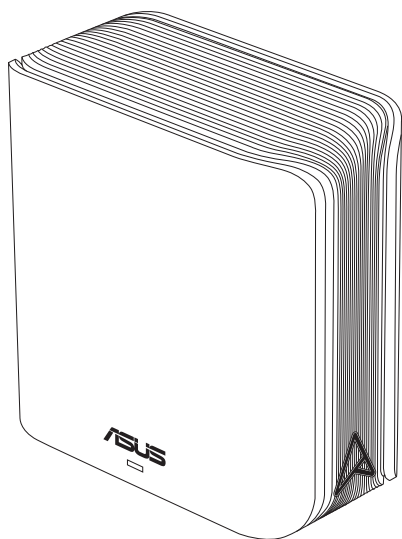


Manuel de l'utilisateur

ZenWiFi BD4

Routeur à double bande BE3600



ASUS
IN SEARCH OF INCREDIBLE

F23951

Première Édition

Juillet 2024

Copyright © 2024 ASUSTeK Computer Inc. Tous droits réservés.

Aucun extrait de ce manuel, incluant les produits et logiciels qui y sont décrits, ne peut être reproduit, transmis, transcrit, stocké dans un système de restitution, ou traduit dans quelque langue que ce soit sous quelque forme ou quelque moyen que ce soit, à l'exception de la documentation conservée par l'acheteur dans un but de sauvegarde, sans la permission écrite expresse de ASUSTeK Computer Inc ("ASUS").

La garantie sur le produit ou le service ne sera pas prolongée si (1) le produit est réparé, modifié ou altéré, à moins que cette réparation, modification ou altération ne soit autorisée par écrit par ASUS ; ou (2) si le numéro de série du produit est dégradé ou manquant.

ASUS fournit ce manuel "en l'état" sans garantie d'aucune sorte, explicite ou implicite, y compris, mais non limité aux garanties implicites ou aux conditions de commerciabilité ou d'adéquation à un but particulier. En aucun cas ASUS, ses directeurs, ses cadres, ses employés ou ses agents ne peuvent être tenus responsables des dégâts indirects, spéciaux, accidentels ou consécutifs (y compris les dégâts pour manque à gagner, pertes de profits, perte de jouissance ou de données, interruption professionnelle ou assimilé), même si ASUS a été prévenu de la possibilité de tels dégâts découlant de tout défaut ou erreur dans le présent manuel ou produit.

Les spécifications et les informations contenues dans ce manuel sont fournies à titre indicatif seulement et sont sujettes à des modifications sans préavis, et ne doivent pas être interprétées comme un engagement de la part d'ASUS. ASUS n'est en aucun cas responsable d'éventuelles erreurs ou inexactitudes présentes dans ce manuel, y compris les produits et les logiciels qui y sont décrits.

Les noms des produits et des sociétés qui apparaissent dans le présent manuel peuvent être, ou non, des marques commerciales déposées, ou sujets à copyrights pour leurs sociétés respectives, et ne sont utilisés qu'à des fins d'identification ou d'explication, et au seul bénéfice des propriétaires, sans volonté d'infraction.

Table des matières

1	Présentation de votre routeur WiFi	
1.1	Bienvenue !	6
1.2	Contenu de la boîte.....	6
1.3	Votre routeur WiFi	7
1.4	Placer le routeur WiFi	8
1.5	Pré-requis	9
2	Prise en main	
2.1	Configurer le routeur	10
	A. Connexion filaire.....	11
	B. Connexion WiFi.....	12
2.2	Configuration internet rapide avec auto-détection	14
2.3	Connexion à un réseau WiFi.....	16
3	Configurer les paramètres généraux et avancés	
3.1	Se connecter à l'interface de gestion.....	17
	3.1.1 Configurer les paramètres de sécurité WiFi	19
	3.1.2 Gérer les clients du réseau	20
3.2	Service Adaptive QoS	21
	3.2.1 Gérer le service QoS (Qualité de service)	21
3.3	Administration.....	24
	3.3.1 Mode de fonctionnement.....	24
	3.3.2 Système	25
	3.3.3 Mise à jour du firmware	26
	3.3.4 Restauration/Sauvegarde/Transfert de paramètres.....	26
3.4	AiProtection.....	27
	3.4.1 Protection du réseau	27
	3.4.2 Configurer le contrôle parental	31
3.5	Pare-feu	34
	3.5.1 Paramètres de base.....	34
	3.5.2 Filtrage d'URL	35
	3.5.3 Filtrage de mots-clés	36
	3.5.4 Filtrage de services réseau.....	37

Table des matières

3.6	IPv6 (Protocole IPv6)	38
3.7	Réseau local (LAN)	39
3.7.1	Adresse IP du routeur.....	39
3.7.2	Serveur DHCP.....	40
3.7.3	Routage	42
3.7.4	Télévision sur IP	43
3.8	Réseau.....	44
3.8.1	Réseau principal - Filtrage d'adresses MAC.....	44
3.8.2	Réseau invité.....	46
3.8.2.1	Réseau invité	46
3.8.2.2	Maître domotique (Smart Home Master).....	48
3.9	Journal système	52
3.10	Dispositif d'analyse du trafic.....	53
3.11	Réseau étendu (WAN)	54
3.11.1	Connexion internet.....	54
3.11.2	Dual WAN (Double WAN).....	57
3.11.3	Déclenchement de port	58
3.11.4	Serveur virtuel et redirection de port.....	60
3.11.5	Zone démilitarisée	63
3.11.6	Service DDNS	64
3.11.7	NAT Passthrough.....	65
3.12	WiFi.....	66
3.12.1	WPS	66
3.12.2	Pontage WDS.....	68
3.12.3	Service RADIUS.....	70
3.12.4	Professionnel	71

Table des matières

4 Utilitaires

4.1 Device Discovery (Détection d'appareils)74

4.2 Firmware Restoration (Restauration du firmware)74

5 Dépannage

5.1 Dépannage de base76

5.2 Foire aux questions (FAQ)79

Annexes

Consignes de sécurité97

Service et assistance.....99

1 Présentation de votre routeur WiFi

1.1 Bienvenue !

Merci d'avoir acheté un routeur WiFi ASUS ZenWiFi BD4 !

Avec l'accent métallique du monogramme A sur un châssis blanc minimaliste, le ZenWiFi BD4 est compatible avec les réseaux WiFi sur les bandes 2,4 GHz et 5 GHz, offrant un streaming HD WiFi et simultanément inégalable. Il intègre également les serveurs SMB, UPnP AV et FTP pour un partage de fichiers 24h/24, 7j/7 et possède la capacité de prendre en charge 300 000 sessions. Enfin la technologie ASUS Green Network permet de faire jusqu'à 70 % d'économie d'énergie.

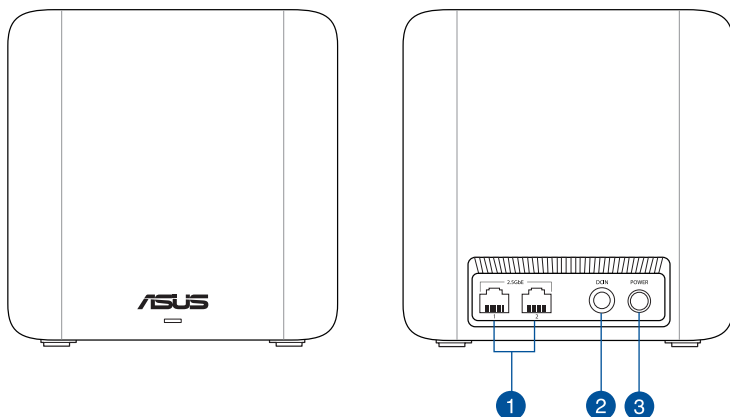
1.2 Contenu de la boîte

- Routeur WiFi ZenWiFi BD4
- Câble réseau (RJ-45)
- Adaptateur secteur
- Guide de démarrage rapide
- Carte de garantie

REMARQUES :

- Contactez votre service après-vente ASUS si l'un des éléments est manquant ou endommagé. Consultez la section **Service et assistance** à la fin de ce manuel d'utilisation.
 - Conservez l'emballage d'origine pour toutes futures demandes de prises sous garantie.
-

1.3 Votre routeur WiFi



- 1 Ports 2.5GbE (détection automatique WAN/LAN)**
Connectez un câble réseau à l'un de ces ports pour établir une connexion WAN/LAN 2.5GbE.
- 2 Prise d'alimentation (CC)**
Insérez l'adaptateur secteur dans ce port puis reliez votre routeur à une source d'alimentation.
- 3 Bouton d'alimentation**
Ce bouton permet d'allumer ou d'éteindre le routeur.

REMARQUES :

- Utilisez uniquement l'adaptateur secteur fourni avec votre appareil. L'utilisation d'autres adaptateurs peut endommager l'appareil.
- Caractéristiques :**

Adaptateur secteur CC	Sortie (CC) : 12V (1,5A max.)		
Température de fonctionnement	0-40°C	Stockage	0-70°C
Humidité de fonctionnement	50-90 %	Stockage	20-90 %

1.4 Placer le routeur WiFi

Pour optimiser la transmission du signal WiFi entre votre routeur et les périphériques réseau y étant connectés, veuillez vous assurer des points suivants :

- Placez le routeur WiFi dans un emplacement central pour obtenir une couverture WiFi optimale.
- Maintenez le routeur à distance des obstructions métalliques et des rayons du soleil.
- Maintenez le routeur à distance d'appareils ne fonctionnant qu'avec les normes/fréquences WiFi 802.11g ou 20MHz, les périphériques 2,4 GHz et Bluetooth, les téléphones sans fil, les transformateurs électriques, les moteurs à service intense, les lumières fluorescentes, les micro-ondes, les réfrigérateurs et autres équipements industriels pour éviter les interférences ou les pertes de signal WiFi.
- Mettez toujours le routeur à jour dans la version de firmware la plus récente. Visitez le site web d'ASUS sur <http://www.asus.com> pour consulter la liste des mises à jour.

1.5 Pré-requis

Pour établir votre réseau WiFi, vous aurez besoin d'un ou deux ordinateurs répondant aux critères suivants :

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Compatible avec la norme WiFi IEEE 802.11a/b/g/n/ac/ax
- Un service TCP/IP installé
- Navigateur internet tel qu'Internet Explorer, Firefox, Safari ou Google Chrome

REMARQUES :

- Si votre ordinateur ne possède pas de module WiFi, installez une carte WiFi compatible avec la norme IEEE 802.11a/b/g/n/ac/ax sur votre ordinateur pour vous connecter au réseau.
- Grâce à sa technologie à double bande, votre routeur WiFi prend en charge les signaux WiFi des bandes 2,4 GHz et 5 GHz simultanément. Ceci vous permet de naviguer sur Internet ou de lire/écrire des e-mails sur la bande 2,4 GHz tout en profitant de streaming audio/vidéo en haute définition sur la bande 5 GHz.
- Certains appareils dotés de capacités WiFi IEEE 802.11n ne sont pas compatibles avec la bande à 5 GHz. Consultez le mode d'emploi de vos dispositifs WiFi pour plus d'informations.
- Les câbles réseau Ethernet RJ-45 utilisés pour établir une connexion réseau ne doivent pas excéder une longueur de 100 mètres.

IMPORTANT !

- Certains adaptateurs sans fil peuvent avoir des problèmes de connexion aux points d'accès WiFi 802.11ax.
- Si vous rencontrez ce problème, assurez-vous d'utiliser le dernier pilote pour votre matériel. Consultez le site de support officiel de votre fabricant pour obtenir des pilotes de logiciels, des mises à jour et autres informations connexes.
 - Realtek : <https://www.realtek.com/en/downloads>
 - Mediatek : <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel : <https://downloadcenter.intel.com/>

2 Prise en main

2.1 Configurer le routeur

IMPORTANT !

- Il est recommandé d'utiliser une connexion filaire pour la configuration initiale afin d'éviter des problèmes d'installation causés par l'instabilité du réseau WiFi.
 - Avant toute chose, veuillez vous assurer des points suivants :
 - Si vous remplacez un routeur existant, déconnectez-le de votre réseau.
 - Déconnectez tous les câbles de votre configuration modem actuelle. Si votre modem possède une batterie de secours, retirez-la.
 - Redémarrez votre ordinateur (recommandé).
-



AVERTISSEMENT !

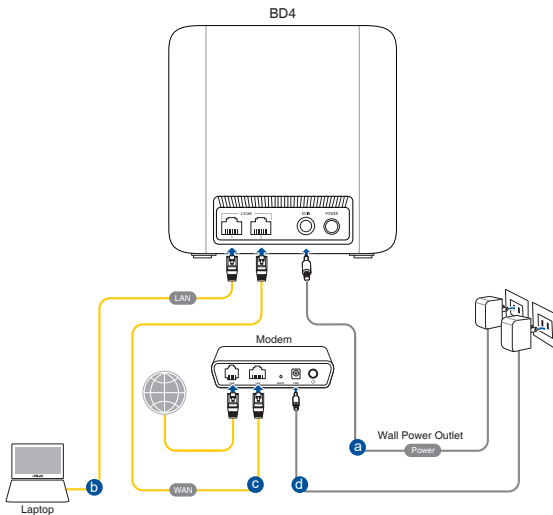
- Les cordons d'alimentation doivent être branchés sur une prise électrique correctement reliée à la terre. Connectez l'équipement uniquement à une prise de courant à proximité et facilement accessible.
 - Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien qualifié ou votre revendeur.
 - NE PAS utiliser de cordons d'alimentation, accessoires ou autres périphériques endommagés.
 - NE PAS placer cet équipement à une hauteur supérieure à 2 mètres.
 - Utilisez ce produit dans un environnement dont la température ambiante est comprise entre 0°C (32°F) et 40°C (104°F).
-

A. Connexion filaire

REMARQUE : Une fonction de détection de croisement automatique est intégrée au routeur WiFi pour que vous puissiez aussi bien utiliser un câble Ethernet droit que croisé.

Pour configurer votre routeur via une connexion filaire :

1. Branchez le routeur sur une prise électrique, puis allumez-le. Utilisez le câble réseau pour relier votre ordinateur à l'un des ports 2.5GbE du routeur.

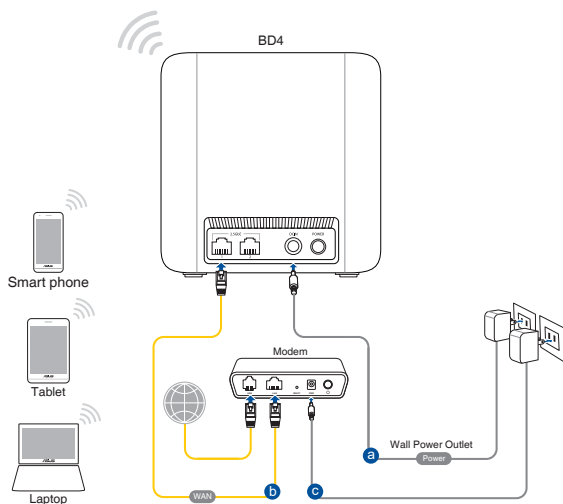


2. L'interface de gestion du routeur s'affiche automatiquement lors de l'ouverture de votre navigateur internet. Si ce n'est pas le cas, saisissez <http://www.asusrouter.com> dans la barre d'adresse
3. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.

B. Connexion WiFi

Pour configurer votre routeur via une connexion WiFi :

1. Branchez le routeur sur une prise électrique, puis allumez-le.



2. Connectez-vous au réseau dont le nom (SSID) est affiché sur l'étiquette du produit située à l'arrière du routeur. Pour garantir une plus grande sécurité, modifiez le nom du réseau et le mot de passe.

Nom du réseau WiFi (SSID) : ASUS_XX

* **XX** correspond aux deux derniers chiffres de l'adresse MAC 2,4 GHz. Vous pouvez les trouver sur l'étiquette située à l'arrière de votre routeur.

3. Une fois connecté, l'interface de gestion du routeur s'affiche automatiquement lors de l'ouverture de votre navigateur internet. Si ce n'est pas le cas, saisissez <http://www.asusrouter.com> dans la barre d'adresse.

4. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.
-

REMARQUES :

- Référez-vous au manuel de la carte WiFi pour la procédure de configuration de la connexion WiFi.
 - Pour configurer les paramètres de sécurité de votre réseau, consultez la section **3.1.1 Définir les paramètres de sécurité WiFi** de ce manuel.
-

2.2 Configuration internet rapide avec auto-détection

L'assistant de configuration vous aide à configurer rapidement votre connexion internet.

REMARQUE : Lors de la toute première configuration de connexion internet, appuyez sur le bouton de réinitialisation de votre routeur WiFi pour restaurer ses paramètres par défaut.

Utilisation de l'assistant de configuration internet avec auto-détection :

1. Ouvrez un navigateur internet. Vous serez automatiquement redirigé vers l'assistant de configuration ASUS (Configuration internet rapide). Si ce n'est pas le cas, tapez manuellement : <http://www.asusrouter.com>.
2. Le routeur WiFi détecte automatiquement si la connexion internet fournie par votre FAI utilise une **IP dynamique** ou le protocole **PPPoE**, **PPTP** ou **L2TP**. Entrez les informations nécessaires en fonction de votre type de connexion.

IMPORTANT ! Vous pouvez obtenir vos informations de connexion auprès de votre FAI (Fournisseur d'accès à Internet).

REMARQUES :

- L'auto-détection de votre type de connexion a lieu lorsque vous configurez le routeur WiFi pour la première fois ou lorsque vous restaurez les paramètres par défaut du routeur.
 - Si votre type de connexion internet n'a pas pu être détecté, cliquez sur **Manual Setting** (Configuration manuelle) pour configurer manuellement vos paramètres de connexion.
-
3. Attribuez un nom au réseau (SSID) ainsi qu'une clé de sécurité pour votre connexion WiFi 7. Cliquez sur **Apply** (Appliquer) une fois terminé.



4. Dans la page de **Configuration des informations de connexion**, modifiez le mot de passe de connexion du routeur afin d'éviter les accès non autorisés au routeur WiFi.

REMARQUE : Le nom d'utilisateur et le mot de passe de connexion sont différents de l'identifiant WiFi 7 et de sa clé de sécurité. Le nom d'utilisateur et le mot de passe de connexion permettent d'accéder à l'interface de gestion des paramètres du routeur WiFi. Le SSID (nom du réseau WiFi 7) et la clé de sécurité permettent aux dispositifs WiFi de se connecter au réseau WiFi 7 de votre routeur.

2.3 Connexion à un réseau WiFi

Après avoir configuré la connexion internet sur votre routeur, vous pouvez connecter votre ordinateur, ou tout autre appareil disposant d'une connectivité WiFi, à votre réseau WiFi.

Pour vous connecter à un réseau WiFi sous Windows :

1. Sur votre ordinateur, cliquez sur l'icône réseau  de la zone de notification pour afficher la liste des réseaux WiFi disponibles.
2. Sélectionnez le réseau WiFi avec lequel vous souhaitez établir une connexion, puis cliquez sur **Connect** (Connecter).
3. Si nécessaire, entrez la clé de sécurité du réseau WiFi, puis cliquez sur **OK**.
4. Patientez le temps que votre ordinateur puisse établir une connexion au réseau WiFi. L'état de la connexion apparaît et l'icône réseau  affiche le statut Connecté.

REMARQUES :

- Consultez les chapitres suivants pour plus de détails sur les divers paramètres de configuration WiFi disponibles.
 - Référez-vous au mode d'emploi de votre appareil pour plus de détails sur la connexion à un réseau WiFi.
-

3 Configurer les paramètres généraux et avancés

3.1 Se connecter à l'interface de gestion

Le routeur WiFi ASUS intègre une interface utilisateur en ligne qui permet de configurer le routeur WiFi sur votre ordinateur à l'aide d'un navigateur internet tel qu'Internet Explorer, Firefox, Safari ou Google Chrome.

REMARQUE : Les fonctionnalités présentées peuvent varier en fonction du modèle.

Pour vous connecter à l'interface de gestion :

1. Dans la barre d'adresse de votre navigateur internet, entrez l'adresse IP par défaut de votre routeur WiFi :
<http://www.asusrouter.com>.
2. Dans la page de connexion, saisissez le nom d'utilisateur et le mot de passe que vous avez configuré dans **2.2 Configuration internet rapide avec auto-détection**.
3. Vous pouvez dès lors configurer une grande variété de paramètres dédiés à votre routeur WiFi ASUS.



* L'image est fournie à titre indicatif uniquement.

REMARQUE : Lors du tout premier accès à l'interface de gestion du routeur, vous serez automatiquement redirigé vers la page de configuration de connexion internet.

3.1.1 Configurer les paramètres de sécurité WiFi

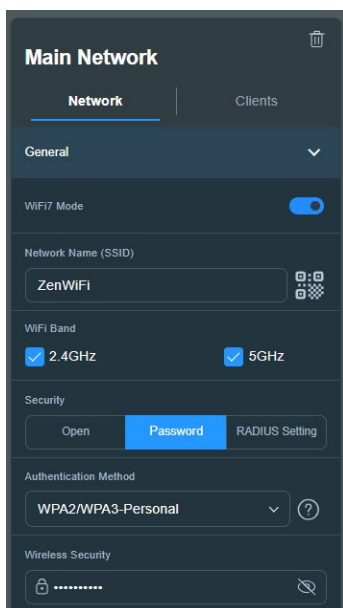
Pour protéger votre réseau WiFi contre les accès non autorisés, vous devez configurer les paramètres de sécurité du routeur.

Pour configurer les paramètres de sécurité WiFi :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Sélectionnez le réseau pour configurer les options de sécurité telles que le SSID, le niveau de sécurité et la méthode de chiffrement.

REMARQUE : Vous pouvez définir des paramètres de sécurité différents pour les bandes 2,4 GHz et 5 GHz.

Paramètres de sécurité 2,4GHz/5GHz

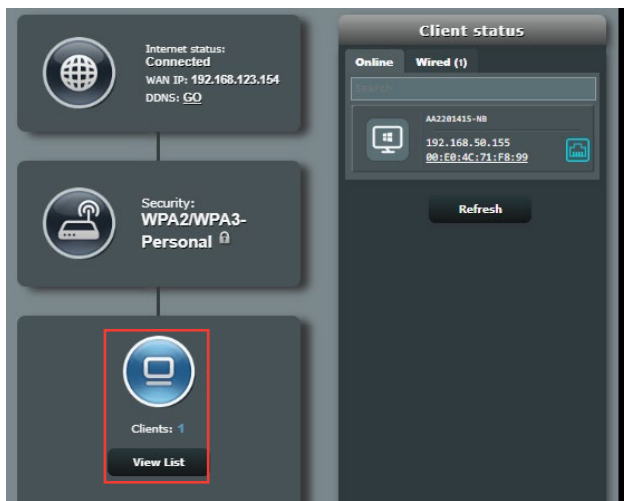


3. Dans le champ **Network Name (SSID)** (Nom du réseau (SSID)), spécifiez un nom unique pour votre réseau WiFi.
4. Dans le menu déroulant **WEP Encryption** (Chiffrement WEP), sélectionnez la méthode de chiffrement.

IMPORTANT ! La norme IEEE 802.11n/ac/ax n'autorise pas l'utilisation du haut débit avec les méthodes de chiffrement WEP ou WPA-TKIP. Si vous utilisez ces méthodes de chiffrement, votre débit ne pourra pas excéder les limites de vitesse établies par la norme IEEE 802.11g 54 Mb/s.

5. Saisissez votre clé de sécurité.
6. Cliquez sur **Apply** (Appliquer) une fois terminé.

3.1.2 Gérer les clients du réseau



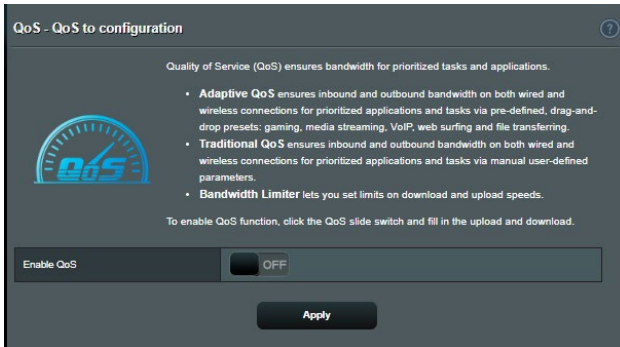
Pour gérer les clients de votre réseau :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Dans l'écran Network Map (Carte du réseau), cliquez sur l'icône **Client status** (États clients) pour afficher les informations relatives aux clients de votre réseau.
3. Pour bloquer l'accès d'un client à votre réseau, sélectionnez le client, puis cliquez sur **Block** (Bloquer).

3.2 Service Adaptive QoS

3.2.1 Gérer le service QoS (Qualité de service)

Le service QoS (Quality of Service) vous permet de définir la priorité de la bande passante et de gérer le trafic du réseau.



Pour configurer l'ordre de priorité de la bande passante :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Adaptive QoS** (Service Adaptive QoS) > **QoS**.
2. Cliquez sur **ON** (Activer) pour activer le service QoS. Remplissez les champs réservés à la bande passante montante et descendante.

REMARQUE : Obtenez vos informations de bande passante auprès de votre FAI (Fournisseur d'accès à Internet).

3. Cliquez sur **Apply** (Appliquer).

REMARQUE : La liste des règles personnalisées fait partie des paramètres avancés. Si vous souhaitez hiérarchiser des applications ou des périphériques réseau spécifiques, sélectionnez l'une des règles QoS disponibles.

4. Lorsque vous sélectionnez l'option **User-defined QoS rules** (Règles QoS personnalisées), trois types de services en ligne par défaut sont déjà disponibles : la navigation internet, le protocole HTTPS et le transfert de fichiers. Utilisez le menu déroulant en haut de tableau pour ajouter un service spécifique. Puis, remplissez les colonnes **Source IP or MAC** (Adresse IP ou MAC source), **Destination Port** (Port de destination), **Protocol** (Protocole), **Transferred** (Trafic) et **Priority** (Priorité). Une fois terminé, cliquez sur **Apply** (Appliquer). Les informations seront configurées dans l'écran des règles QoS.

REMARQUES :

- Pour le champ réservé à l'adresse IP ou MAC, vous pouvez :
 - a) Saisir une adresse IP spécifique, telle que "192.168.122.1".
 - b) Entrer l'adresse IP d'un sous-réseau ou d'une plage d'IP spécifique, telle que "192.168.123.*" ou "192.168.*.*"
 - c) Saisir toutes les adresses IP sous forme "*.*.*.*" ou laisser le champ vide.
 - d) Une adresse MAC est composée de six groupes de deux valeurs hexadécimales séparées par deux points (:) (ex : 12:34:56:aa:bc:ef)
 - Pour les plages de port source ou de destination, vous pouvez :
 - a) Saisir une valeur de port spécifique, telle que "95".
 - b) Entrer une plage de ports, comme "103:315", ">100", ou "<65535".
 - La colonne **Transferred** contient des informations sur les débits montant et descendant (trafic réseau sortant et entrant) pour une section. Dans la colonne **Transferred** (Trafic), définissez la limite du trafic réseau (en Ko) pour un service spécifique affecté à un port spécifique. Par exemple, si deux clients réseau, PC 1 et PC 2, accèdent tous deux à Internet (via le port 80) mais que le PC 1 excède le seuil de trafic limite, en raison de l'exécution de multiples tâches de téléchargement, celui-ci se verra affecté une faible priorité. La colonne se réfère au trafic montant et descendant pour une session. Si vous ne souhaitez pas limiter le trafic, vous pouvez ignorer cette colonne.
-

5. Lorsque vous sélectionnez l'option **User-defined Priority** (Priorité de la bande passante), vous pouvez définir la priorité des applications ou des périphériques réseau sur l'un des 5 niveaux disponibles. En fonction du niveau de priorité, la fonction QoS utilisera les méthodes suivantes pour le transfert de paquets :
 - Modification de l'ordre des paquets réseau ascendants, soit l'ordre dans lequel les paquets sont transmis sur Internet.
 - Dans le tableau **Upload Bandwidth** (Bande passante montante), réglez **les limites de bande passante maximum et minimum** pour diverses applications réseau disposant de différents niveaux de priorité. Les pourcentages font référence aux taux de bande passante montante disponibles pour des applications réseau spécifiques.
-

REMARQUES :

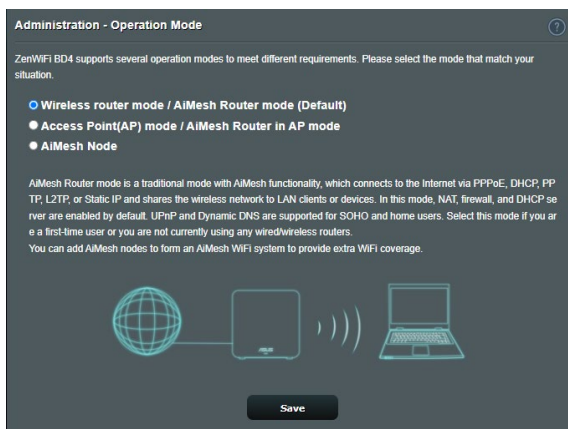
- Les paquets à faible priorité sont ignorés pour garantir le transfert des paquets de haute priorité.
 - Dans le tableau **Download Bandwidth** (Bande passante descendante), réglez **Maximum Bandwidth Limit** (la limite de bande passante maximum) pour diverses applications réseau par ordre correspondant. Un paquet montant à haute priorité entraînera un paquet descendant à haute priorité.
 - Si aucun paquet n'est transmis par des applications à haute priorité, le débit de transmission complet de la connexion internet est disponible pour les paquets à faible priorité.
-
6. Si nécessaire, cochez une ou plusieurs des options dédiées aux paquets auxquels vous souhaitez attribuer la plus haute priorité. Pour les jeux en ligne, il est recommandé de cocher les options ACK, SYN et ICMP.
-

REMARQUE : Assurez-vous d'avoir d'abord activé le service QoS avant de modifier les limites de bande passante montante et descendante.

3.3 Administration

3.3.1 Mode de fonctionnement

Le routeur WiFi dispose de plusieurs modes de fonctionnement offrant une plus grande flexibilité d'utilisation, selon vos besoins.



Pour définir le mode de fonctionnement du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **Operation Mode** (Mode de fonctionnement).
2. Sélectionnez l'un des modes disponibles :
 - **Wireless router mode (default) (Mode routeur WiFi (par défaut))**: Ce mode permet d'établir une connexion à Internet et d'en ouvrir l'accès aux clients disponibles sur le réseau local du routeur.
 - **Access Point mode (Point d'accès)**: Ce mode permet de créer un nouveau réseau WiFi à partir d'un réseau existant.
 - **Nœud AiMesh**: Vous pouvez configurer ce routeur comme un nœud AiMesh pour étendre la couverture WiFi existante des routeurs AiMesh.
3. Cliquez sur **Save** (Enregistrer).

REMARQUE : Le changement de mode de fonctionnement requiert un redémarrage du routeur.

3.3.2 Système

L'onglet **System** (Système) permet de configurer certains paramètres système du routeur WiFi.

Pour configurer les paramètres système du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **System** (Système).
2. Configurez les paramètres listés ci-dessous :
 - **Change router login password (Modification des identifiants de connexion du routeur)**: Cette zone vous permet de modifier le nom d'utilisateur et le mot de passe d'accès à l'interface de gestion du routeur WiFi.
 - **WPS button behavior (Comportement du bouton WPS)**: Le bouton physique WPS du routeur peut être utilisé pour activer la fonction WPS.
 - **Time Zone (Fuseau horaire)**: Sélectionnez votre fuseau horaire.
 - **NTP Server (Serveur NTP)**: Le routeur peut accéder à un serveur NTP (Network time Protocol) pour synchroniser l'heure.
 - **Enable Telnet (Activer le protocole Telnet)**: Cochez **Yes** (Oui) / **No** (Non) pour activer / désactiver le protocole Telnet.
 - **Authentication Method (Méthode d'authentification)**: Les protocoles d'authentification HTTP, HTTPS aident à sécuriser le routeur.
 - **Enable Web Access from WAN (Autoriser l'accès au routeur depuis Internet)**: Cochez **Yes** (Oui) / **No** (Non) pour autoriser / ne pas autoriser l'accès à l'interface de gestion du routeur depuis Internet. Sélectionnez **No** (Non) pour empêcher l'accès.
 - **Only allow specified IP (Filtrage d'adresse IP)** : Cochez **Yes** (Oui) si vous souhaitez spécifier les adresses IP des clients pouvant accéder à l'interface de gestion du routeur depuis Internet.
3. Cliquez sur **Apply** (Appliquer).

3.3.3 Mise à jour du firmware

REMARQUE : Téléchargez la dernière version du firmware sur le site internet d'ASUS : <http://www.asus.com>.

Pour mettre à niveau le firmware :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **Firmware Upgrade** (Mise à jour du firmware).
 2. Dans le champ **Firmware Version** (Version du firmware), cliquez sur **Check** (Vérifier) pour localiser le fichier téléchargé.
 3. Cliquez sur **Upload** (Charger).
-

REMARQUES :

- Une fois le processus de mise à niveau terminé, patientez quelques instants le temps que le routeur redémarre.
 - Si la mise à niveau échoue, le routeur bascule automatiquement en mode de secours et le voyant d'alimentation situé en façade du routeur clignote lentement. Pour restaurer le routeur, consultez la section **4.2 Firmware Restoration (Restauration du firmware)**.
-

3.3.4 Restauration/Sauvegarde/Transfert de paramètres

Pour restaurer/sauvegarder/transférer les paramètres de configuration du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres).
 2. Sélectionnez une tâche :
 - Pour restaurer la configuration d'usine du routeur, cliquez sur **Restore** (Restaurer) puis sur **OK** lorsque le message de confirmation apparaît.
 - Pour effectuer une copie de sauvegarde des paramètres du routeur, cliquez sur **Save setting** (Sauvegarder la configuration), sélectionnez le dossier souhaité et cliquez sur **Save** (Sauvegarder).
 - Pour restaurer le routeur à partir d'un fichier de configuration précédent, cliquez sur **Upload** (Charger) et localisez le fichier, puis cliquez sur **Open** (Ouvrir).
-

IMPORTANT ! En cas de défaillance du routeur, chargez la dernière version du firmware. Ne restaurez pas la configuration d'usine du routeur.

3.4 AiProtection

AiProtection fournit une surveillance en temps réel qui permet de détecter les logiciels malveillants, les logiciels espions et les accès non autorisés. Game IPS filtre également les sites internet et les applications indésirables et vous permet de planifier le temps d'accès à Internet d'un périphérique connecté.

3.4.1 Protection du réseau

Protection du réseau évite les risques d'exploitation du réseau et protège le réseau contre les accès non autorisés.

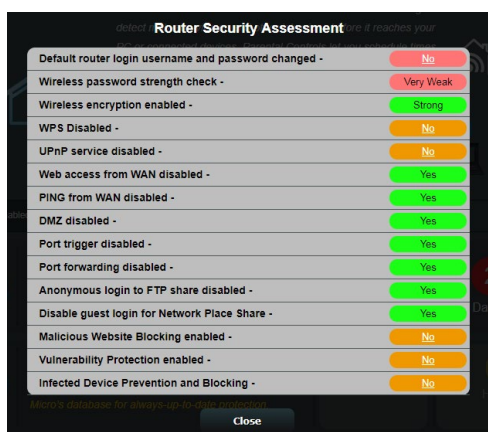


Configurer la protection du réseau

Pour configurer la protection du réseau :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale **AiProtection**, cliquez sur **Network Protection** (Protection du réseau).
3. À partir de l'onglet **Network Protection** (Protection du réseau), cliquez sur **Scan** (Analyser).

Une fois l'analyse terminée, l'utilitaire affiche les résultats sur la page **Router Security Assessment** (Évaluation de la sécurité du routeur).



IMPORTANT ! Les éléments suivis de la marque **Yes** (Oui) sur la page **Router Security Assessment** (Évaluation de la sécurité du routeur) sont considérés comme sûrs. Les éléments suivis de la marque **No** (Non), **Weak** (Faible) ou **Very Weak** (Très faible) signifient qu'une faiblesse a été détectée et qu'une configuration différente est recommandée.

4. (Optionnel) Dans la page **Router Security Assessment** (Évaluation de la sécurité du routeur), configurez manuellement les éléments suivis de la marque **No** (Non), **Weak** (Faible) ou **Very Weak** (Très faible). Pour ce faire :
 - a. Cliquez sur un élément.

REMARQUE : Lorsque vous cliquez sur un élément, vous serez automatiquement redirigé vers la page de configuration appropriée.

- b. À partir de la page des paramètres de sécurité de l'élément, modifiez les paramètres nécessaires puis cliquez sur **Apply** (Appliquer) une fois terminé.
 - c. Revenez à la page **Router Security Assessment** (Évaluation de la sécurité du routeur), puis cliquez sur **Close** (Fermer) pour quitter la page.
5. Pour configurer automatiquement les paramètres de sécurité, cliquez sur **Secure Your Router** (Sécuriser votre routeur).
 6. Cliquez sur **OK** lors de l'apparition du message de confirmation.

Blocage de sites malveillants

Cette fonctionnalité restreint l'accès aux sites internet malveillants connus figurant sur une base de données dans le Cloud pour une protection toujours à jour.

REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer le blocage des sites malveillants :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale **AiProtection**, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau de blocage des sites malveillants, cliquez sur **ON** (OUI).

Two-Way IPS

Two-Way IPS (Système de Prévention des Intrusions ou "Intrusion Prevention System" en anglais) protège votre routeur des attaques réseau en bloquant les paquets entrants malveillants et en détectant les paquets sortants suspects.

REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer Two-Way IPS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale **AiProtection**, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau **Two-Way IPS**, cliquez sur **ON** (OUI).

Protection et blocage des périphériques infectés

Cette fonctionnalité permet d'empêcher les périphériques infectés de communiquer des informations personnelles ou un état infecté à des entités tierces.

REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer la protection et le blocage des périphériques infectés :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale **AiProtection**, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau de protection et de blocage des périphériques infectés, cliquez sur **ON** (OUI).

Pour configurer les préférences d'envoi d'alertes :

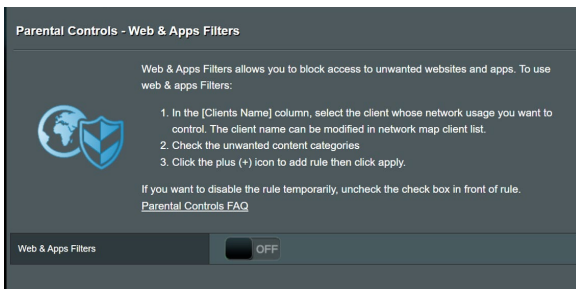
1. À partir du panneau de protection et de blocage des périphériques infectés, cliquez sur **Alert Preference** (Préférence d'envoi d'alertes).
2. Sélectionnez ou entrez le nom du service de messagerie électronique, l'adresse e-mail et le mot de passe, puis cliquez sur **Apply** (Appliquer).

3.4.2 Configurer le contrôle parental

Le contrôle parental permet de contrôler le temps d'accès à Internet ou de limiter le temps d'accès au réseau d'un client.

Pour accéder à la page principale du contrôle parental :

À partir du volet de navigation, cliquez sur **General** (Général) > **Parental Controls** (Contrôles parentaux).



Filtrage de sites et d'applications

Le filtrage de sites et d'applications est une fonctionnalité du contrôle parental qui permet de bloquer l'accès à certains sites internet ou applications indésirables.

Pour configurer le filtrage de sites et d'applications :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Parental Controls** (Contrôles parentaux).
2. À partir du panneau **Web & Apps Filters** (Filtrage de sites et d'applications), cliquez sur **ON** (OUI).
3. Cliquez sur **I agree** (J'accepte) pour accepter le contrat de licence pour utilisateur final.
4. Dans la colonne **Client List** (Liste des clients), sélectionnez un client ou tapez son nom dans la liste déroulante.
5. Dans la colonne **Content Category** (Catégorie de contenu), sélectionnez le contenu à filtrer : **Adult** (Adulte), **Instant Message and Communication** (Messagerie instantanée et communications), **P2P and File Transfer** (P2P et transfert de fichiers) et **Streaming and Entertainment** (Streaming et divertissement).
6. Cliquez sur  pour ajouter le profil du client.
7. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Parental Controls - Web & Apps Filters

Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:



1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.
[Parental Controls FAQ](#)

Web & Apps Filters

ON

Client List (Max Limit : 64)

<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	<input type="text" value="192.168.1.100"/>	<ul style="list-style-type: none"><input type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.<input type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.<input type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	<input type="button" value="+"/>
No data in table.			

Apply

Planification horaire

La planification horaire vous permet de limiter le temps d'accès d'un client au réseau.

REMARQUE : Vérifiez que la date et l'heure du système sont bien synchronisés avec le serveur NTP.

Parental Controls - Time Scheduling

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

Enable block all devices OFF

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 ON

System Time **Thu, Sep 21 12:34:41 2023**

Client List (Max Limit : 64)

Select	Client Name (MAC Address)	Time Management	Add / Delete
all		-	+

No data in table.

Apply

Pour configurer la planification horaire :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Parental Controls** (Contrôle parental) > **Time Scheduling** (Planification horaire).
2. À partir du panneau **Enable Time Scheduling** (Activer la planification horaire), cliquez sur **ON** (OUI).
3. Dans la colonne **Clients Name** (Nom des clients), sélectionnez un client ou tapez son nom dans la liste déroulante.

REMARQUE : Vous pouvez aussi entrer l'adresse MAC du client dans la colonne **Client MAC Address** (Adresse MAC du client). Assurez-vous que le nom du client ne possède pas de caractères spéciaux ou d'espaces car cela peut causer un dysfonctionnement du routeur.

4. Cliquez sur pour ajouter le profil du client.
5. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

3.5 Pare-feu

Le routeur WiFi peut faire office de pare-feu matériel sur votre réseau.

REMARQUE : Le pare-feu est activé par défaut sur votre routeur.

3.5.1 Paramètres de base

Firewall

General

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.

[DoS Protection FAQ](#)

Enable Firewall Yes No

Enable DoS protection Yes No

Logged packets type None

Respond ICMP Echo (ping) Request from WAN Yes No

Basic Config

Enable IPv4 inbound firewall rules Yes No

Inbound Firewall Rules: (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
		TCP	

No data in table.

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (2001::1111:2222:3333:64 for example)

Basic Config

Enable IPv6 Firewall Yes No

Famous Server List Please select

Inbound Firewall Rules: (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
				TCP	

No data in table.

Apply

Pour configurer les paramètres de base du pare-feu :

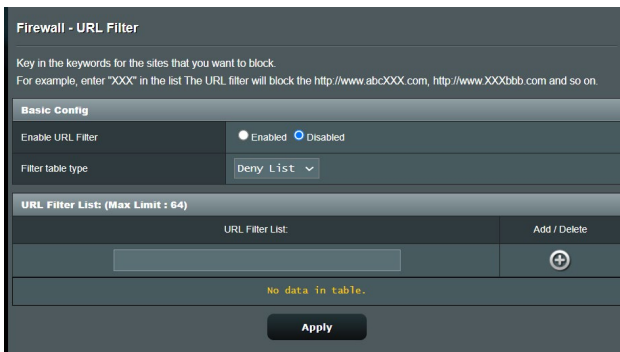
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > **General** (Général).
2. Dans le champ **Enable Firewall** (Activer le pare-feu), cochez **Yes** (Oui).
3. Dans le champ **Enable DoS Protection** (Activer la protection contre les attaques DoS), cochez **Yes** (Oui) pour protéger votre réseau contre les attaques de déni de service (DoS). Veuillez toutefois noter que l'activation de cette fonctionnalité peut affecter les performances du routeur.

4. Vous pouvez aussi surveiller l'échange de paquets entre le réseau local (LAN) et le réseau étendu (WAN). Dans le menu déroulant Logged packets (Types de paquets), sélectionnez **Dropped** (Ignorés), **Accepted** (Acceptés) ou **Both** (Les deux).
5. Cliquez sur **Apply** (Appliquer).


3.5.2 Filtrage d'URL

Le routeur WiFi offre la possibilité de filtrer l'accès à certaines adresses internet (URL).

REMARQUE : Le filtrage d'URL est fondé sur les requêtes DNS. Si un client du réseau a déjà accédé à un site internet, celui-ci ne sera pas bloqué (un cache DNS stockant une liste des sites internet visités). Pour résoudre ce problème, effacez la mémoire cache dédiée au DNS avant d'utiliser le filtrage d'URL.

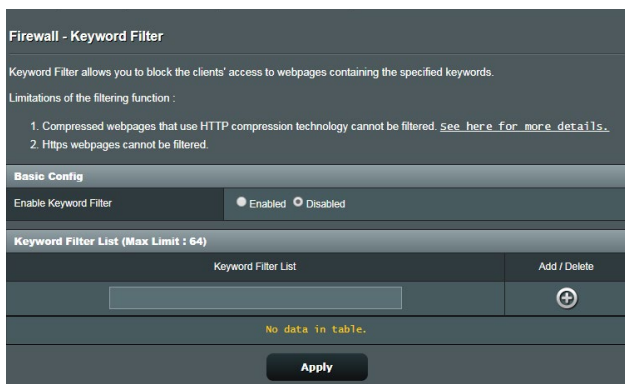


Pour configurer le filtrage d'URL :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > **URL Filter** (Filtrage d'URL).
2. Dans le champ Enable URL Filter (Activer le filtrage d'URL), cochez **Enabled** (Activer).
3. Entrez une adresse URL et cliquez sur le bouton .
4. Cliquez sur **Apply** (Appliquer).

3.5.3 Filtrage de mots-clés

Vous pouvez bloquer l'accès à des sites internet contenant certains mots clés.



Pour configurer le filtrage de mots clés :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > **Keyword Filter** (Filtrage de mots clés).
2. Dans le champ Enable Keyword Filter (Activer le filtrage de mots clés), cochez **Enabled** (Activer).
3. Entrez un mot ou une phrase, puis cliquez sur le bouton **Add** (Ajouter).
4. Cliquez sur **Apply** (Appliquer).

REMARQUES :

- Le filtrage de mots clés est fondé sur les requêtes DNS. Si un client du réseau a déjà accédé à un site internet, celui-ci ne sera pas bloqué (un cache DNS stockant une liste des sites internet visités). Pour résoudre ce problème, effacez la mémoire cache dédiée au DNS avant d'utiliser le filtrage de mots clés.
 - Les pages internet compressées au format HTTP ne peuvent pas être filtrées. Les pages utilisant le standard HTTPS ne peuvent également pas être filtrées.
-

3.5.4 Filtrage de services réseau

Le filtrage de services réseau permet de bloquer l'échange de paquets entre le réseau local (LAN) et le réseau étendu (WAN), et de restreindre l'accès des clients à certains services internet (ex : Telnet ou FTP).

Firewall - Network Services Filter

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

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use 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

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter Yes No

Filter table type

Well-Known Applications

Date to Enable LAN to WAN Filter Mon Tue Wed Thu Fri

Time of Day to Enable LAN to WAN Filter : - :

Date to Enable LAN to WAN Filter Sat Sun

Time of Day to Enable LAN to WAN Filter : - :

Filtered ICMP packet types

Network Services Filter Table (Max Limit : 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>

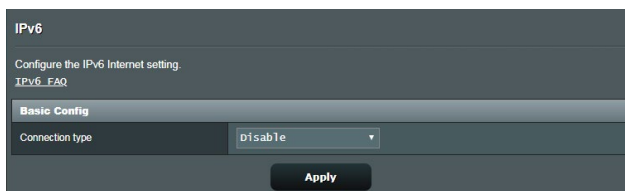
No data in table.

Pour configurer le filtrage de services réseau :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > **Network Services Filter** (Filtrage de services réseau).
2. Dans le champ Enable Network Services Filter (Activer le filtrage de services réseau), cochez **Yes** (Oui).
3. Sélectionnez ensuite le type de filtrage. **Deny** (Refuser) bloque les services réseau spécifiés. **Allow** (Accepter) limite l'accès à certains services réseau uniquement.
4. Si nécessaire, spécifiez les jours et les horaires d'activité du filtre.
5. Remplissez ensuite le tableau de filtrage. Cliquez sur le bouton .
6. Cliquez sur **Apply** (Appliquer).

3.6 IPv6 (Protocole IPv6)

Ce routeur WiFi est compatible avec le protocole d'adressage IPv6, un protocole disposant d'un espace d'adressage bien plus important que l'IPv4. Cette norme n'étant pas encore largement utilisée, contactez votre FAI pour en confirmer sa prise en charge. Contactez votre FAI si votre connexion Internet est compatible IPv6.



Pour configurer le protocole IPv6 :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **IPv6**.
2. Dans le menu **Connection Type** (Type de connexion), sélectionnez le type de connexion. Les options de configuration apparaissant ensuite peuvent varier selon le type de connexion choisi.
3. Entrez les informations IPv6 et de serveur DNS.
4. Cliquez sur **Apply** (Appliquer).

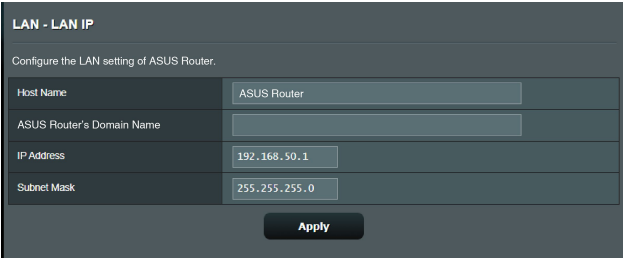
REMARQUE : Consultez votre FAI en cas de doute sur les informations nécessaires à la configuration de l'adressage IPv6.

3.7 Réseau local (LAN)

3.7.1 Adresse IP du routeur

L'onglet dédié à l'adresse IP du réseau local fait référence à l'adresse IP du routeur WiFi.

REMARQUE : Toute modification de l'adresse IP locale influence certains réglages du serveur DHCP.



The screenshot shows the 'LAN - LAN IP' configuration page. At the top, it says 'Configure the LAN setting of ASUS Router.' Below this, there are four input fields: 'Host Name' with the value 'ASUS Router', 'ASUS Router's Domain Name' (empty), 'IP Address' with the value '192.168.50.1', and 'Subnet Mask' with the value '255.255.255.0'. At the bottom right, there is an 'Apply' button.

Pour modifier l'adresse IP du réseau local :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > **LAN IP** (Adresse IP locale).
2. Remplissez les champs **IP address** (Adresse IP) et **Subnet Mask** (Masque de sous-réseau).
3. Une fois terminé, cliquez sur **Apply** (Appliquer).

3.7.2 Serveur DHCP

Votre routeur WiFi utilise le protocole DHCP pour affecter automatiquement des adresses IP aux clients du réseau. Vous pouvez néanmoins spécifier une plage d'adresses IP et le délai du bail.

LAN - DHCP Server

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 informs the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.
Manually Assigned IP around the DHCP list FAQ

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

Apply

Pour configurer le serveur DHCP :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > **DHCP Server** (Serveur DHCP).
2. Dans le champ **Enable the DHCP Server** (Activer le serveur DHCP), cochez **Yes** (Oui).
3. Dans la zone de texte **Domain Name** (Nom de domaine), attribuez un nom de domaine au routeur WiFi.

4. Dans le champ **IP Pool Starting Address** (Adresse de départ de plage IP), entrez l'adresse IP de départ.
5. Dans le champ **IP Pool Ending Address** (Adresse de fin de plage IP), entrez l'adresse IP de fin.
6. Dans le champ **Lease Time** (Délai du bail), spécifiez le délai d'expiration (en secondes) du bail des adresses IP. Lorsque ce délai est atteint, le serveur DHCP renouvellera les adresses IP affectées.

REMARQUES :

- Il est recommandé d'utiliser un format d'adresse IP de type 192.168.50.xxx (où xxx correspond à une valeur numérique comprise entre 2 et 254) lors de la saisie d'une plage d'adresses IP.
 - L'adresse de départ d'une plage IP ne peut pas être supérieure à l'adresse de fin.
-
7. Dans la zone **DNS and WINS Server Settings** (Configuration des serveurs DNS et WINS), entrez, si nécessaire, les adresses dédiées au serveur DNS et WINS.
 8. Vous pouvez également affecter manuellement des adresses IP aux clients de votre réseau WiFi. Dans le champ **Enable Manual Assignment** (Activer l'affectation manuelle), cochez **Yes** (Oui) pour affecter manuellement une IP à une adresse MAC spécifique du réseau. Jusqu'à 32 adresses MAC peuvent être ajoutées à la liste DHCP.

3.7.3 Routage

Si votre réseau est composé de plus d'un routeur WiFi, vous pouvez configurer un tableau de routage permettant de partager le même service internet.

REMARQUE : Il est recommandé de ne pas modifier les paramètres de routage par défaut, sauf si vous possédez les connaissances suffisantes pour le faire.

LAN - Route

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

Basic Config

Enable static routes Yes No

Static Route List (Max Limit : 32)

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

No data in table.

Apply

Pour configurer le tableau de routage :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > **Route** (Routage).
2. Dans le champ **Enable static routes** (Activer le routage statique), cochez **Yes** (Oui).
3. Dans la zone **Static Route List** (Liste de routage statique), entrez les informations réseau des autres points d'accès. Cliquez sur le bouton **+** ou sur **-** pour ajouter ou supprimer un dispositif de la liste.
4. Cliquez sur **Apply** (Appliquer).

3.7.4 Télévision sur IP

Le routeur WiFi prend en charge la connexion à un service de télévision sur IP. L'onglet IPTV (Télévision sur IP) offre divers paramètres nécessaires à la configuration des protocoles IPTV, VoIP, multi-diffusion et UDP. Contactez votre fournisseur d'accès internet pour plus de détails sur ce service.

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there is a note: '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.' Below this, the 'LAN Port' section contains two dropdown menus: 'Select ISP Profile' set to 'None' and 'Choose IPTV STB Port' set to 'None'. The 'Special Applications' section contains three settings: 'Use DHCP routes' set to 'Microsoft', 'Enable multicast routing (IGMP Proxy)' set to 'Disable', and 'UDP Proxy (Udpxy)' set to '0'. An 'Apply' button is located at the bottom right of the configuration area.

LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None

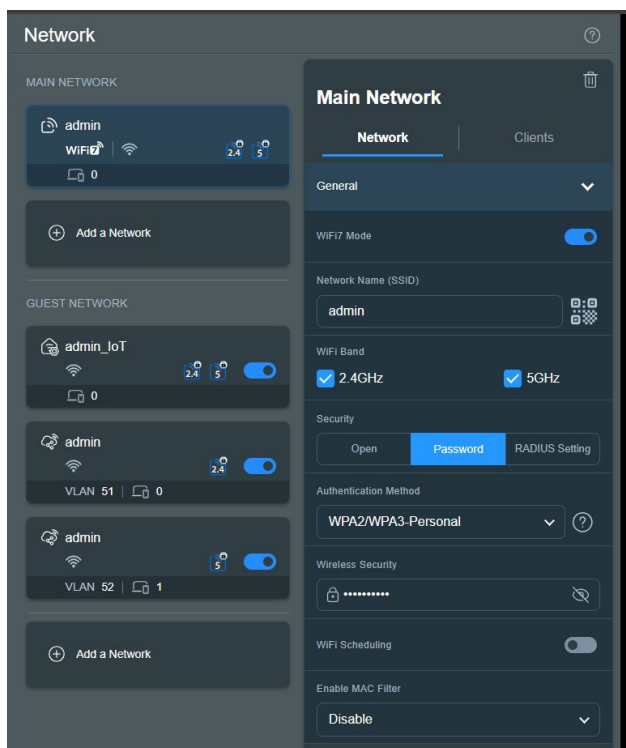
Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
UDP Proxy (Udpxy)	0

Apply

3.8 Réseau

3.8.1 Réseau principal - Filtrage d'adresses MAC

Le filtrage d'adresses MAC offre un certain contrôle sur les paquets transmis vers une adresse MAC spécifique de votre réseau WiFi.





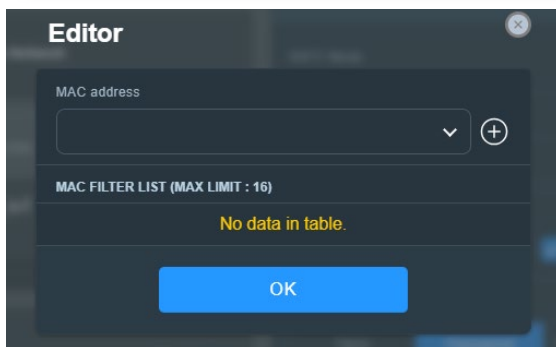
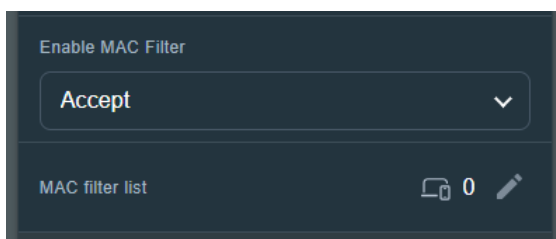
Pour configurer le filtrage d'adresses MAC :

1. À partir du volet de navigation, accédez à **Général > Réseau > Réseau principal** et sélectionnez le nom (SSID) du réseau principal.
2. Dans le menu déroulant **Enable Mac Filter** (Activer le filtrage d'adresses MAC), sélectionnez **Accept** (Accepter) ou **Reject** (Rejeter).

- Sélectionnez **Accept** (Accepter) pour autoriser les appareils faisant partie de la liste de filtrage d'adresses MAC à accéder au réseau WiFi.
- Sélectionnez **Reject** (Rejeter) pour ne pas autoriser les appareils faisant partie de la liste de filtrage d'adresses MAC à accéder au réseau WiFi.

REMARQUE : Sélectionnez **Désactiver** si vous souhaitez désactiver le **filtrage d'adresses MAC**.

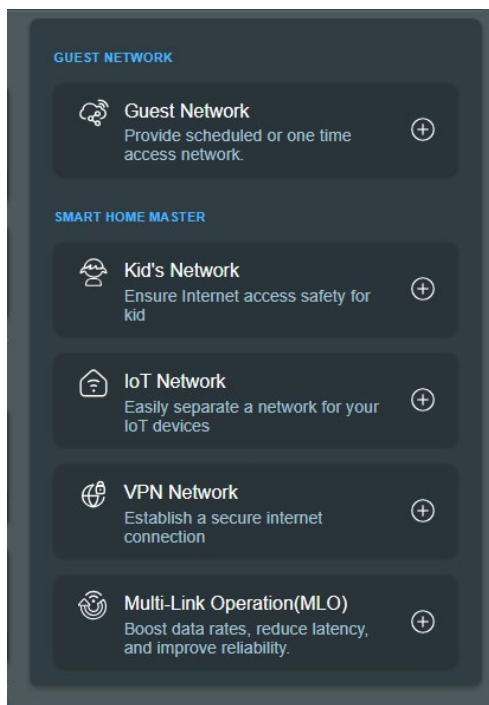
4. Dans la liste de filtrage d'adresse MAC, cliquez sur  pour accéder à la page **Editor** (Éditeur), puis cliquez sur  et saisissez l'adresse MAC du périphérique sans fil.
5. Cliquez sur **OK**.



3.8.2 Réseau invité

3.8.2.1 Réseau invité

Un réseau invité permet d'offrir une connexion internet aux utilisateurs temporaires via l'accès à un SSID ou réseau séparé, et restreint l'accès au réseau local privé.



REMARQUE : Le ZenWiFi BD4 prend en charge jusqu'à trois SSID pour le réseau invité.

Pour créer un réseau invité :

1. À partir du volet de navigation, accédez à **General** (Général) > **Network** (Réseau) > **Guest Network** (Réseau invité) > **Add a Network** (Ajouter un réseau).
2. Sélectionnez **Réseau invité** et attribuez un nom à votre réseau temporaire dans le champ **Network Name (SSID)** (Nom du réseau (SSID)).

3. Sélectionnez une méthode d'authentification sous **Security** (Sécurité).
4. Spécifiez l'heure d'accès ou choisissez **Scheduled** (Planifié) pour ajouter un profil de planification en ligne.
5. Sélectionnez la **WiFi Band** (Bande WiFi) pour le réseau invité que vous souhaitez créer.
6. Activez ou désactivez le **Bandwidth Limiter** (Limiteur de bande passante).
7. Activez ou désactivez **Access Intranet** (Accès Internet).
8. Une fois terminé, cliquez sur **Apply** (Appliquer).

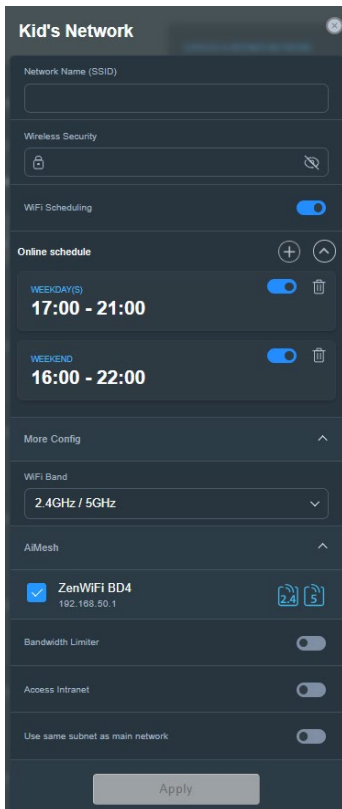
The screenshot shows the 'Guest Network' configuration page. At the top, there is a 'Network Name (SSID)' field. Below it, the 'Security' section has two options: 'Open' (selected) and 'Password'. The 'WiFi Scheduling' section is toggled on, with 'One Time Access' selected over 'Scheduled'. Under 'One Time Access', there are buttons for '30 mins', '1 hr(s)', '2 hr(s)' (selected), '4 hr(s)', '6 hr(s)', and 'Custom'. The 'More Config' section is expanded to show 'WiFi Band' set to '2.4GHz / 5GHz'. The 'AiMesh' section shows 'ZenWiFi BD4' (192.168.50.1) with '2.4' and '5' frequency icons. At the bottom, there are three toggle switches for 'Bandwidth Limiter', 'Access Intranet', and 'Use same subnet as main network', all of which are currently turned off. An 'Apply' button is located at the very bottom of the form.

3.8.2.2 Maître domotique (Smart Home Master)

Smart Home Master (maître domotique) est un outil puissant et convivial pour la segmentation du réseau. Il simplifie le processus de création et de gestion de sous-réseaux avancés, tels que la création d'un SSID dédié pour les appareils de vos enfants, la connexion à un VPN via un sous-réseau dédié ou même la création d'un SSID sécurisé pour tous vos appareils IoT.

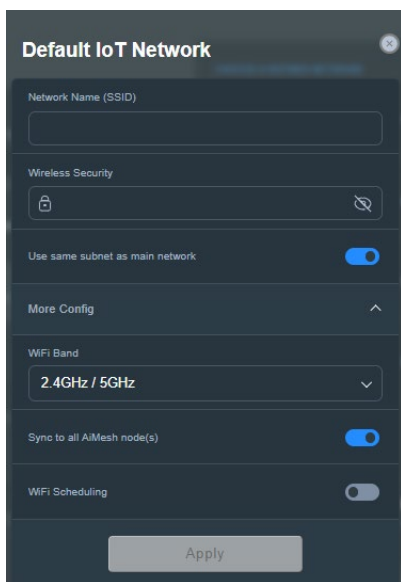
Pour créer un réseau pour enfants :

1. À partir du volet de navigation, accédez à **General** (Général) > **Network** (Réseau) > **Guest Network** (Réseau invité) > **Add a Network** (Ajouter un réseau).
2. Sélectionnez **Kid's Network** (Réseau pour enfants) et attribuez un nom de réseau et une clé de sécurité dans les champs **Network Name (SSID)** (Nom du réseau (SSID)) et **Wireless Security** (Sécurité WiFi).
3. Personnalisez l'heure d'accès à Internet dans le champ **Online schedule** (Planification en ligne).
4. Sélectionnez la **WiFi Band** (Bande WiFi) pour le réseau pour enfants que vous souhaitez créer.
5. Activez ou désactivez le **Bandwidth Limiter** (Limiteur de bande passante).
6. Activez ou désactivez **Access Intranet** (Accès Internet).
7. Une fois terminé, cliquez sur **Apply** (Appliquer).



Pour créer un réseau IoT :

1. À partir du volet de navigation, accédez à **General** (Général) > **Network** (Réseau) > **Guest Network** (Réseau invité) > **Add a Network** (Ajouter un réseau).
2. Sélectionnez **IoT Network** (Réseau IoT) et attribuez un nom de réseau et une clé de sécurité dans les champs **Network Name (SSID)** (Nom du réseau (SSID)) et **Wireless Security** (Sécurité WiFi).
3. Sélectionnez la **WiFi Band** (Bande WiFi) pour le réseau pour enfants que vous souhaitez créer.
4. Personnalisez le temps d'accès à Internet en activant **WiFi Scheduling** (Planification WiFi).
5. Une fois terminé, cliquez sur **Apply** (Appliquer).



Pour créer un réseau VPN :

1. À partir du volet de navigation, accédez à **General** (Général) > **Network** (Réseau) > **Guest Network** (Réseau invité) > **Add a Network** (Ajouter un réseau).
2. Sélectionnez **VPN Network** (Réseau VPN) et attribuez un nom de réseau et une clé de sécurité dans les champs **Network Name (SSID)** (Nom du réseau (SSID)) et **Wireless Security** (Sécurité WiFi).
3. Si vous n'avez pas configuré de profil VPN pour le serveur VPN ou le client VPN, cliquez sur **Go Setting** (Configurer) pour créer un profil VPN.
4. Sélectionnez la **WiFi Band** (Bande WiFi) pour le réseau VPN que vous souhaitez créer.
5. Personnalisez le temps d'accès à Internet en activant **WiFi Scheduling** (Planification WiFi).
6. Activez ou désactivez le **Bandwidth Limiter** (Limiteur de bande passante).
7. Activez ou désactivez **Access Intranet** (Accès Internet).
8. Une fois terminé, cliquez sur **Apply** (Appliquer).



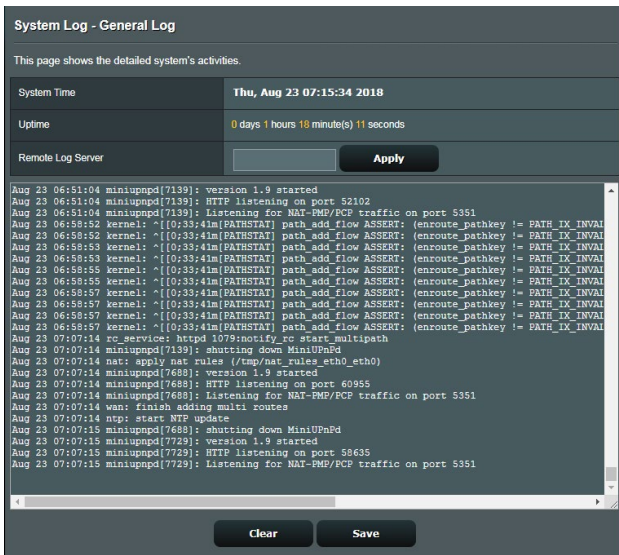
3.9 Journal système

Le journal système contient les activités du réseau enregistrées par le routeur.

REMARQUE : Le journal système est réinitialisé à chaque extinction ou redémarrage du routeur.

Pour afficher le journal système :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **System Log** (Journal système).
2. Les activités du réseau sont répertoriées dans les 5 onglets suivants :
 - General Log (Général)
 - Wireless Log (Réseau WiFi)
 - DHCP Leases (Baux DHCP)
 - IPv6 (Protocole IPv6)
 - Routing Table (Tableau de routage)
 - Port Forwarding (Redirection de port)
 - Connexions



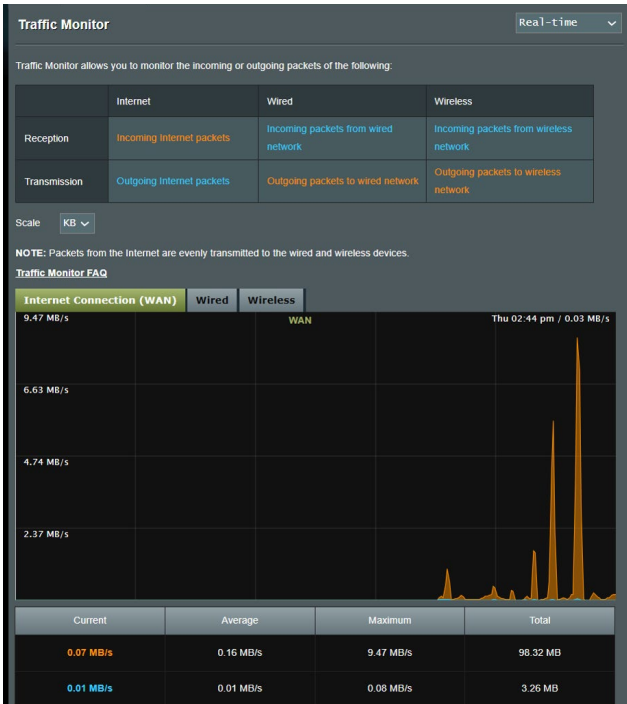
The screenshot displays the 'System Log - General Log' interface. At the top, it indicates the system time as 'Thu, Aug 23 07:15:34 2018' and the uptime as '0 days 1 hours 18 minute(s) 11 seconds'. There is a 'Remote Log Server' field with an 'Apply' button. The main area contains a scrollable log of system events, including:

```
Aug 23 06:51:04 miniupnpd[7139]: version 1.9 started
Aug 23 06:51:04 miniupnpd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 miniupnpd[7139]: Listening for NAT-FMP/PCP traffic on port 5351
Aug 23 06:58:52 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:53 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:53 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:53 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ~[0:33:41m(PATHSTAT) path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 07:07:14 rc_service: httpd 1079:notify_rc start multipath
Aug 23 07:07:14 miniupnpd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 ntp: apply nat rules (/tmp/nat_rules_etc0_etc0)
Aug 23 07:07:14 miniupnpd[7688]: version 1.9 started
Aug 23 07:07:14 miniupnpd[7688]: HTTP listening on port 60955
Aug 23 07:07:14 miniupnpd[7688]: Listening for NAT-FMP/PCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 ntp: start NTP update
Aug 23 07:07:15 miniupnpd[7688]: shutting down MiniUPnPd
Aug 23 07:07:15 miniupnpd[7729]: version 1.9 started
Aug 23 07:07:15 miniupnpd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 miniupnpd[7729]: Listening for NAT-FMP/PCP traffic on port 5351
```

At the bottom, there are 'Clear' and 'Save' buttons.

3.10 Dispositif d'analyse du trafic

La fonctionnalité de surveillance du trafic vous permet d'évaluer l'usage de la bande passante et la vitesse des connexions internet, du réseau local ou du réseau étendu. Vous pouvez surveiller le trafic du réseau en temps réel ou de manière quotidienne. Le trafic peut aussi être affiché pour les dernières 24 heures.



REMARQUE : Les paquets internet sont transmis de manière égale sur les appareils avec ou sans fil.

3.11 Réseau étendu (WAN)

3.11.1 Connexion internet

L'écran Internet Connection (Connexion internet) vous permet de configurer les paramètres de divers types de connexions au réseau étendu.

WAN - Internet Connection

ASUS Router 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.

Configure the Ethernet WAN settings of ASUS Router.

Basic Config

WAN Connection Type	Automatic IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). WAN Aggregation FAQ</small>

WAN DNS Setting

Default status: Get the DNS IP from your ISP automatically

DNS Server	Assign a DNS service to improve security, block advertisement and gain faster performance. Assign
Forward local domain queries to upstream DNS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNS Rebind protection	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNSSEC support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

DHCP Option

Class-identifier (Option 60)	<input type="text"/>
Client-identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>
Class-identifier (Option 60)	<input type="text"/>
Client-identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>

Account Settings

Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

Special Requirement from ISP

Host Name	<input type="text"/>
MAC Address	<input type="text"/> MAC Clone
DHCP query frequency	Aggressive Mode
Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

Pour configurer les paramètres de connexion au réseau étendu :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **Internet Connection** (Connexion internet).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **WAN Connection Type (Type de connexion au réseau étendu)** : Sélectionnez votre type de connexion internet. Les choix suivants sont disponibles : **Automatic IP** (Adresse IP automatique), **PPPoE**, **PPTP**, **L2TP** et **Fixed IP** (Adresse IP fixe). Consultez votre FAI si le routeur n'est pas en mesure d'établir une connexion à Internet ou si vous n'êtes pas sûr du type de connexion à utiliser.
 - **Enable WAN (Activer le réseau étendu)**: Cochez **Yes** (Oui) pour autoriser un accès internet au routeur. Cochez **No** (Non) pour désactiver l'accès internet.
 - **Enable NAT (Activer le NAT)**: La fonction NAT (Network Address Translation) permet à une adresse IP publique (IP du réseau étendu) d'être utilisée pour fournir un accès internet aux clients disposant d'une adresse IP locale. L'adresse IP privée de chaque client est enregistrée dans le tableau NAT et est utilisée pour le routage des paquets entrants.
 - **Enable UPnP (Activer le protocole UPnP)** : Le protocole UPnP (Universal Plug and Play) permet à de nombreux appareils (routeurs, téléviseurs, systèmes stéréo, consoles de jeu, téléphones portables, etc.) d'être contrôlés par le biais d'un réseau à IP (avec ou sans hub de contrôle central) via une passerelle. Le protocole UPnP connecte des ordinateurs de toute forme, afin d'offrir un réseau fluide pour la configuration distante et le transfert de fichiers. Grâce à l'UPnP, un périphérique réseau peut être automatiquement découvert. Une fois connectés au réseau, les périphériques peuvent être contrôlés à distance pour la prise en charge d'applications P2P, les jeux vidéo, les visioconférences et les serveurs Web ou proxy. Contrairement à la redirection de port, qui implique la configuration manuelle des ports, le protocole UPnP configure automatiquement le routeur de sorte que ce dernier accepte les connexions entrantes avant de rediriger les requêtes vers un client spécifique du réseau local.

- **Enable WAN Aggregation (Activer l'agrégation WAN):**
L'agrégation WAN combine deux connexions pour augmenter la vitesse du réseau étendu (WAN) jusqu'à 2 Gb/s. Connectez le port WAN et le port LAN 4 du routeur aux ports LAN de votre modem.
- **Connect to DNS Server (Obtenir automatiquement l'adresse de serveur DNS):** Permet au routeur d'obtenir automatiquement les adresses des serveurs DNS auprès du FAI. Un DNS est un service permettant de traduire les noms de domaine internet en adresses IP numériques.
- **Authentication:** Authentication (Authentification). Cette option peut être requise par certains FAI. Si nécessaire, consultez votre FAI pour plus de détails.
- **Host Name (Nom d'hôte):** Permet d'attribuer un nom d'hôte au routeur. Ceci peut être requis par votre FAI. Si nécessaire, consultez votre FAI pour plus de détails.
- **MAC Address (Adresse MAC):** Une adresse MAC (Media Access Control) est un identifiant unique attribué aux appareils dotés d'une connectivité WiFi. Certains FAI surveillent l'adresse MAC des appareils se connectant à leur service et peuvent rejeter toute tentative d'un appareil non enregistré d'établir une connexion. Pour surmonter le problème lié à une adresse MAC non enregistrée, vous pouvez :
 - Contacter votre FAI et mettre à jour l'adresse MAC associée à votre abonnement internet.
 - Cloner ou modifier l'adresse MAC de votre routeur WiFi ASUS de sorte que celle-ci corresponde à celle enregistrée auprès de votre FAI.

3.11.2 Dual WAN (Double WAN)

Le réseau Dual WAN vous permet d'acheminer les connexions de deux FAI vers votre routeur, un réseau étendu (WAN) principal et un réseau étendu (WAN) secondaire.

Pour configurer un réseau Dual WAN :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu).
2. Sur le champ **Dual WAN**, basculez l'interrupteur sur **ON** (OUI).
3. Sélectionnez un réseau étendu (WAN) principal et un réseau étendu (WAN) secondaire. Vous pouvez utiliser deux ports WAN/LAN 2.5GbE.
4. Sélectionnez **Fail Over** (Basculement) ou **Load Balance** (Équilibrage de charge).
5. Cliquez sur **Apply** (Appliquer).

REMARQUE : Des explications détaillées sont disponibles dans la FAQ du site de support d'ASUS <https://www.asus.com/fr/support/FAQ/1011719>

WAN - Dual WAN

ZenWiFi BD4 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)

Basic Config

Enable Dual WAN OFF

Primary WAN WAN

Auto Network Detection

Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.

Detect Interval Every seconds

Internet Connection Diagnosis When the current WAN fails continuous times, it is deemed a disconnection.

Network Monitoring DNS Query Ping

Apply

3.11.3 Déclenchement de port

Le déclenchement de port permet d'ouvrir un port entrant pré-déterminé pendant une période limitée lorsqu'un client du réseau local établit une connexion sortante vers un port spécifique. Le déclenchement de port est utilisé dans les cas suivants :

- Plus d'un client local requiert la redirection d'un port d'une même application à un moment différent.
- Une application nécessite des ports entrants spécifiques dissemblables des ports sortants.

WAN - Port Trigger

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	Delete
No data in table					

Pour configurer le déclenchement de port :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **Port Trigger** (Déclenchement de port).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **Enable Port Trigger (Activer le déclenchement de port):** Cochez **Yes** (Oui) pour activer le déclenchement de port.
 - **Well-Known Applications (Applications connues):** Sélectionnez un jeu ou un service internet à ajouter à la liste de déclenchement de port.
 - **Description:** Entrez une description du service/jeu.
 - **Trigger Port (Port de déclenchement):** Entrez le port à déclencher.

- **Protocol (Protocole):** Sélectionnez le protocole TCP ou UDP.
 - **Incoming Port (Port entrant):** Spécifiez le port entrant recevant les données en provenance d'Internet.
 - **Protocol (Protocole):** Sélectionnez le protocole TCP ou UDP.
-

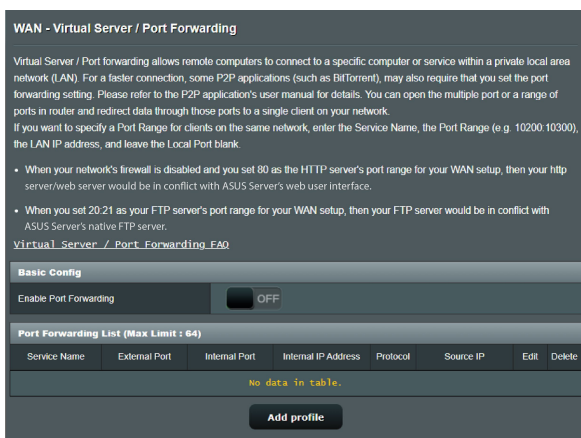
REMARQUES :

- Lors de la connexion à un serveur IRC, un PC client établit une connexion sortante par le biais de la plage de déclenchement 66660-7000. Le serveur IRC répond en vérifiant le nom d'utilisateur et en créant une nouvelle connexion au PC client via un port entrant.
 - Si le déclenchement de port est désactivé, le routeur met fin à la connexion car celui-ci n'est pas en mesure de déterminer quel ordinateur souhaite se connecter à un serveur IRC. Lorsque le déclenchement de port est activé, le routeur affecte un port entrant dédié à la réception des paquets. Ce port entrant est fermé après un certain temps car le routeur ne peut pas déterminer le moment auquel l'application a été arrêtée.
 - Le déclenchement de port ne permet qu'à un seul client à la fois d'utiliser un service et un port entrant spécifiques.
 - Il n'est pas possible d'utiliser la même application pour déclencher un port sur plus d'un ordinateur à la fois. Le routeur ne redirigera le port que vers le dernier ordinateur à avoir envoyé une requête.
-

3.11.4 Serveur virtuel et redirection de port

La redirection de port est une méthode permettant de diriger le trafic internet vers un port ou une plage de ports spécifique(s), et ensuite vers un ou plusieurs clients du réseau local. L'utilisation de la redirection de port sur le routeur autorise des ordinateurs extérieurs à un réseau d'accéder à des services répartis sur plusieurs ordinateurs de ce réseau.

REMARQUE : Lorsque la redirection de port est activée, le routeur ASUS bloque le trafic internet entrant non sollicité et n'autorise que les réponses à partir des requêtes sortantes en provenance du réseau local. Le client réseau ne dispose pas d'un accès direct à Internet, et vice versa.



Pour utiliser la redirection de port :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **Virtual Server / Port Forwarding** (Redirection de port).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **OK**.
 - **Enable Port Forwarding (Activer la redirection de port):** Basculez sur **ON** (OUI) pour activer la redirection de port.
 - **Famous Server List (Liste des serveurs connus):** Déterminez à quel type de service vous souhaitez accéder.

- **Famous Game List (Liste de jeux):** Cet élément identifie les ports nécessaires pour permettre aux jeux en ligne populaires de fonctionner correctement.
- **FTP Server Port (Port Serveur FTP):** Évitez d'attribuer la plage de ports 20:21 à votre serveur FTP car cela entraînerait un conflit avec la configuration FTP native du routeur.
- **Service Name (Nom du service):** Spécifiez le nom du service.
- **Port Range (Plage de ports):** Si vous souhaitez spécifier une plage de ports pour des clients du même réseau, entrez le nom du service, la plage de ports (ex : 10200:10300), l'adresse IP locale et laissez le champ dédié au port local vide. Le champ spécifique à la plage de ports prend en charge plusieurs formats : 300:350, 566,789 ou 1015:1024,3021.

REMARQUES :

- Lorsque le pare-feu du réseau est désactivé et que vous utilisez le port 80 pour le protocole HTTP du réseau étendu, votre serveur http/Web entrera en conflit avec l'interface de gestion du routeur.
- Un réseau utilise les ports pour l'échange de données, chaque port étant doté d'une valeur numérique et d'une tâche spécifique. Par exemple, le port 80 est utilisé pour le protocole HTTP. Un port spécifique ne peut être utilisé que pour une seule application ou service à la fois. Ainsi, deux ordinateurs ne peuvent pas accéder simultanément aux données via un même port. Il n'est, par exemple, pas possible pour deux ordinateurs d'utiliser la redirection de port sur le port 100 au même moment.

-
- **Local IP (Adresse IP locale):** Adresse IP locale du client.

REMARQUE : Utilisez une adresse IP statique pour le client local afin que la redirection de port puisse fonctionner correctement. Consultez la section **3.8 Réseau local** pour plus de détails.

- **Local Port (Port local):** Entrez un numéro de port spécifique dédié à la redirection des paquets. Laissez ce champ vide si vous souhaitez que les paquets entrants soient redirigés vers une plage de ports spécifique.
- **Protocol (Protocole):** Sélectionnez un protocole. En cas d'incertitude, sélectionnez **BOTH** (Les deux).

Pour vérifier que la redirection de port a bien été configurée :

- Vérifiez que votre serveur ou que l'application est configuré(e) et prêt(e) à être utilisé(e).
- Un client en dehors du réseau local mais ayant accès à Internet (ou "Client internet") est nécessaire. Ce client ne doit pas être connecté au routeur ASUS.
- Sur le client internet, utilisez l'adresse IP du réseau étendu (WAN) du routeur pour accéder au serveur. Si la redirection de port fonctionne correctement, vous serez en mesure d'accéder aux fichiers ou aux applications souhaités.

Différences entre le déclenchement et la redirection de port :

- Le déclenchement de port peut être utilisé sans spécifier d'adresse IP locale. Contrairement à la redirection de port, nécessitant une adresse IP statique, le déclenchement de port autorise la redirection dynamique de port par le biais du routeur. Des plages de ports pré-déterminées sont configurées pour accepter les connexions entrantes pendant une période de temps spécifique. La redirection de port permet à plusieurs ordinateurs d'exécuter des applications nécessitant normalement la redirection manuelle des mêmes ports sur chaque ordinateur du réseau.
- Le déclenchement de port est plus sûr que la redirection de port dans la mesure où les ports entrants ne sont pas constamment ouverts. En effet, ceux-ci ne sont ouverts que lorsqu'une application effectue une connexion sortante par le biais du port déclencheur.

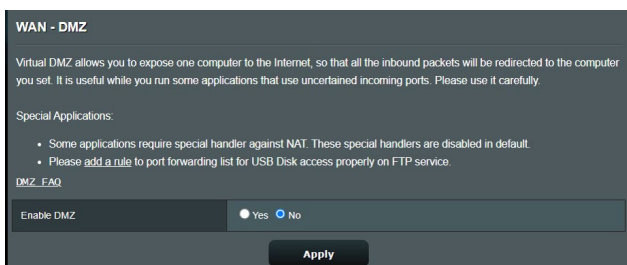
3.11.5 Zone démilitarisée

La zone démilitarisée (ou DMZ en anglais) est un sous-réseau exposant un client à Internet pour lui permettre de recevoir tous les paquets entrants acheminés sur le réseau local.

Le trafic en provenance d'Internet est normalement rejeté et acheminé vers un client spécifique si la redirection ou le déclenchement de port a été configuré sur le réseau. En configuration à zone démilitarisée, un client réseau reçoit tous les paquets entrants.

Le déploiement de cette fonctionnalité sur un réseau est particulièrement utile lorsque vous souhaitez ouvrir des ports entrants ou héberger un nom de domaine ou un serveur de messagerie électronique.

AVERTISSEMENT : L'ouverture de tous les ports d'un client au trafic internet rend le réseau vulnérable aux attaques extérieures. Veuillez prendre en compte les risques encourus lors de la configuration d'une zone démilitarisée.



Pour configurer la zone démilitarisée :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **DMZ** (Zone démilitarisée).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **IP address of Exposed Station (Adresse IP du client) :** Entrez dans ce champ l'adresse IP du client hébergeant le service DMZ et exposé à Internet. Vérifiez que le client serveur possède une adresse IP statique.

Pour désactiver la zone démilitarisée :

1. Effacez l'adresse IP du client du champ **IP address of Exposed Station** (Adresse IP du client).
2. Une fois terminé, cliquez sur **Apply** (Appliquer).

3.11.6 Service DDNS

La configuration d'un serveur DDNS (DNS dynamique) vous permet d'accéder au routeur en dehors de votre réseau par le biais du service DDNS d'ASUS ou d'une société tierce.

WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.asus.com <input type="button" value="Deregister"/>
Host Name	A8878A175D4A6FD54D2E68D6195D85EF7.asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None

Pour configurer le service DDNS :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **DDNS**.
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **Enable the DDNS Client (Activer le client DDNS)**: Active l'accès à distance du routeur ASUS par le biais d'un nom de serveur DNS plutôt que de l'adresse IP du réseau étendu (WAN).
 - **Server (Serveur) et Host Name (Nom d'hôte)**: Sélectionnez l'une des options disponibles. Si vous souhaitez utiliser le service de DDNS d'ASUS, spécifiez le nom d'hôte au format xxx.asuscomm.com (xxx correspondant à votre nom d'hôte).
 - Si vous choisissez un service DDNS différent, cliquez sur **Essai gratuit** pour être redirigé vers la page Web du service sélectionné. Remplissez les champs Nom d'utilisateur, Adresse e-mail, Mot de passe et Clé DDNS.

- **Enable wildcard (Utiliser une Wildcard):** Activez la Wildcard si le service DDNS utilisé requiert une Wildcard.

REMARQUES :

Le service DDNS ne peut pas fonctionner sous les conditions suivantes :

- Le routeur WiFi utilise une adresse IP du réseau étendu (WAN) privée (de type 192.168.x.x, 10.x.x.x ou 172.16.x.x).
 - Le routeur fait partie d'un réseau utilisant plusieurs tableaux NAT.
-

3.11.7 NAT Passthrough

La fonction NAT Passthrough permet à une connexion VPN (réseau privé virtuel) d'être acheminée vers les clients du réseau par le biais du routeur. Les fonctionnalités PPTP Passthrough, L2TP Passthrough, IPsec Passthrough et RTSP Passthrough sont activées par défaut.

Pour activer ou désactiver la fonction NAT Passthrough, allez dans **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **NAT Passthrough**. Une fois terminé, cliquez sur **Apply** (Appliquer).

WAN - NAT Passthrough	
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

3.12 WiFi

3.12.1 WPS

WPS (WiFi Protected Setup) est une norme de sécurité simplifiant la connexion d'un appareil à un réseau WiFi. Vous pouvez utiliser la fonctionnalité WPS par le biais d'un code de sécurité ou du bouton WPS dédié.

REMARQUE : Vérifiez que votre périphérique WiFi soit compatible avec la norme WPS avant de tenter d'utiliser cette fonctionnalité.

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/> ON
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled <input type="button" value="Reset"/> <small>Pressing the reset button resets the network name (SSID) and WPA encryption key.</small>
AP PIN Code	<input type="text" value="51246044"/>

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: Push button Client PIN Code

Pour activer et utiliser la fonctionnalité WPS sur votre réseau WiFi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **WPS**.
2. Déplacez l'interrupteur sur **ON** (OUI) pour activer la fonctionnalité WPS.

3. Par défaut, la norme WPS utilise la bande de fréquence 2,4 GHz. Si vous souhaitez plutôt utiliser la bande à 5 GHz, déplacez l'interrupteur sur **OFF** (Désactiver), cliquez sur le bouton **Switch Frequency** (Changer de fréquence) dans le champ **Current Frequency** (Fréquence actuelle), puis déplacez de nouveau l'interrupteur sur **ON** (OUI).

REMARQUE : La norme WPS est compatible avec les méthodes d'authentification à système ouvert, WPA-Personal et WPA2-Personal. Les chiffrements à clés partagées, WPA-Enterprise, WPA2-Enterprise et RADIUS ne sont pas pris en charge.

3. Dans le champ WPS Method (Méthode de connexion WPS), sélectionnez **Push Button** (Pression de bouton) ou **Client PIN Code** (Code PIN). Si vous souhaitez utiliser le bouton WPS, continuez à l'étape 4. Si vous optez plutôt pour le code PIN, passez directement à l'étape 5.
4. Pour utiliser le bouton WPS :
 - a. Cliquez sur **Start** (Démarrer) ou sur le bouton WPS placé à l'arrière du routeur.
 - b. Appuyez ensuite sur le bouton WPS de votre périphérique WiFi. Un logo WPS figure normalement sur ce bouton.

REMARQUE : Inspectez votre périphérique WiFi ou consultez son mode d'emploi pour localiser l'emplacement du bouton WPS.

- c. Le routeur WiFi recherchera automatiquement la présence de dispositifs WPS à proximité. Si aucun appareil WPS n'est détecté, le routeur basculera en mode veille.
5. Pour utiliser un code PIN :
 - a. Munissez-vous du code PIN de votre périphérique WiFi. Celui-ci est généralement situé sur l'appareil lui-même ou dans son mode d'emploi.
 - b. Entrez le code PIN dans le champ réservé à cet effet.
 - c. Cliquez sur **Start** (Démarrer) pour basculer le routeur WiFi en mode d'attente WPS. Le voyant lumineux WPS clignote rapidement trois fois de manière consécutive jusqu'à ce que la connexion WPS soit établie.

3.12.2 Pontage WDS

Le pontage WDS (Wireless Distribution System) permet à votre routeur ASUS de se connecter de manière exclusive à un autre point d'accès WiFi, empêchant d'autres périphériques WiFi ou stations d'établir une connexion au routeur WiFi ASUS. Dans ce scénario d'utilisation, le routeur ASUS peut faire office de répéteur WiFi communiquant avec un autre point d'accès et d'autres clients.

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your ASUS Router to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first. [Click Here to modify.](#) Please refer to this [FAQ](#) for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. [Click Here to modify.](#)

You are currently using the Auto channel. [Click Here to modify.](#)

Basic Config

2.4 GHz MAC	<input type="text" value="c8:7f:54:12:69:c8"/>
5 GHz MAC	<input type="text" value="c8:7f:54:12:69:cc"/>
Band	2.4 GHz ▾
AP Mode	AP Only ▾
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="⊕"/>
No data in table.	

Pour configurer un pont WiFi :


1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **WDS**.
2. Sélectionnez une bande de fréquence WiFi.
3. Dans le champ **AP Mode** (Mode point d'accès), sélectionnez l'une des options suivantes :
 - **AP Only (Point d'accès uniquement)**: Désactive le pontage WiFi.

- **WDS Only (WDS uniquement):** Active le pontage WiFi mais bloque la connexion d'autres périphériques WiFi/clients au routeur.
- **HYBRID (Hybride):** Active le pontage WiFi et autorise la connexion d'autres périphériques WiFi/clients au routeur.

REMARQUE : En mode hybride, les périphériques WiFi connectés au routeur WiFi ASUS ne bénéficieront que de la moitié du débit WiFi du point d'accès.

4. Dans le champ **Connect to APs in list** (Se connecter aux points d'accès de la liste), cliquez sur **Yes** (Oui) si vous souhaitez établir une connexion à un point d'accès distant.
5. Dans le champ **Control Channel** (Canal de contrôle), sélectionnez le canal d'opération du pont WiFi. Choisissez **Auto** pour autoriser le routeur à sélectionner automatiquement le canal générant le moins d'interférences.

REMARQUE : Les canaux disponibles varient en fonction du pays ou de la région.

6. Dans **Remote AP List** (Liste des points d'accès distants), entrez une adresse MAC, puis cliquez sur le bouton **Ajouter**  pour ajouter l'adresse à la liste des points d'accès disponibles.

REMARQUE : Tous les points d'accès ajoutés à la liste doivent posséder le même canal d'opération que celui utilisé par le routeur WiFi ASUS.

7. Cliquez sur **Apply** (Appliquer).

3.12.3 Service RADIUS

Le service RADIUS (Remote Authentication Dial in User Service) offre un niveau de sécurité additionnel lorsque vous sélectionnez la méthode de chiffrement WPA-Enterprise, WPA2-Enterprise ou Radius with 802.1x.

Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	2.4GHz
Server IP Address	<input type="text"/>
Server Port	1812
Connection Secret	<input type="text"/>

Apply

Pour configurer le service RADIUS :

1. Assurez-vous que le mode d'authentification du routeur est bien de type WPA-Enterprise, WPA2-Enterprise ou Radius with 802.1x.
2. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > onglet **RADIUS Setting** (RADIUS).
3. Sélectionnez une bande de fréquence.
4. Dans le champ **Server IP Address** (Adresse IP du serveur), saisissez l'adresse IP du serveur RADIUS.
5. Dans le champ **Connection Secret** (Phrase secrète), affectez le mot de passe d'accès au serveur RADIUS.
6. Cliquez sur **Apply** (Appliquer).

3.12.4 Professionnel

L'onglet Professionnel offre diverses options de configuration avancées.

REMARQUE : Il est recommandé de conserver les valeurs par défaut de cet onglet.

Wireless - Professional	
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.	
Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
Set AP Isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No
Roaming assistant	Enable Disconnect clients with RSSI lower than: -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitrOQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="range"/> Performance
Apply	

Sur l'écran **Professional** (Professionnel), les options de configuration suivantes sont disponibles :

- **Band (Bande):** Sélectionnez une bande de fréquence.

- **Enable Radio (Activer la radio):** Sélectionnez **Yes** (Oui) pour activer le module radio WiFi, ou **No** (Non) pour le désactiver. Cochez **No** (Non) pour désactiver le réseau sans fil.
- **Enable Wireless Scheduler (Activer le planificateur WiFi) :** Vous pouvez choisir le format horaire 24 heures ou 12 heures. Les couleurs du tableau indiquent Allow (Autoriser) ou Deny (Refuser). Cliquez sur une cellule pour changer les paramètres de l'horaire en fonction des jours de la semaine et cliquez sur **OK**.

Wireless - Professional

* Reminder: The System time zone is different from your locale setting.

Clock Format: 24-hour | Allow: | Deny:

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **Set AP isolated (Isoler le point d'accès):** Permet de ne pas autoriser la communication entre les clients du réseau. Ceci est utile si votre réseau héberge fréquemment des utilisateurs invités. Sélectionnez **Yes** (Oui) ou **No** (Non) pour activer ou désactiver cette fonctionnalité.
- **Multicast rate (Mb/s) (Débit multi-diffusion):** Entrez une valeur ou cliquez sur **Disable** (Désactiver) pour désactiver cette fonctionnalité.

- **Preamble Type (Type de préambule)** : Détermine le temps alloué au routeur pour vérifier les redondances cycliques permettant de détecter les erreurs lors du transfert de paquets CRC (Cyclic Redundancy Check). Le CRC est une méthode de détection d'erreurs pendant la transmission de données. Sélectionnez **Short** (Court) pour un réseau disposant d'un trafic élevé, **Long** si votre réseau WiFi est composé de périphériques WiFi plus anciens ou hérités. Sélectionnez **Long** si votre réseau sans fil est composé de périphériques WiFi plus anciens ou hérités.
- **RTS Threshold (Palier RTS)**: Spécifiez une valeur de palier RTS basse pour améliorer les communications WiFi dans un réseau au trafic chargé et disposant d'un grand nombre d'appareils.
- **DTIM Interval (Intervalle DTIM)**: L'intervalle DTIM (Delivery Traffic Indication Message) est l'intervalle de temps avant lequel un signal est envoyé sur un périphérique WiFi en veille pour indiquer qu'un paquet attend d'être transmis. La valeur par défaut est de 3 millisecondes.
- **Beacon Interval (Intervalle de balise)**: L'intervalle de balise (Beacon Interval) correspond au temps en un DTIM et le suivant. La valeur par défaut est de 100 ms. Baissez la durée de l'intervalle si la connexion est instable ou pour les appareils itinérants.
- **Enable TX Bursting (État TX Burst)**: Cette fonctionnalité permet d'améliorer la vitesse de transfert entre le routeur WiFi et les appareils 802.11g.
- **Enable WMM APSD (WMM APSD)**: Activez l'option WMM APSD (WiFi Multimedia Automatic Power Save Delivery) pour améliorer la gestion de l'alimentation des périphériques WiFi. Sélectionnez **Disable** (Désactiver) pour désactiver cette fonctionnalité.

4 Utilitaires

4.1 Device Discovery (Détection d'appareils)

Détection d'appareils est un utilitaire WiFi ASUS qui détecte les routeurs WiFi ASUS et permet de les configurer facilement.

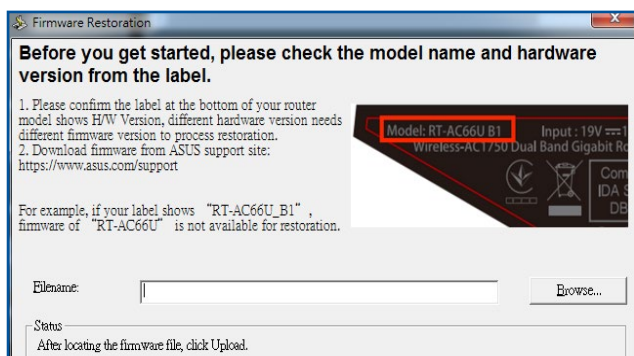
Pour lancer l'utilitaire Détection d'appareils :

- Depuis le Bureau de votre ordinateur, cliquez sur **Start** (Démarrer) > **All Programs** (Tous les programmes) > **ASUS Utility** (Utilitaire ASUS) > **Wireless Router** (Routeur WiFi) > **Device Discovery** (Détection d'appareils).

REMARQUE : Lorsque le routeur fonctionne en mode point d'accès, cet utilitaire est nécessaire pour obtenir l'adresse IP du routeur.

4.2 Firmware Restoration (Restauration du firmware)

Restauration du firmware est un utilitaire qui recherche automatiquement les routeurs WiFi ASUS dont la mise à jour du firmware a échoué, puis restaure ou charge le firmware que vous avez spécifié. Cela télécharge le firmware que vous avez choisi. Le processus prend de 3 à 4 minutes.



IMPORTANT ! Placez le routeur en mode de secours avant de lancer l'utilitaire Restauration du firmware.

REMARQUE : Cet utilitaire n'est pas compatible avec le système d'exploitation MAC OSX.

Pour basculer le routeur en mode de secours et utiliser l'utilitaire Restauration du firmware :

1. Débranchez la source d'alimentation de votre routeur WiFi.
2. Maintenez enfoncé le bouton de réinitialisation situé à l'arrière du routeur et rebranchez l'adaptateur secteur au routeur. Relâchez le bouton de réinitialisation une fois que le voyant d'alimentation en façade se met à clignoter lentement pour indiquer que le routeur est en mode de secours.
3. Configurez une adresse IP statique sur votre ordinateur et utilisez les éléments suivants pour configurer les paramètres TCP/IP :

Adresse IP: 192.168.1.x

Masque de sous-réseau: 255.255.255.0

4. Depuis le Bureau de votre ordinateur, cliquez sur **Start** (Démarrer) > **All Programs** (Tous les programmes) > **ASUS Utility** (Utilitaire ASUS) > **Wireless Router** (Routeur WiFi) > **Firmware Restoration** (Restauration du firmware).
5. Spécifiez un fichier de firmware, puis cliquez sur **Upload** (Charger).

REMARQUE : Cet utilitaire n'est pas un outil de mise à niveau du firmware et ne doit pas être utilisé avec un routeur WiFi ASUS fonctionnant normalement. Les mises à niveau du firmware doivent être effectuées via l'interface de gestion du routeur. Consultez le **Chapitre 3 : Configurer les paramètres généraux et avancés** pour plus de détails.

5 Dépannage

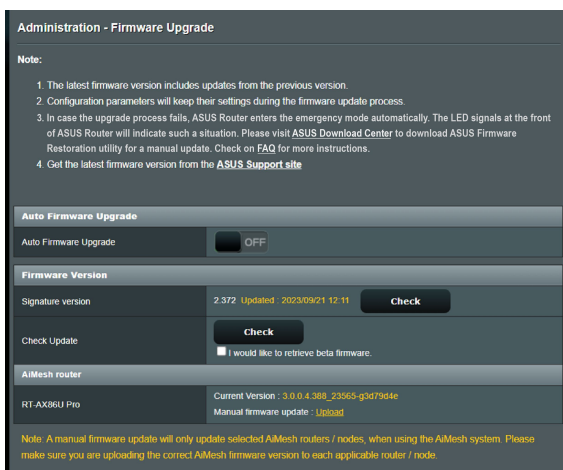
Ce chapitre offre des solutions aux problèmes pouvant survenir lors de l'utilisation de votre routeur. Si vous rencontrez un problème non traité dans ce chapitre, rendez-vous sur le site d'assistance d'ASUS sur : <https://www.asus.com/fr/support/> pour plus d'informations sur votre produit et obtenir les coordonnées du service technique d'ASUS.

5.1 Dépannage de base

Si votre routeur ne fonctionne pas correctement, essayez les solutions de dépannage de base suivantes.

Mettez à jour le firmware.

1. Ouvrez l'interface de gestion du routeur. Cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **Firmware Upgrade** (Mise à jour du firmware). Cliquez sur **Check** (Vérifier) pour vérifier si une mise à jour du firmware est disponible.



2. Si c'est le cas, rendez-vous sur [https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/](https://www.asus.com/Networking/ZenWiFi_BD4/HelpDesk/) pour télécharger le dernier firmware disponible.
3. Dans l'onglet **Firmware Version** (Version du firmware), cliquez sur **Check** (Vérifier) pour localiser le fichier téléchargé.
4. Cliquez sur **Upload** (Charger) pour lancer le processus de mise à niveau du firmware.

Réinitialisez votre réseau dans l'ordre suivant :

1. Éteignez le modem.
2. Débranchez la prise d'alimentation du modem.
3. Éteignez le routeur et les ordinateurs connectés.
4. Branchez la prise d'alimentation du modem.
5. Allumez le modem et patientez environ 2 minutes.
6. Allumez le routeur et patientez environ 2 minutes.
7. Allumez vos ordinateurs.

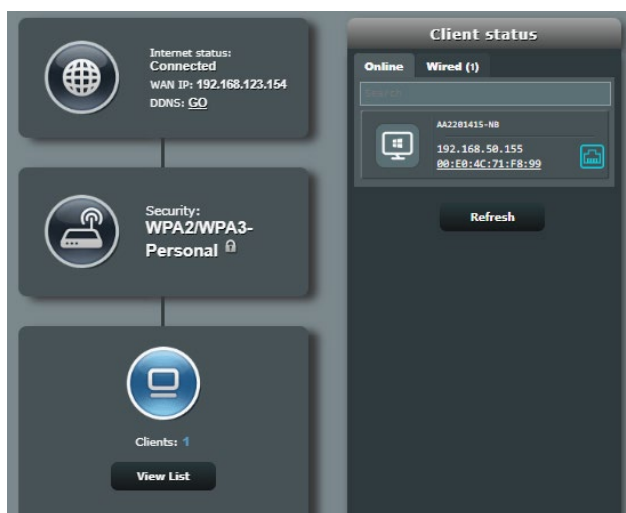
Vérifiez que les paramètres de connexion WiFi de l'ordinateur correspondent à ceux du routeur.

- Lorsque vous tentez d'établir une connexion WiFi entre un ordinateur et le routeur, assurez-vous que le SSID (nom du réseau WiFi), la méthode de chiffrement et le mot de passe sont corrects.

Vérifiez que les paramètres de configuration du réseau sont corrects.

- Chaque client du réseau se doit de posséder une adresse IP valide. Il est recommandé d'utiliser le serveur DHCP du routeur pour affecter automatiquement les adresses IP aux clients du réseau.

- Certains fournisseurs d'accès internet au câble requièrent l'adresse MAC de l'ordinateur enregistré sur leur réseau. Vous pouvez obtenir l'adresse MAC d'un client à partir de l'interface de gestion du routeur, en cliquant sur **Network Map** (Carte du réseau) > page **Clients**. Placez le curseur de souris au-dessus d'un client pour visualiser son adresse MAC.

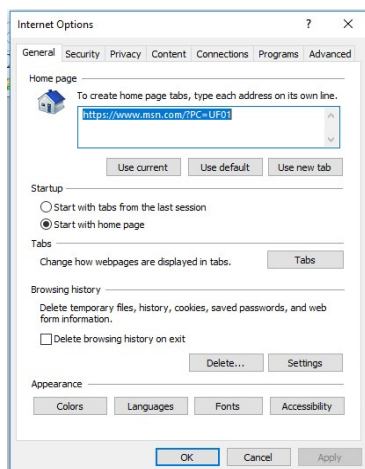


5.2 Foire aux questions (FAQ)

Impossible d'accéder à l'interface de gestion du routeur

- Si vous utilisez une connexion filaire, vérifiez le câble Ethernet et l'état des différents voyants lumineux tel qu'expliqué dans la section précédente.
- Assurez-vous d'utiliser les bons identifiants de connexion. Vérifiez également que la touche de verrouillage des majuscules n'a pas été activée.
- Supprimez les cookies et les fichiers temporaires de votre navigateur internet. Pour Internet Explorer, suivez les instructions suivantes :

1. Ouvrez Internet Explorer, puis cliquez sur **Tools** (Outils) > **Internet Options** (Options internet).
2. Dans l'onglet **General** (Général), sous **Browsing history** (Historique de navigation), cliquez sur **Delete...** (Supprimer...), sélectionnez **Temporary Internet Files** (Fichiers internet temporaires) et **Cookies** puis cliquez sur **Delete** (Supprimer).



REMARQUES :

- Les options de suppression des cookies et des fichiers temporaires peuvent varier en fonction du navigateur internet utilisé.
- Si applicable, désactivez votre proxy, la numérotation de votre connexion à distance, et configurez les paramètres TCP/IP de sorte à obtenir une adresse IP automatiquement. Pour plus de détails, consultez le chapitre 1 de ce manuel.
- Assurez-vous d'utiliser des câbles réseau Ethernet de catégorie 5 ou 6.

Le client ne peut pas établir de connexion WiFi avec le routeur

REMARQUE : Si vous rencontrez des problèmes de connexion au réseau 5 GHz, assurez-vous que votre appareil soit compatible avec cette bande de fréquence.

- **Hors de portée :**

- Rapprochez le routeur du client.

- **Serveur DHCP désactivé :**

1. Ouvrez l'interface de gestion du routeur. Dans l'interface de gestion du routeur, cliquez sur **General** (Général) > **Network Map** (Carte du réseau) > **Clients..**
2. Si l'appareil n'apparaît pas dans la liste, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **DHCP Server** (Serveur DHCP), et vérifiez que la case **Yes** (Oui) du champ **Enable the DHCP Server** (Activer le serveur DHCP) est bien cochée.

LAN - DHCP Server

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 informs the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.
[Manually Assigned IP around the DHCP list FAQ](#)

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
No data in table.				

Apply

- Le SSID est masqué. Si votre appareil est en mesure de détecter d'autres réseaux WiFi sauf celui de votre routeur, allez dans **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > onglet **General** (Général), cochez l'option **No** (Non) du champ **Hide SSID** (Masquer le SSID), et l'option **Auto** du champ **Control Channel** (Canal).

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4 GHz
Network Name (SSID)	LIAO
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> big Protection <input type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check FAQ.</small>
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto <small>Current Control Channel: 5</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** Weak
Group Key Rotation Interval	3600

Apply

- Si vous utilisez une carte WiFi, vérifiez que le canal WiFi utilisé est disponible dans votre pays/région. Dans ce cas, modifiez le canal et les autres paramètres WiFi appropriés.
- Si vous ne parvenez toujours pas à établir une connexion WiFi au routeur, restaurez sa configuration d'usine. Pour ce faire, dans l'interface de gestion du routeur, allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer).

Administration - Restore/Save/Upload Setting

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

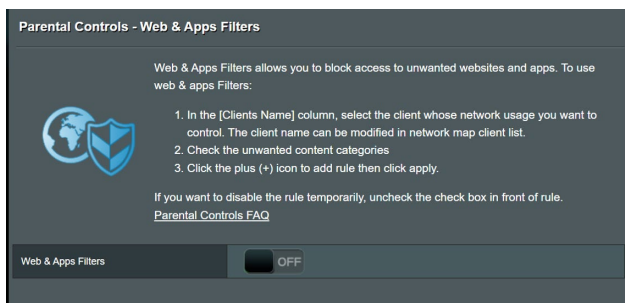
Factory default	Restore	<input type="checkbox"/> Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History
Save setting	Save setting	<input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router. <input type="checkbox"/> Transfer ASUS DNS name
Restore setting	Upload	

Internet n'est pas accessible.

- Vérifiez que votre routeur peut se connecter à l'adresse IP du réseau étendu (WAN) de votre FAI. Pour ce faire, dans l'interface de gestion du routeur, allez dans **General** (Général) > **Network Map** (Carte du réseau) et vérifiez **l'état de la connexion internet**.
- Si votre routeur ne peut pas se connecter à Internet, essayez de réinitialiser le réseau comme décrit à la sous-section **Réinitialisez votre réseau dans l'ordre suivant** sous **Dépannage de base**.



- Le client a été bloqué par la fonctionnalité de contrôle parental. Dans l'interface de gestion du routeur, allez dans **General** (Général) > **Parental Controls** (Contrôle parental) et vérifiez que l'appareil figure dans la liste. Si c'est le cas, utilisez le bouton **Supprimer** pour retirer le client de la liste, ou modifiez les horaires de blocage.



- Si Internet n'est toujours pas accessible, essayez de redémarrer l'ordinateur et vérifiez son adresse IP et de passerelle.

Oubli du SSID (nom du réseau) ou du mot de passe de connexion au réseau

- Configurez un nouveau SSID et une nouvelle clé de chiffrement par le biais d'une connexion filaire (câble Ethernet). Ouvrez l'interface de gestion du routeur, allez sur la page **Network Map** (Carte du réseau), spécifiez un nouveau SSID ainsi qu'une nouvelle clé de chiffrement, puis cliquez sur **Apply** (Appliquer).
- Restaurer la configuration d'usine du routeur. Pour ce faire, dans l'interface de gestion du routeur, allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer).

Restauration des paramètres par défaut du routeur ?

- Allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer).

Échec de la mise à jour du firmware.

Placez le routeur en mode de secours et exécutez l'utilitaire Restauration du firmware. Consultez la section **4.2 Firmware Restoration (Restauration du firmware)** pour en savoir plus sur l'utilisation de cet utilitaire.

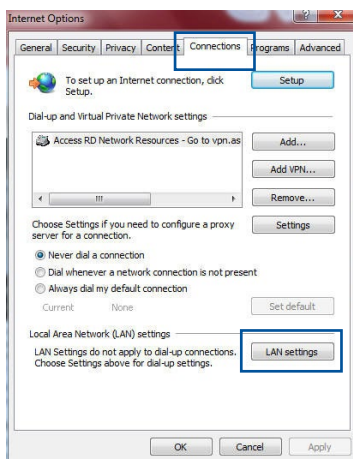
Impossible d'accéder à l'interface de gestion du routeur

Avant de configurer votre routeur WiFi, suivez les instructions suivantes pour votre ordinateur hôte et les autres clients du réseau.

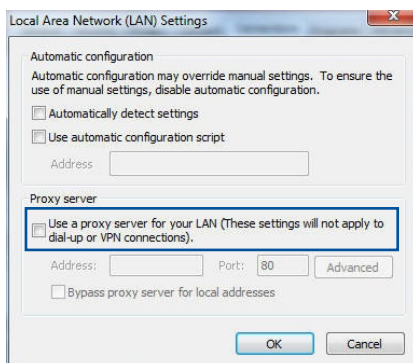
A. Désactivez le serveur proxy si celui-ci est activé.

Windows®

1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > **Connections** (Connexions) > **LAN settings** (Paramètres réseau).

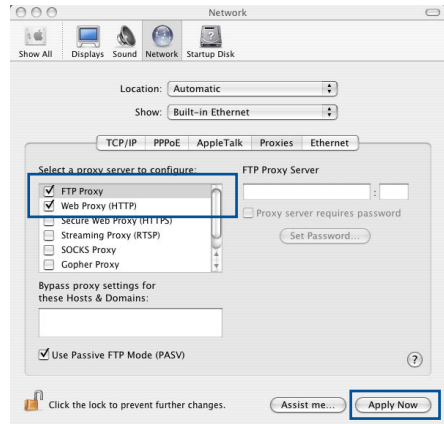


3. À partir de l'écran des paramètres du réseau local, décochez l'option **Use a proxy server for your LAN** (Utiliser un serveur proxy pour votre réseau local).
4. Cliquez sur **OK** une fois terminé.



Sous MAC OS

1. Dans votre navigateur Safari, cliquez sur **Safari > Preferences** (Préférences) > **Advanced** (Avancées) > **Change Settings** (Modifier les réglages)
2. Dans la liste des protocoles, décochez les options **FTP Proxy** (Proxy FTP) et **Web Proxy (HTTP)** (Proxy web sécurisé (HTTP)).
3. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

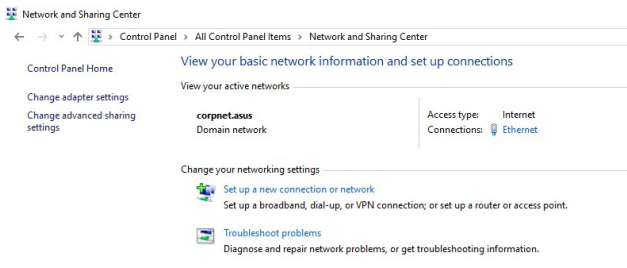


REMARQUE : Consultez le fichier d'aide de votre navigateur internet pour plus de détails sur la désactivation du serveur proxy.

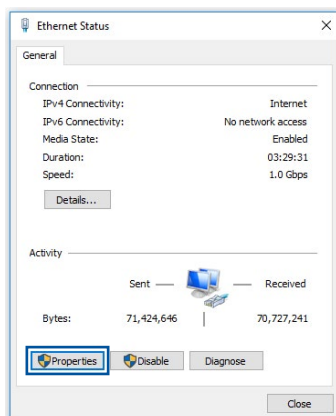
B. Configurez les paramètres TCP/IP pour l'obtention automatique d'une adresse IP.

Windows®

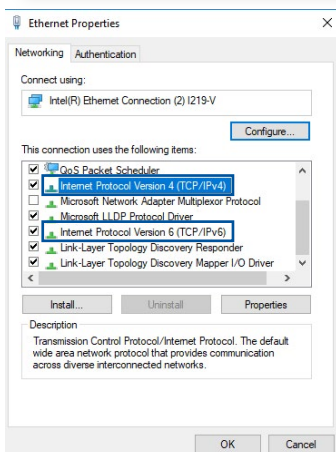
1. Cliquez sur **Start** (Démarrer) > **Control Panel** (Panneau de configuration) > **Network and Sharing Center** (Centre réseau et partage), puis cliquez sur la connexion réseau pour afficher sa fenêtre d'état.



2. Cliquez sur **Propriétés** (Propriétés) pour afficher la fenêtre des propriétés réseau.



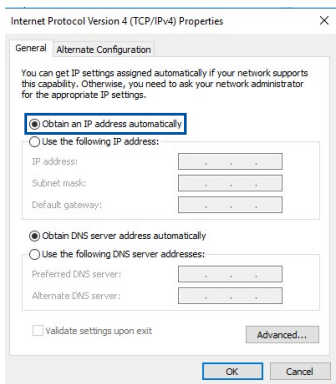
3. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)** (Protocole internet version 4 (TCP/IPv4)) ou **Internet Protocol Version 6 (TCP/IPv6)** (Protocole internet version 6 (TCP/IPv6)), puis cliquez sur **Propriétés** (Propriétés).




4. Pour obtenir une adresse IP IPv4, cochez l'option **Obtain an IP address automatically** (Obtenir une adresse IP automatiquement).

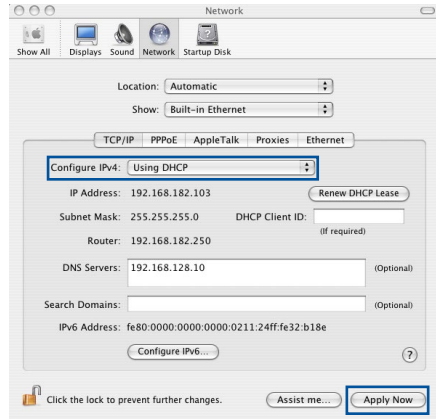
Pour obtenir une adresse IP IPv6, cochez l'option **Obtain an IPv6 address automatically** (Obtenir une adresse IPv6 automatiquement).

5. Cliquez sur **OK** une fois terminé.



Sous MAC OS

1. Cliquez sur l'icône Apple  située en haut à gauche de votre écran.
2. Cliquez sur **System Preferences** (Préférences Système) > **Network** (Réseau) > **Configure...** (Configurer...)
3. Dans l'onglet **TCP/IP**, sélectionnez **Using DHCP** (Via DHCP) dans le menu déroulant **Configure IPv4** (Configurer IPv4).
4. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

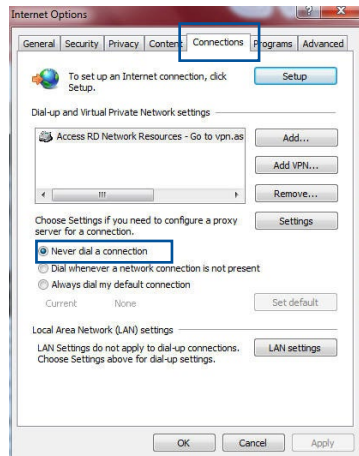


REMARQUE : Consultez l'aide de votre système d'exploitation pour plus de détails sur la configuration des paramètres TCP/IP de votre ordinateur.

C. Désactivez la numérotation de votre connexion à distance (le cas échéant).

Windows®

1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > **Connections** (Connexions).
3. Cochez l'option **Never dial a connection** (Ne jamais établir de connexion).
4. Cliquez sur **OK** une fois terminé.



REMARQUE : Consultez le fichier d'aide de votre navigateur internet pour plus de détails sur la désactivation d'une connexion à distance.

Annexes

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

Consignes de sécurité

Lorsque vous utilisez ce produit, suivez toujours les précautions de sécurité fondamentales, y compris, mais sans s'y limiter, les suivantes :



AVERTISSEMENT !

- Les cordons d'alimentation doivent être branchés sur une prise électrique correctement reliée à la terre. Connectez l'équipement uniquement à une prise de courant à proximité et facilement accessible.
- Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien qualifié ou votre revendeur.
- NE PAS utiliser de cordons d'alimentation, accessoires ou autres périphériques endommagés.
- NE PAS placer cet équipement à une hauteur supérieure à 2 mètres.
- Utilisez ce produit dans un environnement dont la température ambiante est comprise entre 0°C (32°F) et 40°C (104°F).
- Lisez les directives opérationnelles et la plage de température fournies avant d'utiliser le produit.
- Soyez particulièrement vigilant quant à votre sécurité lors de l'utilisation de cet appareil dans certains lieux (les aéroports, les hôpitaux, les stations-service et les garages professionnels).
- Évitez d'utiliser cet appareil à proximité de dispositifs médicaux implantés. Si vous portez un implant électronique (stimulateurs cardiaques, pompes à insuline, neurostimulateurs...), veuillez impérativement respecter une distance minimale de 15 centimètres entre cet appareil et votre corps pour réduire les risques d'interférence.
- Utilisez cet appareil dans de bonnes conditions de réception pour minimiser le niveau de rayonnement. Ce n'est pas toujours le cas dans certaines zones ou situations, notamment dans les parkings souterrains, dans les ascenseurs, en train, en voiture, ou tout simplement dans un secteur mal couvert par le réseau.
- Tenez cet appareil à distance des femmes enceintes et du bas-ventre des adolescents.
- N'utilisez pas ce produit si des anomalies sont visibles ou s'il a été mouillé, endommagé ou modifié. Faites appel au service après-vente pour obtenir de l'aide.



AVERTISSEMENT !

- NE PAS placer sur une surface irrégulière ou instable.
 - Ne placez pas et ne laissez pas tomber d'objets sur le produit. Évitez d'exposer le produit à des chocs mécaniques tels que l'écrasement, la flexion, la perforation ou le broyage.
 - NE PAS démonter, ouvrir, passer au micro-ondes, incinérer, peindre ou insérer des objets étrangers dans ce produit.
 - Référez-vous à l'étiquette située au dessous du produit pour vérifier que l'adaptateur secteur répond aux exigences de tension.
 - Gardez le produit à l'écart du feu et des sources de chaleur.
 - NE PAS exposer l'appareil à la pluie ou à l'humidité, tenez-le à distance des liquides. NE PAS utiliser le produit lors d'un orage.
 - Connectez les circuits de sortie PoE de ce produit exclusivement aux réseaux PoE, sans routage vers des installations externes.
 - Pour éviter tout risque de choc électrique, débranchez le câble d'alimentation de la prise électrique avant de toucher au système.
 - Utilisez uniquement des accessoires approuvés par le fabricant de l'appareil pour fonctionner avec ce modèle. L'utilisation d'autres types d'accessoires peut invalider la garantie ou enfreindre les réglementations et lois locales, tout en présentant des risques pour la sécurité. Contactez votre revendeur local pour connaître la disponibilité des accessoires autorisés.
 - L'utilisation de ce produit d'une manière non recommandée dans les instructions fournies peut entraîner un risque d'incendie ou de blessures.
-

Service et assistance

Visitez notre site multilingue d'assistance en ligne sur :
<https://www.asus.com/fr/support>.

