E23335

REPUBLIC OF GAMERS

USER MANUAL

RAPTURE GT-BE98

BE25000 Quad-band Gaming Router

ASUS

F23335
Première Édition
Février 2024

Table des matières

Table des matières

Table des matières

5 Dépannage

Annexes

1 Présentation de votre routeur WiFi

1.1 Bienvenue !

Merci d'avoir acheté un routeur WiFi ROG Rapture !

Ce routeur élégant dispose de quatre bandes WiFi (2,4 GHz x1, 5 GHz x2, 6 GHz x1) pour un streaming HD simultané 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. La technologie ASUS Green Network vous permet de plus de réaliser jusqu'à 70 % d'économie d'énergie.

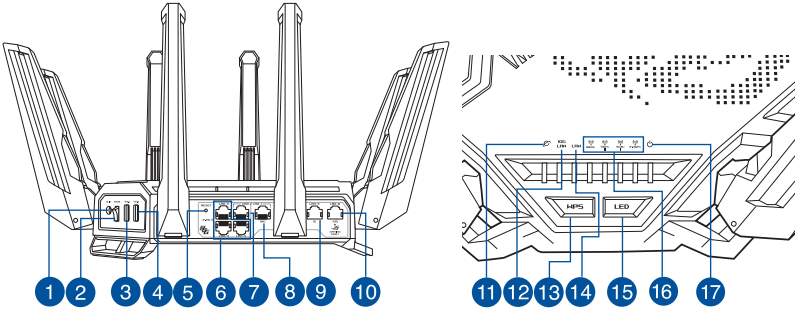
1.2 Contenu de la boîte

- ☑ Routeur gaming ROG Rapture
- ☑ Câble réseau (RJ-45)
- ☑ Adaptateur secteur
- ☑ Guide de démarrage rapide

REMARQUES :

- Contactez votre service après-vente ASUS si l'un des éléments est manquant ou endommagé. Consultez la liste des centres d'appel ASUS en fin de manuel.
- Conservez l'emballage d'origine pour toutes futures demandes de prises sous garantie.

1.3 Votre routeur WiFi



1	**Prise d'alimentation (CC)** Insérez l'adaptateur secteur dans ce port puis reliez votre routeur à une source d'alimentation.
2	**Interrupteur d'alimentation** Cet interrupteur permet d'allumer ou d'éteindre le routeur.
3	**Port USB 2.0** Insérez un dispositif USB 2.0 tel qu'un périphérique de stockage USB dans ce port.
4	**Port USB 3.2 Gen 1** Insérez un dispositif USB 3.2 Gen 1 tel qu'un périphérique de stockage USB dans ce port.
5	**Bouton de réinitialisation** Ce bouton permet de restaurer les paramètres par défaut du routeur.
6	**Ports réseau local 2 à 4 (LAN) 2.5GE** Connectez des câbles réseau sur ces ports pour établir une connexion LAN 2.5GE.
7	**Port WAN/LAN1 2.5GE** Connectez un câble réseau à ce port pour établir une connexion WAN/LAN1 2.5GE.
8	**Port WAN/LAN1 10GE** Connectez un câble réseau à ce port pour établir une connexion WAN/LAN1 10GE.
9	**Port réseau local 5 (LAN) 1GE** Connectez un câble réseau à ce port pour établir une connexion LAN5 10GE.
10	**Port réseau local 6 (LAN) 10GE** Connectez un câble réseau à ce port pour prioriser les paquets.
11	**Voyant réseau étendu (WAN) (Internet) 10 / 2.5GE** **Rouge** : Aucune adresse IP ou aucune connexion physique. **Allumé** : Connexion établie à un réseau étendu (WAN).

12	**Voyant réseau local (LAN) 10GE** **Éteint** : Routeur éteint ou aucune connexion physique. **Allumé** : Connexion établie à un réseau local (LAN) 10GE.
13	**Bouton WPS** Ce bouton permet de lancer l'assistant WPS.
14	**Voyant réseau local (LAN)** **Éteint** : Routeur éteint ou aucune connexion physique. **Allumé** : Connexion établie à un réseau local (LAN).
15	**Bouton LED** Appuyez sur ce bouton pour activer/désactiver le voyant LED.
16	**Voyant WiFi 6GHz/5GHz-2/5GHz-1/2,4GHz** **Éteint** : Aucun signal 6 GHz / 5 GHz-2 / 5 GHz-1 / 2,4 GHz. **Allumé** : Routeur prêt à établir une connexion WiFi. **Clignotant** : Transmission ou réception de données WiFi.
17	**Voyant d'alimentation** **Éteint** : Aucune alimentation. **Allumé** : Le routeur est prêt. **Clignote lentement** : Mode de secours.

REMARQUES :

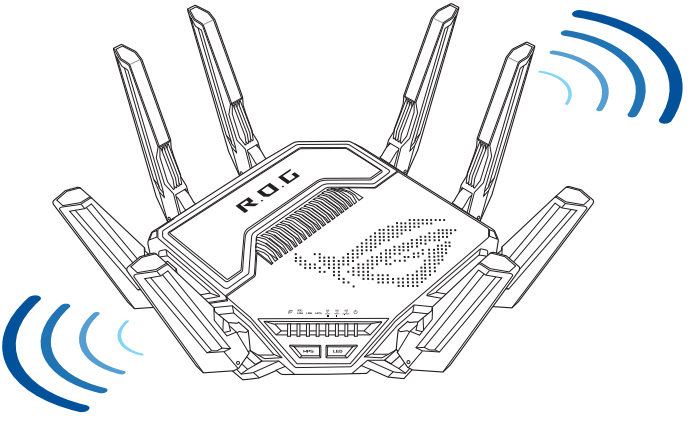
- Utilisez uniquement l'adaptateur secteur fourni avec votre appareil. L'utilisation d'autres adaptateurs peut endommager l'appareil.
- **Caractéristiques :**

Adaptateur secteur CC	Sortie (CC) : 19,5V (3,33A max.)		
Température de fonctionnement	0-40°C	Stockage	0-70°C
Humidité de fonctionnement	50-90 %	Stockage	20-90 %

1.4 Placer le routeur

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.
- Pour assurer le meilleur signal WiFi, orientez les huit antennes externes comme illustré sur le schéma ci-dessous.



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/be
- 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/be sur votre ordinateur pour vous connecter au réseau.
- Avec sa technologie quadri-bande, votre routeur WiFi prend en charge les signaux WiFi des bandes 2,4 GHz, 5 GHz et 6 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 les bandes 5 GHz et 6 GHz.
- Certains appareils dotés de capacités WiFi IEEE 802.11n ne sont pas compatibles avec les bandes 5 GHz et 6 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 802.11be.
- 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 !

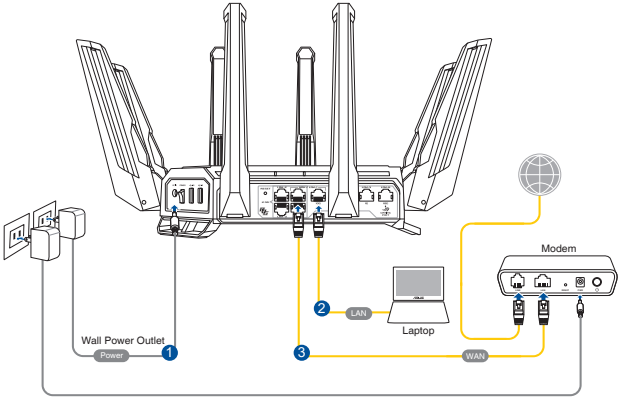
- Les cordons d'alimentation doivent être branchés sur une prise électrique correctement reliée à la terre. Connectez l'équipement uniquement à une prise de courant à proximité et facilement accessible.
- Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien électrique 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

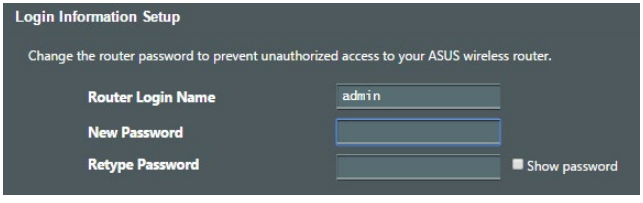
REMARQUE : Une fonction de détection de croisement automatique est intégrée au routeur WiFi pour que vous puissiez aussi bien utiliser un câble Ethernet droit que croisé.

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 au port de réseau local (LAN) du routeur.



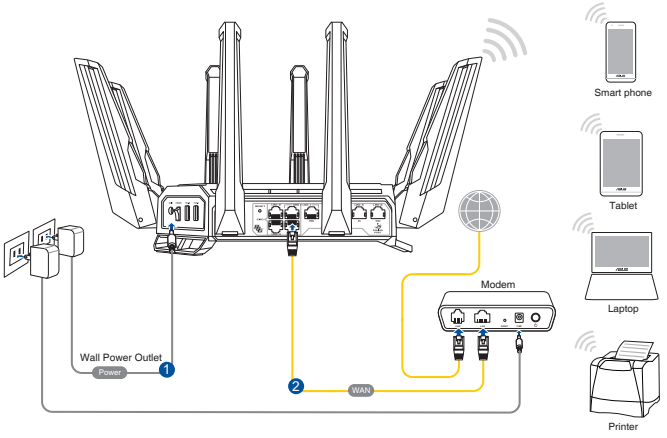
2. L'interface de gestion du routeur s'affiche automatiquement lors de l'ouverture de votre navigateur internet. Si ce n'est pas le cas, saisissez http://www.asusrouter.com dans la barre d'adresse
3. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.



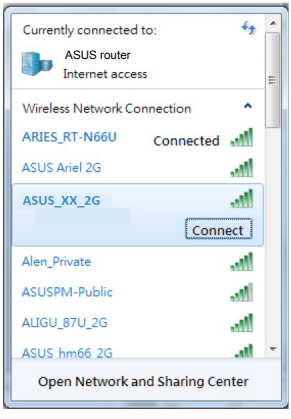
B. Connexion WiFi

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.



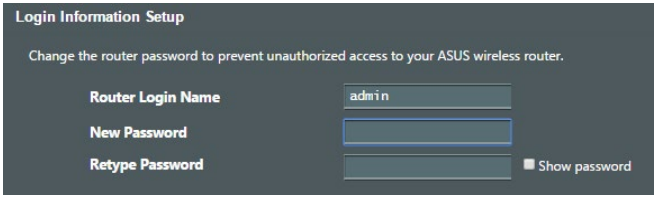
Nom du réseau WiFi 2,4G (SSID) :	ASUS_XX_2G
Nom du réseau WiFi 5G-1 (SSID) :	ASUS_XX_5G-1
Nom du réseau WiFi 5G-2 (SSID) :	ASUS_XX_5G-2
Nom du réseau WiFi 6G (SSID) :	ASUS_XX_6G

* **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 ROG.

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 **Définir les paramètres de sécurité** du chapitre 3 de ce manuel.



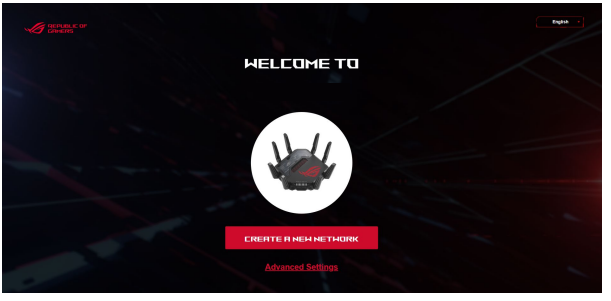
2.2 Configuration internet rapide avec auto-détection

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.



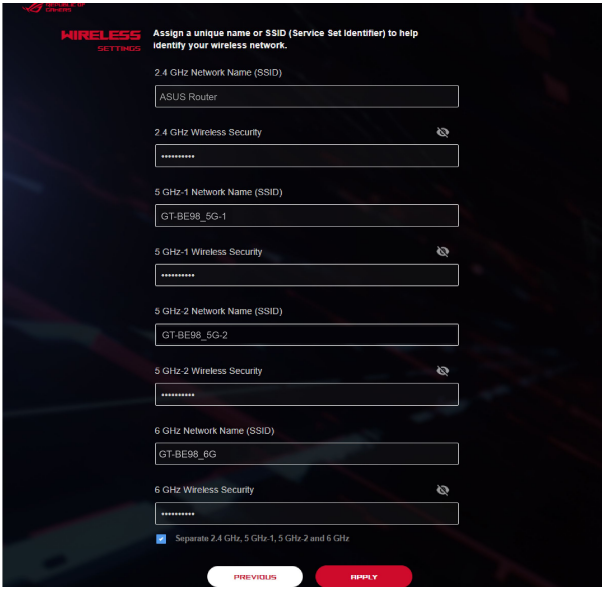
2. Le routeur WiFi détecte automatiquement si la connexion internet fournie par votre FAI utilise une **IP dynamique** ou le protocole **PPPoE**, **PPTP** ou **L2TP**. Entrez les informations nécessaires en fonction de votre type de connexion.

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

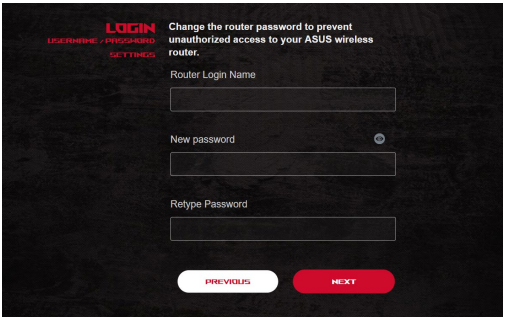
REMARQUES :

- 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 **Skip to 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 2,4 GHz, 5 GHz-1, 5 GHz-2 et 6 GHz. 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 des identifiants dédiés au SSID (2,4GHz / 5GHz-1 / 5GHz-2 / 6GHz) et à la 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) et la clé de sécurité permettent aux dispositifs WiFi de se connecter au réseau 2,4 GHz, 5 GHz-1, 5 GHz-2 et 6 GHz 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.

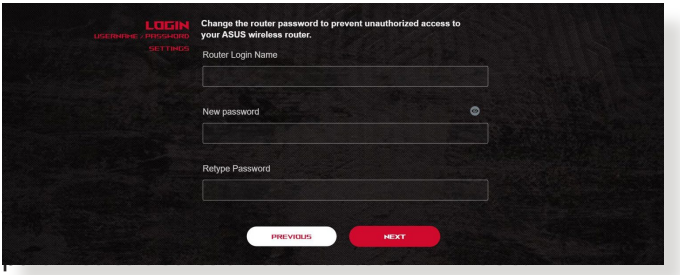
3 Configurer les paramètres généraux et avancés

3.1 Se connecter à l'interface de gestion

Votre routeur WiFi ROG intègre une interface utilisateur en ligne - ROG Gaming Center, qui vous donne un contrôle total sur votre réseau et vous fournit les informations à savoir telles que l'état des périphériques connectés et les valeurs pings des serveurs internet de jeu ainsi qu'un accès immédiat à toutes les fonctionnalités de jeu.

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, entrez le nom d'utilisateur par défaut (**admin**) et le mot de passe que vous avez configuré dans **2.2 Configuration internet rapide**.
3. 

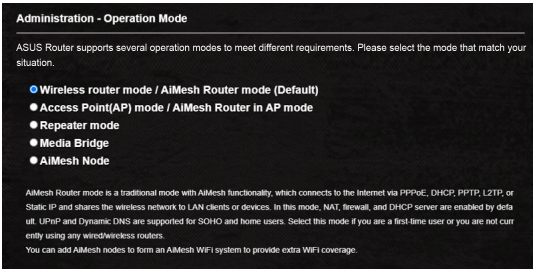
* L'image est fournie à titre indicatif uniquement.

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.

3.2 Administration

3.2.1 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 :
   - **Mode routeur WiFi / mode routeur AiMesh (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(AP) / AiMesh Router in AP mode** (Point d'accès (AP) / Routeur AiMesh en mode AP) : Ce mode permet de créer un nouveau réseau WiFi à partir d'un réseau existant.
   - **Repeater Mode** (Répéteur) : Lorsque le mode Répéteur est activé, votre routeur WiFi se connecte à un réseau WiFi existant afin d'étendre la couverture réseau. Dans ce mode, les fonctions de pare-feu, de partage d'IP et de NAT sont désactivées.
   - **Media Bridge (Pont média)** : La sélection de ce mode nécessite deux routeurs WiFi. Le second routeur faisant office de pont multimédia sur lequel divers appareils (TV connectée, console de jeu, etc.) peuvent être connectés par le réseau Ethernet.
   - **AiMesh node** (Nœud AiMesh) : Cette configuration nécessite au moins deux routeurs ASUS compatibles AiMesh. Activez le mode AiMesh, puis connectez-vous à l'interface de gestion du routeur pour rechercher les nœuds à proximité pour lier votre système AiMesh. AiMesh fournit une couverture pour toute la maison et une gestion centralisée.

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

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

3.2.2 System (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.
   - **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.
   - **Allow only specified IP address (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.
   - **Client List (Liste des clients)**: Entrez les adresses IP du réseau étendu (WAN) des clients autorisés à accéder à l'interface de gestion du routeur depuis Internet. Cette liste ne sera utilisée que si vous avez coché **Yes** (Oui) pour l'option précédente.
3. Cliquez sur **Apply** (Appliquer).

3.2.3 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 **New Firmware File** (Nouveau fichier de firmware), cliquez sur **Browse** (Parcourir) 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)**.

3.2.4 Restauration/Sauvegarde/Transfert de paramètres

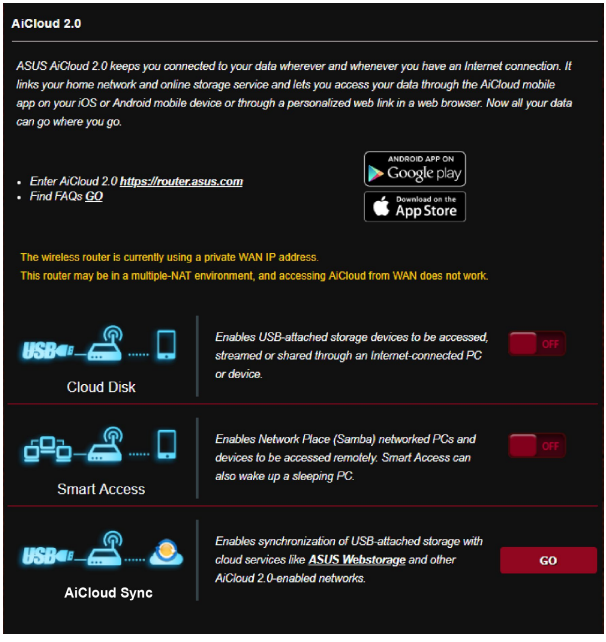
Pour restaurer/sauvegarder/transférer les paramètres de configuration du routeur :

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** (Sauvegarder), sélectionnez le dossier souhaité et cliquez sur **Save** (Sauvegarder).
   - Pour restaurer le routeur à partir d'un fichier de configuration précédent, cliquez sur **Browse** (Parcourir) et localisez le fichier, puis cliquez sur **Upload** (Charger).

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

3.3 AiCloud 2.0

AiCloud 2.0 est une application dans le Cloud vous permettant de sauvegarder, de synchroniser, de partager et d'accéder à distance à vos fichiers.



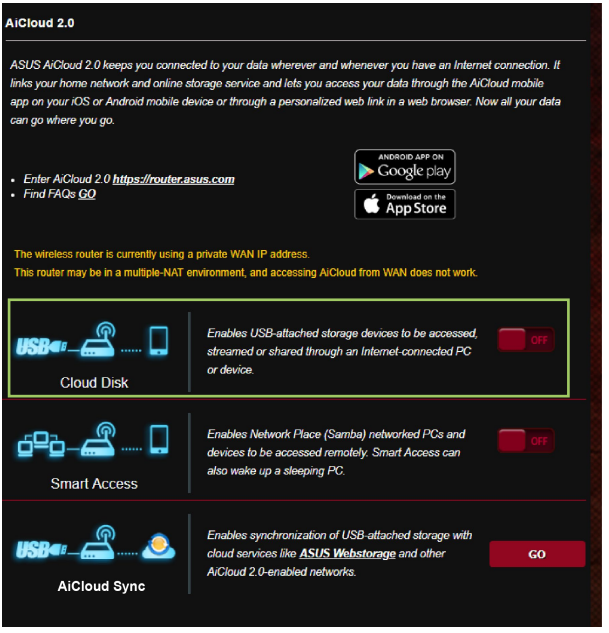
Pour utiliser AiCloud :

1. Téléchargez et installez l'application ASUS AiCloud sur votre appareil mobile à partir de la boutique en ligne Google Play ou Apple Store.
2. Connectez l'appareil mobile à votre réseau. Suivez les instructions pour effectuer la configuration d'AiCloud.

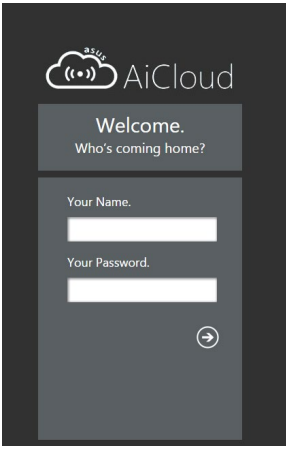
3.3.1 Cloud Disk

Pour créer un disque de stockage dans le Cloud :

1. Insérez un périphérique de stockage USB sur l'un des ports USB de votre routeur WiFi.
2. Activez **Cloud Disk**.

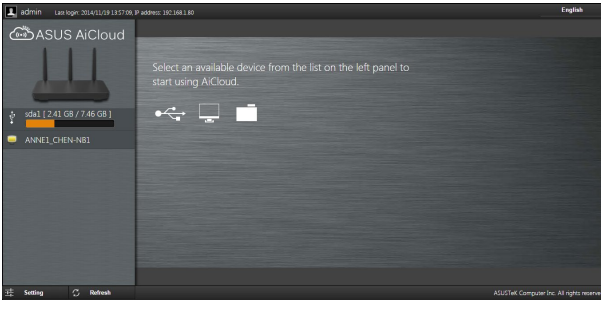


3. Rendez-vous sur http://www.asusrouter.com et saisissez les identifiants de connexion de votre routeur. Pour améliorer votre expérience d'utilisation, il est recommandé d'utiliser **Google Chrome** ou **Firefox**.



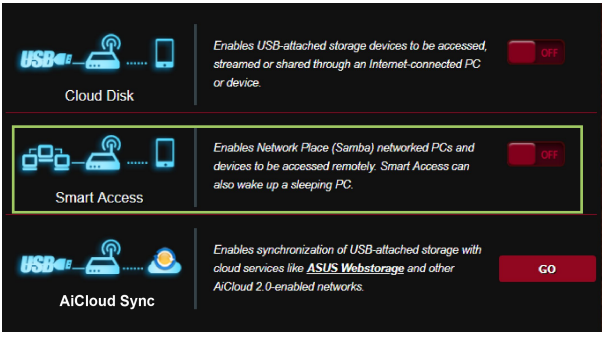
4. Vous pouvez dès lors accéder aux fichiers Cloud Disk des appareils connectés au réseau.

REMARQUE : Lorsque vous accédez aux appareils connectés au réseau, vous devez saisir manuellement le nom d'utilisateur et le mot de passe de l'appareil. Pour des raisons de sécurité, AiCloud ne mémorise pas vos identifiants de connexion.



3.3.2 Smart Access

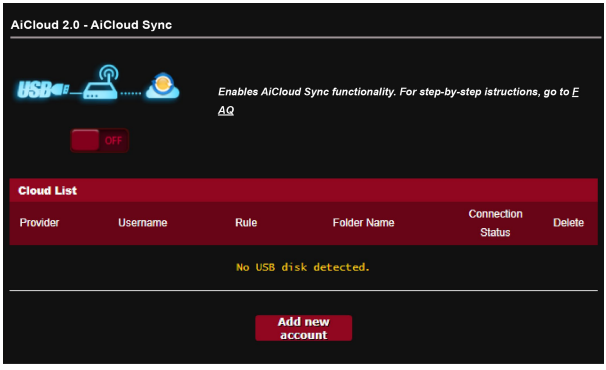
La fonctionnalité Smart Access vous permet d'accéder aisément à votre réseau domestique par le biais du nom de domaine de votre routeur.



REMARQUES :

- Vous pouvez créer un nom de domaine pour votre routeur grâce au service DDNS d'ASUS. Pour plus de détails, consultez la section **3.21.6 DDNS**.
- Par défaut, AiCloud offre une connexion HTTPS sécurisée. Entrez **https://[nomduDDNSASUS].asuscomm.com** pour une utilisation extrêmement sûre des fonctionnalités Cloud Disk et Smart Access.

3.3.3 AiCloud Sync



Pour utiliser AiCloud Sync :

1. Lancez AiCloud, cliquez sur **AiCloud Sync** > **Go**.
2. Sélectionnez **ON** (Activé) pour activer AiCloud Sync.
3. Cliquez sur **Add new account** (Ajouter un compte).
4. Entrez votre nom d'utilisateur et mot de passe ASUS WebStorage et sélectionnez le répertoire à synchroniser avec WebStorage.
5. Cliquez sur **Apply** (Appliquer).

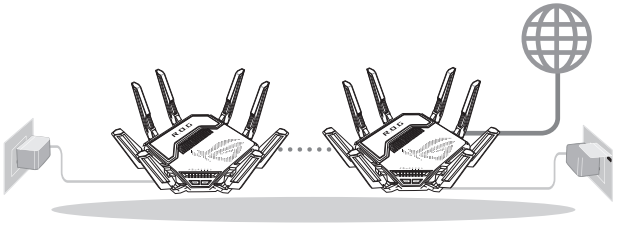
3.4 ASUS AiMesh

3.4.1 Avant de configurer

Préparation de la configuration d'un système WiFi AiMesh

1. Deux (2) routeurs ASUS (modèles prenant en charge AiMesh : https://www.asus.com/AiMesh/).
2. Assignez un routeur comme routeur AiMesh et l'autre comme nœud AiMesh.

REMARQUE : Si vous avez plusieurs routeurs AiMesh, nous vous recommandons d'utiliser le routeur disposant des spécifications les plus élevées en tant que routeur AiMesh et les autres routeurs en tant que nœuds AiMesh.



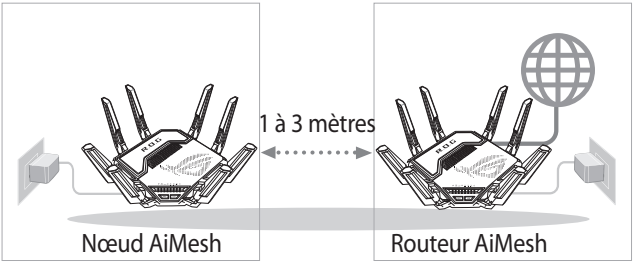
3.4.2 Étapes de configuration AiMesh

Préparation

Placez le routeur et le nœud AiMesh à une distance de 1 à 3 mètres l'un de l'autre pendant le processus de configuration.

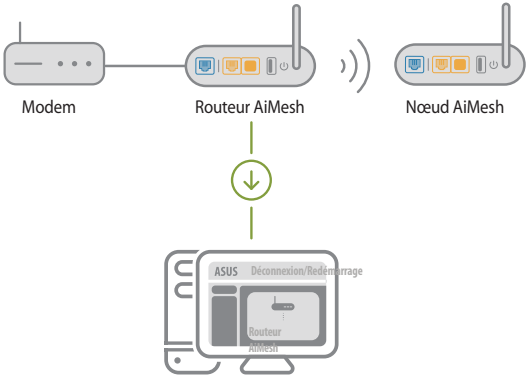
Nœud AiMesh

Paramètres par défaut. Gardez le nœud AiMesh sous tension et en veille lors de la configuration du système AiMesh.



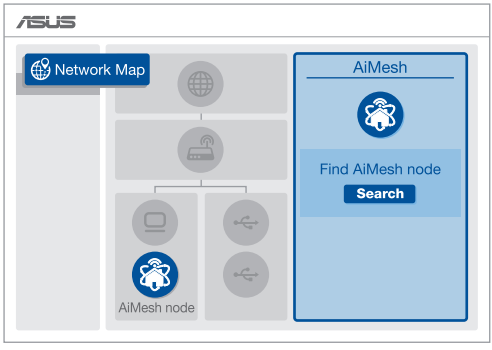
Routeur AiMesh

1) Consultez le **Guide de démarrage rapide** de l'autre routeur pour connecter votre routeur AiMesh à votre ordinateur et à votre modem, puis connectez-vous à l'interface de gestion.



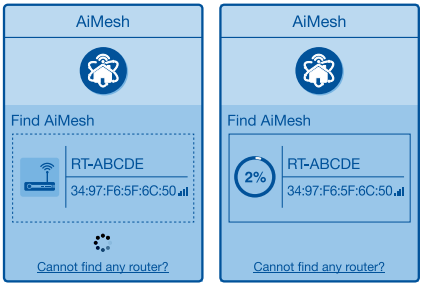
2) Accédez à la page Network Map (Carte du réseau), cliquez sur l'icône AiMesh puis sur Search (Rechercher) pour rechercher votre nœud AiMesh étendu.

REMARQUE : Si vous ne trouvez pas l'icône AiMesh ici, cliquez sur la version du firmware et mettez à jour le firmware.

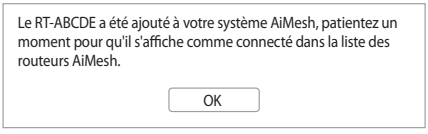


3) Cliquez sur **Search** (Rechercher), l'appareil recherche automatiquement le nœud AiMesh. Lorsque le nœud AiMesh apparaît sur cette page, cliquez dessus pour l'ajouter au système AiMesh.

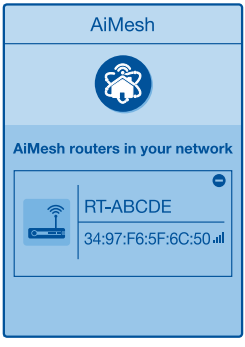
REMARQUE : Si vous ne trouvez aucun nœud AiMesh, allez dans **DÉPANNAGE**.



4) Un message s'affiche lorsque la synchronisation est terminée.



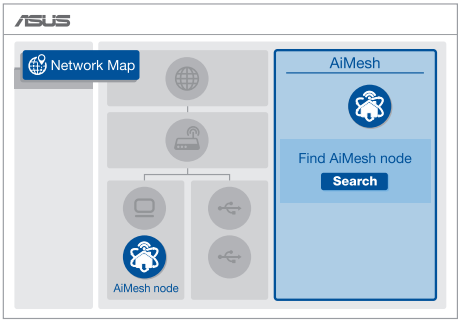
5) Félicitations ! Les pages ci-dessous s'afficheront une fois le nœud AiMesh ajouté au réseau AiMesh.



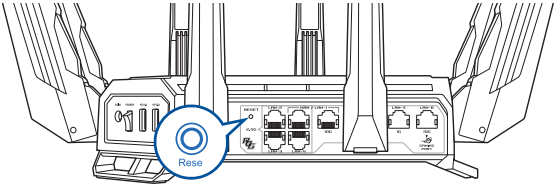
3.4.3 Dépannage

Si votre routeur AiMesh ne trouve aucun nœud AiMesh à proximité ou si la synchronisation échoue, veuillez vérifier les points suivants et réessayer.

1) Rapprochez votre nœud AiMesh du routeur AiMesh dans un rayon de 3 mètres. Assurez-vous qu'il se situe à une distance comprise entre 1 et 3 mètres.
2) Le nœud AiMesh est sous tension.
3) Le nœud AiMesh est mis à niveau vers le firmware pris en charge par AiMesh.
   i. Téléchargez le firmware pris en charge par AiMesh à l'adresse suivante: https://www.asus.com/AiMesh/
   ii. Mettez votre nœud AiMesh sous tension et connectez-le à votre ordinateur à l'aide d'un câble réseau.
   iii. Ouvrez l'interface de gestion du routeur. Vous serez automatiquement redirigé vers l'assistant de configuration ASUS. Dans le cas contraire, rendez-vous sur : http://www.asusrouter.com.
   iv. Cliquez sur **Administration** > **Firmware Upgrade** (Mise à jour du firmware). Cliquez sur **Choose File** (Choisir un fichier) et téléchargez le firmware pris en charge par AiMesh.
   v. Une fois le firmware téléchargé, rendez-vous sur la page Network Map (Carte du réseau) pour confirmer que l'icône AiMesh est apparue.



   vi. Appuyez sur le bouton de réinitialisation du nœud AiMesh pendant au moins 5 secondes. Relâchez le bouton de réinitialisation une fois que le voyant d'alimentation se met à clignoter lentement.



3.4.4 Placement

Les meilleures performances:

Placez le routeur et le nœud AiMesh au meilleur endroit.

REMARQUES :

- Pour réduire les interférences, ne placez pas les routeurs à proximité d'appareils tels que les téléphones sans fil, les appareils Bluetooth ou les fours à micro-ondes.
- Il est recommandé de placer les routeurs dans un endroit dégagé et spacieux.

3.4.5 FAQ (Foire Aux Questions)

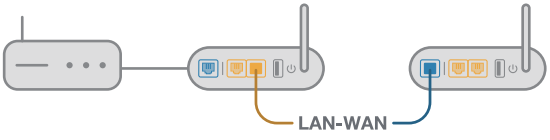
Q1 : Est-ce que le routeur AiMesh prend en charge le mode point d'accès ?

R : Oui. Vous pouvez configurer le routeur AiMesh en mode routeur ou en mode point d'accès. Veuillez accéder à l'interface de gestion (http://www.asusrouter.com) et aller dans **Administration** > **Operation Mode** (Mode de fonctionnement).

Q2 : Puis-je configurer une connexion filaire entre les routeurs AiMesh (Ethernet backhaul) ?

R : Oui. Le système AiMesh prend en charge les connexions sans fil et filaires entre le routeur et le nœud AiMesh pour optimiser le débit et la stabilité. AiMesh analyse la puissance du signal sans fil pour chaque bande de fréquence disponible, puis détermine automatiquement si une connexion sans fil ou filaire est la meilleure pour servir de backbone de connexion inter-routeur.

1) Suivez d'abord les étapes de configuration pour établir une connexion entre le routeur et le nœud AiMesh via le WiFi.
2) Placez le nœud à l'emplacement idéal pour une couverture optimale. Reliez le port réseau local (LAN) du routeur AiMesh et le port réseau étendu (WAN) du nœud AiMesh à l'aide d'un câble Ethernet.



3) Le système AiMesh sélectionnera automatiquement le meilleur chemin pour la transmission de données, avec ou sans fil.

3.5 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.

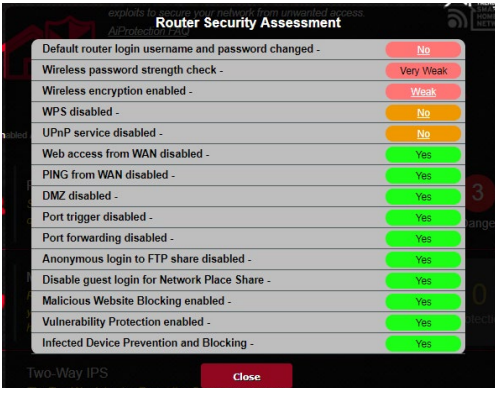
3.5.1 Configurer AiProtection

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

Pour configurer AiProtection :

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

Les résultats de l'analyse s'affichent 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.

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 pour aller à la page de configuration de l'élément.
   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. Cliquez sur **OK** à l'apparition du message de confirmation.

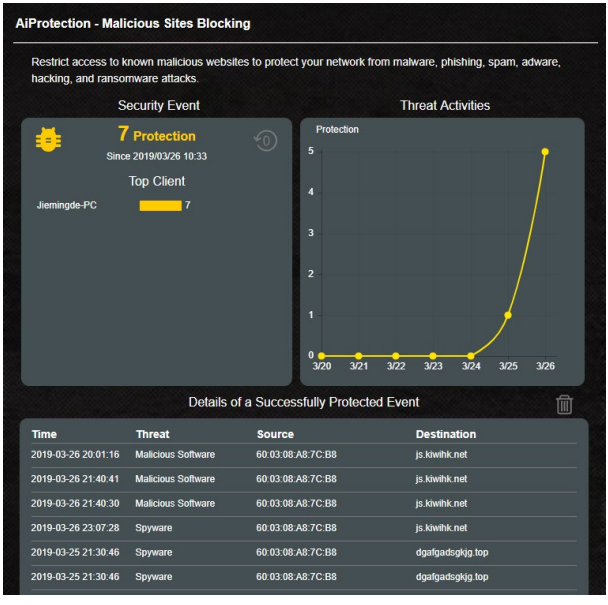
3.5.2 Blocage de sites malveillants

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 de AiProtection, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau de blocage des sites malveillants, cliquez sur **ON** (OUI).



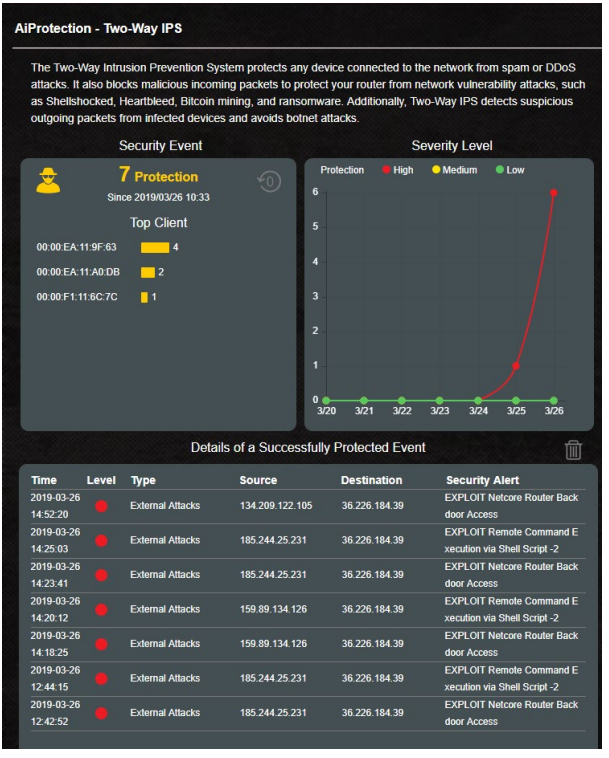
3.5.3 Two-Way IPS

Cette fonctionnalité résout les exploitations courantes pouvant subsister dans la configuration du routeur.

> **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 de AiProtection, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau Two-Way IPS, cliquez sur **ON** (OUI).



3.5.4 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.

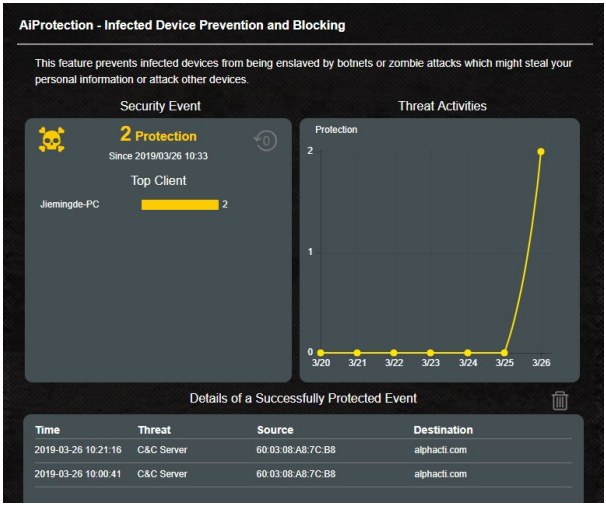
REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

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 de 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).

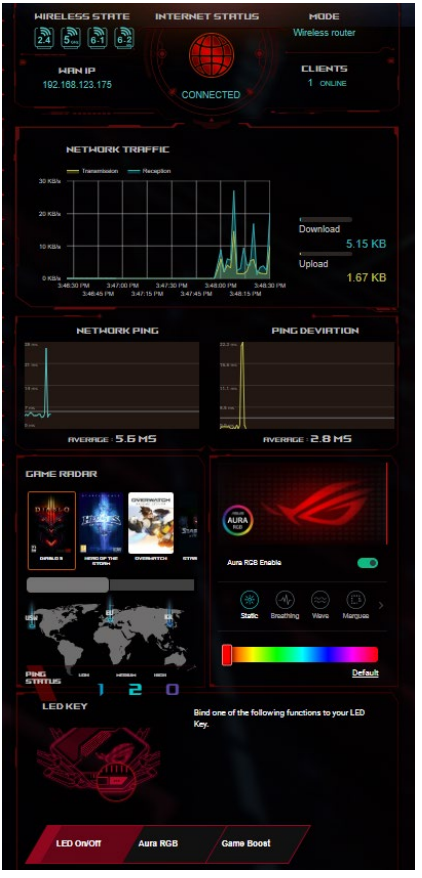
Pour configurer les préférences d'envoi d'alertes :

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).



3.6 Tableau de bord

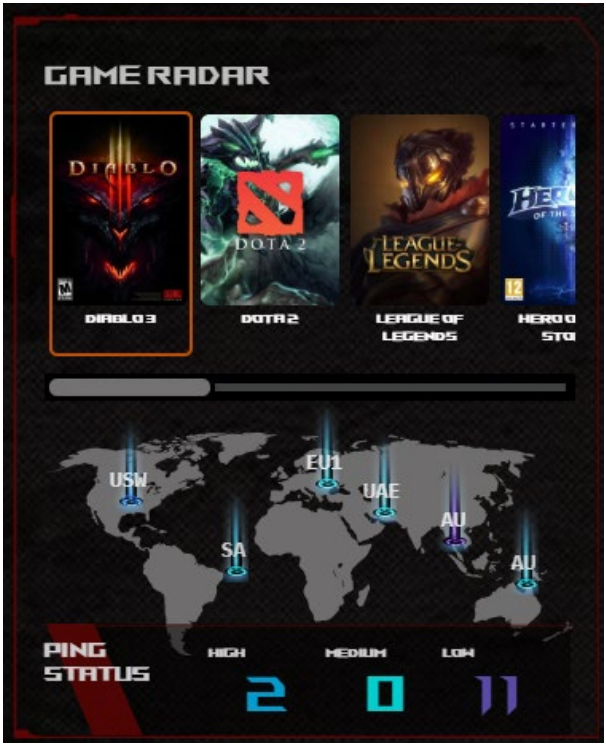
Le tableau de bord vous permet de surveiller le trafic en temps réel de votre environnement réseau et d'analyser le ping de réseau en temps réel ainsi que la déviation de ping.



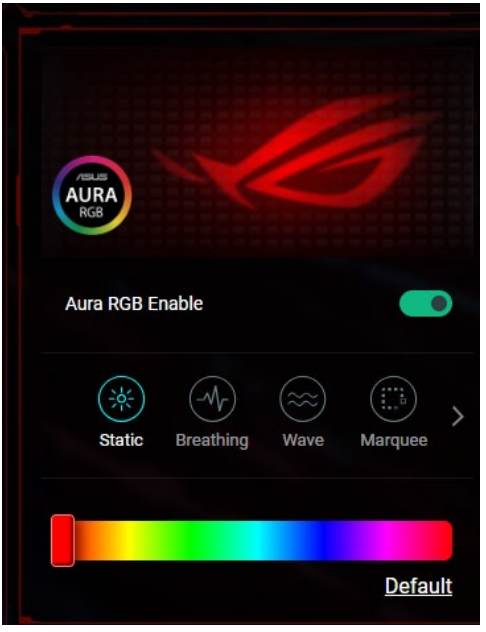
Le ping de réseau fait référence aux expériences de jeu en ligne. Plus le ping est élevé plus la latence est élevée pour les jeux en temps réel. Un ping de réseau inférieur à 99 ms est considéré comme de bonne qualité pour la plupart des jeux en ligne. Si le ping de réseau est inférieur à 150 ms, la qualité est considérée comme acceptable. En général, si le ping de réseau est supérieur à 150 ms, il est difficile de pouvoir jouer de manière fluide.

La déviation de ping influence aussi fortement l'expérience de jeu en ligne. Avec une déviation de ping élevée, il est plus facile de créer un toggle lors d'un jeu en ligne. Il n'existe pas de référence pour la déviation de ping. Toutefois, une faible déviation de ping est préférable.

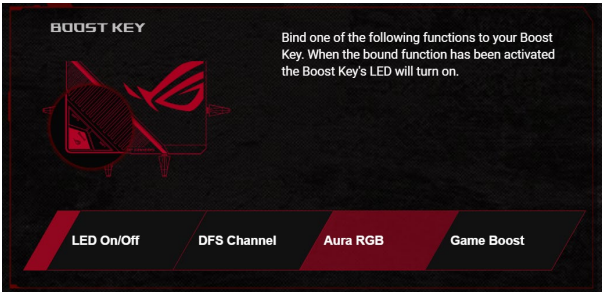
- **Game Radar :** La page Game Radar du tableau de bord vous donne un aperçu rapide du temps de ping pour un serveur spécifique.



- **Aura RGB :** Permet aux utilisateurs de configurer ou d'activer/désactiver Aura RGB depuis le tableau de bord. Vous pouvez choisir n'importe quelle couleur ou l'un des cinq effets lumineux.



- **Bouton LED :** Un bouton LED est placé sur votre routeur ROG Rapture. Sa fonction peut être définie depuis le tableau de bord.
  - Voyant allumé/éteint
  - Aura RGB activé/désactivé
  - Game Boost : activer/désactiver la priorisation des paquets réseau des jeux.



3.7 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.

3.7.1 General (Général)

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).

3.7.2 Filtrage d'URL

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

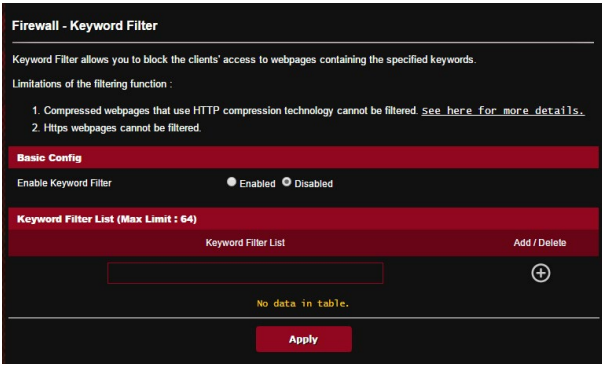
REMARQUE : Le filtrage d'URL est fondé sur les requêtes DNS. Si un client du réseau a déjà accédé à un site internet, celui-ci ne sera pas bloqué (un cache DNS stockant une liste des sites internet visités). Pour résoudre ce problème, effacez la mémoire cache dédiée au DNS avant d'utiliser le filtrage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

3.7.3 Filtrage de mots-clés

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



Pour configurer le filtrage de mots clés :

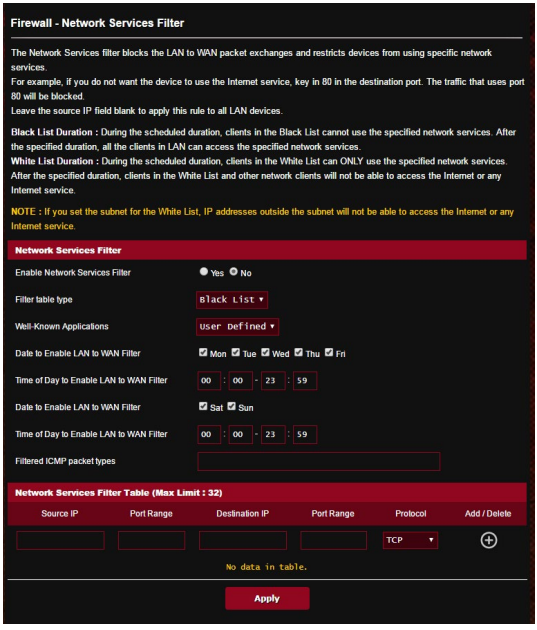
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > **Keyword Filter** (Filtrage de mots clés).
2. Dans le champ **Enable Keyword Filter** (Activer le filtrage de mots clés), cochez **Enabled** (Activer).
3. Saisissez un mot ou une phrase,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

3.7.4 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).

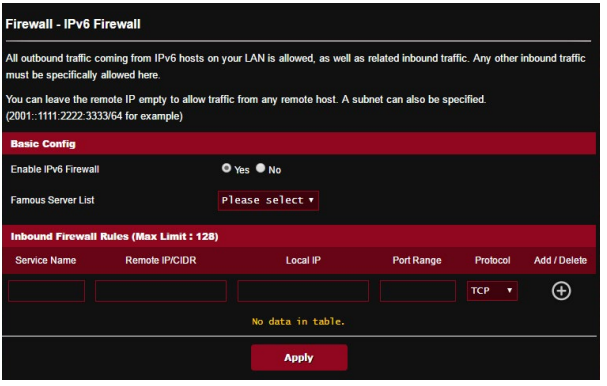


Pour configurer le filtrage de services réseau :

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. **Black List** (Liste noire) bloque les services réseau spécifiés. **White List** (Liste blanche) 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).

3.7.5 Pare-feu IPv6

Par défaut, votre routeur ASUS bloque tout le trafic entrant non sollicité. La fonction de pare-feu IPv6 permet toutefois d'autoriser le trafic entrant en provenance de services spécifiques.



3.8 Accélération de Jeu

Cette fonctionnalité vous permet d'activer Game Boost en un clic. Lorsque la fonctionnalité Game Boost est activée, le routeur ROG Rapture donne la priorité aux paquets de jeu pour vous offrir une expérience de jeu optimale.

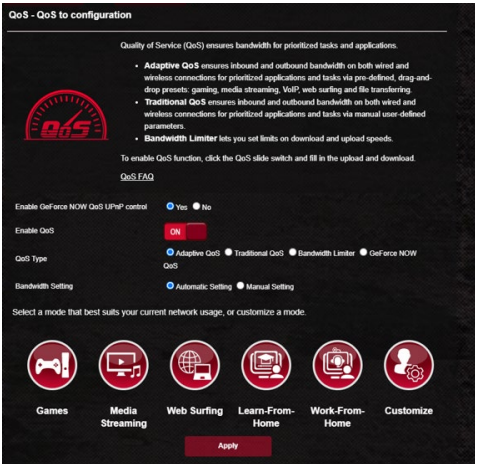
Game Boost

Pour activer Game Boost :

Dans **Game Boost**, déplacez le curseur **Enable Game Boost** (Activer Game Boost) sur **ON** (OUI).

3.8.1 QoS

Cette fonctionnalité permet d'assurer une bande passante suffisante pour les tâches et les applications prioritaires.



Pour activer la fonction QoS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Acceleration** (Accélération de jeu) > **QoS**.
2. À partir du panneau **Enable QoS** (Activer QoS), cliquez sur **ON** (OUI).
3. Sélectionnez le type de service QoS (adaptatif, standard ou limiteur de bande passante) de votre configuration.

   REMARQUE : La définition de chacun des types de service QoS est expliquée dans l'onglet QoS.

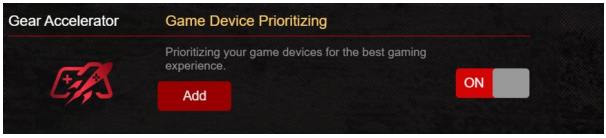
4. Cliquez sur **Automatic Setting** (Réglage automatique) pour une bande passante optimale ou sur **Manual Setting** (Réglage manuel) pour définir manuellement la bande passante (montante et descendante).

   REMARQUE : Obtenez vos informations de bande passante auprès de votre FAI (Fournisseur d'accès à Internet). Vous pouvez aussi vous rendre sur le site http://speedtest.net pour vérifier et obtenir vos informations de bande passante.

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

3.8.2 Gear Accelerator

La fonction Gear Accelerator vous permet de donner la priorité à vos périphériques de jeu sans fil via un panneau de contrôle en ligne, pour une meilleure expérience de jeu.



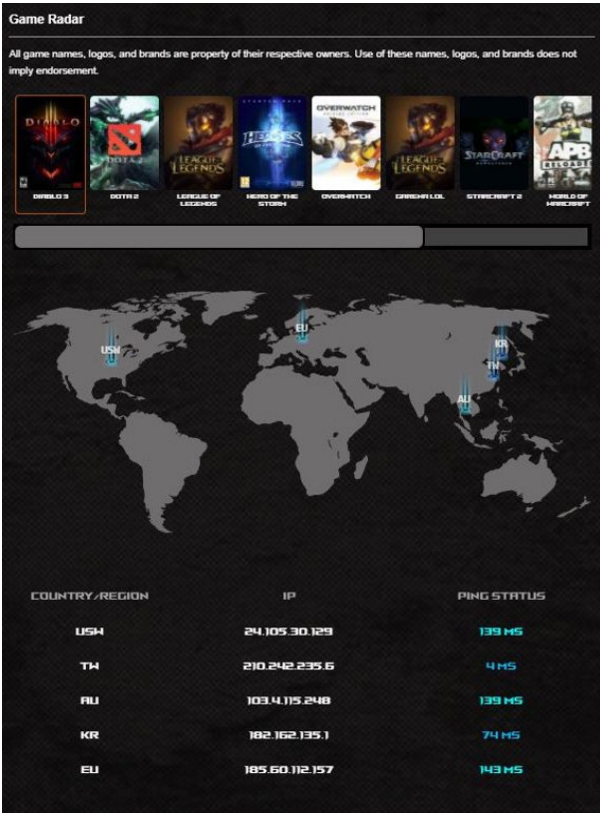
Pour configurer Gear Accelerator :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Acceleration** (Accélération de jeu).
2. Depuis l'onglet **Gear Accelerator**, cliquez sur **ON** (OUI).
3. Après avoir appliqué les réglages, cliquez sur **Add** (Ajouter) pour choisir le nom du client.
4. Cliquez sur ⊕ pour ajouter le profil du client.
5. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications

REMARQUE : Si vous souhaitez supprimer un profil client, cliquez sur ⊖

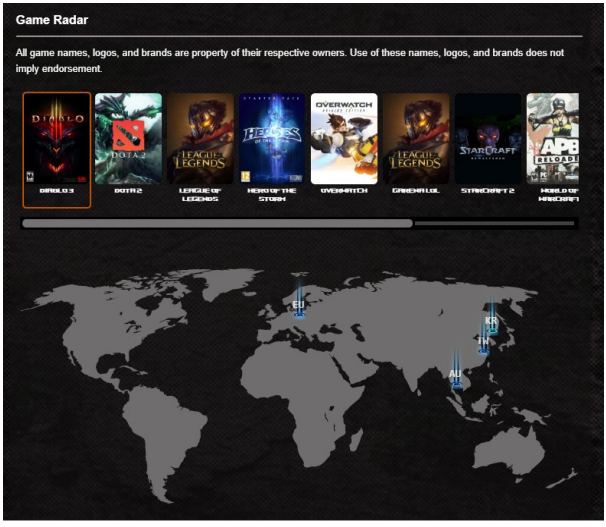
3.9 Game Radar

Game Radar est un outil de diagnostic qui vous aide à identifier la qualité de la connexion des serveurs pour des jeux spécifiques.



Pour utiliser Game Radar :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Radar** et sélectionnez un jeu de la liste.



2. Vérifiez le **Ping Status** (l'état de ping) de chaque serveur.
3. Pour une expérience de jeu en ligne fluide, sélectionnez un serveur de jeu disposant d'un état de ping faible.

3.10 Réseau invité Pro

Le réseau invité Pro (Guest Network Pro) est une version avancée du réseau invité qui est configurée au sein d'un réseau plus vaste, généralement dans une maison ou un bureau. Le réseau invité Pro est généralement utilisé pour fournir un accès internet aux visiteurs ou invités sans leur permettre d'accéder au réseau principal ou à d'autres appareils connectés. Il fournit également un filtre de contenu réseau utilisé pour bloquer ou autoriser l'accès à certains types de contenu en ligne sur le réseau.

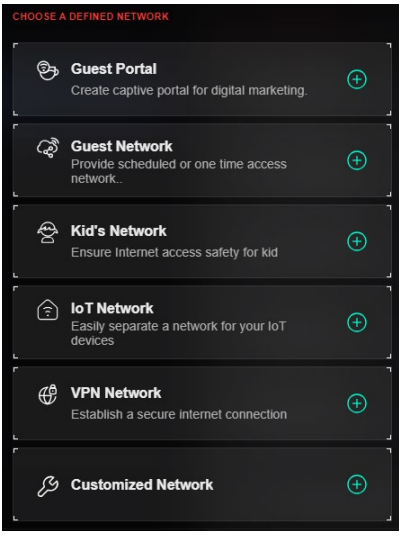
- **Guest Portal (Portail invité)**: Créez un portail captif pour le marketing numérique.
- **Réseau invité**: Créez un réseau invité avec une planification WiFi et des droits d'accès pour contrôler quand et comment les invités peuvent utiliser le réseau.
- **Kid's Network (Réseau pour enfants)**: Créez un réseau pour enfants qui bloque l'accès au contenu pour adultes* et dispose d'une planification pour contrôler la disponibilité du réseau.
- **IoT network (Réseau IoT)**: Créez un réseau Internet des objets (IoT) qui bloque le trafic malveillant* et permet uniquement aux appareils 2,4 GHz de se connecter.
- **VPN Network (Réseau VPN)**: Créez un réseau VPN qui se connecte à des services VPN tiers ou utilisez un VPN de site à site ASUS (https://www.asus.com/support/FAQ/1048281/) pour chiffrer votre connexion internet et masquer votre adresse IP, afin que vos activités en ligne ne soient pas suivies ou surveillées.

REMARQUES :

- Le routeur prend en charge jusqu'à cinq SSID (2,4 GHz + 5 GHz).
- Lorsqu'un réseau invité Pro est créé, un VLAN sera également créé dans les paramètres VLAN.
- Le filtre de contenu fonctionne grâce à des services DNS.

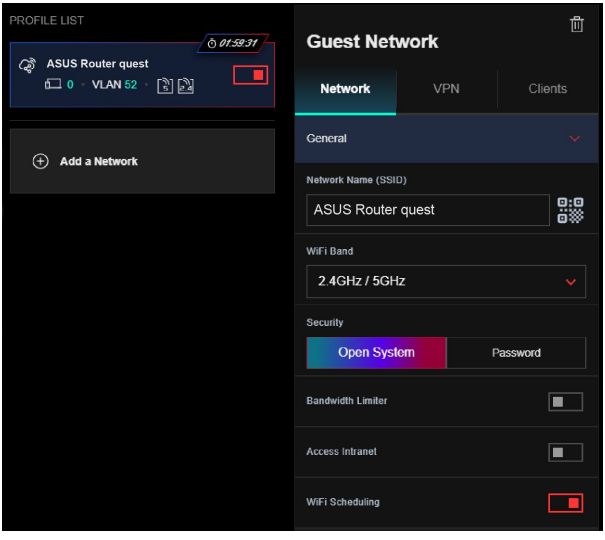
Pour configurer un réseau invité Pro :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Guest Network Pro** (Réseau invité Pro).
2. Cliquez sur **Add a Network** (Ajouter un réseau) pour créer un réseau invité Pro.

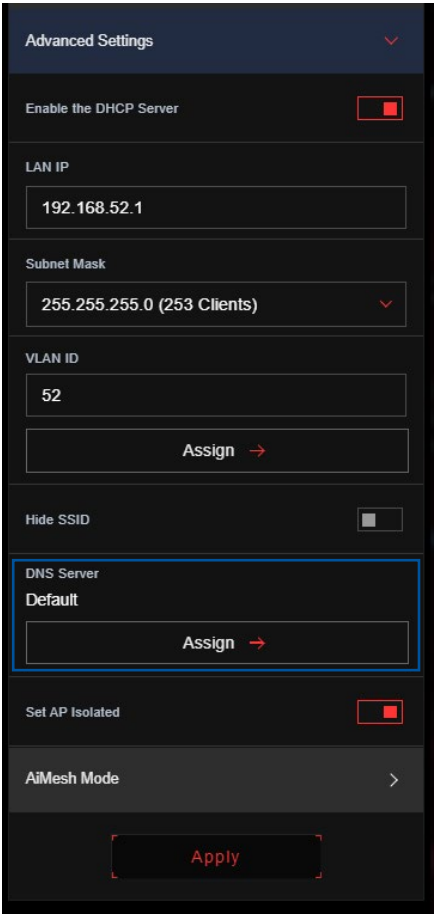


Pour attribuer un filtre dans un réseau invité Pro :

1. Créez un réseau invité Pro ou sélectionnez-en un dans la liste.
2. Cliquez sur **Advanced Settings** (Paramètres avancés).

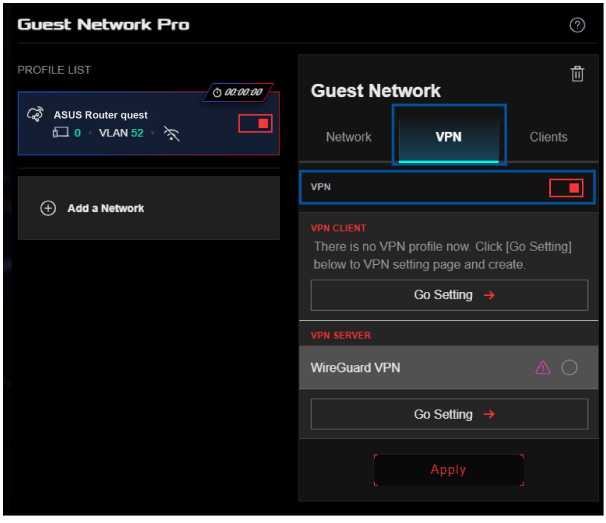


3. **Attribuer** un serveur DNS que vous souhaitez utiliser ou saisissez un serveur DNS personnalisé.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

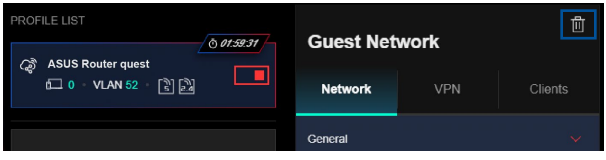


Pour attribuer un VPN dans un réseau invité Pro :

1. Créez un réseau invité Pro ou sélectionnez-en un dans la liste.
2. Cliquez sur l'onglet **VPN** et activez-le.
3. Sélectionnez un VPN dans la liste. S'il n'y a pas de client VPN sur votre routeur, cliquez sur **Go Setting** (Configurer) et suivez les instructions à l'écran pour en créer un.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

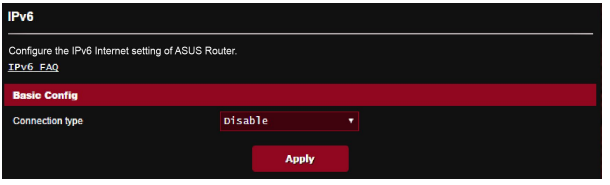


REMARQUE : Vous pouvez cliquer sur les paramètres d'un profil pour le modifier ou cliquer sur dans le coin supérieur droit pour le supprimer.



3.11 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).

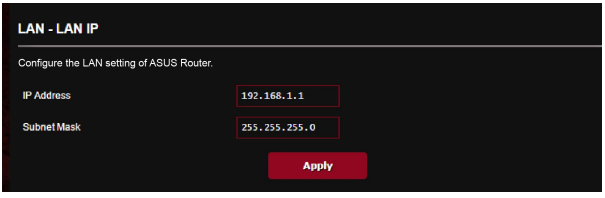
REMARQUE : Consultez votre FAI en cas de doute sur les informations nécessaires à la configuration de l'adressage IPv6.

3.12 Réseau local (LAN)

3.12.1 IP réseau local (LAN)

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.

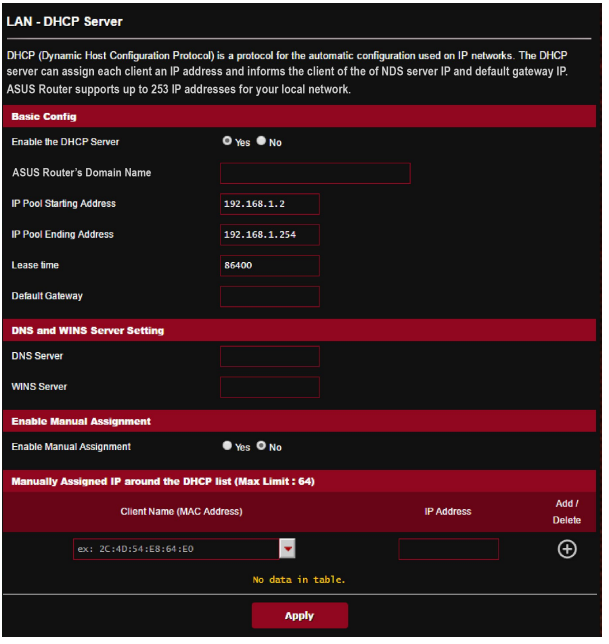


Pour modifier l'adresse IP du réseau local :

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).

3.12.2 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.



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 :

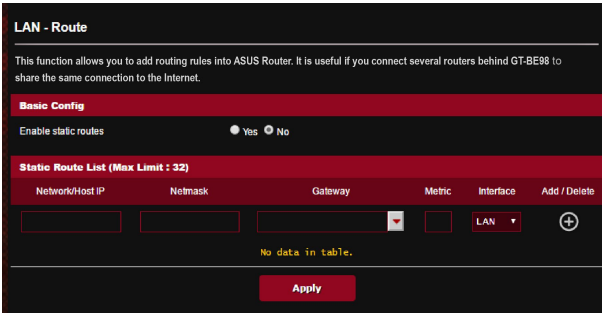
- Il est recommandé d'utiliser un format d'adresse IP de type 192.168.1.xxx (où xxx correspond à une valeur numérique comprise entre 2 et 254) lors de la saisie d'une plage d'adresses IP.
- L'adresse de départ d'une plage IP ne peut pas être supérieure à l'adresse de fin.

7. Dans la zone **DNS and 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.

3.12.3 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.

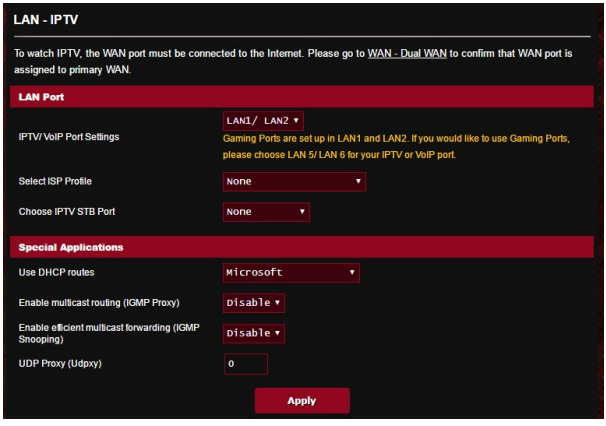


Pour configurer le tableau de routage :

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).

3.12.4 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.

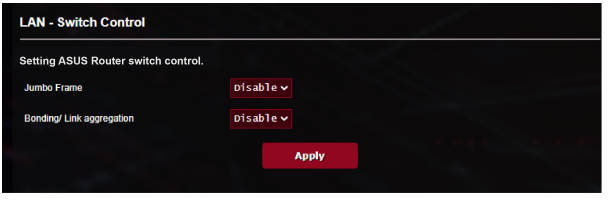


3.12.5 Contrôle de commutation

Permet de configurer le routeur pour la fonction de contrôle de commutation. Vous pouvez combiner deux ports réseau 10 Gb/s pour offrir un débit allant jusqu'à 20 Gb/s via une liaison à votre NAS compatible ou à un autre périphérique réseau à large bande passante.

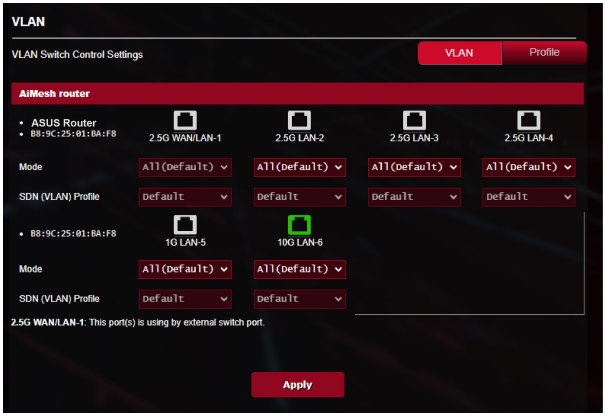
REMARQUES :

- Pour utiliser la fonction LACP (Protocole de contrôle d'agrégation de liens), les appareils doivent prendre en charge le protocole IEEE 802.3ad.
- La fonction d'agrégation du réseau local (LAN) peut être utilisée en associant les deux ports 10 Gb/s.



3.12.6 VLAN

Un VLAN (Réseau local virtuel) est un réseau logique créé au sein d'un réseau physique plus vaste. Les VLAN permettent de segmenter un réseau en sous-réseaux virtuels plus petits, qui peuvent être utilisés pour isoler le trafic et améliorer les performances du réseau.



Pour configurer un VLAN :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > **VLAN**.
2. Cliquez sur l'onglet **Profile** (Profil) puis sur ⊕ pour créer un profil VLAN. Vous pouvez attribuer votre propre identifiant VLAN.
3. **Port isolation** (Isolation de port) restreint le droit d'accès de différents appareils dans le même VLAN. Vous créez maintenant un "réseau VLAN uniquement", c'est-à-dire un réseau avec VID mais sans DHCP.

4. Cliquez sur l'onglet **VLAN** pour sélectionner un port avec un profil et un mode spécifiques (**Trunk** (Tronc) / **Access** (Accès)).

REMARQUE : Vous pouvez sélectionner l'un des modes par défaut suivants :

All (Tout) (par défaut) permet l'accès à tous les paquets balisés et non balisés.

Access (Accès) permet à un SDN (VLAN) sélectionné d'accéder. Vous pouvez sélectionner des profils créés par Guest Network Pro ou par VLAN.

Mode **Trunk** (Tronc) :

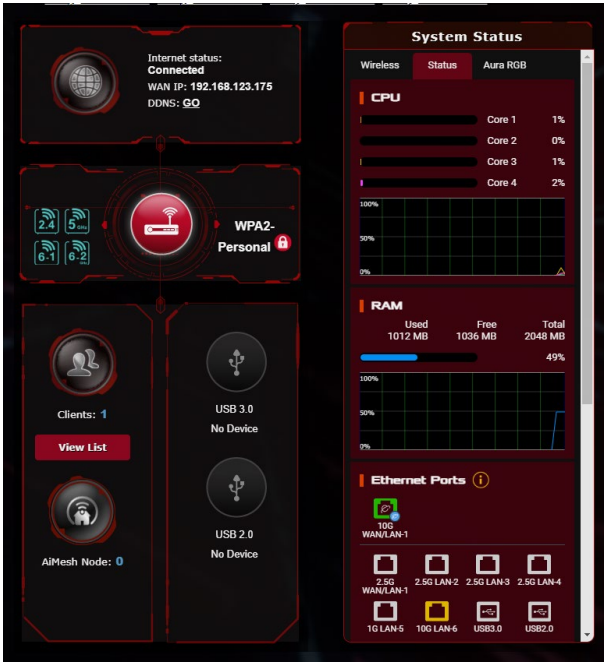
- **Allow all tagged (Autoriser tous les paquets balisés)** : Seuls les paquets balisés sont autorisés à accéder.
- **With selected SDN(VLAN) (Avec le SDN/VLAN sélectionné) :** Seuls les SDN ou VLAN sélectionnés sont autorisés à accéder.

5. Une fois terminé, cliquez sur **Apply** (Appliquer).

REMARQUE : Pour plus d'informations, consultez : https://www.asus.com/support/FAQ/1049415/.

3.13 Carte du réseau

La carte du réseau vous permet d'avoir une vue d'ensemble du réseau, mais aussi de configurer certains paramètres de sécurité, de gérer les clients du réseau et de surveiller les dispositifs USB connectés au routeur.



3.13.1 Configurer les paramètres de sécurité WiFi

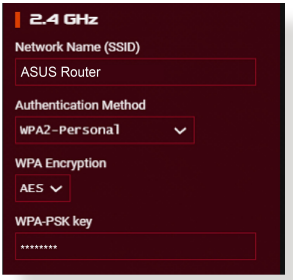
Pour protéger votre réseau WiFi contre les accès non autorisés, vous devez configurer les paramètres de sécurité du routeur.

Pour configurer les paramètres de sécurité WiFi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. La colonne **System Status** (État du système) affiche 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 connexions 2,4 GHz, 5 GHz-1, 5 GHz-2 et 6 GHz.

Paramètres de sécurité 2,4 GHz



Paramètres de sécurité 5 GHz-1

Paramètres de sécurité 5 GHz-2

Paramètres de sécurité 6 GHz

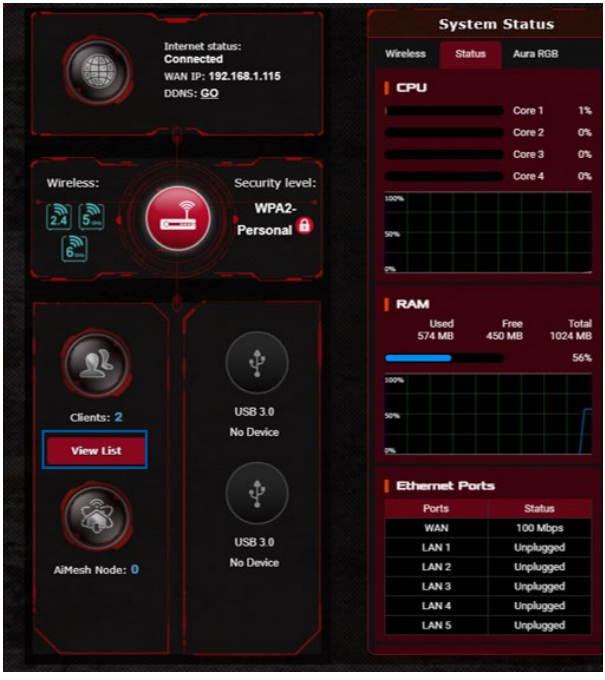
3. Dans le champ **Network Name (SSID)** (Nom du réseau (SSID)), spécifiez un nom unique pour votre réseau WiFi.
4. Dans le menu déroulant **Authentication Method** (Méthode d'authentification), sélectionnez la méthode de chiffrement.

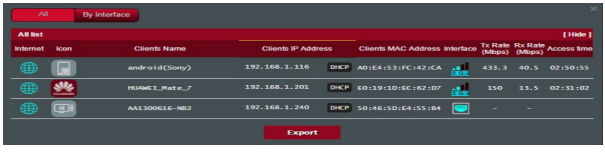
   Si vous sélectionnez WPA/WPA2/WPA3-Personal comme méthode de chiffrement, saisissez une clé de sécurité appropriée.

IMPORTANT ! La norme IEEE 802.11n/ac 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 Cliquez sur **Apply** (Appliquer) une fois terminé.

3.13.2 Gérer les clients du réseau



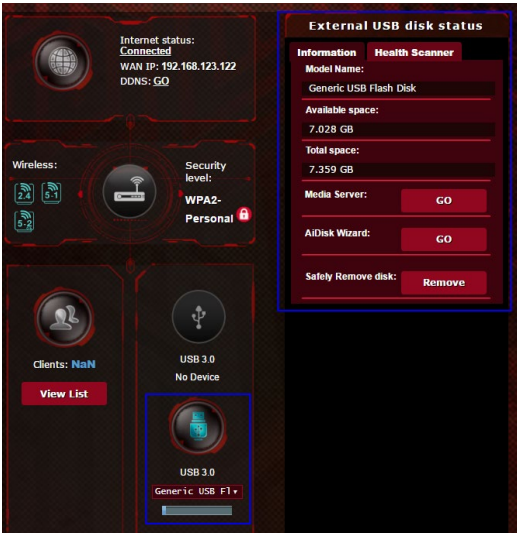


Pour gérer les clients de votre réseau :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Dans l'écran **Network Map** (Carte du réseau), cliquez sur l'icône **Clients** (Clients) pour afficher les informations relatives aux clients de votre réseau.
3. Cliquez sur View List (Afficher la liste) sous l'icône **Clients** pour afficher tous les clients.
4. Pour bloquer l'accès d'un client à votre réseau, sélectionnez le client, puis cliquez sur l'icône représentant un cadenas ouvert.

3.13.3 Surveiller un périphérique USB

Le routeur WiFi ASUS intègre deux ports USB pour la connexion de périphériques USB, tels qu'un périphérique de stockage ou une imprimante USB. Ces ports vous permettent de surveiller votre environnement de travail, partager des fichiers ou une imprimante avec les clients de votre réseau.



REMARQUES :

- Pour utiliser cette fonctionnalité, vous devez connecter un périphérique de stockage USB (ex : disque dur ou clé USB) à l'un des ports USB 2.0 / 3.0 situés à l'arrière de votre routeur WiFi. Assurez-vous que le périphérique de stockage USB est formaté et correctement partitionné. Visitez le site internet d'ASUS sur http://event.asus.com/networks/disksupport pour consulter la liste des formats de fichiers pris en charge
- Les ports USB prennent en charge deux lecteurs USB ou un lecteur USB plus une imprimante USB.

IMPORTANT ! Vous devrez d'abord créer un compte de partage (doté des permissions d'accès nécessaires) avant de pouvoir autoriser d'autres clients du réseau à accéder au périphérique USB par le biais d'un site FTP, des centres de serveurs, Samba ou AiCloud. Pour plus de détails, consultez les sections **3.19 Utiliser les applications USB** et **3.3 Utiliser AiCloud** de ce manuel.

Pour surveiller votre périphérique USB :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Dans l'écran Network Map (Carte du réseau), cliquez sur l'icône **USB Disk Status** (État de disque USB) pour afficher les informations du disque USB connecté au routeur WiFi.
3. Dans le champ AiDisk Wizard (Assistant AiDisk), cliquez sur **GO** pour configurer un serveur FTP permettant le partage de fichiers sur Internet.

REMARQUES :

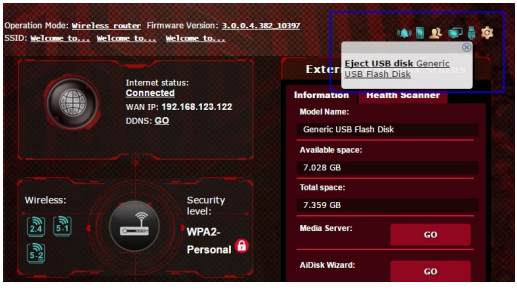
- Pour plus de détails, consultez la section **3.19.2 Utiliser les centres de serveurs** de ce manuel.
- Le routeur WiFi fonctionne avec la plupart des périphériques de stockage USB d'une capacité maximale de 4 To et prend en charge la lecture/écriture pour les formats de fichiers FAT16, FAT32, NTFS et HFS+.

Éjecter un disque USB

IMPORTANT ! Une mauvaise éjection du périphérique de stockage USB peut endommager les données contenues sur le disque.

Pour éjecter un disque USB en toute sécurité :

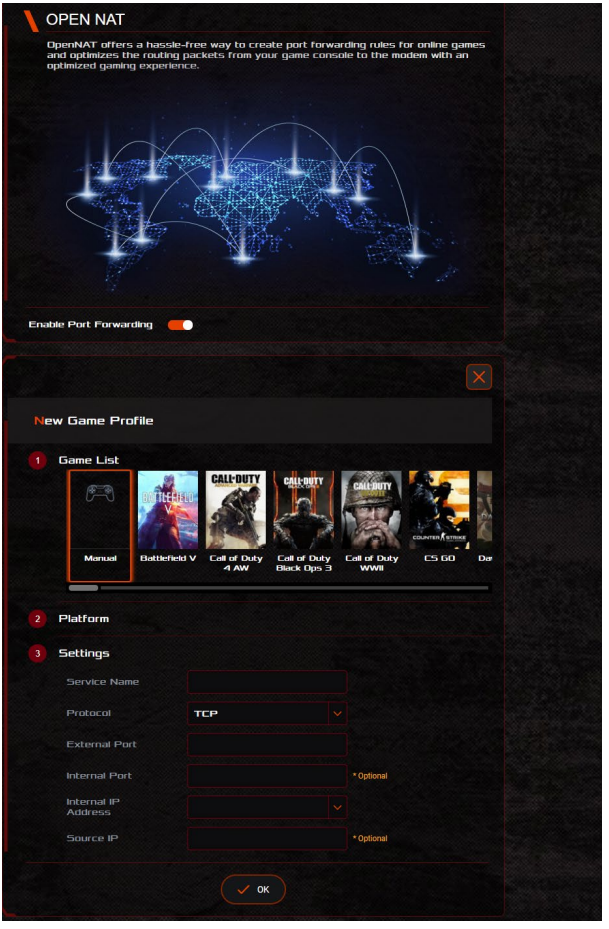
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Cliquez d'abord sur l'icône  située dans le coin supérieur droit de l'écran, puis sur l'option **Eject USB disk** (Éjecter le disque USB). Lorsque le disque a été éjecté, l'état du disque apparaît comme étant **Unmounted** (Non monté).



3.14 Open NAT & Profil de jeu

Open NAT vous offre une manière simple de créer des règles de redirection de port pour les jeux en ligne et ainsi optimiser le routage des paquets réseau entre votre console de jeu et le modem, pour une expérience de jeu optimisée.

En jouant sur ordinateur ou sur console de jeu, certains problèmes de connexion peuvent apparaître en raison du FAI ou des paramètres du routeur de votre environnement tels que le NAT et les blocs port. Game Profile (Profil de jeu) garantit que le routeur ROG Rapture ne bloque pas la connexion au jeu.



Pour configurer Open NAT :

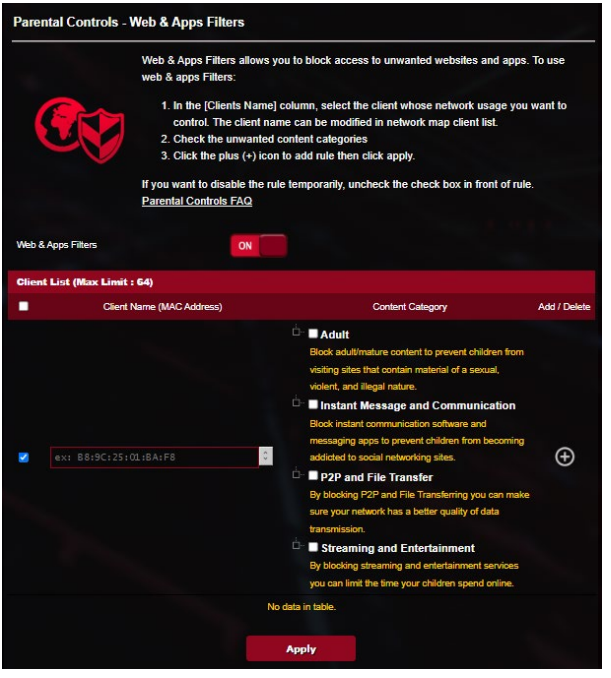
1. À partir du volet de navigation, cliquez sur **General** (Général) > **Open NAT**.
2. Activez **Enable Port Forwarding** (Activer la redirection de port).
3. Dans la **Liste de jeux**, sélectionnez votre jeu et effectuez les réglages de base.
4. Cliquez sur **OK**.

3.15 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 activer Two-Way IPS :

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 :

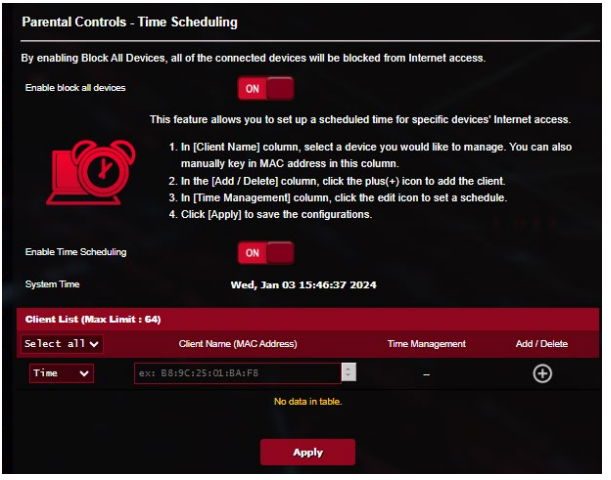
1. À partir du volet de navigation, cliquez sur **General** (Général) > **Parental Controls** (Contrôles parentaux).

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.

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.



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.

3.16 Smart Connect

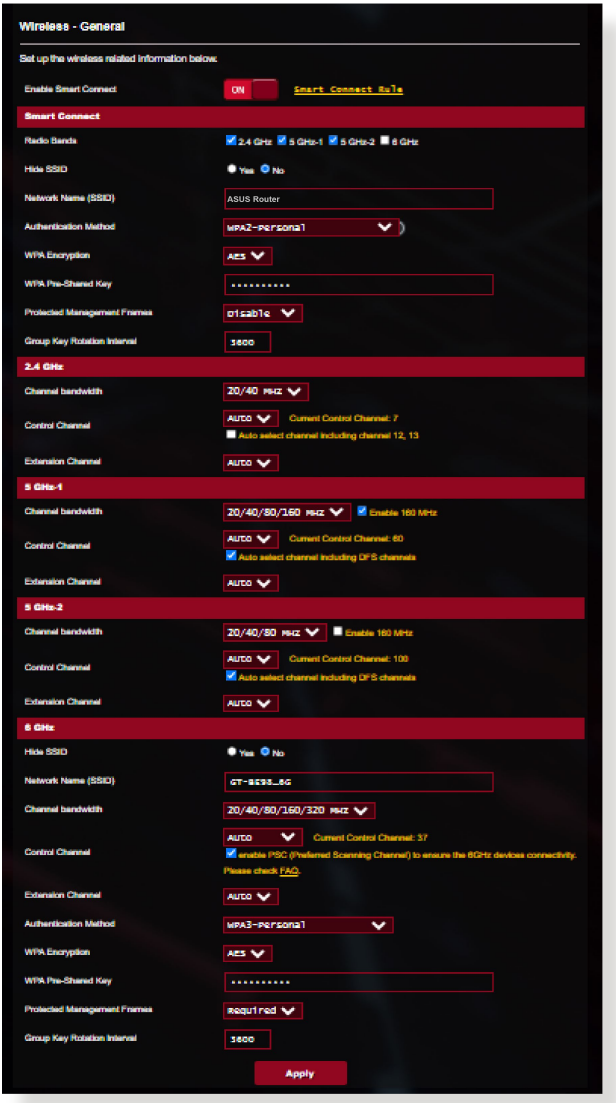
Smart Connect est conçu pour diriger automatiquement les clients vers l'une des quatre bandes (2,4 GHz, 5 GHz-1, 5 GHz-2 et 6 GHz) pour optimiser l'utilisation de la bande passante.

3.16.1 Configurer Smart Connect

Vous pouvez activer Smart Connect depuis l'interface de gestion des deux façons suivantes :

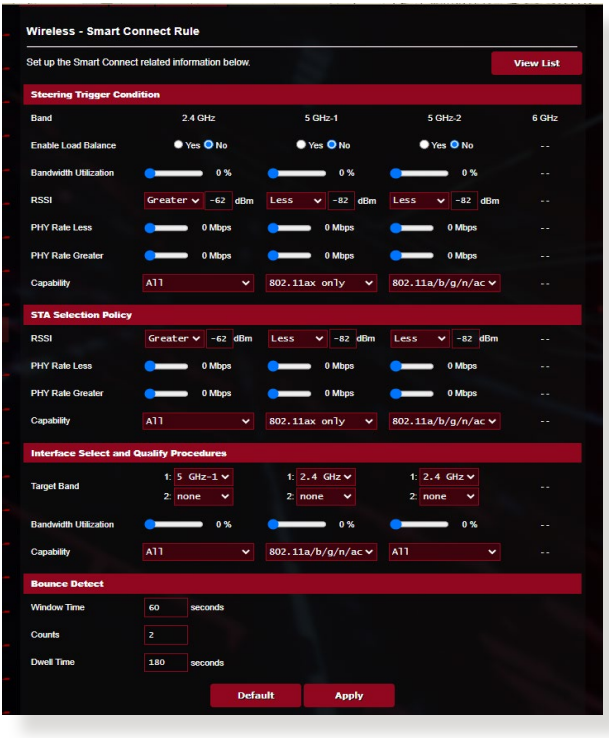
- ***Depuis l'écran de configuration "WiFi" (Paramètres avancés)***

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 fenêtre de connexion, saisissez le nom d'utilisateur par défaut (**admin**) et le mot de passe (**admin**), puis cliquez sur **OK**. L'assistant de configuration internet s'exécute automatiquement.
3. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **General** (Général).
4. Déplacez l'interrupteur de l'élément **Enable Smart Connect** (Activer Smart Connect) sur **ON** (OUI) pour activer cette fonction permettant de connecter automatiquement les clients WiFi à la bande de fréquence appropriée pour une vitesse optimale. Cette fonction permet de connecter automatiquement les clients WiFi à la bande de fréquence appropriée pour une vitesse optimale.


Wireless - General
Set up the wireless related information below.
Enable Smart Connect
ON
Smart Connect Rule
Smart Connect
Radio Bands
2.4 GHz
5 GHz-1
5 GHz-2
6 GHz
Hide SSID
Yes
No
Network Name (SSID)
ASUS Router
Authentication Method
WPA2-Personal
WPA Encryption
AES
WPA Pre-Shared Key
Protected Management Frames
Disable
Group Key Rotation Interval
3600
2.4 GHz
Channel bandwidth
20/40 MHz
Control Channel
AUTO
Current Control Channel: 7
Auto select channel including channel 12, 13
Extension Channel
AUTO
5 GHz-1
Channel bandwidth
20/40/80/160 MHz
Enable 160 MHz
Control Channel
AUTO
Current Control Channel: 60
Auto select channel including DFS channels
Extension Channel
AUTO
5 GHz-2
Channel bandwidth
20/40/80 MHz
Enable 160 MHz
Control Channel
AUTO
Current Control Channel: 100
Auto select channel including DFS channels
Extension Channel
AUTO
6 GHz
Hide SSID
Yes
No
Network Name (SSID)
GT-BE98_6G
Channel bandwidth
20/40/80/160/320 MHz
Control Channel
AUTO
Current Control Channel: 37
enable PSC (Preferred Scanning Channel) to ensure the 6GHz devices connectivity.
Please check FAQ.
Extension Channel
AUTO
Authentication Method
WPA3-Personal
WPA Encryption
AES
WPA Pre-Shared Key
Protected Management Frames
Required
Group Key Rotation Interval
3600
Apply

3.16.2 Règles de Smart Connect

ASUSWRT fournit des paramètres par défaut pour déclencher le mécanisme de commutation. Vous pouvez également modifier les conditions de déclenchement en fonction de l'environnement de mise en réseau. Pour modifier les paramètres, allez dans l'onglet **Règles de Smart Connect** dans la section Network Tools (Outils réseau).

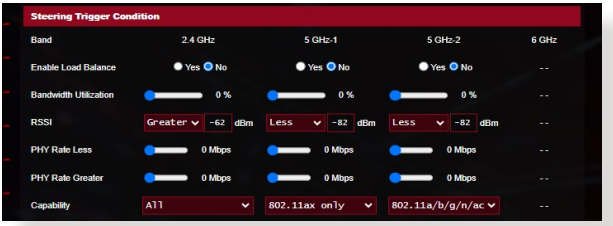


Les commandes des règles de Smart Connect sont divisées en quatre sections :

- Steering Trigger Condition (Conditions de déclenchement de redirection)
- STA Selection Policy (Politique de sélection de la station STA)
- Interface Select and Qualify Procedures (Sélection de l'interface et procédures de qualité)
- Bounce Detect (Détecteur de rebonds)

Steering Trigger Condition (Conditions de déclenchement de redirection)

Cet ensemble de commandes définit les critères pour lancer la redirection de bande.



- **Bandwidth Utilization (Utilisation de bande passante)**

  Si l'utilisation de la bande passante dépasse ce pourcentage, la redirection est lancée.
- **Enable Load Balance (Activer l'équilibrage des charges)**

  Cet élément contrôle l'équilibrage des charges.
- **RSSI**

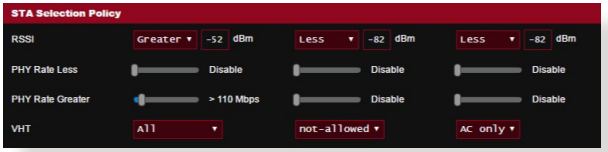
  Si le niveau du signal reçu répond à ce critère, la redirection est déclenchée.
- **PHY Rate Less (Réduire le taux PHY) / PHY Rate Greater (Augmenter le taux PHY)**

  Ces commandes déterminent le taux des liaisons STA pour déclencher la redirection de bande.
- **VHT**

  Cette commande détermine comment les clients 802.11ac et non ac sont traités.
  - **ALL (TOUS)** (par défaut) signifie que tous les types de clients peuvent déclencher la redirection.
  - **AC only** (AC uniquement) signifie qu'un client doit prendre en charge 802.11ac pour déclencher la redirection.
  - **Not-allowed** (Non autorisé) signifie que seuls les clients non 802.11ac déclenchent la redirection, tels que 802.11a/b/g/n.

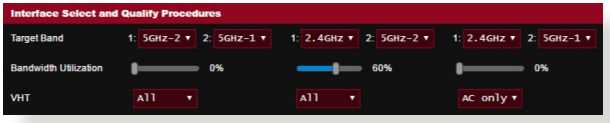
STA Selection Policy (Politique de sélection de la station STA)

Une fois la redirection déclenchée, ASUSWRT suit la politique de sélection STA pour sélectionner un client (STA) qui va être redirigé vers la bande la plus appropriée.



Interface Select and Qualify Procedures (Sélection de l'interface et procédures de qualité)

Ces commandes déterminent où le client redirigé aboutira. Les commandes **Target Band** (Bande cible) spécifient le premier et le deuxième choix de redirection. Les clients répondant aux critères de sélection STA pour la radiodiffusion seront orientés vers la première cible si la **Bandwidth Utilization** (Utilisation de la bande passante) est inférieure à la valeur définie. Dans le cas contraire, le client sera envoyé à la deuxième cible.



Bounce Detect (Détecteur de rebonds)

Cet ensemble de commandes détermine la fréquence à laquelle un client peut être redirigé. Ceci est destiné à éviter aux clients de se déplacer constamment. Cependant, cela n'empêche pas les clients de se déconnecter de leur propre initiative, ou de se compter eux-mêmes comme un rebond. Chaque client peut être redirigé N **Counts** (fois) dans la **Window Time** (Fenêtre de temps). Si le nombre limite est atteint, le client ne sera pas redirigé pendant le **Dwell Time** (Temps d'arrêt).

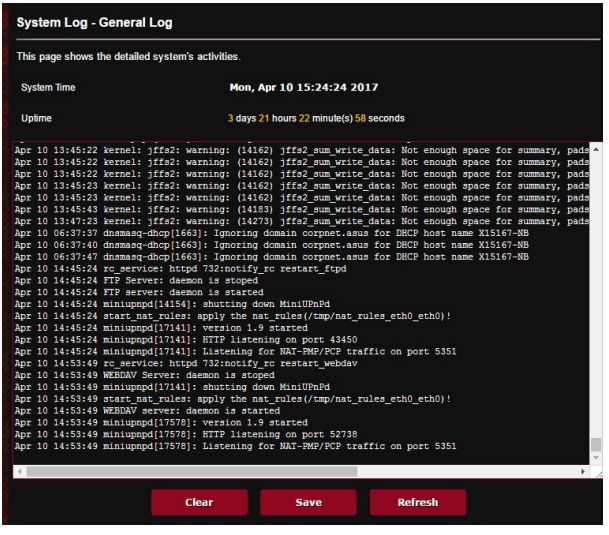
3.17 Journal système

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.

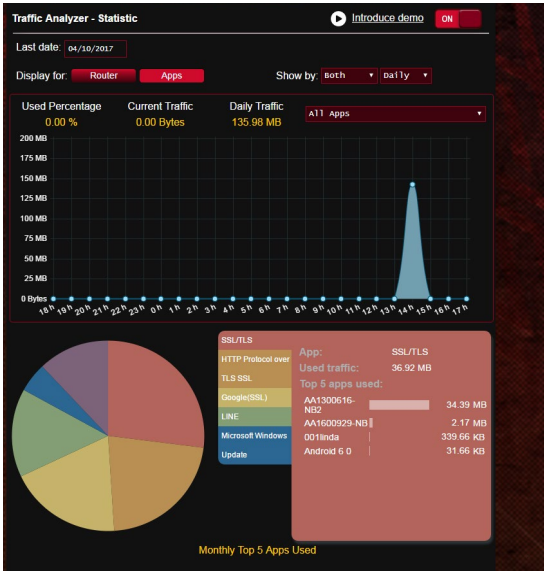
Pour afficher le journal système :

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



3.18 Dispositif d'analyse du trafic

Le dispositif d'analyse du trafic vous donne un aperçu rapide des événements de votre réseau de manière quotidienne, hebdomadaire ou mensuelle. Il vous permet de visualiser rapidement l'utilisation de la bande passante de chaque utilisateur, les appareils et applications utilisées, pour vous aider à réduire les congestions de votre connexion internet. C'est aussi un moyen de surveiller l'utilisation et les activités internet des utilisateurs.



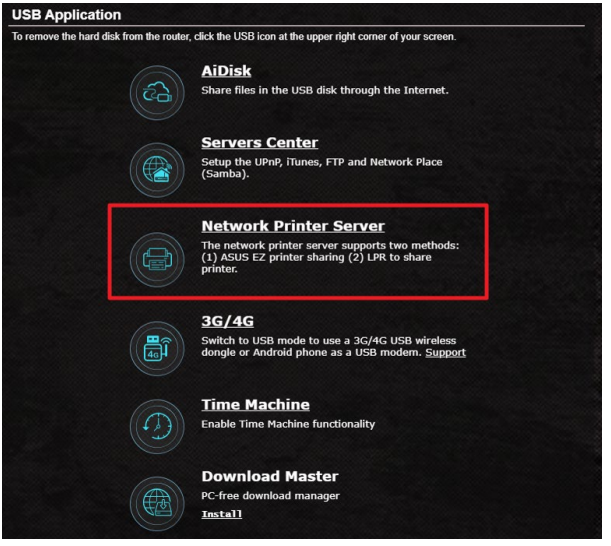
Pour configurer le dispositif d'analyse du trafic :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Traffic Analyzer** (Dispositif d'analyse du trafic).
2. À partir de la page principale de **Traffic Analyzer** (Dispositif d'analyse du trafic), activez les statistiques du dispositif d'analyse du trafic.
3. Sélectionnez la date du graphique à afficher.
4. Dans le champ **Display for** (Afficher pour), sélectionnez Router (Routeur) ou Apps (Applications) pour afficher les informations de trafic.
5. Dans le champ Show by (Afficher par), sélectionnez comment afficher les informations de trafic.

3.19 Application USB

La page des applications USB contient les sous-menus AiDisk, Servers Center (Centres de serveurs), Network Printer Server (Serveur d'impression réseau) et Download Master.

IMPORTANT ! Pour utiliser la fonction de serveur multimédia, vous devez connecter un périphérique de stockage USB (ex : disque dur ou clé USB) au port USB 3.0 situé à l'arrière du routeur WiFi. Assurez-vous que le périphérique de stockage USB est formaté et correctement partitionné. Rendez-vous sur le site internet d'ASUS sur http://event.asus.com/2009/networks/disksupport/ pour plus de détails.

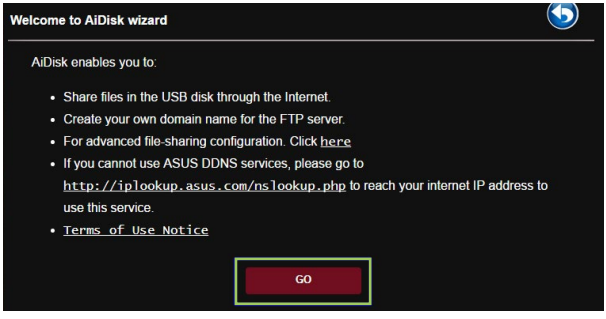


3.19.1 Utiliser AiDisk

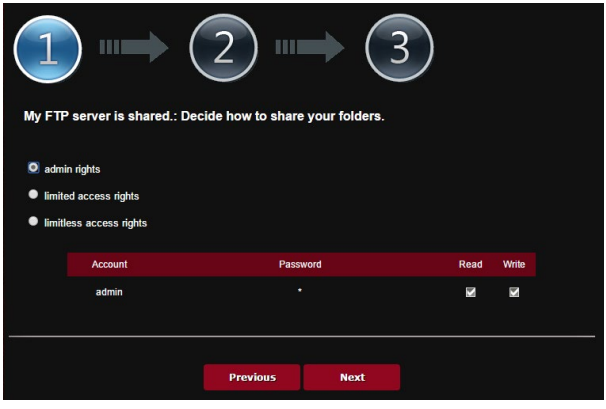
AiDisk vous permet de partager les fichiers contenus sur un périphérique de stockage USB connecté au routeur via Internet. AiDisk offre aussi la possibilité de configurer le service DDNS d'ASUS ou un serveur FTP.

Pour utiliser AiDisk :

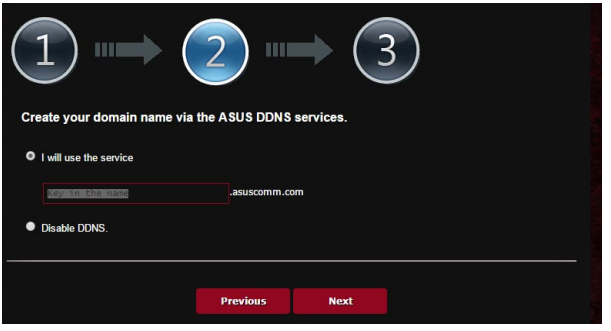
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB Application** (Applications USB) > icône **AiDisk**.
2. À partir de l'écran Welcome to AiDisk wizard (Bienvenue sur l'assistant AiDisk), cliquez sur **Go** (Démarrer).



3. Définissez les droits d'accès des différents clients accédant aux données partagées.



4. Si vous souhaitez créer votre propre nom de domaine dédié au serveur FTP grâce au service DDNS d'ASUS, sélectionnez **I will use the service and accept the Terms of service** (Je souhaite utiliser ce service et en accepte les conditions) et spécifiez le nom de votre domaine. Cliquez sur **Next** (Suivant).



   Vous pouvez aussi sélectionner **Skip ASUS DDNS settings** (Ignorer la configuration du service DDNS ASUS), puis cliquez sur **Next** (Suivant) pour ignorer cette étape.

5. Cliquez sur **Finish** (Terminé) pour terminer la configuration.
6. Pour accéder au site FTP que vous venez de créer, ouvrez votre navigateur internet ou un client FTP tiers et saisissez l'adresse suivante : **(ftp://<nom de domaine>.asuscomm.com)**.

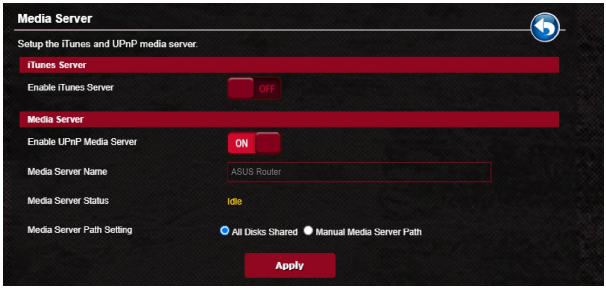
3.19.2 Utiliser les centres de serveurs

Les centres de serveurs vous permettent de partager vos fichiers à partir d'un disque USB par le biais des protocoles DLNA, Samba et FTP. Vous pouvez aussi configurer d'autres paramètres pour le disque USB dans les centres de serveurs.

Utiliser le service de partage DLNA

Votre routeur WiFi autorise les appareils compatibles avec le protocole UPnP à accéder aux fichiers multimédia stockés sur un disque de stockage USB connecté au routeur.

REMARQUE : Avant d'utiliser le partage de fichiers via le protocole UPnP, connectez votre appareil au réseau du routeur WiFi.

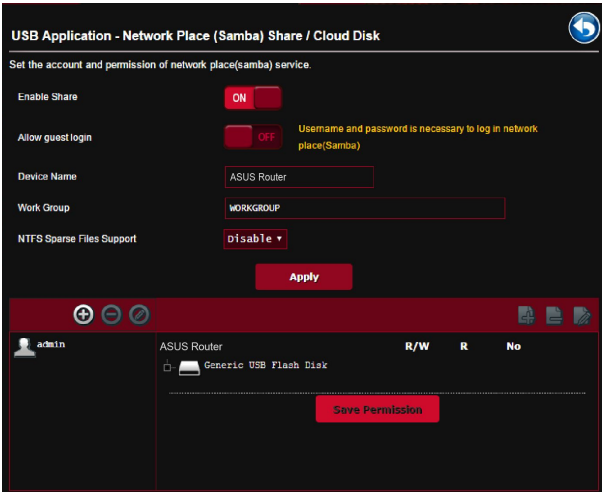


Pour utiliser le service de partage DLNA, allez dans **Advanced Settings** (Paramètres avancés) > **USB Application** (Applications USB) > **Media Servers** (Serveurs multimédia). Vous trouverez ci-dessous une description de chacun des champs disponibles :

- **Enable iTunes Server? (Activer le serveur iTunes ?) ?**: Déplacez l'interrupteur ON/OFF pour activer ou désactiver le serveur iTunes.
- **Enable UPnP Media Server (Activer le serveur UPnP)**: Déplacez l'interrupteur ON/OFF pour activer ou désactiver le serveur UPnP.
- **Media Server Status (État du serveur)**: Affiche l'état du serveur.
- **Media Server Path Setting (Répertoire de partage)**: Sélectionnez le répertoire du serveur multimédia et cliquez sur Apply (Appliquer) pour partager le contenu d'un répertoire du disque USB avec les clients du réseau.

Utiliser le service de partage Samba

Le partage Samba vous permet de configurer des comptes de partage et leurs permissions d'accès au service Samba.



Pour utiliser le partage Samba :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB Application** (Applications USB) > **Network Place (Samba) Share / Cloud Disk** (Partage de favoris réseau (Samba) / Cloud Disk).

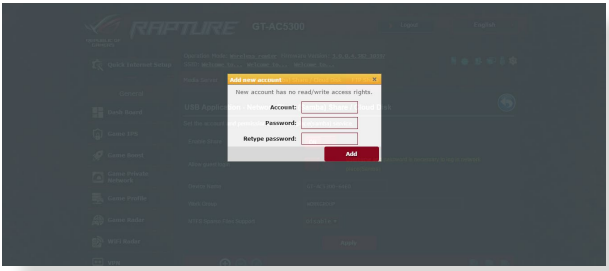
   REMARQUE : Le partage Samba est activé par défaut.

2. Suivez les instructions suivantes pour ajouter, supprimer ou modifier un compte de partage.

Pour créer un nouveau compte :

a) Cliquez sur ⊕ pour ajouter un compte.

b)Remplissez les champs **Account** (Compte) et **Password** (Mot de passe). Ressaisissez le mot de passe pour le confirmer. Cliquez sur **Add** (Ajouter) pour ajouter le compte.



Pour supprimer un compte existant :

a) Sélectionnez le compte à supprimer.

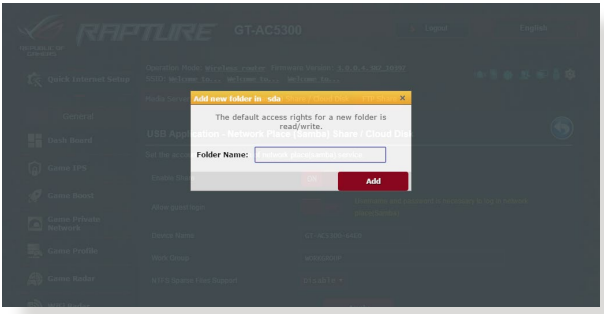
b) Cliquez sur .

c) À l'apparition de la fenêtre de confirmation, cliquez sur **Delete** (Supprimer) pour confirmer la suppression.

Pour ajouter un dossier :

a) Cliquez sur .

b) Spécifiez le nom du dossier, et cliquez sur **Add** (Ajouter). Le dossier créé sera ajouté à la liste des dossiers partagés.



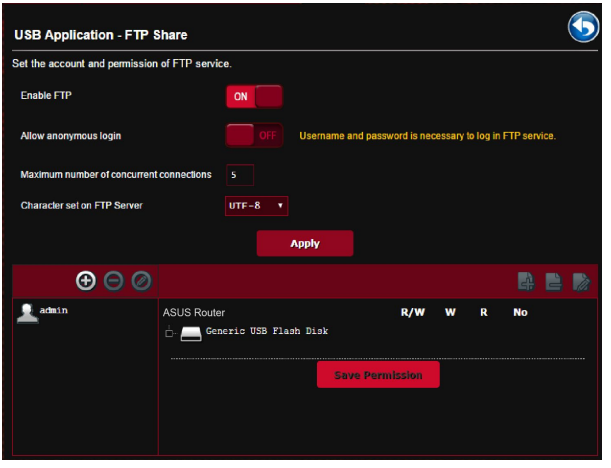
3. Dans la liste des fichiers/dossiers, sélectionnez le type de droits d'accès à affecter aux différents types de fichiers/dossiers :
   - **R/W**: Sélectionnez cette option pour affecter un droit de lecture/écriture à un type spécifique de fichier/dossier.
   - **R**: Sélectionnez cette option pour affecter un accès en lecture seule à un type spécifique de fichier/dossier.
   - **No (Non)**: Sélectionnez cette option si vous ne souhaitez pas partager un type spécifique de fichier/dossier.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Utiliser le service de partage FTP

Le routeur WiFi ASUS vous permet de partager les fichiers contenus sur un périphérique de stockage USB, via un serveur FTP, avec d'autres ordinateurs du réseau local, via Internet.

IMPORTANT !

- Assurez-vous de retirer le périphérique USB en toute sécurité. Une mauvaise éjection du périphérique de stockage USB peut endommager les données contenues sur le disque.
- Pour plus de détails sur l'éjection en toute sécurité d'un lecteur USB, consultez la sous-section **Éjecter un disque USB** de la section **3.13.3 Surveiller un périphérique USB**.



Pour utiliser le service de partage FTP :

REMARQUE : Assurez-vous d'avoir configuré votre serveur FTP avec AiDisk. Pour plus de détails, consultez la section **3.19.1 Utiliser AiDisk**.

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB Application** (Applications USB) > **FTP Share** (Partage FTP).

2. Dans la liste des fichiers/dossiers, sélectionnez le type de droits d'accès à affecter aux différents types de fichiers/dossiers :
   - **R/W**: Sélectionnez cette option pour affecter un droit de lecture/écriture à un type spécifique de fichier/dossier.
   - **W**: Sélectionnez cette option pour affecter un accès en écriture seule à un type spécifique de fichier/dossier.
   - **R**: Sélectionnez cette option pour affecter un accès en lecture seule à un type spécifique de fichier/dossier.
   - **No (Non)**: Sélectionnez cette option si vous ne souhaitez pas partager un type spécifique de fichier/dossier.
3. Vous pouvez également autoriser les connexions anonymes en déplaçant l'interrupteur du champ **Allow anonymous login** (Autoriser les connexions anonymes) sur **ON** (OUI).
4. Dans le champ **Maximum number of concurrent connections** (Nombre maximum de connexions simultanées), entrez le nombre maximum d'appareils pouvant se connecter simultanément au serveur FTP.
5. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.
6. Pour accéder au serveur FTP, entrez le lien ftp **ftp://<nomd'hôte>.asuscomm.com** ainsi que votre nom d'utilisateur et mot de passe dans la barre d'adresse de votre navigateur internet ou d'un client FTP tiers.

3.19.3 3G/4G

Des modems 3G/4G USB peuvent être connectés au routeur pour permettre un accès à Internet.

REMARQUE : Rendez-vous sur le site http://event.asus.com/2009/networks/3gsupport/ pour consulter la liste des modems compatibles

Pour configurer une connexion internet 3G/4G :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **3G/4G**.
2. Dans le champ **Enable USB Modem** (Activer le modem USB), cochez **Yes** (Oui).
3. Réglez les options suivantes :
   - **Location (Emplacement)**: Sélectionnez l'emplacement de votre fournisseur de service 3G/4G.
   - **ISP (FAI)**: Sélectionnez votre FAI (Fournisseur d'accès internet).
   - **APN (Access Point Name) service (optional) (Service d'accès internet WiFi (optionnel))**: Contactez votre fournisseur d'accès 3G/4G pour plus de détails.
   - **Dial Number (Numéro à composer)** et **PIN code (Code PIN)**: Entrez le numéro d'accès et le code PIN de votre fournisseur d'accès 3G/4G.

   REMARQUE : Le code PIN peut varier en fonction du fournisseur d'accès.

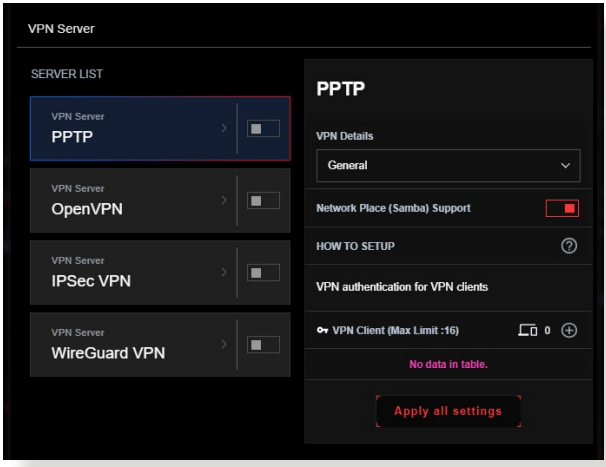
   - **Username / Password (Nom d'utilisateur / Mot de passe)** : Entrez le nom d'utilisateur et le mot de passe fournis par votre fournisseur d'accès 3G/4G.
   - **USB Adapter (Adaptateur USB)**: Choisissez votre adaptateur 3G / 4G USB à partir du menu déroulant. Si vous n'êtes pas certain du modèle ou si celui-ci n'apparaît pas dans la liste, sélectionnez **Auto**.
4. Cliquez sur **Apply** (Appliquer).

REMARQUE : Le routeur doit redémarrer pour que les modifications puissent prendre effet.

3.20 VPN

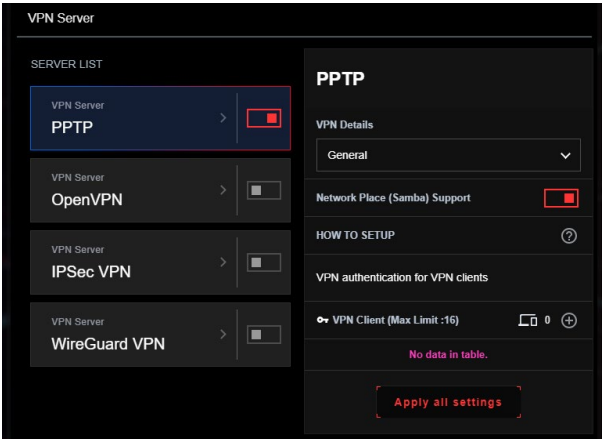
Un VPN (Virtual Private Network) offre un moyen de communication sécurisé sur un ordinateur ou réseau distant par le biais d'un réseau public tel qu'Internet.

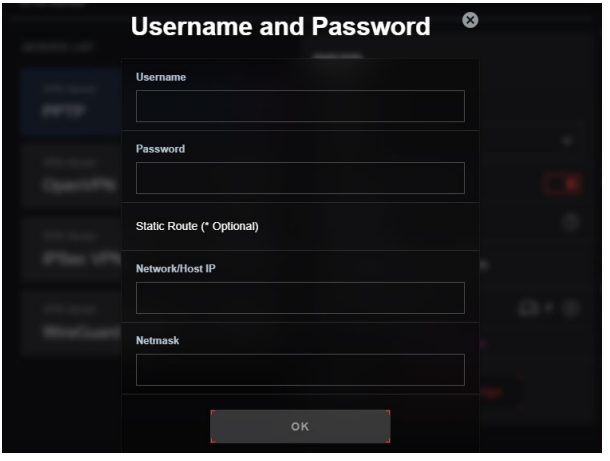
REMARQUE : Avant de configurer une connexion VPN, l'adresse IP ou le nom de domaine d'un serveur VPN sont nécessaires.



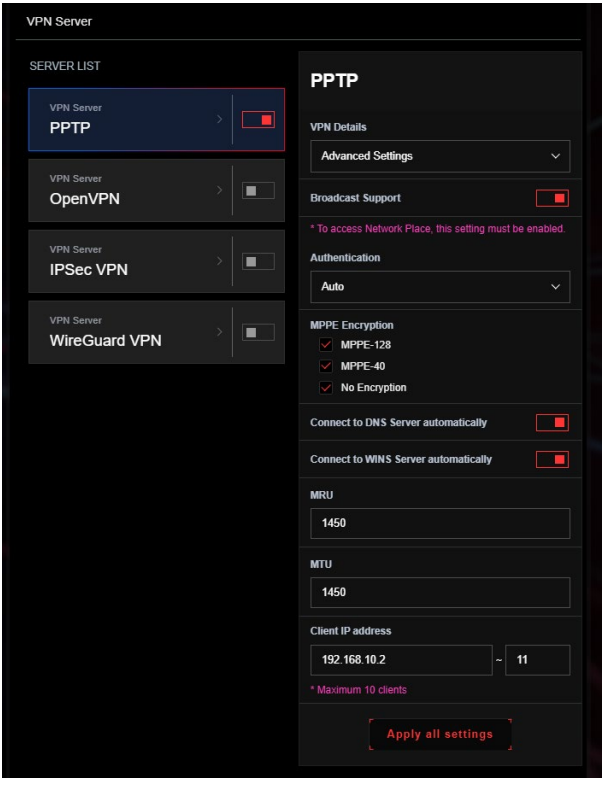
Pour configurer l'accès à un serveur VPN :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **VPN**.
2. Dans le champ **Enable PPTP VPN Server** (Activer le serveur VPN PPTP), sélectionnez **ON** (OUI).
3. Dans la liste déroulante **VPN Details** (Détails VPN), sélectionnez **General** (Général) et activez la prise en charge de **Network Place (Samba)** (Service de partage Samba).
4. Cliquez sur ⊕ pour ajouter un client VPN, puis saisissez le nom d'utilisateur et le mot de passe pour l'accès au VPN.


VPN Server
SERVER LIST
VPN Server
PPTP
VPN Server
OpenVPN
VPN Server
IPSec VPN
VPN Server
WireGuard VPN
PPTP
VPN Details
General
Network Place (Samba) Support
HOW TO SETUP
VPN authentication for VPN clients
VPN Client (Max Limit :16)
0
No data in table.
Apply all settings

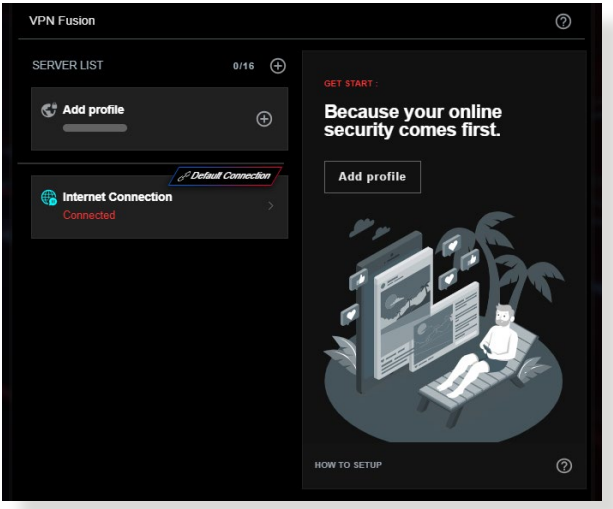

Username and Password
Username
Password
Static Route (* Optional)
Network/Host IP
Netmask
OK

5. Dans la liste déroulante **VPN Details** (Détails VPN), sélectionnez **Advanced Settings** (Paramètres avancés) pour configurer d'autres paramètres avancés comme la diffusion de contenu, l'authentification, le chiffrement MPPE et la plage d'adresses IP.
6. Cliquez sur **Apply all settings** (Appliquer tous les paramètres).



3.20.1 VPN Fusion

VPN Fusion permet de se connecter à plusieurs serveurs VPN simultanément et d'assigner vos périphériques clients à différents tunnels VPN. Certains appareils tels les décodeurs numériques, les Smart TV et les lecteurs Blu-ray ne prennent pas en charge les logiciels VPN. Cette fonction fournit un accès VPN aux appareils du réseau domestique sans passer par un logiciel VPN, alors que votre smartphone reste quant à lui connecté à Internet sans VPN. Pour les joueurs, la connexion VPN neutralise les attaques de déni de service distribué (DDoS) pour empêcher votre jeu PC ou votre streaming de se déconnecter des serveurs de jeu. La mise en place d'une connexion VPN vous permet également de choisir une adresse IP située dans une région géographique proche du serveur de jeu, améliorant ainsi le temps de ping vers les serveurs.



Pour commencer, suivez les instructions ci-dessous :

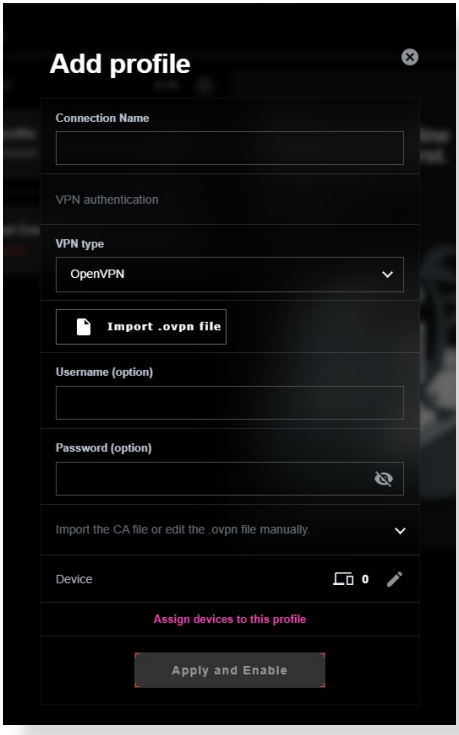
1. À partir du volet de navigation, accédez à **General** (Général) > **VPN** > **VPN Fusion** et cliquez sur ⊕ pour créer un nouveau profil.
2. Sélectionnez **PPTP** dans la liste déroulante **VPN type** (Type de VPN) pour créer un profil client VPN.

IMPORTANT ! Le serveur VPN et le client VPN doivent être du même type.

3. Saisissez les informations du serveur VPN dans le client VPN.
   (1) **Nom de la connexion**: Créez un nom personnalisé pour représenter ce profil.
   (2) **Serveur VPN**: Saisissez l'adresse IP ou le nom DDNS de votre serveur VPN.
   (3) **Nom d'utilisateur**: Saisissez les informations fournies par le serveur VPN.
   Mot de passe: Saisissez les informations fournies par le serveur VPN.
   (4) Cliquez sur **Apply and Enable** (Appliquer et activer) pour compléter le profil du client VPN et vous connecter au serveur VPN.

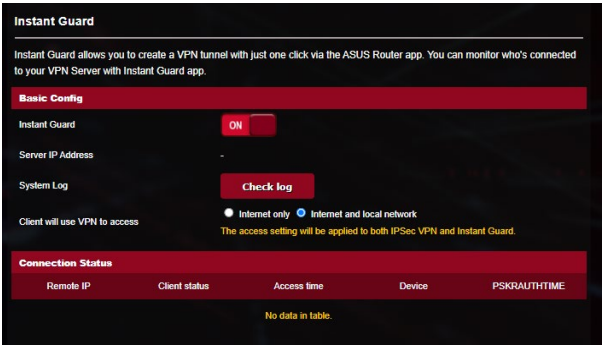
REMARQUE : Contactez l'administrateur du serveur VPN pour obtenir des informations sur le serveur.

4. Lorsque **Connected** (Connecté) apparaît, la connexion VPN PPTP est correctement configurée.



3.20.2 Instant Guard

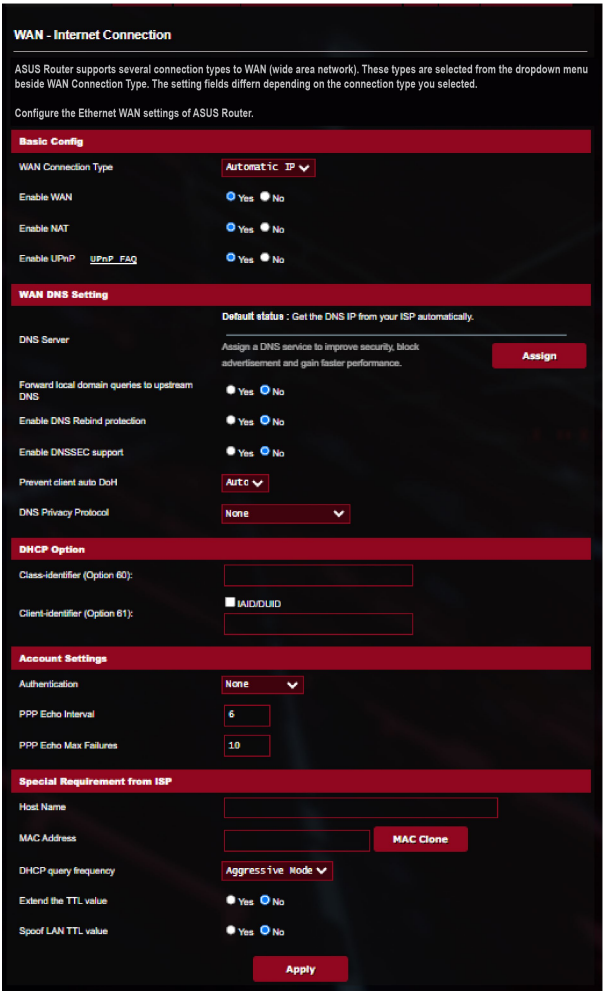
Instant Guard exécute votre propre serveur VPN sur votre routeur. Lorsque vous utilisez un tunnel VPN, toutes vos données transitent par le serveur. Avec Instant Guard, vous avez le contrôle total de votre propre serveur, ce qui en fait la solution la plus sûre.



3.21 Réseau étendu (WAN)

3.21.1 Connexion internet

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



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 **static IP** (Adresse IP statique). 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.

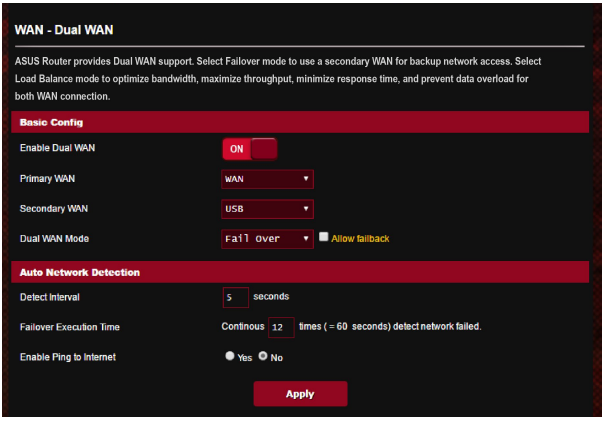
Une fois connectés au réseau, les périphériques peuvent être contrôlés à distance pour la prise en charge d'applications P2P, les jeux vidéo, les visioconférences et les serveurs Web ou proxy. Contrairement à la redirection de port, qui implique la configuration manuelle des ports, le protocole UPnP 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.

- **Connect to DNS Server automatically (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.
- **Authentification**: 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.
- **DHCP query frequency (Fréquence d'interrogation DHCP)**: Modifie l'intervalle de découverte DHCP pour éviter de surcharger le serveur DHCP.

3.21.2 Dual WAN (Double WAN)

Votre routeur ASUS prend en charge la fonctionnalité double WAN. Vous pouvez configurer cette fonctionnalité dans l'un des modes suivants :

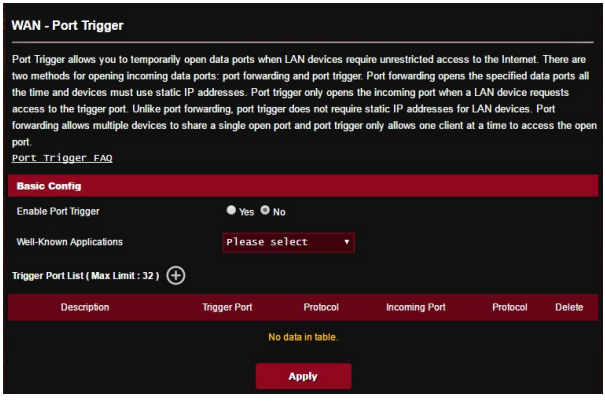
- **Failover Mode (Mode basculement)**: Sélectionnez ce mode pour utiliser le réseau étendu (WAN) secondaire comme connexion réseau de secours.
- **Mode d'équilibrage de charge**: Sélectionnez ce mode pour optimiser la bande passante, les délais de réponse et éviter les surcharges de données des deux WAN.



3.21.3 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.



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. Dans le champ **Enable Port Trigger** (Activer le déclenchement de port), cochez **Yes** (Oui) pour activer le déclenchement de port.
3. Dans le champ **Well-Known Applications** (Applications connues), sélectionnez un jeu ou un service internet à ajouter à la liste de déclenchement de port.
4. Dans le tableau **Trigger Port List** (Liste des ports de déclenchement), spécifiez les informations suivantes :
   - **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.

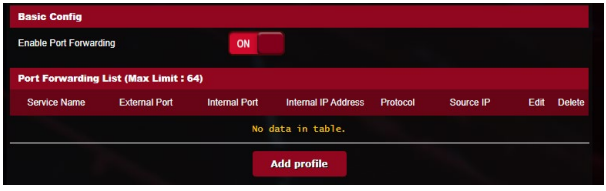
5. Cliquez sur ⊕ pour ajouter les informations à la liste. Cliquez sur ⊖ pour supprimer une entrée de la liste.
6. Une fois terminé, cliquez sur **Apply** (Appliquer).

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.

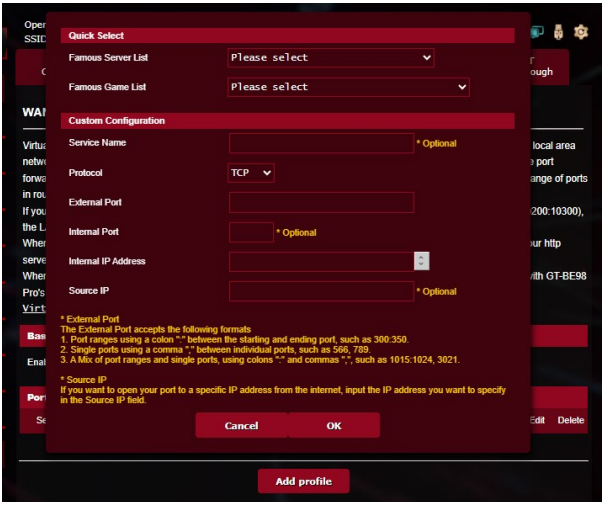
3.21.4 Serveur virtuel et redirection de port

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.



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. Dans le champ **Enable Port Forwarding** (Activer la redirection de port), sélectionnez **ON** (Oui).
3. Cliquez sur **Add profile** (Ajouter un profil).



4. Dans le champ **Famous Server List** (Liste de serveurs), spécifiez le type de service auquel vous souhaitez accéder.
5. Dans le champ **Famous Game List** (Liste de jeux), sélectionnez l'une des options disponibles. Ce menu déroulant liste une liste de jeux et de services de jeu en ligne.
6. Dans le tableau **Port Forwarding List** (Liste des ports à rediriger), spécifiez les informations suivantes :
   - **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 **3.12 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).

7. Cliquez sur ⊕ pour ajouter les informations à la liste. Cliquez sur ⊖ pour supprimer une entrée de la liste.
8. Une fois terminé, cliquez sur **Apply** (Appliquer).

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.

3.21.5 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 risque 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).

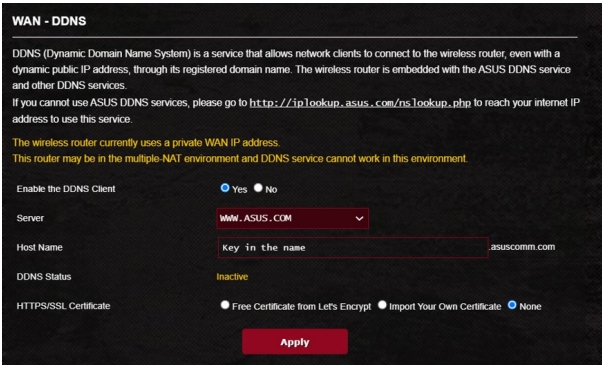
- **IP address of Exposed Station (Adresse IP du client) :** Entrez dans ce champ l'adresse IP du client hébergeant le service DMZ et exposé à Internet. Vérifiez que le client serveur possède une adresse IP statique.

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).

3.21.6 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.



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 :

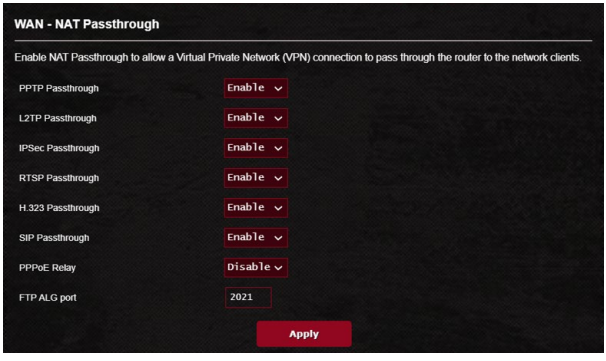
Le service DDNS ne peut pas fonctionner sous les conditions suivantes :

- 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.

3.21.7 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.

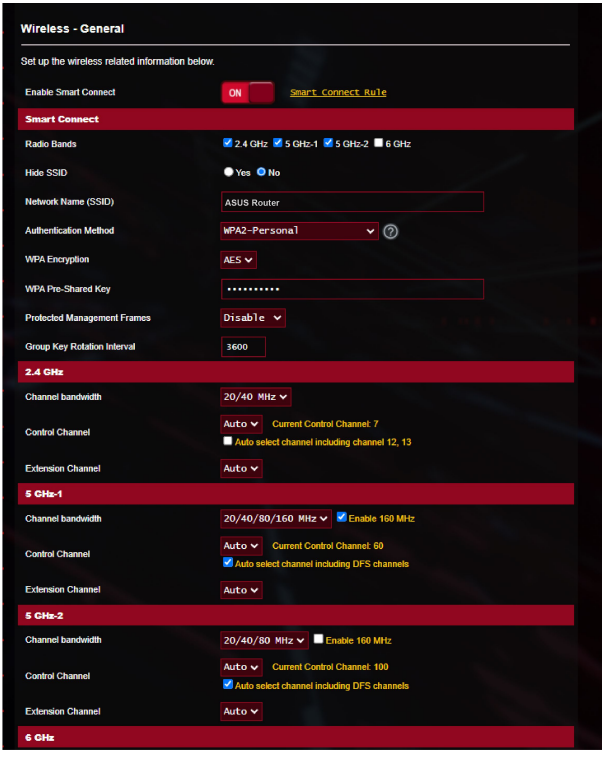
Pour activer ou désactiver la fonction NAT Passthrough, allez dans **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > **NAT Passthrough**. Une fois terminé, cliquez sur **Apply** (Appliquer).



3.22 WiFi

3.22.1 Général

L'onglet General (Général) vous permet de configurer les paramètres WiFi de base.



Pour configurer les paramètres WiFi de base :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **General** (Général).
2. Sélectionnez la bande de fréquence 2,4 GHz, 5 GHz-1, 5 GHz-2 ou 6 GHz pour votre réseau WiFi.
3. Déplacez l'interrupteur de l'élément **Enable Smart Connect** (Activer Smart Connect) sur **ON** (Activé) pour activer la fonction Smart Connect. Cette fonction permet de connecter automatiquement les clients WiFi à la bande de fréquence 2,4 GHz, 5 GHz-1, 5 GHz-2 ou 6 GHz appropriée pour une vitesse optimale.

4. Attribuez un nom unique composé d'un maximum de 32 caractères faisant office de SSID (Service Set Identifier) et permettant d'identifier votre réseau WiFi. Les appareils disposant de capacités WiFi peuvent identifier et se connecter à votre réseau WiFi par le biais du SSID. Les SSID de la barre d'informations sont mis à jour une fois les nouveaux SSID sauvegardés dans les paramètres.

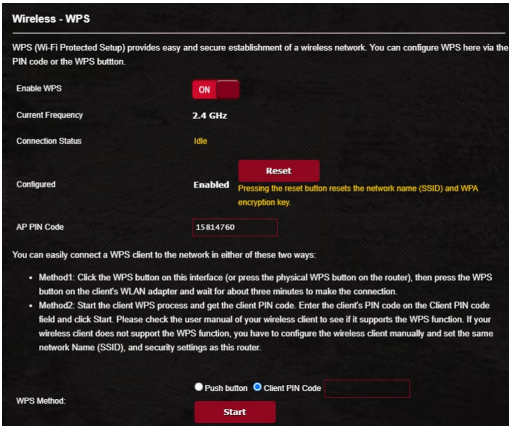
   REMARQUE : Vous pouvez affecter différents SSID pour les bandes de fréquence 2,4 GHz, 5 GHz-1, 5 GHz-2 et 6 GHz.

5. Dans le champ **Hide SSID** (Masquer le SSID), sélectionnez **Yes** (Oui) si vous ne souhaitez pas que les périphériques WiFi puissent détecter votre SSID. Lorsque cette option est activée, vous devez saisir manuellement le SSID sur l'appareil souhaitant se connecter à votre réseau WiFi.
6. Sélectionnez ensuite l'un des modes WiFi disponibles pour déterminer quels types d'appareils WiFi peuvent se connecter à votre routeur :
   - **Auto**: Les appareils utilisant les normes 802.11ac, 802.11n, 802.11g et 802.11b peuvent se connecter au routeur WiFi.
   - **N only (N uniquement)**: Permet de maximiser les performances de la norme 802.11n. Toutefois, le matériel prenant en charge les normes 802.11g et 802.11b ne pourra pas établir de connexion au routeur WiFi.
   - **Legacy (Hérité)**: Les appareils utilisant les normes 802.11b/g/n peuvent se connecter au routeur WiFi. Toutefois le matériel prenant en charge la norme 802.11n de manière native, ne fonctionnera qu'à une vitesse maximum de 54 Mb/s.
7. Sélectionnez le canal d'opération du routeur. Choisissez **Auto** pour autoriser le routeur à sélectionner automatiquement le canal générant le moins d'interférences.
8. Sélectionnez l'un des canaux de bande passante disponibles.
9. Choisissez l'une des méthodes d'authentification disponibles.
10. Une fois terminé, cliquez sur **Apply** (Appliquer).

3.22.2 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.



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 et WPA/WPA2/WPA3-Personal. Les chiffrements à clés partagées, WPA/WPA2/WPA3-Enterprise et RADIUS ne sont pas pris en charge.

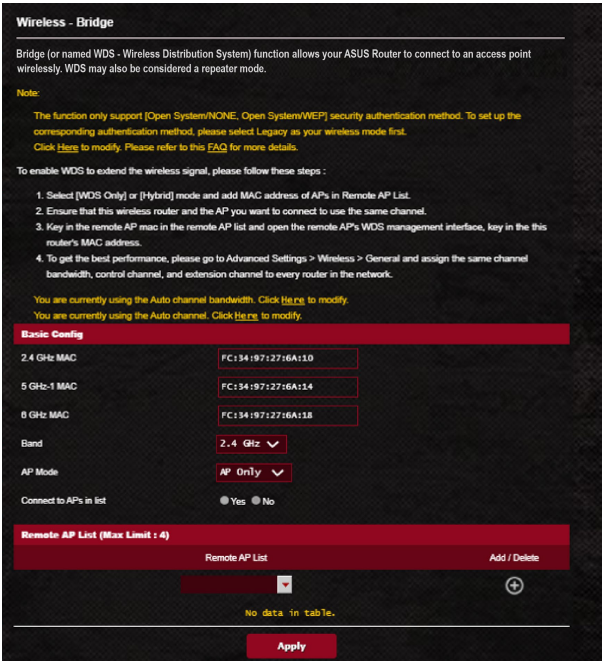
4. Dans le champ WPS Method (Méthode de connexion WPS), sélectionnez **Push Button** (Pression de bouton) ou **Client PIN code** (Code PIN). Si vous souhaitez utiliser le bouton WPS, continuez à l'étape 5. Si vous optez plutôt pour le code PIN, passez directement à l'étape 6.
5. Pour utiliser le bouton 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.
6. 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.

3.22.3 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.



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. Par défaut, le canal d'opération / de contrôle du pont WiFi est réglé sur **Auto** pour autoriser le routeur à choisir automatiquement le canal générant le moins d'interférences.

   Vous pouvez modifier le **Control Channel** (Canal de contrôle) dans **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **General** (Général).

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

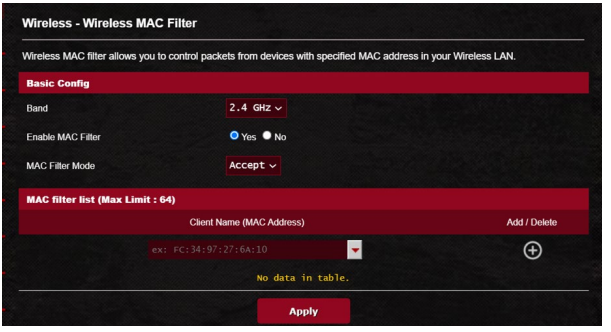
6. Dans **Remote AP List** (Liste des points d'accès distants), entrez une adresse MAC, puis cliquez sur le bouton **Ajouter** pour ajouter l'adresse à la liste des points d'accès disponibles.

   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).

3.22.4 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.

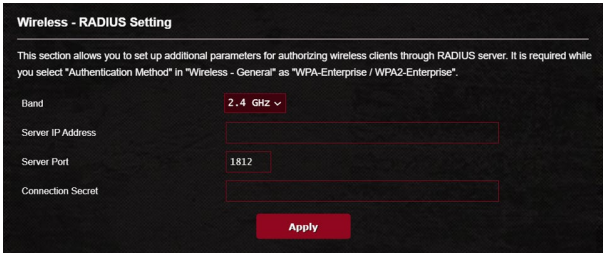


Pour configurer le filtrage d'adresses MAC :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (WiFi) > **Wireless MAC Filter** (Filtrage d'adresses MAC).
2. Sélectionnez une bande de fréquence.
3. Cochez **Yes** (Oui) dans le champ **Enable Mac Filter** (Activer le filtrage d'adresses MAC).
4. Dans le menu déroulant **MAC Filter Mode** (Mode de 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.
5. Entrez une adresse MAC, puis cliquez sur le bouton **Add** (Ajouter) ⊕ pour l'ajouter à la liste.
6. Cliquez sur **Apply** (Appliquer).

3.22.5 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/WPA2/WPA3-Enterprise ou Radius avec 802.1be.



Pour configurer le service RADIUS :

1. Assurez-vous que le mode d'authentification du routeur est bien de type WPA/WPA2/WPA3-Enterprise.

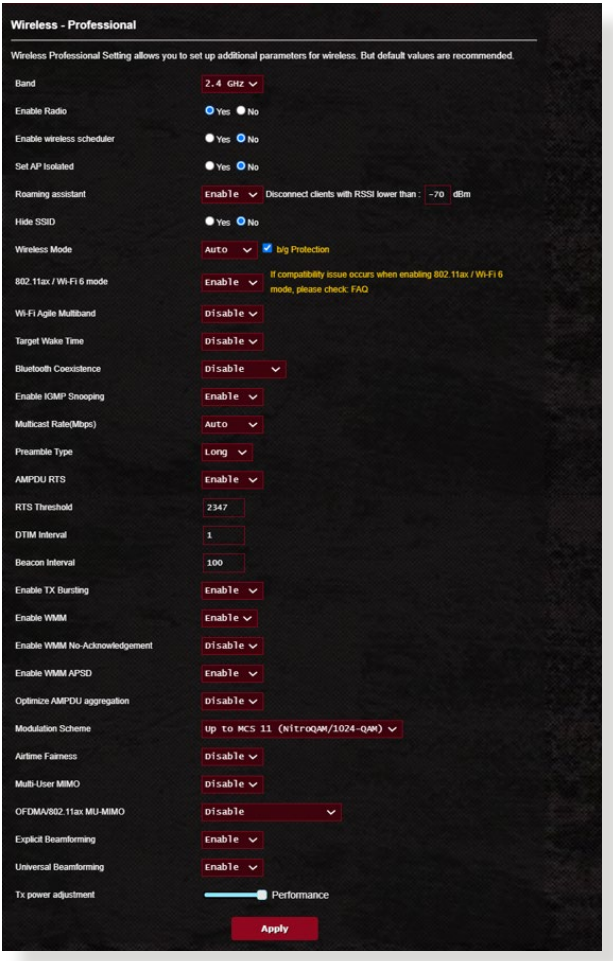
   REMARQUE : Consultez la section **3.22.1 Général** pour en savoir plus sur les différents modes d'authentification de votre routeur WiFi.

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 **Server Port** (Port du serveur), entrez l'adresse du port du serveur RADIUS.
6. Dans le champ **Connection Secret** (Phrase secrète), affectez le mot de passe d'accès au serveur RADIUS.
7. Cliquez sur **Apply** (Appliquer).

3.22.6 Professionnel

L'onglet Professionnel offre diverses options de configuration avancées.

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



Sur l'écran **Professional Settings** (Paramètres professionnels), 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) :** Sélectionnez **Yes** (Oui) pour activer et configurer le planificateur WiFi. Cochez **No** (Non) pour désactiver le planificateur WiFi.
  - **Date to Enable Radio (weekdays) (Jours d'activation de la radio (semaine))**: Permet de spécifier les jours de semaine pour lesquels vous souhaitez activer le module radio WiFi.
  - **Time of Day to Enable Radio (Horaires d'activation de la radio)**: Permet de spécifier une plage horaire (en semaine) spécifique pour laquelle vous souhaitez activer le module radio WiFi.
  - **Date to Enable Radio (weekend) (Jours d'activation de la radio (week-end))**: Permet de spécifier les jours pour lesquels vous souhaitez activer le module radio WiFi le week-end.
  - **Time of Day to Enable Radio (Horaires d'activation de la radio)**: Permet de spécifier une plage horaire (le week-end) spécifique pour laquelle vous souhaitez activer le module radio WiFi.
- **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.
- **Roaming Assistant (Assistant itinérance)**: Dans les configurations réseau impliquant plusieurs points d'accès, ou un répéteur, les clients WiFi se retrouvent parfois dans l'incapacité de se connecter automatiquement aux points d'accès disponibles car ils sont toujours connectés au routeur principal. En activant ce paramètre, le client se déconnectera du routeur principal si la force du signal est inférieure à un certain seuil pour se connecter à un signal plus puissant.
- **Enable IGMP Snooping (Activer le filtrage IGMP)**: Activer cette fonction permet de surveiller et d'optimiser le trafic IGMP (Internet Group Management Protocol) entre plusieurs périphériques.

- **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.
- **AMPDU RTS :** Activer cette fonction permet de créer un groupe de trames avant leur transmission ainsi que d'activer le RTS pour chaque AMPDU lors des communications entre les appareils 802.11g et 802.11b.
- **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.

- **Reducing USB 3.0 interference (Réduire les interférences USB 3.0)** : Activer cette fonction assure les meilleures performances WiFi sur la bande 2,4 GHz. Désactiver cette fonction augmente la vitesse de transfert des ports USB 3.0 et peut affecter la portée de la bande WiFi 2,4 GHz.
- **Optimize AMPDU aggregation (Optimiser l'agrégation AMPDU)**: Optimise le nombre maximal de MPDU dans un AMPDU et évite de perdre ou de corrompre les paquets pendant la transmission dans des canaux WiFi sujets à des erreurs
- **Turbo QAM**: Activer cette fonction permet de prendre en charge 256-QAM (MCS 8/9) sur la bande 2,4 GHz pour obtenir une meilleure portée et capacité de traitement sur cette fréquence.
- **Airtime Fairness**: Avec Airtime Fairness, la vitesse du réseau n'est pas déterminée par le trafic le plus lent. En allouant le même temps à tous les clients, Airtime Fairness permet d'effectuer chaque transfert à une vitesse optimale.
- **Explicit Beamforming (Beamforming explicite)** : L'adaptateur et le routeur WLAN du client prennent en charge la technologie de Beamforming. Cette technologie permet à ces périphériques de s'échanger des informations telles que l'estimation du canal et le sens de transmission pour améliorer le débit montant et descendant.
- **Universal Beamforming (Beamforming universel)**: Pour les anciens adaptateurs réseau sans fil qui ne prennent pas en charge le Beamforming, le routeur estime le canal et détermine le sens de la transmission pour améliorer le débit descendant.

4 Utilitaires

REMARQUES :

- Téléchargez et installez les utilitaires WiFi du routeur à partir du site ASUS :
- Device Discovery (v1.4.7.1) : http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
- Firmware Restoration (v1.9.0.4) : http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
- Utilitaire d'impression pour Windows (v1.0.5.5) : http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip
- Les utilitaires ne sont pas compatibles avec le système d'exploitation MAC OS.

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.

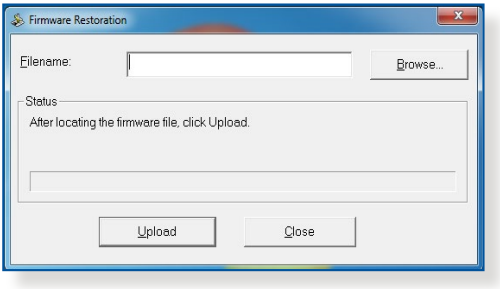
Pour lancer l'utilitaire Détection d'appareils :

- 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 échouée, 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: 192.168.50.1

   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 GT-BE98 Wireless Router** (Utilitaire ASUS Routeur WiFi GT-BE98) > **Firmware Restoration** (Restauration du firmware).

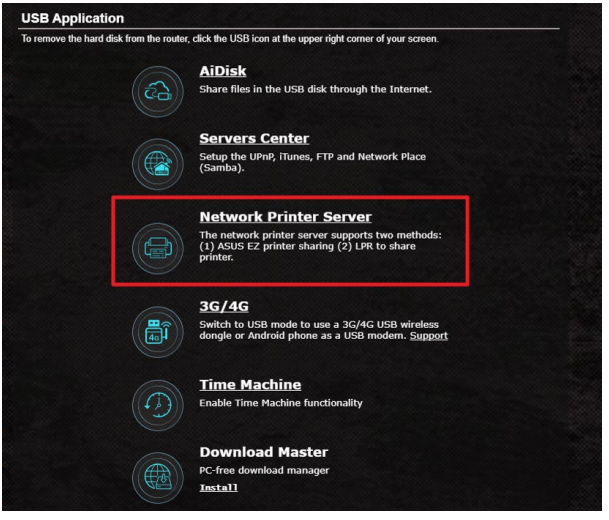
5. Spécifiez un fichier de firmware, puis cliquez sur **Upload** (Charger).

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.

4.3 Configurer un serveur d'impression

4.3.1 Utilitaire ASUS EZ Printer Sharing

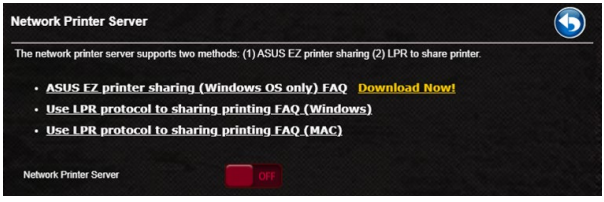
L'utilitaire ASUS EZ Printing Sharing vous permet de connecter une imprimante réseau au port USB du routeur et de configurer un serveur d'impression. Ceci permet aux clients du réseau d'imprimer et de scanner des fichiers en passant par le WiFi.



REMARQUE : Les serveurs d'impression ne sont pris en charge que sur Windows® 10/11.

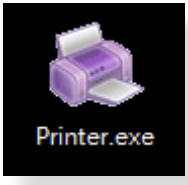
Pour partager une imprimante avec EZ Printer :

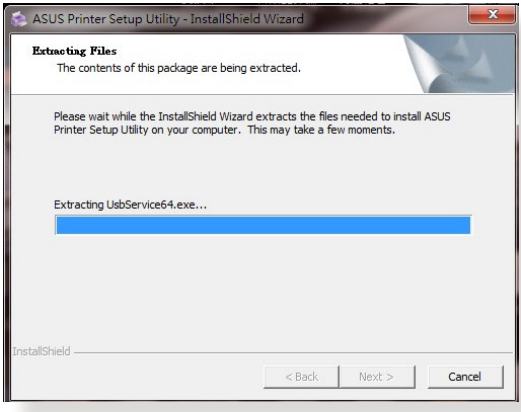
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Network Printer Server** (Serveur d'impression réseau).
2. Cliquez sur **Download Now!** (Télécharger maintenant!) pour télécharger l'utilitaire pour imprimante réseau



REMARQUE : L'utilitaire d'imprimante réseau est pris en charge sur Windows® 10/11. Pour installer l'utilitaire sur Mac OS, sélectionnez **Use LPR protocol for sharing printer** (Utiliser le protocole LPR pour partager une imprimante).

3. Décompressez le fichier téléchargé et cliquez sur l'icône représentant une imprimante pour exécuter le programme de configuration d'imprimante réseau.



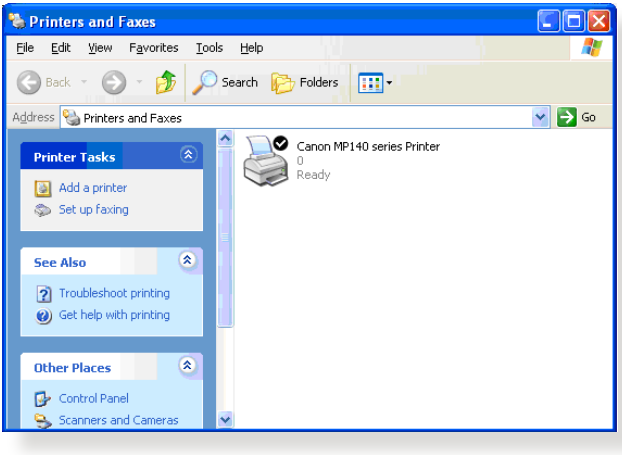


4. Suivez les instructions apparaissant à l'écran pour configurer le matériel, puis cliquez sur **Next** (Suivant).

5. Patientez quelques minutes le temps que la configuration initiale se termine. Cliquez sur **Next** (Suivant).
6. Cliquez sur **Finish** (Terminé) pour conclure l'installation.

7. Suivez les instructions du système d'exploitation Windows® pour installer le pilote de l'imprimante.

8. Une fois le pilote installé, les clients du réseau pourront utiliser l'imprimante.



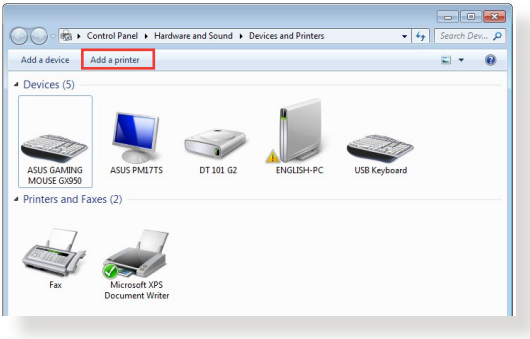
4.3.2 Utiliser le protocole LPR pour partager une imprimante

Vous pouvez utiliser les protocoles LPR/LPD (Line Printer Remote/ Line Printer Daemon) pour partager votre imprimante sous Windows® et MAC OS.

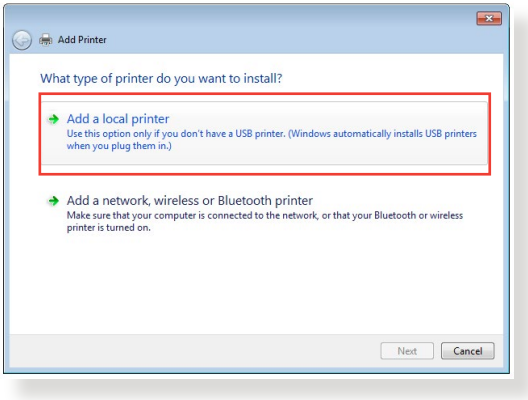
Partage d'imprimante LPR :

Pour partager une imprimante via le protocole LPR :

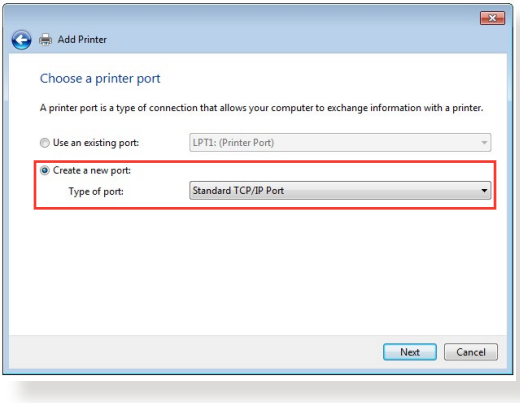
1. À partir du Bureau de Windows®, cliquez sur **Start** (Démarrer) > **Devices and Printers** (Périphériques et imprimantes) > **Add Printer Wizard** (Ajouter une imprimante).



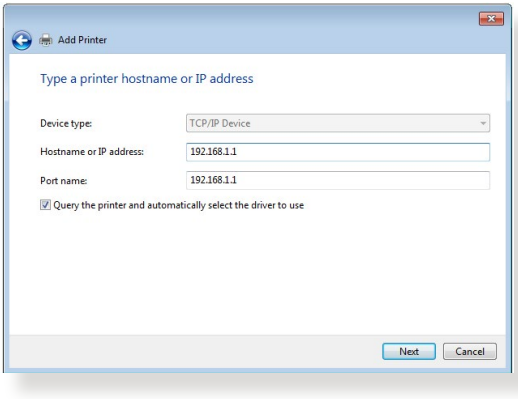
2. Sélectionnez **Add a local printer** (Ajouter une imprimante locale) et cliquez sur **Next** (Suivant).



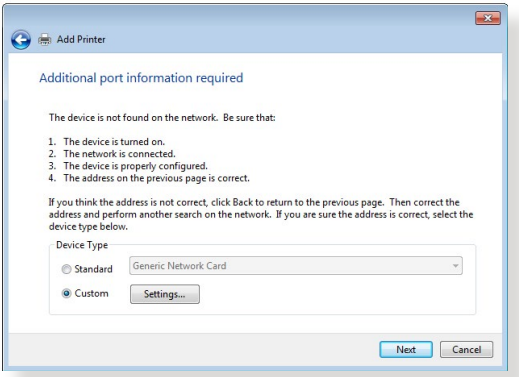
3. Sélectionnez **Create a new port** (Créer un nouveau port) puis sélectionnez l'option **Standard TCP/IP Port** (Port TCP/IP standard) du menu déroulant **Type of Port** (Type de port). Cliquez sur **Next** (Suivant).



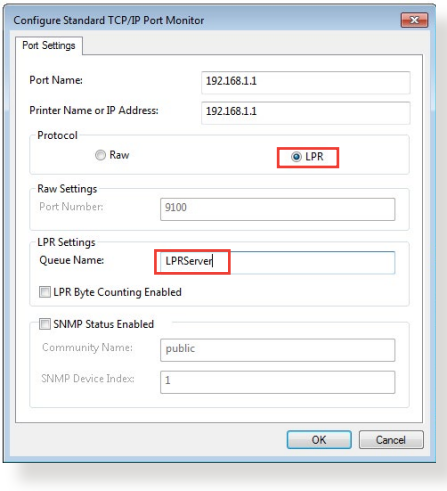
4. Dans le champ **Hostname or IP address** (Nom d'hôte ou adresse IP), entrez l'adresse IP du routeur WiFi et cliquez sur **Next** (Suivant).



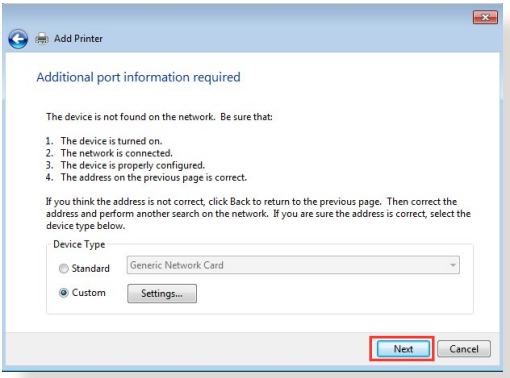
5. Sélectionnez **Custom** (Personnalisé) puis cliquez sur **Settings** (Paramètres).



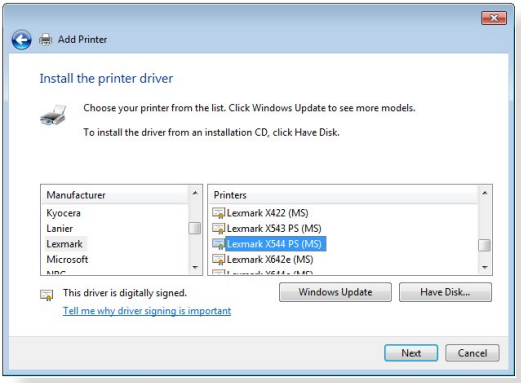
6. Réglez le **Protocol** (Protocole) sur **LPR**. Dans le champ **Queue Name** (Nom de la file d'attente), entrez **LPRServer** puis cliquez sur **OK** pour continuer.



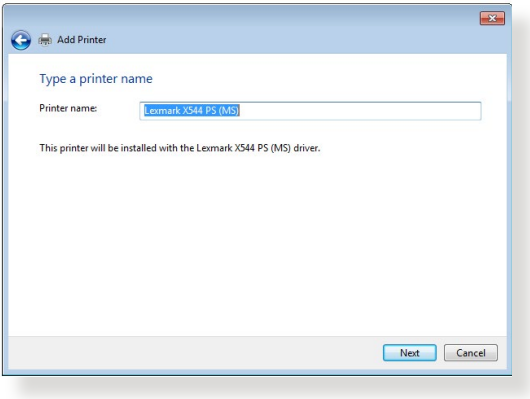
7. Cliquez sur **Next** (Suivant) pour terminer la configuration TCP/IP.



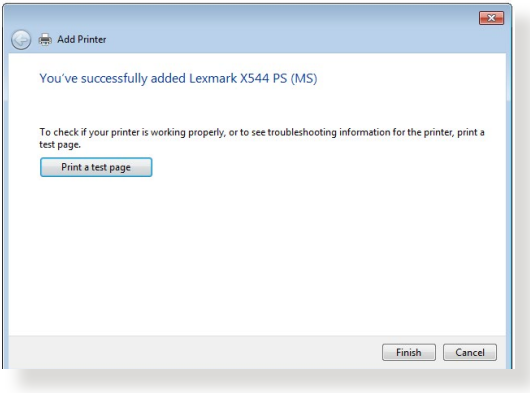
8. Installez le pilote d'impression à partir de la liste. Si votre imprimante ne figure pas dans la liste, cliquez sur **Have Disk** (Disque fourni) pour installer le pilote à partir d'un disque optique ou d'un fichier.



9. Cliquez sur **Next** (Suivant) pour accepter le nom par défaut de l'imprimante.



10. Cliquez sur **Finish** (Terminé) pour conclure l'installation.



4.4 Download Master

Download Master est un utilitaire vous permettant de télécharger des fichiers même lorsque votre ordinateur est éteint.

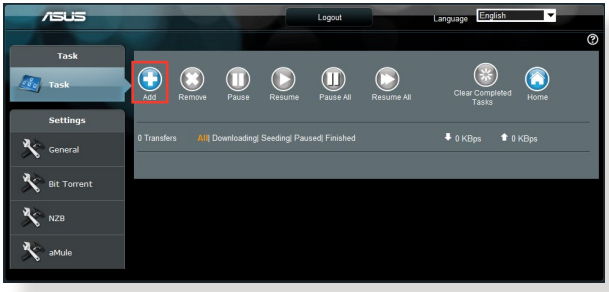
REMARQUE : Un périphérique de stockage USB doit être connecté au routeur WiFi pour pouvoir utiliser Download Master.

Pour utiliser Download Master :

1. Cliquez sur **Advanced Settings** (Paramètres avancés) > **USB Application** (Applications USB) > **Download Master** pour télécharger et installer l'utilitaire.

   REMARQUE : Si plus d'un périphérique de stockage USB est relié au routeur WiFi, sélectionnez celui sur lequel vous souhaitez télécharger vos fichiers.

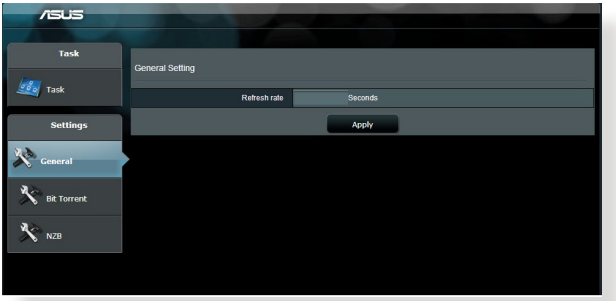
2. Une fois le téléchargement terminé, cliquez sur l'icône Download Master pour commencer à l'utiliser.
3. Cliquez sur **Add** (Ajouter) pour ajouter une tâche à télécharger.



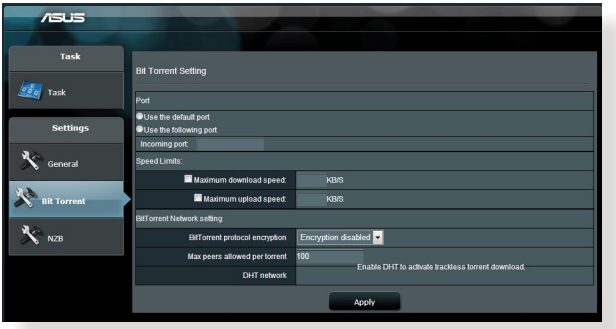
4. Sélectionnez un type de téléchargement, soit BitTorrent, HTTP, ou FTP. Spécifiez un fichier torrent ou une URL pour lancer le téléchargement.

   REMARQUE : Pour plus de détails sur le protocole BitTorrent, consultez la section **4.4.1 Configurer les paramètres BitTorrent**.

5. Utilisez le panneau de navigation pour configurer les paramètres avancés.



4.4.1 Configurer les paramètres BitTorrent

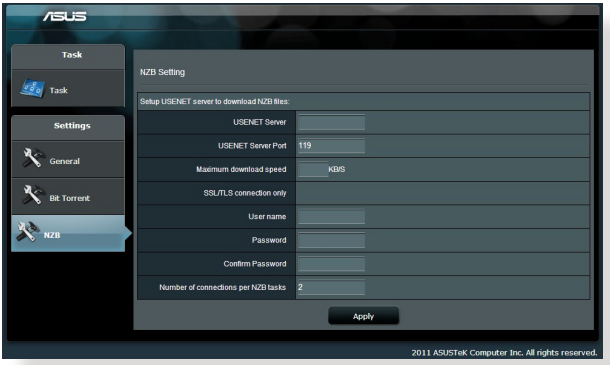


Pour configurer les paramètres de téléchargement BitTorrent :

1. Dans le panneau de navigation de Download Master, cliquez sur **BitTorrent**.
2. Sélectionnez un port de téléchargement spécifique.
3. Pour éviter les congestions réseau, vous pouvez limiter les vitesses de téléchargement en amont ou en aval sous l'élément **Speed Limits** (Limites de vitesse).
4. Vous pouvez aussi limiter le nombre maximum de clients autorisés et activer ou désactiver le chiffrement lors des téléchargements.

4.4.2 Paramètres NZB

Vous pouvez utiliser un serveur USENET pour télécharger des fichiers NZB. Après avoir configuré les paramètres USENET, cliquez sur **Apply** (Appliquer).



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/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://rog.asus.com/networking/rog-rapture-gt-be98-model/helpdesk_bios/ pour télécharger le dernier firmware disponible.
3. Dans l'onglet **Firmware Upgrade** (Mise à jour du firmware), cliquez sur **Browse** (Parcourir) 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 câbles réseau Ethernet sont correctement branchés.

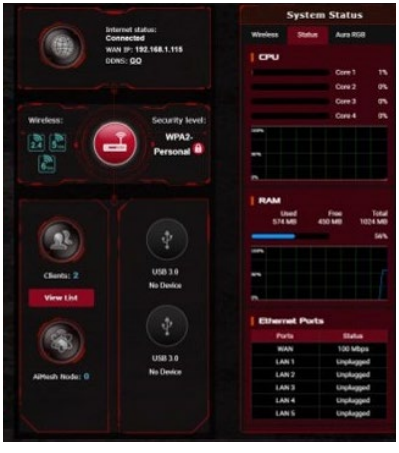
- Lorsque le câble Ethernet connectant le routeur au modem est correctement branché, le témoin lumineux du routeur dédié au réseau internet (WAN) s'allume.
- Lorsque le câble Ethernet connectant un ordinateur sous tension au routeur est correctement branché, le témoin lumineux du routeur dédié au réseau local (LAN) s'allume.

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.

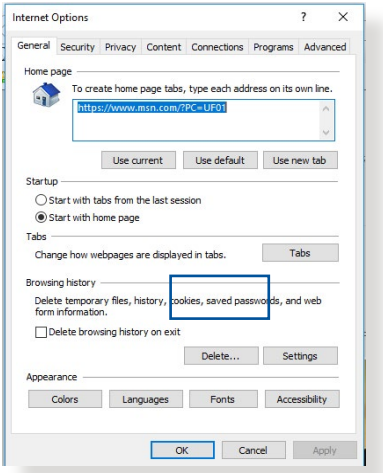


5.2 Foire aux questions (FAQ)

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. Le nom d'utilisateur/mot de passe par défaut est “admin”. 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).



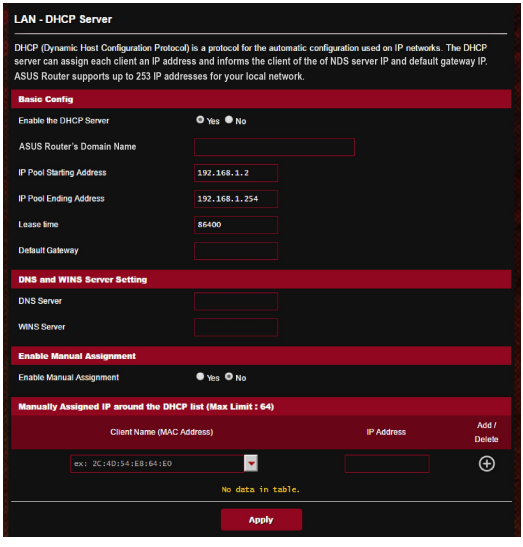
REMARQUES :

- 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.

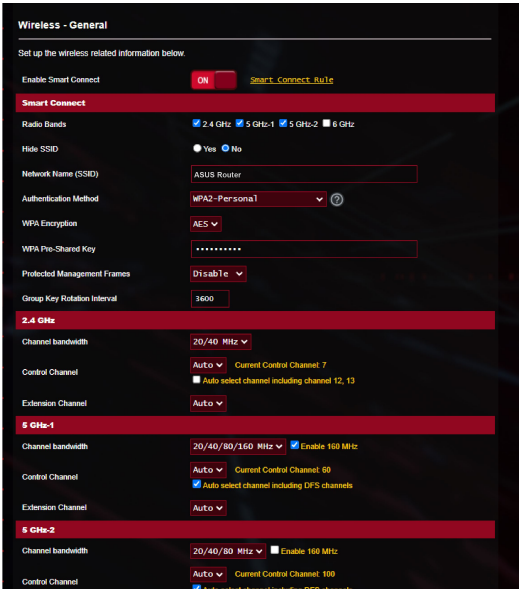
Le client ne peut pas établir de connexion WiFi avec le routeur

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

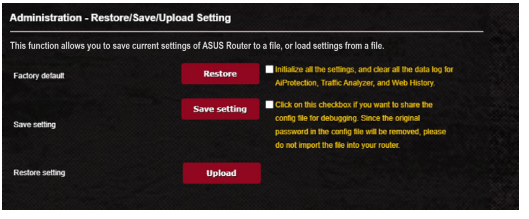
- **Hors de portée :**
  - Rapprochez le routeur du client.
  - Si disponibles, essayez d'ajuster l'angle des antennes du routeur. Pour plus de détails, consultez la section **1.4 Placer votre routeur**.
- **Serveur DHCP désactivé :**
  1. Ouvrez l'interface de gestion du routeur. Dans l'interface de gestion du routeur, cliquez sur **Advanced Settings** (Paramètres avancés) > **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.



- Le SSID est masqué. Si votre appareil est en mesure de détecter d'autre 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).



- 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).



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 **Advanced Settings** (Paramètres avancés) > **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.
- Vérifiez les témoins lumineux du modem ADSL et du routeur WiFi. Si le voyant lumineux dédié au réseau étendu (WAN) du routeur est éteint, vérifiez l'état de connexion des câbles.

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). Le nom d'utilisateur / mot de passe par défaut est "admin".

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).

  Les éléments suivants sont les paramètres par défaut du routeur :

Nom d'utilisateur :	admin
Mot de passe :	admin
Serveur DHCP :	Activé (Si le câble WAN est branché)
Adresse IP :	http://www.asusrouter.com (ou 192.168.50.1)
Nom de domaine :	(aucun)
Masque de sous-réseau :	255.255.255.0
Serveur DNS 1 :	192.168.50.1
Serveur DNS 2 :	(aucun)
SSID (2,4 GHz) :	ASUS_XX_2G
SSID (5GHz-1) :	ASUS_XX_5G-1
SSID (5GHz-2) :	ASUS_XX_5G-2
SSID (6 GHz):	ASUS_XX_6G

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.

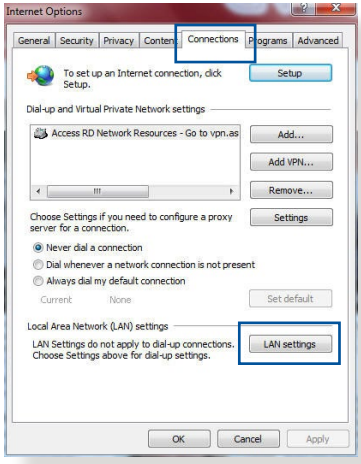
Impossible d'accéder à l'interface de gestion du routeur

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

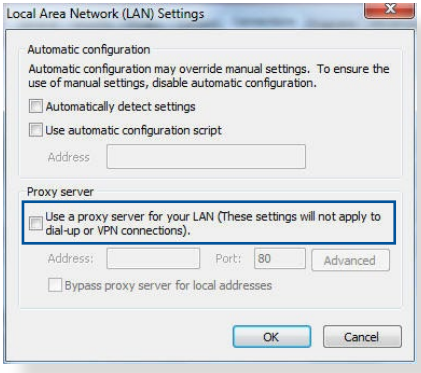
A. Désactivez le serveur proxy si celui-ci est activé.

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).

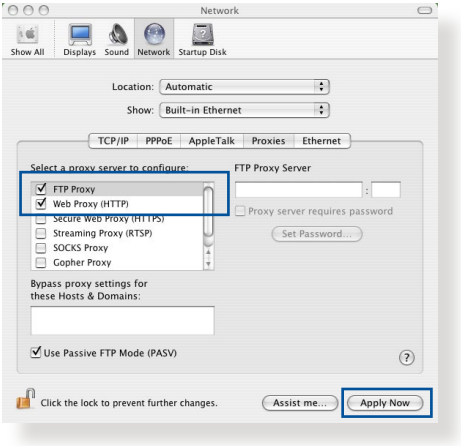


3. À partir de l'écran des paramètres du réseau local, décochez l'option **Use a proxy server for your LAN** (Utiliser un serveur proxy pour votre réseau local).
4. Cliquez sur **OK** une fois terminé.



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)).



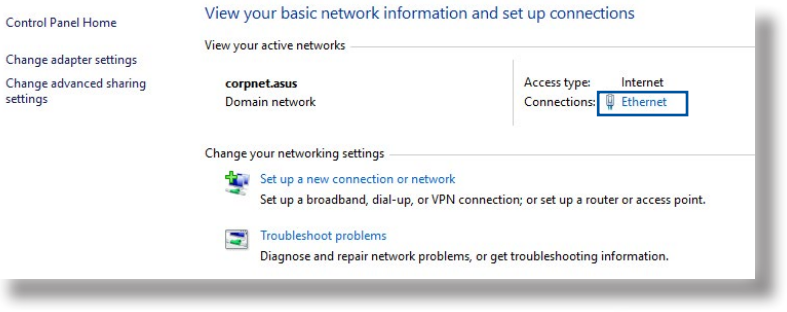
3. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

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

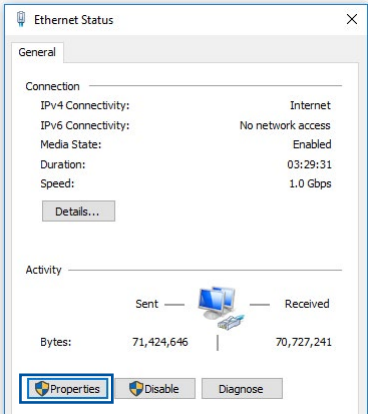
B. Configurez les paramètres TCP/IP pour l'obtention automatique d'une adresse IP.

Windows®

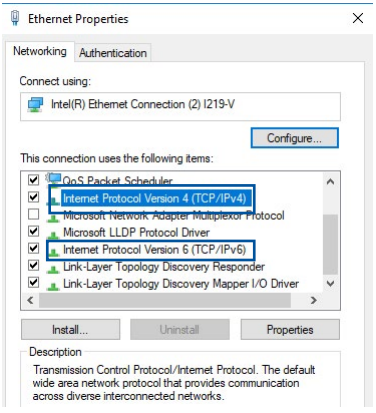
1. Cliquez sur **Start** (Démarrer) > **Control Panel** (Panneau de configuration) > **Network and Sharing Center** (Centre réseau et partage) > **Manage network connections** (Gérer les connexions réseau).



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



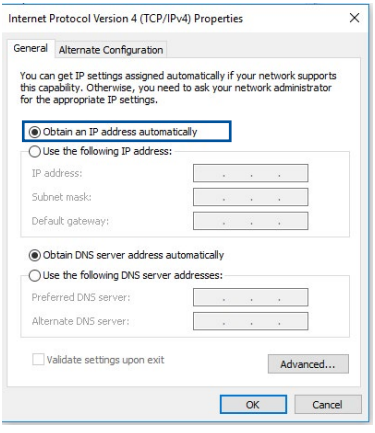
3. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)** (Protocole internet version 4 (TCP/IPv4)) ou **Internet Protocol Version 6 (TCP/IPv6)** (Protocole internet version 6 (TCP/IPv6)), puis cliquez sur **Properties** (Propriétés).



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

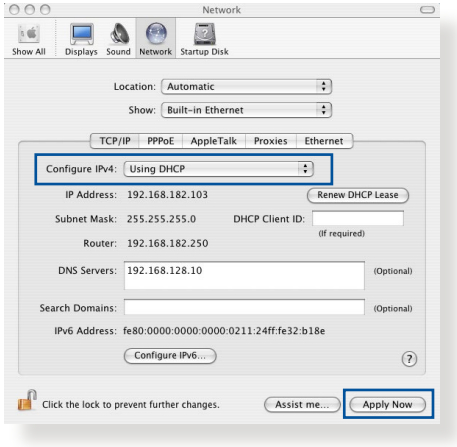
   Pour obtenir une adresse IP IPv6, cochez l'option **Obtain an IPv6 address automatically** (Obtenir une adresse IPv6 automatiquement).

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).



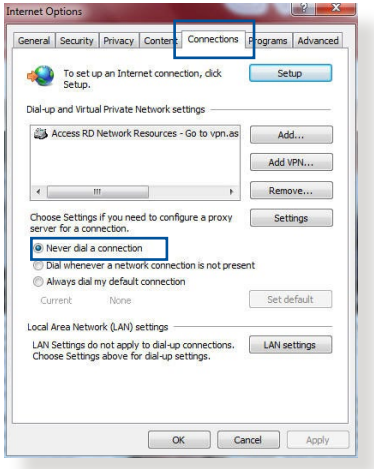
4. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

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 électrique 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/support.