bezpieczeństwa, takich jak możliwość ujawnienia informacji do otoczenia sieciowego lub zasad zabezpieczeń. |
| Komunikacja SSL/TLS | Podczas uzyskiwania dostępu do serwera Epson przez Internet z urządzenia, np. komunikacja z komputerem za pośrednictwem przeglądarki lub aktualizacja oprogramowania układowego, zawartość jest szyfrowana za pośrednictwem protokołu SSL/TLS. | Administrator musi uzyskać certyfikat podpisany przez zaufany urząd certyfikacji, a następnie zaimportować go na skanerze. | Identyfikacja urządzenia 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 drukowania i informacji o konfiguracji urządzenia. |
| Kontrolowanie protokołów | Kontrolowanie protokołów używanych do komunikacji między urządzeniami i komputerami, a także włączanie / wyłączanie 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. |

### Powiązane informacje

➡ „Informacje o Web Config” na stronie 22
➡ „Narzędzie EpsonNet Config” na stronie 55
➡ „Epson Device Admin” na stronie 55
➡ „Konfigurowanie hasła administratora” na stronie 33
➡ „Kontrola dostępu do protokołów” na stronie 35

# Konfigurowanie hasła administratora

Ustawienia hasła administratora uniemożliwi użytkownikom innym niż administratorzy modyfikowanie ustawień używanych do administrowania urządzeniem. Hasło administratora można ustawiać i zmieniać za pomocą narzędzia Web Config, panelu sterowania skanera lub oprogramowania (Epson Device Admin lub EpsonNet Config). Więcej informacji o używaniu oprogramowania można znaleźć w jego dokumentacji.

### Powiązane informacje

➡ „Konfigurowanie hasła administratora na panelu sterowania” na stronie 33

➡ „Konfigurowanie hasła administratora za pomocą narzędzia Web Config” na stronie 33

➡ „Narzędzie EpsonNet Config” na stronie 55

➡ „Epson Device Admin” na stronie 55

## Konfigurowanie hasła administratora na panelu sterowania

Możliwe jest ustawienie hasła administratora z poziomu panelu sterowania skanera.

1. Na ekranie głównym dotknij pozycji **Ustaw.**.
2. Dotknij pozycji **Administr. systemu** > **Ustawienia administratora**.

   Jeśli pozycja nie jest wyświetlana, przesuń ekran w górę, aby ją wyświetlić.
3. Dotknij pozycji **Hasło administratora** > **Zarejestruj**.
4. Wprowadź nowe hasło, a następnie dotknij przycisku **OK**.
5. Wprowadź hasło ponownie, a następnie dotknij przycisku **OK**.
6. Na ekranie potwierdzenia dotknij pozycji **OK**.

   Zostanie wyświetlony ekran ustawień administratora.
7. Dotknij pozycji **Zablokuj ustawienie**, a następnie na ekranie potwierdzenia przycisku **OK**.

   Opcja Zablokuj ustawienie zostanie ustawiona na **Wł.** i podczas uzyskiwania dostępu do zablokowanych pozycji menu będzie wyświetlany monit o hasło administratora.

***Uwaga:***

❏ *Jeśli dla opcji **Ustaw.** > **Ustawienia wspólne** > **Zak. czasu operacji** zostanie wybrane ustawienie **Wł.**, po pewnym okresie nieaktywności panelu sterowania zostanie wykonana operacja automatycznego wylogowania.*

❏ *Aby zmienić lub usunąć hasło administratora, należy nacisnąć przycisk **Zmień** lub **Resetuj** na ekranie **Hasło administratora**, a następnie wprowadzić hasło administratora.*

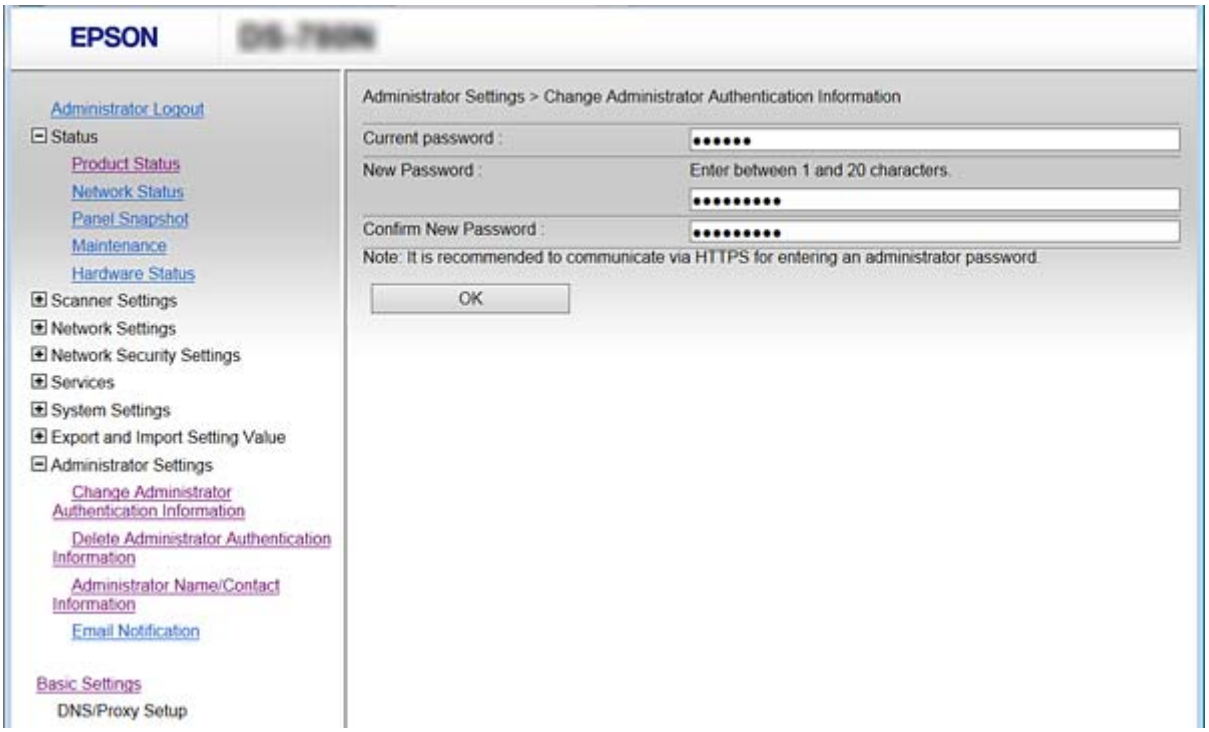
## Konfigurowanie hasła administratora za pomocą narzędzia Web Config

Można ustawić hasło administratora, używając narzędzia Web Config.

1. Otwórz narzędzie Web Config i wybierz pozycje **Administrator Settings** > **Change Administrator Authentication Information**.

2. Wprowadź hasło w polach **New Password** oraz **Confirm New Password**. Wprowadź nazwę użytkownika w razie potrzeby.

   Aby zmienić hasło na nowe, wprowadź bieżące hasło.




3. Naciśnij przycisk **OK**.

   ***Uwaga:***

   ❏ *Aby skonfigurować lub zmienić zablokowane pozycje menu, należy kliknąć pozycję **Administrator Login**, a następnie wprowadzić hasło administratora.*

   ❏ *Aby usunąć hasło administratora, należy kliknąć pozycje **Administrator Settings** > **Delete Administrator Authentication Information**, a następnie wprowadzić hasło administratora.*

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

# Pozycje, które można zablokować przy użyciu hasła administratora

Administratorzy mają uprawnienia do ustawiania i zmiany wszystkich funkcji urządzenia.

Co więcej, ustawiając hasło administratora na urządzeniu, można zablokować możliwość zmiany pozycji związanych z zarządzaniem urządzeniem.

Poniżej przedstawiono pozycje, które może kontrolować administrator.

| Pozycja | Opis |
|---|---|
| Ustawienia skanera | Ustawienia wykrywania podawania dwóch oryginałów i trybu niskiej prędkości. |

**Podstawowe ustawienia zabezpieczeń**

| Pozycja | Opis |
|---|---|
| Ustawienia połączenia Ethernet | Zmiana nazwy urządzeń i adresu IP, konfiguracja serwera DNS lub serwera proxy, a także zmiany ustawień związanych z połączeniami sieciowymi. |
| Ustawienia usług użytkownika | Konfiguracja kontroli protokołów komunikacyjnych, skanowania sieciowego i usług Document Capture Pro. |
| Ustawienia serwera poczty e-mail | Konfiguracja serwera poczty e-mail, z którym urządzenia komunikują się bezpośrednio. |
| Ustawienia zabezpieczeń | Ustawienia zabezpieczeń sieciowych, takie jak komunikacja SSL/TLS, IPsec/filtrowanie IP i IEEE802.1X. |
| Aktualizacja głównego certyfikatu | Aktualizacja głównych certyfikatów wymaganych do uwierzytelniania Document Capture Pro Server i aktualizacja oprogramowania układowego za pomocą narzędzia Web Config. |
| Aktualizacja oprogramowania układowego | Sprawdzanie i aktualizacja oprogramowania układowego urządzeń. |
| Ustawienia godziny, minutnika | Czas przełączenia w tryb uśpienia, funkcja automatycznego wyłączenia, data/godzina, czas braku aktywności, inne ustawienia powiązane z minutnikiem. |
| Przywracanie ustawień domyślnych | Konfigurowanie skanera umożliwiające przywrócenie ustawień fabrycznych. |
| Ustawienia administratora | Ustawienia blokady administratora lub hasła administratora. |
| Ustawienia certyfikowanego urządzenia | Konfigurowanie identyfikatora urządzenia uwierzytelniającego. Włącz tę opcję w przypadku używania skanera w systemie uwierzytelniania obsługującym urządzenia uwierzytelniające. |

# Kontrola dostępu do protokołów

Przy skanowaniu można korzystać z rozmaitych ścieżek i protokołów. Można też używać skanowania sieciowego z nieograniczonej liczby komputerów przyłączonych do sieci. Przykładowo dozwolone jest tylko skanowanie z określonych ścieżek i przy użyciu konkretnych protokołów. Powstające przy tym zagrożenia można zredukować, wprowadzając ograniczenia w skanowaniu z pewnych ścieżek lub kontrolując dostęp do funkcji.

Skonfiguruj ustawienia protokołów.

1. Otwórz narzędzie Web Config i wybierz pozycje **Services** > **Protocol**.
2. Skonfiguruj poszczególne parametry.
3. Kliknij przycisk **Next**.
4. Kliknij przycisk **OK**.

   Ustawienia zostaną zastosowane do skanera.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Protokoły, które można włączyć lub wyłączyć” na stronie 36

➡ „Opcje ustawień protokołów” na stronie 37

# Protokoły, które można włączyć lub wyłączyć

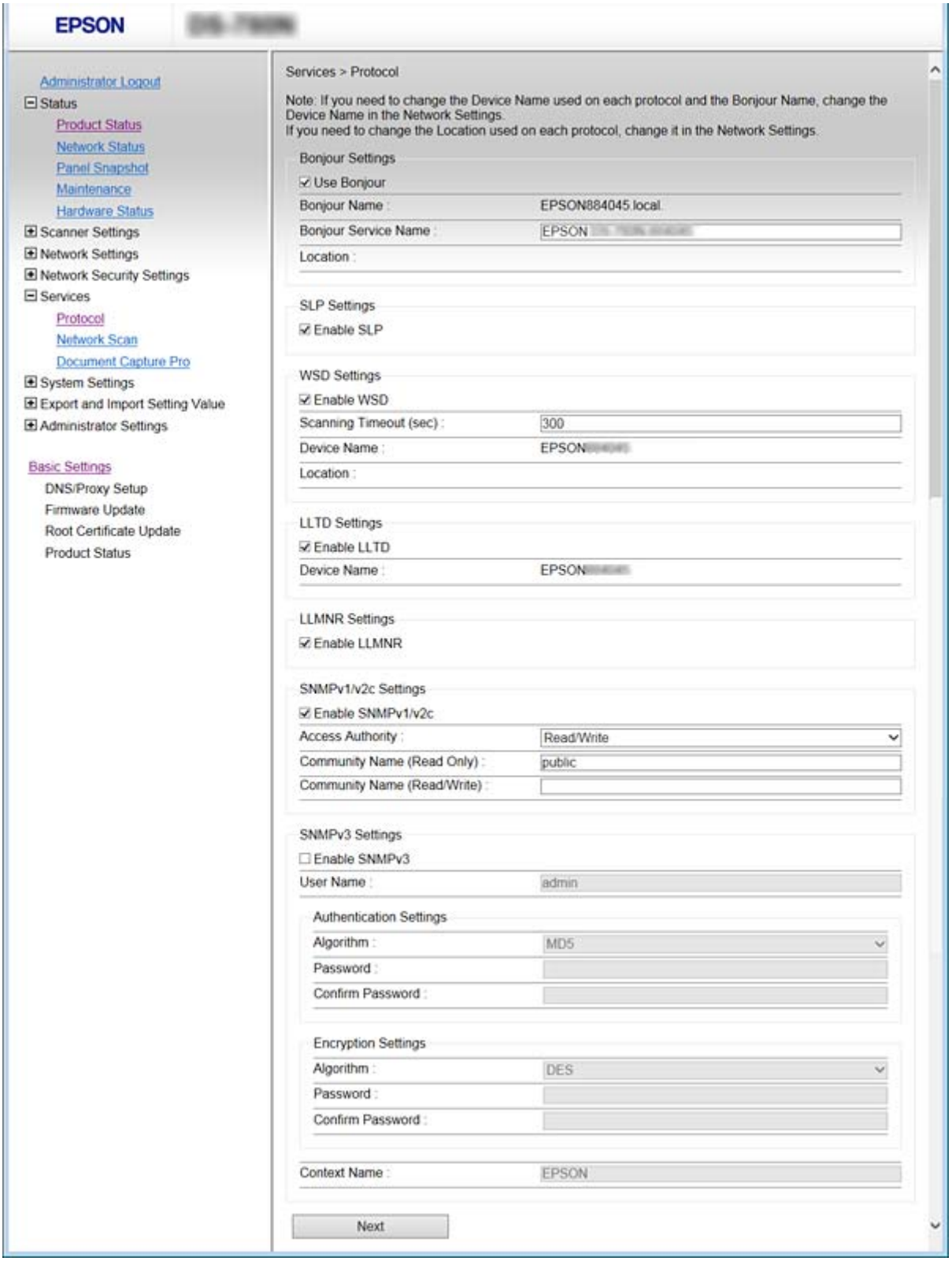
| Protokół | Opis |
|---|---|
| Bonjour Settings | Określa, czy ma być używany protokół Bonjour. Bonjour jest protokołem używanym do wykrywania urządzeń, skanowania i innych usług. |
| SLP Settings | Pozwala włączyć lub wyłączyć funkcję SLP. SLP jest protokołem używanym w narzędziu Epson Scan 2 i wyszukiwania sieci w aplikacji EpsonNet Config. |
| WSD Settings | Pozwala włączyć lub wyłączyć funkcję WSD. Po jej włączeniu można dodawać urządzenia WSD lub skanować za pośrednictwem portu WSD. |
| LLTD Settings | Pozwala włączyć lub wyłączyć funkcję LLTD. Po jej włączeniu opcja ta jest wyświetlana w mapie sieci systemu Windows. |
| LLMNR Settings | Pozwala włączyć lub wyłączyć funkcję LLMNR. Po jej włączeniu można używać interpretacji nazw bez pośrednictwa usług NetBIOS, nawet przy braku dostępu do DNS. |
| SNMPv1/v2c Settings | Określa, czy ma być włączona funkcja SNMPv1/v2c. Służy ona między innymi do konfigurowania i monitorowania urządzeń. |
| SNMPv3 Settings | Określa, czy ma być włączona funkcja SNMPv3. Służy ona między innymi do konfigurowania i monitorowania urządzeń zaszyfrowanych itd. |

### Powiązane informacje

➡ „Kontrola dostępu do protokołów” na stronie 35

➡ „Opcje ustawień protokołów” na stronie 37

# Opcje ustawień protokołów




| Elementy | Wartość i opis |
|---|---|
| Bonjour Settings | |

## Podstawowe ustawienia zabezpieczeń

| Elementy | Wartość i opis |
|---|---|
| Use Bonjour | Zaznacz tę opcję, aby używać protokołu Bonjour do wyszukiwania i obsługi urządzeń. |
| Bonjour Name | Wyświetla nazwę Bonjour. |
| Bonjour Service Name | Można wyświetlić i ustawić nazwę usługi Bonjour. |
| Location | Wyświetla nazwę lokalizacji Bonjour. |
| SLP Settings | |
| Enable SLP | Zaznacz tę opcję, aby włączyć funkcję SLP. Służy do wykrywania sieci w aplikacji Epson Scan 2 i narzędziu EpsonNet Config. |
| WSD Settings | |
| Enable WSD | Zaznacz tę opcję, aby umożliwić dodawanie urządzeń za pomocą WSD oraz drukowanie i skanowanie przez port WSD. |
| Scanning Timeout (sec) | Określ limit czasu komunikacji podczas skanowania przez WSD, wprowadzając wartość z zakresu od 3 do 3600 sekund. |
| Device Name | Wyświetla nazwę urządzenia WSD. |
| Location | Wyświetla nazwę lokalizacji WSD. |
| LLTD Settings | |
| Enable LLTD | Ta opcja włącza protokół LLTD. Skaner jest wyświetlany na mapie sieci Windows. |
| Device Name | Wyświetla nazwę urządzenia LLTD. |
| LLMNR Settings | |
| Enable LLMNR | Ta opcja włącza protokół LLMNR. Można korzystać z interpretacji nazw bez pośrednictwa usług NetBIOS, nawet przy braku dostępu do DNS. |
| SNMPv1/v2c Settings | |
| Enable SNMPv1/v2c | Ta opcja włącza protokół SNMPv1/v2c. Wyświetlane są tylko skanery z obsługą protokołu SNMPv3. |
| Access Authority | Określ uprawnienia dostępu, gdy włączony jest protokół SNMPv1/v2c. Wybierz opcję **Read Only** lub **Read/Write**. |
| Community Name (Read Only) | Wprowadź od 0 do 32 znaków ASCII (0x20 do 0x7E). |
| Community Name (Read/Write) | Wprowadź od 0 do 32 znaków ASCII (0x20 do 0x7E). |
| SNMPv3 Settings | |
| Enable SNMPv3 | Włączenie protokołu SNMPv3 (zaznaczenie pola). |
| User Name | Wprowadzenie od 1 do 32 znaków jednobajtowych. |
| Authentication Settings | |
| Algorithm | Wybór algorytmu uwierzytelniania na potrzeby protokołu SNMPv3. |

**Podstawowe ustawienia zabezpieczeń**

| Elementy | Wartość i opis |
|---|---|
| Password | Wprowadzanie hasła uwierzytelniania na potrzeby protokołu SNMPv3.<br>Wprowadź od 8 do 32 znaków ASCII (0x20–0x7E). Jeśli opcja nie zostanie określona, trzeba zostawić ją pustą. |
| Confirm Password | Wprowadź skonfigurowane hasło w celu potwierdzenia. |
| Encryption Settings | |
| Algorithm | Wybór algorytmu szyfrowania na potrzeby protokołu SNMPv3. |
| Password | Wprowadzanie hasła szyfrowania na potrzeby protokołu SNMPv3.<br>Wprowadź od 8 do 32 znaków ASCII (0x20–0x7E). Jeśli opcja nie zostanie określona, trzeba zostawić ją pustą. |
| Confirm Password | Wprowadź skonfigurowane hasło w celu potwierdzenia. |
| Context Name | Wprowadzenie do 32 znaków w formacie Unicode (UTF-8). Jeśli opcja nie zostanie określona, trzeba zostawić ją pustą. Liczba znaków, które można wprowadzić, zależy od języka. |

### Powiązane informacje

➡ „Kontrola dostępu do protokołów” na stronie 35

➡ „Protokoły, które można włączyć lub wyłączyć” na stronie 36

# Ustawienia obsługi i zarządzania

W tym rozdziale przedstawiono pozycje związane z codziennymi czynnościami i zarządzaniem urządzeniem.

## Sprawdzanie informacji o urządzeniu

Można przeglądać następujące informacje o urządzeniu na karcie **Status** w narzędziu Web Config.

❏ Product Status

Przeglądanie informacji o języku, stanie, numerze produktu, adresie MAC itd.

❏ Network Status

Przeglądanie informacji o stanie połączenia sieciowego, adresie IP, adresie serwera DNS itd.

❏ Panel Snapshot

Wyświetlanie zrzutu obrazu ekranu z panelu sterowania urządzenia.

❏ Maintenance

Przeglądanie daty początkowej, informacji o skanowaniu itd.

❏ Hardware Status

Przeglądanie stanu skanera.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Zarządzanie urządzeniami (Epson Device Admin)

Możliwe jest zarządzanie i obsługiwanie wielu urządzeń za pomocą narzędzia Epson Device Admin. Program Epson Device Admin umożliwia zarządzanie urządzeniami z innych sieci. W tym rozdziale przedstawiono główne funkcje służące do zarządzania urządzeniami.

Więcej informacji o funkcjach i sposobie używania oprogramowania można znaleźć w dokumentacji programu Epson Device Admin oraz jego systemie pomocy.

❏ Wykrywanie urządzeń

Można wykrywać urządzenia w sieci i zapisywać je na liście. Jeśli urządzenia Epson, takie jak drukarki i skanery, są połączone z tym samym segmentem sieci, co komputer administratora, można znaleźć je, nawet gdy nie mają przydzielonych adresów IP.

Możliwe jest też wykrywanie urządzeń podłączonych kablem USB do komputerów w sieci. Aby można to było zrobić, należy na komputerze zainstalować oprogramowanie Epson Device USB Agent.

❏ Konfigurowanie urządzeń

Można utworzyć szablon z pozycjami ustawień, takimi jak interfejs sieciowy i źródło papieru, a następie zastosować je do innych urządzeń w ramach udostępnianych ustawień. Jeśli urządzenie jest połączone z siecią, można przydzielić mu adres IP, o ile jeszcze go nie ma.

❏ Monitorowanie urządzeń

Można regularnie pobierać informacje o stanie i inne szczegółowe dane dotyczące urządzeń w sieci. Możliwe jest też monitorowanie urządzeń podłączonych kablem USB do komputerów w sieci, a także urządzeń innych firm, które zostały dodane do listy urządzeń. Aby monitorować urządzenia podłączone kablami USB, należy zainstalować oprogramowanie Epson Device USB Agent.

❏ Zarządzanie alertami

Można monitorować alerty o stanie urządzeń i materiałów eksploatacyjnych. System automatycznie wysyła powiadomienia e-mail do administratora na podstawie zdefiniowanych kryteriów.

❏ Zarządzanie raportami

Można tworzyć raporty w miarę gromadzenia danych na temat użycia urządzeń i materiałów eksploatacyjnych. Raporty można zapisywać i wysyłać je pocztą e-mail.

**Powiązane informacje**

➡ „Epson Device Admin” na stronie 55

# Otrzymywanie powiadomień e-mail w przypadku występowania zdarzeń

## Informacje o powiadomieniach e-mail

Funkcji tej można używać, aby otrzymywać alerty pocztą e-mail w razie wystąpienia zdarzeń. Można zarejestrować do pięciu adresów e-mail i wybrać zdarzenia, dla których mają być wysyłane powiadomienia.

Aby móc używać tej funkcji, trzeba skonfigurować serwer poczty.

**Powiązane informacje**

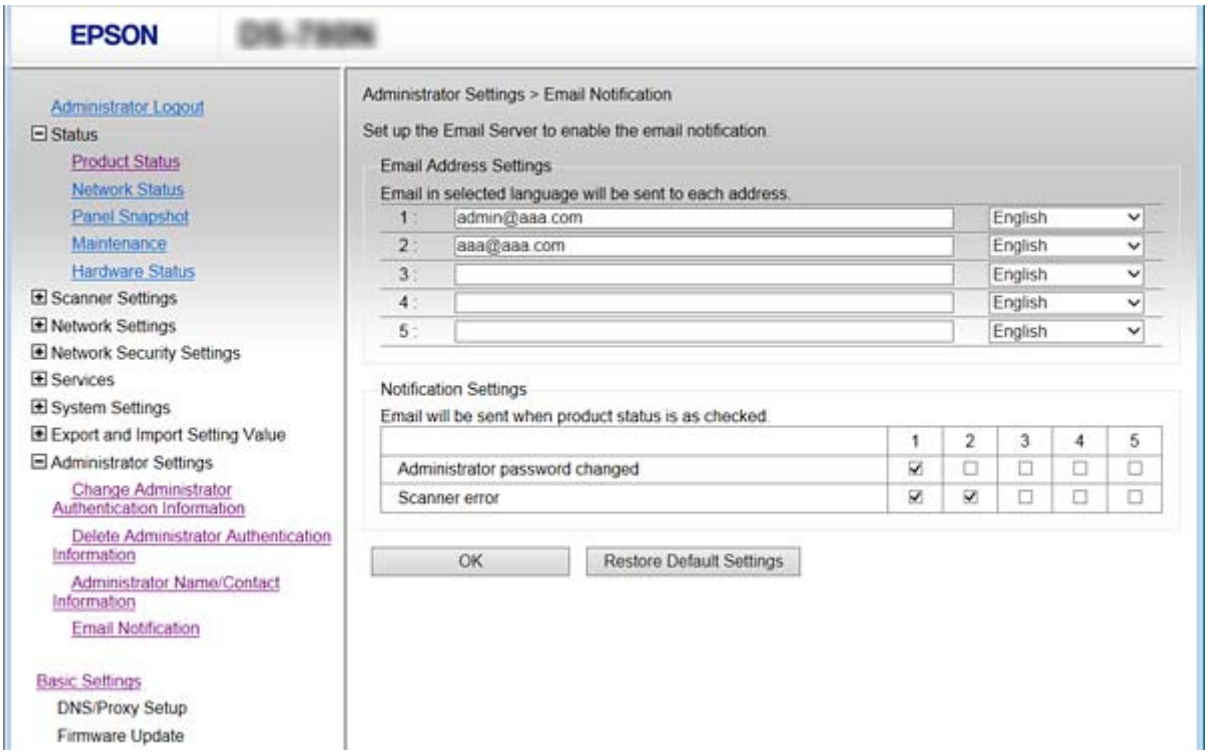
➡ „Konfigurowanie serwera pocztowego” na stronie 42

## Konfigurowanie powiadomień e-mail

Aby można było używać tej funkcji, należy uprzednio skonfigurować serwer pocztowy.

1. Otwórz aplikację Web Config i wybierz pozycje **Administrator Settings** > **Email Notification**.
2. Wprowadź adres e-mail, na który chcesz otrzymywać powiadomienia e-mail.
3. Wybierz język powiadomień e-mail.

4. Zaznacz pola wyboru rodzajów powiadomień, które chcesz otrzymywać.




5. Kliknij przycisk **OK**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Konfigurowanie serwera pocztowego” na stronie 42

## Konfigurowanie serwera pocztowego

Przed dalszą częścią procedury.

❏ Sprawdź, czy skaner jest podłączony do sieci.

❏ Sprawdź dane serwera e-mail z komputera.

1. Otwórz aplikację Web Config i wybierz pozycje **Network Settings** > **Email Server** > **Basic**.

2. Wprowadź wartość dla każdej pozycji.

3. Kliknij przycisk **OK**.

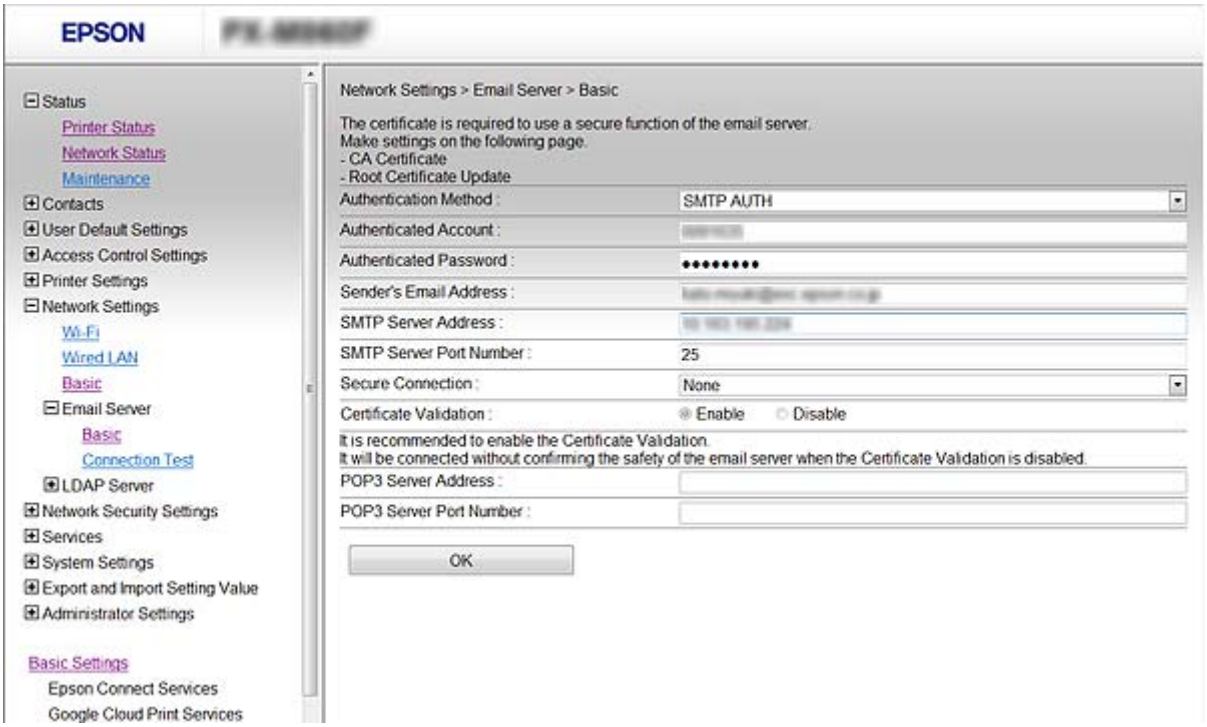
   Wyświetlone zostaną wybrane ustawienia.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Opcje ustawień serwera pocztowego” na stronie 43

# Opcje ustawień serwera pocztowego




| Obsługiwane algorytmy | Ustawienia i objaśnienie | |
|---|---|---|
| Authentication Method | Określ metodę uwierzytelniania używaną przez skaner w celu uzyskania dostępu do serwera pocztowego. | |
| | Off | Uwierzytelnianie jest wyłączone w przypadku komunikacji z serwerem pocztowym. |
| | SMTP AUTH | Serwer pocztowy musi obsługiwać uwierzytelnianie SMTP. |
| | POP before SMTP | W przypadku wybrania tej metody należy skonfigurować serwer POP3. |
| Authenticated Account | Jeśli dla opcji **Authentication Method** zostanie wybrane ustawienie **SMTP AUTH** lub **POP before SMTP**, wprowadź nazwę uwierzytelnianego konta o długości od 0 do 255 znaków ASCII (0x20–0x7E). | |
| Authenticated Password | Jeśli dla opcji **Authentication Method** zostanie wybrane ustawienie **SMTP AUTH** lub **POP before SMTP**, wprowadź hasło uwierzytelniania o długości od 0 do 20 znaków A–Z a–z 0–9 ! # $ % & ' * + -. / = ? ^ _ { \| } ~ @. | |
| Sender's Email Address | Podaj adres e-mail nadawcy. Wprowadź od 0 do 255 znaków ASCII (0x20–0x7E) z wyjątkiem następujących znaków: : ( ) < > [ ] ; ¥. Kropka „.” nie może być pierwszym znakiem. | |
| SMTP Server Address | Wprowadź od 0 do 255 znaków: A–Z a–z 0–9. -. Można użyć formatu IPv4 lub FQDN. | |
| SMTP Server Port Number | Podaj liczbę od 1 do 65535. | |

| Obsługiwane algorytmy | Ustawienia i objaśnienie | |
|---|---|---|
| Secure Connection | Określ bezpieczną metodę połączenia dla serwera e-mail. | |
| | None | Jeśli wybrano opcję **POP before SMTP** jako ustawienie **Authentication Method**, metoda połączenia będzie mieć ustawienie **None**. |
| | SSL/TLS | Opcja ta jest dostępna, jeśli **Authentication Method** ma ustawienie **Off** lub **SMTP AUTH**. |
| | STARTTLS | Opcja ta jest dostępna, jeśli **Authentication Method** ma ustawienie **Off** lub **SMTP AUTH**. |
| Certificate Validation | Włączenie tej opcji powoduje zweryfikowanie certyfikatu. Zalecane jest ustawienie **Enable**. | |
| POP3 Server Address | Jeśli dla opcji **Authentication Method** zostanie wybrane ustawienie **POP before SMTP**, wprowadź adres serwera POP3 o długości od 0 do 255 znaków A–Z a–z 0–9. -. Można użyć formatu IPv4 lub FQDN. | |
| POP3 Server Port Number | Jeśli dla opcji **Authentication Method** zostanie wybrane ustawienie **POP before SMTP**, wprowadź liczbę z zakresu od 1 do 65535. | |

### Powiązane informacje

➡ „Konfigurowanie serwera pocztowego” na stronie 42

## Sprawdzanie połączenia z serwerem pocztowym

1. Otwórz aplikację Web Config i wybierz pozycje **Network Settings** > **Email Server** > **Connection Test**.
2. Kliknij przycisk **Start**.

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

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Objaśnienia do testu połączenia z serwerem pocztowym” na stronie 44

## Objaśnienia do testu połączenia z serwerem pocztowym

| Komunikat | Objaśnienie |
|---|---|
| Connection test was successful. | Ten komunikat jest wyświetlany w przypadku pomyślnego nawiązania połączenia z serwerem. |
| SMTP server communication error. Check the following. - Network Settings | Ten komunikat pojawia się w następujących sytuacjach<br>❏ Skaner nie jest podłączony do sieci<br>❏ Serwer SMTP jest wyłączony<br>❏ Połączenie sieciowe zostało zerwane w trakcie komunikacji<br>❏ Odebrano niekompletne dane |

**Ustawienia obsługi i zarządzania**

| Komunikat | Objaśnienie |
|---|---|
| POP3 server communication error. Check the following. - Network Settings | Ten komunikat pojawia się w następujących sytuacjach<br>❏ Skaner nie jest podłączony do sieci<br>❏ Serwer POP3 jest wyłączony<br>❏ Połączenie sieciowe zostało zerwane w trakcie komunikacji<br>❏ Odebrano niekompletne dane |
| An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server | Ten komunikat pojawia się w następujących sytuacjach<br>❏ Nie udało się nawiązać połączenia z serwerem DNS<br>❏ Nie udało się zinterpretować nazwy serwera SMTP |
| An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server | Ten komunikat pojawia się w następujących sytuacjach<br>❏ Nie udało się nawiązać połączenia z serwerem DNS<br>❏ Nie udało się zinterpretować nazwy serwera POP3 |
| SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password | Ten komunikat pojawia się po nieudanym uwierzytelnieniu na serwerze SMTP. |
| POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password | Ten komunikat pojawia się po nieudanym uwierzytelnieniu na serwerze POP3. |
| Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number | Ten komunikat pojawia się w przypadku próby połączenia za pomocą nieobsługiwanych protokołów. |
| Connection to SMTP server failed. Change Secure Connection to None. | Ten komunikat pojawia się w przypadku niezgodności SMTP między serwerem a klientem lub gdy serwer nie obsługuje zabezpieczonego połączenia SMTP (połączenie SSL). |
| Connection to SMTP server failed. Change Secure Connection to SSL/TLS. | Ten komunikat pojawia się w przypadku niezgodności SMTP między serwerem a klientem lub gdy serwer żąda użycia protokołu SSL/TLS w przypadku zabezpieczonego połączenia SMTP. |
| Connection to SMTP server failed. Change Secure Connection to STARTTLS. | Ten komunikat pojawia się w przypadku niezgodności SMTP między serwerem a klientem lub gdy serwer żąda użycia protokołu STARTTLS w przypadku zabezpieczonego połączenia SMTP. |
| The connection is untrusted. Check the following. - Date and Time | Ten komunikat oznacza, że ustawienia daty i godziny na skanerze są nieprawidłowe lub certyfikat stracił ważność. |
| The connection is untrusted. Check the following. - CA Certificate | Ten komunikat pojawia się, gdy skaner nie ma certyfikatu głównego, który odpowiadałby serwerowi lub gdy CA Certificate nie został zaimportowany. |
| The connection is not secured. | Ten komunikat pojawia się, gdy uzyskany certyfikat jest uszkodzony. |
| SMTP server authentication failed. Change Authentication Method to SMTP-AUTH. | Ten komunikat pojawia się w przypadku niezgodności metod uwierzytelnienia między serwerem a klientem. Serwer obsługuje SMTP AUTH. |
| SMTP server authentication failed. Change Authentication Method to POP before SMTP. | Ten komunikat pojawia się w przypadku niezgodności metod uwierzytelnienia między serwerem a klientem. Serwer nie obsługuje metody SMTP AUTH. |

| Komunikat | Objaśnienie |
|---|---|
| Sender's Email Address is incorrect. Change to the email address for your email service. | Ten komunikat pojawia się, gdy podany adres e-mail nadawcy jest nieprawidłowy. |
| Cannot access the product until processing is complete. | Ten komunikat jest wyświetlany, gdy skaner jest zajęty (nie odpowiada). |

**Powiązane informacje**

➡ „Sprawdzanie połączenia z serwerem pocztowym” na stronie 44

# Aktualizowanie oprogramowania układowego

## Aktualizowanie oprogramowania układowego za pomocą narzędzia Web Config

Możliwe jest zaktualizowanie oprogramowania układowego za pomocą narzędzia Web Config. Urządzenie musi być połączone z Internetem.

1. Otwórz narzędzie Web Config i wybierz pozycje **Basic Settings** > **Firmware Update**.
2. Kliknij przycisk **Start**.

   Zostanie wyświetlone potwierdzenie aktualizacji oprogramowania układowego, a także informacje o oprogramowaniu układowym, jeśli jest dostępna aktualizacja.
3. Kliknij przycisk **Start**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

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

**Powiązane informacje**

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Epson Device Admin” na stronie 55

## Aktualizowanie oprogramowania układowego za pomocą programu Epson Firmware Updater

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.

1. Otwórz witrynę firmy Epson i pobierz oprogramowanie układowe.
2. Połącz komputer z pobranym oprogramowaniem układowym z urządzeniem za pomocą kabla USB.

3. Kliknij dwukrotnie pobrany plik .exe.

   Zostanie uruchomiony program Epson Firmware Updater.

4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

# Tworzenie kopii zapasowej ustawień

Eksportując pozycje ustawień w narzędziu Web Config, można skopiować je do innych skanerów.

## Eksport ustawień

Eksportuj wszystkie ustawienia skanera.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Export and Import Setting Value** > **Export**.

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. Podaj hasło do zaszyfrowania eksportowanego pliku.

   Hasło trzeba będzie później podać przy imporcie. Pozostaw puste pole, jeśli nie chcesz szyfrować pliku.

4. Kliknij przycisk **Export**.

> ***Ważne:***
>
> *Aby wyeksportować ustawienia sieciowe skanera, jak nazwa i adres IP, zaznacz opcję **Enable to select the individual settings of device** i wybierz dodatkowe pozycje. Wybranych wartości należy używać tylko w przypadku skanera zastępczego.*

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Import ustawień

Zaimportuj wyeksportowany plik Web Config na skanerze.

> ***Ważne:***
>
> *Przy importowaniu ustawień zawierających nazwę skanera lub jego adres IP należy się upewnić, czy nie są one powielane w obrębie tej samej sieci. Jeśli adres IP jest powielony, nie zostanie wprowadzony do konfiguracji skanera.*

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Export and Import Setting Value** > **Import**.

2. Wybierz wyeksportowany plik i podaj hasło szyfrowania.

3. Kliknij przycisk **Next**.

4. Zaznacz ustawienia, które mają być zaimportowane, a następnie kliknij przycisk **Next**.
5. Kliknij przycisk **OK**.

Ustawienia zostaną zastosowane do skanera.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

# Rozwiązywanie problemów

## Wskazówki dotyczące rozwiązywania problemów

Więcej informacji na temat rozwiązywania problemów można znaleźć w poniższym podręczniku.

❏ Przewodnik użytkownika

Zawiera instrukcje dotyczące używania skanera, konserwacji i rozwiązywania problemów.

## Sprawdzanie dziennika serwera i urządzenia sieciowego

W razie problemów z połączeniem sieciowym można określić przyczynę, sprawdzając dzienniki serwera poczty, serwera LDAP itd., sprawdzając stan urządzenia, przeglądając dziennik sieciowy, dziennik systemowy urządzenia sieciowego, np. routera, lub dziennik poleceń.

## Inicjowanie ustawień sieciowych

### Przywracanie ustawień sieci za pomocą panelu sterowania

Można przywrócić wszystkie domyślne ustawienia sieciowe.

1. Na ekranie głównym dotknij pozycji **Ustaw.**.
2. Dotknij pozycji **Administr. systemu** > **Przywr. ust. domyśl.** > **Ustawienia sieciowe**.
3. Sprawdź komunikat, a następnie dotknij pozycji **Tak**.
4. Kiedy zostanie wyświetlony komunikat z potwierdzeniem zakończenia operacji, dotknij przycisku **Zamknij**.

   Ekran zostanie zamknięty automatycznie, jeśli przycisk nie zostanie dotknięty **Zamknij** przez określony czas.

## Sprawdzanie komunikacji między urządzeniami i komputerami

### Sprawdzanie połączenia przy użyciu polecenia ping — Windows

Polecenie ping umożliwia sprawdzenie, czy komputer jest połączony ze skanerem. Wykonaj poniższe czynności, aby sprawdzić połączenie za pomocą polecenia ping.

1. Sprawdź adres IP połączenia skanera, które ma być przetestowane.

   Można to sprawdzić za pomocą aplikacji Epson Scan 2.

2. Wyświetl ekran wiersza poleceń komputera.

   ❏ Windows 10

   Kliknij prawym przyciskiem myszy przycisk Start lub naciśnij i przytrzymaj go, a następnie wybierz polecenie **Wiersz polecenia**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Wyświetl ekran aplikacji, a następnie wybierz pozycję **Wiersz polecenia**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 lub starszy

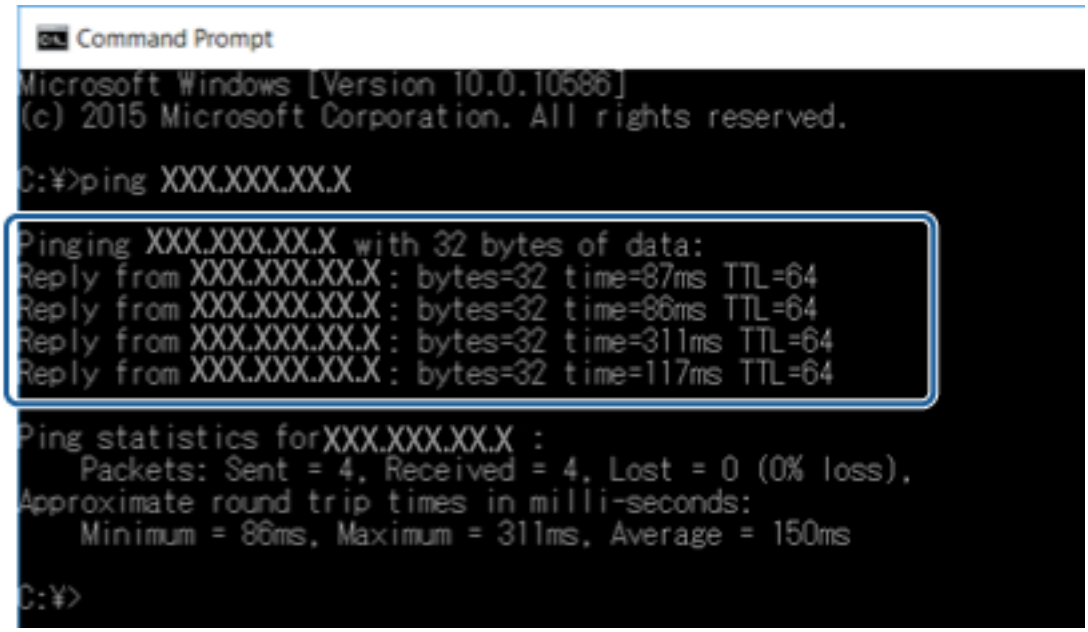
   Kliknij przycisk Start, wybierz polecenie **Wszystkie programy** lub **Programy** > **Akcesoria** > **Wiersz polecenia**.

3. Wprowadź polecenie „ping xxx.xxx.xxx.xxx”, a następnie naciśnij klawisz Enter.

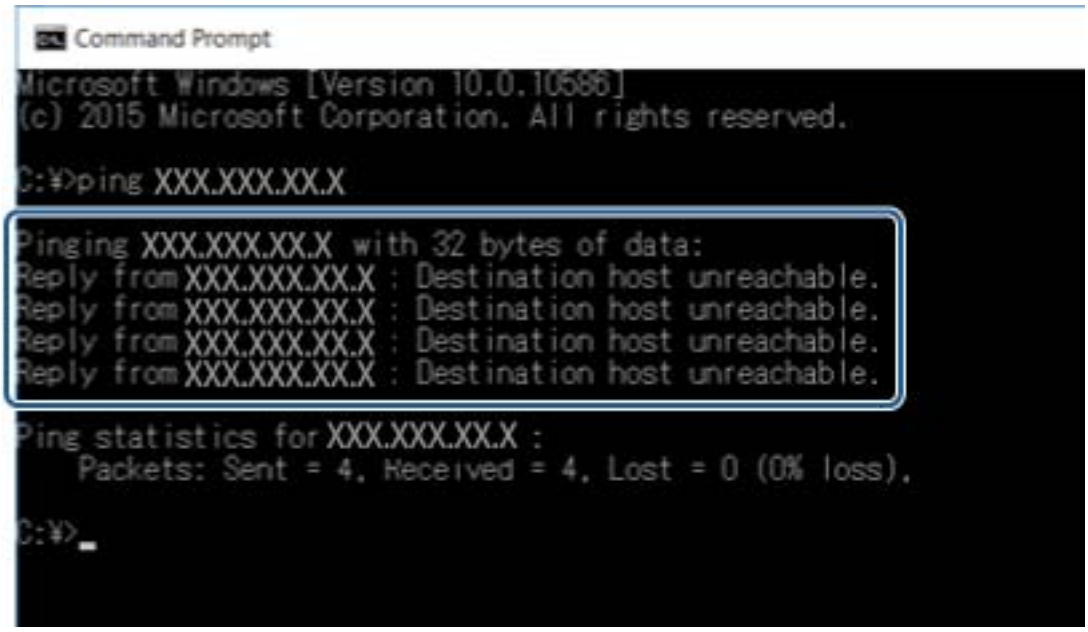
   Wprowadź adres IP skanera, tj. xxx.xxx.xxx.xxx.

4. Sprawdź stan komunikacji.

   Jeżeli skaner i komputer komunikują się ze sobą, wyświetlany jest następujący komunikat.



Jeżeli skaner i komputer nie komunikują się ze sobą, wyświetlany jest następujący komunikat.




## Sprawdzanie połączenia przy użyciu polecenia ping — Mac OS

Polecenie ping umożliwia sprawdzenie, czy komputer jest połączony ze skanerem. Wykonaj poniższe czynności, aby sprawdzić połączenie za pomocą polecenia ping.

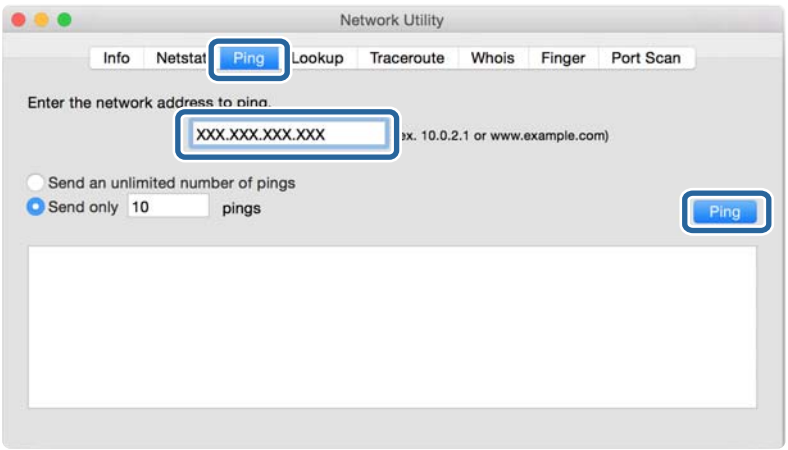
1. Sprawdź adres IP połączenia skanera, które ma być przetestowane.

   Można to sprawdzić za pomocą aplikacji Epson Scan 2.

2. Uruchomić narzędzie sieciowe Network Utility.

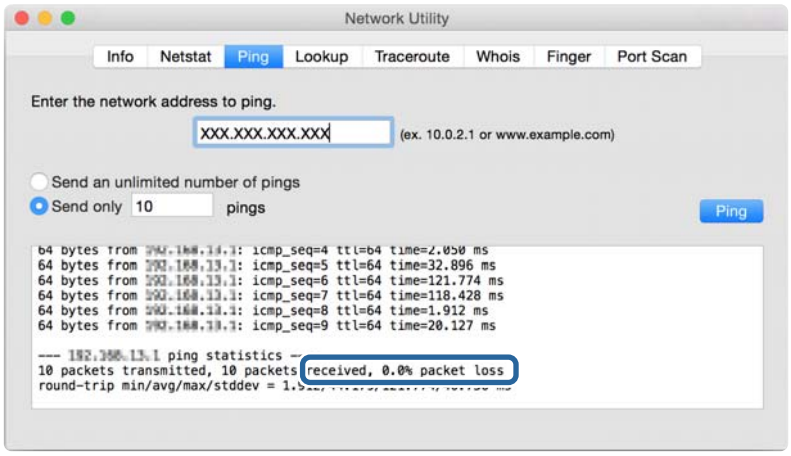
   Wejść w narzędzie „Network Utility” w aplikacji **Spotlight**.

3. Kliknąć zakładkę **Ping**, wprowadzić adres IP sprawdzony w kroku 1, a następnie kliknąć przycisk **Ping**.

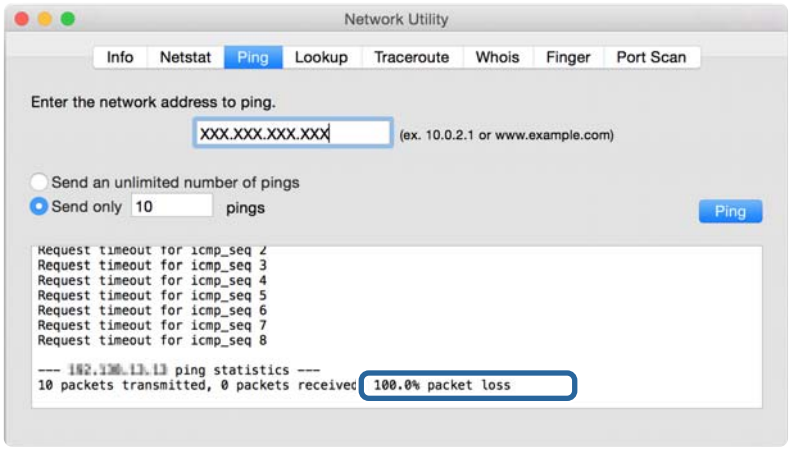


4. Sprawdzić status komunikacji.

   Jeśli skaner i komputer komunikują się ze sobą, wyświetlany jest następujący komunikat.




   Jeśli skaner i komputer nie komunikują się ze sobą, wyświetlany jest następujący komunikat.




# Problemy z używaniem oprogramowania sieciowego

## Nie można uzyskać dostępu do narzędzia Web Config

### Czy adres IP skanera został prawidłowo skonfigurowany?

Ustaw adres IP za pomocą aplikacji Epson Device Admin lub EpsonNet Config.

### Czy przeglądarka obsługuje szyfrowanie wsadowe na potrzeby ustawienia Encryption Strength protokołu SSL/TLS?

Szyfrowanie wsadowe na potrzeby ustawienia Encryption Strength protokołu SSL/TLS opisano poniżej. Dostęp do aplikacji Web Config można uzyskać tylko w przeglądarce obsługującej następujące szyfrowanie wsadowe. Sprawdź, jakie standardy szyfrowania obsługuje używana przeglądarka internetowa.

❏ 80-bitowe: AES256/AES128/3DES

❏ 112-bitowe: AES256/AES128/3DES

❏ 128-bitowe: AES256/AES128

❏ 192-bitowe: AES256

❏ 256-bitowe: AES256

### Podczas uzyskiwania dostępu do aplikacji Web Config przy użyciu szyfrowania SSL (https) wyświetlany jest komunikat „Nieaktualny”.

Jeśli certyfikat jest nieaktualny, pobierz certyfikat ponownie. Jeśli komunikat jest wyświetlany przed upływem daty ważności certyfikatu, sprawdź, czy ustawienie daty i godziny na skanerze jest prawidłowe.

### Podczas uzyskiwania dostępu do aplikacji Web Config przy użyciu szyfrowania SSL (https) wyświetlany jest komunikat „Nazwa certyfikatu zabezpieczeń nie jest zgodna z…”.

Adres IP skanera podany w polu **Common Name** na potrzeby utworzenia certyfikatu z podpisem własnym lub żądania CSR nie jest zgodny z adresem wpisanym w przeglądarce internetowej. Uzyskaj i zaimportuj certyfikat ponownie lub zmień nazwę skanera.

### Dostęp do skanera odbywa się za pośrednictwem serwera proxy.

W przypadku korzystania w skanerze z serwera proxy należy skonfigurować ustawienia proxy w przeglądarce internetowej.

❏ Windows:

Wybierz kolejno pozycje **Panel sterowania** > **Sieć i Internet** > **Opcje internetowe** > **Połączenia** > **Ustawienia sieci LAN** > **Serwer proxy**, po czym zaznacz pole wyboru „Nie używaj serwera proxy dla adresów lokalnych”.

❏ Mac OS:

Wybierz kolejno opcje **Preferencje systemowe** > **Sieć** > **Zaawansowane** > **Proxy**, po czym podaj adres lokalny w polu **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

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Przydzielanie adresu IP” na stronie 15

➡ „Przydzielanie adresu IP za pomocą programu EpsonNet Config” na stronie 56

## Nazwa modelu drukarki i/lub adres IP nie są wyświetlane w aplikacji EpsonNet Config

### Czy wybrana została opcja Zablokuj, Anuluj lub Wyłącz po wyświetleniu ekranu zabezpieczeń lub ekranu zapory sieciowej systemu Windows?

Wybranie opcji **Zablokuj**, **Anuluj** lub **Wyłącz** powoduje niewyświetlenie adresu IP i nazwy modelu w aplikacji EpsonNet Config lub EpsonNet Setup.

Aby naprawić ten błąd, zarejestruj aplikację EpsonNet Config jako wyjątek w regułach zapory systemu Windows i/lub w innym oprogramowaniu zabezpieczającym. W przypadku korzystania z programu antywirusowego lub zabezpieczającego zamknij go i spróbuj ponownie skorzystać z aplikacji EpsonNet Config.

### Czy limit czasu błędu komunikacji jest zbyt krótki?

Uruchom aplikację EpsonNet Config i wybierz kolejno opcje **Tools** > **Options** > **Timeout**. Następnie podaj dłuższy czas w polu **Communication Error**. Uwaga: może to również spowodować spowolnienie działania aplikacji EpsonNet Config.

### Powiązane informacje

➡ „Uruchamianie aplikacji EpsonNet Config — Windows” na stronie 56

➡ „Uruchamianie aplikacji EpsonNet Config — Mac OS” na stronie 56

# Dodatek

## Opis oprogramowania sieciowego

W tym rozdziale opisano oprogramowanie służące do konfigurowania i zarządzania urządzeniami.

### Epson Device Admin

Epson Device Admin to aplikacja pozwalająca na zainstalowanie urządzeń w sieci, konfigurowanie ich i zarządzanie nimi. Można uzyskać szczegółowe informacje o urządzeniach, takie jak stan i poziom materiałów eksploatacyjnych, wysyłać powiadomienia o alertach i tworzyć raporty o użyciu urządzenia. Można też utworzyć szablon z ustawionymi elementami i zastosować je do innych urządzeń w ramach udostępnianych ustawień. Możesz pobrać Epson Device Admin z serwisu WWW wsparcia firmy Epson. Więcej informacji na ten temat zawiera dokumentacja programu Epson Device Admin oraz jego system pomocy.

#### Uruchamianie programu Epson Device Admin (tylko system Windows)

Wybierz pozycje **Wszystkie programy** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

***Uwaga:***
*Jeżeli zostanie wyświetlone powiadomienie zapory, zezwól na dostęp programu Epson Device Admin do sieci.*

### Narzędzie EpsonNet Config

Aplikacja EpsonNet Config umożliwia administratorowi konfigurowanie ustawień sieciowych skanera, takich jak przydzielenie adresu IP czy zmiana trybu połączenia. Funkcja wsadowego zmieniania ustawień jest obsługiwana w systemie Windows. Więcej informacji na ten temat zawiera dokumentacja programu EpsonNet Config oraz jego system pomocy.

### Uruchamianie aplikacji EpsonNet Config — Windows

Wybierz pozycje **Wszystkie programy** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

***Uwaga:***
*Jeśli zostanie wyświetlone powiadomienie zapory, zezwól na dostęp programu EpsonNet Config do sieci.*

### Uruchamianie aplikacji EpsonNet Config — Mac OS

Wybierz opcję **Idź** > **Programy** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

## EpsonNet SetupManager

Aplikacja EpsonNet SetupManager służy do tworzenia pakietów upraszczających instalację skanera, np. przez zainstalowanie sterownika skanera i jego skonfigurowanie, a także zainstalowanie aplikacji Document Capture Pro. Ponadto aplikacja ta umożliwia administratorowi tworzenie unikalnych pakietów oprogramowania i późniejsze dystrybuowanie ich wśród grup użytkowników.

Więcej informacji można znaleźć w lokalnej wersji witryny firmy Epson.

# Przydzielanie adresu IP za pomocą programu EpsonNet Config

Adres IP można przydzielać do skanera za pomocą programu EpsonNet Config. Program EpsonNet Config umożliwia przydzielenie adresu IP do skanera, którego adres nie został przydzielony po podłączeniu kablem Ethernet.

## Przydzielanie adresu IP za pomocą ustawień wsadowych

### Tworzenie pliku do wsadowego konfigurowania ustawień

Używając adresu MAC i nazwy modelu jako kluczy, można utworzyć nowy plik SYLK do przydzielania adresów IP.

1. Otwórz aplikację arkusza kalkulacyjnego (np. Microsoft Excel) lub edytor tekstu.

2. W pierwszym wierszu wprowadź nazwy pozycji ustawień, takie jak: „Info_MACAddress”, „Info_ModelName” i „TCPIP_IPAddress”.

   Wprowadź następujące ciągi tekstowe na potrzeby pozycji ustawień. Rozróżniane są wielkie i małe litery, a także znaki dwubajtowe i jednobajtowe. Jeśli nazwy pozycji ustawień będą się różnić choć jednym znakiem, nie zostaną rozpoznane.

   Wprowadź nazwy pozycji ustawień zgodnie z poniższą tabelą; w przeciwnym razie program EpsonNet Config ich nie rozpozna.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| | | |
| | | |

3. Wprowadź adres MAC, nazwę modelu i adres IP każdego interfejsu sieciowego.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| 0000XXXX0001 | ALC-XXXXX | 192.168.100.102 |
| 0000XXXX0002 | ALC-XXXXX | 192.168.100.103 |
| 0000XXXX0003 | ALC-XXXXX | 192.168.100.104 |

4. Wprowadź nazwę pliku SYLK (*.slk) i zapisz go.

## Wsadowe konfigurowanie ustawień przy użyciu pliku konfiguracyjnego

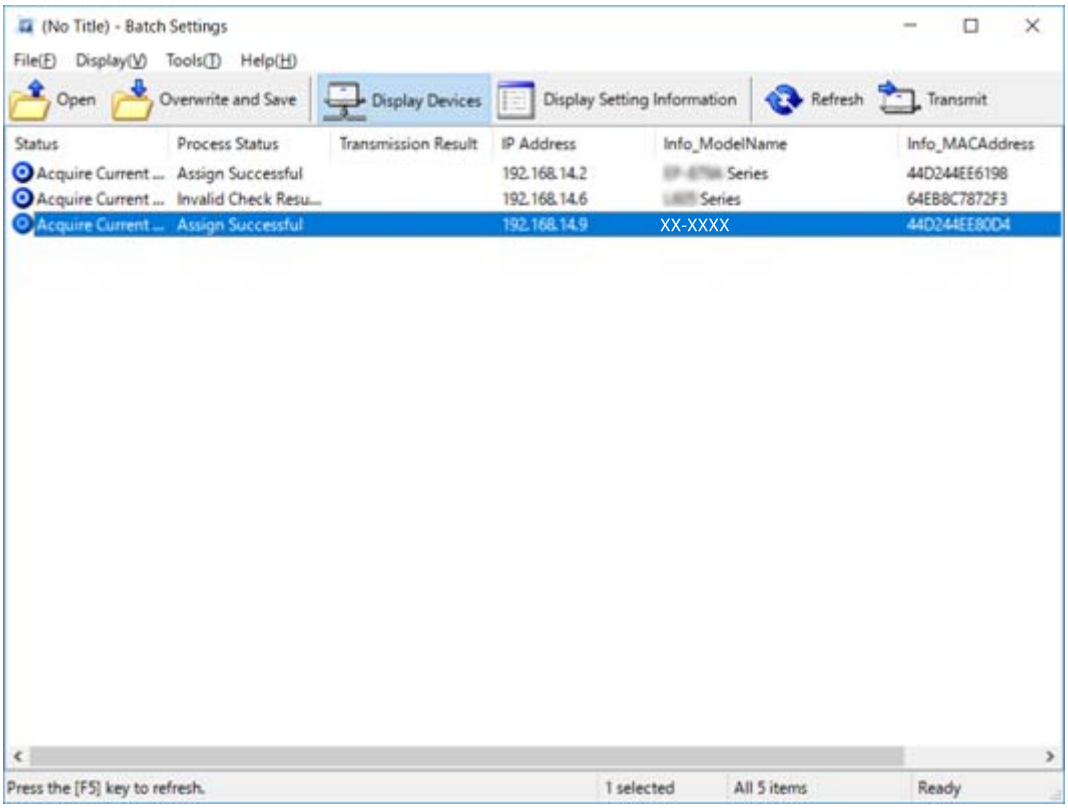
Można przydzielać wsadowo adresy IP, używając pliku konfiguracyjnego (plik SYLK). Aby można to było zrobić, należy najpierw utworzyć taki plik.

1. Podłącz wszystkie urządzenia do sieci za pomocą kabli Ethernet.
2. Włącz skaner.
3. Uruchom aplikację EpsonNet Config.

   Zostanie wyświetlona lista skanerów w sieci. Jej wyświetlenie może zająć trochę czasu.
4. Kliknij pozycje **Tools** > **Batch Settings**.
5. Kliknij przycisk **Open**.
6. Na ekranie wyboru pliku wybierz plik SYLK (*.slk) zawierający ustawienia, a następnie kliknij przycisk **Open**.

7. Wybierz urządzenia, dla których ma być wykonana wsadowa konfiguracja ustawień. Urządzenia powinny mieć w kolumnie **Status** wartość **Unassigned**, a w kolumnie **Process Status** — **Assign Successful**.

   Zaznaczając wiele urządzeń, naciśnij klawisz Ctrl lub Shift i kliknij lub przeciągnij wskaźnik myszy.




8. Kliknij przycisk **Transmit**.

9. Jeśli zostanie wyświetlony ekran wprowadzania hasła, wprowadź hasło, a następnie kliknij przycisk **OK**.

   Prześlij ustawienia.

   ***Uwaga:***
   *Informacje są przesyłane do interfejsu sieciowego, aż postęp procesu zostanie zakończony. Nie należy wyłączać urządzenia ani karty sieci bezprzewodowej, a także wysyłać żadnych danych do urządzenia.*

10. Na ekranie **Transmitting Settings** kliknij przycisk **OK**.

11. Sprawdź stan ustawionego urządzenia.

    W przypadku urządzeń ze stanem  lub  sprawdź zawartość pliku ustawień lub upewnij się, czy urządzenie zostało prawidłowo uruchomione ponownie.

| Ikona | Status | Process Status | Objaśnienie |
|---|---|---|---|
|  | Setup Complete | Setup Successful | Konfiguracja została zakończona normalnie. |
|  | Setup Complete | Rebooting | Po przesłaniu informacji każde urządzenie musi zostać uruchomione ponownie, aby ustawienia zostały zastosowane. Wykonywany jest test w celu określenia, czy urządzenie można połączyć po ponownym uruchomieniu. |
|  | Setup Complete | Reboot Failed | Nie można znaleźć urządzenia po przesłaniu ustawień. Sprawdź, czy urządzenie jest włączone i czy zostało prawidłowo uruchomione ponownie. |
|  | Setup Complete | Searching | Wyszukiwanie urządzenia wskazanego w pliku ustawień.* |
|  | Setup Complete | Search Failed | Nie można przetestować urządzeń, które zostały już skonfigurowane. Sprawdź, czy urządzenie jest włączone i czy zostało prawidłowo uruchomione ponownie.* |

    * Dotyczy tylko sytuacji, gdy wyświetlane są informacje o ustawieniach.

**Powiązane informacje**

➡ „Uruchamianie aplikacji EpsonNet Config — Windows” na stronie 56

➡ „Uruchamianie aplikacji EpsonNet Config — Mac OS” na stronie 56

# Przydzielanie adresu IP do każdego urządzenia

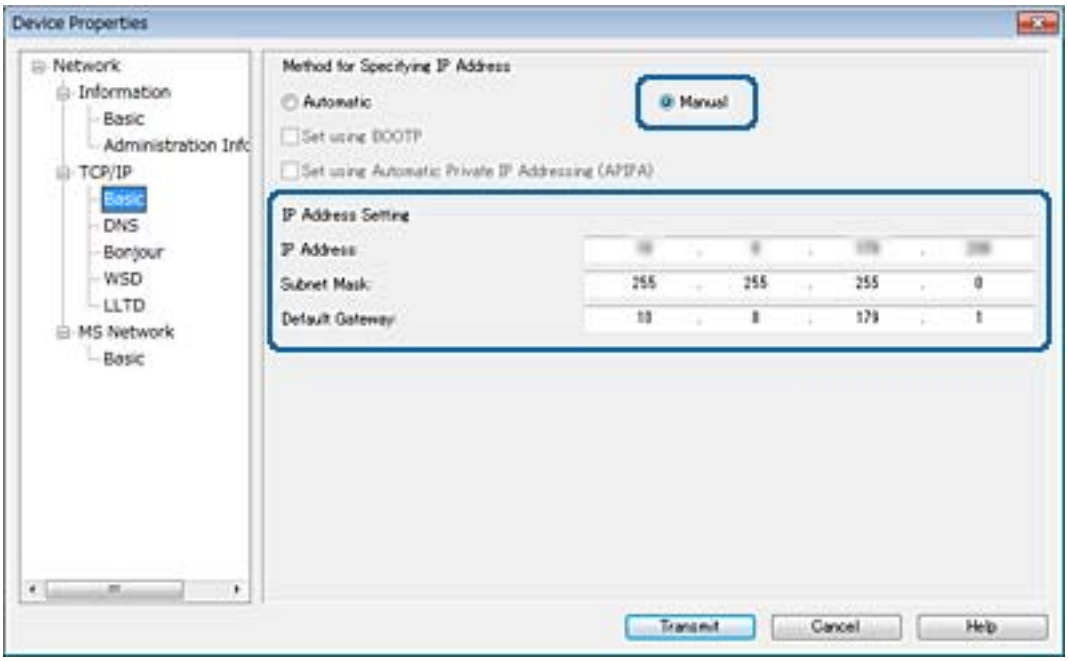
Adres IP można przydzielać do skanera za pomocą programu EpsonNet Config.

1. Włącz skaner.
2. Podłącz skaner do sieci za pomocą kabla Ethernet.
3. Uruchom aplikację EpsonNet Config.

   Zostanie wyświetlona lista skanerów w sieci. Jej wyświetlenie może zająć trochę czasu.
4. Kliknij dwukrotnie skaner, do którego adres ma być przydzielony.

   ***Uwaga:***
   *Jeśli podłączono wiele skanerów tego samego modelu, skaner można zidentyfikować po jego adresie MAC.*
5. Wybierz pozycje **Network** > **TCP/IP** > **Basic**.

6. Wprowadź adresy w polach **IP Address**, **Subnet Mask** i **Default Gateway**.




***Uwaga:***
*Wprowadź statyczny adres w przypadku podłączenia skanera do bezpiecznej sieci.*

7. Kliknij przycisk **Transmit**.

   Zostanie wyświetlony ekran z potwierdzeniem transmisji.

8. Kliknij przycisk **OK**.

   Zostanie wyświetlony ekran zakończenia transmisji.

   ***Uwaga:***
   *Informacje zostaną przesłane do urządzenia, a następnie zostanie wyświetlony komunikat „Konfiguracja zakończona pomyślnie". Nie należy wyłączać urządzenia, a także wysyłać żadnych danych do usługi.*

9. Kliknij przycisk **OK**.

### Powiązane informacje

➡ „Uruchamianie aplikacji EpsonNet Config — Windows" na stronie 56
➡ „Uruchamianie aplikacji EpsonNet Config — Mac OS" na stronie 56

# Używanie portów na skanerze

Skaner wykorzystuje następujące porty. Administrator sieci musi zezwolić na ruch przez te porty, aby można było korzystać z odpowiednich funkcji.

**Dodatek**

| Nadawca (klient) | Używaj | Miejsce docelowe (serwer) | Protokół | Numer portu |
|---|---|---|---|---|
| Skaner | Wysyłanie wiadomości e-mail (powiadomienia e-mail) | Serwer SMTP | SMTP (TCP) | 25 |
| | | | SMTP SSL/TLS (TCP) | 465 |
| | | | SMTP STARTTLS (TCP) | 587 |
| | Połączenie POP przed SMTP (powiadomienia e-mail) | Serwer POP | POP3 (TCP) | 110 |
| | Kontrola WSD | Komputer kliencki | WSD (TCP) | 5357 |
| | Wyszukiwanie komputera podczas skanowania inicjowanego w programie Document Capture Pro | Komputer kliencki | Wykrywanie skanowania sieciowego | 2968 |
| | Gromadzenie informacji o zadaniu podczas skanowania inicjowanego w programie Document Capture Pro | Komputer kliencki | Wypychanie skanowania sieciowego | 2968 |
| Komputer kliencki | 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 zeskanowanych danych z programu Document Capture Pro | Skaner | Skanowanie sieciowe (TCP) | 1865 |

# Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

W tym rozdziale omówiono zaawansowane funkcje zabezpieczeń.

## Ustawienia zabezpieczeń i zapobieganie niebezpieczeństwom

Jeśli urządzenie jest połączone z siecią, można uzyskać do niego dostęp z lokalizacji zdalnej. Ponadto wiele osób może współużytkować urządzenie, 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 urządzenia w środowisku, w którym jest zapewniony dostęp do Internetu, zagrożenia są jeszcze większe.

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

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

| Nazwa | Typ funkcji | Konfigurowane opcje | Działania zapobiegawcze |
|---|---|---|---|
| Komunikacja SSL/TLS | Komunikacja komputera i urządzenia jest szyfrowana za pośrednictwem protokołów SSL/TLS. Zawartość komunikacji przesyłana za pośrednictwem przeglądarki jest chroniona. | Konfigurowanie certyfikatu urzędu certyfikacji na serwerze, który jest certyfikatem podpisanym przez urząd certyfikacji na potrzeby urządzenia. | Zapobieganie ujawnianiu informacji o ustawieniach i zawartości danych przesyłanych do skanera z komputera. Dostęp do serwera Epson przez Internet można też chronić przez aktualizację oprogramowania układowego itd. |
| 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 skanowania. | Utwórz podstawowe zasady i indywidualne zasady, aby ustawić klienty lub typy danych, które są dozwolone na urządzeniu. | Ochrona przed nieupoważnionym dostępem, a także manipulacją i przechwyceniem danych przesyłanych do urządzenia. |
| SNMPv3 | Dodano funkcje, takie jak monitorowanie urządzeń połączonych z siecią, integralność danych protokołu SNMP używanych do kontroli, szyfrowania i uwierzytelniania użytkowników itd. | Włącz protokół SNMPv3, a następnie skonfiguruj uwierzytelnianie i metodę szyfrowania. | Umożliwienie zmiany ustawień przez sieć, poufność monitorowania stanu. |

**Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach**

| Nazwa | Typ funkcji | Konfigurowane opcje | Działania zapobiegawcze |
|---|---|---|---|
| IEEE802.1X | Umożliwia połączenie tylko użytkownikom uwierzytelnionym w sieci Ethernet. Urządzenia mogą używać tylko użytkownicy z uprawnieniami. | Konfigurowanie uwierzytelniania na serwerze RADIUS (serwer uwierzytelniający). | Ochrona przed nieupoważnionym dostępem i użytkowaniem urządzenia. |
| Odczyt karty ID | Można używać urządzenia, przytrzymując kartę ID nad podłączonym urządzeniem uwierzytelniającym. Możliwe jest ograniczanie uzyskiwania dzienników każdego użytkownika i urządzenia, a także ograniczyć użycie urządzeń i dostępne funkcje na poziomie użytkownika i grupy. | Podłącz urządzenie uwierzytelniające do urządzenia, a następnie skonfiguruj informacje o użytkowniku w systemie uwierzytelniania. | Zapobieganie nieupoważnionemu użytkowaniu urządzenia. |

**Powiązane informacje**


➡ „Komunikacja SSL/TLS ze skanerem” na stronie 63

➡ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 71

➡ „Korzystanie z protokołu SNMPv3” na stronie 83

➡ „Podłączanie skanera do sieci IEEE802.1X” na stronie 85


## Ustawienia funkcji zabezpieczeń

Podczas konfiguracji funkcji IPsec/Filtrowanie IP lub IEEE802.1X zaleca się uzyskanie dostępu do narzędzia Web Config za pośrednictwem protokołu SSL/TLS, aby ograniczyć ryzyko modyfikacji lub przechwycenia informacji.

# 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.

## Informacje o certyfikatach cyfrowych

❏ Certyfikat podpisany przez urząd certyfikacji

Certyfikat podpisany przez urząd certyfikacji (CA) należy najpierw uzyskać z takiego urzędu. Użycie takiego certyfikatu pozwala zapewnić bezpieczeństwo przesyłanych danych. Można użyć oddzielnego certyfikatu do każdej funkcji zabezpieczeń.

❏ Certyfikat urzędu certyfikacji

Certyfikat urzędu certyfikacji wskazuje, że podmiot zewnętrzny zweryfikował tożsamość serwera. Jest to najważniejszy element zabezpieczeń typu „sieć zaufania”. W celu przeprowadzania uwierzytelniania serwera należy uzyskać certyfikat urzędu certyfikacji od odpowiedniego urzędu wydającego takie certyfikaty.

❏ Certyfikat z podpisem własnym

Certyfikat z podpisem własnym to rodzaj certyfikatu wydawanego i podpisywanego przez sam skaner. Taki certyfikat nie jest godny zaufania i nie gwarantuje uniknięcia fałszowania ruchu sieciowego. W przypadku wykorzystywania certyfikatu tego rodzaju na potrzeby komunikacji SSL/TLS w przeglądarce internetowej może zostać wyświetlony komunikat ostrzegawczy. Certyfikatów z podpisem własnym nie można używać na potrzeby komunikacji innej niż SSL/TLS.

**Powiązane informacje**

➡ „Uzyskiwanie i importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 64

➡ „Usuwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 68

➡ „Aktualizowanie certyfikatu z podpisem własnym” na stronie 68

# Uzyskiwanie i importowanie certyfikatu podpisanego przez urząd certyfikacji

## 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 pozycję **Network Security Settings**. Następnie wybierz pozycje **SSL/TLS** > **Certificate** lub **IPsec/IP Filtering** > **Client Certificate** lub **IEEE802.1X** > **Client Certificate**.

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

   Zostanie wyświetlona strona tworzenia żądania CSR.

3. Wprowadź wartość dla każdej 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. Kliknij przycisk **Network Security Settings**. Następnie wybierz pozycje **SSL/TLS** > **Certificate** lub **IPsec/IP Filtering** > **Client Certificate** lub **IEEE802.1X** > **Client Certificate**.

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 CA-signed Certificate może nie być możliwe.*

7. Pobrane żądanie CSR wyślij do urzędu certyfikacji, aby uzyskać CA-signed Certificate.

   Należy przestrzegać reguł dotyczących metody i formy przesyłania żądań CSR obowiązujących w danym urzędzie certyfikacji.

8. Otrzymany CA-signed Certificate zapisz na komputerze podłączonym do skanera.

   Proces uzyskiwania CA-signed Certificate zostanie zakończony w chwili zapisania certyfikatu w miejscu docelowym.

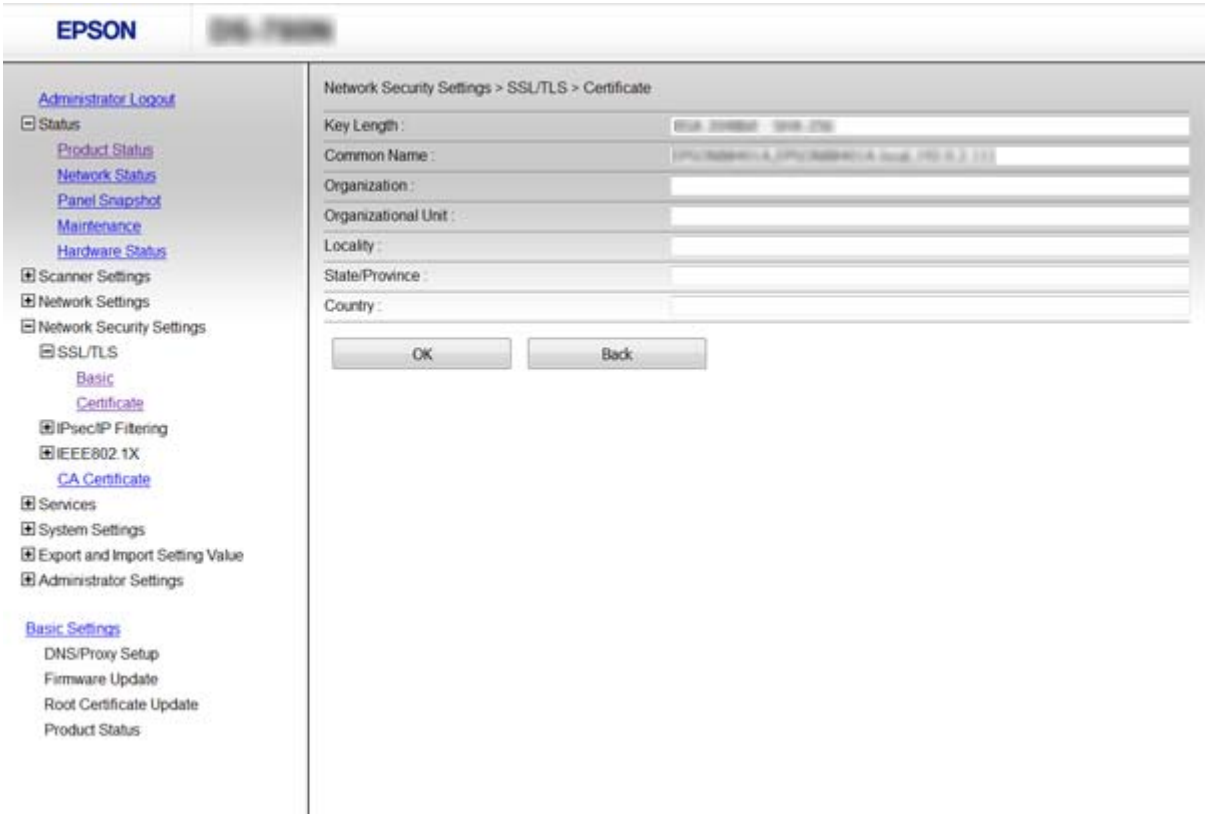
### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Opcje ustawień żądania CSR” na stronie 65

➡ „Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 66

## *Opcje ustawień żądania CSR*



| Elementy | Ustawienia i objaśnienie |
|---|---|
| Key Length | Wybierz długość klucza. |
| Common Name | Można wprowadzić od 1 do 128 znaków. Jeśli jest to adres IP, powinien to być adres statyczny.<br>Przykład:<br>Adres URL do uzyskiwania dostępu do narzędzia Web Config: https://10.152.12.225<br>Nazwa publiczna: 10.152.12.225 |
| Organization/ Organizational Unit/ Locality/ State/Province | Można wprowadzić od 0 do 64 znaków ASCII (0x20–0x7E). Nazwy wyróżniające można rozdzielić przecinkami. |
| Country | Podaj dwucyfrowy kod kraju zgodnie z normą ISO-3166. |

### Powiązane informacje

➡ „Uzyskiwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 64

## Importowanie certyfikatu podpisanego przez urząd certyfikacji

***Ważne:***

❏ *Upewnij się, że ustawienia daty i godziny na skanerze są prawidłowe.*

❏ *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 pozycję **Network Security Settings**. Następnie wybierz pozycje **SSL/TLS** > **Certificate** lub **IPsec/IP Filtering** > **Client Certificate** lub **IEEE802.1X** > **Client Certificate**.

2. Kliknij przycisk **Import**.

   Zostanie wyświetlona strona importowania certyfikatu.

3. Wprowadź wartość dla każdej pozycji.

   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

   ❏ **Private Key**: nie konfiguruj, ponieważ skaner ma już klucz prywatny.

   ❏ **Password**: nie konfiguruj.

   ❏ **CA Certificate 1**/**CA Certificate 2**: pole opcjonalne

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

   ❏ **Private Key**: wprowadź wartość.

   ❏ **Password**: nie konfiguruj.

   ❏ **CA Certificate 1**/**CA Certificate 2**: pole opcjonalne

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

❏ **Private Key**: nie konfiguruj.

❏ **Password**: pole opcjonalne

❏ **CA Certificate 1/CA Certificate 2**: nie konfiguruj.

4. Kliknij przycisk **OK**.

Wyświetlony zostanie komunikat z potwierdzeniem zakończenia operacji.

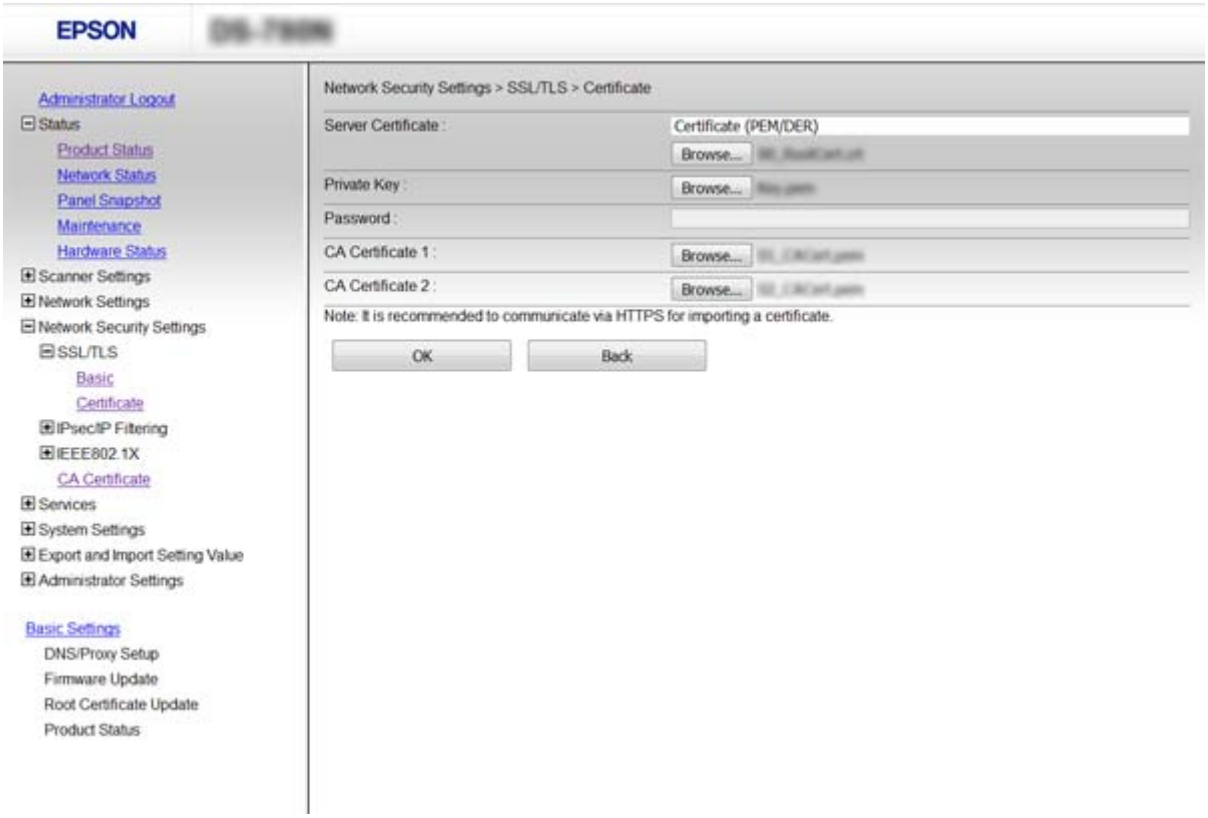
***Uwaga:***
*Kliknij przycisk **Confirm**, aby zweryfikować dane certyfikatu.*

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Opcje ustawień importowania certyfikatu podpisanego przez urząd certyfikacji” na stronie 67

## *Opcje ustawień importowania certyfikatu podpisanego przez urząd certyfikacji*




| Obsługiwane algorytmy | Ustawienia i wyjaśnienie |
|---|---|
| Server Certificate lub Client Certificate | Wybierz format certyfikatu. |
| Private Key | W przypadku uzyskania certyfikatu w formacie PEM/DER przy użyciu żądania CSR utworzonego na komputerze wskaż plik z kluczem prywatnym właściwym dla uzyskanego certyfikatu. |
| Password | Podaj hasło do zaszyfrowania klucza prywatnego. |

| Obsługiwane algorytmy | Ustawienia i wyjaśnienie |
|---|---|
| CA Certificate 1 | Jeśli format certyfikatu to **Certificate (PEM/DER)**, zaimportuj certyfikat urzędu certyfikacji, który wydał certyfikat serwera. W razie potrzeby można wskazać plik. |
| CA Certificate 2 | Jeśli format certyfikatu to **Certificate (PEM/DER)**, zaimportuj certyfikat urzędu certyfikacji, który wydał certyfikat **CA Certificate 1**. W razie potrzeby można wskazać plik. |

### Powiązane informacje

➡ „Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 66

## 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 pozycje **Network Security Settings**. Następnie wybierz pozycje **SSL/TLS** > **Certificate** lub **IPsec/IP Filtering** > **Client Certificate** lub **IEEE802.1X** > **Client Certificate**.
2. Kliknij przycisk **Delete**.
3. W oknie komunikatu potwierdź, że certyfikat ma zostać usunięty.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Aktualizowanie certyfikatu z podpisem własnym

Jeśli skaner obsługuje funkcję serwera HTTPS, można zaktualizować certyfikat z podpisem własnym. W przypadku uzyskiwania dostępu do aplikacji Web Config z wykorzystaniem certyfikatu z podpisem własnym wyświetlony zostanie komunikat ostrzegawczy.

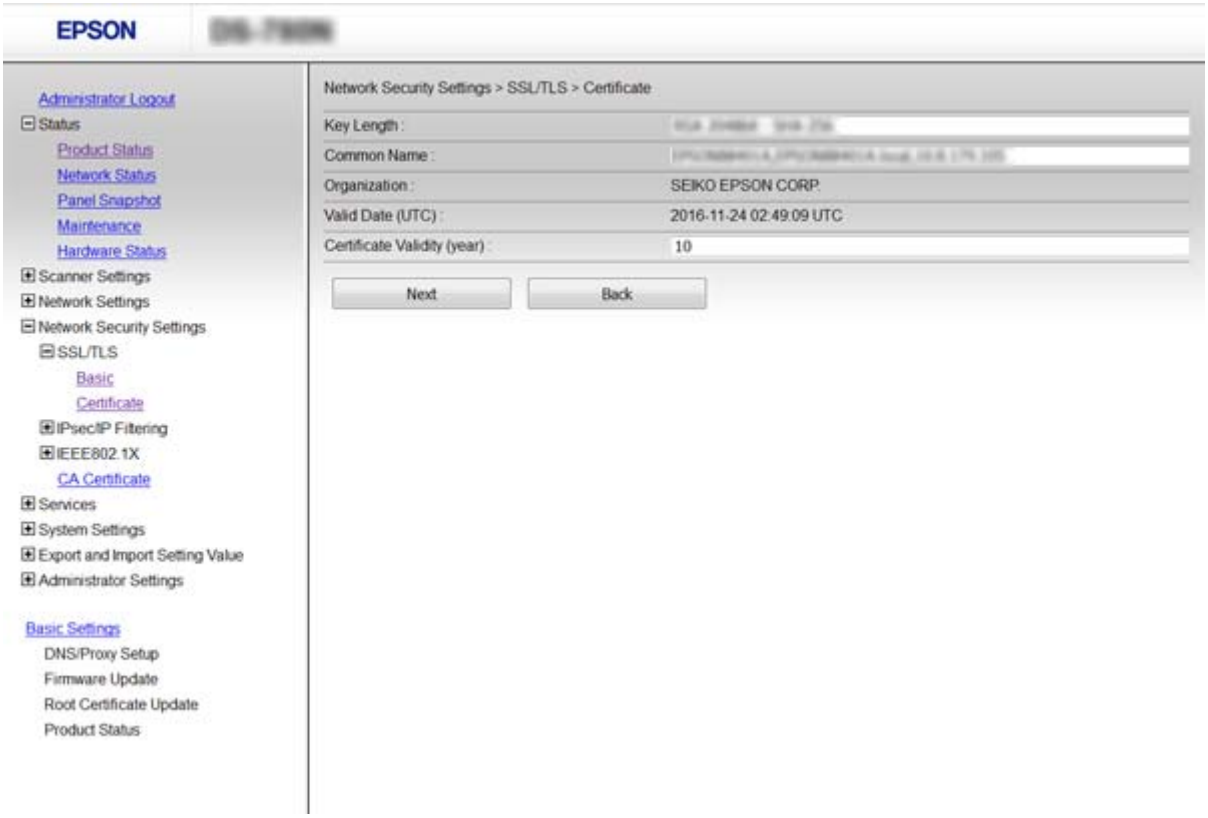
Certyfikatu z podpisem własnym należy używać wyłącznie tymczasowo (do czasu uzyskania i zaimportowania certyfikatu podpisanego przez urząd certyfikacji).

1. Otwórz narzędzie Web Config i wybierz pozycje **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Kliknij przycisk **Update**.
3. Wprowadź nazwę **Common Name**.

   Podaj adres IP lub inny identyfikator skanera (np. nazwę FQDN). Można wprowadzić od 1 do 128 znaków.

***Uwaga:***
*Można podać wiele nazw wyróżniających (CN) rozdzielonych przecinkami.*

4. Podaj okres ważności certyfikatu.




5. Kliknij przycisk **Next**.

   Wyświetlony zostanie komunikat z potwierdzeniem.

6. Kliknij przycisk **OK**.

   Ustawienia skanera zostały zaktualizowane.

***Uwaga:***
*Kliknij przycisk **Confirm**, aby zweryfikować dane certyfikatu.*

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Konfigurowanie CA Certificate

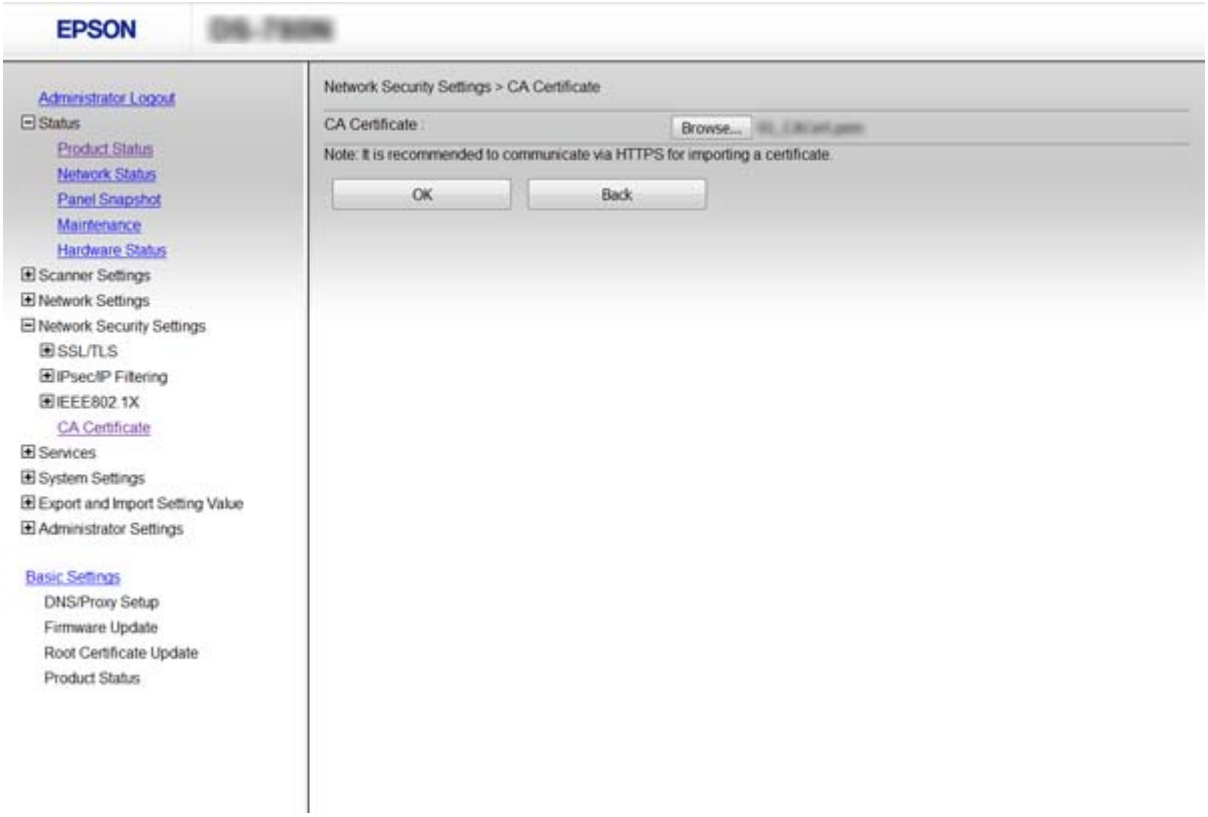
CA Certificate można zaimportować, wyświetlić lub usunąć.

### Importowanie CA Certificate

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Network Security Settings** > **CA Certificate**.

2. Kliknij przycisk **Import**.

3. Wskaż CA Certificate, który chcesz zaimportować.




4. Kliknij przycisk **OK**.

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

### Powiązane informacje

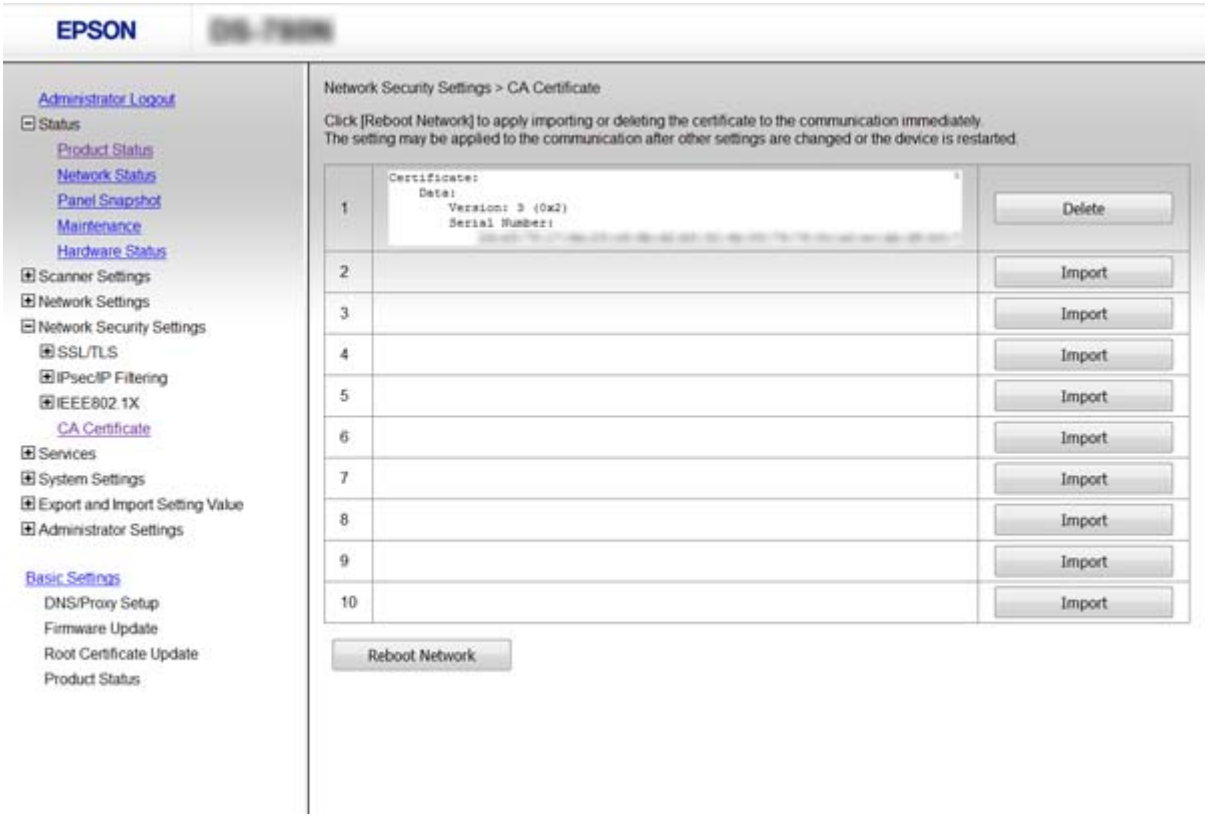
➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Usuwanie CA Certificate

Zaimportowany CA Certificate można usunąć.

1. Otwórz aplikację Web Config, a następnie wybierz pozycje **Network Security Settings** > **CA Certificate**.

2. Kliknij przycisk **Delete** obok CA Certificate, który chcesz usunąć.




3. W oknie komunikatu potwierdź, że certyfikat ma zostać usunięty.

**Powiązane informacje**

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

# Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP

## Informacje o IPsec/IP Filtering

Jeśli skaner obsługuje filtrowanie IPsec/IP, można filtrować ruch w zależności od adresu IP, usługi lub portu. 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.

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. 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.

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

# Konfigurowanie opcji Default Policy

1. Otwórz aplikację Web Config i wybierz pozycje **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Wprowadź wartość dla każdej pozycji.
3. Kliknij przycisk **Next**.

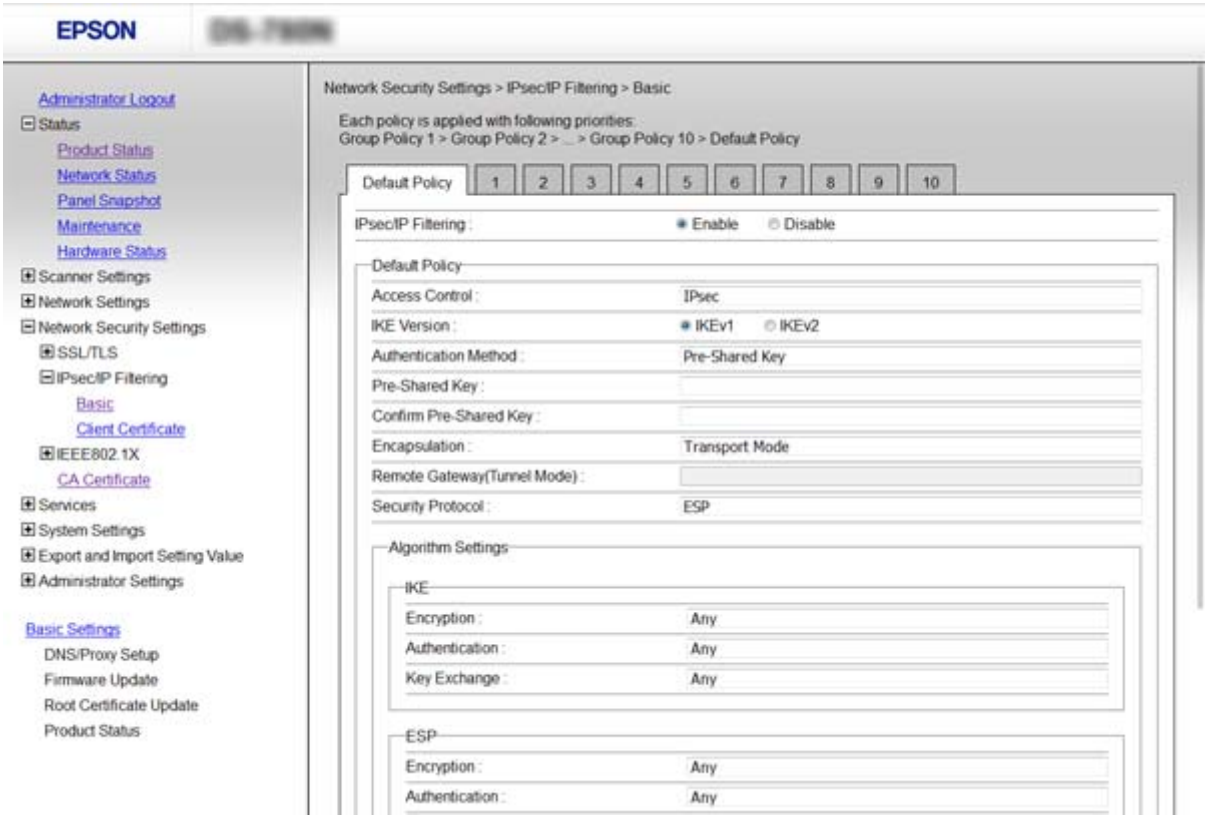
   Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.

   Ustawienia skanera zostały zaktualizowane.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Elementy ustawień opcji Default Policy” na stronie 72

# Elementy ustawień opcji Default Policy



## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| IPsec/IP Filtering | Umożliwia włączenie lub wyłączenie funkcji filtrowania IPsec/IP. | |
| Access Control | Umożliwia skonfigurowanie metody weryfikowania pakietów protokołu IP. | |
| | Permit Access | Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IP. |
| | Refuse Access | Wybierz tę opcję, aby zablokować przekazywanie skonfigurowanych pakietów protokołu IP. |
| | IPsec | Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IPsec. |
| IKE Version | Umożliwia wybór wersji protokołu IKE: IKEv1 lub IKEv2.<br>Wybierz jedną z nich odpowiednio do urządzenia, z którym skaner jest połączony. | |
| IKEv1 | Po wybraniu ustawienia **IKEv1** dla opcji **IKE Version** wyświetlane są następujące pozycje. | |
| | Authentication Method | Aby wybrać opcję **Certificate**, należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji. |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |
| IKEv2 | Po wybraniu ustawienia **IKEv2** dla opcji **IKE Version** wyświetlane są następujące pozycje. | |
| Local | Authentication Method | Aby wybrać opcję **Certificate**, należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji. |
| | ID Type | Umożliwia wybór typu identyfikatora skanera. |
| | ID | Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora.<br>Na początku identyfikatora nie można używać znaków: @, # i =.<br>**Distinguished Name**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=”.<br>**IP Address**: wprowadź adres w formacie IPv4 lub IPv6.<br>**FQDN**: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.).<br>**Email Address**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@”.<br>**Key ID**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |

## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Remote | Authentication Method | Aby wybrać opcję **Certificate**, należy najpierw uzyskać i zaimportować certyfikat podpisany przez urząd certyfikacji. |
| | ID Type | Umożliwia wybór typu identyfikatora urządzenia, które ma być uwierzytelnione. |
| | ID | Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora.<br>Na początku identyfikatora nie można używać znaków: @, # i =.<br>**Distinguished Name**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=".<br>**IP Address**: wprowadź adres w formacie IPv4 lub IPv6.<br>**FQDN**: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.).<br>**Email Address**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@".<br>**Key ID**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |
| Encapsulation | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, skonfiguruj tryb hermetyzacji. | |
| | Transport Mode | Wybierz tę opcję, jeśli skaner jest używany tylko w jednej sieci LAN. Pakiety protokołu IP w warstwie 4. lub wyższej będą szyfrowane. |
| | Tunnel Mode | Wybierz tę opcję, jeśli skaner jest używany w sieci obsługującej Internet, np. IPsec-VPN. Szyfrowane będą nagłówki i zawartość pakietów IP. |
| Remote Gateway(Tunnel Mode) | Jeśli dla opcji **Tunnel Mode** zostanie wybrane ustawienie **Encapsulation**, w tym polu wprowadź adres bramy o długości od 1 do 39 znaków. | |
| Security Protocol | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, wybierz jedno z poniższych ustawień. | |
| | 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. |
| Algorithm Settings | | |

**Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach**

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| IKE | Encryption | Umożliwia wybór algorytmu szyfrowania protokołu IKE.<br>Dostępne pozycje różnią się w zależności od wersji protokołu IKE. |
| | Authentication | Umożliwia wybór algorytmu uwierzytelniania protokołu IKE. |
| | Key Exchange | Umożliwia wybór algorytmu wymiany kluczy protokołu IKE.<br>Dostępne pozycje różnią się w zależności od wersji protokołu IKE. |
| ESP | Encryption | Umożliwia wybór algorytmu szyfrowania protokołu ESP.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **ESP** dla opcji **Security Protocol**. |
| | Authentication | Umożliwia wybór algorytmu uwierzytelniania protokołu ESP.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **ESP** dla opcji **Security Protocol**. |
| AH | Authentication | Umożliwia wybór algorytmu szyfrowania protokołu AH.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **AH** dla opcji **Security Protocol**. |

### Powiązane informacje

➡ „Konfigurowanie opcji Default Policy” na stronie 72

## Konfigurowanie opcji Group Policy

1. Otwórz aplikację Web Config i wybierz pozycje **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Kliknij numerowaną kartę, którą chcesz skonfigurować.
3. Wprowadź wartość dla każdej pozycji.
4. Kliknij przycisk **Next**.

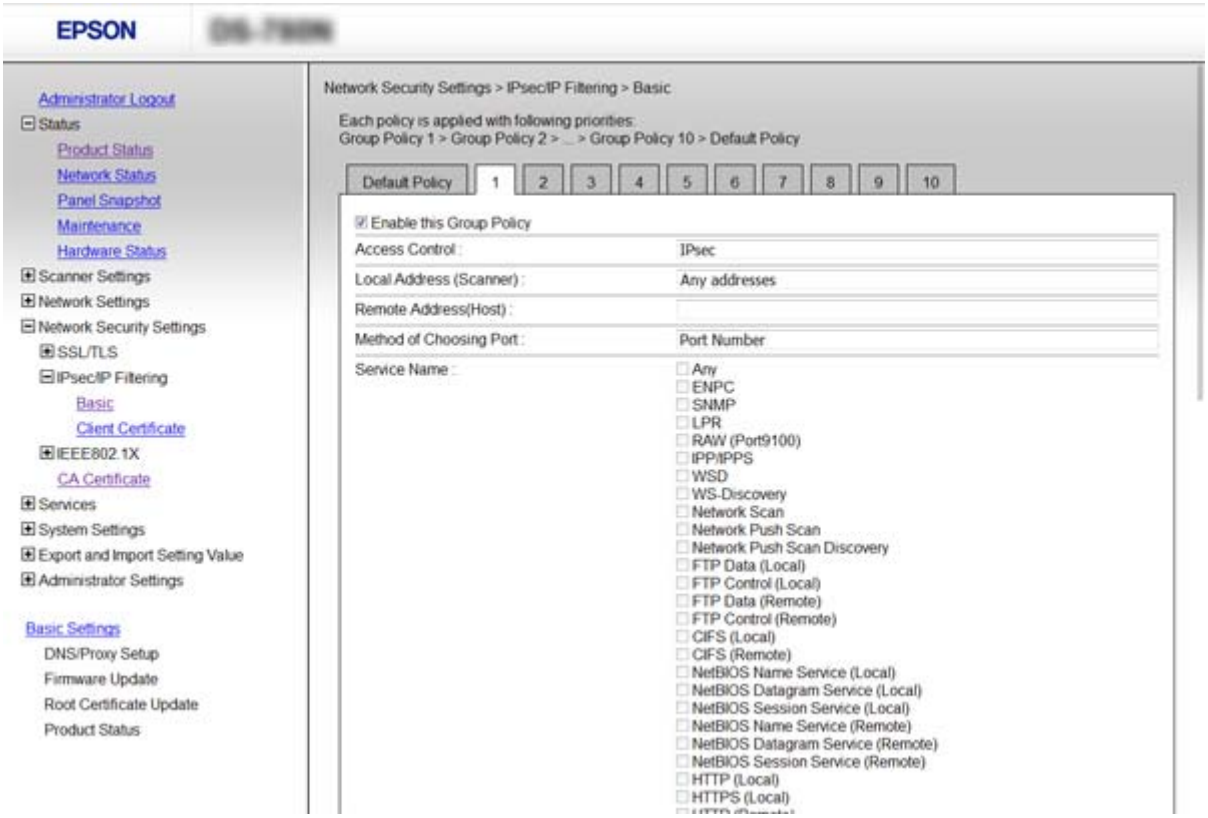
   Wyświetlony zostanie komunikat z potwierdzeniem.
5. Kliknij przycisk **OK**.

   Ustawienia skanera zostały zaktualizowane.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Elementy ustawień opcji Group Policy” na stronie 76

# Elementy ustawień opcji Group Policy




| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Enable this Group Policy | Umożliwia włączenie lub wyłączenie zasad grupowych. | |
| Access Control | Umożliwia skonfigurowanie metody weryfikowania pakietów protokołu IP. | |
| | Permit Access | Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IP. |
| | Refuse Access | Wybierz tę opcję, aby zablokować przekazywanie skonfigurowanych pakietów protokołu IP. |
| | IPsec | Wybierz tę opcję, aby umożliwić przekazywanie skonfigurowanych pakietów protokołu IPsec. |
| Local Address (Scanner) | Wybierz adres IPv4 lub adres IPv6 dopasowany do otoczenia sieciowego. Jeśli adres IP jest przydzielany automatycznie, można wybrać opcję **Use auto-obtained IPv4 address**. | |
| Remote Address(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.<br>***Uwaga:***<br>*Jeśli adres IP jest przydzielany automatycznie (np. przez serwer DHCP), połączenie może być niedostępne. Należy skonfigurować statyczny adres IP.* | |
| Method of Choosing Port | Umożliwia wybranie metody określania portów. | |
| Service Name | Jeśli dla opcji **Service Name** zostanie wybrane ustawienie **Method of Choosing Port**, wybierz jedno z poniższych ustawień. | |

## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Transport Protocol | Jeśli dla opcji **Port Number** zostanie wybrane ustawienie **Method of Choosing Port**, skonfiguruj tryb hermetyzacji. | |
| | Any Protocol | 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. |
| Local Port | Jeśli dla opcji **Method of Choosing Port** zostanie wybrane ustawienie **Port Number**, a dla opcji **Transport Protocol** — ustawienie **TCP** lub **UDP**, wprowadź numery portów, na których odbierane pakiety mają być kontrolowane. Rozdziel numery portów przecinkami. Można podać maksymalnie 10 numerów portów.<br>Przykład: 20,80,119,5220<br>Jeśli nie zostanie podany żaden numer portu, kontrolowane będą wszystkie porty. | |
| Remote Port | Jeśli dla opcji **Method of Choosing Port** zostanie wybrane ustawienie **Port Number**, a dla opcji **Transport Protocol** — ustawienie **TCP** lub **UDP**, wprowadź numery portów, na których wysyłane pakiety mają być kontrolowane. Rozdziel numery portów przecinkami. Można podać maksymalnie 10 numerów portów.<br>Przykład: 25,80,143,5220<br>Jeśli nie zostanie podany żaden numer portu, kontrolowane będą wszystkie porty. | |
| IKE Version | Umożliwia wybór wersji protokołu IKE: IKEv1 lub IKEv2.<br>Wybierz jedną z nich odpowiednio do urządzenia, z którym skaner jest połączony. | |
| IKEv1 | Po wybraniu ustawienia **IKEv1** dla opcji **IKE Version** wyświetlane są następujące pozycje. | |
| | Authentication Method | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych. |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |
| IKEv2 | Po wybraniu ustawienia **IKEv2** dla opcji **IKE Version** wyświetlane są następujące pozycje. | |

## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Local | Authentication Method | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych. |
| | ID Type | Umożliwia wybór typu identyfikatora skanera. |
| | ID | Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora.<br>Na początku identyfikatora nie można używać znaków: @, # i =.<br>**Distinguished Name**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=".<br>**IP Address**: wprowadź adres w formacie IPv4 lub IPv6.<br>**FQDN**: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.).<br>**Email Address**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@".<br>**Key ID**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |

## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Remote | Authentication Method | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, wybierz jedno z poniższych ustawień. Wykorzystywany certyfikat jest taki sam, jak w zasadach domyślnych. |
| | ID Type | Umożliwia wybór typu identyfikatora urządzenia, które ma być uwierzytelnione. |
| | ID | Umożliwia wprowadzenie identyfikatora skanera pasującego do typu identyfikatora.<br>Na początku identyfikatora nie można używać znaków: @, # i =.<br>**Distinguished Name**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „=".<br>**IP Address**: wprowadź adres w formacie IPv4 lub IPv6.<br>**FQDN**: wprowadź od 1 do 255 znaków: A–Z a–z 0–9, - i kropkę (.).<br>**Email Address**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Trzeba użyć znaku „@".<br>**Key ID**: wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). |
| | Pre-Shared Key | Jeśli dla opcji **Pre-Shared Key** zostanie wybrane ustawienie **Authentication Method**, w tym polu wprowadź wartość klucza wstępnego o długości od 1 do 127 znaków. |
| | Confirm Pre-Shared Key | Wprowadź skonfigurowany klucz w celu potwierdzenia. |
| Encapsulation | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, skonfiguruj tryb hermetyzacji. | |
| | Transport Mode | Wybierz tę opcję, jeśli skaner jest używany tylko w jednej sieci LAN. Pakiety protokołu IP w warstwie 4. lub wyższej będą szyfrowane. |
| | Tunnel Mode | Wybierz tę opcję, jeśli skaner jest używany w sieci obsługującej Internet, np. IPsec-VPN. Szyfrowane będą nagłówki i zawartość pakietów IP. |
| Remote Gateway(Tunnel Mode) | Jeśli dla opcji **Tunnel Mode** zostanie wybrane ustawienie **Encapsulation**, w tym polu wprowadź adres bramy o długości od 1 do 39 znaków. | |
| Security Protocol | Jeśli dla opcji **IPsec** zostanie wybrane ustawienie **Access Control**, wybierz jedno z poniższych ustawień. | |
| | 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. |
| Algorithm Settings | | |

**Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach**

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| IKE | Encryption | Umożliwia wybór algorytmu szyfrowania protokołu IKE.<br>Dostępne pozycje różnią się w zależności od wersji protokołu IKE. |
| | Authentication | Umożliwia wybór algorytmu uwierzytelniania protokołu IKE. |
| | Key Exchange | Umożliwia wybór algorytmu wymiany kluczy protokołu IKE.<br>Dostępne pozycje różnią się w zależności od wersji protokołu IKE. |
| ESP | Encryption | Umożliwia wybór algorytmu szyfrowania protokołu ESP.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **ESP** dla opcji **Security Protocol**. |
| | Authentication | Umożliwia wybór algorytmu uwierzytelniania protokołu ESP.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **ESP** dla opcji **Security Protocol**. |
| AH | Authentication | Umożliwia wybór algorytmu uwierzytelniania protokołu AH.<br>Opcja jest dostępna, tylko jeśli wybrano ustawienie **AH** dla opcji **Security Protocol**. |

### Powiązane informacje


- „Konfigurowanie opcji Group Policy” na stronie 75
- „Kombinacja ustawienia Local Address (Scanner) i Remote Address(Host) w Group Policy” na stronie 80
- „Odwołania nazw usług w zasadach grupowych” na stronie 81


## Kombinacja ustawienia Local Address (Scanner) i Remote Address(Host) w Group Policy

| | | Ustawianie Local Address (Scanner) | | |
|---|---|---|---|---|
| | | IPv4 | IPv6*2 | Any addresses*3 |
| **Ustawianie Remote Address(Host)** | IPv4*1 | ✓ | – | ✓ |
| | IPv6*1, *2 | – | ✓ | ✓ |
| | Puste | ✓ | ✓ | ✓ |

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

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

*3 Poza adresami połączeń lokalnych IPv6.

## 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 |
|---|---|---|---|---|
| Any | – | – | – | Wszystkie usługi |
| ENPC | UDP | 3289 | Dowolny port | Wyszukiwanie skanera w aplikacjach, takich jak EpsonNet Config i sterownik skanera |
| SNMP | UDP | 161 | Dowolny port | Uzyskiwanie i konfiguracja MIB w aplikacjach, takich jak EpsonNet Config i sterownik skanera Epson |
| WSD | TCP | Dowolny port | 5357 | Kontrolowanie WSD |
| WS-Discovery | UDP | 3702 | Dowolny port | Wyszukiwanie skanera z WSD |
| Network Scan | TCP | 1865 | Dowolny port | Przesyłanie zeskanowanych danych z Document Capture Pro |
| Network Push Scan Discovery | UDP | 2968 | Dowolny port | Wyszukiwanie komputera ze skanera |
| Network Push Scan | TCP | Dowolny port | 2968 | Pozyskiwanie informacji o zadaniach skanowania inicjowanego z oprogramowania Document Capture Pro lub Document Capture |
| HTTP (Local) | TCP | 80 | Dowolny port | Serwer HTTP(S) (przesyłanie danych Web Config i WSD) |
| HTTPS (Local) | TCP | 443 | Dowolny port | |
| HTTP (Remote) | TCP | Dowolny port | 80 | Klient HTTP(S) (komunikacja między aktualizacją oprogramowania układowego i certyfikatu głównego) |
| HTTPS (Remote) | TCP | Dowolny port | 443 | |

# Przykłady konfiguracji opcji IPsec/IP Filtering

### Wyłącznie odbieranie pakietów protokołu IPsec

Poniższy przykład przedstawia konfigurowanie wyłącznie zasad domyślnych.

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: wprowadź maksymalnie 127 znaków.

**Group Policy**:

nie konfiguruj.

### Akceptowanie skanowania za pomocą narzędzia Epson Scan 2 i ustawień skanera

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

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

**Group Policy**:

❏ **Enable this Group Policy**: zaznacz to pole wyboru.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: adres IP klienta

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: zaznacz pole wyboru **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** i **HTTPS (Local)**.

### Uzyskiwanie dostępu wyłącznie z określonego adresu IP

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

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

**Group Policy**:

❏ **Enable this Group Policy**: zaznacz to pole wyboru.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: adres IP klienta administratora

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

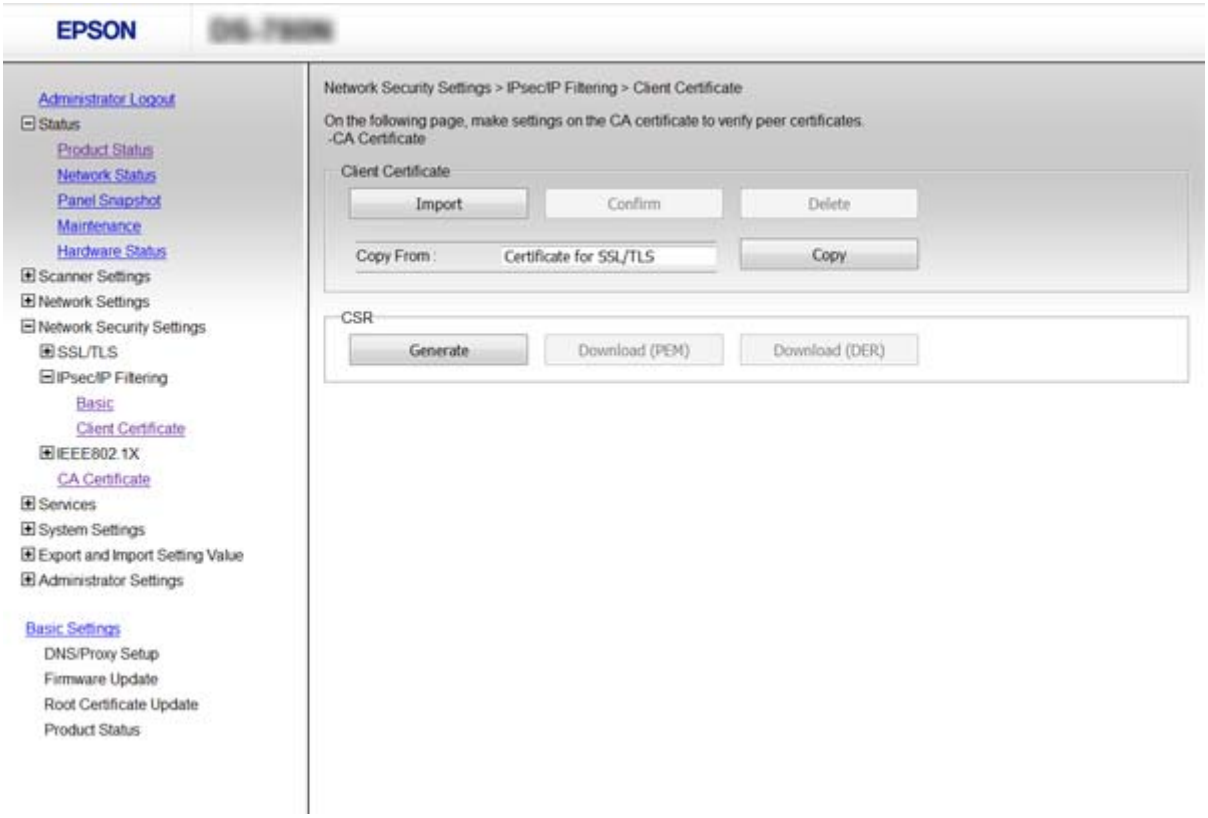
## Konfigurowanie certyfikatu na potrzeby protokołu IPsec/IP Filtering

Skonfiguruj certyfikat klienta na potrzeby filtrowania IPsec/IP. Jeśli chcesz skonfigurować centrum certyfikacji, przejdź do ustawienia **CA Certificate**.

1. Otwórz aplikację Web Config i wybierz pozycje **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Zaimportuj certyfikat w oknie **Client Certificate**.

   Jeśli certyfikat opublikowany przez centrum certyfikacji zaimportowano już wcześniej w ustawieniach IEEE802.1X lub SSL/TLS, można skopiować ten sam certyfikat na użytek filtrowania IPsec/IP. W celu skopiowania wybierz certyfikat w polu **Copy From** i kliknij przycisk **Copy**.




**Powiązane informacje**

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Uzyskiwanie i importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 64

# Korzystanie z protokołu SNMPv3

## Informacje o protokole SNMPv3

SNMP jest protokołem umożliwiającym monitorowanie i kontrolowanie gromadzenia informacji o urządzeniach połączonych z siecią. SNMPv3 ma ulepszone wersje funkcje zabezpieczeń zarządzania.

W przypadku korzystania z wersji SNMPv3 można uwierzytelniać i szyfrować pakiety SNMP dotyczące monitorowania stanu i zmian ustawień w celu ochrony komunikacji SNMP (pakietów) przed zagrożeniami sieciowymi, takimi jak podsłuchiwanie, podszywanie się i modyfikowanie.

## Konfigurowanie protokołu SNMPv3

Jeśli skaner obsługuje protokół SNMPv3, można monitorować i kontrolować dostęp do skanera.

1. Otwórz aplikację Web Config i wybierz pozycje **Services** > **Protocol**.
2. Wprowadź wartość dla każdej pozycji w obszarze **SNMPv3 Settings**.
3. Kliknij przycisk **Next**.

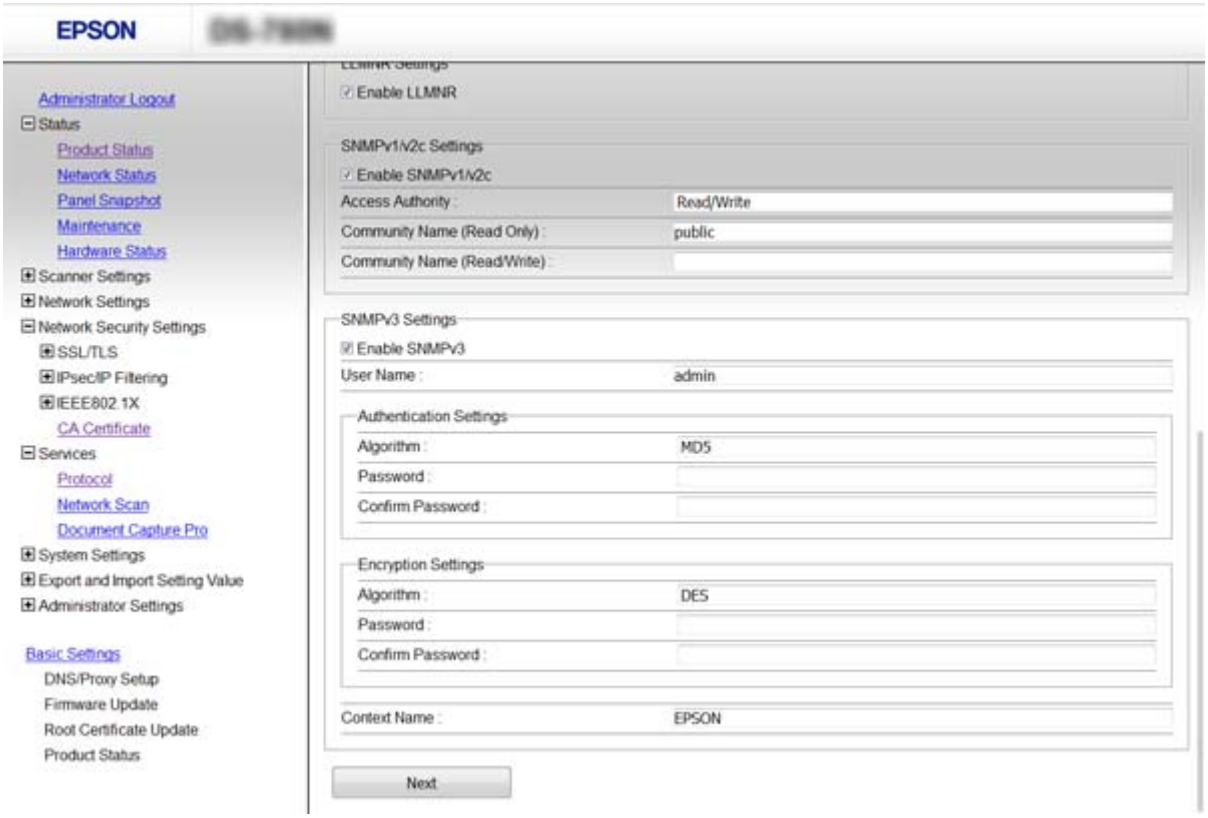
   Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.

   Ustawienia skanera zostały zaktualizowane.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Opcje ustawień protokołu SNMPv3” na stronie 84

## Opcje ustawień protokołu SNMPv3




| Obsługiwane algorytmy | Ustawienia i wyjaśnienie |
|---|---|
| Enable SNMPv3 | Protokół SNMPv3 jest włączony, gdy to pole wyboru jest zaznaczone. |
| User Name | Wprowadź od 1 do 32 jednobajtowych znaków. |
| Authentication Settings | |
| Algorithm | Wybierz algorytm uwierzytelniania. |

| Obsługiwane algorytmy | Ustawienia i wyjaśnienie |
|---|---|
| Password | Wprowadź od 8 do 32 znaków w kodowaniu ASCII (0x20–0x7E). |
| Confirm Password | Wprowadź skonfigurowane hasło w celu potwierdzenia. |
| Encryption Settings | |
| Algorithm | Wybierz algorytm szyfrowania. |
| Password | Wprowadź od 8 do 32 znaków w kodowaniu ASCII (0x20–0x7E). |
| Confirm Password | Wprowadź skonfigurowane hasło w celu potwierdzenia. |
| Context Name | Wprowadź od 1 do 32 jednobajtowych znaków. |

**Powiązane informacje**

➡ „Konfigurowanie protokołu SNMPv3” na stronie 83

# Podłączanie skanera do sieci IEEE802.1X

## Konfigurowanie sieci IEEE802.1X

Jeśli skaner obsługuje standard IEEE802.1X, można go używać w sieci z uwierzytelnianiem opartym na serwerze RADIUS z wykorzystaniem koncentratora jako elementu uwierzytelniającego.

1. Otwórz narzędzie Web Config i wybierz pozycje **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Wprowadź wartość dla każdej pozycji.
3. Kliknij przycisk **Next**.

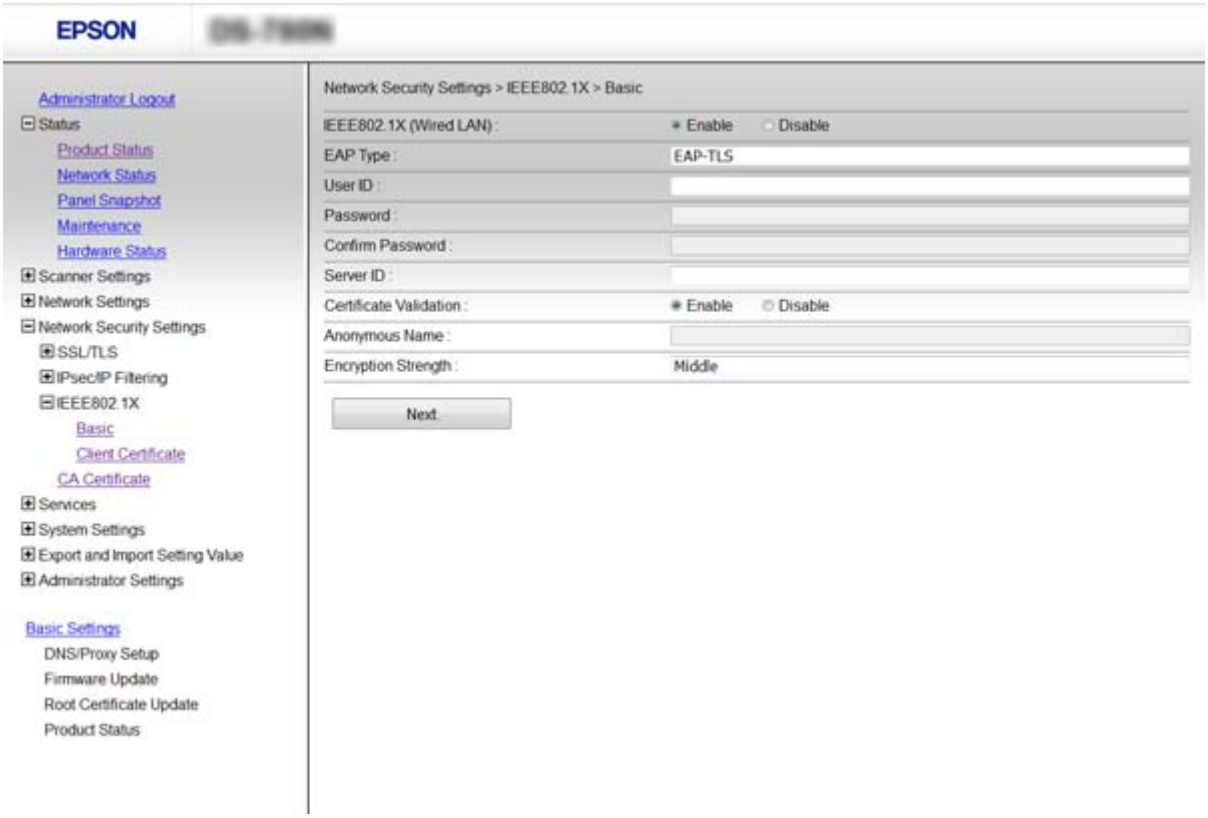
   Wyświetlony zostanie komunikat z potwierdzeniem.
4. Kliknij przycisk **OK**.

   Ustawienia skanera zostały zaktualizowane.

**Powiązane informacje**

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23
➡ „Opcje ustawień dla sieci IEEE802.1X” na stronie 86
➡ „Nie można uzyskać dostępu do drukarki lub skanera po skonfigurowaniu funkcji IEEE802.1X” na stronie 90

# Opcje ustawień dla sieci IEEE802.1X




| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| IEEE802.1X (Wired LAN) | Można włączać lub wyłączać ustawienia na stronie (**IEEE802.1X** > **Basic**) dla sieci IEEE802.1X (przewodowa sieć LAN). | |
| EAP Type | 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. |
| User ID | Określ identyfikator, który będzie służył do uwierzytelniania na serwerze RADIUS.<br>Wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). | |
| Password | Określ hasło do uwierzytelniania skanera.<br>Wprowadź od 1 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). Jeśli serwer Windows pełni rolę serwera RADIUS, można wprowadzić do 127 znaków. | |
| Confirm Password | Wprowadź skonfigurowane hasło w celu potwierdzenia. | |
| Server ID | 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.<br>Wprowadź od 0 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). | |
| Certificate Validation | Można włączyć weryfikację certyfikatu bez względu na metodę uwierzytelniania. Zaimportuj certyfikat w oknie **CA Certificate**. | |

| Elementy | Ustawienia i objaśnienie | |
|---|---|---|
| Anonymous Name | Jeśli dla opcji **Authentication Method** zostanie wybrane ustawienie **PEAP-TLS** lub **PEAP/MSCHAPv2**, zamiast identyfikatora użytkownika na potrzeby pierwszej fazy uwierzytelniania PEAP można wybrać nazwę anonimową.<br>Wprowadź od 0 do 128 jednobajtowych znaków ASCII (0x20 do 0x7E). | |
| Encryption Strength | Dostępne są następujące opcje. | |
| | High | AES256/3DES |
| | Middle | AES256/3DES/AES128/RC4 |

### Powiązane informacje

➡ „Konfigurowanie sieci IEEE802.1X” na stronie 85

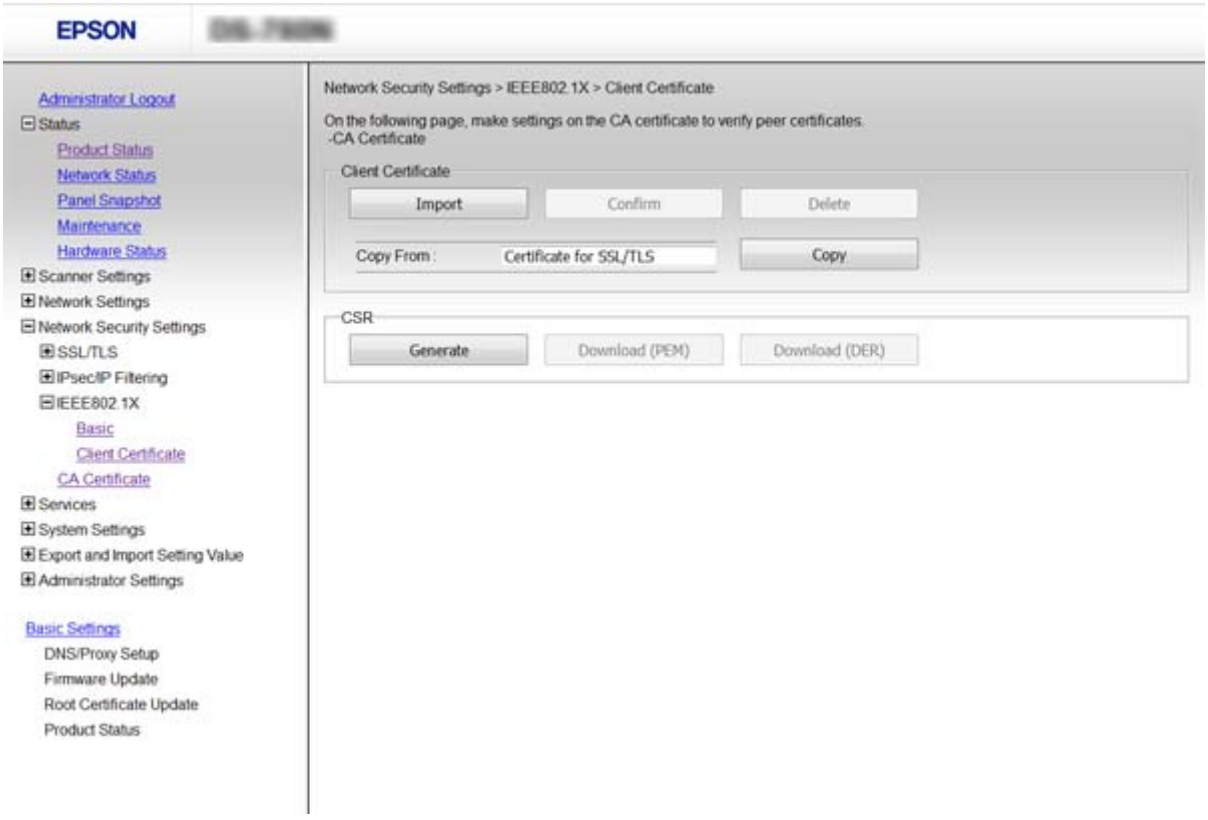
## Konfigurowanie certyfikatu na potrzeby protokołu IEEE802.1X

Skonfiguruj certyfikat klienta dla połączeń IEEE802.1X. Jeśli chcesz skonfigurować certyfikat centrum certyfikacji, przejdź do ustawienia **CA Certificate**.

1. Otwórz aplikację Web Config i wybierz pozycje **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Wprowadź certyfikat w polu **Client Certificate**.

   Jeśli certyfikat jest opublikowany przez centrum certyfikacji, możesz go skopiować. W celu skopiowania wybierz certyfikat w polu **Copy From** i kliknij przycisk **Copy**.



**Powiązane informacje**

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Uzyskiwanie i importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 64

# Rozwiązywanie problemów związanych z zaawansowanymi zabezpieczeniami

## Przywracanie ustawień zabezpieczeń

Utworzenie bardzo bezpiecznego środowiska, np. IPsec/Filtrowanie IP lub IEEE802.1X, 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 za pomocą panelu sterowania

Możliwe jest wyłączenie IPsec/filtrowania IP lub funkcji IEEE802.1X z poziomu panelu sterowania skanera.

1. Dotknij pozycji **Ustaw.** > **Ustawienia sieciowe**.
2. Dotknij pozycji **Zmień ustawienia**.
3. Dotknij pozycji, które mają być wyłączone.
   - ❏ **IPsec/Filtrowanie IP**
   - ❏ **IEEE802.1X**
4. Kiedy zostanie wyświetlony komunikat z potwierdzeniem zakończenia operacji, dotknij przycisku **Kont.**.

### Przywracanie funkcji zabezpieczeń za pomocą narzędzia Web Config

W przypadku IEEE802.1X urządzenia mogą nie być rozpoznawane w sieci. W takim przypadku wyłącz tę funkcję z poziomu panelu sterowania skanera.

W przypadku funkcji IPsec/Filtrowanie IP można wyłączyć tę funkcję, jeżeli możliwe jest uzyskanie dostępu do urządzenia z komputera.

#### *Wyłączanie IPsec/filtrowania IP za pomocą narzędzia Web Config*

1. Otwórz narzędzie Web Config i wybierz pozycje **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Wybierz ustawienie **Disable** dla opcji **IPsec/IP Filtering** w obszarze **Default Policy**.
3. Kliknij przycisk **Next**, a następnie usuń zaznaczenie opcji **Enable this Group Policy** w odniesieniu do wszystkich zasad grupowych.
4. Kliknij przycisk **OK**.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

# Problemy z korzystaniem z funkcji zabezpieczeń sieciowych

## Zapomniany klucz wstępny

### Ustaw klucz ponownie za pomocą aplikacji Web Config.

Aby zmienić klucz, otwórz aplikację Web Config i wybierz pozycje **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** lub **Group Policy**.

Po zmianie klucza wstępnego trzeba skonfigurować klucz wstępny na komputerach.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

## Brak możliwości nawiązania połączenia z wykorzystaniem protokołu IPsec

### Czy w ustawieniach komputera został skonfigurowany nieobsługiwany algorytm szyfrowania?

Skaner obsługuje algorytmy wymienione w poniższej tabeli.

| 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 ESP | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES |
| Algorytm uwierzytelniania ESP | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algorytm uwierzytelniania 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 71

## Nagły brak możliwości nawiązania komunikacji

### Czy adres IP skanera jest prawidłowy? Czy adres nie uległ zmianie?

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 narzędzia Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) może nie zostać znaleziony.

Należy używać statycznego adresu IP.

### Czy adres IP komputera jest prawidłowy? Czy adres nie uległ zmianie?

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 narzędzia Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) może nie zostać znaleziony.

Należy używać statycznego adresu IP.

### Powiązane informacje

➡ „Uzyskiwanie dostępu do aplikacji Web Config” na stronie 23

➡ „Szyfrowanie komunikacji za pośrednictwem funkcji IPsec/Filtrowanie IP” na stronie 71

## Brak połączenia po skonfigurowaniu filtrowania IPsec/IP

### Wybrana wartość może być nieprawidłowa.

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 71

## Nie można uzyskać dostępu do drukarki lub skanera po skonfigurowaniu funkcji IEEE802.1X

### Może to oznaczać, że ustawienia są nieprawidłowe.

Wyłącz łączność IEEE802.1X z poziomu panelu sterowania skanera. Połącz skaner i komputer, a następnie ponownie skonfiguruj połączenie IEEE802.1X.

### Powiązane informacje

➡ „Konfigurowanie sieci IEEE802.1X” na stronie 85

# Problemy z używaniem certyfikatu cyfrowego

## Brak możliwości zaimportowania certyfikatu podpisanego przez urząd certyfikacji

### Czy certyfikat podpisany przez urząd certyfikacji oraz informacje podane w żądaniu CSR są ze sobą zgodne?

Jeśli certyfikat podpisany przez urząd certyfikacji 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.

### Czy certyfikat podpisany przez urząd certyfikacji ma ponad 5 KB?

Zaimportowanie certyfikatu podpisanego przez urząd certyfikacji o wielkości przekraczającej 5 KB jest niemożliwe.

### Czy hasło do importu certyfikatu jest prawidłowe?

Jeśli nie pamiętasz hasła, zaimportowanie certyfikatu będzie niemożliwe.

### Powiązane informacje

➡ „Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 66

## Brak możliwości aktualizacji certyfikatu z podpisem własnym

### Czy podana została Common Name?

**Common Name** musi zostać podana.

### Czy Common Name zawiera nieobsługiwane znaki? Nieobsługiwane są na przykład znaki alfabetu japońskiego.

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

### Czy Common Name zawiera przecinek lub znak spacji?

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

### Powiązane informacje

➡ „Aktualizowanie certyfikatu z podpisem własnym” na stronie 68

## Brak możliwości utworzenia żądania CSR

### Czy podana została Common Name?

**Common Name** musi zostać podana.

### Czy opcje Common Name, Organization, Organizational Unit, Locality, State/Province zawierają nieobsługiwane znaki? Nieobsługiwane są na przykład znaki alfabetu japońskiego.

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

### Czy Common Name zawiera przecinek lub znak spacji?

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

### Powiązane informacje

➡ „Uzyskiwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 64

## Wyświetlane jest ostrzeżenie dotyczące certyfikatu cyfrowego

| Komunikat | Przyczyna i sposób rozwiązania problemu |
|---|---|
| Enter a Server Certificate. | **Przyczyna:**<br>Nie wybrano pliku do zaimportowania.<br>**Rozwiązanie:**<br>Wybierz plik i kliknij przycisk **Import**. |
| CA Certificate 1 is not entered. | **Przyczyna:**<br>Nie podano pierwszego certyfikatu urzędu certyfikacji. Podano wyłącznie drugi certyfikat urzędu certyfikacji.<br>**Rozwiązanie:**<br>Najpierw należy zaimportować pierwszy certyfikat urzędu certyfikacji. |
| Invalid value below. | **Przyczyna:**<br>Ścieżka dostępu do pliku i/lub hasło zawierają nieobsługiwane znaki.<br>**Rozwiązanie:**<br>Upewnij się, że wszystkie pozycje zostały podane prawidłowo. |
| Invalid date and time. | **Przyczyna:**<br>Nie ustawiono daty i godziny na skanerze.<br>**Rozwiązanie:**<br>Ustaw datę i godzinę za pomocą aplikacji Web Config lub EpsonNet Config. |
| Invalid password. | **Przyczyna:**<br>Podane hasło jest niezgodne z hasłem ustawionym dla certyfikatu urzędu certyfikacji.<br>**Rozwiązanie:**<br>Podaj prawidłowe hasło. |

## Zaawansowane ustawienia zabezpieczeń używane w przedsiębiorstwach

| Komunikat | Przyczyna i sposób rozwiązania problemu |
|---|---|
| Invalid file. | **Przyczyna:**<br>Importowany plik certyfikatu nie jest plikiem w formacie X509.<br>**Rozwiązanie:**<br>Upewnij się, że wybrano prawidłowy plik certyfikatu wysłany przez zaufany urząd certyfikacji. |
| | **Przyczyna:**<br>Zaimportowany plik jest zbyt duży. Maksymalny dopuszczalny rozmiar pliku to 5 KB.<br>**Rozwiązanie:**<br>Jeśli wybrano prawidłowy plik, zachodzi podejrzenie uszkodzenia lub sfałszowania certyfikatu. |
| | **Przyczyna:**<br>Łańcuch zawarty w certyfikacie jest nieprawidłowy.<br>**Rozwiązanie:**<br>Więcej informacji na temat certyfikatu zawiera serwis WWW urzędu certyfikacji. |
| Cannot use the Server Certificates that include more than three CA certificates. | **Przyczyna:**<br>Plik certyfikatu w formacie PKCS#12 zawiera więcej niż 3 certyfikaty urzędów certyfikacji.<br>**Rozwiązanie:**<br>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. |
| The certificate has expired. Check if the certificate is valid, or check the date and time on the product. | **Przyczyna:**<br>Certyfikat jest nieaktualny.<br>**Rozwiązanie:**<br>❏ Jeśli certyfikat jest nieaktualny, pobierz i zaimportuj nowy certyfikat.<br>❏ Jeśli certyfikat jest aktualny, sprawdź, czy ustawienia daty i godziny na skanerze są prawidłowe. |
| Private key is required. | **Przyczyna:**<br>Z certyfikatem nie jest powiązany klucz prywatny.<br>**Rozwiązanie:**<br>❏ Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PEM/DER, należy wskazać plik klucza prywatnego.<br>❏ Jeśli na podstawie żądania CSR na komputerze został pobrany certyfikat w formacie PKCS#12, należy utworzyć plik z kluczem prywatnym. |
| | **Przyczyna:**<br>Ponownie zaimportowano certyfikat w formacie PEM/DER uzyskany na podstawie żądania CSR za pomocą aplikacji Web Config.<br>**Rozwiązanie:**<br>Jeśli na podstawie żądania CSR w aplikacji Web Config został pobrany certyfikat w formacie PEM/DER, certyfikat ten można zaimportować tylko raz. |

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

### Powiązane informacje

➡ „Informacje o certyfikatach cyfrowych” na stronie 63

## Plik z certyfikatem podpisanym przez urząd certyfikacji został omyłkowo usunięty

### Czy istnieje plik kopii zapasowej certyfikatu?

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

➡ „Usuwanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 68

➡ „Importowanie certyfikatu podpisanego przez urząd certyfikacji” na stronie 66