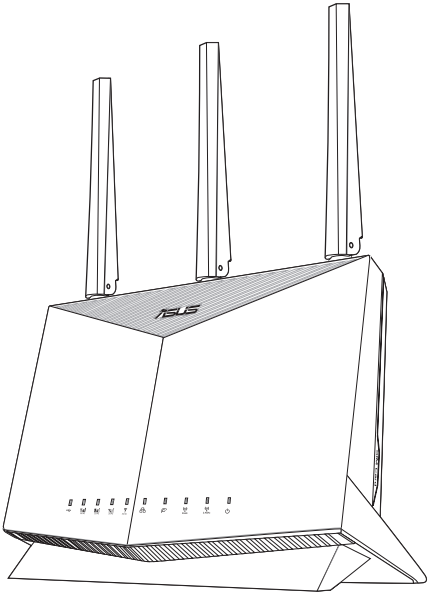
Manuel de l'utilisateur

4G-AC86U

Routeur Wi-Fi LTE Cat.12 AC2600



IN SEARCH OF INCREDIBLE

F18231
Première Édition
Avril 2021

Copyright © 2021 ASUSTeK Computer Inc. Tous droits réservés.

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

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

ASUS FOURNIT CE MANUEL "EN L'ÉTAT" SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS NON LIMITÉ AUX GARANTIES IMPLICITES OU AUX CONDITIONS DE COMMERCIABILITÉ OU D'ADÉQUATION À UN BUT PARTICULIER. En aucun cas ASUS, ses directeurs, ses cadres, ses employés ou ses agents ne peuvent être tenus responsables des dégâts indirects, spéciaux, accidentels ou consécutifs (y compris les dégâts pour manque à gagner, pertes de profits, perte de jouissance ou de données, interruption professionnelle ou assimilé), même si ASUS a été prévenu de la possibilité de tels dégâts découlant de tout défaut ou erreur dans le présent manuel ou produit.

LES SPÉCIFICATIONS ET LES INFORMATIONS CONTENUES DANS CE MANUEL SONT FOURNIES À TITRE INDICATIF SEULEMENT ET SONT SUJETTES À DES MODIFICATIONS SANS PRÉAVIS, ET NE DOIVENT PAS ÊTRE INTERPRÉTÉES COMME UN ENGAGEMENT DE LA PART D'ASUS. ASUS N'EST EN AUCUN CAS RESPONSABLE D'ÉVENTUELLES ERREURS OU INEXACTITUDES PRÉSENTES DANS CE MANUEL, Y COMPRIS LES PRODUITS ET LES LOGICIELS QUI Y SONT DÉCRITS.

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

Table des matières

1 Présentation de votre routeur Wi-Fi

1.1 Bienvenue ! 7
1.2 Contenu de la boîte 7
1.3 Votre routeur Wi-Fi 8
1.4 Placer le routeur 10
1.5 Installer une carte Nano SIM dans votre routeur 11

2 Prise en main

2.1 Configurer le routeur 12
A. Connexion filaire 13
B. Connexion Wi-Fi 14
2.2 Assistant de configuration internet 16

3 Configurer les paramètres généraux

3.1 Utiliser la carte du réseau 21
3.1.1 Configurer les paramètres de sécurité Wi-Fi 22
3.1.2 État du système 23
3.1.3 Gérer les clients du réseau 24
3.1.4 Surveiller l'état de la connexion internet 26
3.1.5 Surveiller un périphérique USB 27
3.2 Réseau invité 28
3.3 AiProtection 30
3.3.1 Protection du réseau 31
3.3.2 Configurer le contrôle parental 35
3.4 QoS adaptative 39
3.4.1 Surveillance de la bande passante 39
3.4.2 QoS 40
3.4.3 Historique internet 41
3.5 Dispositif d'analyse du trafic 42
3.6 Utiliser les applications USB 43
3.6.1 Utiliser AiDisk 43
3.6.2 Utiliser les centres de serveurs 46

Table des matières

3.7 Utiliser AiCloud 2.0 51
3.7.1 Cloud Disk 51
3.7.2 Smart Access 53
3.7.3 Smart Sync 53
3.7.4 Sync Server 55
3.7.5 Paramètres 58
3.8 Utilisation du service SMS 59
3.8.1 Envoyer un message 59
3.8.2 Boîte de réception 60

4 Configurer les paramètres avancés

4.1 Wi-Fi 61
4.1.1 Paramètres de base 61
4.1.2 WPS 63
4.1.3 Pontage WDS 65
4.1.4 Filtrage d'adresses MAC 67
4.1.5 Service RADIUS 68
4.1.6 Professional (Professionnel) 69
4.2 Réseau local (LAN) 72
4.2.1 IP réseau local (LAN) 72
4.2.2 Serveur DHCP 73
4.2.3 Routage 75
4.2.4 Télévision sur IP 76
4.2.5 Switch Control (Contrôle de commutation) 76
4.3 Réseau étendu (WAN) 77
4.3.1 Connexion internet 77
4.3.2 Protocole IPv6 (Paramètres internet) 86
4.3.3 Dual WAN (Double WAN) 87
4.3.4 Déclenchement de port 89
4.3.5 Serveur virtuel et redirection de port 91
4.3.6 Zone démilitarisée 94
4.3.7 Service DDNS 95
4.3.8 NAT Passthrough 96

Table des matières

4.4 IPv6 (Protocole IPv6) 97
4.5 Serveur VPN 98
4.6 Pare-feu 99
4.6.1 Paramètres de base 99
4.6.2 Filtrage d'URL 99
4.6.3 Filtrage de mots-clés 100
4.6.4 Filtrage de services réseau 101
4.6.5 Pare-feu IPv6 101
4.7 Administration 102
4.7.1 Mode de fonctionnement 102
4.7.2 System (Système) 103
4.7.3 Mise à jour du firmware 105
4.7.4 Restauration/Sauvegarde/Transfert de paramètres. 106
4.8 Journal système 107
4.9 Liste des fonctions prises en charge 108

5 Utilitaires

5.1 Device Discovery (Détection d'appareils) 110
5.2 Firmware Restoration (Restauration du firmware) 111
5.3 Configurer un serveur d'impression 113
5.3.1 Utilitaire ASUS EZ Printer Sharing 113
5.3.2 Utiliser le protocole LPR pour partager une imprimante 116
5.4 Download Master 121
5.4.1 Configurer les paramètres BitTorrent 123
5.4.2 Paramètres NZB 124
5.4.3 Paramètres eMule 124

6 Dépannage
6.1 Dépannage de base 125
6.2 Foire aux questions (FAQ) 128

Annexes
Notices 137
Informations de contact ASUS 151

1 Présentation de votre routeur Wi-Fi

1.1 Bienvenue !

Merci d'avoir acheté un routeur Wi-Fi ASUS 4G-AC86U

Puissant et élégant, le routeur 4G-AC86U est compatible avec les réseaux Wi-Fi à double bande 2,4 GHz et 5 GHz, offrant un streaming HD Wi-Fi et 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. Enfin la technologie ASUS Green Network permet de faire jusqu'à 70 % d'économie d'énergie.

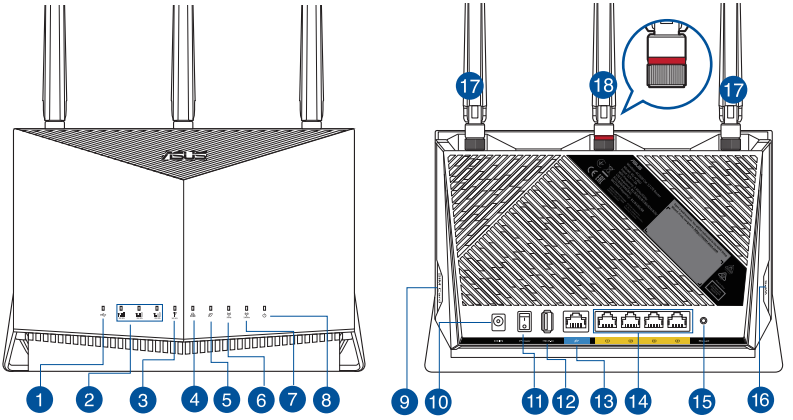
1.2 Contenu de la boîte

- ☑ Routeur Wi-Fi 4G-AC86U
- ☑ Câble réseau (RJ-45)
- ☑ 2 x Antennes 3G/4G
- ☑ Adaptateur secteur
- ☑ Guide de démarrage rapide
- ☑ 1 x Antenne Wi-Fi (avec anneau rouge)

REMARQUES :

- Contactez votre revendeur ou 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 Wi-Fi



1	**Voyant USB** Éteint : Routeur éteint ou aucune connexion physique. Allumé : Connexion établie à un périphérique USB.
2	**Voyants d'indication de la puissance du signal 3G/4G** 1 voyant allumé : Signal faible 2 voyants allumés : Signal normal 3 voyants allumés : Signal puissant
3	**Voyant LED du haut débit mobile** Blanc : Connexion 4G établie. Bleu : Connexion 3G établie. Rouge : Aucune connexion au réseau mobile haut débit. Éteint : Aucune carte nano SIM détectée.
4	**Voyant LED réseau local (LAN)** Éteint : Aucune activité de données ou aucune connexion physique. Allumé : Connexion Ethernet établie.
5	**Voyant réseau étendu (WAN) (Internet)** Éteint : Aucune activité de données ou aucune connexion physique. Allumé : Connexion établie à un réseau étendu (WAN).
6	**Voyant Wi-Fi 5 GHz** Éteint : Aucun signal 5 GHz. Allumé : Routeur prêt à établir une connexion Wi-Fi 5 GHz. Clignotant : Transmission ou réception de données Wi-Fi.
7	**Voyant Wi-Fi 2,4 GHz** Éteint : Aucun signal 2,4 GHz. Allumé : Routeur prêt à établir une connexion Wi-Fi 2,4 GHz. Clignotant : Transmission ou réception de données Wi-Fi.

8	**Voyant d'alimentation** Éteint : Aucune alimentation. Allumé : Le routeur est prêt. Clignote lentement : Mode de secours Clignote rapidement : WPS est en cours de traitement.
9	**Fente pour carte nano SIM** Installez une carte nano SIM dans ce slot pour établir une connexion internet à un réseau mobile haut débit.
10	**Prise d'alimentation (CC)** Insérez l'adaptateur secteur dans ce port puis reliez votre routeur à une source d'alimentation.
11	**Bouton d'alimentation** Ce bouton permet d'allumer ou d'éteindre le routeur.
12	**Port USB 2.0** Insérez un dispositif USB 2.0 tel qu'un périphérique de stockage USB dans ce port.
13	**Port réseau étendu (WAN) (Internet)** Connectez un câble réseau sur ce port pour établir une connexion à un réseau étendu (WAN).
14	**Ports réseau local (LAN) 1 à 4** Connectez des câbles réseau sur ces ports pour établir une connexion à un réseau local (LAN).
15	**Bouton de réinitialisation** Ce bouton permet de restaurer les paramètres par défaut du routeur.
16	**Bouton WPS** Maintenez ce bouton enfoncé pour lancer l'assistant WPS.
17	Antennes LTE amovibles
18	Antenne Wi-Fi amovible

REMARQUES :

- Utilisez uniquement l'adaptateur secteur fourni avec votre appareil. L'utilisation d'autres adaptateurs peut endommager l'appareil.
- Assurez-vous d'avoir bien inséré la carte nano SIM dans son slot avant d'allumer le routeur.

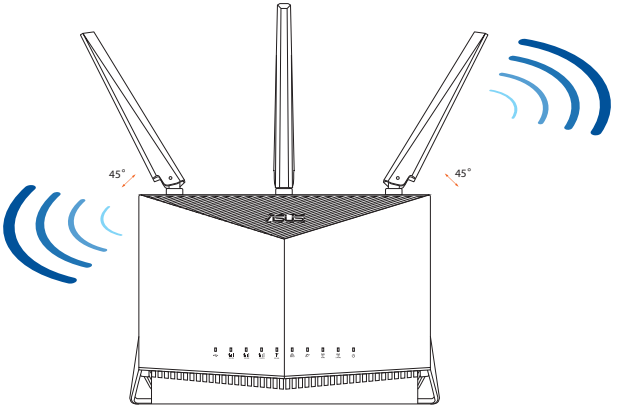
Conditions environnementales :

Adaptateur secteur CC	Sortie CC : +12V (3A max.)		
Température de fonctionnement	0-40°C	Température de stockage	-40~70°C
Humidité de fonctionnement	10 ~ 95%	Humidité de stockage	5 ~ 95%

1.4 Placer le routeur

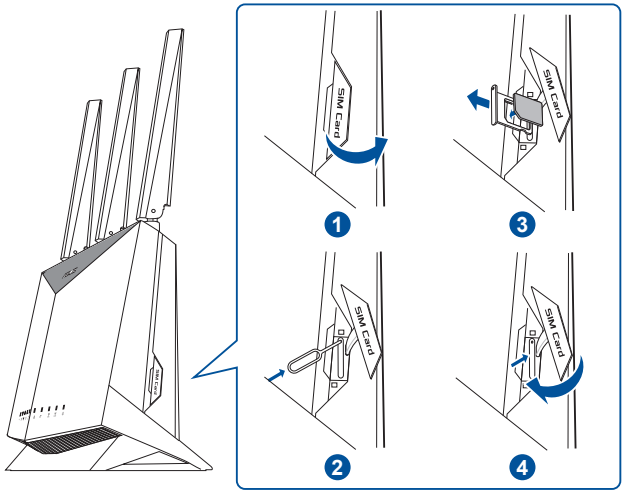
Pour optimiser la transmission du signal Wi-Fi entre votre routeur et les périphériques réseau y étant connectés, veuillez vous assurer des points suivants :

- Placez le routeur Wi-Fi dans un emplacement central pour obtenir une couverture Wi-Fi 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 Wi-Fi 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 Wi-Fi.
- 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.
- Orientez les antennes comme sur l'illustration ci-dessous.



1.5 Installer une carte Nano SIM dans votre routeur

1. Retirez le cache de la fente Nano SIM sur le côté droit de votre routeur.
2. Insérez une pointe dans l'orifice d'éjection de la fente pour carte nano SIM pour éjecter le plateau.
3. Placez la carte Nano SIM sur le plateau.
4. Poussez légèrement le plateau pour le refermer.



2 Prise en main

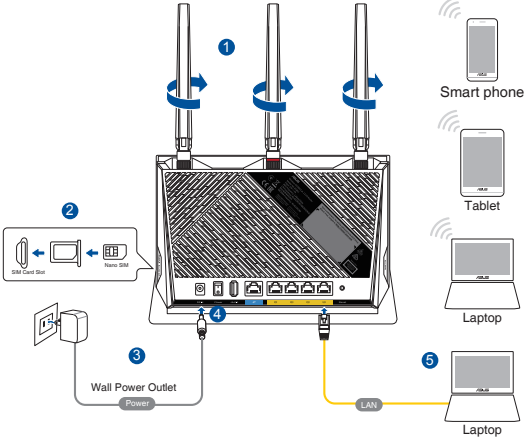
2.1 Configurer le routeur

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 Wi-Fi.
- L'identification de l'emplacement de l'antenne-relais la plus proche vous aidera à trouver le meilleur signal.
- Le nom d'utilisateur et le mot de passe par défaut sont **admin** et **admin**.

REMARQUES :

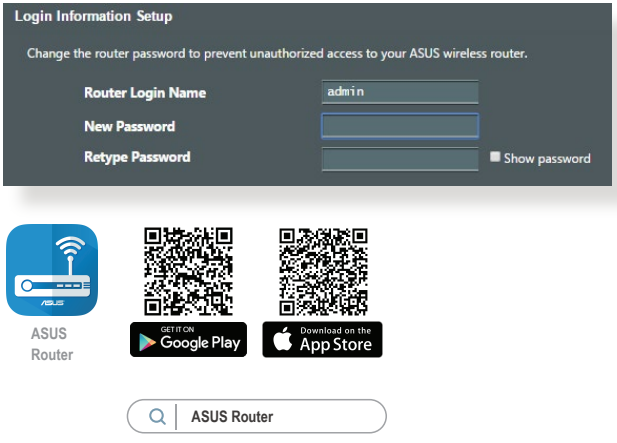
- La LED haut débit mobile s'allume lorsque vous démarrez le routeur avec une carte Nano SIM installée.
- Assurez-vous que la LED haut débit mobile soit allumée avant de configurer votre routeur grâce à l'assistant de configuration internet rapide.
- Vous pouvez utiliser une connexion haut débit mobile ou WAN Ethernet pour accéder à Internet.
- L'auto-détection de votre type de connexion a lieu lorsque vous configurez votre routeur haut débit mobile pour la première fois ou lorsque vous restaurez les paramètres par défaut routeur. Pendant le processus de configuration internet rapide, vous devrez peut-être saisir le code PIN de la carte SIM et l'identifiant du point d'accès réseau (APN) que vous avez obtenu auprès de votre fournisseur d'accès internet (FAI).



A. Connexion filaire

Pour configurer votre routeur via une connexion filaire :

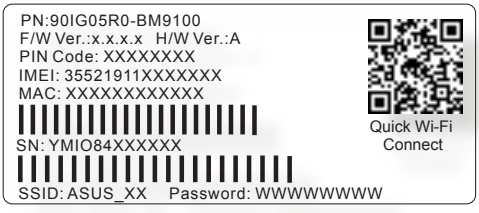
1. Connectez les antennes 3G/4G aux connecteurs gauche et droit, et l'antenne WiFi au connecteur central.
2. Insérez la carte Nano SIM dans la fente pour carte Nano SIM.
3. Reliez une extrémité de l'adaptateur secteur au port d'alimentation (CC) du routeur et l'autre extrémité à une prise électrique.
4. Appuyez sur le bouton d'alimentation pour démarrer votre routeur haut débit mobile et patientez quelques minutes pour obtenir une connexion internet.
5. Connectez votre ordinateur au routeur à l'aide d'un câble réseau Ethernet.
6. Configurez votre routeur grâce à l'assistant de configuration internet rapide après que la LED haut débit mobile ⚲ se soit allumée.
   a. Ouvrez votre navigateur internet et saisissez http://router.asus.com dans la barre d'adresse pour ouvrir l'interface de gestion. Suivez les instructions apparaissant à l'écran pour effectuer la configuration.
   b. Vous pouvez également configurer votre routeur à l'aide de l'application ASUS Router. Téléchargez l'application ASUS Router pour configurer votre routeur par le biais de vos appareils mobiles.
7. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.



B. Connexion Wi-Fi

Pour configurer votre routeur via une connexion Wi-Fi :

1. Connectez les antennes 3G/4G aux connecteurs gauche et droit, et l'antenne WiFi au connecteur central.
2. Insérez la carte Nano SIM dans la fente pour carte Nano SIM.
3. Reliez une extrémité de l'adaptateur secteur au port d'alimentation (CC) du routeur et l'autre extrémité à une prise électrique.
4. Appuyez sur le bouton d'alimentation pour démarrer votre routeur haut débit mobile et patientez quelques minutes pour obtenir une connexion internet.
5. Connectez-vous au réseau Wi-Fi dont le nom (SSID) est affiché sur l'étiquette du produit située à l'arrière du routeur. Vous pouvez vous connecter en parcourant la liste des SSID ou en scannant le code QR pour une connexion rapide.

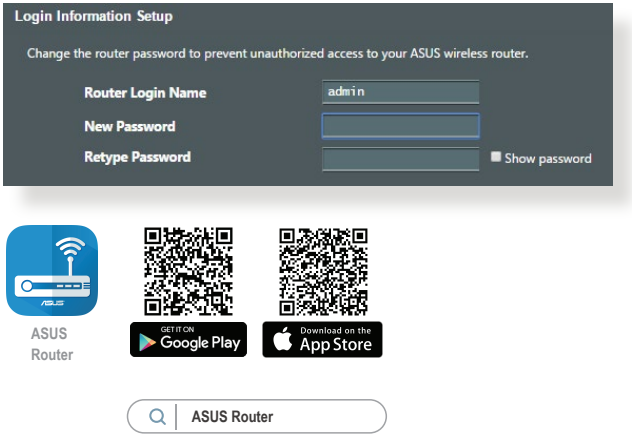


* **XX** correspond aux deux derniers chiffres de l'adresse MAC 2,4 GHz. Vous pouvez les trouver sur l'étiquette située à l'arrière de votre routeur.

6. Configurez votre routeur grâce à l'assistant de configuration internet rapide après que la LED haut débit mobile ⚲ se soit allumée.
   a. Ouvrez votre navigateur internet et saisissez http://router.asus.com dans la barre d'adresse pour ouvrir l'interface de gestion. Suivez les instructions apparaissant à l'écran pour effectuer la configuration.
   b. Vous pouvez également configurer votre routeur à l'aide de l'application ASUS Router. Téléchargez l'application ASUS Router pour configurer votre routeur par le biais de vos appareils mobiles.
7. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.

REMARQUES :

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



2.2 Assistant de configuration internet

Pour configurer votre routeur à l'aide de l'assistant de configuration internet :

1. Vérifiez que les voyants suivants sont allumés :
   - Voyant d'alimentation
   - Voyant réseau étendu (WAN) ou haut débit mobile
   - Voyant Wi-Fi 2,4 GHz
   - Voyant Wi-Fi 5 GHz
2. Ouvrez votre navigateur internet (ex : Internet Explorer, Google Chrome, Safari ou Firefox).

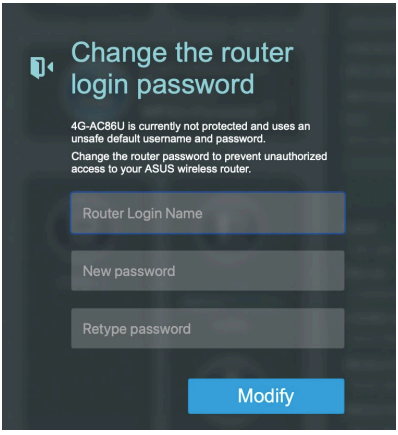
REMARQUE : Si l'assistant de configuration internet ne s'exécute pas automatiquement, entrez http://router.asus.com dans la barre d'adresse et réactualisez le navigateur.

---

3. Connectez-vous à l'interface de gestion du routeur. L'assistant de configuration internet s'exécute automatiquement. Par défaut, le nom d'utilisateur et le mot de passe de connexion à l'interface de gestion du routeur sont "admin".

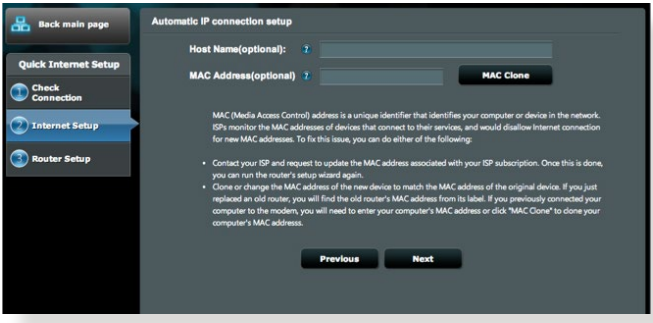


4. Attribuez un nom de connexion et un mot de passe au routeur, puis cliquez sur **Suivant**. Ces identifiants vous seront demandés à chaque tentative de connexion à l'interface de gestion du routeur. Veuillez noter et conserver vos identifiants pour une utilisation ultérieure.

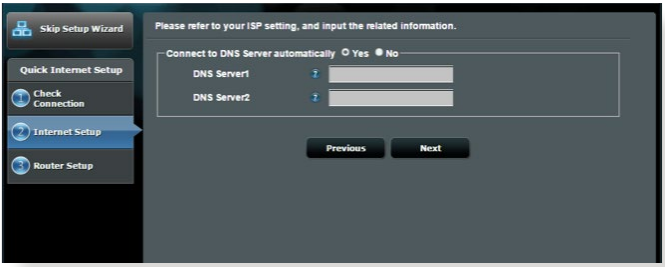


5. Si le port réseau étendu (WAN) est connecté, le routeur Wi-Fi détecte automatiquement si votre connexion utilise une **IP dynamique** ou **statique**, le protocole **PPPoE**, **PPTP** ou **L2TP**. Vous pouvez obtenir vos informations de connexion auprès de votre FAI (Fournisseur d'accès à Internet). Si vous utilisez une connexion à adresse IP dynamique (DHCP), l'assistant de configuration internet vous redirigera vers l'étape suivante.

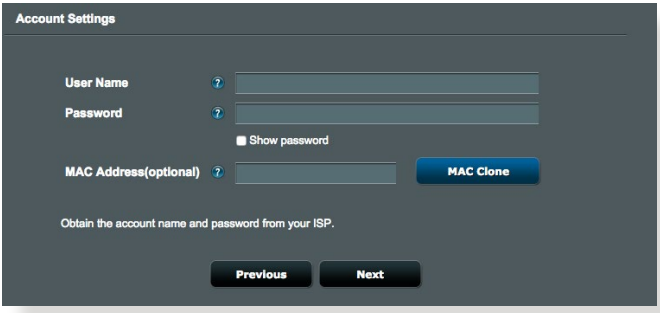
Connexion à adresse IP automatique (DHCP)



Connexion utilisant le protocole PPPoE, PPTP ou L2TP

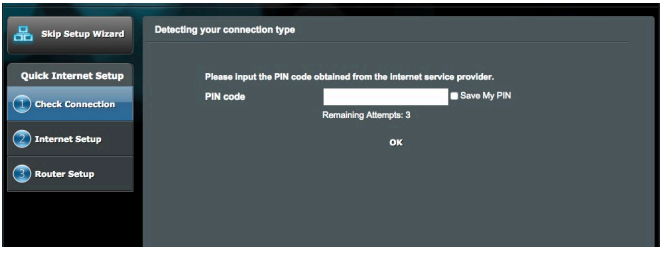


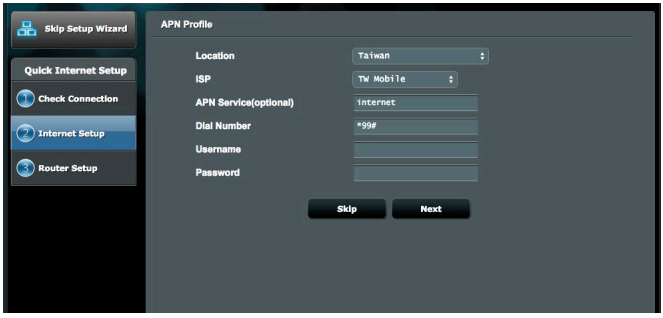
Connexion à adresse IP statique



6. Si vous utilisez une connexion 3G/4G, les paramètres de connexion sont automatiquement détectés et appliqués. Si ce n'est pas le cas, réglez ces paramètres manuellement.

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



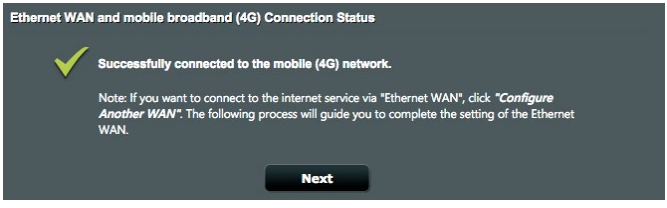


7. L'état de la connexion internet apparaît à l'écran. Cliquez sur **Next** (Suivant) pour continuer.

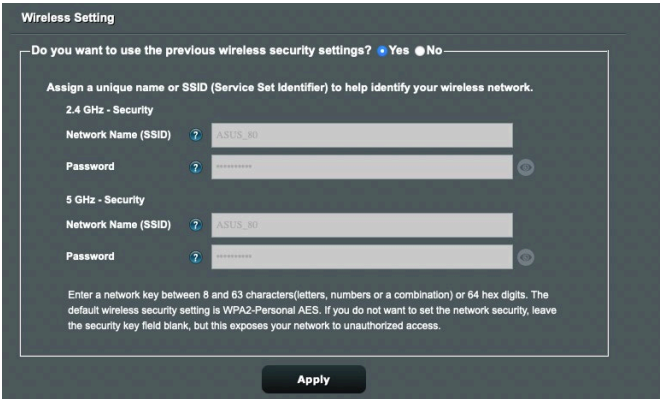
   Connexion Wi-Fi cellulaire établie



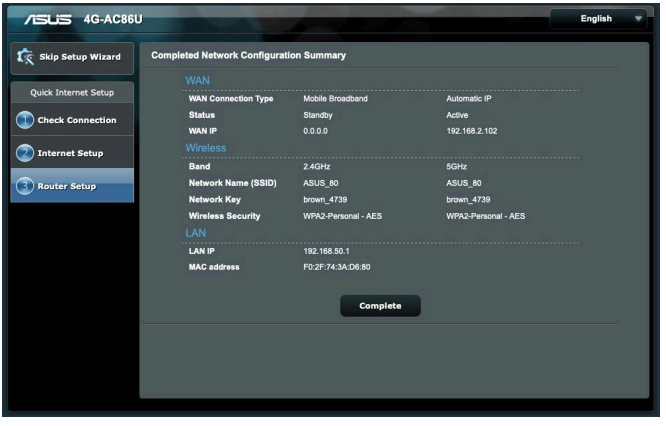
   Connexion filaire WAN Ethernet établie



8. Passez à l'étape suivante pour configurer les paramètres de connexion Wi-Fi.



9. Attribuez un nom (SSID) au réseau ainsi qu'une clé de sécurité pour votre connexion Wi-Fi 2,4 GHz. Cliquez sur **Apply** (Appliquer) une fois terminé.
10. Les paramètres de connexion internet et Wi-Fi apparaissent. Cliquez sur **Next** (Suivant) pour terminer.



11. Les voyants d'indication de la puissance du signal 3G/4G s'allument pour indiquer que la connexion a bien été établie.

3 Configurer les paramètres généraux

3.1 Utiliser la carte du réseau

Carte du réseau La carte du réseau vous permet d'avoir une vue d'ensemble du réseau, gérer les clients du réseau et contrôler votre périphérique USB.



3.1.1 Configurer les paramètres de sécurité Wi-Fi

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

Pour configurer les paramètres de sécurité Wi-Fi :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Dans l'écran Network Map (Carte du réseau), cliquez sur l'icône d'état du système . La colonne **System status** (État du système) affiche les options de sécurité telles que le SSID, la méthode d'authentification et les paramètres de chiffrement.

Paramètres de sécurité 2,4 GHz



Paramètres de sécurité 5 GHz



3. Dans le champ **Wireless name (SSID)** (Nom Wi-Fi (SSID)), spécifiez un nom unique pour votre réseau Wi-Fi.
4. Dans le menu déroulant **Authentication Method** (Méthode d'authentification), sélectionnez la méthode de chiffrement.

   Si vous sélectionnez **WPA-Personal** ou **WPA-2 Personal** comme méthode de chiffrement, entrez une clé de sécurité appropriée.

IMPORTANT ! La norme IEEE 802.11n/ac n'autorise pas l'utilisation du bas 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.

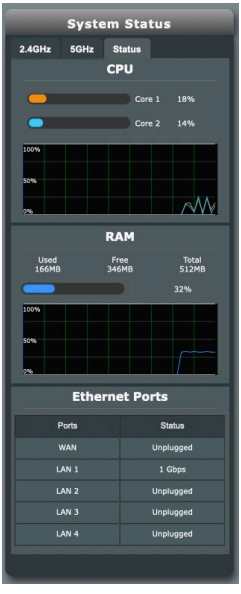
---

5 Cliquez sur **Apply** (Appliquer) une fois terminé.

3.1.2 État du système

Pour surveiller les ressources du système :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Dans l'écran Network Map (Carte du réseau), cliquez sur l'icône d'état du système . pour afficher l'état d'utilisation du processeur et de la mémoire.



3.1.3 Gérer les clients du réseau

Pour gérer les clients de votre réseau :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).

2. Dans l'écran **Network Map** (Carte du réseau), cliquez sur l'icône Client Status (États clients) pour afficher les informations relatives aux clients de votre réseau.



3. Dans la liste des clients, cliquez sur l'icône appareil pour afficher le profil détaillé d'un appareil client spécifique.

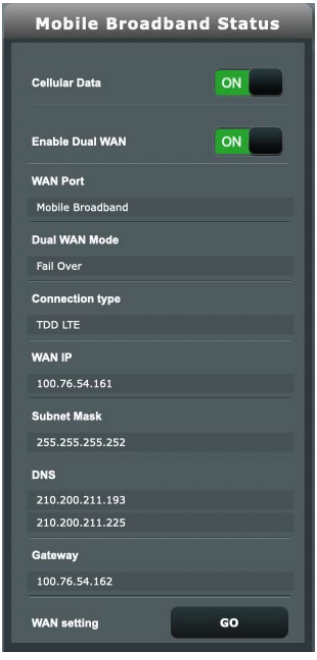


3.1.4 Surveiller l'état de la connexion internet

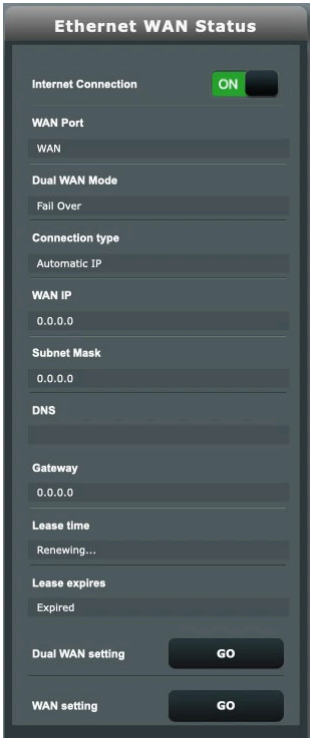
Pour surveiller l'état de la connexion internet :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Dans l'écran **Network Map** (Carte du réseau), cliquez sur l'icône internet pour afficher les informations relatives à la connexion internet. Vous pouvez aussi sélectionner l'icône de haut débit mobile pour afficher les informations relatives au haut débit mobile.
3. Pour désactiver l'interface WAN (réseau étendu), cliquez sur les boutons commutateurs de **Cellular Data** (Données cellulaires) et **Internet Connection** (Connexion internet).

Réseau cellulaire à haut débit



Réseau étendu (WAN) sur Ethernet



3.1.5 Surveiller un périphérique USB

Le routeur Wi-Fi ASUS intègre un port USB pour la connexion de périphériques USB, tels qu'un périphérique de stockage ou une imprimante USB. Ce port vous permet de surveiller votre environnement de travail, partager des fichiers ou une imprimante avec les clients de votre réseau.

Pour surveiller votre périphérique USB :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Network Map** (Carte du réseau).
2. Dans l'écran **Network Map** (Carte du réseau), cliquez sur l'icône USB Disk Status (État de disque USB) pour afficher les informations du disque USB connecté au routeur Wi-Fi.
3. Dans le champ **Media Server** (Serveur multimédia), cliquez sur **GO** pour configurer un serveur iTunes ou DLNA permettant le partage de fichiers.

REMARQUE : Le routeur Wi-Fi fonctionne avec la plupart des périphériques de stockage USB d'une capacité maximale de 2 To et prend en charge la lecture/écriture pour les formats de fichiers FAT16, FAT32, EXT2, EXT3 et NTFS.

---

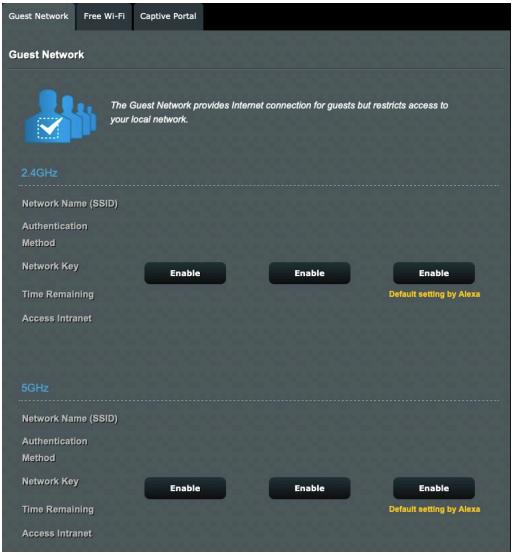
4. Dans le champ **AiDisk Wizard** (Assistant AiDisk), cliquez sur **GO** pour configurer un serveur FTP permettant le partage de fichiers sur Internet.
5. Pour éjecter un disque USB de l'interface USB, cliquez sur le bouton **Remove** (Éjecter) du champ **Safely Remove disk** (Éjecter le disque USB en toute sécurité). Lorsque le disque a été éjecté, l'état du disque apparaît comme étant **Unmounted** (Non monté).





3.2 Réseau invité

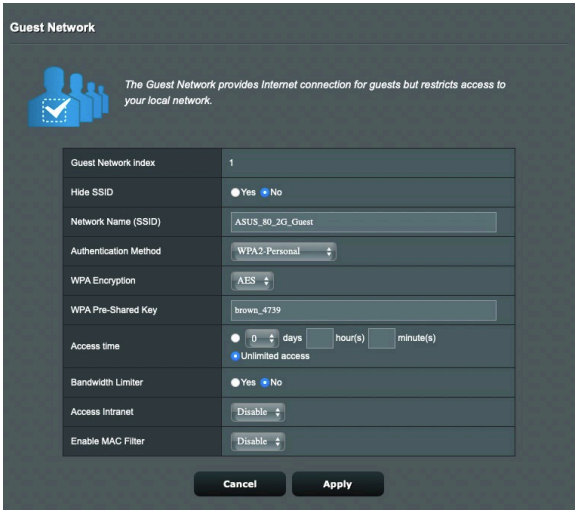
Un réseau invité permet d'offrir une connexion internet aux utilisateurs temporaires via l'accès à un SSID ou réseau séparé, et restreint l'accès au réseau local privé.



Pour créer un réseau invité :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Guest Network** (Réseau invité).
2. Sélectionnez la bande de fréquence à utiliser (2,4 GHz ou 5 GHz) pour le réseau invité.
3. Cliquez sur **Enable** (Activer).
4. Configurez les paramètres invités dans la fenêtre contextuelle
5. Assignez un nom au réseau pour pouvoir identifier votre réseau invité.
6. Sélectionnez une méthode d'authentification.
7. Si vous avez sélectionné une méthode d'authentification WPA, sélectionnez un chiffrement WPA.
8. Définissez les valeurs du champ **Access time** (Temps d'accès) ou cochez l'option **Limitless** (Illimité).

9. Sélectionnez l'option **Disable** (Désactiver) ou **Enable** (Activer) du champ **Access Intranet** (Accès au réseau local).
10. Sélectionnez **Disable** (Désactiver) ou **Enable** (Activer) sur l'élément **Enable MAC Filter** (Activer le filtrage d'adresses MAC) pour votre réseau invité.



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

REMARQUES :

- Visitez https://www.asus.com/fr/support/FAQ/1034977/ pour savoir **Comment configurer le portail captif**.
- Visitez https://www.asus.com/fr/support/FAQ/1034971/ pour savoir **Comment configurer le Wi-Fi gratuit**.

3.3 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.



3.3.1 Protection du réseau

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

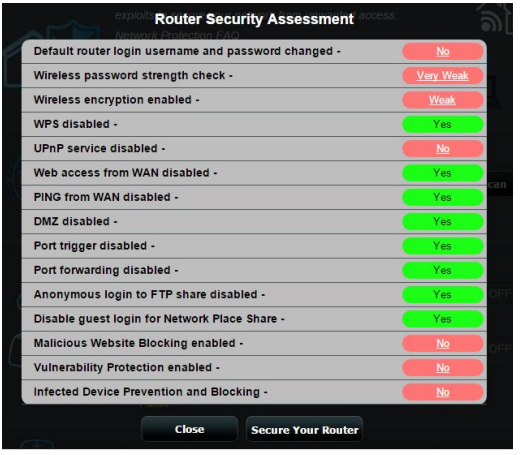


Configurer la protection du réseau

Pour configurer la protection du réseau :

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

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



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

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

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

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

Blocage de sites malveillants

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

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

Pour activer le blocage des sites malveillants :

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

Protection contre les vulnérabilités

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 la protection contre les vulnérabilités :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale **AiProtection**, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau de protection contre les vulnérabilités, cliquez sur **ON** (OUI).

Protection et blocage des périphériques infectés

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

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

Pour activer la protection et le blocage des périphériques infectés :

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

Pour configurer les préférences d'envoi d'alertes :

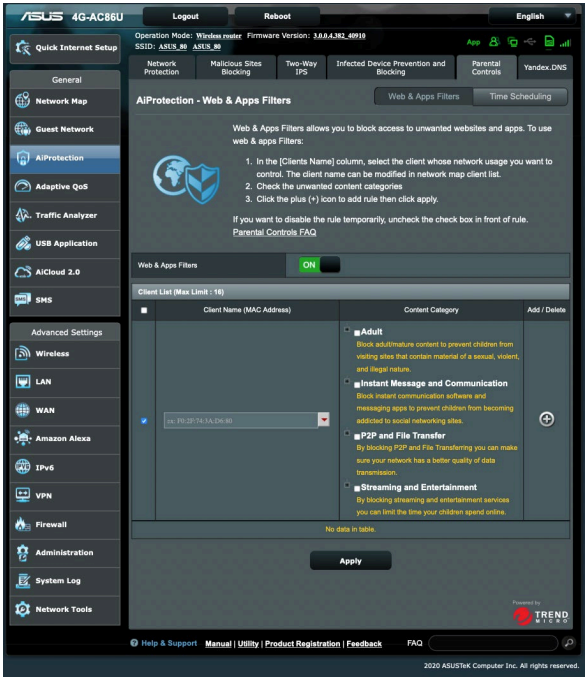
1. À partir du panneau de protection et de blocage des périphériques infectés, cliquez sur **Alert Preference** (Préférence d'envoi d'alertes).
2. Sélectionnez ou entrez le nom du service de messagerie électronique, l'adresse email et le mot de passe, puis cliquez sur **Apply** (Appliquer).

3.3.2 Configurer le contrôle parental

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

Pour accéder à la page principale du contrôle parental :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale de **AiProtection**, cliquez sur l'onglet **Parental Controls** (Contrôle parental).



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.

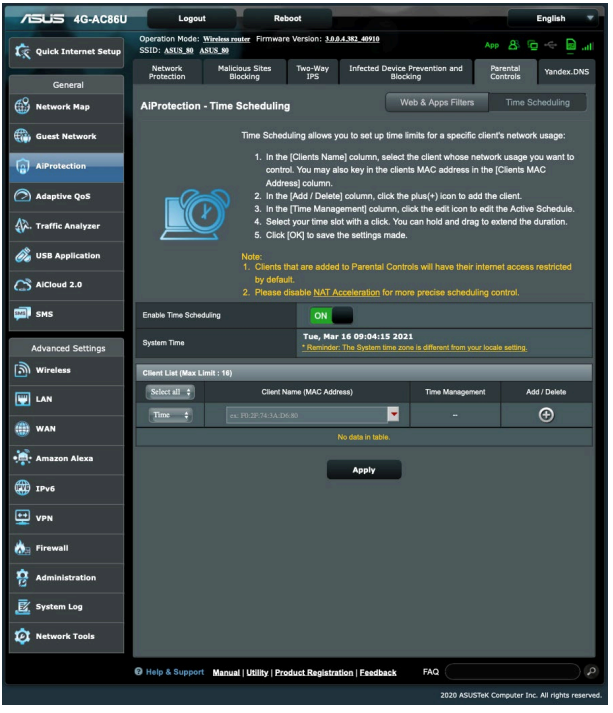
Pour configurer le filtrage de sites et d'applications :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **AiProtection**.
2. À partir de la page principale de **AiProtection**, cliquez sur l'icône **Parental Controls** (Contrôle parental) pour accéder à l'onglet de contrôle parental.
3. À partir du panneau **Web & Apps Filters** (Filtrage de sites et d'applications), cliquez sur **ON** (OUI).
4. Cliquez sur **I agree** (J'accepte) pour accepter le contrat de licence pour utilisateur final.
5. Dans la colonne **Client List** (Liste des clients), sélectionnez un client ou tapez son nom dans la liste déroulante.
6. 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).
7. Cliquez sur ⊕ pour ajouter le profil du client.
8. 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) > **AiProtection** > **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 **Client Name (MAC address)** (Nom du client (Adresse MAC)), sélectionnez un client ou saisissez son nom dans la liste déroulante.

REMARQUE : Vous pouvez aussi saisir l'adresse MAC du client dans la colonne **Client Name (MAC address)** (Nom du client (Adresse MAC)). 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.

3.4 QoS adaptative

3.4.1 Surveillance de la bande passante

Cette fonctionnalité vous permet de surveiller la bande passante consommée par le réseau local (LAN) ou étendu (WAN) et affiche les débits montants et descendants de votre connexion.



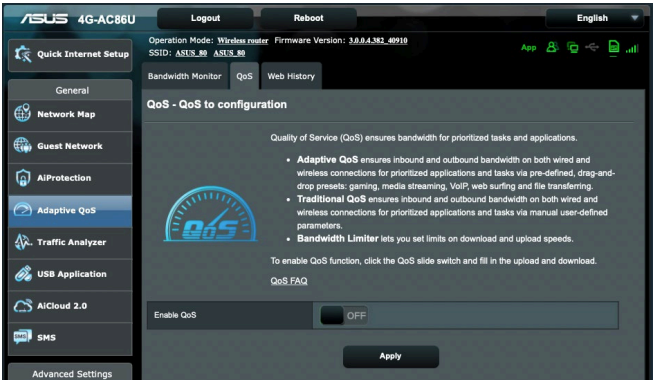
Analyse des applications

Pour activer la fonction d'analyse des applications :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Adaptive QoS** (Service Adaptive QoS) > onglet **Bandwidth Monitor** (Surveillance de la bande passante).
2. À partir du panneau **Apps Analysis** (Analyse des applications), cliquez sur **ON** (OUI).

3.4.2 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) > **Adaptive QoS** (Service Adaptive QoS) > onglet **QoS**.
2. À partir du panneau **Enable QoS** (Activer QoS), cliquez sur **ON** (OUI).
3. Remplissez les champs réservés à la bande passante montante et descendante.

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

---

4. Sélectionnez le type de service QoS (adaptatif ou standard) de votre configuration.

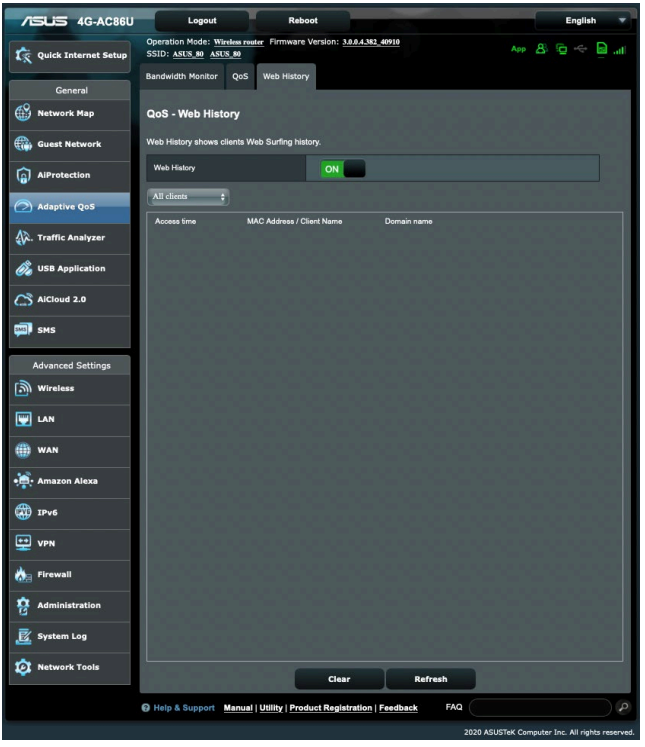
REMARQUE : La définition de chacun des types de service QoS est expliquée dans l'onglet QoS.

---

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

3.4.3 Historique internet

Cette fonctionnalité affiche l'historique et les détails des sites ou des URL visités par le client.

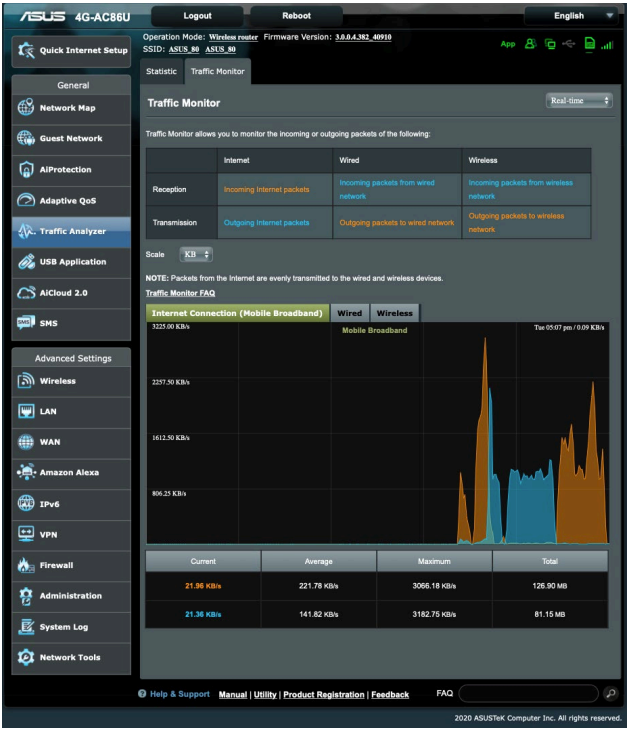


Pour visualiser l'historique internet :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Adaptive QoS** (Service Adaptive QoS) > onglet **Web History** (Historique internet).
2. (Optionnel) Cliquez sur **Refresh** (Actualiser) pour rafraîchir la liste.

3.5 Dispositif d'analyse du trafic

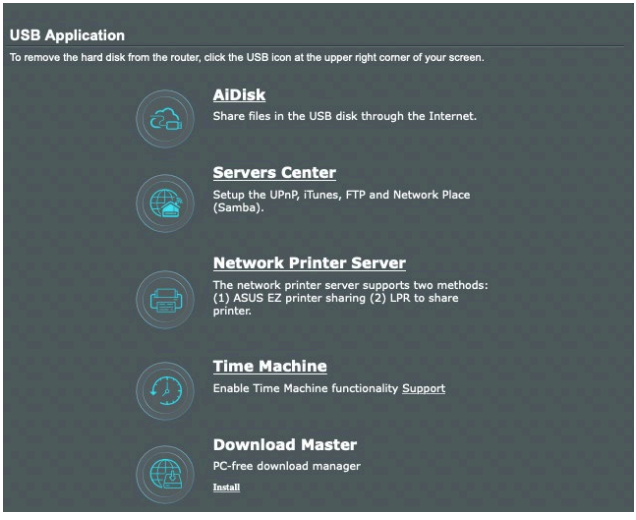
La fonctionnalité de surveillance du trafic vous permet d'évaluer l'usage de la bande passante et la vitesse des connexions internet, du réseau local ou du réseau étendu. Vous pouvez surveiller le trafic du réseau en temps réel ou de manière quotidienne. Le trafic peut aussi être affiché pour les dernières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



3.6 Utiliser les applications USB

La page des applications USB contient les sous-menus AiDisk, Servers Center (Centres de serveurs), Network Printer Server (Serveur d'impression réseau), Time Machine 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 2.0 situé à l'arrière du routeur Wi-Fi. 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.

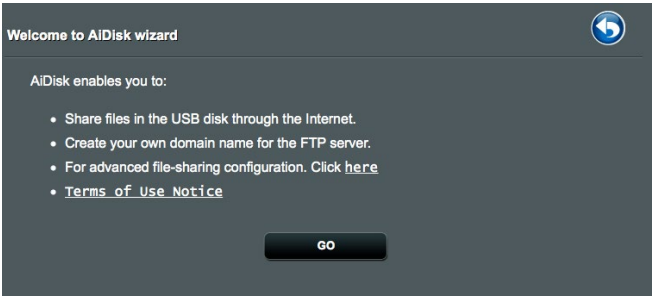


3.6.1 Utiliser AiDisk

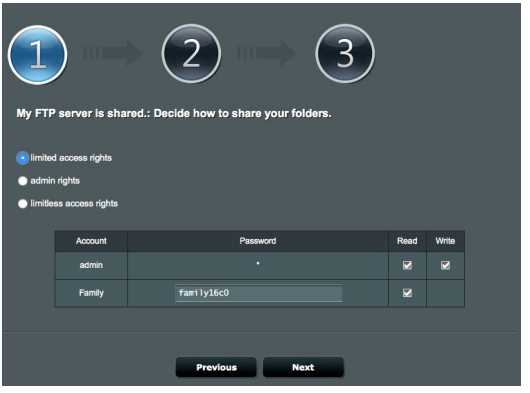
AiDisk vous permet de partager les fichiers contenus sur un périphérique de stockage USB connecté au routeur via Internet. AiDisk offre aussi la possibilité de configurer le service DDNS d'ASUS ou un serveur FTP.

Pour utiliser AiDisk :

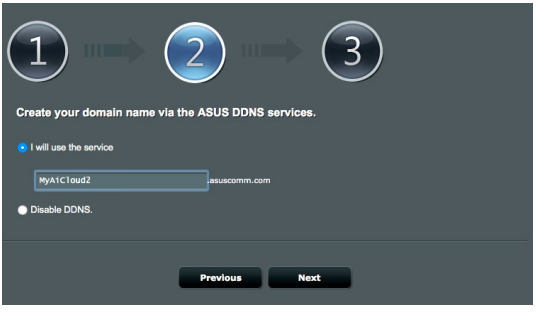
1. À partir du volet de navigation, cliquez sur **General** (Général) > **USB application** (Applications USB) > icône **AiDisk**.
2. À partir de l'écran Welcome to AiDisk wizard (Bienvenue sur l'assistant AiDisk), cliquez sur **Go** (Démarrer).



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



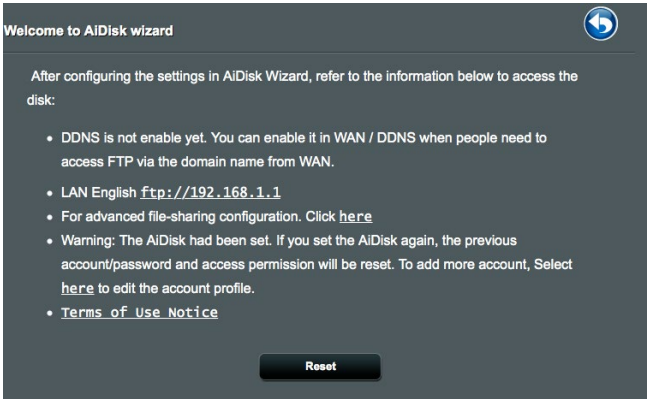
4. Si vous souhaitez créer votre propre nom de domaine dédié au serveur FTP grâce au service DDNS d'ASUS, sélectionnez **I will use the service** (Je souhaite utiliser ce service) et spécifiez le nom de votre domaine. Cliquez sur **Next** (Suivant).





Vous pouvez aussi sélectionner **Disable DDNS** (Désactiver le service DDNS), 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)**.



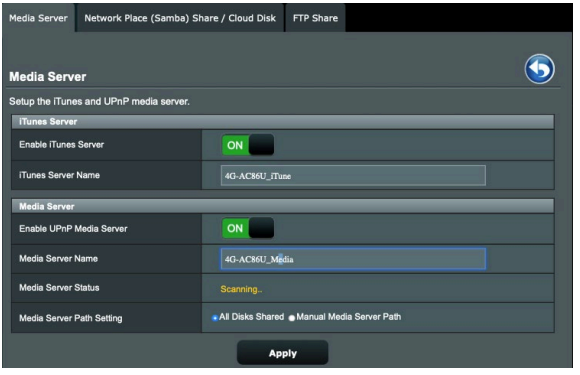
3.6.2 Utiliser les centres de serveurs

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 Wi-Fi autorise les appareils compatibles avec le protocole DLNA 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 DLNA, connectez votre appareil au réseau du routeur Wi-Fi.

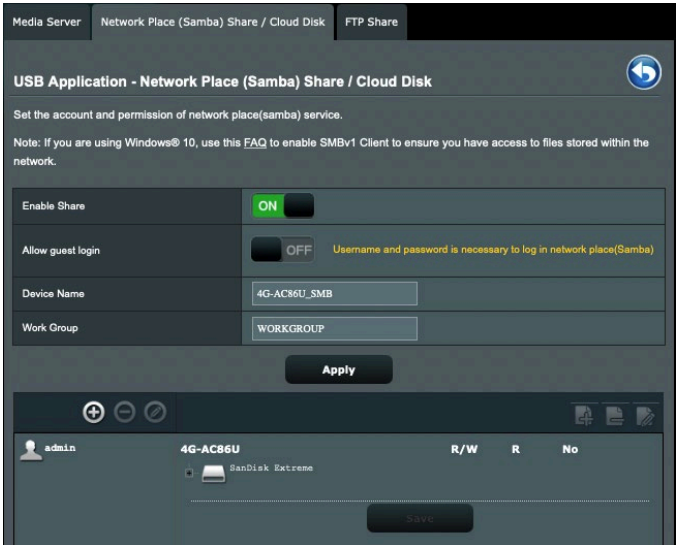


Pour utiliser le service de partage DLNA, allez dans **General** (Général) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > onglet **Media Server** (Serveur multimédia). Vous trouverez ci-dessous une description de chacun des champs disponibles :

- **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.

3.6.3 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 **General** (Général) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > onglet **Network Place (Samba) Share / Cloud Disk** (Partage de favoris réseau / Cloud Disk).

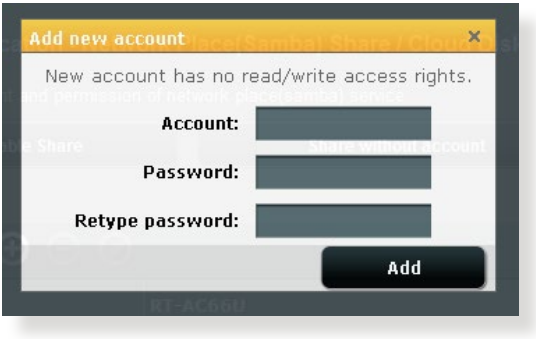
REMARQUE : Le partage Samba est activé par défaut.

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.

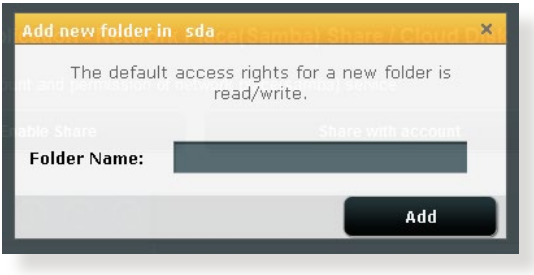
b) Cliquez sur .

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.



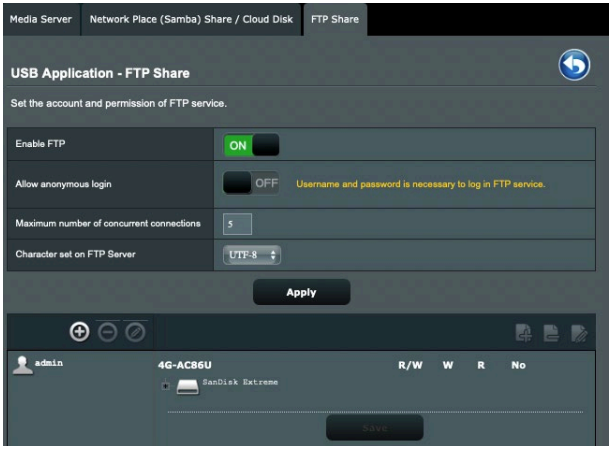
3. Dans la liste des fichiers/dossiers, sélectionnez le type de droits d'accès à affecter aux différents types de fichiers/dossiers :
   - **R/W :** Sélectionnez cette option pour affecter un droit de lecture/écriture à un type spécifique de fichier/dossier.
   - **R :** Sélectionnez cette option pour 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.

3.6.4 Utiliser le service de partage FTP

Le routeur Wi-Fi 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 **3.1.5 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 **3.6.1 Utiliser AiDisk**.

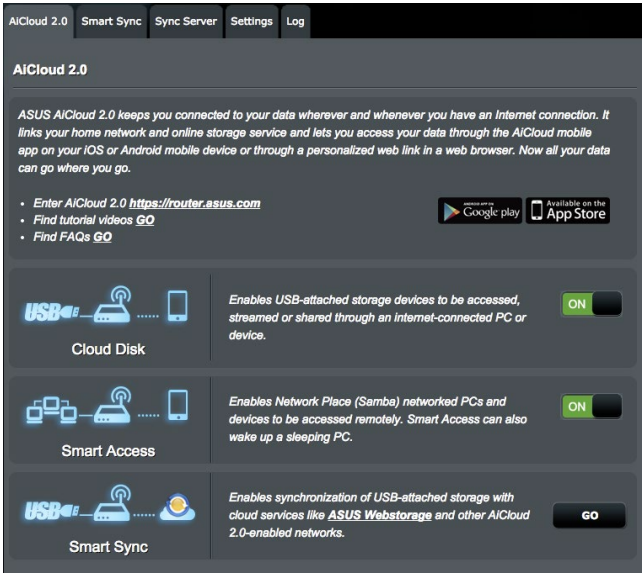
1. À partir du volet de navigation, cliquez sur **General** (Général) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > **Servers Center** (Centres de serveurs) > onglet **FTP Share** (Partage FTP).
2. Dans la liste des fichiers/dossiers, sélectionnez 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.

3.7 Utiliser 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.

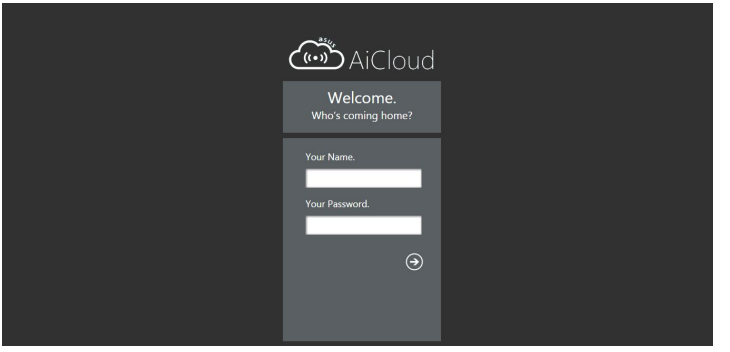
3.7.1 Cloud Disk

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 Wi-Fi.
2. Activez **Cloud Disk**.

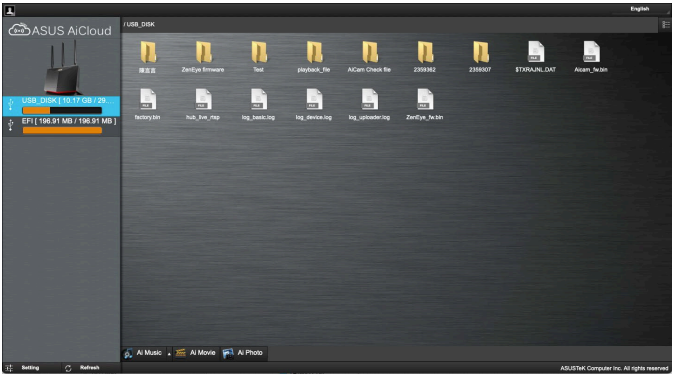


3. Rendez-vous sur https://router.asus.com et entrez les identifiants de connexion de votre routeur. Pour améliorer votre expérience d'utilisation, il est recommandé d'utiliser **Google Chrome** ou **Firefox**.



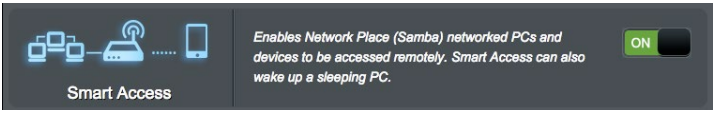
4. Vous pouvez dès lors accéder aux fichiers Cloud Disk des appareils connectés au réseau.

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.



3.7.2 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.



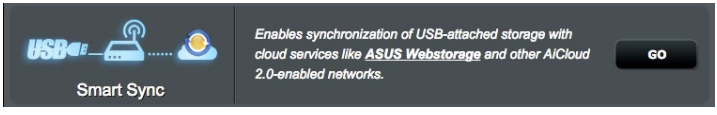
REMARQUES :

- Vous pouvez créer un nom de domaine pour votre routeur grâce au service DDNS d'ASUS. Pour plus de détails, consultez la section **4.3.7 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.

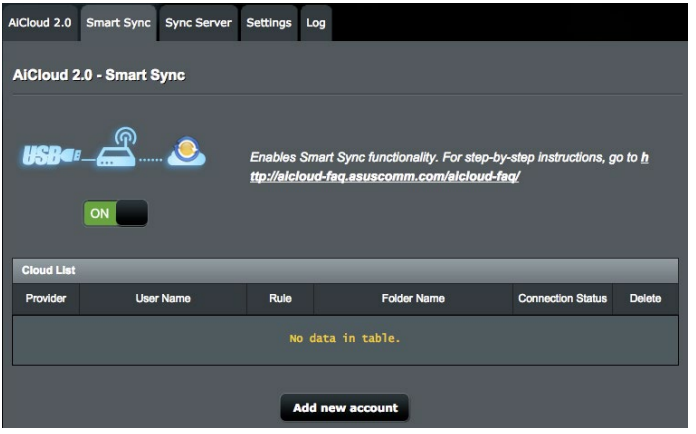
3.7.3 Smart Sync

Pour utiliser Smart Sync :

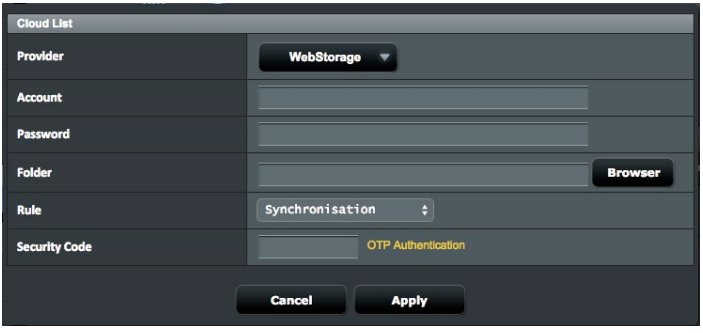
1. À partir du volet de navigation, cliquez sur **AiCloud 2.0** > **AiCloud 2.0** >**Smart Sync** > **Go** (Démarrer).



2. Déplacez l'interrupteur sur **ON** (OUI) pour activer Smart Sync.
3. Cliquez sur **Add new account** (Ajouter un compte).



4. Entrez votre nom d'utilisateur et mot de passe ASUS WebStorage ou Dropbox et sélectionnez le répertoire à synchroniser avec WebStorage.
5. Sélectionnez les règles de synchronisation.
   - **Synchronization (Synchronisation)**: Sélectionner **Synchronization** (Synchronisation) permet de synchroniser un dossier entre deux serveurs.
   - **Download to USB Disk (Télécharger sur disque USB)**: Sélectionner **Download to USB Disk** (Télécharger sur disque USB) permet de copier les fichiers distants sur le dossier local du disque USB.
   - **Upload to Cloud (Télécharger dans le Cloud)**: Sélectionner **Upload to Cloud** (Télécharger dans le Cloud) permet de copier les fichiers locaux sur un service de stockage dans le Cloud tel qu'**ASUS WebStorage**.



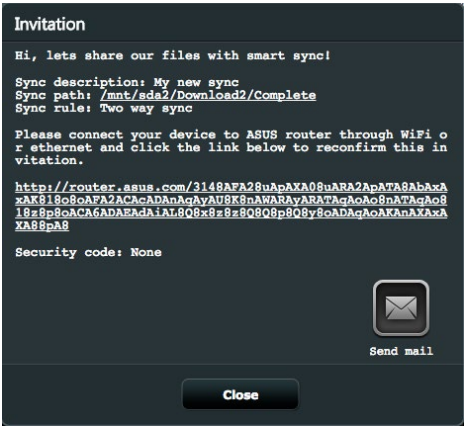
6. Cliquez sur **Apply** (Appliquer)

3.7.4 Sync Server



Pour utiliser Sync Server :

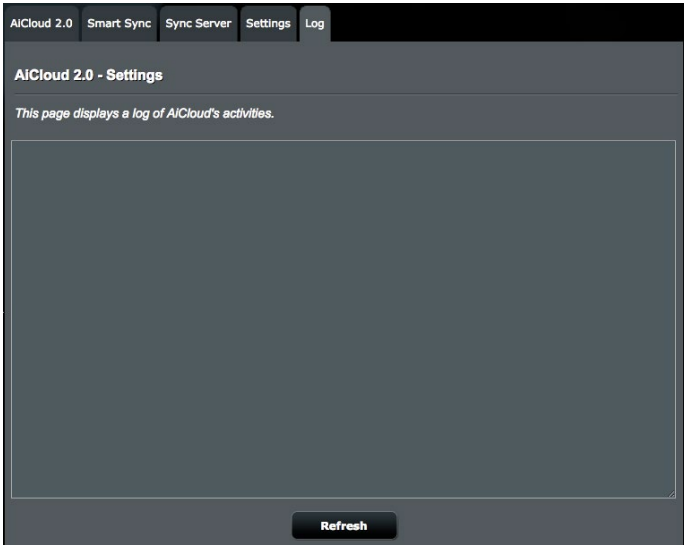
1. À partir du volet de navigation, cliquez sur **AiCloud 2.0** > **Sync Server**.
2. Allez dans les paramètres de Sync Server dans le menu **Invitation Generator** (Générateur d'invitation) pour activer **Smart Sync**.
3. Envoyez l'invitation de synchronisation à votre ami.



4. Une fois l'invitation générée, vous pouvez consulter la tâche de synchronisation dans le tableau **Sync List** (Liste de synchronisation)



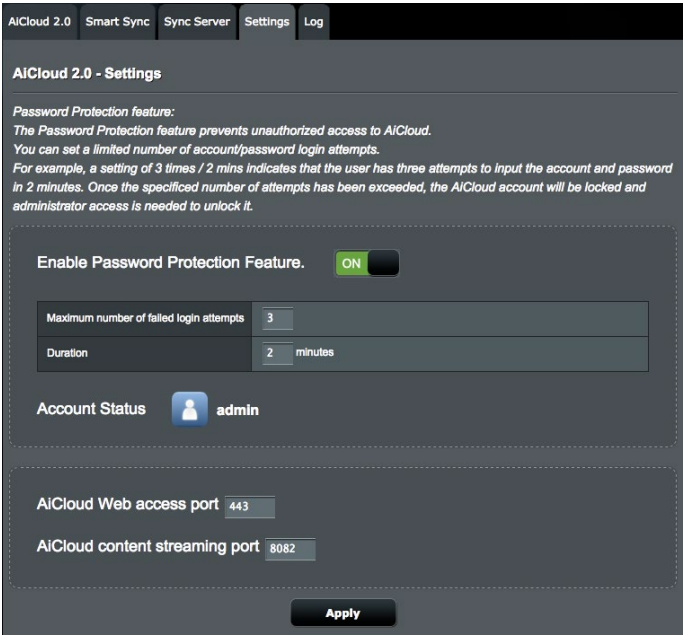
5. Vous pouvez cliquer sur le bouton de suppression pour arrêter une tâche.
6. Vous pouvez aussi consulter les tâches de synchronisation en cliquant sur le bouton **Check log** (Vérifier le journal) ou sur l'onglet **Log** (Journal).


AiCloud 2.0
Smart Sync
Sync Server
Settings
Log
AiCloud 2.0 - Settings
This page displays a log of AiCloud's activities.
Refresh

3.7.5 Paramètres

AiCloud 2.0 vous permet de configurer des règles d'accès pour éviter les intrusions malveillantes, telles que les attaques par dictionnaire. Lorsqu'un hôte tente d'accéder à AiCloud et excède le nombre de tentatives de connexion pré-établi, et ce dans une période de temps donnée, le service AiCloud sera automatiquement désactivé.

Le protocole SSL (Secure Socket Layer) offre une méthode de communication chiffrée entre un serveur internet et un navigateur de sorte à garantir des transferts de données sécurisés, par le biais de la saisie d'un mot de passe par exemple. L'accès au service AiCloud sur Internet requiert l'utilisation d'un port spécifique (443) au travers du protocole HTTPS. L'acheminement de contenu utilise quant à lui le port 8082 au travers du protocole HTTP.



3.8 Utilisation du service SMS

Le service de messagerie SMS est un service de messagerie texte qui vous permet d'envoyer ou de recevoir des messages depuis ou sur votre routeur Wi-Fi.

3.8.1 Envoyer un message

Cette fonction vous permet d'envoyer des messages courts à partir de votre routeur Wi-Fi.

Pour envoyer un nouveau message SMS :

1. Cliquez sur le bouton **New** (Nouveau) New.
2. Saisissez le numéro de téléphone du destinataire.
3. Rédigez votre message.
4. Cliquez sur **Send** (Envoyer) pour envoyer le message.



Pour enregistrer un brouillon :

1. Vous pouvez également enregistrer le brouillon de message en cliquant sur **Save** (Enregistrer).
2. Vous verrez le message répertorié dans la liste **Draft** (Brouillon).
3. Cliquez sur l'icône de modification pour éditer et envoyer le message, ou cochez la case de sélection et cliquez sur pour supprimer le brouillon.



3.8.2 Boîte de réception

La boîte de réception vous permet d'afficher les messages SMS reçus enregistrés dans votre appareil.
Cliquez sur pour afficher plus d'informations, ou cochez la case de sélection d'un message et cliquez sur pour le supprimer.

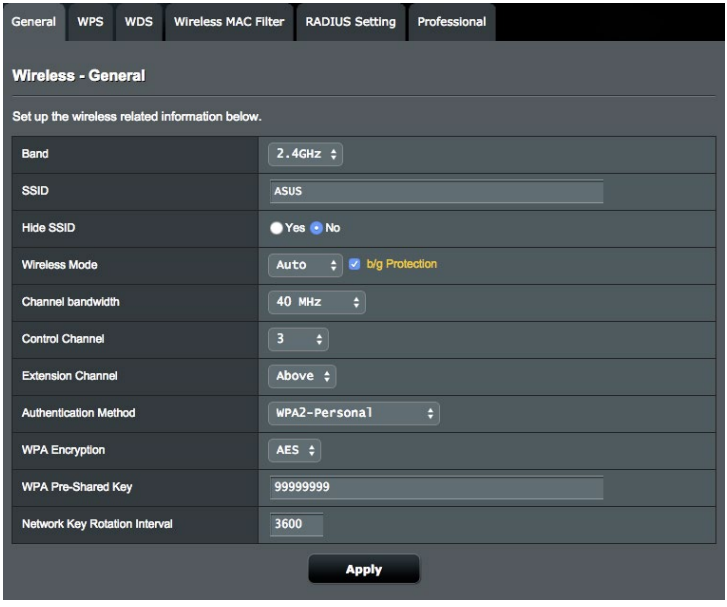


4 Configurer les paramètres avancés

4.1 Wi-Fi

4.1.1 Paramètres de base

L'onglet General (Général) vous permet de configurer les paramètres Wi-Fi de base.



Pour configurer les paramètres Wi-Fi de base :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **General** (Général).
2. Configurez les paramètres Wi-Fi de base pour les bandes de fréquence 2,4 GHz ou 5 GHz.
3. Dans le champ **SSID**, attribuez un nom unique composé d'un maximum de 32 caractères faisant office de SSID (Service Set Identifier) et permettant d'identifier votre réseau Wi-Fi. Les appareils disposant de capacités Wi-Fi peuvent identifier et se connecter à votre réseau Wi-Fi 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.

4. Dans le champ **Hide SSID** (Masquer le SSID), sélectionnez **Yes** (Oui) si vous ne souhaitez pas que les périphériques Wi-Fi puissent détecter votre SSID. Lorsque cette option est activée, vous devez saisir manuellement le SSID sur l'appareil souhaitant se connecter à votre réseau Wi-Fi.
5. Dans le champ **Wireless Mode** (Mode Wi-Fi), sélectionnez l'un de ces options de mode Wi-Fi pour déterminer les types de périphériques Wi-Fi pouvant se connecter à votre routeur Wi-Fi
   - **Auto :** Les appareils utilisant les normes 802.11ac, 802.11n, 802.11g , 802.11b et 802.11a peuvent se connecter au routeur Wi-Fi.
   - **Legacy (Hérité)**: Les appareils utilisant les normes 802.11b/g/n peuvent se connecter au routeur Wi-Fi. Toutefois le matériel prenant en charge la norme 802.11n de manière native, ne fonctionnera qu'à une vitesse maximum de 54 Mb/s.
   - **b/g Protection (Protection b/g)**: Activez cette option pour autoriser le routeur Wi-Fi à protéger les transmissions 802.11n des périphériques hérités avec la connexion 802.11g et 802.11b.
6. Dans le champ **Control Channel** (Canal de contrôle), sélectionnez le canal d'opération du routeur Wi-Fi. Choisissez **Auto** pour autoriser le routeur à sélectionner automatiquement le canal générant le moins d'interférences.
7. Dans le champ **Channel bandwidth** (Bande passante), sélectionnez l'une de ces bandes passantes pour permettre des vitesses de transmission plus élevées :
   - **20/40MHz** (Par défaut) : Sélectionnez cette bande passante pour automatiquement sélectionner la meilleure bande passante pour votre environnement Wi-Fi. Pour la bande des 5 GHz, la bande passante par défaut est **20/40/80MHz**.
   - **80MHz**: Maximise le débit Wi-Fi de la bande des 5 GHz.
   - **40MHz**: Maximise le débit Wi-Fi de la bande des 2,4 GHz.
   - **20MHz**: Sélectionnez cette bande passante si vous rencontrez des problèmes avec votre connexion Wi-Fi.
8. Si l'option **20/40/80MHz**, **20/40MHz**, **40MHz** ou **80MHz** est sélectionnée, vous pouvez définir un canal adjacent inférieur ou supérieur dans le champ **Extension Channel** (Canal d'extension)
9. Dans le champ **Authentication Method** (Méthode d'authentification), sélectionnez l'une des méthodes

d'authentification disponibles :

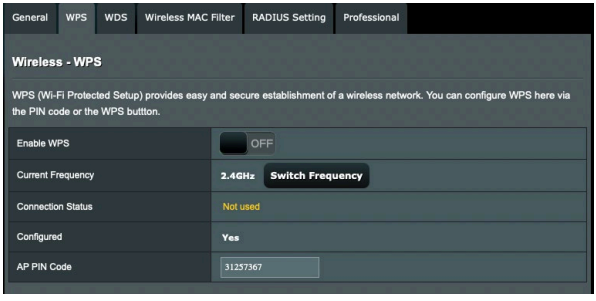
- **Open System (Système ouvert)** : Cette option n'offre aucune forme de sécurité.
- **WPA2-Personal** / **WPA Auto-Personal** : Cette option offre une sécurité plus élevée. Ces méthodes de chiffrement se basent sur les protocoles TKIP et/ou AES et doivent être combinées à un mot de passe. Si vous sélectionnez cette option, vous devez saisir la clé WPA pré-partagée (clé réseau).
- **WPA2 Enterprise** / **WPA Auto-Enterprise** : Cette option offre une sécurité très élevée. Elle comprend un serveur EAP intégré ou un serveur d'authentification dorsal RADIUS externe.

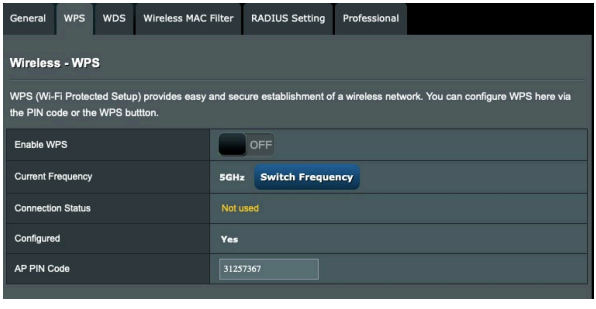
10. Une fois terminé, cliquez sur **Apply** (Appliquer).

4.1.2 WPS

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

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





Pour activer et utiliser la fonctionnalité WPS sur votre réseau Wi-Fi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **WPS**.
2. Déplacez l'interrupteur sur **ON** (OUI) pour activer la fonctionnalité WPS.
3. La norme WPS utilise les bandes de fréquence 2,4 GHz et 5 GHz séparément.
4. Vous pouvez utiliser l'une des méthodes WPS suivantes pour l'association Wi-Fi :
   - **Mode PBC (Pression de bouton)**:
     - Méthode 1 : Appuyez sur le bouton WPS situé à l'arrière du routeur, puis appuyez sur le bouton WPS de votre appareil Wi-Fi pendant environ trois (3) minutes.
     - Méthode 2 : Cochez l'option <Push button> (Pression de bouton) du champ **WPS Method** (Méthode WPS), cliquez sur **Start** (Démarrer), puis appuyez sur le bouton WPS de votre appareil Wi-Fi pendant environ trois (3) minutes.
   - **Mode code PIN**:
     - À partir du client Wi-Fi : Appuyez sur le bouton WPS du routeur puis entrez le code PIN apparaissant dans le champ **AP PIN Code** (Code PIN) dans l'interface du client Wi-Fi.
     - À partir du routeur : Appuyez sur le bouton WPS du client sans fil, puis entrez le code PIN du client dans le champ **WPS Method** (Méthode WPS) > **Client PIN Code** (Code PIN du client) de l'interface de configuration du routeur. Vérifiez que le code PIN est correct puis cliquez sur **Start** (Démarrer) pour établir la connexion Wi-Fi entre le client et le routeur.

REMARQUES :

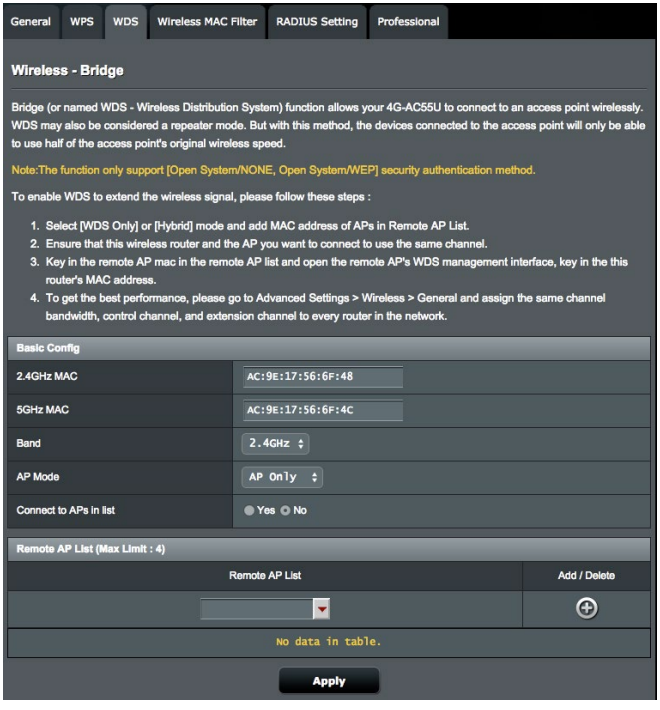
- La norme WPS est compatible avec les méthodes d'authentification à système ouvert et WPA2-Personal. Les chiffrements à clés partagées, WPA-Personal, WPA-Enterprise, WPA2-Enterprise et RADIUS ne sont pas pris en charge.
- Inspectez votre périphérique Wi-Fi ou consultez son mode d'emploi pour localiser l'emplacement du bouton WPS.
- Le routeur Wi-Fi recherchera automatiquement la présence d'appareils WPS à proximité. Si aucun appareil WPS n'est détecté, le routeur basculera en mode veille.
- Le voyant lumineux WPS clignote rapidement pendant trois minutes jusqu'à ce que la connexion WPS soit établie.

4.1.3 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 Wi-Fi, empêchant d'autres périphériques Wi-Fi ou stations d'établir une connexion au routeur Wi-Fi ASUS. Dans ce scénario d'utilisation, le routeur ASUS peut faire office de répéteur Wi-Fi communiquant avec un autre point d'accès et d'autres clients.

Pour configurer un pont Wi-Fi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **WDS** (Pontage).



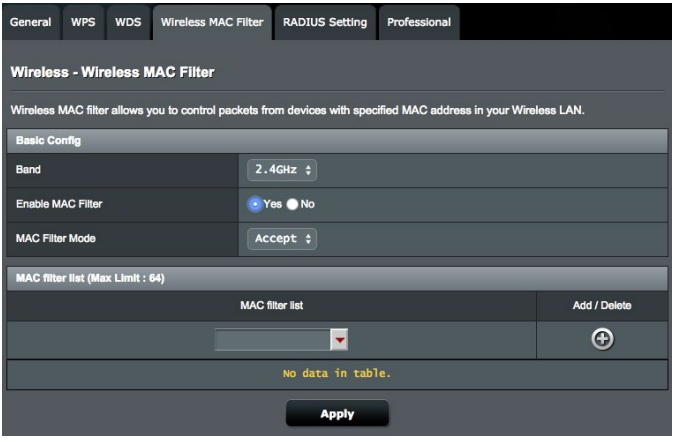
2. Sélectionnez une bande de fréquence Wi-Fi.
3. Dans le champ **AP Mode** (Mode point d'accès), sélectionnez l'une des options suivantes :
   - **AP Only (Point d'accès uniquement)**: Désactive la fonction WDS (Pontage Wi-Fi).
   - **WDS Only (WDS uniquement)**: Active le pontage Wi-Fi mais bloque la connexion d'autres périphériques Wi-Fi/clients au routeur.
   - **HYBRID (Hybride)**: Active le pontage Wi-Fi et autorise la connexion d'autres périphériques Wi-Fi/clients au routeur.
4. Dans le champ **Connect to APs in list** (Se connecter aux points d'accès de la liste), cliquez sur **Yes** (Oui) si vous souhaitez établir une connexion à un point d'accès distant.
5. Dans **Remote AP List** (Liste des points d'accès distants), entrez une adresse MAC, puis cliquez sur le bouton **Add** (Ajouter) pour ajouter l'adresse à la liste des points d'accès disponibles
6. Cliquez sur **Apply** (Appliquer).

REMARQUES :

- En mode hybride, les périphériques Wi-Fi connectés au routeur Wi-Fi ASUS ne bénéficieront que de la moitié du débit Wi-Fi du point d'accès.
- Tous les points d'accès ajoutés à la liste doivent posséder le même canal d'opération que celui utilisé par le routeur Wi-Fi ASUS. Vous pouvez modifier le **Control Channel** (Canal de contrôle) dans **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > **General** (Général).

4.1.4 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 Wi-Fi.



Pour configurer le filtrage d'adresses MAC :

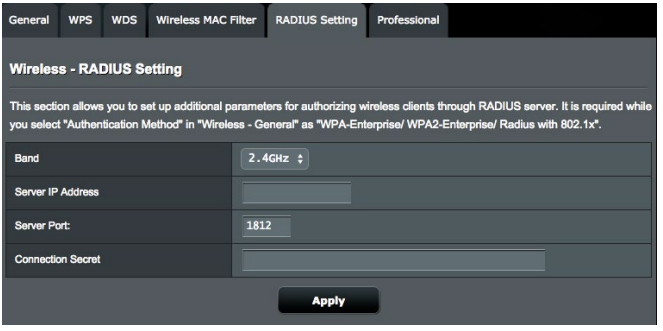
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **Wireless MAC Filter** (Filtrage d'adresses MAC).
2. Cochez **Yes** (Oui) dans le champ **Enable MAC Filter** (Activer le filtrage d'adresses MAC).
3. Dans le menu déroulant **MAC 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 Wi-Fi.
- Sélectionnez **Reject** (Rejeter) pour ne pas autoriser les appareils faisant partie de la liste de filtrage d'adresses MAC à accéder au réseau Wi-Fi.

4. Entrez une adresse MAC, puis cliquez sur le bouton **Add** (Ajouter) pour l'ajouter à la liste.
5. Cliquez sur **Apply** (Appliquer).

4.1.5 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-Enterprise, WPA2-Enterprise ou Radius with 802.1x.



Pour configurer le service RADIUS :

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

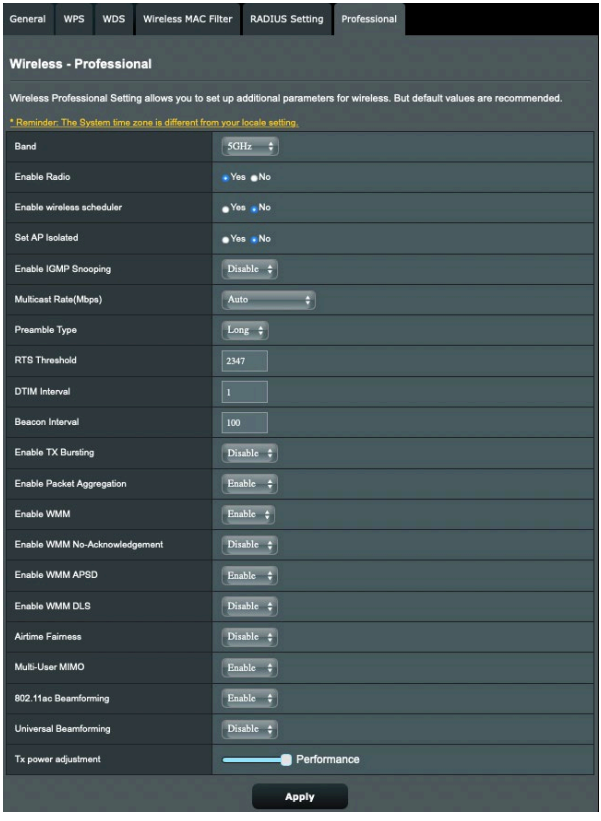
REMARQUE : Consultez la section **4.1.1 Général** pour en savoir plus sur les différents modes d'authentification de votre routeur Wi-Fi.

2. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > 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).

4.1.6 Professional (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 Wi-Fi, ou **No** (Non) pour le désactiver. Cochez **No** (Non) pour désactiver le réseau sans fil.

- **Enable Wireless Scheduler (Activer le planificateur Wi-Fi):** Sélectionnez **Yes** (Oui) pour établir une programmation horaire de la disponibilité de la connexion Wi-Fi. Sélectionnez **No** (Non) pour ne pas utiliser de programmation horaire.
- **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 Wi-Fi.
- **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 Wi-Fi.
- **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 Wi-Fi 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 Wi-Fi.
- **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)**: Lorsque votre environnement Wi-Fi a fourni plusieurs PA (points d'accès) ou répéteurs Wi-Fi pour couvrir toutes les zones mortes Wi-Fi. Lorsqu'un client qui s'est connecté sur PA1 se déplace depuis un endroit ayant un bon signal vers un endroit ayant un signal faible, mais qu'un autre signal provient de PA2. Pour empêcher le client d'être bloqué sur le PA1, vous pouvez activer l'assistant itinérance et définir une valeur RSSI minimale en tant que seuil. Si la qualité de la connexion est inférieure au seuil, PA1 déconnecte le client Wi-Fi afin qu'il puisse réévaluer l'environnement Wi-Fi pour sélectionner un PA avec la meilleure qualité de signal, tel qu'AP2.
- **Enable IGMP Snooping (Activer le filtrage IGMP)**: Lorsque le filtrage IGMP est activé, le trafic de multidiffusion est uniquement transmis aux clients Wi-Fi qui sont membres d'un groupe de multidiffusion spécifique.
- **Multicast Rate (Mbps) (Débit de multidiffusion)**: 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 Wi-Fi est composé de périphériques Wi-Fi plus anciens ou hérités. Sélectionnez **Long** si votre réseau sans fil est composé de périphériques Wi-Fi plus anciens ou hérités.
- **AMPDU RTS :** En 802.11n ou 802.11ac utilisant une méthode, AMPDU, pour agréger des paquets courts en un paquet plus long pour la même adresse MAC. Envoie un signal de contrôle RTS (Request to Send) lorsqu'un appareil sans fil est prêt pour la transmission de données. Après avoir activé AMPDU RTS, chaque trame AMPDU est envoyée avec le processus RTS.
- **RTS Threshold (Palier RTS)**: Spécifiez une valeur de palier RTS basse pour améliorer les communications Wi-Fi 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 Wi-Fi 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 Wi-Fi et les appareils 802.11g.
- **Enable WMM APSD (WMM APSD)**: WMM APSD (Automatic Power Save Delivery) est l'amélioration du mode d'économie de puissance hérité. Ajoutez WMM APSD et le point d'accès Wi-Fi gérera l'utilisation de la radio afin d'accroître l'autonomie de la batterie pour les clients sans fil alimentés par batterie, tels que les smartphones et les ordinateurs portables. APSD devient automatiquement un plus long intervalle de balise lorsque le trafic ne nécessite pas un intervalle d'échange de paquet court.

4.2 Réseau local (LAN)

4.2.1 IP réseau local (LAN)

L'onglet dédié à l'adresse IP du réseau local fait référence à l'adresse IP du routeur Wi-Fi.

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

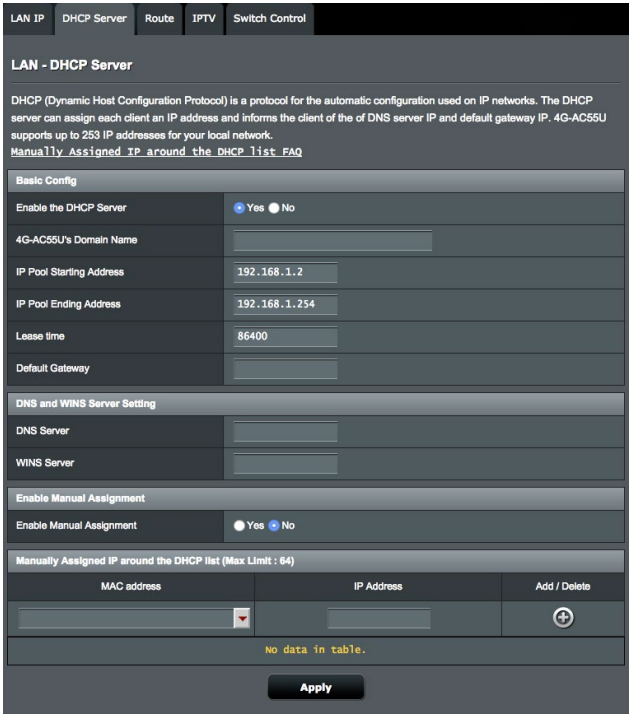


Pour modifier l'adresse IP du réseau local :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **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).

4.2.2 Serveur DHCP

Votre routeur Wi-Fi 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) > onglet **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 Wi-Fi.
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.

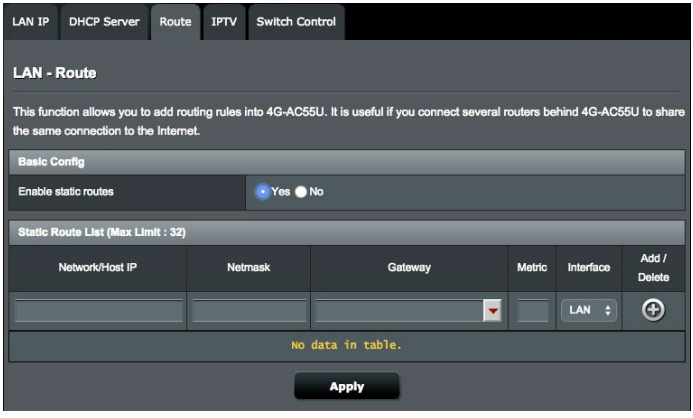
---

7. Dans la zone **DNS and WINS Server Settings** (Configuration des serveurs DNS et WINS), entrez, si nécessaire, les adresses dédiées au serveur DNS et WINS.
8. Vous pouvez également affecter manuellement des adresses IP aux clients de votre réseau Wi-Fi. 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.

4.2.3 Routage

Si votre réseau est composé de plus d'un routeur Wi-Fi, 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.

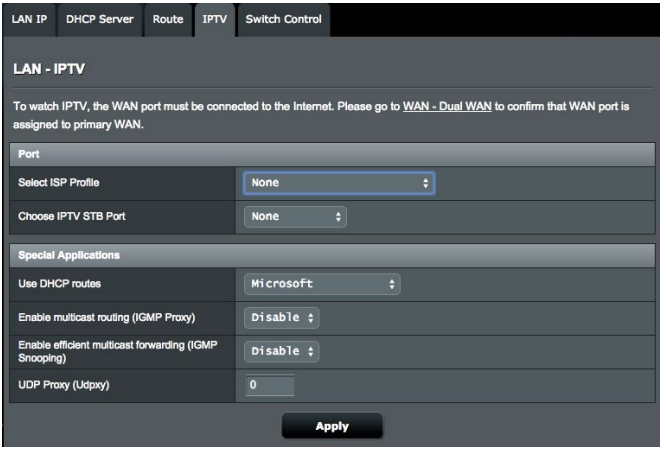


Pour configurer le tableau de routage :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **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).

4.2.4 Télévision sur IP

Le routeur Wi-Fi 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.



4.2.5 Switch Control (Contrôle de commutation)

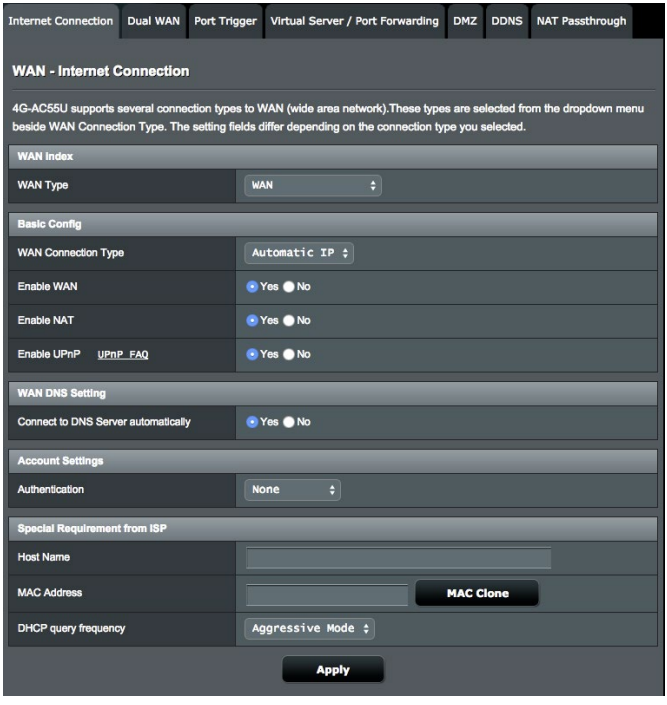
Le contrôle de commutation permet de configurer l'accélération NAT et les trames Jumbo de sorte à améliorer les performances du réseau. Il est recommandé de ne pas modifier les paramètres par défaut, sauf si vous possédez les connaissances suffisantes pour le faire.



4.3 Réseau étendu (WAN)

4.3.1 Connexion internet

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



4.3.1.1 Réseau étendu (WAN)

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) > onglet **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.

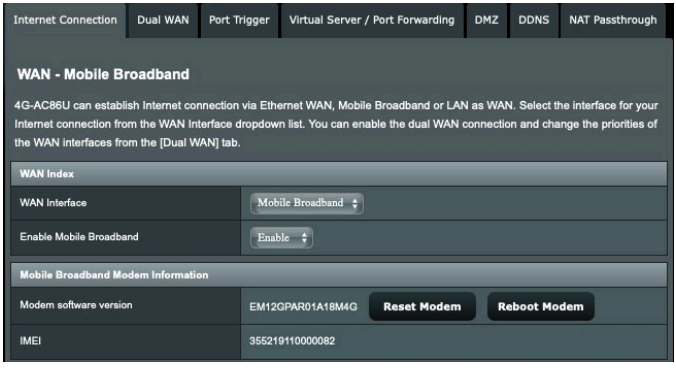
- **MAC Address (Adresse MAC)**: Une adresse MAC (Media Access Control) est un identifiant unique attribué aux appareils dotés d'une connectivité Wi-Fi. Certains FAI surveillent l'adresse MAC des appareils se connectant à leur service et peuvent rejeter toute tentative d'un appareil non enregistré d'établir 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 Wi-Fi 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.

4.3.1.2 Réseau cellulaire mobile

Le routeur intègre un module 3G/4G permettant d'utiliser une connexion cellulaire pour accéder à Internet.

Pour configurer les paramètres de connexion au réseau cellulaire :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Internet Connection** (Connexion Internet), sélectionnez l'option **Mobile Broadband** (Réseau mobile haut débit) du champ **WAN Interface** (Interface WAN).

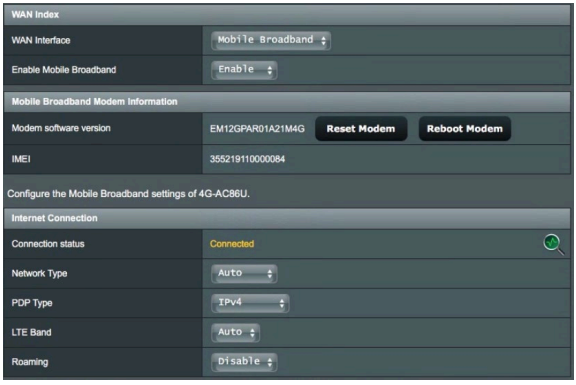


2. Dans le champ **Enable Mobile Broadband** (Activer le réseau mobile haut débit), sélectionnez **Enable** (Activer).
3. Vérifiez que vous avez correctement inséré la carte SIM, et configurez les paramètres mobiles de votre routeur.
4. Réglez les options suivantes :
   - **Location (Emplacement)**: 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 Wi-Fi (optionnel))** (Contactez votre fournisseur d'accès 3G/4G pour plus de détails.
   - **Dial Number (Numéro)**: Le numéro d'accès de votre opérateur de téléphone portable 3G/4G
   - **PIN Code (Code PIN)**: Entrez le code PIN de votre carte SIM.

REMARQUE :

- Le code PIN par défaut peut varier en fonction de l'opérateur.
- Lorsque vous configurez pour la première fois ou redémarrez votre routeur, vous devez saisir le code PIN dans l'un des deux scénarios :
  - Votre fournisseur d'accès internet a activé la vérification du code PIN par défaut.
  - Vous avez activé manuellement la vérification du code PIN depuis l'interface de gestion de votre routeur ou de votre téléphone portable.
- Si la vérification du code PIN est activée, vous verrez l'icône d'état de verrouillage SIM dans la zone des icônes d'état.

   - **Username / Password (Nom d'utilisateur / Mot de passe)**: Entrez le nom d'utilisateur et le mot de passe fournis par votre opérateur de téléphonie mobile 3G/4G.
   - **Idle Time (Délai d'inactivité)**: Entrez le délai (en minutes) de basculement en mode veille du routeur lorsqu'aucune activité n'est détectée sur le réseau.



4. Configuration de connexion internet :
   1) Dans le champ **Network Type** (Type de réseau), sélectionnez votre réseau favori :
      - **Auto** (Par défaut): Sélectionnez **Auto** pour autoriser le routeur Wi-Fi à choisir automatiquement le canal approprié, 4G ou 3G.
      - **4G only (4G uniquement)**: Sélectionnez cette option pour connecter automatiquement le routeur sans fil à un réseau 4G uniquement.
      - **3G only (3G uniquement)**: Sélectionnez cette option pour connecter automatiquement le routeur sans fil à un réseau 3G uniquement.
   2) **PDP Type** (Type de PDP) : Le routeur Wi-Fi prend en charge les protocoles PDP suivants : PPP, IPv4, IPv6 et IPv6 to IPv4.
   3) **LTE Band** (Bande LTE) : Ce champ vous permet de sélectionner la bande LTE.
   4) **Roaming** (Itinérance) : Permet d'utiliser les connexions en itinérance lors de déplacements à l'étranger. Activez cette fonction pour vous permettre d'accéder au réseau local.
      - Cliquez sur **Scan** (Rechercher) pour afficher la liste des réseaux cellulaires disponibles.
      - Sélectionnez un réseau puis cliquez sur **Apply** (Appliquer) pour y établir une connexion.

REMARQUES:

- Le routeur LTE peut détecter votre opérateur de téléphonie mobile en fonction des informations IMSI stockées sur la carte SIM. Si le réseau mobile de votre opérateur est introuvable, établissez une connexion au réseau d'un autre opérateur.
- L'utilisation du service d'itinérance engendre des coûts d'appel additionnels. Contactez votre opérateur de téléphonie mobile pour en savoir plus sur le coût des appels depuis l'étranger.



5. Data usage limitation (Limitation des données)
   - **Data usage (Utilisation des données)**: Affiche le volume de données utilisées.
   - **Cycle Start Day (Date de début de cycle)**: Sélectionnez le jour où vous souhaitez que l'utilisation des données commence à s'accumuler. La valeur d'utilisation de données est réinitialisée à la fin de chaque cycle.
   - **Data usage limit (Limitation des données)**: Activez cette option pour définir une limite mensuelle des données internet (en Go) de la connexion cellulaire. Lorsque la valeur limite est atteinte, un message d'alerte apparaîtra lors de votre connexion à la page d'administration et l'accès Internet cellulaire sera bloqué.
   - **Data Usage Alert (Alerte d'utilisation des données)**: Définissez l'utilisation de bande passante internet maximale à laquelle une alerte est envoyée. Dès que votre utilisation d'Internet atteint cette limite, l'accès à Internet est bloqué.
   - **Envoyer une notification par SMS**: Activez cette fonction pour recevoir une notification par SMS une fois que la limite maximale d'utilisation d'Internet est atteinte.





6. Configuration APN
   1) **Auto** (Par défaut) : Par défaut, le système sélectionne automatiquement le nom du point d'accès (Auto APN).
   2) **Manuel**: Si la connexion d'accès à distance automatique échoue, sélectionnez **Manual** (Manuel) pour configurer manuellement le nom du point d'accès.
      A. **Location (Emplacement)**: Sélectionnez l'emplacement de votre fournisseur de service 3G/4G.
      B. **ISP (FAI)**: Sélectionnez votre FAI (Fournisseur d'accès internet).
      C. **APN (Access Point Name) service (optional) (Service d'accès internet Wi-Fi (optionnel))**: Contactez votre fournisseur d'accès 3G/4G pour plus de détails.
      J. **Appeler**: Le numéro d'accès de votre opérateur de téléphone portable 3G/4G
      E. **Nom d'utilisateur** / **Password** (Mot de passe) : Saisissez le nom d'utilisateur et le mot de passe fournis par votre opérateur de téléphonie mobile 3G/4G.

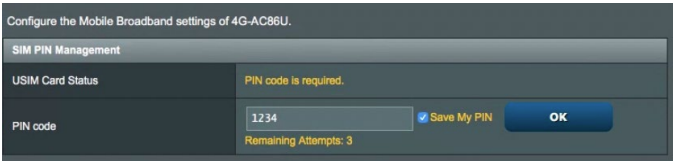
7. Configuration du code PIN

PIN Code (Code PIN): Entrez le code PIN de votre carte SIM.

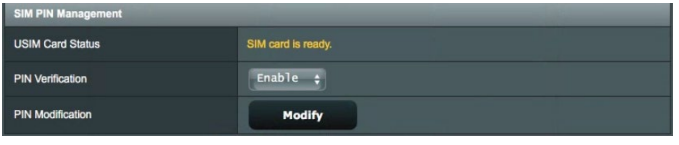
- Le code PIN par défaut peut varier en fonction de l'opérateur. Si votre FAI a désactivé la vérification du code PIN par défaut, vous pouvez ignorer ce paramètre.

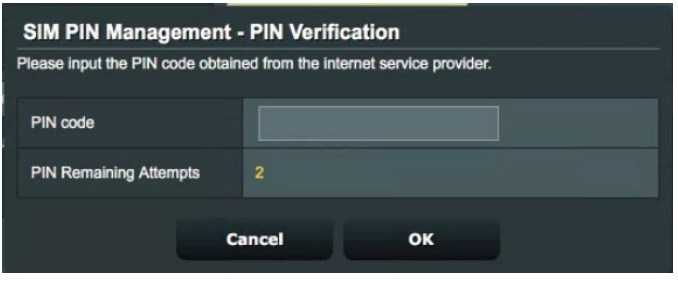


- Si votre FAI a activé la vérification du code PIN par défaut, vous verrez l'icône d'état de verrouillage SIM dans la zone des icônes d'état et vous devrez saisir le code PIN.



- Vous pouvez activer manuellement la vérification du code PIN à partir de l'interface de gestion de votre routeur ou de votre téléphone mobile. Vous devez également saisir le code PIN.





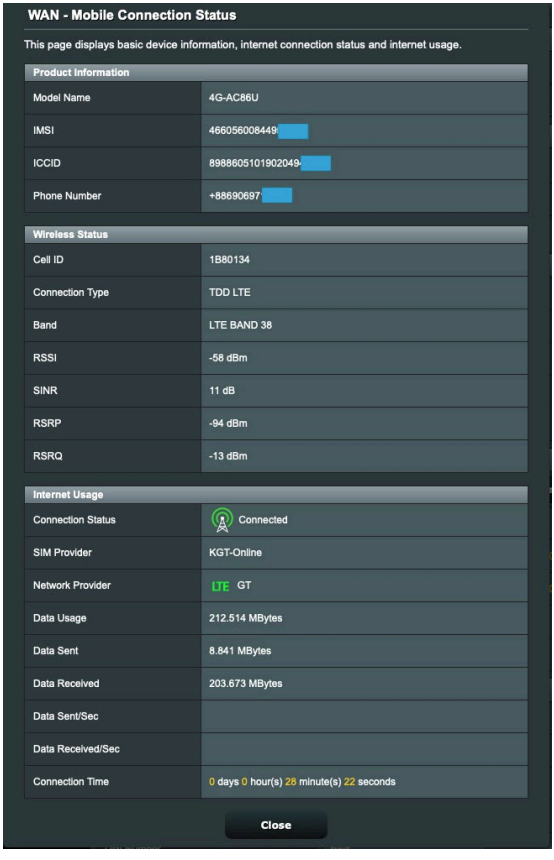
État de la connexion cellulaire à haut débit

Pour obtenir les informations de connexion cellulaire à haut débit :

1. Cliquez sur pour plus de détails.

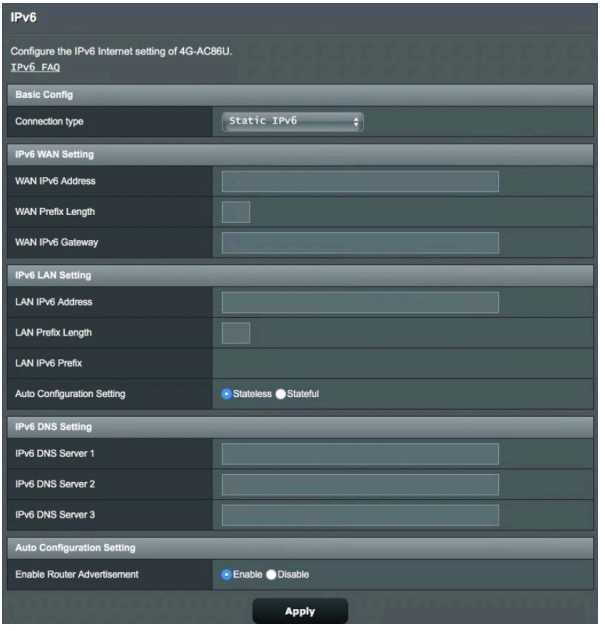


2. Le menu **Mobile Connection Status** (État de la connexion cellulaire) offre des informations détaillées sur l'état de la connexion cellulaire à haut débit.



4.3.2 Protocole IPv6 (Paramètres internet)

Ce routeur Wi-Fi 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 :

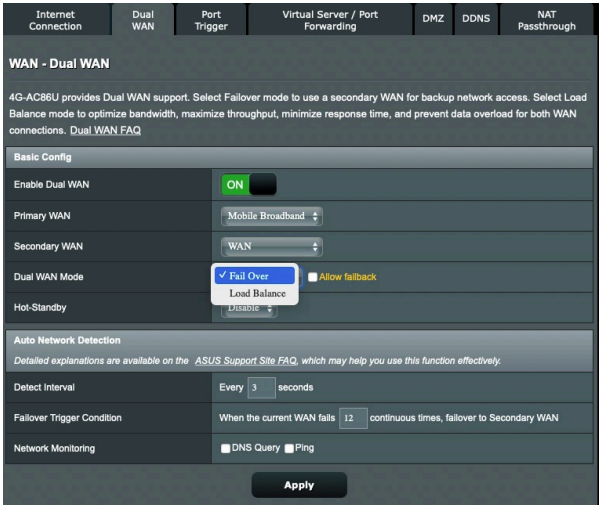
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **IPv6**.
2. Dans le menu **Connection Type** (Type de connexion), sélectionnez le type de connexion. Les options de configuration apparaissant ensuite peuvent varier selon le type de connexion choisi.
3. Entrez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

4.3.3 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 :

- **Fail Over (Basculement) :** Sélectionnez ce mode pour utiliser le réseau étendu (WAN) secondaire comme connexion réseau de secours.
- **Load Balance Mode (Mode équilibrage de charge) :** Sélectionnez ce mode afin de permettre l'utilisation simultanée de deux connexions WAN, pour une bande passante et une fiabilité améliorées.
- **Allow failback (Autoriser la restauration automatique) :** Sélectionnez ce mode pour autoriser le routeur à restaurer automatiquement la connexion au réseau étendu (WAN) primaire lorsque celle-ci redevient disponible.



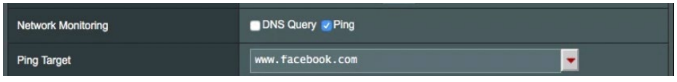
- **Intervalle de détection**: Définit l'intervalle de temps (en secondes) entre deux paquets Ping.
- **Condition de déclenchement du basculement**: Définit la durée après laquelle le système déclenche l'action de basculement ou de restauration, après avoir atteint la limite du compteur de requêtes ping et n'avoir obtenu aucune réponse de l'adresse IP cible.

- **Surveillance réseau**

  1) **Requête DNS**: Sélectionnez cette option si vous souhaitez résoudre périodiquement le FQDN cible (nom de domaine pleinement qualifié).



  2) **Ping**: Sélectionnez cette option si vous souhaitez envoyer périodiquement une requête ping au domaine ou à l'adresse IP cible.

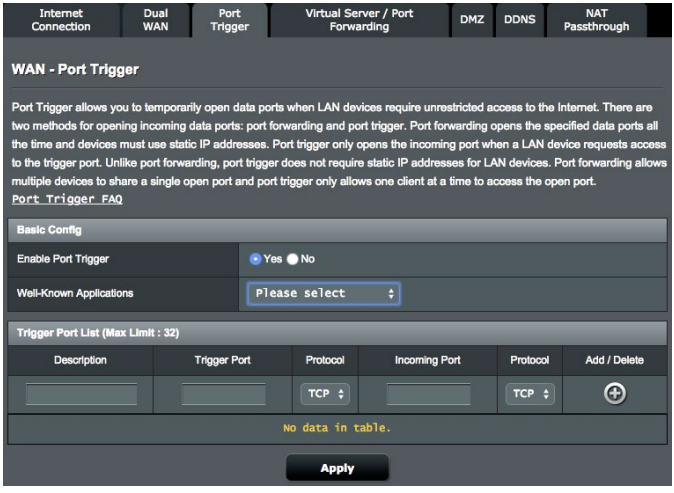


Si un problème de connexion internet se produit en raison d'un problème de bail DHCP (tel que l'expiration de l'adresse IP), vous pouvez activer la requête DNS ou le ping pour résoudre le problème.

4.3.4 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) > onglet **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 des ports de déclenchement.

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

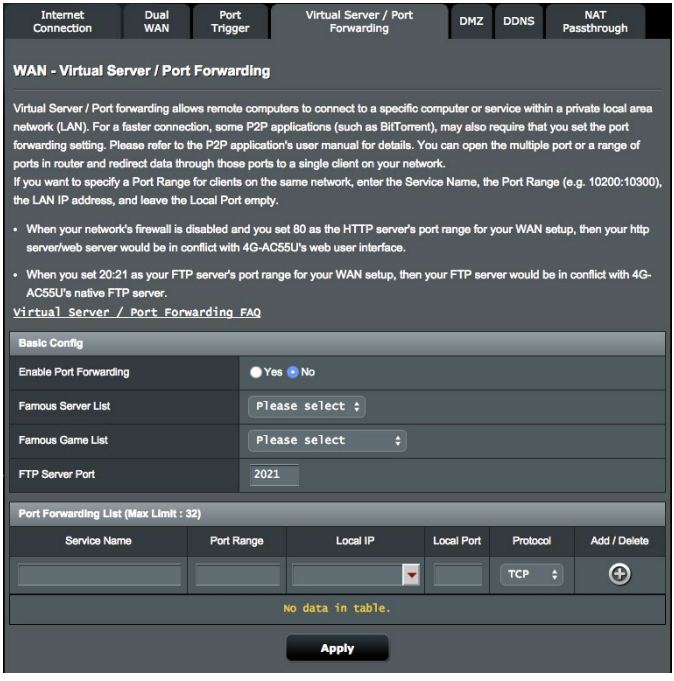
REMARQUES :

- 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.

4.3.5 Serveur virtuel et redirection de port

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

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



Pour utiliser la redirection de port :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Virtual Server / Port Forwarding** (Redirection de port).
2. Dans le champ **Enable Port Forwarding** (Activer la redirection de port), cochez **Yes** (Oui).

3. Dans le champ **Famous Server List** (Liste de serveurs), spécifiez le type de service auquel vous souhaitez accéder.
4. 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.
5. 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 **4.2 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).

6. Cliquez sur pour ajouter les informations à la liste. Cliquez sur pour supprimer une entrée de la liste.
7. 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 :

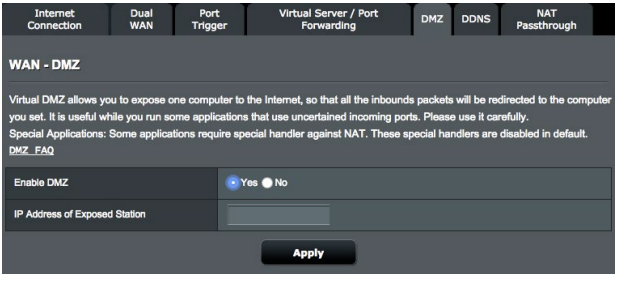
- Le déclenchement de port peut être utilisé sans spécifier d'adresse IP locale. Contrairement à la redirection de port, nécessitant une adresse IP statique, le déclenchement de port autorise la redirection dynamique de port par le biais du routeur. Des plages de ports pré-déterminées sont configurées 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.

4.3.6 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 :

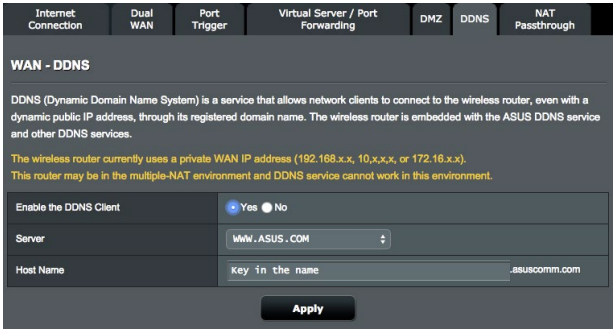
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **DMZ** (Zone démilitarisée).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
   - **IP address of Exposed Station (Adresse 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).

4.3.7 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) > onglet **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).
   - **Serveur** et **Host Name** (Nom d'hôte) : sélectionnez ASUS DDNS ou un autre service DDNS. 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 email, 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 :

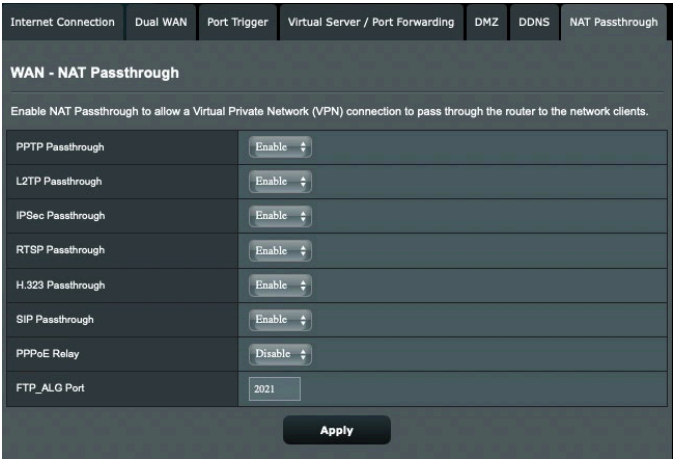
- Le routeur Wi-Fi utilise une adresse IP du réseau étendu (WAN) privée (de type 192.168.x.x, 10.x.x.x ou 172.16.x.x).
- Le routeur fait partie d'un réseau utilisant plusieurs tableaux NAT.

4.3.8 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.

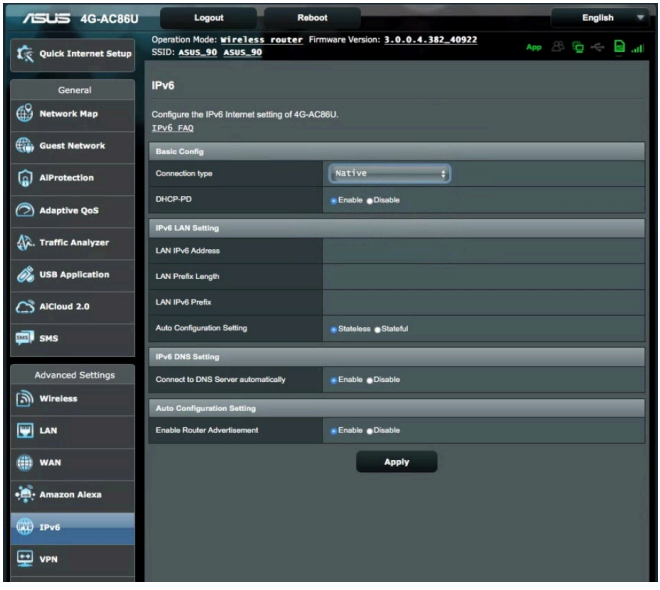
Pour activer ou désactiver la fonction NAT Passthrough :

1. Allez dans **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **NAT Passthrough**.
2. Sélectionnez **Enable** (Activer) ou **Disable** (Désactiver).
3. Une fois terminé, cliquez sur **Apply** (Appliquer).



4.4 IPv6 (Protocole IPv6)

Ce routeur Wi-Fi 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 :

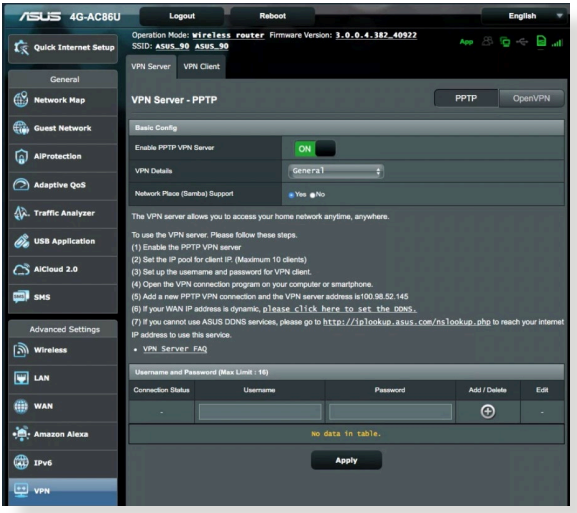
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **IPv6**.
2. Dans le menu **Connection Type** (Type de connexion), sélectionnez le type de connexion. Les options de configuration apparaissant ensuite peuvent varier selon le type de connexion choisi.
3. Entrez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

4.5 Serveur VPN

La connexion à un serveur 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 **Advanced Settings** (Paramètres avancés) > **VPN Server** (Serveur VPN).
2. Dans le champ **Enable PPTP VPN Server** (Activer le serveur VPN PPTP), déplacez le curseur sur **ON** (OUI) pour activer le serveur VPN PPTP.
3. 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.
4. Dans le champ **Network Place (Samba) Support** (Prise en charge de serveur Samba), cochez **Yes** (Oui).
5. Entrez le nom d'utilisateur et le mot de passe d'accès au serveur VPN. Cliquez sur le bouton .
6. Cliquez sur **Apply** (Appliquer).

4.6 Pare-feu

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

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

4.6.1 Paramètres de base

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) > onglet **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).

4.6.2 Filtrage d'URL

Le routeur Wi-Fi 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) > onglet **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).

4.6.3 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) > onglet **Keyword Filter** (Filtrage de mots clés).
2. Dans le champ **Enable Keyword Filter** (Activer le filtrage de mots clés), cochez **Enabled** (Activer).
3. Entrez un mot ou une phrase, puis cliquez sur le bouton **Add** (Ajouter).
4. Cliquez sur **Apply** (Appliquer).

REMARQUES :

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

4.6.4 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) > onglet **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. **L'option Black List** (Liste noire) bloque les services réseau spécifiés 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).

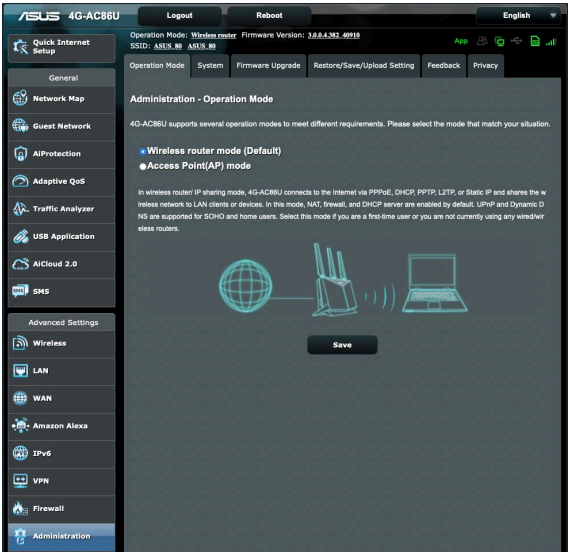
4.6.5 Pare-feu IPv6

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.

4.7 Administration

4.7.1 Mode de fonctionnement

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



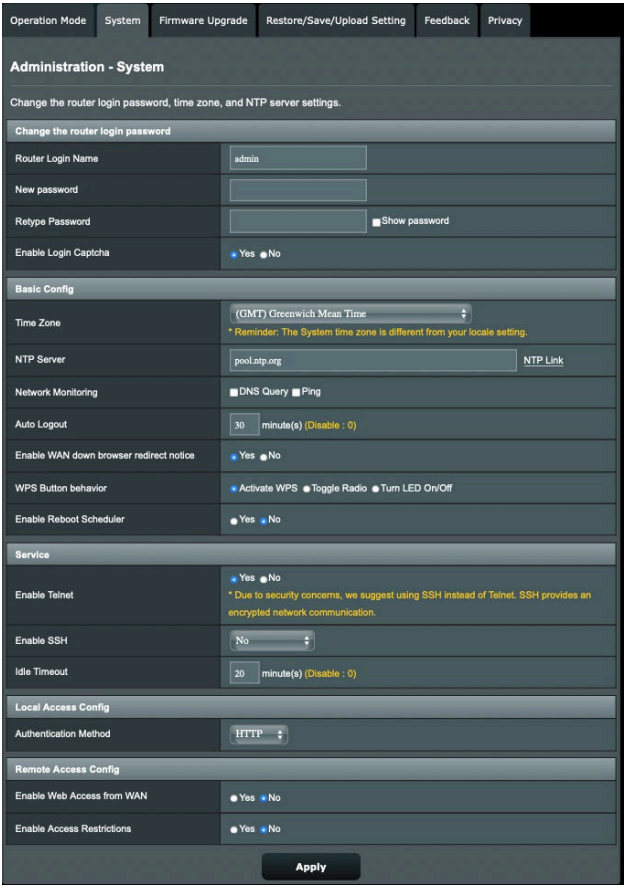
Pour définir le mode de fonctionnement du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **Operation Mode** (Mode de fonctionnement).
2. Sélectionnez l'un des modes disponibles :
   - **Wireless router mode (default) (Mode routeur Wi-Fi (par défaut))**: Ce mode permet d'établir une connexion à Internet et d'en ouvrir l'accès aux clients disponibles sur le réseau local du routeur.
   - **Access Point mode (Mode point d'accès)**: Ce mode permet de créer un nouveau réseau Wi-Fi à partir d'un réseau existant.
3. Cliquez sur **Apply** (Appliquer).

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

4.7.2 System (Système)

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

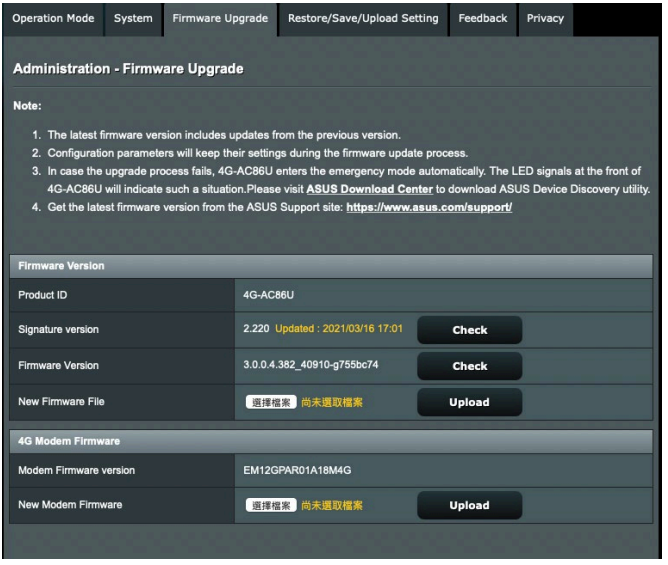


Pour configurer les paramètres système du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **System** (Système).
2. Configurez les paramètres listés ci-dessous :
   - **Change the 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 Wi-Fi.
   - **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.
   - **Auto Logout (Déconnexion automatique)**: Détermine le délai de déconnexion de la page d'administration. Entrez la valeur 0 pour désactiver cette option.
   - **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.
   - **Enable Access Restrictions (Activer les restrictions d'accès):** Sélectionnez **Yes** (Oui) pour définir une liste blanche qui permet à l'administrateur de limiter et de contrôler l'accès uniquement pour une adresse IP de confiance.
     a) . **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.
     b) . **Specified IP Address (Adresses IP)**: Entrez les adresses IP du réseau étendu (WAN) des clients autorisés à accéder à l'interface de gestion du routeur depuis Internet. La liste des clients permet d'ajouter un maximum de 4 adresses IP.
3. Cliquez sur **Apply** (Appliquer).

4.7.3 Mise à jour du firmware

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



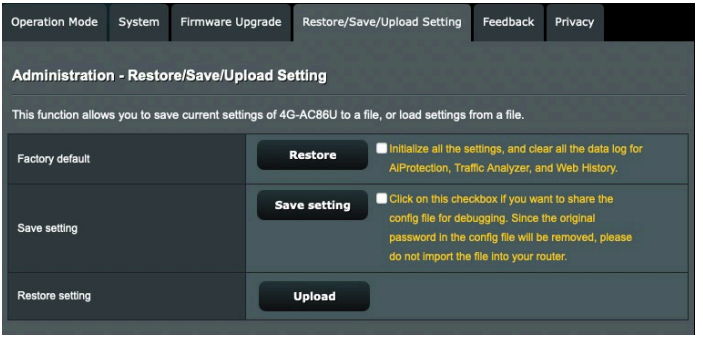
Pour mettre à niveau le firmware du routeur ou du modem 4G :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **Firmware Upgrade** (Mise à jour du firmware).
2. Dans le champ **New Firmware File** (Nouveau fichier de firmware) ou **New Modem Firmware** (Nouveau firmware du modem), 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 **5.2 Firmware Restoration (Restauration du firmware)**.

4.7.4 Restauration/Sauvegarde/Transfert de paramètres



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

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

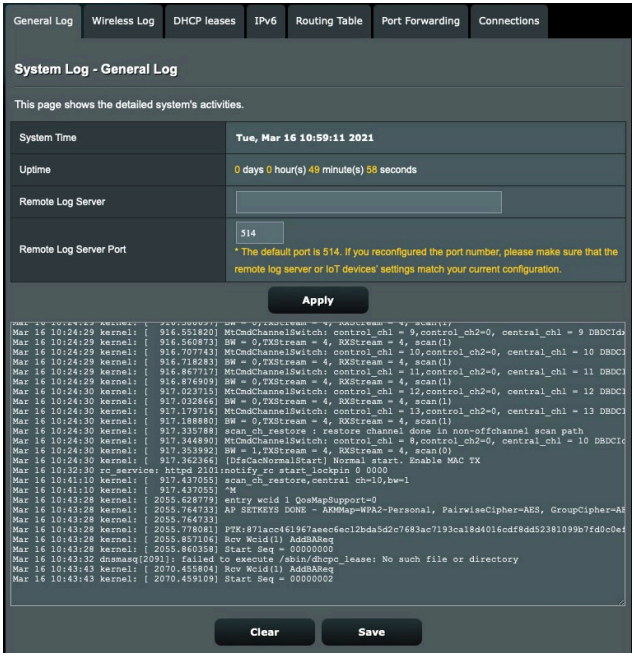
4.8 Journal système

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 Wi-Fi)
   - DHCP Leases (Baux DHCP)
   - IPv6 (Infos des réseaux locaux et étendus)
   - Routing Table (Tableau de routage)
   - Port Forwarding (Redirection de port)
   - Connexions



4.9 Liste des fonctions prises en charge

Le routeur Wi-Fi prend en charge les connexions filaires et cellulaires au réseau étendu (WAN) en modes basculement et restauration. Le réseau cellulaire mobile est utilisé pour l'accès internet et comme connexion de secours. Les réseaux locaux (LAN), étendus (WAN) et VPN ainsi que le pare-feu prennent en charge différentes fonctions telles que listées dans le tableau ci-dessous. Consultez le tableau de comparaison ci-dessous.

	Réseau étendu (WAN) filaire	Réseau local (LAN) comme réseau étendu (WAN)	Réseau cellulaire à haut débit
		Réseau local (LAN)	
Télévision sur IP	V	N/D	N/D
Contrôle de commutation >> Accélération NAT (IPv4 uniquement)	V	N/D	N/D
Contrôle de commutation >> Frame Jumbo	V	N/D	N/D
		Réseau étendu (WAN)	
IPv6 (Protocole IPv6)	V	V	V (1)
Déclenchement de port	V	V	V (2)
Serveur virtuel et redirection de port	V	V	V (2)
Zone démilitarisée	V	V	V (2)
Service DDNS	V	V	V (2)
NAT Passthrough	V	V	V (2)
		Gestionnaire de trafic	
QoS	V	V	V
		Pare-feu	
Paramètres de base	V	V	V
Filtrage d'URL	V	V	V
Filtrage de mots-clés	V	V	V
Filtrage de services réseau	V	V	V
Pare-feu IPv6	V	V	N/D
		Administration	
Système >> Enable Web Access from WAN (Autoriser l'accès au routeur depuis Internet)	V	V	V (2)

		Applications	
AiCloud Accès depuis Internet	V	V	V (2)
Serveur VPN	V	V	V (2)
Serveur FTP	V	V	V (2)

REMARQUES :

V (1) : La connexion internet via un réseau cellulaire à haut débit possède un menu de configuration distinct

V (2) : De manière générale, le fournisseur de service internet assigne une adresse IP privée au réseau cellulaire à haut débit et pouvant causer l'échec du service au réseau étendu.

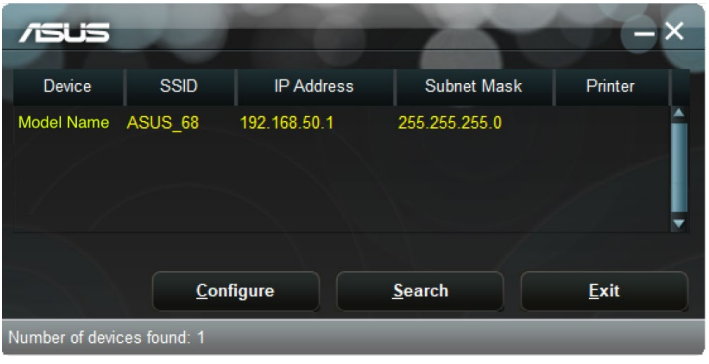
5 Utilitaires

REMARQUE : Téléchargez et installez les utilitaires pour votre routeur sur le site officiel ASUS:
https://www.asus.com/fr/support/Download-Center/

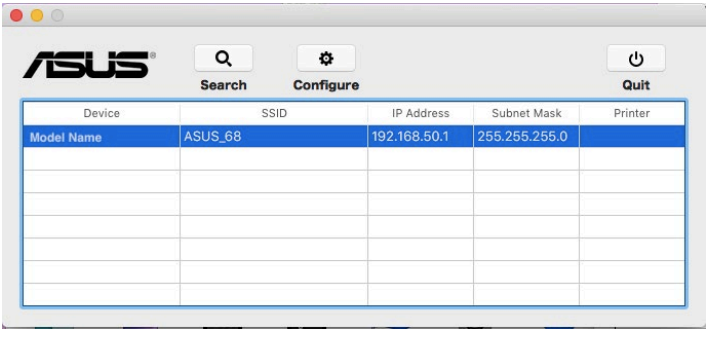
5.1 Device Discovery (Détection d'appareils)

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

Windows:



Mac OS:

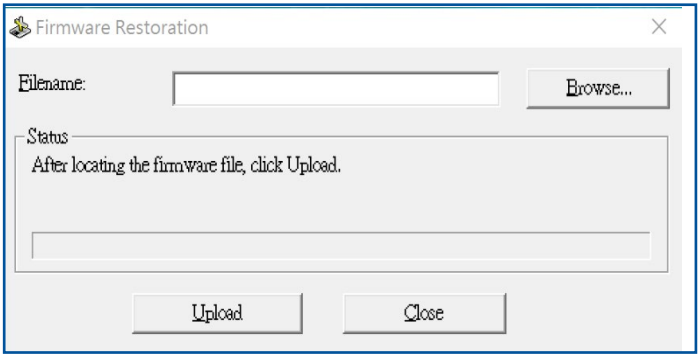


REMARQUE : Lorsque le routeur fonctionne en mode point d'accès, cet utilitaire est nécessaire pour obtenir l'adresse IP du routeur.

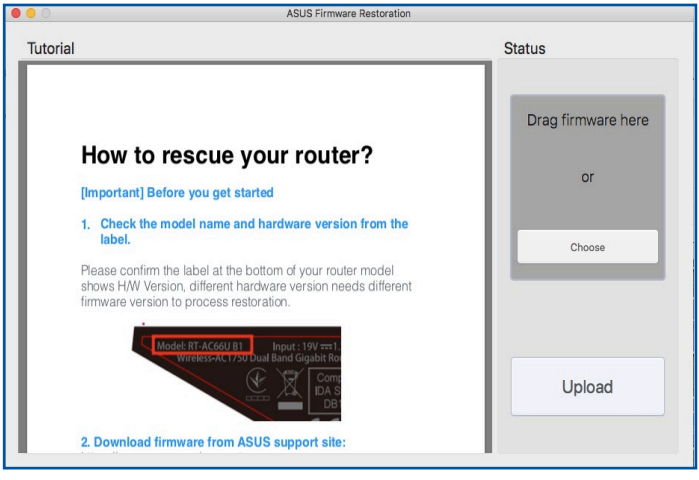
5.2 Firmware Restoration (Restauration du firmware)

Restauration du firmware est un utilitaire qui recherche automatiquement les routeurs Wi-Fi 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.

Windows:



Mac OS:



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

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

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

   Adresse IP: 192.168.1.x

   Masque de sous-réseau: 255.255.255.0
4. Depuis le Bureau de votre ordinateur, cliquez sur **Start** (Démarrer) > **All Programs** (Tous les programmes) > **ASUS Utility** (Utilitaire ASUS) > **Wireless Router** (Routeur Wi-Fi) > **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 Wi-Fi ASUS fonctionnant normalement. Les mises à niveau du firmware doivent être effectuées via l'interface de gestion du routeur. Consultez le **Chapitre 4 : Configurer les paramètres avancés** pour plus de détails.

5.3 Configurer un serveur d'impression

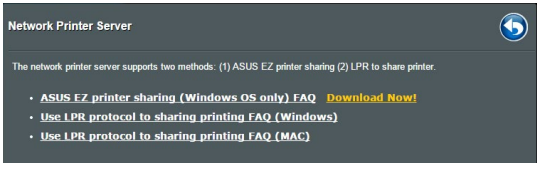
5.3.1 Utilitaire ASUS EZ Printer Sharing

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 Wi-Fi.



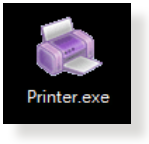
Pour partager une imprimante avec EZ Printer :

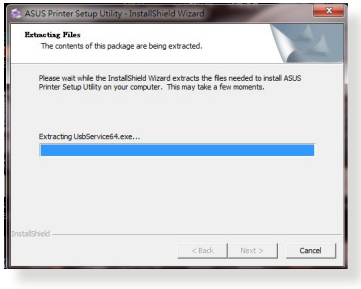
1. À partir du volet de navigation, cliquez sur **General** (Général) > **USB application** (Applications USB) > **Network Printer Server** (Serveur d'impression réseau).
2. Cliquez sur **Download Now!** (Télécharger maintenant!) pour télécharger l'utilitaire pour imprimante réseau .



REMARQUE : L'utilitaire d'imprimante réseau est pris en charge sur Windows® XP, Windows® Vista et Windows® 7 uniquement. 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.





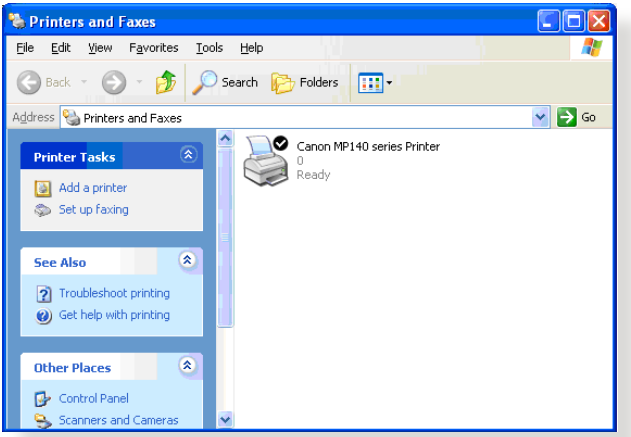
4. Suivez les instructions apparaissant à l'écran pour configurer le matériel, puis cliquez sur **Next** (Suivant).



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.



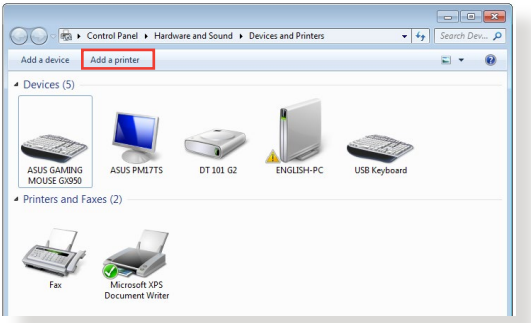
5.3.2 Utiliser le protocole LPR pour partager une imprimante

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

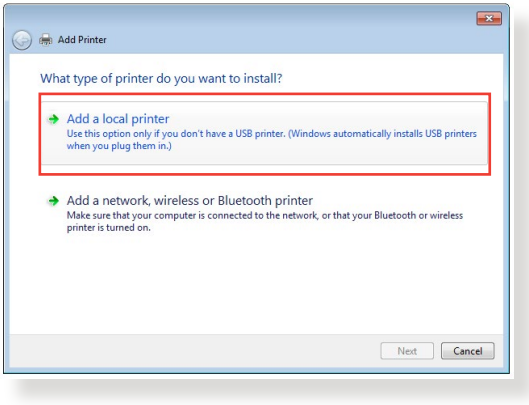
Partage d'imprimante LPR :

Pour partager une imprimante via le protocole LPR :

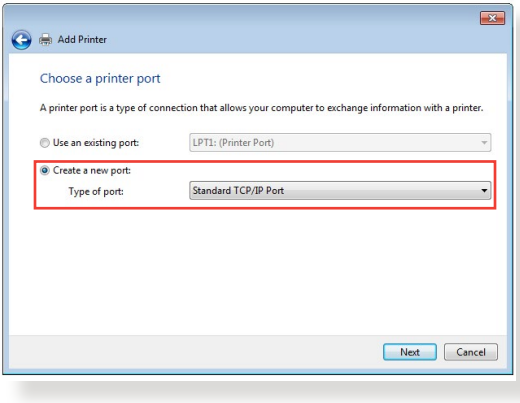
1. À partir du Bureau de Windows®, cliquez sur **Start** (Démarrer) > **Devices and Printers** (Périphériques et imprimantes) > **Add Printer Wizard** (Ajouter une imprimante).



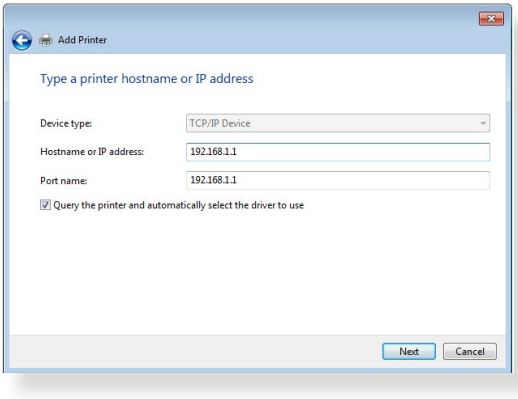
2. Sélectionnez **Add a local printer** (Ajouter une imprimante locale) et cliquez sur **Next** (Suivant).



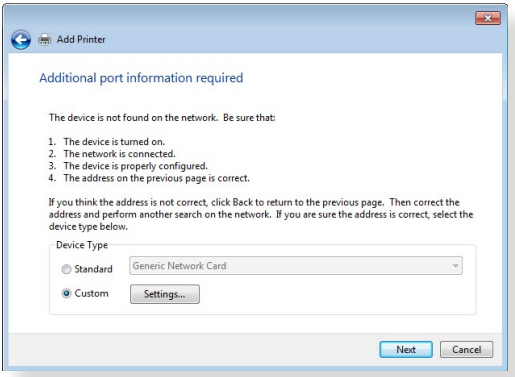
3. Sélectionnez **Create a new port** (Créer un nouveau port) puis sélectionnez l'option **Standard TCP/IP Port** (Port TCP/IP standard) du menu déroulant **Type of Port** (Type de port). Cliquez sur **New Port** (Nouveau port).



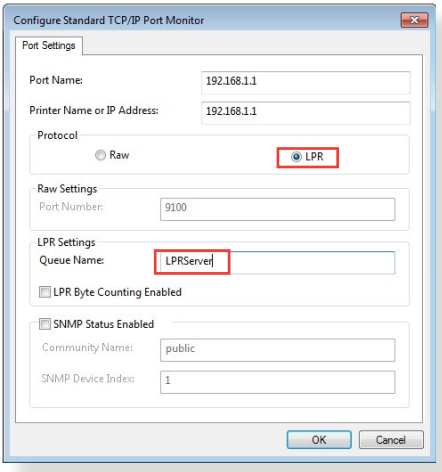
4. Dans le champ **Hostname or IP address** (Nom d'hôte ou adresse IP), entrez l'adresse IP du routeur Wi-Fi et cliquez sur **Next** (Suivant).



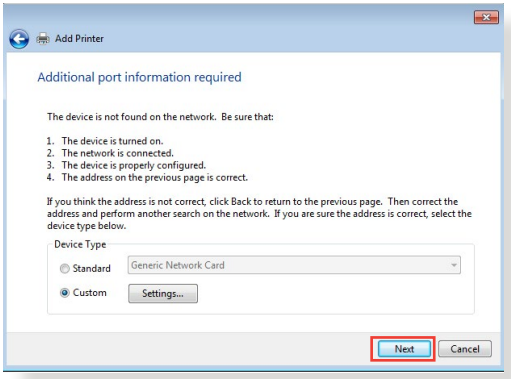
5. Sélectionnez **Custom** (Personnalisé) puis cliquez sur **Settings** (Paramètres).



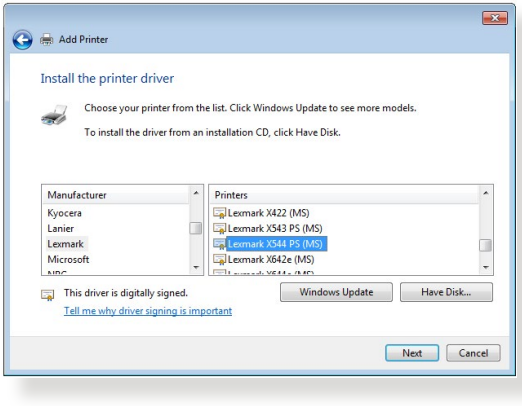
6. Réglez le **Protocol** (Protocole) sur **LPR**. Dans le champ **Queue Name** (Nom de la file d'attente), entrez **LPRServer** puis cliquez sur **OK** pour continuer.



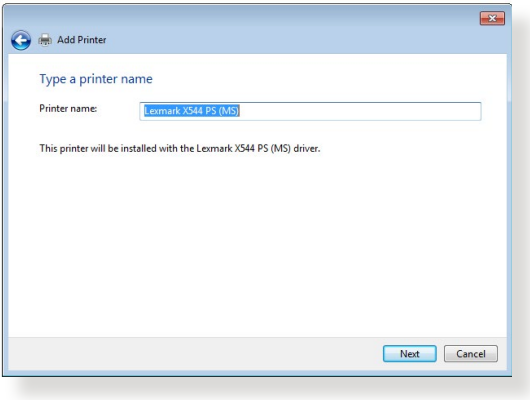
7. Cliquez sur **Next** (Suivant) pour terminer la configuration TCP/IP.



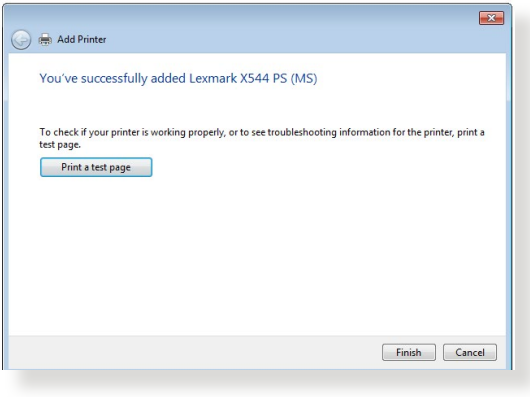
8. Installez le pilote d'impression à partir de la liste. Si votre imprimante ne figure pas dans la liste, cliquez sur **Have Disk** (Disque fourni) pour installer le pilote à partir d'un disque optique ou d'un fichier.



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



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



5.4 Download Master

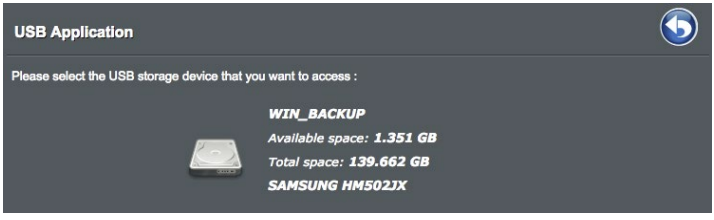
Download Master est un utilitaire vous permettant de télécharger des fichiers même lorsque votre ordinateur est éteint.

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

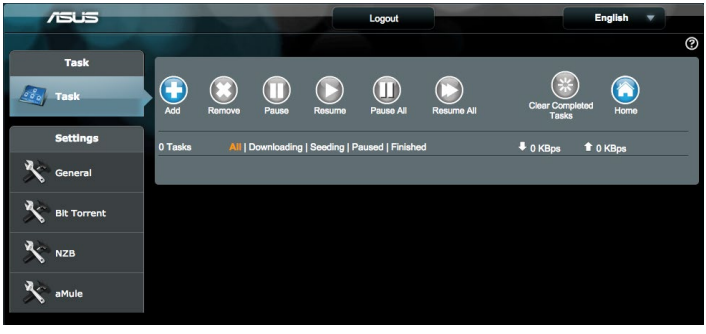
Pour utiliser Download Master :

1. Cliquez sur **General** (Général) > **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 Wi-Fi, sélectionnez celui sur lequel vous souhaitez télécharger vos fichiers.



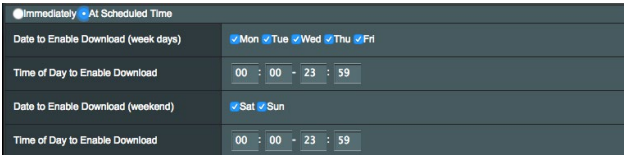
2. Une fois le téléchargement terminé, cliquez sur l'icône Download Master pour commencer à l'utiliser.
3. Cliquez sur **Add** (Ajouter) pour ajouter une tâche à télécharger.



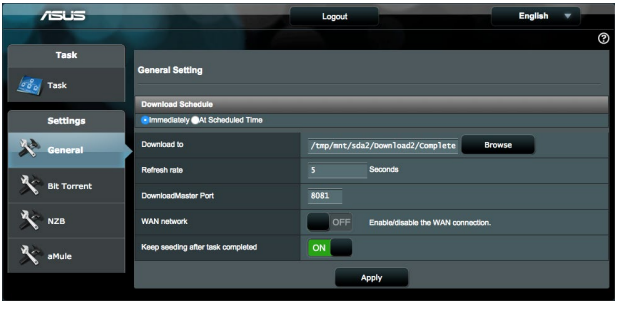
4. Sélectionnez un type de téléchargement, soit BitTorrent, HTTP, ou FTP. Spécifiez un fichier torrent ou une URL pour lancer le téléchargement.

REMARQUE : Pour plus de détails sur le protocole BitTorrent, consultez la section **5.4.1 Configurer les paramètres BitTorrent**.

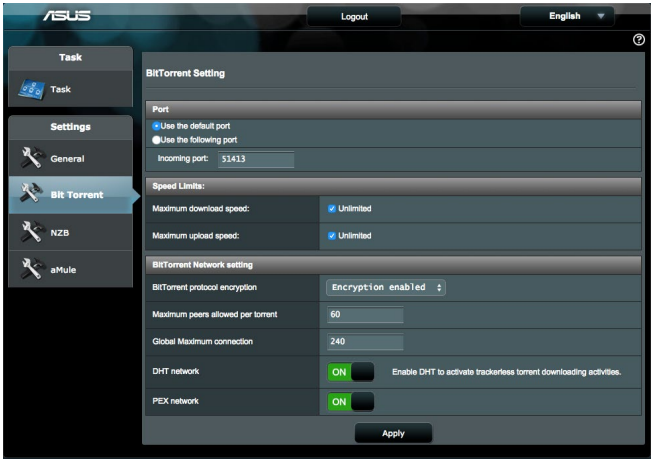
5. Utilisez le panneau de navigation pour configurer les paramètres généraux.
   - Vous pouvez télécharger un fichier immédiatement ou définir les horaires de téléchargement.



   - Les informations des tâches de téléchargement sont mises à jour toutes les 5 secondes. L'option **Refresh rate** (Délai d'actualisation) vous permet toutefois de définir manuellement la période de mise à jour.
   - Le champ **Download to** (Dossier de téléchargement) permet de définir l'emplacement de sauvegarde du fichier téléchargé.
   - Le port par défaut attribué à **DownloadMaster** est 8081. Si ce port est en conflit avec d'autres applications, vous pouvez le modifier librement.
   - Pour gérer **DownloadMaster** à partir d'internet, déplacez l'interrupteur **WAN network** (Réseau étendu) sur **ON** (OUI).
   - Si votre ressource réseau est limitée, nous vous conseillons de désactiver Keep seeding after task completed (Continuer de partager une fois que la tâche est terminée) en déplaçant l'interrupteur sur DÉSACTIVÉ.



5.4.1 Configurer les paramètres BitTorrent

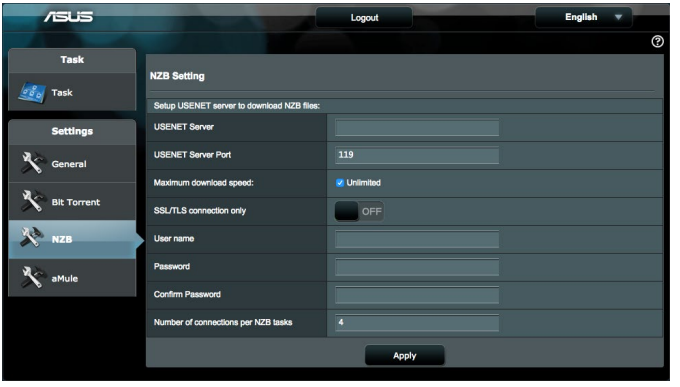


Pour configurer les paramètres de téléchargement BitTorrent :

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.
5. L'activation du réseau DHT (Distributed Hash Table) peut aider à améliorer les débits. Toutefois, pour l'utiliser le routeur doit pouvoir partager des informations avec les autres membres du réseau
6. L'activation du réseau PEX (Peer Exchange) autorise l'échange d'informations entre deux pairs connectés de sorte à pouvoir regrouper plus de pairs sur le réseau.

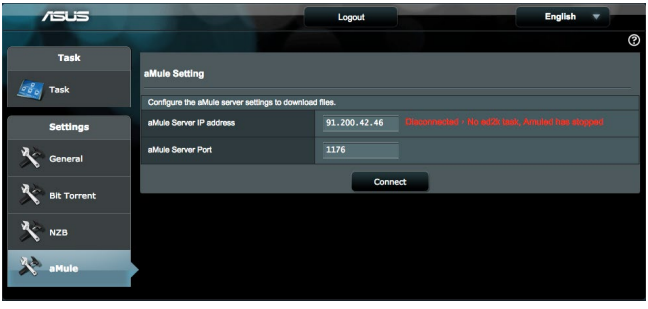
5.4.2 Paramètres NZB

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



5.4.3 Paramètres eMule

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



6 Dépannage

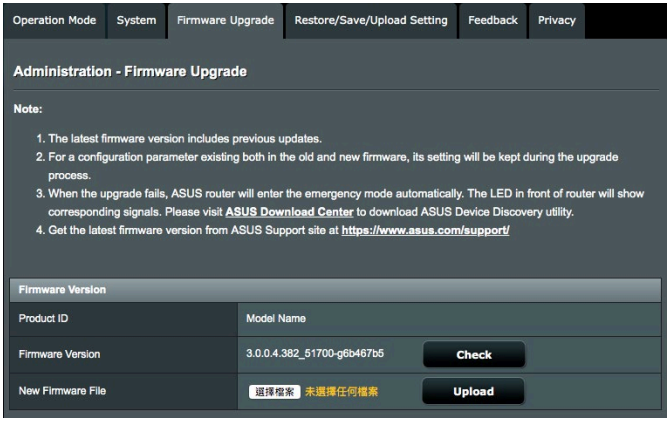
Ce chapitre offre des solutions aux problèmes pouvant survenir lors de l'utilisation de votre routeur. Si vous rencontrez un problème non traité dans ce chapitre, rendez-vous sur le site d'assistance d'ASUS sur: https://www.asus.com/fr/support pour plus d'informations sur votre produit et obtenir les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

6.1 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** > onglet **Firmware Upgrade** (Mise à jour du firmware). Cliquez sur **Check** (Vérifier) pour vérifier si une mise à jour du firmware est disponible.



2. Si un nouveau firmware est disponible, rendez-vous sur http://www.asus.com/fr/support pour le télécharger.
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 Wi-Fi de l'ordinateur correspondent à ceux du routeur.

- Lorsque vous tentez d'établir une connexion Wi-Fi entre un ordinateur et le routeur, assurez-vous que le SSID (nom du réseau Wi-Fi), 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.

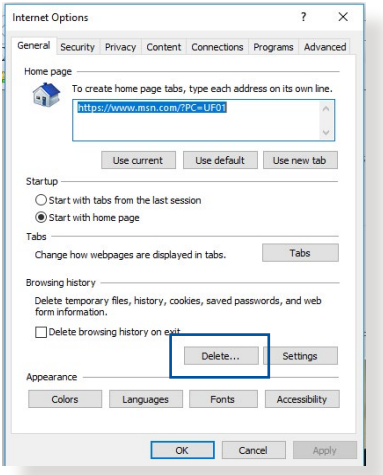


6.2 Foire aux questions (FAQ)

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 Wi-Fi 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 **General** (Général) > **Network Map** (Carte du réseau) > icône **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 Wi-Fi sauf celui de votre routeur, allez dans **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > 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 Wi-Fi, vérifiez que le canal Wi-Fi utilisé est disponible dans votre pays/région. Dans ce cas, modifiez le canal et les autres paramètres Wi-Fi appropriés.
- Si vous ne parvenez toujours pas à établir une connexion Wi-Fi 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 **General** (Général) > **Network Map** (Carte du réseau) et vérifiez **l'état de la connexion internet**.
- Si votre routeur ne peut pas se connecter à Internet, essayez de réinitialiser le réseau comme décrit à la sous-section **Réinitialisez votre réseau dans l'ordre suivant** sous **Dépannage de base**.
- Le client a été bloqué par la fonctionnalité de contrôle parental. Dans l'interface de gestion du routeur, allez dans **General** (Général) > **Parental Control** (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 Wi-Fi. Si le voyant lumineux dédié au réseau étendu (WAN) du routeur est éteint, vérifiez l'état de connexion des câbles.

L'accès au réseau cellulaire n'est pas disponible.

- Insérez une carte SIM dotée d'un accès à Internet et vérifiez que le voyant lumineux dédié à la connexion 3G/4G est allumé. Si ce n'est pas le cas, vérifiez que la carte SIM est correctement insérée.
- Les paramètres de connexion au réseau mobile ne sont pas appliqués automatiquement. Vérifiez les paramètres de connexion au réseau mobile auprès de votre opérateur de téléphonie mobile.
    - Allez ensuite dans **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Internet Connection** (Connexion internet).
    - Dans le champ **WAN Type** (Type de connexion au réseau étendu), sélectionnez **Mobile broadband** (Réseau cellulaire à haut débit).

- Si le problème persiste :
  - Vérifiez que la bande de fréquence utilisée est prise en charge par votre opérateur de téléphonie mobile.
  - Placez le routeur Wi-Fi à proximité d'une fenêtre pour garantir une bonne réception du signal 3G/4G.
- Vérifiez que le déclenchement de port, la redirection de port et les services DDNS et DMZ ne fonctionnent pas. La plupart des FAI fournissent une adresse IP privée à un appareil haut débit mobile. C'est pourquoi, certains services, tels que AiCloud, ne sont pas accessibles. Veuillez contacter votre FAI pour obtenir une assistance technique.

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
Adresse IP du routeur :	192.168.50.1 / router.asus.com
Paramètres Wi-Fi :	
SSID (2,4GHz):	ASUS_XX
SSID (5GHz):	ASUS_XX
Clé Wi-Fi par défaut :	Située sur l'étiquette collée sous le routeur.

REMARQUE : 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.

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 **5.2 Firmware Restoration (Restauration du firmware)** pour en savoir plus sur l'utilisation de cet utilitaire.

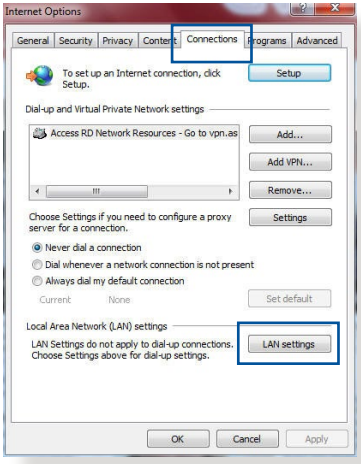
Impossible d'accéder à l'interface de gestion du routeur

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

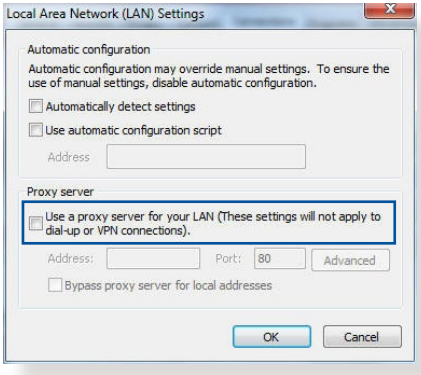
A. Désactivez le serveur proxy si celui-ci est activé.

Windows®

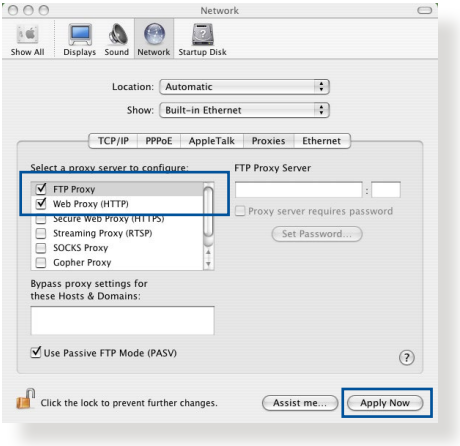
1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > onglet **Connections** (Connexions) > **LAN settings** (Paramètres réseau).



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



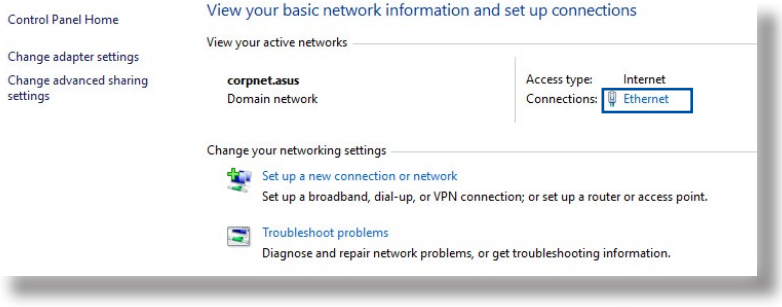
1. Dans votre navigateur Safari, cliquez sur **Safari** > **Preferences** (Préférences) > **Advanced** (Avancées) > **Change Settings** (Modifier les réglages)
2. Dans la liste des protocoles, décochez les options **FTP Proxy** (Proxy FTP) et **Web Proxy (HTTP)** (Proxy web sécurisé (HTTP)).
3. Cliquez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

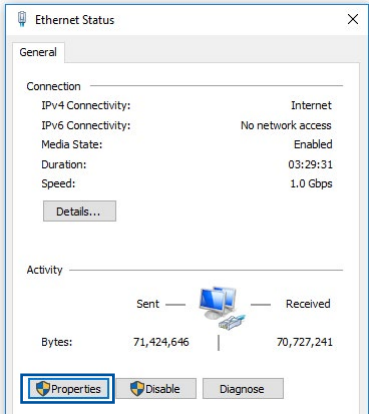
B. Configurez les paramètres TCP/IP pour l'obtention automatique d'une adresse IP.

Windows®

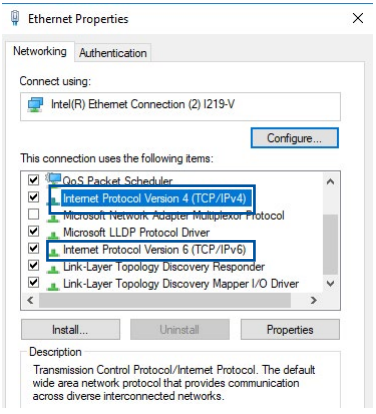
1. Cliquez sur **Start** (Démarrer) > **Control Panel** (Panneau de configuration) > **Network and Sharing Center** (Centre réseau et partage) > **Manage network connections** (Gérer les connexions réseau).



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



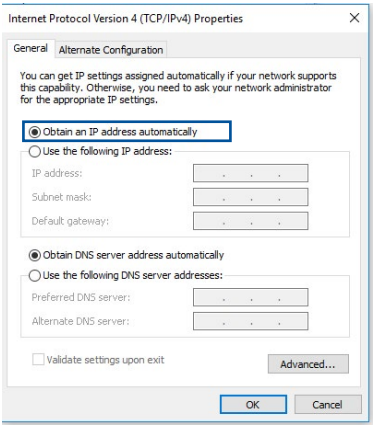
3. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)** (Protocole internet version 4 (TCP/IPv4)) ou **Internet Protocol Version 6 (TCP/IPv6)** (Protocole internet version 6 (TCP/IPv6)), puis cliquez sur **Properties** (Propriétés).



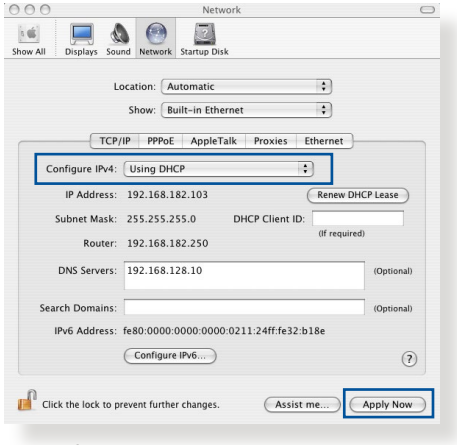
4. Pour obtenir une adresse IP IPv4, cochez l'option **Obtain an IP address automatically** (Obtenir une adresse IP automatiquement).

   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

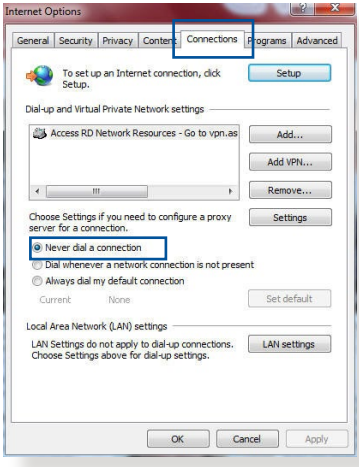


1. Cliquez sur l'icône Apple située en haut à gauche de votre écran.
2. Cliquez sur **System Preferences** (Préférences Système) > **Network** (Réseau) > **Configure...** (Configurer...)
3. Dans l'onglet **TCP/IP**, sélectionnez **Using DHCP** (Via DHCP) dans le menu déroulant **Configure IPv4** (Configurer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

Windows®



1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > onglet **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

Notices

Services de reprise et de recyclage

Les programmes de recyclage et de reprise d'ASUS découlent de nos exigences en terme de standards élevés de respect de l'environnement. Nous souhaitons apporter à nos clients des solutions permettant de recycler de manière responsable nos produits, batteries et autres composants ainsi que nos emballages. Veuillez consulter le site http://csr.asus.com/english/Takeback.htm pour plus de détails sur les conditions de recyclage en vigueur dans votre pays.

REACH

En accord avec le cadre réglementaire REACH (Enregistrement, Evaluation, Autorisation, et Restriction des produits chimiques), nous publions la liste des substances chimiques contenues dans nos produits sur le site ASUS REACH :

http://csr.asus.com/english/index.aspx

Rapport de la Commission Fédérale des Communications (FCC)

Cet appareil est conforme à l'alinéa 15 des règles établies par la FCC. Son utilisation est sujette aux deux conditions suivantes :

- Cet appareil ne doit pas créer d'interférences nuisibles, et.
- Cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Cet appareil a été testé et déclaré conforme aux limites relatives aux appareils numériques de classe B, en accord avec la Section 15 de la réglementation de la Commission Fédérale des Communications (FCC). Ces limites sont conçues pour offrir une protection raisonnable contre les interférences nuisibles en installation résidentielle.

Cet appareil génère, utilise et peut émettre de l'énergie de radiofréquence et, s'il n'est pas installé et utilisé en accord avec les instructions, peut créer des interférences nuisibles aux communications radio. Cependant, il n'y a pas de garantie que des interférences ne surviendront pas dans une installation particulière. Si cet appareil crée des interférences nuisibles à la réception de la radio ou de la télévision (il est possible de le déterminer en éteignant puis en rallumant l'appareil), l'utilisateur est encouragé à essayer de corriger les interférences par l'une ou plusieurs des mesures suivantes :

- Réorienter ou repositionner l'antenne de réception.
- Augmenter la distance de séparation entre l'appareil et le récepteur.
- Brancher l'appareil sur une prise secteur d'un circuit différent de celui auquel le récepteur est branché.
- Consulter le revendeur ou un technicien radio/TV qualifié pour obtenir de l'aide.

IMPORTANT ! Cet appareil est restreint à une utilisation en intérieur et à un fonctionnement dans la plage de fréquence de 5,15 à 5,25 GHz.

AVERTISSEMENT!

- Tout changement ou modification non expressément approuvé(e) par le responsable de la conformité peut annuler le droit de l'utilisateur à faire fonctionner cet appareil.
- Les utilisateurs ne sont pas autorisés à modifier l'appareil. Les changements ou modifications apportés à cette unité n'étant pas expressément approuvés par la partie responsable de la conformité (FCC) peuvent annuler le droit de l'utilisateur à faire fonctionner cet appareil.
- Pour les produits disponibles aux États-Unis et au Canada, seuls les canaux 1 à 11 peuvent être utilisés. Selection of other channels is not possible.

Déclaration de la Communauté Européenne

Déclaration simplifiée de conformité de l'UE

ASUSTeK COMPUTER INC. déclare par la présente que cet appareil est conforme aux critères essentiels et autres clauses pertinentes de la directive 2014/53/UE. La déclaration de conformité de l'UE peut être téléchargée à partir du site internet suivant : https://www.asus.com/fr/support/

Déclaration de conformité (Directive sur l'écoconception 2009/125/CE)

Test de la conformité aux exigences d'écoconception selon [CE 1275/2008] et [UE 801/2013]. Lorsque l'appareil est en mode Networked Standby, son panneau d'E/S et son interface réseau sont en mode veille et peuvent ne pas fonctionner correctement. Pour sortir l'appareil du mode veille, appuyez sur le bouton Wi-Fi, LED, de réinitialisation ou WPS.

Cet équipement a été testé et s'est avéré conforme aux limites établies par la l'UE en matière d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Tous les modes de fonctionnement :

2.4GHz : 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40)

5GHz : 802.11a, 802.11n (HT20), 802.11n (HT40) , 802.11n (HT80)

La fréquence, le mode et la puissance maximale transmise de l'UE sont listés ci-dessous :

2412-2472 MHz (802.11n HT40 MCS 8) : 19,97 dBm

5180-5240 MHz (802.11n HT40 MCS 8) : 22,43 dBm

5260-5320 MHz (802.11n HT40 MCS 8) : 22,81 dBm

5500-5700 MHz (802.11n HT20 MCS 8) : 29,75 dBm

Cet appareil est restreint à une utilisation en intérieur lors d'un fonctionnement dans la plage de fréquence de 5150 à 5350 MHz.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR		

Consignes de sécurité

- Utilisez ce produit dans un environnement dont la température ambiante est comprise entre 0˚C (32°F) et 40˚C (104°F).
- Référez-vous à l'étiquette située au dessous du produit pour vérifier que l'adaptateur secteur répond aux exigences de tension.
- NE PAS placer sur une surface irrégulière ou instable. Contactez le service après-vente si le châssis a été endommagé.
- NE PAS placer, faire tomber ou insérer d'objets sur/dans le produit.
- NE PAS exposer l'appareil à la pluie ou à l'humidité, tenez-le à distance des liquides. NE PAS utiliser le modem lors d'un orage.
- NE PAS bloquer les ouvertures destinées à la ventilation du système pour éviter que celui-ci ne surchauffe.
- NE PAS utiliser de cordons d'alimentation, d'accessoires ou autres périphériques endommagés.
- Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien électrique qualifié ou votre revendeur.
- Pour éviter tout risque de choc électrique, débranchez le câble d'alimentation de la prise électrique avant de toucher au système.

Avertissement concernant la marque CE

Ceci est un produit de classe B. Dans un environnement domestique, ce produit peut créer des interférences radio, auquel cas l'utilisateur pourra être amené à prendre les mesures adéquates.

Cet appareil peut être utilisé dans les pays suivants : AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Informations concernant l'exposition aux fréquences radio (RF)

Cet équipement a été testé et s'est avéré conforme aux limites établies par Industrie Canada en matière d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Canada, avis d'Industrie Canada (IC)

Le présent appareil est conforme aux normes CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

Son utilisation est sujette aux deux conditions suivantes : (1) cet appareil ne doit pas créer d'interférences et (2) cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Précautions d'emploi de l'appareil

a. N'utilisez pas le produit ou soyez particulièrement vigilant quant à votre sécurité lors de l'utilisation de cet appareil dans certains lieux (les avions, les aéroports, les hôpitaux, les stations-service et les garages professionnels).

b. Évitez d'utiliser cet appareil à proximité de dispositifs médicaux implantés lors d'un appel téléphonique. 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 l'implant pour réduire les risques d'interférence.

c. 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 les parkings souterrains, les ascenseurs, en train ou en voiture ou tout simplement dans un secteur mal couvert par le réseau.

d. Tenez cet appareil à distance du ventre des femmes enceintes et du bas-ventre des adolescents.

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. We include a copy of the GPL with every CD shipped with our product. 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

Informations de contact ASUS

ASUSTeK COMPUTER INC.

Adresse	1F, No. 15, Lide Rd., Beitou, Taipei 112, Taïwan
Téléphone	+886-2-2894-3447
Fax	+886-2-2893-1687
Site Web	https://www.asus.com

Support technique

Téléphone	+86-21-38429911
Support en ligne	https://qr.asus.com/techserv

ASUS COMPUTER INTERNATIONAL (Amérique)

Adresse	48720 Kato Rd., Fremont, CA 94538, USA
Téléphone	+1-510-739-3777
Fax	+1-510-608-4555
Site Web	https://www.asus.com/us/

Support technique

Fax	+1-812-284-0883
Téléphone	+1-812-282-2787
Support en ligne	https://qr.asus.com/techserv

ASUS COMPUTER GmbH (Allemagne et Autriche)

Adresse	Harkortstrasse 21-23, 40880 Ratingen, Allemagne
Site Web	http://www.asus.com/de
Contact en ligne	https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=de-de

Support technique

Téléphone (DE) :	+49-2102-5789557
Téléphone (AT) :	+43-1360-2775461
Support en ligne	https://www.asus.com/de/support