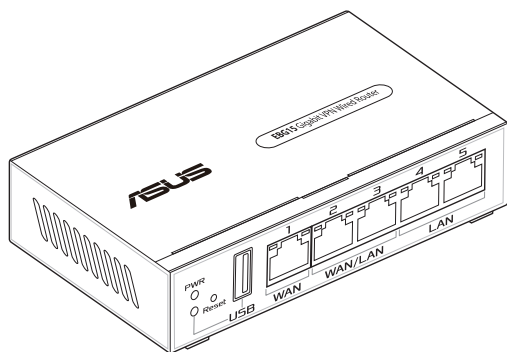


Podręcznik użytkownika

ASUS EBG15

Przewodowy gigabitowy router VPN

Model: EBG15



PL23348

Wydanie pierwsze

Kwiecień 2024

Copyright © 2024 ASUSTeK Computer Inc. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Spis treści

1 Poznanie EBG15

1.1	Witamy!	7
1.2	Zawartość opakowania	7
1.3	Przewodowy router	8
1.4	Usytuowanie routera.....	10
1.5	Wymagania dotyczące instalacji.....	11
1.6	Instalacja routera	12
1.6.1	Połączenie przewodowe.....	13

2 Ustawienia sprzętu

2.1	Logowanie do GUI web.....	14
2.2	Automatyczne wykrywanie sieci WAN	15

3 Konfiguracja EBG15

3.1	Adaptacyjna funkcja QoS	17
3.1.1	Monitor przepustowości	17
3.1.2	QoS	18
3.1.3	Historia stron sieci Web.....	18
3.1.4	Szybkość Internetu	19
3.2	Administration (Administracja)	20
3.2.1	Operation Mode (Tryb działania)	20
3.2.2	System.....	21
3.2.3	Aktualizacja firmware	22
3.2.4	Przywracanie/zapisywanie/przesyłanie ustawień.....	23
3.2.5	Raport.....	24
3.2.6	Prywatność.....	25
3.3	AiMesh.....	26
3.3.1	Konfiguracja systemu ExpertWiFi AiMesh.....	26
3.3.2	Zarządzanie klientami sieci	27
3.4	AiProtection.....	28
3.4.1	Network Protection	28

Spis treści

3.5	Pulpit nawigacyjny	32
3.6	Kontrola dostępu do urządzenia	33
3.6.1	Filtry sieci Web i aplikacji.....	33
3.6.2	Ustalanie harmonogramu.....	34
3.7	Zapora	35
3.7.1	Ogólne	35
3.7.2	Filtr adresów URL	36
3.7.3	Filtr słów kluczowych.....	37
3.7.4	Network Services Filter (Filtr usług sieciowych).....	38
3.8	IPv6 (Protokół IPv6).....	39
3.9	LAN (Sieć LAN).....	40
3.9.1	LAN IP (Adres IP sieci LAN).....	40
3.9.2	DHCP Server (Serwer DHCP)	41
3.9.3	Route (Trasa).....	43
3.9.4	IPTV	44
3.9.5	Przełączanie sterowania	44
3.9.6	VLAN.....	45
3.10	Narzędzia sieciowe	47
3.10.1	Analiza sieci.....	47
3.10.2	Netstat.....	47
3.10.3	Wake on LAN.....	47
3.10.4	Reguła inteligentnego łączenia	47
3.11	Sieć programowalna	48
3.11.1	Pracownicy	49
3.11.2	Portal gościnny	49
3.11.3	Sieć gościnna	50
3.11.4	Sieć z harmonogramem	50
3.11.5	Sieć IoT	51
3.11.6	Sieć VPN.....	51
3.11.7	Eksplorator scenariuszy	52

Spis treści

3.11.8	Sieć niestandardowa.....	53
3.12	System Log (Dziennik systemu)	54
3.13	Monitor ruchu.....	55
3.13.1	Analizator ruchu	55
3.14	Aplikacja USB.....	56
3.14.1	Media Server (Serwer multimediiów)	56
3.14.2	Udostępnianie miejsca sieciowego (Samba)	57
3.14.3	FTP Share (Udostępnianie FTP).....	57
3.14.4	Serwer drukarki sieciowej.....	58
3.14.5	Modem USB	66
3.15	Połącz sieci VPN.....	67
3.15.1	Połączone sieci VPN.....	67
3.15.2	Internet Connection (Połączenie internetowe).....	68
3.16	Serwer VPN	69
3.16.1	PPTP	69
3.16.2	OpenVPN.....	70
3.16.3	IPSec VPN	71
3.16.4	WireGuard® VPN.....	72
3.17	WAN (Sieć WAN).....	73
3.17.1	Internet Connection (Połączenie internetowe).....	73
3.17.2	Wiele sieci WAN.....	75
3.17.3	Port Trigger (Wyzwalanie portów).....	77
3.17.4	Virtual Server/Port Forwarding (Serwer wirtualny/ Przekierowanie portów)	79
3.17.5	DMZ (Strefa DMZ)	82
3.17.6	DDNS (Usługa DDNS).....	83
3.17.7	NAT Passthrough (Przekazywanie NAT)	84
3.18	Wireless (Sieć bezprzewodowa).....	85
3.18.1	General (Ogólne).....	85
3.18.2	Filtr adresów MAC urządzeń bezprzewodowych	86
3.18.3	Lista blokady roamingu	87

4 Rozwiązywanie problemów

4.1 Rozwiązywanie podstawowych problemów 88

4.2 Często zadawane pytania (FAQ) 90

Załączniki

Uwagi dotyczące bezpieczeństwa 107

Obsługę i Pomoc 109

1 Poznanie EBG15

1.1 Witamy!

Dziękujemy za zakup routera ASUS EBG15!

Router EBG15 zapewnia szybką, bezpieczną i skalowalną sieć, zwiększoną stabilność sieci dzięki łączności Ethernet oraz zapasowe łącza internetowe dzięki dwóm portom WAN/LAN i jednemu portowi USB do obsługi operacji.

1.2 Zawartość opakowania

- | | |
|---|--|
| ☒ EBG15 | ☒ Kabel RJ45 |
| ☒ Adapter zasilania | ☒ Naklejka z informacjami o logowaniu lokalnym |
| ☒ Instrukcja szybkiego uruchomienia | ☒ Karta gwarancyjna |

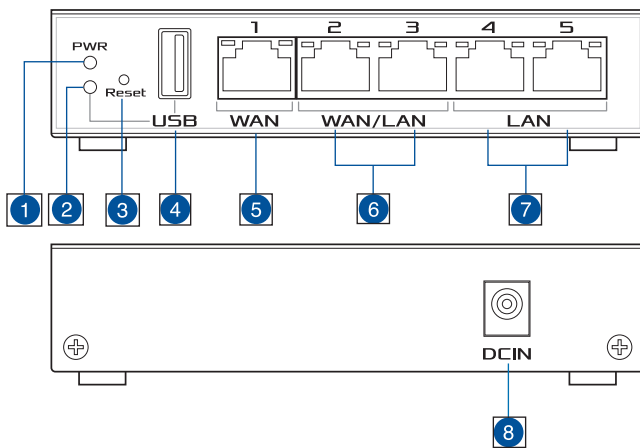
UWAGI:

- Jeżeli którykolwiek z elementów jest uszkodzony lub brakuje go, skontaktować się z firmą ASUS celem uzyskania pomocy technicznej; patrz **Obsługę i Pomoc** na tylnej stronie okładki niniejszej instrukcji obsługi.
 - Zachować oryginalne opakowanie na wypadek skorzystania w przyszłości z usług gwarancyjnych takich jak naprawa lub wymiana.
-

1.3 Przewodowy router

- 1 Podłącz zasilacz do portu DCIN.
- 2 Gdy urządzenie będzie gotowe do użytkowania, zaświeci się wskaźnik LED zasilania.

Informacje o przyciskach i portach



- 1 **Dioda zasilania**
Wyłączona: Brak zasilania.
Włączona: Urządzenie jest gotowe.
Powolne miganie: Tryb ratunkowy.
- 2 **Wskaźnik LED portu USB 3.2 Gen 1**
Wyłączona: Brak zasilania lub brak fizycznego połączenia.
Włączona: Urządzenie jest gotowe.
Powolne miganie: Przesyłanie lub odbieranie danych.
- 3 **Przycisk RESET**
Przycisk służy do przywracania domyślnych ustawień systemu.
- 4 **Port USB 3.2 Gen 1**
Port ten służy do podłączenia urządzenia zgodnego z USB 3.2 Gen 1 takich jak dysk twardy USB lub napęd flash USB.
- 5 **Port sieci WAN (Internet)**
Służy do podłączania kabla sieciowego w celu ustanowienia WAN połączenia.
- 6 **Porty sieci WAN / LAN**
Służy do podłączania kabla sieciowego w celu ustanowienia WAN / LAN połączenia.
- 7 **Porty LAN**
Podłącz komputer do portu LAN za pomocą kabla sieciowego.
- 8 **Gniazdo zasilania (DCIN)**
Służy do podłączenia wtyczki zasilacza prądu przemiennego wchodzącego w skład zestawu i podłączenia routera do zasilacza.

Wskaźniki LED portu Ethernet

Wskaźnik LED			
Dioda LED szybkości (Zielony)		Wskaźnik LED Link/Act (bursztynowy)	
1G	Wł.	1G/100M/10M	Miganie
100M/10M	WYł.	Brak ruchu	Wł.

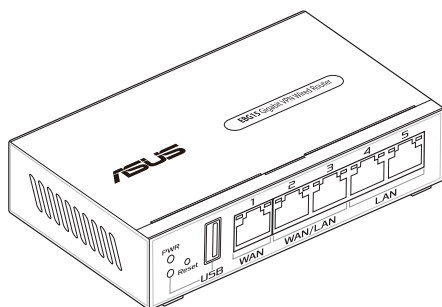
Specyfikacje:

Zasilacz DC	Wyjście DC: +12 V oraz maks. natężenie 1,5 A		
Temperatura robocza	0°C~40°C	Przechowywanie	0°C~70°C
Wilgotność robocza	50%~90%	Przechowywanie	20%~90%

1.4 Usytuowanie routera

Aby zapewnić najlepszą jakość korzystania z sieci, należy upewnić się, że:

- Zawsze zaktualizować oprogramowanie do najnowszej wersji oprogramowania sprzętowego. Najnowsze informacje dotyczące aktualizacji oprogramowania można uzyskać na stronie internetowej ASUS pod adresem <http://www.asus.com>.



1.5 Wymagania dotyczące instalacji

Do wykonania ustawień sieci potrzeba jednego lub dwóch komputerów, które spełniają następujące wymagania systemowe:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Zainstalowana usługa TCP/IP
- Przeglądarka sieci web, taka jak Internet Explorer, Firefox, Safari lub Google Chrome

UWAGA: Kable Ethernet RJ-45 wykorzystywane do połączenia z urządzeniami sieciowymi nie powinny być dłuższe niż 100 metrów.

1.6 Instalacja routera

WAŻNE!

- Przed skonfigurowaniem przewodowy router ASUS wykonać następujące czynności:
 - W przypadku zastępowania istniejącego routera odłączyć router od sieci.
 - Odłączyć kable/przewody od istniejącego modemu. Jeżeli modem ma baterię zasilania awaryjnego należy ją również wyciągnąć.
 - Ponownie uruchomić komputer (zalecane).
-

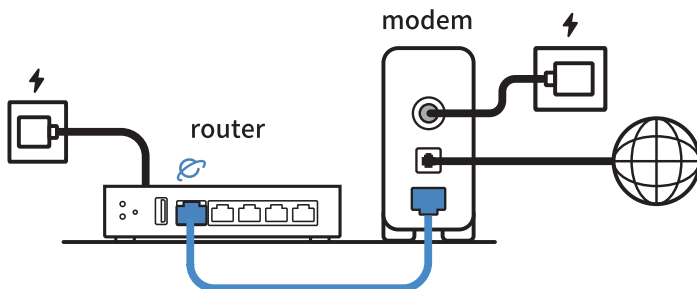


OSTRZEŻENIE!

- Przewody zasilające należy podłączać do gniazd elektrycznych o odpowiednim uziemieniu. Urządzenie należy podłączyć wyłącznie do znajdującego się w pobliżu gniazda elektrycznego, które jest łatwo dostępne.
 - Jeśli uszkodzony został zasilacz nie należy próbować naprawiać go samemu. Należy skontaktować się z wykwalifikowanym technikiem serwisu lub ze sprzedawcą.
 - NIE NALEŻY przykrywać szczelin wentylacyjnych komputera desktop PC, aby zapobiec przegrzaniu systemu.
 - NIE NALEŻY montować tego urządzenia na wysokości większej niż 2 metry.
 - Ten produkt należy używać w miejscach o temperaturze otoczenia w zakresie 0°C (32°F) do 40°C (104°F).
-

1.6.1 Połączenie przewodowe

UWAGA: Do podłączenia przewodowego można użyć kabla prostego lub skrosowanego.



W celu wykonania ustawienia przewodowy router poprzez połączenie przewodowe:

1. Włożyć wtyczkę zasilacza prądu przemiennego do gniazda wejścia prądu stałego i włożyć zasilacz do gniazda sieciowego.
2. Używając dołączonego kabla sieciowego, podłączyć komputer do gniazda sieci lokalnej przewodowy router.
3. Używając drugiego kabla sieciowego, podłączyć modem do gniazda sieci WAN przewodowy router.
4. Włożyć wtyczkę zasilacza prądu przemiennego modem do gniazda wejścia prądu stałego i włożyć zasilacz do gniazda sieciowego.

2 Ustawienia sprzętu

2.1 Logowanie do GUI web

Przewodowy router ASUS jest dostarczany z intuicyjnym GUI (graphics user interface (graficzny interfejs użytkownika)), który umożliwia łatwą konfigurację jego różnych funkcji poprzez przeglądarkę sieci web, taką jak Microsoft Edge, Safari lub Google Chrome.

UWAGA: Funkcje mogą się różnić w zależności od wersji oprogramowania sprzętowego.

Nawiązywanie przewodowego połączenia z siecią:

Aby zalogować się do GUI web:

1. W przeglądarce sieci web, wprowadź <http://expertwifi.net>.
2. Należy wykonać instrukcje konfiguracji.

2.2 Automatyczne wykrywanie sieci WAN

Funkcja QIS (Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)) pomaga w szybkim wykonaniu połączenia z Internetem.

UWAGA: Podczas ustawiania połączenia z Internetem pierwszy raz, naciśnij i przytrzymaj przycisk Reset na przewodowy router w celu przywrócenia jego ustawień fabrycznych.

Automatyczne wykrywanie sieci WAN:

1. Aby użyć QIS z autodetekcją, i kliknij pozycję **Create A New Network (Utwórz nową sieć)**.



2. Kliknij przycisk **Next (Dalej)**, aby zalogować się za pomocą domyślnej nazwy użytkownika i hasła.

The screenshot displays the 'Local Login' configuration page. On the left, there are navigation links: 'Local Login' (active), 'Username / Password', and 'Settings'. The main heading is 'Set up Local Login username and password to prevent unauthorized access to your ASUS networking device.' Below this, there are two input fields: 'Username' with the value 'admin' and 'New password' which is masked with dots. A checkbox labeled 'Use default Local Login Password' is checked. Below the checkbox, there is a small explanatory text: 'The default encrypted Local Login Password provides a secure login process when you connect to this ASUS networking device locally.' At the bottom, there is a link 'How to find Local Login Password' and two buttons: 'Previous' and 'Next'.

Usun zaznaczenie opcji **Use default Local Login Password (Użyj domyślnego lokalnego hasła logowania)** i wprowadź nową nazwę użytkownika i hasło, a następnie kliknij przycisk **Next (Dalej)**.

Local Login
Username / Password
Settings

Set up Local Login username and password to prevent unauthorized access to your ASUS networking device.

Username
admin

New password

Retype Password

☐ Use default Local Login Password
The default encrypted Local Login Password provides a secure login process when you connect to this ASUS networking device locally.

[How to find Local Login Password](#)

Previous Next

- Kliknij przycisk **Firmware Upgrade (Aktualizacja oprogramowania sprzętowego)**, aby zaktualizować oprogramowanie sprzętowe do najnowszej wersji lub kliknij przycisk **Cancel (Anuluj)**, aby zachować bieżącą wersję.

Firmware Upgrade

The latest firmware is available now. To improve the system efficiency, ASUS highly recommend upgrading your firmware version.

The latest version
3006_102_44136-g94573dc_349-g58e89

Cancel Firmware Upgrade

UWAGA: Ten ekran pojawia się tylko wtedy, gdy dostępna jest nowa wersja oprogramowania sprzętowego.

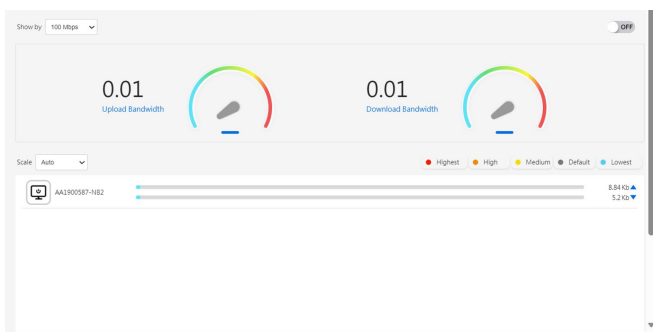
3 Konfiguracja EBG15

3.1 Adaptacyjna funkcja QoS

3.1.1 Monitor przepustowości

Funkcja Bandwidth Monitor (Monitor przepustowości) umożliwia monitorowanie poziomu przepustowości do operacji pobierania i przesyłania wykorzystywanej łącznie, jak i przez poszczególnych klientów.

Aby skorzystać z funkcji **Bandwidth Monitor (Monitor przepustowości)**, przejdź do pozycji **Settings (Ustawienia) > Adaptive QoS (Adaptacyjny QoS) > Bandwidth Monitor (Monitor przepustowości)**.

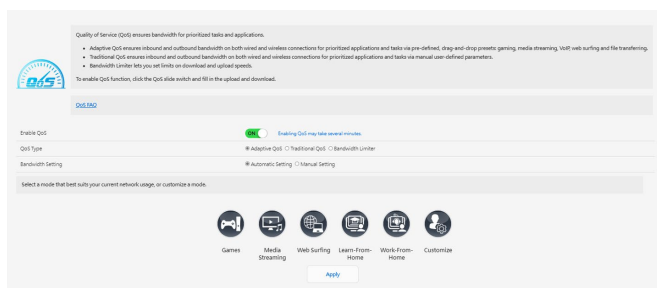


UWAGA: Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/faq/1008717>.

3.1.2 QoS

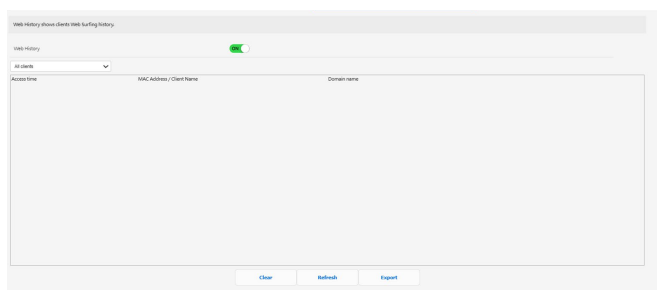
Funkcja QoS (ang. Quality of Service) odpowiada za przydzielanie przepustowości do priorytetowych zadań i aplikacji.

1. **Adaptive QoS (Adaptacyjny QoS)** odpowiada za przydzielanie przepustowości przychodzącej i wychodzącej w przypadku połączeń przewodowych oraz bezprzewodowych w ramach obsługi priorytetowych aplikacji i zadań za pomocą wstępnie zdefiniowanych ustawień konfigurowanych metodą przeciągania i upuszczania: gry, strumieniowe przesyłanie multimediów, VoIP, przeglądanie Internetu i transfer plików.
2. **Traditional QoS (Tradycyjny QoS)** odpowiada za przydzielanie przepustowości przychodzącej i wychodzącej w przypadku połączeń przewodowych oraz bezprzewodowych w ramach obsługi priorytetowych aplikacji i zadań za pomocą parametrów definiowanych ręcznie przez użytkownika.
3. **Bandwidth Limiter (Ogranicznik przepustowości)** umożliwia ustawienie limitów szybkości pobierania i przesyłania.



3.1.3 Historia stron sieci Web

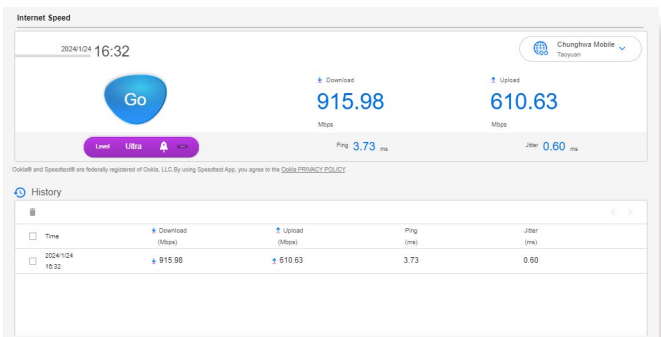
Web History (Historia stron sieci Web) to strona, na której wyświetlana jest historia przeglądania Internetu przez klienta.



3.1.4 Szybkość Internetu

Ta usługa jest zapewniana przez firmę Ookla®. Umożliwia wykrywanie szybkości pobierania i przesyłania z routera do Internetu.

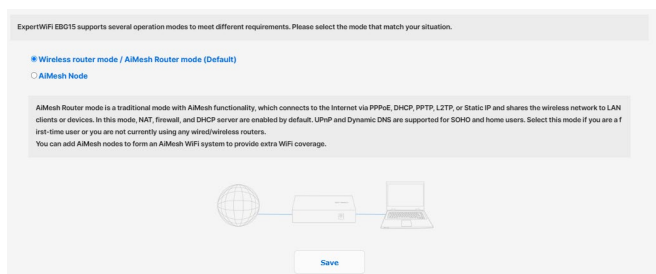
Kliknij przycisk **GO (IDŹ)** aby wykonać test szybkości połączenia internetowego, który trwa ok. minuty.



3.2 Administration (Administracja)

3.2.1 Operation Mode (Tryb działania)

Na stronie Operation Mode (Tryb działania) można wybrać odpowiedni tryb sieci.



W celu skonfigurowania trybu działania:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Operation Mode (Tryb działania)**.
2. Wybierz jeden z podanych trybów działania:
 - **Wireless router mode / AiMesh Router mode (Default) (Tryb routera bezprzewodowego / Tryb routera AiMesh) (domyślny):** Tryb routera AiMesh to tradycyjny tryb z obsługą funkcji AiMesh, który łączy się z Internetem poprzez PPPoE, DHCP, PPTP, L2TP lub statyczny adres IP i udostępnia sieć bezprzewodową klientom lub urządzeniom LAN. W tym trybie domyślnie włączone są funkcje NAT, zapory sieciowej i serwera DHCP. Obsługiwana jest funkcja UPnP i dynamiczny DNS dla użytkowników SOHO i domowych.
 - **AiMesh Node (Węzeł AiMesh):** Można dodać węzły AiMesh w celu utworzenia systemu Wi-Fi AiMesh, tak aby zapewnić dodatkowy zasięg sieci Wi-Fi.
3. Kliknij przycisk **Save (Zapisz)**.

UWAGA: Po zmianie trybu nastąpi ponowne uruchomienie routera.

3.2.2 System

Na stronie **System** można skonfigurować ustawienia przewodowy router.

W celu skonfigurowania ustawień System:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > System**.
2. Można skonfigurować następujące ustawienia:
 - **Change router login password (Zmień hasło logowania routera):** Hasło i nazwę logowania przewodowy router można zmienić, wprowadzając nową nazwę i hasło.
 - **USB setting (Ustawienie USB):** Można włączyć pozycję Enable HDD Hibernation (Włącz hibernację dysku twardego) i zmienić tryb USB.
 - **Time Zone (Strefa czasowa):** Wybierz strefę czasową sieci.
 - **NTP Server (Serwer NTP):** Przewodowy router może uzyskiwać dostęp do serwera NTP (Network time Protocol) w celu synchronizacji godziny.
 - **Network Monitoring (Monitorowanie sieci):** Można włączyć pozycję DNS Query (Zapytanie DNS) w celu zaznaczenia opcji Resolve Hostname (Rozpoznaj nazwę hosta) i Resolved IP Addresses (Rozpoznaj adres IP) lub włączyć pozycję Ping, a następnie zaznaczyć opcję Ping Target (Ping do miejsca docelowego).
 - **Auto Logout (Automatyczne wylogowanie):** Można ustawić czas do automatycznego wylogowania.
 - **Enable WAN down browser redirect notice (Włącz powiadomienie o przekierowaniu przeglądarki z informacją o niedostępności WAN):** Funkcja ta umożliwia wyświetlenie w przeglądarce strony z ostrzeżeniem, gdy router nie jest połączony z Internetem. Po wyłączeniu tej pozycji strona z ostrzeżeniem nie będzie wyświetlana.
 - **Enable Telnet (Włącz usługi Telnet):** Kliknij pozycję **Yes (Tak)**, aby włączyć usługi Telnet w sieci. Kliknij pozycję **No (Nie)**, aby wyłączyć usługi Telnet.
 - **Authentication Method (Metoda uwierzytelniania):** Jako zabezpieczenie dostępu do routera można wybrać protokół HTTP, HTTPS lub oba.
 - **Enable Reboot Scheduler (Włącz harmonogram ponownego uruchamiania):** Po włączeniu tej pozycji można ustawić opcję Date to Reboot (Data ponownego uruchomienia) i Time of Day to Reboot (Pora dnia dla ponownego uruchomienia).
 - **Enable Web Access from WAN (Włącz dostęp do sieci Web z sieci WAN):** Wybierz pozycję **Yes (Tak)**, aby urzędzenia spoza sieci mogły uzyskiwać dostęp do ustawień interfejsu graficznego przewodowy router. Wybierz opcję **No (Nie)**, aby uniemożliwić dostęp.

- **Enable Access Restrictions (Włącz ograniczenia dostępu):** Kliknij pozycję **Yes (Tak)**, jeśli chcesz określić adresy IP urządzeń, które mogą uzyskiwać dostęp do ustawień interfejsu graficznego przewodowy router z sieci WAN/LAN.
- **Service (Usługa):** Funkcja ta umożliwia skonfigurowanie pozycji Enable Telnet (Włącz Telnet)/Enable SSH (Włącz SSH)/SSH Port (Port SSH)/Allow Password Login (Zezwól na logowanie z hasłem)/Authorized Keys (Autoryzowane klucze)/Idle Timeout (Limit czasu bezczynności).

3. Kliknij przycisk **Apply (Zastosuj)**.

3.2.3 Aktualizacja firmware

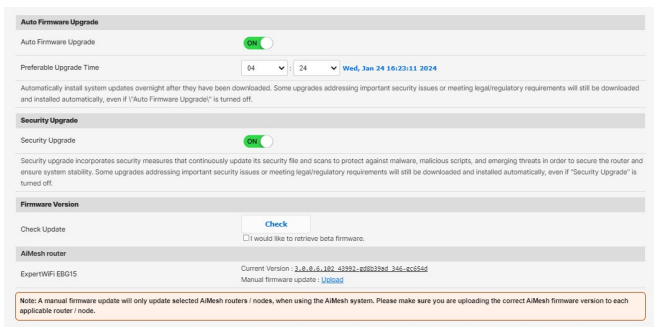
UWAGA: Pobierz najnowszy firmware ze strony sieci web ASUS, pod adresem <http://www.asus.com>.

Aktualizacja firmware:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**.
2. W polu **New Firmware File (Nowy plik oprogramowania sprzętowego)** kliknij pozycję **Browse (Przeglądaj)**, aby zlokalizować pobrany plik.
3. Kliknij **Upload (Prześlij)**.

UWAGI:

- Po ukończeniu procesu uaktualniania należy poczekać, aż system uruchomi się ponownie.
- Jeśli aktualizacja nie powiedzie się, przewodowy router automatycznie przejdzie do trybu awaryjnego, lub zacznie wolno migać wskaźnik LED zasilania na panelu przednim.



3.2.4 Przywracanie/zapisywanie/przesyłanie ustawień

Aby przywrócić/zapisać/przesłać ustawienia:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia)** > **Administration (Administracja)** > **Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)**.
2. Wybierz zadanie:
 - **Factory default (Domyślne ustawienia fabryczne):** Inicjowanie wszystkich ustawień i czyszczenie wszystkich dzienników danych funkcji AiProtection, Traffic Analyzer (Analizator ruchu) i Web History (Historia stron sieci Web).
 - **Save setting (Zapisz ustawienia):** Zaznacz to pole wyboru, jeśli chcesz udostępnić plik konfiguracji do debugowania. Z uwagi na to, że oryginalne hasło zostanie z pliku konfiguracji usunięte, nie należy importować tego pliku do routera.
 - **Restore setting (Ustawienia przywracania):** Załaduj ustawienia przywracania, które chcesz zastosować.

WAŻNE! W razie wystąpienia problemu należy załadować najnowszą wersję oprogramowania sprzętowego i skonfigurować nowe ustawienia. Nie należy przywracać ustawień domyślnych routera.

This function allows you to save current settings of ExpertWiFi EBM68 to a file, or load settings from a file.

Factory default	Restore	☒ Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.
Save setting	Save setting	☐ Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.
Restore setting	Upload	

3.2.5 Raport

W celu skorzystania z funkcji Feedback (Raport):

1. W panelu nawigacyjnym przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Feedback (Raport)**.
2. Aby uzyskać pomoc w rozwiązaniu problemu, wprowadź nazwę regionu, adres e-mail, dodatkowe informacje do debugowania, komentarze i sugestie oraz prześlij dziennik routera.

WAŻNE!

- Opisz szczegółowo problem, aby szybko uzyskać odpowiedź.
 - Zaakceptuj Politykę prywatności firmy ASUS.
-

We welcome your feedbacks, comments, suggestions, and feature ideas about ASUS products.

Your Region *

Your e-mail address *

Enter information for debugging *

System Log Linking File Router Log Port Log

Enable System Diagnostics

Yes No *No USB disk detected

Feedback problem type

Phone reset

Feedback problem description

Others

Comments / Suggestions *

Maximum of 2000 characters - characters left: 2000

☐ I agree to provide the above information, the model name, firmware version of my ASUS router, browser version, MAC address, IP address, internet status, router system information, the time I submit this feedback form to ASUS to diagnose and improve problems of my ASUS router, and to analyze user experience for the purpose of development and evaluation of new products and services of ASUS, and also agree to the [ASUS Privacy Policy](#)

Send

Note

- If you have any questions or urgency, please contact local technical support. <https://www.asus.com/support/Contact>

3.2.6 Prywatność

1. W przypadku powiązania kont, DDNS i połączenia zdalnego (aplikacja ASUS Router/aplikacja Lyra/AiCloud/AiDisk):

Należy pamiętać, że za pośrednictwem powyższych funkcji firmy ASUS gromadzone są takie informacje, jak nazwa modelu produktu, wersja oprogramowania sprzętowego, stan połączenia z Internetem, adres IP, adres MAC i nazwa DDNS.

Aby wyłączyć udostępnianie tych informacji za pośrednictwem funkcji firmy ASUS, należy kliknąć poniższą pozycję **Withdraw (Wycofaj zgodę)**. Należy jednak pamiętać, że po zaprzestaniu udostępniania informacji firmie ASUS funkcje te mogą nie działać.

WAŻNE!

- Kliknięcie pozycji **Withdraw (Wycofaj zgodę)** będzie powodem poniższych zmian:
 - Na routerze nie zostanie zachowana aktualnie używana nazwa DDNS.
 - Z aplikacji ASUS Router, Lyra, AiCloud, AiDisk będzie można korzystać tylko wtedy, gdy urządzenie będzie połączone z tą samą siecią LAN co router.

2. Zasady ochrony prywatności firmy ASUS (w przypadku uaktualniania oprogramowania sprzętowego/zabezpieczeń):

Należy pamiętać, że w celach związanych z uaktualnianiem oprogramowania sprzętowego/zabezpieczeń router ASUS będzie gromadził informacje użytkownika. Aby wyłączyć udostępnianie tych informacji routerowi ASUS, należy kliknąć poniższą pozycję **Withdraw (Wycofaj zgodę)**.

WAŻNE! Kliknięcie pozycji **Withdraw (Wycofaj zgodę)** może poskutkować niepowodzeniem uaktualnienia oprogramowania sprzętowego do najnowszej wersji i zapewnienia najnowocześniejszej ochrony routera ASUS. Jednakże w celu odpowiedniego zabezpieczenia routera i zapewnienia zgodności z przepisami nadal automatycznie pobierane i instalowane będą aktualizacje zawierające rozwiązania ważnych problemów z bezpieczeństwem lub spełniające wymogi prawne/regulacyjne.

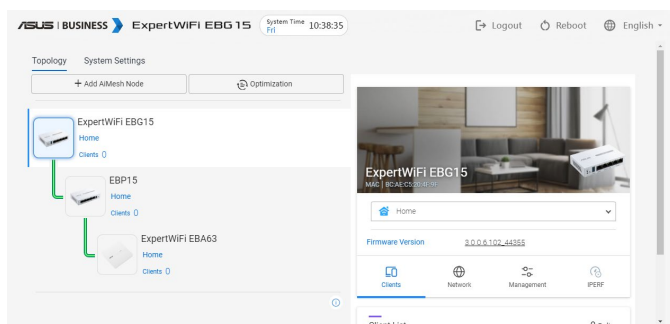
3.3 AiMesh

3.3.1 Konfiguracja systemu ExpertWiFi AiMesh

Aby zbudować system ExpertWiFi AiMesh, należy skonfigurować jego ustawienia.

Aby skonfigurować ustawienia systemu ExpertWiFi AiMesh:

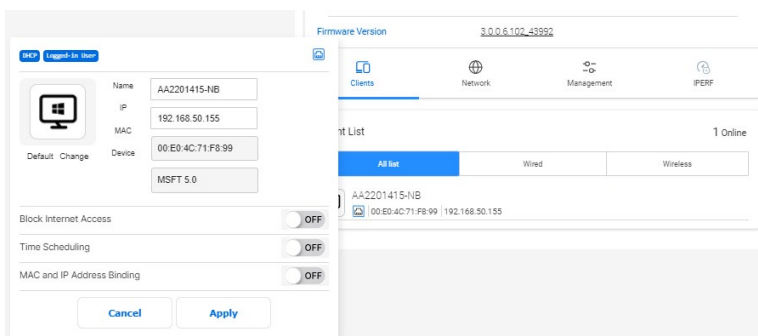
1. W panelu nawigacyjnym przejdź do pozycji **AiMesh > Topology (Topologia)**.
2. Można kliknąć dolną część pozycji **Set up as AiMesh Node (Skonfiguruj jako węzeł AiMesh)**, aby dodać urządzenia ExpertWiFi pod kontrolę routera EBG15.



3. Przejdź do pozycji **AiMesh > System Settings (Ustawienia Systemowe)**, aby włączyć lub wyłączyć pozycję **AiMesh node Ethernet auto setup (Automatyczna konfiguracja sieci Ethernet dla węzła AiMesh)**, **Ethernet Backhaul Mode (Tryb sieci Ethernet typu backhaul)**, skonfigurować pozycję **Roaming Block List (Lista blokady roamingu)**, **System Reset to Factory Default (Przywracanie domyślnych ustawień fabrycznych systemu)** lub **System Reset (Resetowanie systemu)**.



3.3.2 Zarządzanie klientami sieci

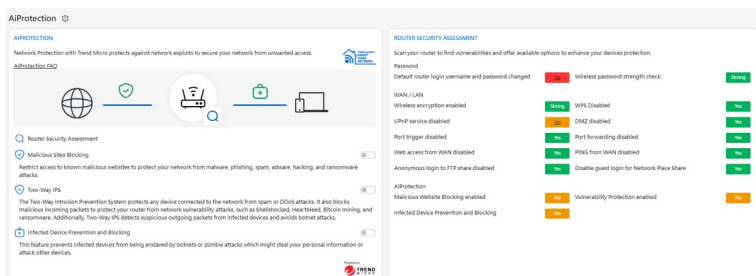


W celu zarządzania klientami sieci:

1. W panelu nawigacyjnym przejdź do pozycji **AiMesh > Topology (Topologia)**.
2. Wybierz ikonę **Clients (Klienci)**, aby wyświetlić takie informacje o kliencie sieci, jak nazwa klienta, adres MAC i IP.
3. Przesuwając suwak do pozycji **OFF (WYŁ.)**, można zablokować dostęp klienta do sieci, wyłączyć jego harmonogram lub wyłączyć powiązanie adresów MAC i IP.
4. Po zakończeniu kliknij **Apply (Zastosuj)**.

3.4 AiProtection

Funkcja AiProtection zapewnia monitorowanie w czasie rzeczywistym, które umożliwia wykrywanie złośliwego oprogramowania, programów szpiegujących oraz niechcianego dostępu. Filtruje ona także niechciane witryny i aplikacje, a także umożliwia ustalenie harmonogramu dostępu do Internetu przez połączone urządzenie.

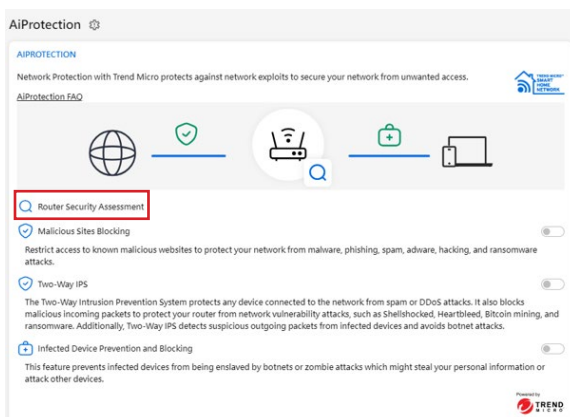


3.4.1 Network Protection

Funkcja Network Protection (Ochrona sieci) zapobiega wykorzystywaniu luk w sieci oraz zabezpiecza przed niechcianym dostępem do sieci.

W celu oceny zabezpieczeń routera:

1. W panelu nawigacji przejdź kolejno do pozycji **AiProtection**.
2. Kliknij pozycję **Router Security Assessment (Ocena zabezpieczeń routera)**, aby wyświetlić wyniki oceny zabezpieczeń.



ROUTER SECURITY ASSESSMENT			
Scan your router to find vulnerabilities and offer available options to enhance your devices protection.			
Password			
Default router login username and password changed	No	Wireless password strength check	Strong
WAN / LAN			
Wireless encryption enabled	Strong	WPS Disabled	Yes
UPnP service disabled	No	DMZ disabled	Yes
Port trigger disabled	Yes	Port forwarding disabled	Yes
Web access from WAN disabled	Yes	PING from WAN disabled	Yes
Anonymous login to FTP share disabled	Yes	Disable guest login for Network Place Share	Yes
AiProtection			
Malicious Website Blocking enabled	No	Vulnerability Protection enabled	No
Infected Device Prevention and Blocking	No		

WAŻNE! Stan pozycji z oznaczeniem **Yes (Tak)** na stronie **ROUTER SECURITY ASSESSMENT (OCENA ZABEZPIECZEŃ ROUTERA)** uważa się za bezpieczny. W przypadku pozycji z oznaczeniem **No (Nie)** zalecana jest odpowiednia konfiguracja.

3. (Opcjonalnie) Na stronie **ROUTER SECURITY ASSESSMENT (OCENA ZABEZPIECZEŃ ROUTERA)** skonfiguruj ręcznie pozycje z oznaczeniem **No (Nie)**. Aby to zrobić:
 - a. Kliknij pozycję.

UWAGA: Po kliknięciu pozycji w narzędziu wyświetlona zostanie strona ustawień pozycji.

- b. Na stronie ustawień zabezpieczeń danej pozycji wykonaj konfigurację i wprowadź wymagane zmiany, a po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
- c. Wróć na stronę **ROUTER SECURITY ASSESSMENT (OCENA ZABEZPIECZEŃ ROUTERA)** i kliknij przycisk **Close (Zamknij)**, aby zamknąć stronę.
4. W celu automatycznej konfiguracji ustawień zabezpieczeń kliknij przycisk **Secure Your Router (Zabezpiecz swój router)**.
5. Po wyświetleniu komunikatu kliknij przycisk **OK**.

W celu włączenia ochrony sieci:

1. W panelu nawigacji przejdź kolejno do pozycji **AiProtection**.
2. Wybierz typ ochrony, jaki chcesz zastosować i włącz go za pomocą przełącznika. Do wyboru są następujące opcje: **Malicious Sites Blocking, Two-Way IPS (Blokowanie niebezpiecznych witryn, Dwukierunkowy system IPS)** oraz **Infected Device Prevention and Blocking (Wykrywanie i blokowanie zainfekowanych urządzeń)**.

Blokowanie niebezpiecznych witryn

Funkcja ta ogranicza dostęp do znanych niebezpiecznych witryn w celu zabezpieczenia sieci przed złośliwym oprogramowaniem, phishingiem, spamem, oprogramowaniem reklamowym, oprogramowaniem wymuszającym okup i atakami hakerskimi.

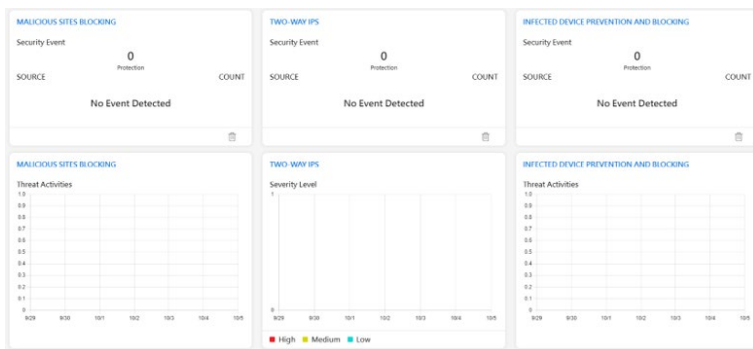
Dwukierunkowy system IPS

Funkcja Two-Way IPS (Dwukierunkowy system IPS) (ang. Intrusion Prevention System) chroni połączone urządzenia przed spamem i atakami typu DDoS. Blokuje ona także złośliwe pakiety przychodzące, zapobiegając atakom na luki w zabezpieczeniach sieci routera, takim jak Shellshocked, Heartbleed, Bitcoin Mining czy oprogramowanie wymuszające okup. Dodatkowo funkcja Two-Way IPS (Dwukierunkowy system IPS) wykrywa podejrzanе pakiety wychodzące z zainfekowanych urządzeń i zapobiega atakom botnetów.

Wykrywanie i blokowanie zainfekowanych urządzeń

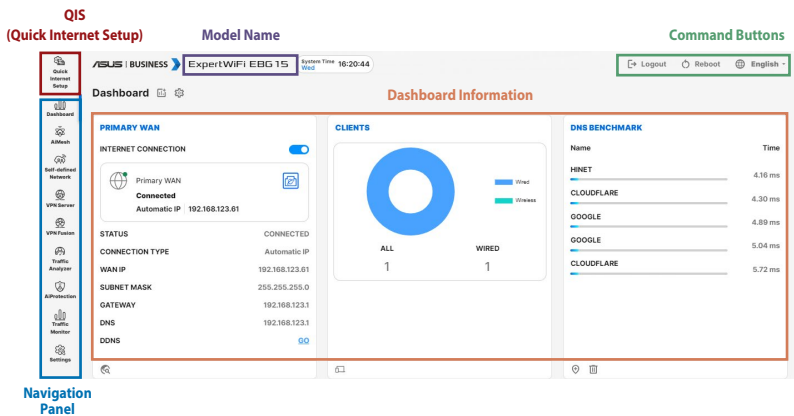
Funkcja ta zapobiega zniewalaniu zainfekowanych urządzeń przez botnety, a także atakom komputerów zombie, w wyniku których może dojść do kradzieży danych osobowych lub ataków na inne urządzenia.

3. Zaakceptuj **Trend Micro End User License Agreement (Umowę licencyjną użytkownika oprogramowania firmy Trend Micro)**.



3.5 Pulpit nawigacyjny

Pozycja Dashboard (Pulpit nawigacyjny) umożliwia zarządzanie takimi ustawieniami sieci, jak połączenie internetowe, połączenie z klientem, testy wydajności DNS, stan systemu, port Ethernet i monitor ruchu.



3.6 Kontrola dostępu do urządzenia

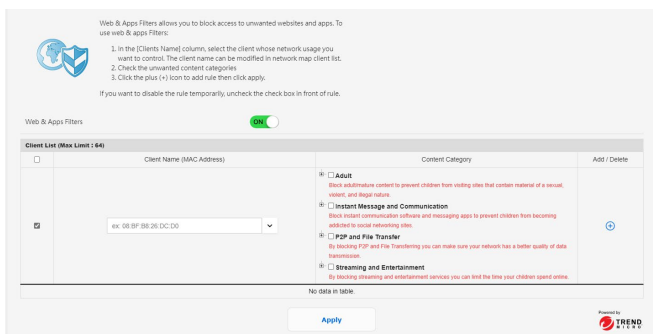
3.6.1 Filtry sieci Web i aplikacji

Funkcja Web & Apps Filters (Filtry sieci Web i aplikacji) umożliwia blokowanie dostępu do niechcianych stron internetowych i aplikacji.

W celu korzystania z funkcji Web & Apps Filters (Filtry sieci Web i aplikacji):

1. W panelu nawigacji przejdź kolejno do pozycji **Settings (Ustawienia) > Device access control (Kontrola dostępu do urządzenia) > Web & Apps Filters (Filtry sieci Web i aplikacji)**.
2. Przesuń suwak do pozycji **ON (WŁ.)**, aby włączyć funkcję **Web & Apps Filters (Filtry sieci Web i aplikacji)**.
3. W kolumnie **Client Name (Nazwa klienta)** wybierz klienta, w przypadku którego chcesz kontrolować korzystanie z sieci. Nazwę klienta można zmienić na liście klientów mapy sieci.
4. Zaznacz niechciane kategorie zawartości.
5. Kliknij **+** w celu dodania reguły, a następnie kliknij przycisk **Apply (Zastosuj)**.

Aby wyłączyć tymczasowo regułę, usuń jej zaznaczenie.



3.6.2 Ustalanie harmonogramu

Funkcja Time Scheduling (Ustalanie harmonogramu) umożliwia zaplanowanie czasu dostępu do Internetu przez określone urządzenia.

W celu korzystania z funkcji Time Scheduling (Ustalanie harmonogramu):

1. W panelu nawigacji przejdź kolejno do pozycji **Settings (Ustawienia) > Device access control (Kontrola dostępu do urządzenia) > Time Scheduling (Ustalanie harmonogramu)**.
2. Przesuń suwak do pozycji **ON (WŁ.)**, aby włączyć funkcję **Enable Time Scheduling (Włącz ustalanie harmonogramu)**.
3. W kolumnie **Client Name (Nazwa klienta)** wprowadź lub wybierz z listy rozwijanej nazwę klienta.
4. Kliknij  w celu dodania profilu klienta.
5. Kliknij przycisk **Apply (Zastosuj)**, aby zapisać ustawienia.

By enabling Block All Devices, all of the connected devices will be blocked from Internet access.

Enable block all devices ☒

This feature allows you to set up a scheduled time for specific devices' Internet access.



1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling ☒

System Time **Fri, Oct 06 16:42:29 2023**

Client List (Max Limit : 64)			
Select all	Client Name (MAC Address)	Time Management	Add / Delete
Time	ex: 08 BF B6 26 DC D0	~	
No data in table			

3.7 Zapora

3.7.1 Ogólne

Przewodowy router może pełnić funkcję zapory sprzętowej w sieci.

UWAGA: Funkcja Firewall (Zapora) jest domyślnie włączona.

W celu skonfigurowania podstawowych ustawień pozycji Firewall (Zapora):

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Firewall (Zapora) > General (Ogólne)**.
2. W polu **Enable Firewall (Włącz zaporę)** zaznacz pozycję **Yes (Tak)**.
3. W pozycji **Enable DoS protection (Włącz ochronę przed atakami typu DoS)** zaznacz pozycję **Yes (Tak)**, aby zapewnić ochronę sieci przed atakami typu „odmowa usługi” (DoS, Denial of Service), chociaż może to mieć wpływ na wydajność routera.
4. Można także monitorować wymianę pakietów między połączeniami w sieci LAN i WAN. W pozycji **Logged packets type (Typ zarejestrowanych pakietów)** wybierz opcję **Dropped (Porzucone)**, **Accepted (Zaakceptowane)** lub **Both (Oba)**.
5. Kliknij przycisk **Apply (Zastosuj)**.

Enable the Firewall to protect your local area network against attacks from hackers. The Firewall filters the incoming and outgoing packets based on the filter rules.

[View Firewall Rules](#)

Enable Firewall ☒ Yes ☐ No

Enable DoS protection ☒ Yes ☐ No

Logged packets type

Respond to DoS (ping) Request from WAN ☒ Yes ☐ No

Basic Config

Enable IPv4 Inbound Firewall Rules ☒ Yes ☐ No

Source IP	Port Range	Protocol	Action
		TCP	Deny

IPv4 Firewall

All outbound traffic coming from IPv4 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed from. You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (192.168.1.111:2222-3333:44 for example)

Basic Config

Enable IPv4 Firewall ☒ Yes ☐ No

Remote Server List

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Action
				TCP	Deny

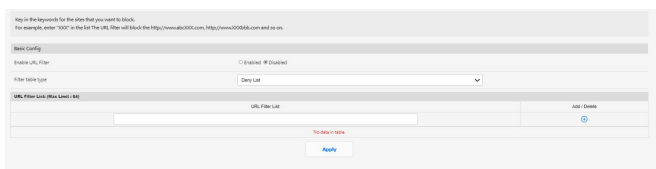
3.7.2 Filtr adresów URL

Można określić słowa kluczowe lub adresy sieci Web, aby uniemożliwić dostęp do pewnych adresów URL.

UWAGA: Pozycja URL Filter (Filtr adresów URL) zależy od zapytania DNS. Jeśli klient sieciowy uzyskał już dostęp do witryny sieci Web, np. `http://www.abcxxx.com`, witryna ta nie zostanie zablokowana (odwiedzone wcześniej witryny sieci Web są zapisywane w pamięci podręcznej DNS). Aby rozwiązać ten problem, należy wyczyścić pamięć podręczną DNS przed skonfigurowaniem pozycji URL Filter (Filtr adresów URL).

W celu skonfigurowania filtra adresów URL:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Firewall (Zapora) > URL Filter (Filtr adresów URL)**.
2. W polu **Enable URL Filter (Włącz filtr adresów URL)** wybierz opcję **Enabled (Włączono)**.
3. Wprowadź adres URL i kliknij przycisk .
4. Kliknij przycisk **Apply (Zastosuj)**.



3.7.3 Filtr słów kluczowych

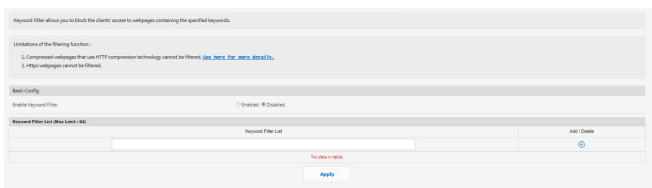
Filtr słów kluczowych blokuje dostęp do stron sieci Web zawierających określone słowa kluczowe.

W celu skonfigurowania filtra słów kluczowych:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Firewall (Zapora) > Keyword Filter (Filtr słów kluczowych)**.
2. W polu Enable Keyword Filter (Włącz filtr słów kluczowych) wybierz pozycję **Enabled (Włączono)**.
3. Wprowadź słowo lub wyrażenie i kliknij przycisk .
4. Kliknij przycisk **Apply (Zastosuj)**.

UWAGI:

- Pozycja Keyword Filter (Filtr słów kluczowych) zależy od zapytania DNS. Jeśli klient sieciowy uzyskał już dostęp do witryny sieci Web, np. <http://www.abcxxx.com>, witryna ta nie zostanie zablokowana (odwiedzone wcześniej witryny sieci Web są zapisywane w pamięci podręcznej DNS). Aby rozwiązać ten problem, należy wyczyścić pamięć podręczną DNS przed skonfigurowaniem pozycji Keyword Filter (Filtr słów kluczowych).
- Nie można filtrować stron sieci Web skompresowanych za pomocą kompresji protokołu HTTP. Przy użyciu filtra słów kluczowych nie można także blokować stron HTTPS.



3.7.4 Network Services Filter (Filtr usług sieciowych)

Za pomocą pozycji Network Services Filter (Filtr usług sieciowych) blokowana jest wymiana pakietów z sieci LAN do sieci WAN oraz ograniczany jest dostęp klientów sieciowych do określonych usług sieci Web, takich jak Telnet lub FTP.

W celu skonfigurowania filtra usług sieciowych:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia)** > **Firewall (Zapora)** > **Network Service Filter (Filtr usług sieciowych)**.
2. W polu **Enable Network Services Filter (Włącz filtr usług sieciowych)** zaznacz pozycję **Yes (Tak)**.
3. Wybierz opcję dla pozycji Filter table type (Typ tabeli filtrów). Pozycja **Deny List (Lista niedozwolonych)** umożliwia blokowanie określonych usług sieciowych. Pozycja **Allow List (Lista dozwolonych)** umożliwia ograniczenie dostępu do określonych usług sieciowych.
4. Określ przedziały czasu i dni, w które filtry mają być aktywne.
5. Aby określić, które usługi sieciowe mają być filtrowane, wprowadź wartości dla pozycji Source IP (Adres IP źródła), Destination IP (Docelowy adres IP), Port Range (Zakres portu) i Protocol (Protokół). Kliknij przycisk .
6. Kliknij przycisk **Apply (Zastosuj)**.

The Network Services Filter blocks the LAN to WAN packet exchanges and restricts clients from using specific network services. For example, if you do not want the clients to use the Internet services, you can block the traffic that uses port 80 to the destination port. The traffic that uses port 80 will be blocked (port 80 cannot be blocked). Leave the source IP field blank to apply this rule to all LAN clients.

Deny List Duration: During the scheduled duration, clients in the Deny List can access the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

Allow List Duration: During the scheduled duration, clients in the Allow List can ONLY use the specified network services.

NOT: If you set the subject for the Deny List, IP addresses outside the subject will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter: ☒ Yes, ☐ No

Filter table type:

Web/known Applications:

Date to Enable LAN to WAN Filter:

Time of Day to Enable LAN to WAN Filter:

Date to Disable LAN to WAN Filter:

Time of Day to Disable LAN to WAN Filter:

Filtered DHCP packet types:

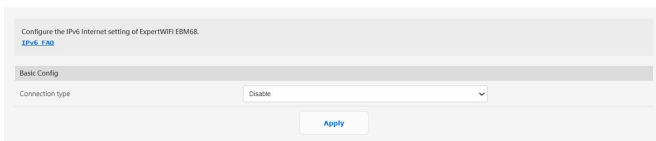
Source IP	Port Range	Destination IP	Port Range	Protocol	Act/Order
				TCP	

This table is blank.

Apply

3.8 IPv6 (Protokół IPv6)

Niniejszy przewodowy router obsługuje adresowanie IPv6, system obsługujący więcej adresów IP. W celu sprawdzenia, czy dana usługa internetowa obsługuje protokół IPv6 należy skontaktować się z usługodawcą internetowym.



W celu skonfigurowania protokołu IPv6:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > IPv6 (Protokół IPv6)**.
2. Wybierz opcję dla pozycji **Connection Type (Typ połączenia)**. Opcje konfiguracji różnią się w zależności od wybranego typu połączenia.
3. Wprowadź ustawienia sieci LAN i DNS dla protokołu IPv6.
4. Kliknij przycisk **Apply (Zastosuj)**.

UWAGI:

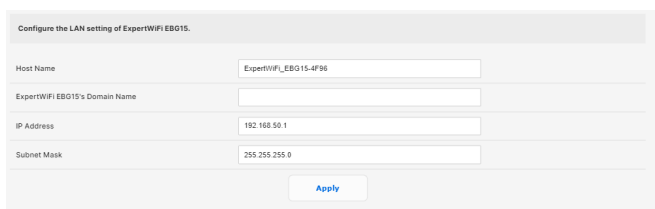
- W celu uzyskania określonych informacji dotyczących protokołu IPv6 dla danej usługi internetowej należy skontaktować się z usługodawcą internetowym.
 - Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/113990>.
-

3.9 LAN (Sieć LAN)

3.9.1 LAN IP (Adres IP sieci LAN)

Na ekranie LAN IP (Adres IP sieci LAN) można modyfikować ustawienia adresu IP sieci LAN przewodowy router.

UWAGA: Wszelkie zmiany adresu IP sieci LAN zostaną odzwierciedlone w ustawieniach DHCP.



The screenshot shows a web interface titled "Configure the LAN setting of ExpertWiFi_EBG15-4F96". It contains four input fields: "Host Name" with the value "ExpertWiFi_EBG15-4F96", "ExpertWiFi_EBG15's Domain Name" which is empty, "IP Address" with the value "192.168.50.1", and "Subnet Mask" with the value "255.255.255.0". Below these fields is a blue "Apply" button.

W celu zmodyfikowania ustawień adresu IP sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > LAN (Sieć LAN) > LAN IP (Adres IP sieci LAN)**.
2. Zmodyfikuj pozycje **IP address (Adres IP)** i **Subnet Mask (Maska podsieci)**.
3. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

3.9.2 DHCP Server (Serwer DHCP)

DHCP (ang. Dynamic Host Configuration Protocol) to protokół automatycznej konfiguracji stosowany w sieciach IP. Serwer DHCP może przypisać adres IP do każdego klienta i przekazać mu adres IP serwera DNS oraz adres IP domyślnej bramy.

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and inform the client of the IP of the DNS server IP and default gateway IP. Supports up to 255 IP addresses for your local network.

Manually Assigned IP - cannot use DHCP Pool

Manually Assigned IP (cannot be DHCP Pool (Static IP) 192.168.80.255)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
192.168.80.255				

W celu wykonania ustawień serwera DHCP:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > LAN (Sieć LAN) > DHCP Server (Serwer DHCP)**.
2. W polu **Enable the DHCP Server (Włączyć serwer DHCP)** zaznacz **Yes (Tak)**.
3. W polu tekstowym **Domain Name (Nazwa domeny)** wprowadź nazwę domeny przewodowy router.
4. W polu **IP Pool Starting Address (Adres początkowy zakresu IP)** wprowadź adres początkowy IP.
5. W polu **IP Pool Ending Address (Adres końcowy zakresu IP)** wprowadź adres końcowy IP.
6. W polu **Lease Time (Czas dzierżawy)** wprowadź czas zakończenia ważności adresów IP, po czym router bezprzewodowy automatycznie przydzieli nowe adresy IP klientom sieci.

UWAGI:

- Podczas określania zakresu adresów IP zalecane jest stosowanie formatu adresów IP: 192.168.1.xxx (xxx może być dowolną liczbą pomiędzy 2 a 254).
 - Pozycja IP Pool Starting Address (Adres początkowy zakresu IP) nie powinna być wyższa niż pozycja IP Pool Ending Address (Adres końcowy zakresu IP).
-

7. W części **DNS and WINS Server Settings (Ustawienia serwera DNS i WINS)** wprowadź w razie potrzeby adres IP serwera DNS i WINS.
8. Przewodowy router może także ręcznie przypisywać adresy IP urządzeniom w sieci. W polu **Enable Manual Assignment (Włącz przypisywanie ręczne)** wybierz opcję **Yes (Tak)**, aby przypisać adres IP do określonych adresów MAC w sieci. W celu ręcznego przypisywania do listy DHCP można dodać maksymalnie 32 adresy MAC.

3.9.3 Route (Trasa)

Funkcja ta umożliwia dodawanie do routera reguł rozsyłania. Jest przydatna w przypadku połączenia kilku routerów za urządzeniem EBG15 w celu współdzielenia tego samego połączenia internetowego.

This function allows you to add routing rules into ExpertWiFi EBM68. It is useful if you connect several routers behind ExpertWiFi EBM68 to share the same connection to the Internet.

Basic Config

Enable static routes ☒ Yes ☐ No

Network/Host IP	Network	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

W celu skonfigurowania tabeli routingu sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia)** > **LAN (Sieć LAN)** > **Route (Trasa)**.
2. W polu **Enable static routes (Włącz trasy statyczne)** zaznacz pozycję **Yes (Tak)**.
3. W obszarze **Static Route List (Lista tras statycznych)** wprowadź informacje o sieci dotyczące innych punktów dostępowych lub węzłów. Kliknij przycisk **Add (Dodaj)** [+](#) lub **Delete (Usuń)** [-](#) w celu dodania urządzenia do listy lub usunięcia go z niej.
4. Kliknij przycisk **Apply (Zastosuj)**.

3.9.4 IPTV

Przewodowy router obsługuje połączenia z usługami IPTV udostępniane przez usługodawcę internetowego lub sieć LAN. Zakładka IPTV zawiera ustawienia konieczne do konfiguracji pozycji IPTV, VoIP, multimedialnej i UDP dla danej usługi. W celu uzyskania konkretnych informacji dotyczących usługi należy skontaktować się z usługodawcą internetowym.

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN > Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None
Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing	Disable
UDP Proxy (latency)	0
Apply	

3.9.5 Przełączanie sterowania

Pozycja ta umożliwia skonfigurowanie routera w celu obsługi funkcji przełączania sterowania. Możliwe jest połączenie dwóch portów LAN 1 Gb/s w celu uzyskania szybkości połączenia przewodowego sięgającej 2 Gb/s dzięki powiązaniu ze zgodnym serwerem NAS lub innym urządzeniem sieciowym o dużej przepustowości.

UWAGI:

- Aby móc korzystać z protokołu LACP (ang. Link Aggregation Control Protocol), urządzenia muszą obsługiwać protokół IEEE 802.3ad.
- Funkcję agregacji portów LAN można zastosować, parując port LAN3 z portem LAN2.

Setting ExpertWiFi (802.3ad) switch control.

Jumbo Frame	Enable
Bonding/ Link aggregation	Enable
Enable Bonding (802.3ad) support for your wired client and then connect it to your Router's LAN3 and LAN2 port.	
Apply	

3.9.6 VLAN

VLAN (ang. Virtual Local Area Network) to sieć logiczna utworzona w ramach większej sieci fizycznej. Sieci VLAN umożliwiają segmentację sieci na mniejsze wirtualne podsieci, które mogą służyć do izolowania ruchu i zwiększenia wydajności sieci.

W celu konfiguracji sieci VLAN:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia)** > **LAN (Sieć LAN)** > **VLAN**.
2. Kliknij kartę **Profile (Profil)**, a następnie **+** w celu utworzenia profilu VLAN. Możesz ustawić własny identyfikator sieci VLAN.
3. Pozycja **Port isolation (Izolacja portów)** umożliwia ograniczenie prawa dostępu różnych urządzeń w danej sieci VLAN. Tutaj tworzona jest sieć „VLAN-only-Network”, czyli sieć z VID, ale bez DHCP.

The screenshot displays two panels from a network management interface. The top panel, titled 'VLAN Profile', has tabs for 'VLAN' and 'Profile'. The 'Profile' tab is active, showing a 'Profile List' table with columns: Network Name (SSID), VLAN ID, Port Isolation, and Add / Delete. The table is currently empty. The bottom panel, titled 'VLAN Switch Control Settings', has tabs for 'VLAN' and 'Profile'. The 'VLAN' tab is active, showing a table for 'AllMesh router' with four columns representing different ports (2, 3, 4, 5). Each column has a 'Mode' dropdown menu (all set to 'All(Default)') and an 'SDN (VLAN) Profile' dropdown menu (all set to 'Default'). An 'Apply' button is at the bottom.

Network Name (SSID)	VLAN ID	Port Isolation	Add / Delete
...		☐	+

Mode	SDN (VLAN) Profile
All(Default)	Default
All(Default)	Default
All(Default)	Default
All(Default)	Default

4. Kliknij kartę **VLAN**, aby wybrać port o określonym profilu i trybie **Trunk (Magistrala)/Access (Dostęp)**.

UWAGI: Można wybrać jeden z poniższych trybów domyślnych:

Tryb **All (Default) (Wszystko (domyślny))** zezwala na dostęp wszystkich oznaczonych i nieoznaczonych pakietów.

Tryb **Access (Dostęp)** zezwala na dostęp wybranych sieci SDN(VLAN). Można wybrać profile utworzone w pozycji Guest Network pro (Profesjonalna sieć gościnna) lub VLAN.

Tryb **Trunk (Magistrala):**

- **Allow all tagged (Zezwalaj na wszystkie oznaczone):**

Zezwalanie na dostęp tylko oznaczonych pakietów.

- **With selected SDN(VLAN) (Z wybraną siecią SDN(VLAN)):**

Zezwalanie na dostęp tylko wybranej sieci SDN lub VLAN.

5. Po zakończeniu kliknij **Apply (Zastosuj)**.

UWAGA: Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/1049415/>.

3.10 Narzędzia sieciowe

W celu skorzystania z narzędzi sieciowych należy w panelu nawigacyjnym przejść do pozycji **Settings (Ustawienia) > Network Tools (Narzędzia sieciowe)**.

3.10.1 Analiza sieci

Wysyłanie pakietów ICMP ECHO_REQUEST do hostów w sieci.

3.10.2 Netstat

Wyświetlanie szczegółowych informacji o sieci.

3.10.3 Wake on LAN

Funkcja WOL (ang. Wake-On-LAN) umożliwia wznawianie działania komputera za pomocą innego urządzenia w sieci.

3.10.4 Reguła inteligentnego łączenia

Konfiguracja ustawień funkcji inteligentnego łączenia.

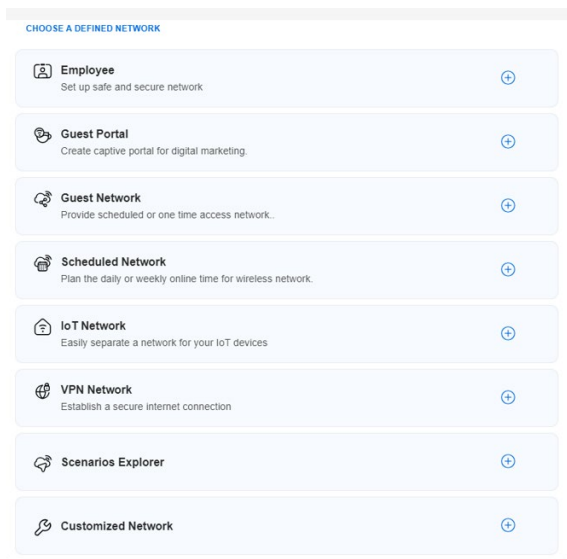
3.11 Sieć programowalna

Sieć SDN (ang. Self-Defined Network) zapewnia maks. pięć identyfikatorów SSID w celu wyodrębnienia urządzeń i nadania im priorytetu w zależności od zastosowania w firmie i alternatywnych sieci, co umożliwia tworzenie segmentów sieci dla pracowników, portali gościnnych, sieci gościnnych, harmonogramów sieci, sieci IoT i sieci VPN.

WAŻNE! Aby udostępnić funkcję Wi-Fi, należy z siecią AiMesh routera EBG15 zintegrować bezprzewodowy punkt dostępowy (AP), taki jak ExpertWiFi EBA63 lub router, taki jak ExpertWiFi EBR63 lub ExpertWiFi EBM68.

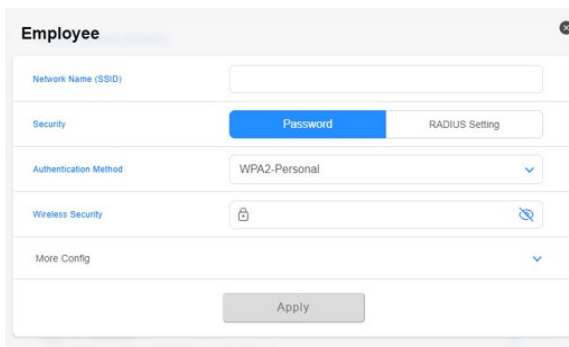
W celu utworzenia sieci Self-Defined Network (Sieć programowalna):

1. W panelu nawigacyjnym przejdź do pozycji **Self-Defined Network (Sieć programowalna)**.
2. Wybierz zdefiniowaną sieć, która jest odpowiednia dla określonego zastosowania.



3.11.1 Pracownicy

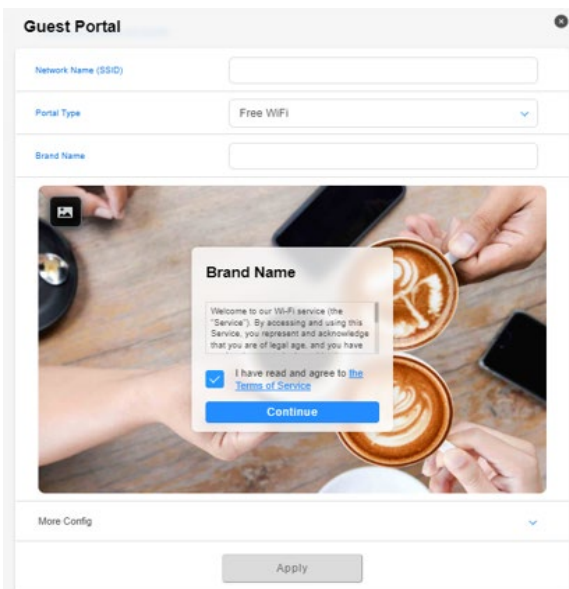
Umożliwia określenie poziomu dostępu dla różnych użytkowników w celu zwiększenia bezpieczeństwa sieci. Zalecana w przypadku biur, które przypisują działom różne uprawnienia.



The 'Employee' configuration window shows fields for 'Network Name (SSID)', 'Security' (with 'Password' and 'RADIUS Setting' tabs), 'Authentication Method' (set to 'WPA2-Personal'), and 'Wireless Security'. An 'Apply' button is at the bottom.

3.11.2 Portal gościnny

Umożliwia utworzenie portalu gościnnego dla marketingu cyfrowego. Zalecana w restauracjach, hotelach lub food truckach.



The 'Guest Portal' configuration window includes fields for 'Network Name (SSID)', 'Portal Type' (set to 'Free WiFi'), and 'Brand Name'. A preview image shows a mobile screen with a 'Brand Name' welcome message and a 'Continue' button. An 'Apply' button is at the bottom.

3.11.3 Sieć gościnna

Zapewnia zaplanowany lub jednorazowy dostęp do sieci dla tymczasowych użytkowników. Zalecana w centrach handlowych, siłowniach lub dla gości.

The screenshot shows the 'Guest Network' configuration window. It includes fields for 'Network Name (SSID)', 'Security' (with 'Open System' and 'Password' options), and 'WiFi Scheduling' (which is turned on). Under 'WiFi Scheduling', there are radio buttons for 'Scheduled' and 'One Time Access' (selected). Below these are buttons for time intervals: '30 mins', '1 hr(s)', '2 hr(s)' (highlighted in blue), '4 hr(s)', '6 hr(s)', and 'Custom'. At the bottom, there is a 'More Config' dropdown and an 'Apply' button.

3.11.4 Sieć z harmonogramem

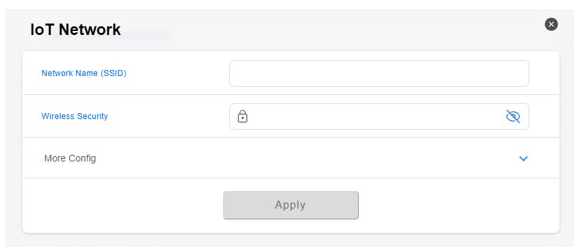
Planowanie czasu, w jakim sieć bezprzewodowa będzie dostępna w trybie online, w przedziale dnia lub tygodnia. Zalecana w przypadku nauczania zdalnego, lekcji szkolnych lub użytkowania przez dzieci.

The screenshot shows the 'Scheduled Network' configuration window. It includes fields for 'Network Name (SSID)', 'Wireless Security', and 'WiFi Scheduling' (which is turned on). Under 'WiFi Scheduling', there is an 'Online schedule' section with a table of scheduled times. The table has two rows: 'WEEKDAY(S)' with the time '17:00 - 21:00' and 'WEEKEND' with the time '16:00 - 22:00'. Each row has a green toggle switch and a trash icon. At the bottom, there is a 'More Config' dropdown and an 'Apply' button.

Schedule Type	Time Range	Status	Action
WEEKDAY(S)	17:00 - 21:00	On	Delete
WEEKEND	16:00 - 22:00	On	Delete

3.11.5 Sieć IoT

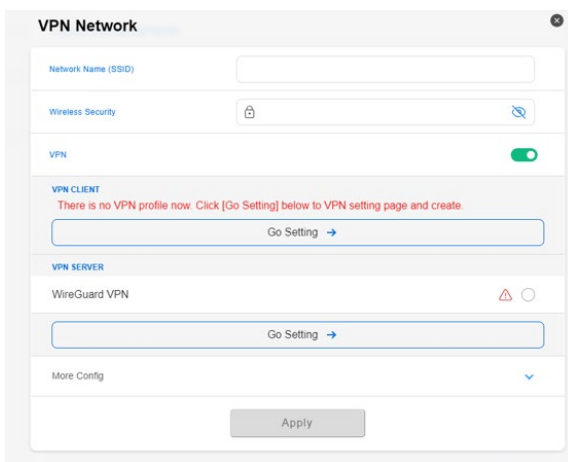
Umożliwia łatwe skonfigurowanie odrębnej sieci dla urządzeń IoT. Zalecana w przypadku urządzeń do monitoringu, asystentów głosowych, oświetlenia, wizjerów z kamerą, inteligentnych zamków elektronicznych i czujników..



The image shows a configuration window titled "IoT Network". It contains three input fields: "Network Name (SSID)", "Wireless Security" (with a lock icon and a visibility toggle), and "More Config" (with a dropdown arrow). An "Apply" button is located at the bottom.

3.11.6 Sieć VPN

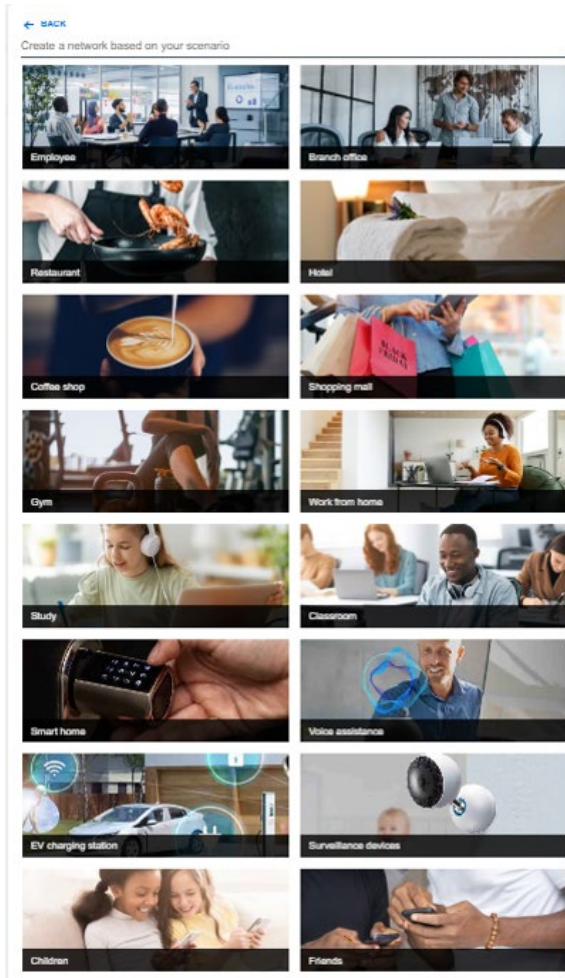
Umożliwia nawiązanie bezpiecznego połączenia internetowego przy użyciu VPN.



The image shows a configuration window titled "VPN Network". It contains several sections: "Network Name (SSID)", "Wireless Security", "VPN" (with a toggle switch), "VPN CLIENT" (with a red warning message and a "Go Setting" button), "VPN SERVER" (with a "WireGuard VPN" entry and a "Go Setting" button), and "More Config" (with a dropdown arrow). An "Apply" button is located at the bottom.

3.11.7 Eksplorator scenariuszy

W razie wątpliwości, którą sieć utworzyć, można wybrać zakres odpowiadający własnym preferencjom dotyczącym tworzonej sieci.



3.11.8 Sieć niestandardowa

Umożliwia wybranie opcji personalizacji sieci.

Customized Network

Network Name (SSID)

Wireless Security

More Config

Apply

3.12 System Log (Dziennik systemu)

W pozycji System Log (Dziennik systemu) znajduje się lista zarejestrowanych aktywności w sieci.

UWAGA: Po ponownym uruchomieniu lub wyłączeniu routera dziennik systemu jest resetowany.

W celu wyświetlenia dziennika systemu:

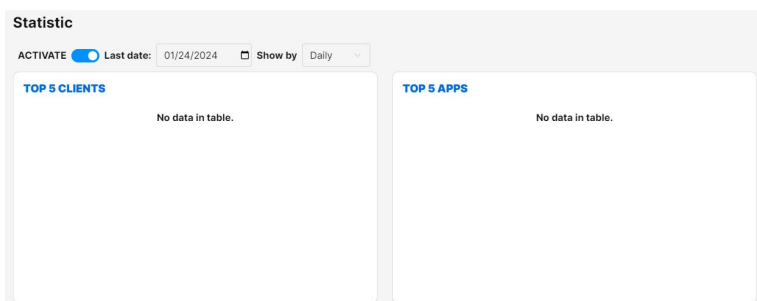
1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > System Log (Dziennik systemu)**.
2. Aktywności w sieci można sprawdzić na dowolnej z poniższych zakładek:
 - Dziennik ogólny
 - Dzierżawy DHCP
 - Przekierowanie portów
 - Tabela routingu
 - IPv6
 - Połączenia

3.13 Monitor ruchu

3.13.1 Analizator ruchu

Aby skorzystać z analizatora ruchu:

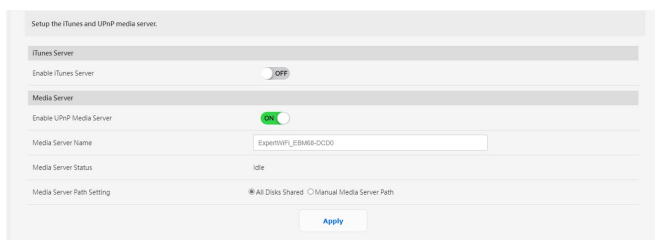
1. Włącz pozycję **ACTIVATE (AKTYWUJ)**.
2. Wybierz ostatnią datę do wyświetlenia, a z listy rozwijanej **Show by (Pokaż według)** wybierz monitorowanie ruchu sieciowego codziennie, co tydzień lub co miesiąc.
3. Wyświetlonych zostanie pięciu głównych klientów, pięć głównych aplikacji, urządzenia, status klienta i analiza aplikacji.



3.14 Aplikacja USB

3.14.1 Media Server (Serwer multimedialny)

Pozycja Media server (Serwer multimedialny) umożliwia skonfigurowanie serwera iTunes i UPnP.



W celu wyświetlenia strony ustawień Media Server (Serwer multimedialny) przejdź do pozycji **Settings (Ustawienia) > USB Application (Aplikacja USB) > Media Server (Serwer multimedialny)**.

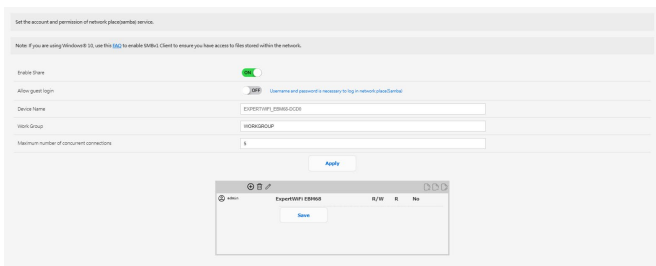
Należy zapoznać się z poniższymi opisami pól:

- **Enable iTunes Server (Włącz serwer iTunes):** Wybierz pozycję ON/OFF (WŁ./WYŁ.) w celu włączenia/wyłączenia serwera iTunes.
- **Enable UPnP Media Server (Włącz serwer multimedialny UPnP):** Wybierz pozycję ON/OFF (WŁ./WYŁ.) w celu włączenia/wyłączenia serwera multimedialny UPnP.
- **Media Server Name (Nazwa serwera multimedialny):** Wprowadzanie nazwy serwera multimedialny.
- **Media Server Path Setting (Ustawienia ścieżki serwera multimedialny):** Wybierz opcję **All Disks Shared (Wszystkie dyski zostały udostępnione)** lub **Manual Media Server Path (Ręczne ustawienia ścieżki serwera multimedialny)**.

Po zakończeniu kliknij **Apply (Zastosuj)**.

3.14.2 Udostępnianie miejsca sieciowego (Samba)

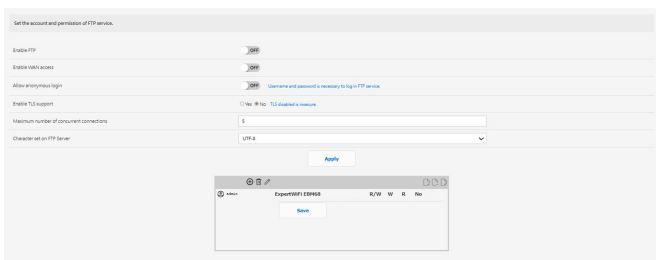
Udostępnianie miejsca sieciowego (Samba), umożliwia ustawienie konta i uprawnień dla usługi Samba.



Aby używać udostępniania Samba, kolejno do pozycji **Settings (Ustawienia) > USB application (Aplikacja USB) > Network Place (Samba) Share [Udostępnianie miejsca sieciowego (Samba)]**.

3.14.3 FTP Share (Udostępnianie FTP)

Pozycja FTP Share (Udostępnianie FTP) umożliwia skonfigurowanie kont i uprawnień dla usługi FTP.



Aby używać Udostępnianie FTP, kolejno do pozycji **Settings (Ustawienia) > USB Application (Aplikacja USB) > FTP Share (Udostępnianie FTP)**.

3.14.4 Serwer drukarki sieciowej

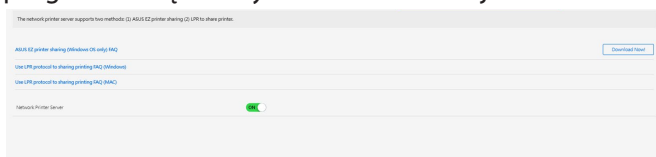
3.14.4.1 Udostępnianie drukarki ASUS EZ

Program narzędziowy ASUS EZ Printing Sharing umożliwia konfigurację serwera wydruku po podłączeniu drukarki USB do portu USB przewodowy router. Zapewnia to bezprzewodowe drukowanie i skanowanie plików przez klientów sieciowych.

UWAGA: Funkcja serwera wydruku jest obsługiwana w systemie Windows® 10 i Windows® 11.

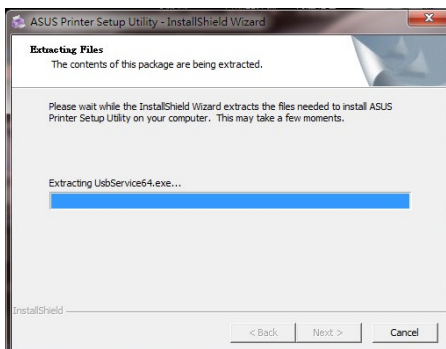
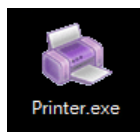
W celu skonfigurowania trybu udostępniania drukarki EZ:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia)** > **USB Application (Aplikacja USB)** > **Network Printer Server (Sieciowy serwer wydruku)**.
2. Kliknij pozycję **Download Now! (Pobierz teraz!)**, aby pobrać program narzędziowy drukarki sieciowej.

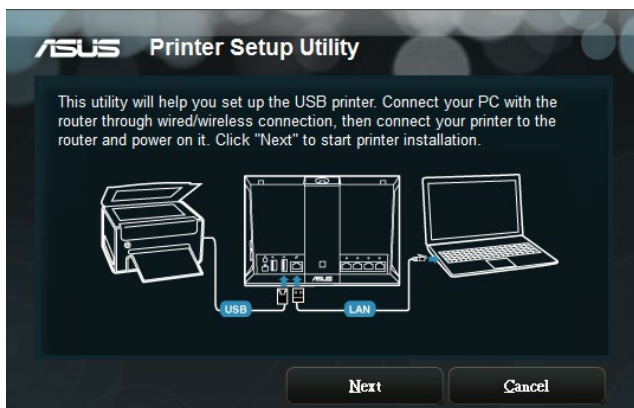


UWAGA: Program narzędziowy drukarki sieciowej jest obsługiwany tylko w systemie Windows® 10 i Windows® 11. Aby zainstalować program narzędziowy w systemie Mac OS, należy wybrać pozycję **Use LPR protocol for sharing printer (Udostępniaj drukarkę za pomocą protokołu LPR)**.

3. Rozpakuj pobrany plik i kliknij ikonę drukarki w celu uruchomienia programu ustawień drukarki sieciowej.



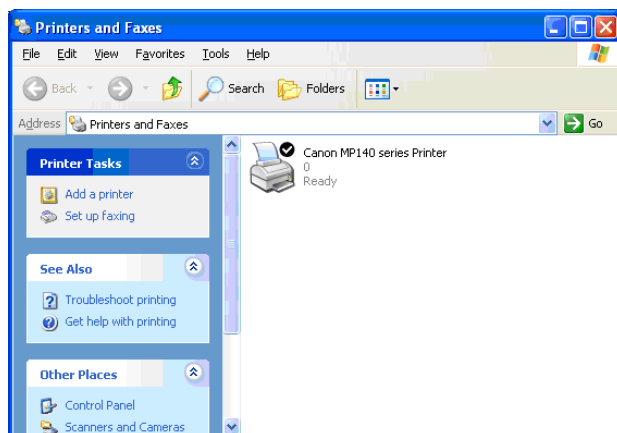
4. Wykonaj instrukcje ekranowe w celu przeprowadzenia ustawień sprzętu, a następnie kliknij **Next (Dalej)**.



5. Zaczekaj kilka minut na zakończenie początkowych ustawień. Kliknij **Next (Dalej)**.
6. Kliknij **Finish (Zakończ)** w celu dokończenia instalacji.
7. Wykonaj instrukcje systemu operacyjnego Windows® w celu instalacji sterownika drukarki.



8. Po zakończeniu instalacji sterownika drukarki klienci sieciowi będą mogli korzystać z drukarki.

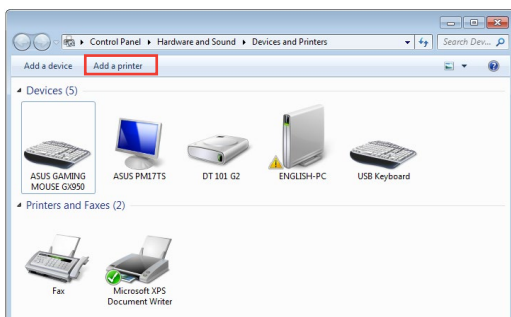


3.14.4.2 Udostępnianie drukarki za pomocą protokołu LPR

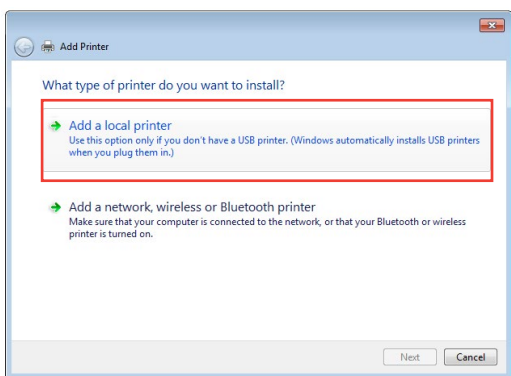
Za pomocą protokołu LPR/LPD (Line Printer Remote/Line Printer Daemon) drukarkę można udostępnić komputerom z systemem operacyjnym Windows® i MAC.

W celu udostępnienia drukarki LPR:

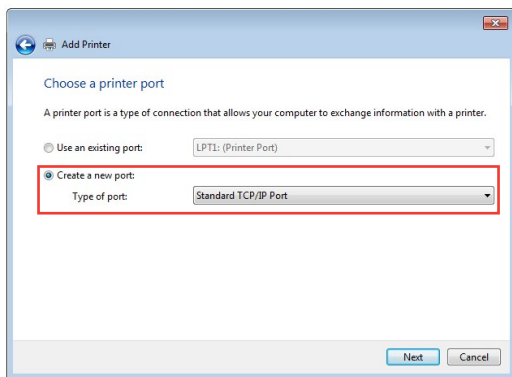
1. Na pulpicie systemu Windows® kliknij kolejno pozycje **Start > Devices and Printers (Urządzenia i drukarki) > Add a printer (Dodaj drukarkę)** w celu uruchomienia pozycji **Add Printer Wizard (Kreator dodawania drukarki)**.



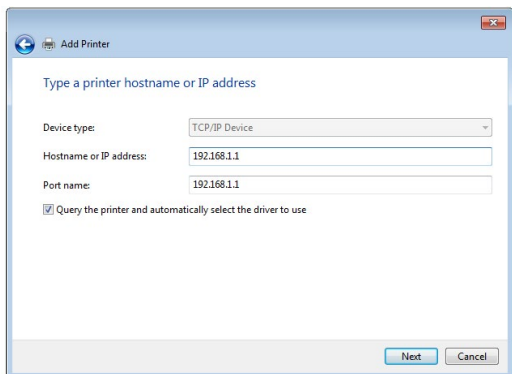
2. Wybierz pozycję **Add a local printer (Dodaj drukarkę lokalną)**, a następnie kliknij przycisk **Next (Dalej)**.



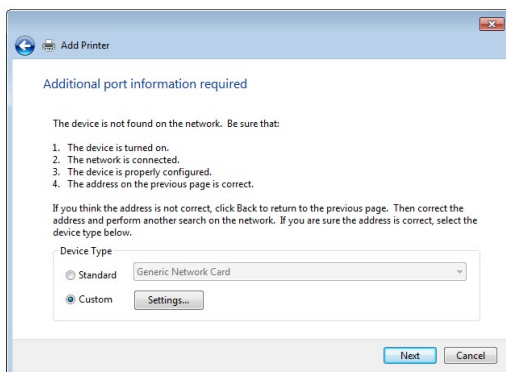
3. Zaznacz pozycję **Create a new port (Utwórz nowy port)**, a następnie ustaw dla pozycji **Type of Port (Typ portu)** opcję **Standard TCP/IP Port (Standardowy port TCP/IP)**. Kliknij przycisk **New Port (Nowy port)**.



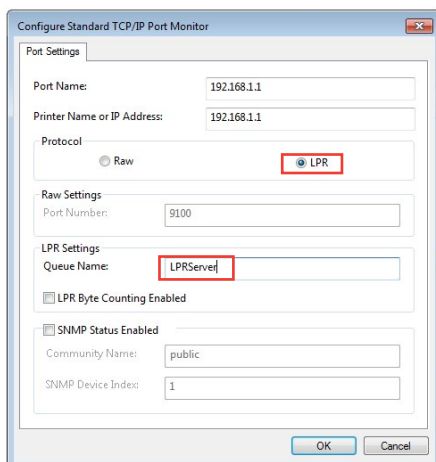
4. W polu **Hostname or IP address (Nazwa hosta drukarki lub adres IP)** wprowadź adres IP przewodowy router, a następnie kliknij przycisk **Next (Dalej)**.



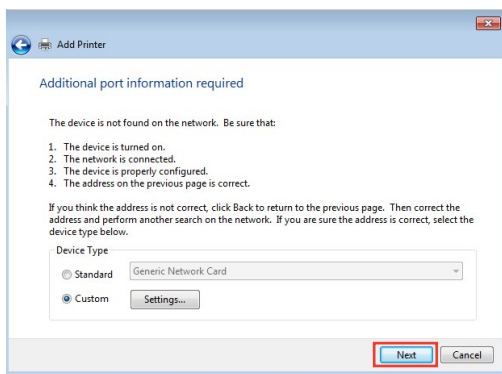
5. Zaznacz pozycję **Custom (Niestandardowy)**, a następnie kliknij przycisk **Settings (Ustawienia)**.



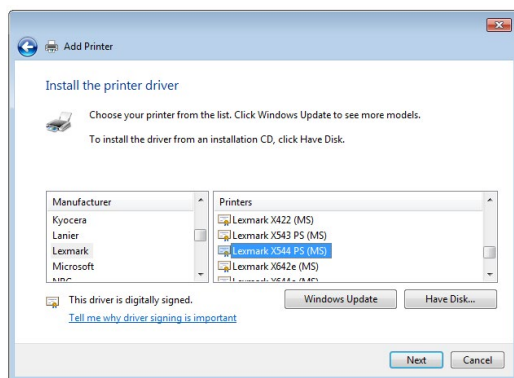
6. Ustaw dla pozycji **Protocol (Protokół)** opcję **LPR**. W polu **Queue Name (Nazwa kolejki)** wprowadź wartość **LPRServer (Serwer LPR)**, a następnie kliknij przycisk **OK**, aby kontynuować.



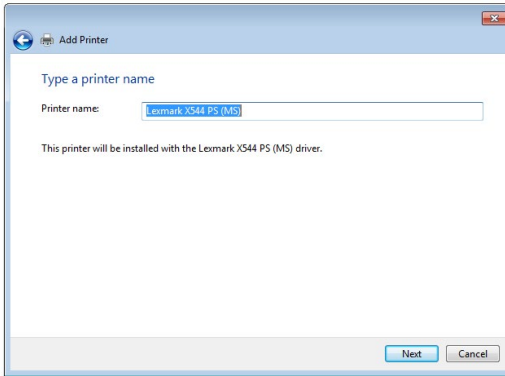
7. Kliknij przycisk **Next (Dalej)**, aby zakończyć konfigurację standardowego portu TCP/IP.



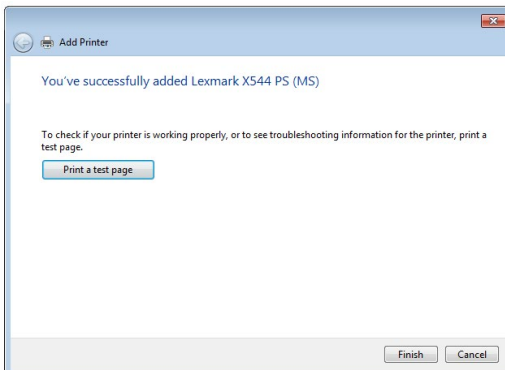
8. Zainstaluj sterownik drukarki podany na liście dostawców. Jeśli danej drukarki nie ma na liście, kliknij przycisk **Have Disk (Z dysku)**, aby ręcznie zainstalować sterowniki drukarki z dysku CD-ROM lub pliku.



9. Kliknij przycisk **Next (Dalej)**, aby zaakceptować domyślną nazwę drukarki.



10. Kliknij przycisk **Finish (Zakończ)**, aby zakończyć instalację.



3.14.5 Modem USB

Przełącz do trybu USB, aby móc korzystać z karty USB sieci bezprzewodowej 3G/4G lub telefonu Android jako modemu USB.

W celu korzystania z modemu USB przejdź do pozycji **Settings (Ustawienia) > USB Application (Aplikacja USB) > USB Modem (Modem USB)**.

Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem.

Basic Config

Enable USB Mode ☒

Select USB Device Auto

APN Configuration Auto

Telecommunications Standards 3GPP2, U.S./T.S. 1.14E

APN (Access Point Name) Internet

Dial Number 9999

Username

Password

Authentication None

PIN code

USB Adapter Auto

USB VDU 0

Special Requirement from USB

Extend the TTL value ☒ Yes ☐ No

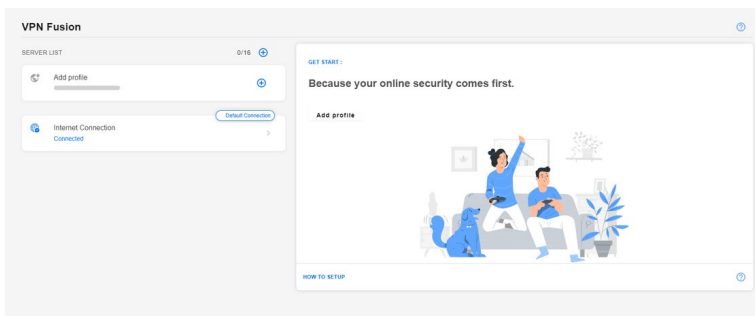
Specify USB TTL value ☐ Yes ☒ No

Apply

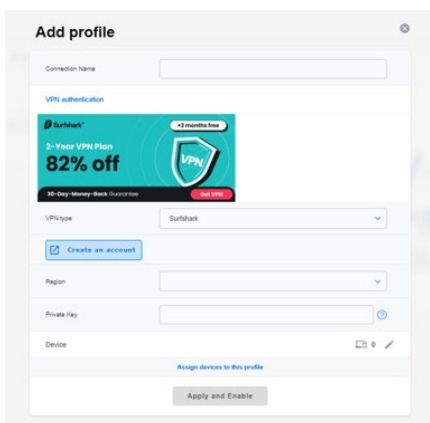
3.15 Połącz sieci VPN

3.15.1 Połączone sieci VPN

VPN Fusion umożliwia równoczesne połączenie wielu serwerów VPN i przypisanie urządzeń klienta w celu połączenia z różnymi tunelami VPN.

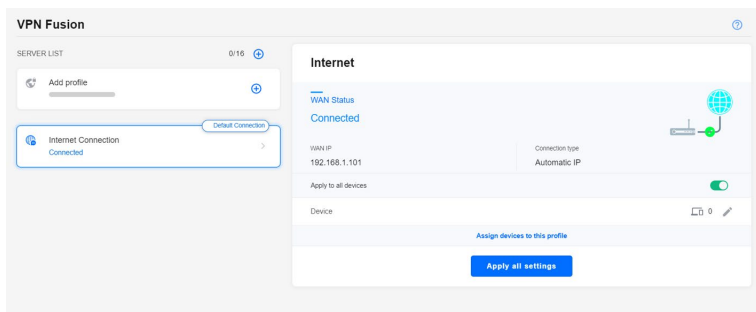


1. W panelu nawigacyjnym przejdź do pozycji **VPN Fusion (Połącz sieci VPN)**.
2. Kliknij **+** w polu **Add profile (Dodaj profil)**, aby skonfigurować nowy tunel sieci VPN.
3. Wprowadź ustawienia sieci VPN, takie jak nazwa połączenia, typ sieci VPN, region, klucz prywatny i urządzenie.
4. Kliknij przycisk **Apply and Enable (Zastosuj i włącz)**.



3.15.2 Internet Connection (Połączenie internetowe)

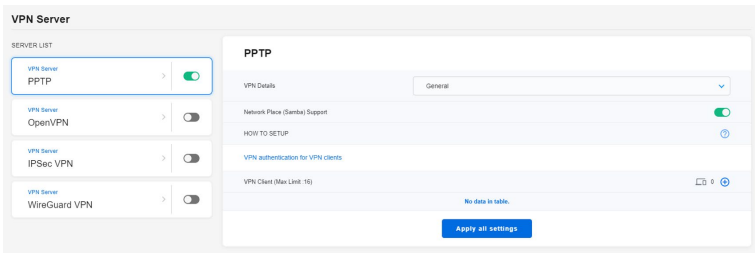
Umożliwia zarządzanie stanem sieci WAN połączonych urządzeń.



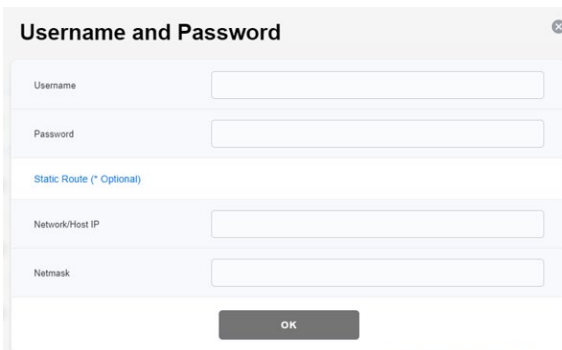
3.16 Serwer VPN

3.16.1 PPTP

1. W panelu nawigacyjnym przejdź do pozycji **VPN Server (Serwer VPN) > PPTP** i przesun suwak w prawo (domyślnie jest on ustawiony z lewej strony w pozycji wyłączenia).
2. W polu **VPN Client (Max Limit: 16) (Klient VPN (maks. 16))** kliknij  w celu dodania konta.



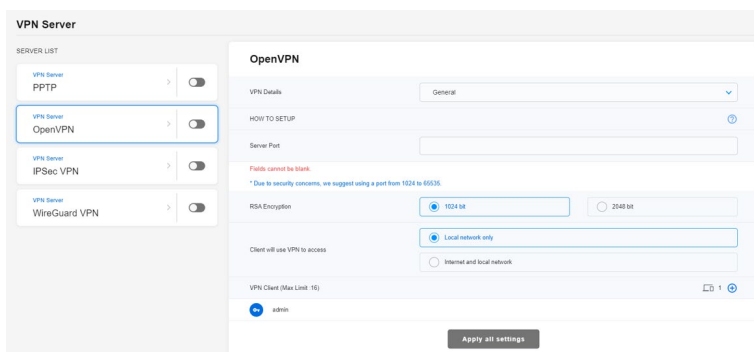
3. Wprowadź niestandardowe wartości w pozycji *[Username]* (*[Nazwa użytkownika]*) i *[Password]* (*[Hasło]*), a następnie kliknij przycisk **OK**.

The screenshot shows a dialog box titled 'Username and Password'. It contains four input fields: 'Username', 'Password', 'Static Route (* Optional)', and 'Network/Host IP'. Below these is a 'Netmask' input field. At the bottom center is an 'OK' button.

NOTE: Skonfigurowanych pozycji *[Username]* (*[Nazwa użytkownika]*) i *[Password]* (*[Hasło]*) nie będzie można zmienić. Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/114892/>.

3.16.2 OpenVPN

1. W panelu nawigacyjnym przejdź do pozycji **VPN Server (Serwer VPN) > OpenVPN** i przesunij suwak w prawo (domyślnie jest on ustawiony z lewej strony w pozycji wyłączenia).
2. Skonfiguruj ogólne ustawienia w polu **Szczegóły sieci VPN**.
3. W pustej kolumnie wprowadź nazwę użytkownika i hasło.
4. W polu **VPN Client (Max Limit: 16) (Klient VPN (maks. 16))** kliknij  w celu dodania konta.
5. Hasło zostanie automatycznie ukryte. Kliknij przycisk **Apply all settings (Zastosuj wszystkie ustawienia)**.



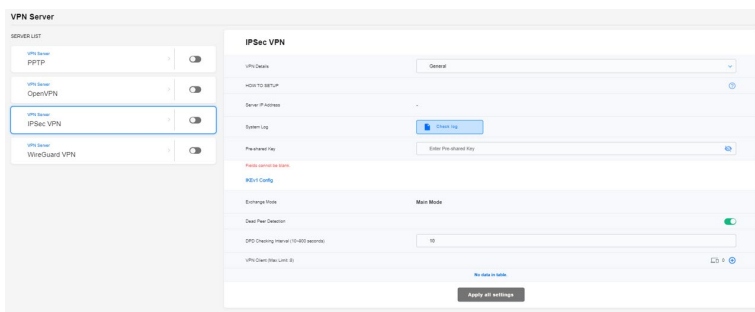
The screenshot shows the 'VPN Server' configuration page. On the left, under 'SERVER LIST', the 'OpenVPN' option is selected and its toggle switch is turned on. The main area is titled 'OpenVPN' and contains the following settings:

- VPN Details:** Set to 'General'.
- HOW TO SETUP:** A link with a question mark icon.
- Server Port:** An empty text field with a note: 'Ports cannot be blank. * Due to security concerns, we suggest using a port from 1024 to 65535.'
- RSA Encryption:** Two radio buttons: '1024 bit' (selected) and '2048 bit'.
- Client will use VPN to access:** Two radio buttons: 'Local network only' (selected) and 'Internet and local network'.
- VPN Client (Max Limit: 16):** A list with one entry 'admin' and a plus icon to add more.
- Apply all settings:** A button at the bottom right.

UWAGA: Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/1008713/>.

3.16.3 IPSec VPN

1. W panelu nawigacyjnym przejdź do pozycji **VPN Server (Serwer VPN) > IPSec VPN** i przesun suwak w prawo (domyślnie jest on ustawiony z lewej strony w pozycji wyłączenia).
2. Wprowadź klucz w polu **Wstępnie współdzielony klucz**.
3. W polu **VPN Client (Max Limit: 8) (Klient VPN (maks. 8))** kliknij **+** w celu dodania konta.
5. Wprowadź niestandardowe wartości w pozycji *[Username]* (*[Nazwa użytkownika]*) i *[Password]* (*[Hasło]*), a następnie kliknij przycisk Zastosuj wszystkie ustawienia.

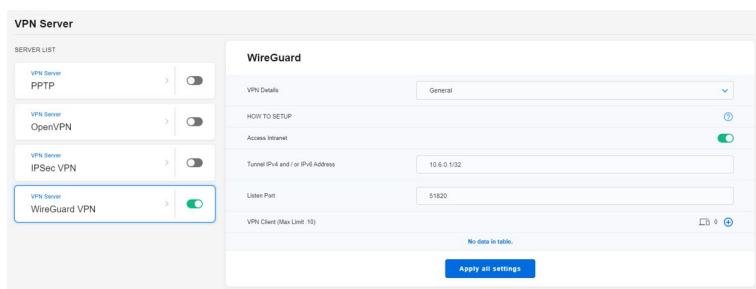


NOTE: Skonfigurowanych pozycji *[Username]* (*[Nazwa użytkownika]*) i *[Password]* (*[Hasło]*) nie będzie można zmienić. Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/1044190/>.

3.16.4 WireGuard® VPN

1. W panelu nawigacyjnym przejdź do pozycji **VPN Server (Serwer VPN) > WireGuard VPN**.
2. W polu **VPN Client (Max Limit: 10) (Klient VPN (maks. 10))** kliknij ⊕ w celu dodania konta. W przypadku urządzeń ogólnych, takich jak laptopy lub smartfony, kliknij przycisk **Apply (Zastosuj)**.
3. Kliknij przycisk **Zastosuj wszystkie ustawienia**, aby włączyć sieć WireGuard® VPN.
4. Kliknij "...” w celu uzyskania szczegółowych informacji.

UWAGA: Jeśli do łączenia z siecią WireGuard® VPN używany jest smartfon, pobierz aplikację WireGuard® ze sklepu Google Play lub App Store, a następnie zeskanuj kod w aplikacji w celu pobrania pliku konfiguracji.



UWAGA: Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/1048280/>.

3.17 WAN (Sieć WAN)

3.17.1 Internet Connection (Połączenie internetowe)

Na ekranie Internet Connection (Połączenie internetowe) można skonfigurować ustawienia różnego typu połączeń WAN.

ExpertWIFI EBM68 supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Add Profile

WAN Index

WAN Type: WAN

Internet Settings

Profile: Internet

WAN Connection Type: Automatic IP

Enable WAN: ☒ Yes ☐ No

Enable NAT: ☒ Yes ☐ No

Enable L2TP: ☒ Yes ☐ No

802.1Q

Enable: ☐ Yes ☒ No

VLAN ID: 0 (2 - 4094)

W celu skonfigurowania ustawień połączenia WAN:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > Internet Connection (Połączenie internetowe)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **WAN Connection Type (Typ połączenia WAN):** Wybierz typ połączenia udostępniany przez usługodawcę internetowego. Dostępne opcje to **Automatic IP (Automatyczny adres IP)**, **PPPoE**, **PPTP**, **L2TP** lub **static IP (statyczny IP)**. W przypadku braku pewności co do typu połączenia WAN lub braku możliwości uzyskania przez router prawidłowego adresu IP należy skontaktować się z usługodawcą internetowym.
 - **Enable WAN (Włącz sieć WAN):** Wybierz opcję **Yes (Tak)**, aby router mógł uzyskać dostęp do Internetu. Wybierz opcję **No (Nie)**, aby wyłączyć dostęp do Internetu.
 - **Enable NAT (Włącz NAT):** Translator adresów sieciowych NAT (Network Address Translation) to system, w którym jeden publiczny adres IP (adres IP sieci WAN) jest używany do zapewniania dostępu do Internetu klientom sieciowym o prywatnym adresie IP w sieci LAN. Prywatny adres IP każdego klienta sieciowego jest zapisywany w tabeli NAT i używany do rozsyłania przychodzących pakietów danych.

- **Enable UPnP (Włącz UPnP):** Protokół UPnP (Universal Plug and Play) umożliwia sterowanie kilkoma urządzeniami (takimi jak routery, telewizory, zestawy stereo, konsole do gier i telefony komórkowe) w sieci z obsługą adresów IP ze sterowaniem centralnym za pomocą bramy lub bez niego. Protokół UPnP łączy komputery o dowolnym współczynniku postaci, zapewniając bezproblemowe połączenie sieciowe do konfiguracji zdalnej i przesyłania danych. Podczas korzystania z protokołu UPnP nowe urządzenie sieciowe jest wykrywane automatycznie. Po połączeniu z siecią urządzenia można skonfigurować zdalnie w celu zapewnienia obsługi aplikacji P2P, gier interaktywnych, konferencji wideo oraz serwerów sieci Web lub proxy. W przeciwieństwie do przekierowania portów, które wymaga ręcznej konfiguracji ustawień portów, protokół UPnP automatycznie konfiguruje router w celu zapewnienia przyjmowania połączeń przychodzących i bezpośrednich żądań do określonego komputera w sieci lokalnej.
- **Connect to DNS Server (Łączenie z serwerem DNS):** Umożliwia automatyczne uzyskiwanie adresu IP serwera DNS przez router od usługodawcy internetowego. DNS to host w Internecie, który tłumaczy nazwy internetowe na numeryczne adresy IP.
- **Authentication (Uwierzytelnianie):** Ta pozycja może być określana przez niektórych usługodawców internetowych. Jeśli to konieczne, sprawdź u usługodawcy internetowego i wprowadź.
- **Host Name (Nazwa hosta):** W tym polu można wprowadzić nazwę hosta danego routera. Jest to zwykle specjalny wymóg usługodawcy internetowego. Jeśli usługodawca internetowy przypisał nazwę hosta do komputera, wprowadź ją w tym polu.
- **MAC Address (Adres MAC):** Pozycja MAC (Media Access Control) address (Adres MAC) to unikatowy identyfikator urządzenia sieciowego. Niektórzy usługodawcy internetowi monitorują adresy MAC urządzeń sieciowych, które łączą się z ich usługą i odrzucają wszelkie próby połączeń urządzeń nierozpoznanych. Aby uniknąć problemów z połączeniami spowodowanych niezarejestrowanym adresem MAC, można:
 - Skontaktować się z usługodawcą internetowym i zaktualizować adres MAC skojarzony z jego usługą.
 - Sklonować lub zmienić adres MAC przewodowy router firmy ASUS w celu jego dopasowania do adresu MAC poprzedniego urządzenia sieciowego rozpoznawanego przez usługodawcę internetowego.

3.17.2 Wiele sieci WAN

Pozycja Multi-WAN (Wiele sieci WAN) umożliwia wybranie wielu połączeń ISP z routerem i grupami WAN zarówno dla podstawowej, jak i dodatkowej sieci WAN.

Aby skonfigurować pozycję Multi-WAN (Wiele sieci WAN):

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > Multi-WAN (Wiele sieci WAN)**.
2. Włącz pozycję **Enable Multi-WAN (Włącz wiele sieci WAN)**.
3. Wybierz sieć w pozycji **Primary WAN (Podstawowa sieć WAN)** i **Secondary WAN (Dodatkowa sieć WAN)**. Dostępne opcje to WAN, USB, Ethernet LAN.
4. Wybierz pozycję **Fail Over (Praca awaryjna)** lub **Time (Czas)**.

Fail Over (Praca awaryjna): Druga sieć WAN pełni funkcję zapasowego dostępu do sieci.

Time (Czas): Ustaw czas planowania reguł wielu sieci WAN.

5. Wybierz **Active Backup WAN when any primary WAN port failed (Aktywne zapasowe łącze WAN w przypadku awarii dowolnego portu podstawowej sieci WAN)** lub **Active Backup WAN when all primary WAN port failed (Aktywne zapasowe łącze WAN w przypadku awarii wszystkich portów podstawowej sieci WAN)**.

The screenshot shows the 'Multi-WAN' configuration page. At the top, there is a toggle switch labeled 'Enable Multi-WAN' which is turned on. Below this, the 'Group Settings' section contains two columns. The left column is for 'Primary WAN' and has a dropdown menu currently showing 'WAN 1' with an 'Add Port' link below it. The right column is for 'Secondary WAN' and has an 'Add Port' link. The 'Set policy with Multi-WAN' section at the bottom has two parts: 'Mode' with radio buttons for 'Fail Over' (selected) and 'Time', and 'Policy' with radio buttons for 'Active Backup WAN when any primary WAN port failed.' (selected) and 'Active Backup WAN when all primary WAN port failed.'

6. Włącz lub wyłącz pozycję **Allow failback (Włącz powrót)**.
7. Określ interwał wykrywania.
8. Określ liczbę ciągłych awarii, po których bieżąca sieć WAN zostanie uznana za rozłączoną.
9. Określ liczbę ciągłych wykryć, że podstawowa sieć WAN ma aktywne połączenie internetowe za pośrednictwem fizycznego kabla, co powoduje powrót po awarii do podstawowej sieci WAN.
10. Wybierz pozycję **DNS Query (Zapytanie DNS)** lub **Ping**.
11. Kliknij przycisk **Apply all settings (Zastosuj wszystkie ustawienia)**.

Allow failback ☒

Per-Port Settings

WAN 1

Detect Interval	Every 3 seconds
Internet Connection Diagnosis	When the current WAN fails 2 continuous times, it is deemed a disconnection.
Failback Trigger Condition	When the Primary WAN is detected to have an active internet connection using a physical cable for 4 continuous times, failback to the Primary WAN.
Network Monitoring	☐ DNS Query ☐ Ping

Apply all settings

UWAGA: Szczegółowe wyjaśnienia są dostępne w witrynie pomocy technicznej firmy ASUS w sekcji FAQ <https://www.asus.com/support/FAQ/1011719>.

3.17.3 Port Trigger (Wyzwalanie portów)

Funkcja Port Trigger (Wyzwalanie portów) umożliwia tymczasowe włączenie portów danych, gdy urządzenia sieci LAN wymagają nieograniczonego dostępu do Internetu. Dostępne są dwie metody otwierania portów danych przychodzących: przekierowanie portów i wyzwalanie portów.

- Przekierowanie portów sprawia, że określone porty danych są stale otwarte, a urządzenia muszą używać statycznych adresów IP.
- Wyzwalanie portów otwiera port przychodzący tylko wtedy, gdy urządzenie w sieci LAN zażąda dostępu do wyzwalanego portu.

Inaczej niż to jest w przypadku przekierowania portów, wyzwalanie portów nie wymaga statycznych adresów IP urządzeń w sieci LAN. Przekierowanie portów umożliwia współdzielenie jednego otwartego portu przez wiele urządzeń, w przypadku wyzwalania portów natomiast do otwartego portu w danym momencie może mieć dostęp tylko jeden klient.

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.

[Port Trigger FAQ](#)

Basic Config

Enable Port Trigger: ☒ Yes ☐ No

Well-Known Applications:

Trigger Port List (Max Limit: 32)

Description	Trigger Port	Protocol	Incoming Port	Protocol	Date
No data in table.					

[Apply](#)

W celu skonfigurowania pozycji Port Trigger (Wyzwalanie portów):

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > Port Trigger (Wyzwalanie portów)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Enable Port Trigger (Włącz wyzwalanie portów):** Wybierz opcję **Yes (Tak)**, aby włączyć funkcję Port Trigger (Wyzwalanie portów).
 - **Well-Known Applications (Dobrze znane aplikacje):** Wybierz popularne gry i usługi sieci Web w celu ich dodania do pozycji Port Trigger List (Lista portów wyzwalania).

- **Opis:** Wprowadź krótką nazwę lub opis usługi.
- **Port wyzwala:** Określ port wyzwalający otwarcie portu przychodzącego.
- **Protokół:** Wybierz protokół TCP lub UDP.
- **Port przychodzący:** Określ port przychodzący do odbierania danych przychodzących z Internetu.

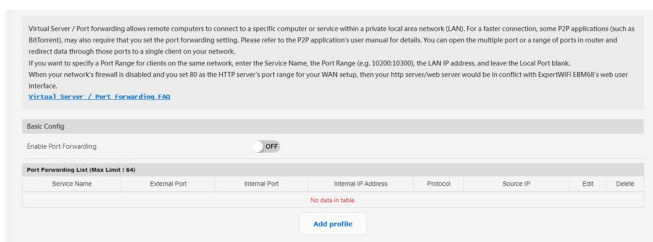
UWAGI:

- Podczas łączenia z serwerem IRC komputer kliencki nawiązuje połączenie wychodzące zgodnie z zakresem portu wyzwala 66660–7000. Serwer IRC odpowiada poprzez weryfikację nazwy użytkownika i nawiązanie nowego połączenia z komputerem klienckim przez port przychodzący.
 - Jeśli funkcja Port Trigger (Wyzwalanie portów) jest wyłączona, router odrzuca połączenia, ponieważ nie może określić, który komputer zgłasza żądanie dostępu do serwera IRC. Po włączeniu funkcji Port Trigger (Wyzwalanie portów) router przypisze port przychodzący do odbierania danych przychodzących. Ten port przychodzący zamknie się po upływie określonego czasu z powodu braku możliwości określenia przez router czasu wyłączenia aplikacji.
 - Funkcja wyzwala portów umożliwia korzystanie z określonej usługi i konkretnego portu przychodzącego w danym czasie tylko przez jednego klienta w sieci.
 - Do jednoczesnego wyzwolenia portu w więcej niż jednym komputerze nie można używać tej samej aplikacji. Router przekieruje port z powrotem do ostatniego komputera w celu wysłania żądania/pakietu wyzwala do routera.
 - Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/114110>.
-

3.17.4 Virtual Server/Port Forwarding (Serwer wirtualny/Przekierowanie portów)

Funkcja Virtual Server / Port forwarding (Serwer wirtualny/przekierowanie portów) umożliwia łączenie się komputerów zdalnych z określonym komputerem lub usługą w prywatnej sieci lokalnej (LAN). W celu zapewnienia szybszego połączenia niektóre aplikacje P2P (takie jak BitTorrent) również mogą wymagać skonfigurowania przekierowania portów. W celu uzyskania szczegółowych informacji należy zapoznać się z instrukcją obsługi aplikacji P2P. Można otworzyć wiele portów lub zakres portów w routerze i przekierowywać przez nie dane do jednego klienta w sieci. Aby określić zakres portów dla klientów w tej samej sieci, wypełnij pozycje Service Name (Nazwa usługi), Port Range (Zakres portów) (np. 10200:10300) i LAN IP address (Adres IP sieci LAN), a pozycję Local Port (Port lokalny) pozostaw pustą.

UWAGA: Po włączeniu przekierowania portów router firmy ASUS blokuje niechciany ruch przychodzący z Internetu i zezwala wyłącznie na odpowiedzi na żądania wychodzące z sieci LAN. Klient sieciowy nie ma bezpośredniego dostępu do Internetu i odwrotnie.



W celu skonfigurowania pozycji Port Forwarding (Przekierowanie portów):

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > Virtual Server / Port Forwarding (Serwer wirtualny/Przekierowanie portów)**.
2. Przesuń suwak do opcji **ON (WŁ.)**, aby włączyć funkcję Port Forwarding (Przekierowanie portów), a następnie kliknij przycisk **Add Profile (Dodaj profil)**. Po skonfigurowaniu poniższych ustawień kliknij przycisk **OK**.

Quick Select

Famous Server List

Please select

Famous Game List

Please select

Custom Configuration

Service Name

* Optional

Protocol

TCP

External Port

Internal Port

* Optional

Internal IP Address

Source IP

* Optional

* External Port

The External Port accepts the following formats

1. Port ranges using a colon ":" between the starting and ending port, such as 300:350.

2. Single ports using a comma "," between individual ports, such as 566, 789.

3. A Mix of port ranges and single ports, using colons ":" and commas "," such as 1015:1024, 3021.

* Source IP

If you want to open your port to a specific IP address from the internet, input the IP address you want to specify in the Source IP field.

Cancel

OK

- **Famous Server List (Lista znanych serwerów):** Określ typ usługi, do której chcesz uzyskiwać dostęp.
- **Famous Game List (Lista znanych gier):** Pozycja ta zawiera listę portów wymaganych do prawidłowego działania popularnych gier online.
- **Service Name (Nazwa usługi):** Wprowadź nazwę usługi.
- **Protocol (Protokół):** Wybierz protokół. W przypadku braku pewności wybierz opcję **BOTH (OBA)**.
- **External Port (Port zewnętrzny):** Akceptowane są następujące formaty:
 - 1) Zakres portów z dwukropkiem ":" po środku w celu określenia górnej i dolnej granicy zakresu, np. 300:350;
 - 2) Numery poszczególnych portów oddzielone przecinkami ",", np. 566, 789;;
 - 3) Kombinacja zakresów i poszczególnych portów z użyciem dwukropków ":" i przecinków ",", np. 1015:1024, 3021.
- **Internal Port (Port wewnętrzny):** Wprowadź określony port do odbierania przekierowanych pakietów. Pozostaw to pole puste, jeśli chcesz, aby pakiety przychodzące były przekierowywane na określony zakres portu.

- **Internal IP Address (Wewnętrzny adres IP):** Wprowadź adres IP sieci LAN klienta.
- **Source IP (Adres IP źródła):** Aby otworzyć port dla określonego adresu IP z Internetu, należy w tym polu wprowadzić żądany adres IP, aby zapewnić do niego dostęp.

UWAGA: W celu zapewnienia prawidłowego działania funkcji przekierowania portów należy wprowadzić statyczny adres IP klienta lokalnego. Informacje na ten temat znajdują się w części **3.9 LAN (Sieć LAN)**.

W celu sprawdzenia, czy funkcja Port Forwarding (Przekierowanie portów) została pomyślnie skonfigurowana:

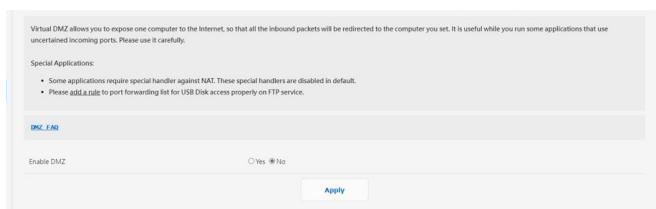
- Upewnij się, że serwer lub aplikacja są skonfigurowane i uruchomione.
- Konieczny będzie klient spoza sieci LAN, ale posiadający dostęp do Internetu (nazywany „klientem internetowym”). Klient ten nie powinien być połączony z routerem firmy ASUS.
- W kliencie internetowym wprowadź adres IP sieci WAN routera w celu zapewnienia dostępu do serwera. Jeśli przekierowanie portów zostało wykonane pomyślnie, dostęp do plików lub aplikacji zostanie zapewniony.

Różnice między wyzwalaniem portów a przekierowaniem portów:

- Wyzwalanie portów działa nawet bez skonfigurowania określonego adresu IP sieci LAN. W przeciwieństwie do przekierowania portów, które wymaga statycznego adresu IP sieci LAN, wyzwalanie portów umożliwia dynamiczne przekierowanie portów przy użyciu routera. Wstępnie określone zakresy portów są konfigurowane w celu przyjmowania połączeń przychodzących w ograniczonym czasie. W przypadku wyzwalania portów na wielu komputerach mogą być uruchomione aplikacje, które normalnie wymagałyby ręcznego przekierowania tych samych portów do każdego komputera w sieci.
- Wyzwalanie portów jest bezpieczniejsze niż przekierowanie portów, ponieważ porty przychodzące nie są zawsze otwarte. Są one otwarte tylko wtedy, gdy aplikacja nawiązuje połączenie wychodzące przez port wyzwalania.

3.17.5 DMZ (Strefa DMZ)

Funkcja Virtual DMZ (Wirtualna strefa DMZ) umożliwia uwidocznienie jednego komputera w Internecie, do którego przekierowywane będą wszystkie pakiety przychodzące. Jest to przydatne podczas używania aplikacji, które korzystają z nieokreślonych portów przychodzących. Funkcji tej należy używać z rozważą.



W celu skonfigurowania strefy DMZ:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > DMZ (Strefa DMZ)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **IP address of Exposed Station (Adres IP uwidocznionej stacji):** Wprowadź adres IP sieci LAN klienta, który będzie obsługiwał usługę strefy DMZ i będzie miał dostęp do Internetu. Klient serwera musi mieć statyczny adres IP.

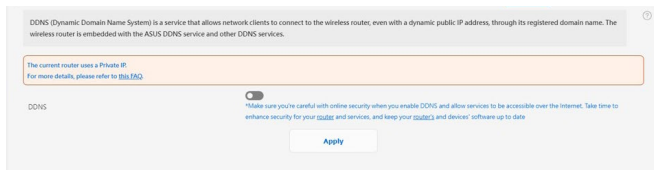
W celu usunięcia strefy DMZ:

1. Usuń adres IP sieci LAN klienta z pola tekstowego **IP Address of Exposed Station (Adres IP uwidocznionej stacji)**.
2. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

UWAGA: Aby uzyskać więcej informacji, odwiedź <https://www.asus.com/support/FAQ/1011723>.

3.17.6 DDNS (Usługa DDNS)

DDNS (ang. Dynamic Domain Name System) to usługa, która umożliwia łączenie się klientów sieciowych z przewodowy router za pomocą zarejestrowanej nazwy domeny, nawet w przypadku dynamicznych publicznych adresów IP. Przewodowy router ma wbudowaną usługę ASUS DDNS i inne usługi DDNS.



W celu skonfigurowania usługi DDNS:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > DDNS (Usługa DDNS)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Enable the DDNS Client (Włącz klienta usługi DDNS):** Włącz usługę DDNS w celu zapewnienia dostępu do routera firmy ASUS za pomocą nazwy DNS, a nie adresu IP sieci WAN.
 - **Server and Host Name (Nazwa serwera i hosta):** Wybierz usługę ASUS DDNS lub inną usługę DDNS. Aby korzystać z usługi ASUS DDNS, w pozycji Host Name (Nazwa hosta) wprowadź wartość w formacie xxx.asuscomm.com (xxx to nazwa hosta).
 - Aby korzystać z innej usługi DDNS, kliknij pozycję FREE TRIAL (BEZPŁATNA WERSJA PRÓBNA) i zarejestruj się w trybie online. Uzupełnij pola User Name or E-mail Address (Nazwa użytkownika lub adres e-mail) i Password or DDNS key (Hasło lub klucz DDNS).
 - **Enable wildcard (Włącz symbole wieloznaczne):** Włącz obsługę symboli wieloznacznych, jeśli jest to wymagane przez usługę DDNS.

UWAGI:

Usługa DDNS nie będzie działać w poniższych przypadkach:

- Przewodowy router korzysta z prywatnego adresu IP sieci WAN (192.168.x.x, 10.x.x.x lub 172.16.x.x), na co wskazuje tekst w kolorze żółtym.
- Router może być w sieci, która korzysta z wielu tabel NAT.

3.17.7 NAT Passthrough (Przekazywanie NAT)

Włączenie funkcji NAT Passthrough umożliwia przekazywanie połączeń wirtualnej sieci prywatnej (VPN) przez router do klientów sieciowych.

Aby skonfigurować funkcję NAT Passthrough, przejdź do pozycji **Settings (Ustawienia) > WAN (Sieć WAN) > NAT Passthrough (Przekazywanie NAT)**. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

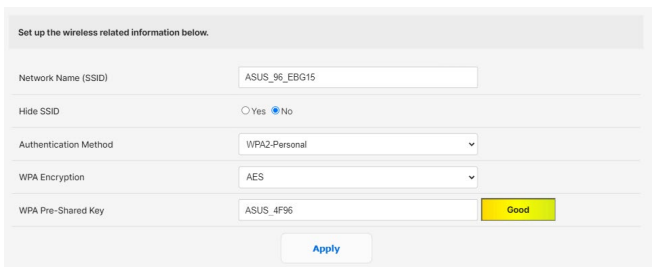
PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP ALG port	2021

Apply

3.18 Wireless (Sieć bezprzewodowa)

3.18.1 General (Ogólne)

Zakładka **General (Ogólne)** umożliwia konfigurację podstawowych ustawień sieci bezprzewodowej.



W celu skonfigurowania podstawowych ustawień sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Wireless (Sieć bezprzewodowa) > General (Ogólne)**.
2. Wprowadź unikatowy identyfikator SSID (ang. Service Set Identifier) lub nazwę sieci w celu identyfikacji sieci bezprzewodowej. Urządzenia Wi-Fi będą identyfikować sieć bezprzewodową i łączyć się z nią za pomocą przypisanego identyfikatora SSID. Identyfikatory SSID widoczne na pasku informacyjnym są aktualizowane po zapisaniu nowych identyfikatorów SSID w ustawieniach.

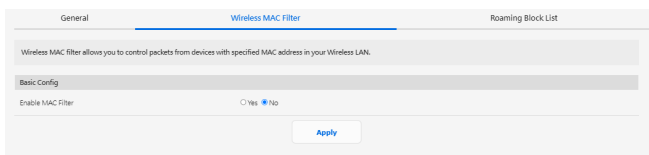
WAŻNE! Aby udostępnić funkcję Wi-Fi, należy z siecią AiMesh routera EBG15 zintegrować bezprzewodowy punkt dostępowy (AP), taki jak ExpertWiFi EBA63 lub router, taki jak ExpertWiFi EBR63 lub ExpertWiFi EBM68.

3. W polu **Hide SSID (Ukryj SSID)** wybierz opcję **Yes (Tak)**, aby nie dopuścić do wykrywania identyfikatora SSID przez urządzenia bezprzewodowe. Po włączeniu tej funkcji konieczne będzie ręczne wprowadzanie identyfikatora SSID w urządzeniu bezprzewodowym w celu zapewnienia jego dostępu do sieci bezprzewodowej.
4. Wybierz jedną z dostępnych metod uwierzytelniania:
 - **Open System (Otwarty system):** Ta opcja nie zapewnia zabezpieczeń.

- **WPA/WPA2/WPA3-Personal (WPA/WPA2/WPA3 -Personal):** Ta opcja zapewnia mocne zabezpieczenia. Można korzystać z zabezpieczenia WPA (z TKIP) lub WPA2 (z AES). Po wybraniu tej opcji konieczne jest korzystanie z szyfrowania TKIP + AES i wprowadzenie hasła WPA (klucza sieciowego).
 - **WPA/WPA2/WPA3-Enterprise (WPA/WPA2/WPA3-Enterprise):** Ta opcja zapewnia bardzo mocne zabezpieczenia. Jest ona dostępna z zintegrowanym serwerem EAP lub zewnętrznym serwerem uwierzytelniania RADIUS z wewnętrzną bazą danych.
5. Przypisz unikatowe hasło do wstępnie współdzielonego klucza WPA.

3.18.2 Filtr adresów MAC urządzeń bezprzewodowych

Pozycja Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych) zapewnia kontrolę nad pakietami przesyłanymi na określony adres MAC (Media Access Control) w danej sieci bezprzewodowej.



W celu skonfigurowania filtra adresów MAC urządzeń bezprzewodowych:

1. W panelu nawigacji przejdź do pozycji **Settings (Ustawienia) > Wireless (Sieć bezprzewodowa) > Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych)**.
2. Zaznacz opcję **Yes (Tak)** w polu **Enable Mac Filter (Włącz filtr adresów MAC)**.
3. Z listy rozwijanej **MAC Filter Mode (Tryb filtra adresów MAC)** wybierz opcję **Accept (Akceptuj)** lub **Reject (Odrzuć)**.
 - Wybierz opcję **Accept (Akceptuj)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) mogły łączyć się z siecią bezprzewodową.

- Wybierz opcję **Reject (Odrzuć)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) nie mogły łączyć się z siecią bezprzewodową.
4. W obszarze MAC filter list (Lista filtrowanych adresów MAC) kliknij przycisk **Add (Dodaj)**  i wprowadź adres MAC urządzenia bezprzewodowego.
 5. Kliknij przycisk **Apply (Zastosuj)**.

3.18.3 Lista blokady roamingu

Funkcja ta umożliwia dodawanie urządzeń do listy blokady roamingu, aby uniemożliwić im roaming między węzłami AiMesh.

You can add devices into roaming deny list, and the devices will not be roamed between AiMesh nodes.

Basic Config

Enable roaming deny list ☒ Yes ☐ No

Roaming Deny List (Max Limit : 64)

Client Name (MAC Address)	Add / Delete
ex. 08:00:20:12:34:56	
No data in table.	

[Apply](#)

4 Rozwiązywanie problemów

W rozdziale tym omówiono rozwiązania problemów, które mogą wystąpić podczas korzystania z routera. W przypadku pojawienia się problemów, których nie opisano w tym rozdziale, należy przejść do witryny pomocy technicznej firmy ASUS dostępnej pod adresem: <https://www.asus.com/support/> w celu uzyskania dalszych informacji o produkcie oraz szczegółowych danych kontaktowych działu pomocy technicznej firmy ASUS.

4.1 Rozwiązywanie podstawowych problemów

W przypadku wystąpienia problemu z routerem należy najpierw wykonać podstawowe czynności opisane w poniższej części, a dopiero potem poszukać innych rozwiązań.

Uaktualnij oprogramowanie sprzętowe do najnowszej wersji.

1. Uruchom sieciowy interfejs graficzny. Przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**. Kliknij przycisk **Check (Sprawdź)** w celu sprawdzenia dostępności najnowszej wersji oprogramowania sprzętowego.
2. Jeśli najnowsza wersja oprogramowania sprzętowego będzie dostępna, przejdź do witryny globalnej firmy ASUS i pobierz najnowszą wersję oprogramowania sprzętowego.
3. Na stronie **Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)** kliknij przycisk **Browse (Przeglądaj)**, aby zlokalizować plik oprogramowania sprzętowego.
4. Kliknij przycisk **Upload (Załaduj)**, aby uaktualnić oprogramowanie sprzętowe. Uruchom ponownie sieć, wykonując czynności w następującej kolejności:

1. Wyłącz modem.
2. Odłącz modem od zasilania.
3. Wyłącz router i komputery.
4. Podłącz modem do zasilania.
5. Włącz modem i odczekaj 2 minuty.
6. Włącz router i odczekaj 2 minuty.
7. Włącz komputery.

Sprawdź, czy kable Ethernet są prawidłowo podłączone.

- Jeśli kabel Ethernet łączący router z modemem jest podłączony w prawidłowy sposób, świecić się będzie dioda LED sieci WAN.
- Jeśli kabel Ethernet łączący uruchomiony komputer z routerem jest podłączony w prawidłowy sposób, świecić się będzie odpowiednia dioda LED sieci LAN.

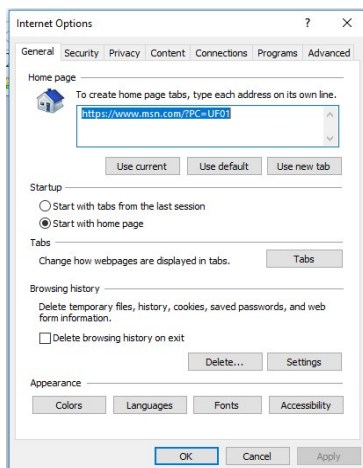
Sprawdź, czy ustawienia sieciowe są prawidłowe.

- Każdy klient w sieci powinien mieć odpowiedni adres IP. Firma ASUS zaleca przypisywanie adresów IP komputerom w sieci za pomocą serwera DHCP przewodowy router.
- W przypadku niektórych dostawców usług internetowych zapewnianych przez modem kablowy wymagane jest używanie adresu MAC komputera, dla którego zarejestrowano wstępnie konto. Adres MAC można sprawdzić za pomocą sieciowego interfejsu graficznego, na stronie **Dashboard (Pulpit nawigacyjny) > Clients (Klienci)**.

4.2 Często zadawane pytania (FAQ)

Nie mogę uzyskać dostępu do interfejsu graficznego routera przy użyciu przeglądarki sieci Web

- Jeśli komputer jest podłączony w sposób przewodowy, sprawdź połączenie kabla Ethernet i stan diody LED zgodnie z opisem w poprzedniej części.
- Upewnij się, że używane dane logowania są prawidłowe. Upewnij się, że podczas wprowadzania danych logowania klawisz Caps Lock jest wyłączony.
- Usuń pliki cookie i pliki w przeglądarce sieci Web. W przypadku programu Internet Explorer należy wykonać poniższe czynności:
 1. Uruchom program Internet Explorer, a następnie kliknij kolejno pozycje **Tools (Narzędzia) > Internet Options (Opcje internetowe)**.
 2. Na karcie **General (Ogólne)**, w obszarze **Browsing history (Historia przeglądania)** kliknij przycisk **Delete... (Usuń...)**, wybierz pozycję **Temporary Internet Files and website files (Tymczasowe pliki internetowe pliki witryn internetowych)** i **Cookies and website data (Cookie i dane witryny internetowej)**, a następnie kliknij przycisk **Delete (Usuń)**.



UWAGI:

- Polecenia usuwania plików cookie i plików zależą od przeglądarki sieci Web.
- W celu automatycznego uzyskiwania adresów IP należy wyłączyć ustawienia serwera proxy, anulować połączenie telefoniczne i wprowadzić ustawienia protokołu TCP/IP. Bardziej szczegółowe informacje można znaleźć w rozdziale 1 niniejszego podręcznika użytkownika.
- Należy używać kabli Ethernet CAT5e lub CAT6.

Klient nie może ustanowić połączenia bezprzewodowego z routerem.

WAŻNE! Aby udostępnić funkcję Wi-Fi, należy z siecią AiMesh routera EBG15 zintegrować bezprzewodowy punkt dostępowy (AP), taki jak ExpertWiFi EBA63 lub router, taki jak ExpertWiFi EBR63 lub ExpertWiFi EBM68.

- **Wyłączono serwer DHCP:**

1. Uruchom sieciowy interfejs graficzny. Przejdź kolejno do pozycji **Dashboard (Pulpit nawigacyjny) > Clients (Klienci)** i wyszukaj urządzenie, które chcesz połączyć z routerem.
2. Jeśli nie można znaleźć urządzenia w pozycji **Dashboard (Pulpit nawigacyjny)**, przejdź kolejno do pozycji **Settings (Ustawienia) > LAN (Sieć LAN) > DHCP Server (Serwer DHCP)**.

The screenshot shows the 'DHCP Server' configuration page. At the top, there is a brief description of DHCP. Below this, the 'Basic Config' section is expanded, showing fields for 'Enable the DHCP Server' (checked), 'ExpertWiFi EBM68's Domain Name', 'IP Pool Starting Address' (192.168.80.2), 'IP Pool Ending Address' (192.168.80.254), 'Lease Time (seconds)' (86400), and 'Default Gateway' (88.88.88.88). The 'DHCP and Static IP Setting' section shows 'DHCP Server 1' and 'DHCP Server 2' fields, and a checkbox for 'Activate router's IP in addition to user specified DHCP' (checked). The 'VLAN Server' section has a 'VLAN Server' field. The 'Manual Assignment' section has an 'Enable Manual Assignment' checkbox (unchecked). At the bottom, the 'Manually Assigned IP Address List (DHCP Excluded List)' table is visible, with columns for 'Client Name (DHCP Excluded)', 'IP Address', 'DHCP Server (Optional)', 'Host Name (Optional)', and 'Add / Delete'. The first row shows an IP address of 192.168.80.200.

- Ukryto identyfikator SSID. Jeśli urządzenie wyszukuje identyfikatory SSID innych routerów, ale nie może znaleźć identyfikatora SSID posiadanego routera, przejdź do pozycji **Settings (Ustawienia) > Wireless (Sieć bezprzewodowa) > General (Ogólne)**, zaznacz opcję **No (Nie)** dla pozycji **Hide SSID (Ukryj SSID)**.

Set up the wireless related information below.

Network Name (SSID)	ASUS_96_EBG15
Hide SSID	☐ Yes ☒ No
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	ASUS_4F96 Good

[Apply](#)

- Jeśli używana jest karta sieci bezprzewodowej, sprawdź, czy używany kanał bezprzewodowy jest zgodny z kanałami dostępnymi w danym kraju/regionie. Jeśli nie, dostosuj kanał, pasmo kanału i tryb bezprzewodowy.
- Jeśli nadal nie można połączyć się przewodowo z routerem, można przywrócić domyślne ustawienia fabryczne routera. W interfejsie graficznym routera kliknij kolejno pozycje **Settings (Ustawienia) > Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

This function allows you to save current settings of ExpertWiFi EEM68 to a file, or load settings from a file.

Factory default	Restore ☒ Initialize all the settings, and clear all the data log for AIProtection, Traffic Analyzer, and Web History.
Save setting	Save setting ☐ Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.
Restore setting	Upload

Niedostępny Internet.

- Sprawdź, czy router może nawiązać połączenie z adresem IP sieci WAN usługodawcy internetowego. Aby to zrobić, uruchom sieciowy interfejs graficzny, przejdź do pozycji **Dashboard (Pulpit nawigacyjny)** i sprawdź pozycję Stan połączenia z Internetem.
- Jeśli router nie może nawiązać połączenia z adresem IP sieci WAN usługodawcy internetowego, uruchom ponownie sieć zgodnie z opisem w części **Restart your network in following sequence (Uruchom ponownie sieć, wykonując czynności w następującej kolejności)** w rozdziale **Basic Troubleshooting (Rozwiązywanie podstawowych problemów)**.
- Jeśli dostęp do Internetu jest nadal niemożliwy, uruchom ponownie komputer, a następnie sprawdź adres IP i adres bramy sieci.
- Sprawdź wskaźniki stanu modemu ADSL i przewodowy router. Jeśli nie świeci się dioda LED sieci WAN przewodowy router, sprawdź, czy wszystkie kable są prawidłowo podłączone.

Nie pamiętam identyfikatora SSID (nazwy sieci) lub hasła sieciowego

- Skonfiguruj nowy identyfikator SSID i klucz szyfrowania za pomocą połączenia przewodowego (kabel Ethernet). Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Dashboard (Pulpit nawigacyjny)**, kliknij ikonę routera, wprowadź nowy identyfikator SSID i klucz szyfrowania, a następnie kliknij przycisk **Apply (Zastosuj)**.
- Przywróć ustawienia domyślne routera. Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Jak przywrócić domyślne ustawienia systemu?

- Przejdź do pozycji **Settings (Ustawienia) > Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Niepowodzenie uaktualnienia oprogramowania sprzętowego.

Uruchom tryb ratunkowy i skorzystaj z narzędzia Firmware Restoration (Odtwarzanie oprogramowania sprzętowego).

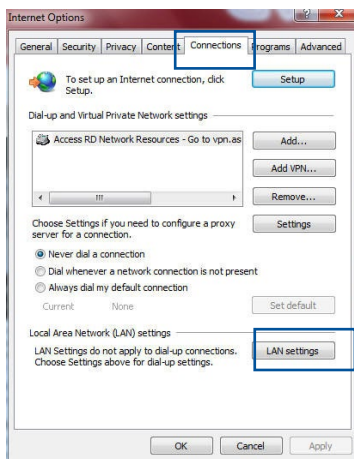
Nie można uzyskać dostępu do sieciowego interfejsu graficznego

Przed konfiguracją przewodowy router wykonać czynności opisane w tej części dla komputera hosta i klientów sieciowych.

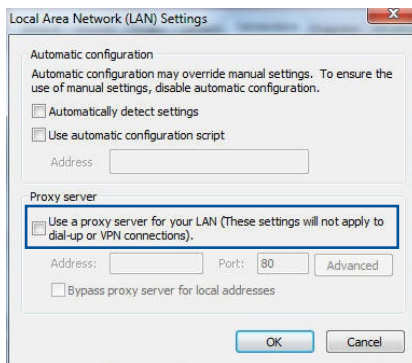
A. Wyłączyć serwer proxy jeżeli jest włączony.

Windows®

1. Kliknij przycisk **Start** > **Internet Explorer** w celu uruchomienia przeglądarki internetowej.
2. Kliknij przycisk **Tools** (Narzędzia) > **Internet options** (Opcje internetowe) > **Connections** (Połączenia) > **LAN settings** (Ustawienia sieci LAN).

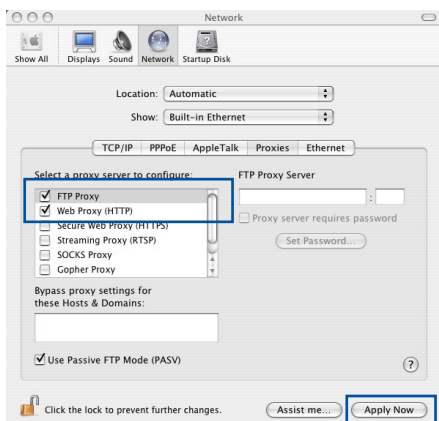


3. Na ekranie Local Area Network (LAN) Settings (Ustawienia sieci lokalnej (LAN)) odznacz opcję **Use a proxy server for your LAN** (Użyj serwera proxy dla sieci LAN).
4. Po zakończeniu kliknij przycisk **OK**.



MAC OS

1. W przeglądarce Safari kliknąć **Safari**
> **Preferences** (Preferencje)
> **Advanced** (Zaawansowane) > **Change Settings...** (Zmień ustawienia...)
2. Na ekranie Network (Sieć) usunąć zaznaczenie **FTP Proxy** (Proxy FTP) i **Web Proxy** (HTTP) (Proxy www (HTTP)).
3. Po zakończeniu kliknąć przycisk **Apply Now** (Zastosuj teraz).

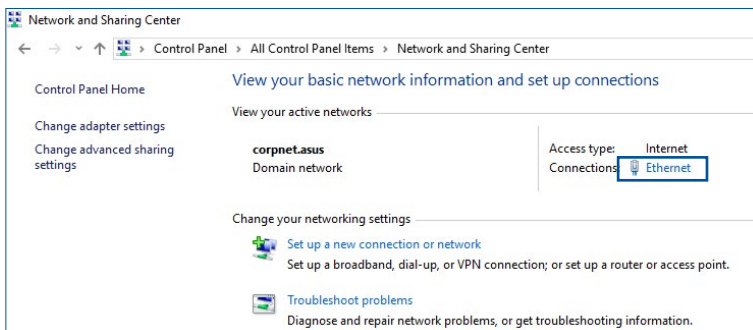


UWAGA: Szczegółowe informacje dotyczące wyłączania serwera proxy, patrz funkcja pomocy danej przeglądarki.

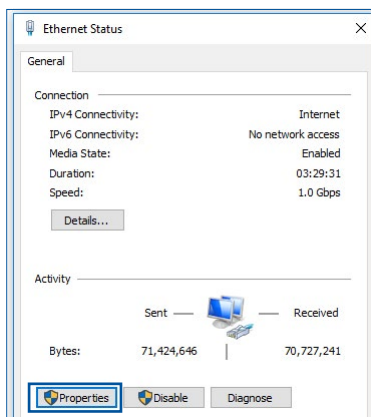
B. Skonfigurować ustawienia TCP/IP do automatycznego uzyskiwania adresu IP.

Windows®

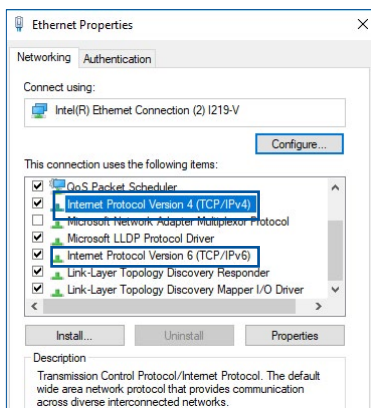
1. Kliknij przycisk **Start** > **Control Panel** (Panel Sterowania) > **Network and Sharing Center** (Centrum sieci i udostępniania), następnie kliknij połączenie sieciowe, aby wyświetlić okno stanu.



2. Kliknij pozycję **Properties** (**Właściwości**), aby wyświetlić okno Ethernet Properties (Właściwości sieci Ethernet).

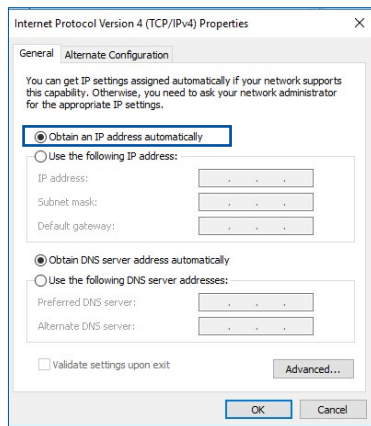


3. Zaznacz opcję **Internet Protocol Version 4 (TCP/IPv4)** (Protokół internetowy w wersji 4 (TCP/IPv4)) lub **Internet Protocol Version 6 (TCP/IPv6)** (Protokół internetowy w wersji 6 (TCP/IPv6)), a następnie kliknij przycisk **Properties** (**Właściwości**).



4. W celu automatycznego uzyskania ustawień IPv4 IP, zaznacz opcję **Obtain an IP address automatically** (Automatycznie uzyskaj adres IP).

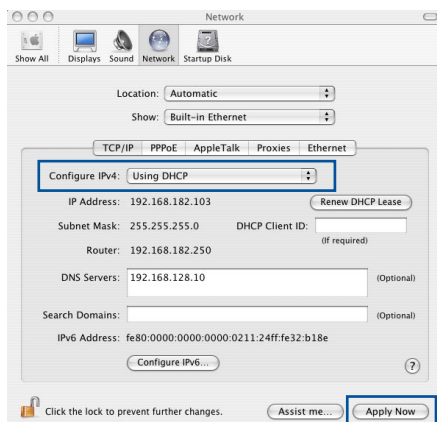
W celu automatycznego uzyskania ustawień IPv6 IP, zaznacz opcję **Obtain an IPv6 address automatically** (Automatycznie uzyskaj adres IPv6).



5. Po zakończeniu kliknij przycisk **OK**.

MAC OS

1. Kliknij ikonę Apple  umieszczoną w górnej lewej części ekranu.
2. Kliknij polecenie **System Preferences (Preferencje systemu) > Network (Sieć) > Configure... (Konfiguruj...)**
3. Na zakładce **TCP/IP** wybierz **Using DHCP (Z użyciem DHCP)** na liście rozwijalnej **Configure IPv4 (Konfiguruj IPv4)**.



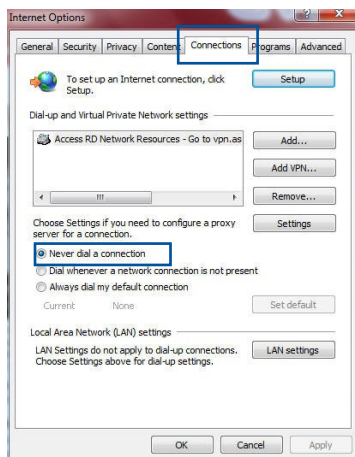
4. Po zakończeniu kliknąć przycisk **Apply Now (Zastosuj teraz)**.

UWAGA: Informacje dotyczące konfiguracji ustawień połączenia TCP/IP komputera patrz pomoc systemu operacyjnego i funkcje wsparcia.

C. Wyłączyć połączenie dial-up jeżeli jest włączone.

Windows®

1. Kliknij przycisk **Start > Internet Explorer** w celu uruchomienia przeglądarki internetowej.
2. Kliknij przycisk **Tools (Narzędzia) > Internet options (Opcje internetowe) > Connections (Połączenia)**.
3. Zaznaczyć opcję **Never dial a connection (Nigdy nie wybieraj połączenia)**.
4. Po zakończeniu kliknij przycisk **OK**.



UWAGA: Szczegółowe informacje o wyłączaniu połączenia dial-up, patrz funkcja pomocy przeglądarki sieciowej.

Załączniki

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Uwagi dotyczące bezpieczeństwa

Podczas korzystania z tego urządzenia należy zawsze stosować się do podstawowych zasad bezpieczeństwa, w tym m.in. do poniższych:



OSTRZEŻENIE!

- Przewody zasilające należy podłączać do gniazd elektrycznych o odpowiednim uziemieniu. Urządzenie należy podłączyć wyłącznie do znajdującego się w pobliżu gniazda elektrycznego, które jest łatwo dostępne.
- Jeśli uszkodzony został zasilacz nie należy próbować naprawiać go samemu. Należy skontaktować się z wykwalifikowanym technikiem serwisu lub ze sprzedawcą.
- NIE NALEŻY przykrywać szczelin wentylacyjnych komputera desktop PC, aby zapobiec przegrzaniu systemu.
- NIE NALEŻY montować tego urządzenia na wysokości większej niż 2 metry.
- Ten produkt należy używać w miejscach o temperaturze otoczenia w zakresie 0°C (32°F) do 40°C (104°F).
- Przed rozpoczęciem korzystania z urządzenia należy przeczytać instrukcję obsługi i zapoznać się z podanymi zakresami temperatur.
- W przypadku korzystania z tego urządzenia na lotniskach, w szpitalach, na stacjach benzynowych czy w warsztatach samochodowych należy zwrócić szczególną uwagę na kwestię ochrony bezpieczeństwa osobistego.
- Zakłócenia działania urządzeń medycznych: Między wszczepionymi urządzeniami medycznymi a produktami firmy ASUS należy zachować odległość wynoszącą co najmniej 15 cm (6 cali) w celu ograniczenia ryzyka wystąpienia zakłóceń w pracy tych urządzeń.
- Z urządzeń firmy ASUS należy korzystać w miejscach o dobrym sygnale, aby zminimalizować poziom promieniowania.
- Kobiety w ciąży nie powinny znajdować się blisko urządzenia, a także należy zachować odpowiednią odległość od dolnych partii brzucha w przypadku nastolatków.
- NIE NALEŻY korzystać z tego urządzenia w przypadku występowania widocznych defektów lub jeśli zostało ono zamoczone, uszkodzone lub przerobione. W takiej sytuacji urządzenie należy oddać do serwisu.



OSTRZEŻENIE!

- NIE NALEŻY umieszczać urządzeń na nierównych lub niestabilnych powierzchniach roboczych.
 - NIE NALEŻY umieszczać ani upuszczać przedmiotów na to urządzenie. Urządzenia nie należy wystawiać na wstrząsy mechaniczne, takie jak przygniecenia, wygięcia, nakłuwanie lub niszczenie.
 - NIE NALEŻY urządzenia demontować, otwierać, podgrzewać w kuchence mikrofalowej, spalać, malować ani wpychać jakichkolwiek przedmiotów do jego wnętrza.
 - Należy sprawdzić tabliczkę znamionową na spodzie produktu i upewnić się, że zasilacz jest zgodny z podanymi wartościami.
 - Urządzenie powinno znajdować się z dala od ognia i źródeł ciepła.
 - NIE NALEŻY umieszczać, upuszczać lub wpychać żadnych obcych obiektów na produkt. NIE NALEŻY korzystać z urządzenia podczas burz z wyładowaniami elektrycznymi.
 - Obwody wyjściowe PoE tego urządzenia należy łączyć wyłącznie z sieciami PoE, nie kierując ich do instalacji zewnętrznych.
 - Aby zapobiec porażeniu prądem elektrycznym, przed przeniesieniem systemu należy odłączyć kabel zasilający od gniazdka elektrycznego.
 - Należy korzystać wyłącznie z akcesoriów, które zostały zatwierdzone przez producenta urządzenia do użytku z tym modelem. Używanie innego rodzaju akcesoriów może spowodować unieważnienie gwarancji lub naruszenie lokalnych przepisów prawnych, a także może stanowić zagrożenie dla bezpieczeństwa. Aby uzyskać informacje o zatwierdzonych akcesoriach, należy skontaktować się z lokalnym sprzedawcą.
 - Korzystanie z tego urządzenia w sposób niezgodny z instrukcją obsługi może stwarzać ryzyko wystąpienia pożaru lub obrażeń ciała.
-

Obsługę i Pomoc

Odwiedź naszą wielojęzyczną witrynę internetową pod adresem
<https://www.asus.com/support>.

