Guide de mise en réseau Wi-Fi d’AccuPoint® Advanced Next Generation

Configuration et dépannage

NEOGEN®
NEOGEN.com

Table des matières

Présentation des exigences réseau d'AccuPoint® Advanced NG

AccuPoint® Advanced NG peut prendre en charge la connectivité Wi-Fi suivante :

- 802.11 b/g/n
- WPA2/WPA Personal et Enterprise
- WEP
- IPV4
- Débit réseau pouvant atteindre 72 Mo
- Le signal porte jusqu'à 450 m. Il est affecté par les superstructures, les obstacles physiques et d'autres interférences de signaux.

Le système est incapable de prendre en charge l'authentification RADIUS ou d'autres formes d'authentification réseau. Dans les environnements d'entreprise qui requièrent une authentification basée sur l'hôte ou l'utilisateur, il est recommandé d'utiliser à la place le filtrage des adresses MAC pour les dispositifs AccuPoint Advanced NG. L'adresse MAC du dispositif est disponible sur l'écran À propos de chaque dispositif AccuPoint Advanced NG. Dans certains environnements, le filtrage MAC peut nécessiter un nouveau SSID ou un réseau Wi-Fi distinct.

Il est fortement recommandé d'activer l'enregistrement d'hôte DHCP (DNS) sur le réseau où le PC du gestionnaire de données et le dispositif AccuPoint Advanced NG se connecteront. Lorsque la fonction Wi-Fi est activée, le dispositif et le PC exécutant le logiciel Data Manager doivent pouvoir communiquer entre eux sur le réseau. La connexion peut être initiée par l'un ou l'autre hôte. Étant donné que le PC et le dispositif peuvent se déplacer entre les segments de réseau ou les points d'accès, entraînant ainsi une modification de l'adresse IP, la possibilité de se connecter en utilisant le nom d'hôte du PC et du dispositif sera une capacité essentielle, afin de s'adapter aux changements d'adresse IP dynamiques. Si le PC et le dispositif AccuPoint Advanced NG ne peuvent pas utiliser les noms d'hôtes pour se connecter et que l'adresse IP du PC ou du dispositif change, il est très probable qu'ils perdront la capacité de communiquer jusqu'à ce que le dispositif AccuPoint Advanced NG soit reconfiguré par l'intermédiaire d'une connexion USB.

Le dispositif AccuPoint Advanced NG communique en toute sécurité avec le PC exécutant le logiciel Data Manager, et ce à l'aide d'un certificat TLS auto-signé. La connexion TLS est hébergée sur le PC à l'aide du composant logiciel du service Data Manager. Cette connexion est établie lorsque le dispositif envoie ou reçoit des données depuis le logiciel Data Manager, mais elle n'est pas conservée en permanence. Après une brève période d'inactivité, la connexion est interrompue par le dispositif afin d'éviter les problèmes de stabilité des connexions au ralenti.

Lorsque le dispositif AccuPoint Advanced NG établit une connexion, toutes les communications s'effectuent par TLS sur le port 443 du PC. Cependant, lorsque l'utilisateur souhaite transmettre un plan de site par la technologie push ou initier des communications réseau avec le dispositif AccuPoint Advanced NG, le PC doit tout d'abord envoyer un signal au dispositif via le port 80, à un service web qui s'exécute sur le dispositif AccuPoint Advanced NG. Lorsque ce dispositif reçoit cette demande du service Web, il ferme ce service et établit une connexion sécurisée avec le PC du gestionnaire de données. Lorsque la connexion sécurisée est interrompue, le dispositif rend à nouveau disponible le service Web basé sur le protocole HTTP.

Dans les environnements d'entreprise, il peut s'avérer nécessaire de créer des exceptions à la politique réseau afin d'autoriser le trafic via le port 80 vers le dispositif AccuPoint® Advanced NG depuis le PC du gestionnaire de données, et via le port 443 depuis le dispositif vers le PC. Le PC et le dispositif peuvent tous deux utiliser des requêtes ICMP pour s'envoyer des requêtes ping. Le trafic ICMP entre le dispositif AccuPoint Advanced NG et le PC doit donc être activé lui aussi.

Sous Windows, sur le PC du gestionnaire de données, le logiciel Data Manager tentera de reconfigurer le pare-feu local et les paramètres de sécurité au moment de l'installation afin de répondre à ses besoins d'accès. Cela ne réussit pas toujours, en fonction des règles de groupe et des logiciels présents sur le PC où le logiciel est installé. Voici les besoins essentiels du réseau :

1. La connexion réseau du PC utilisé pour se connecter à l'AccuPoint Advanced NG doit être configurée pour être privée. Sur Windows, tout le trafic entrant initié par un dispositif externe est bloqué sur une connexion publique.
2. Le pare-feu local du PC du gestionnaire de données doit être configuré pour permettre :
    a. le trafic entrant au niveau du port 443
    b. le trafic sortant au niveau du port 80 (norme HTTP).
    c. le trafic ICMP sortant et entrant
3. Le logiciel de sécurité s'exécutant sur le PC et les règles de groupes de Windows doivent permettre aux exécutables suivants d'accéder au réseau :
    a. C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0\DataManager.Service.exe
    b. C:\ProgramData\NEOGEN\DataManager.Service.RestService\DataManager.Service.RestService.exe
    c. {Installed Location}\HID_UART.exe

Des exceptions supplémentaires peuvent être requises lorsque le logiciel Data Manager est mis à jour. Des bulletins techniques seront fournis lorsque ces changements auront lieu.

De nombreux environnements d'entreprise s'appuient sur la protection des points de terminaison et sur des logiciels de sécurité centralisés, comme CrowdStrike, qui nécessitent des exceptions spécifiques par rapport aux règles. De même, les règles de groupe de Windows peuvent interférer avec la connectivité du dispositif et du PC.

Ces exigences de configuration doivent être testées une fois que le logiciel Data Manager a été installé et qu'un dispositif AccuPoint Advanced NG a été configuré pour l'accès Wi-Fi. Veuillez consulter les directives et les recommandations de dépannage qui suivent.

Si NEOGEN® Analytics est également utilisé, le trafic local (sur le PC du gestionnaire de données uniquement) doit être autorisé sur le port 80. Cependant, ce port n'a pas besoin d'être exposé à l'ensemble du réseau. Veuillez consulter la documentation de NEOGEN Analytics pour découvrir les exigences supplémentaires d'accès au réseau.

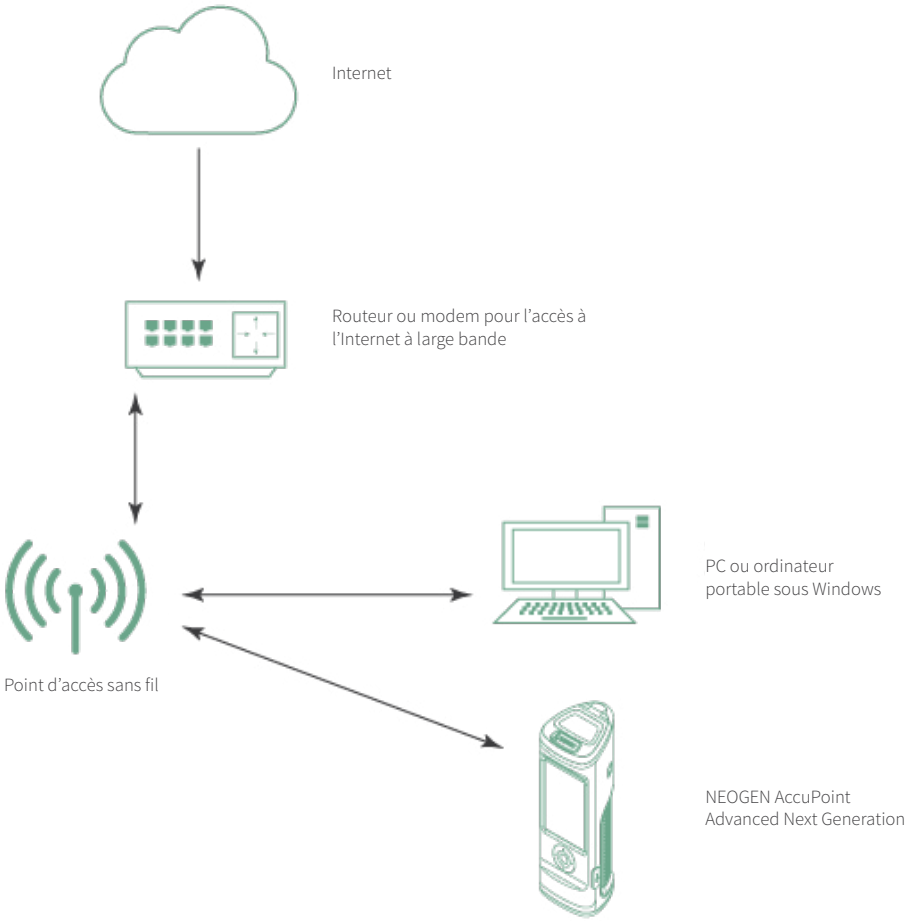
Lors de la modification des configurations sur le PC exécutant le logiciel Data Manager, l'utilisateur qui effectue ces modifications doit disposer de droits d'administrateur. Cette élévation peut être temporaire, le cas échéant. Certaines organisations sont en mesure de répercuter les modifications sur les PC en local. Cependant, le débogage des problèmes de connexion est difficile à mettre en œuvre sans les droits d'administrateur local. L'un des outils fournis avec le logiciel Data Manager est un script PowerShell qui fournit des informations de diagnostic.

Avant de commencer

Comprendre votre environnement réseau

Simple

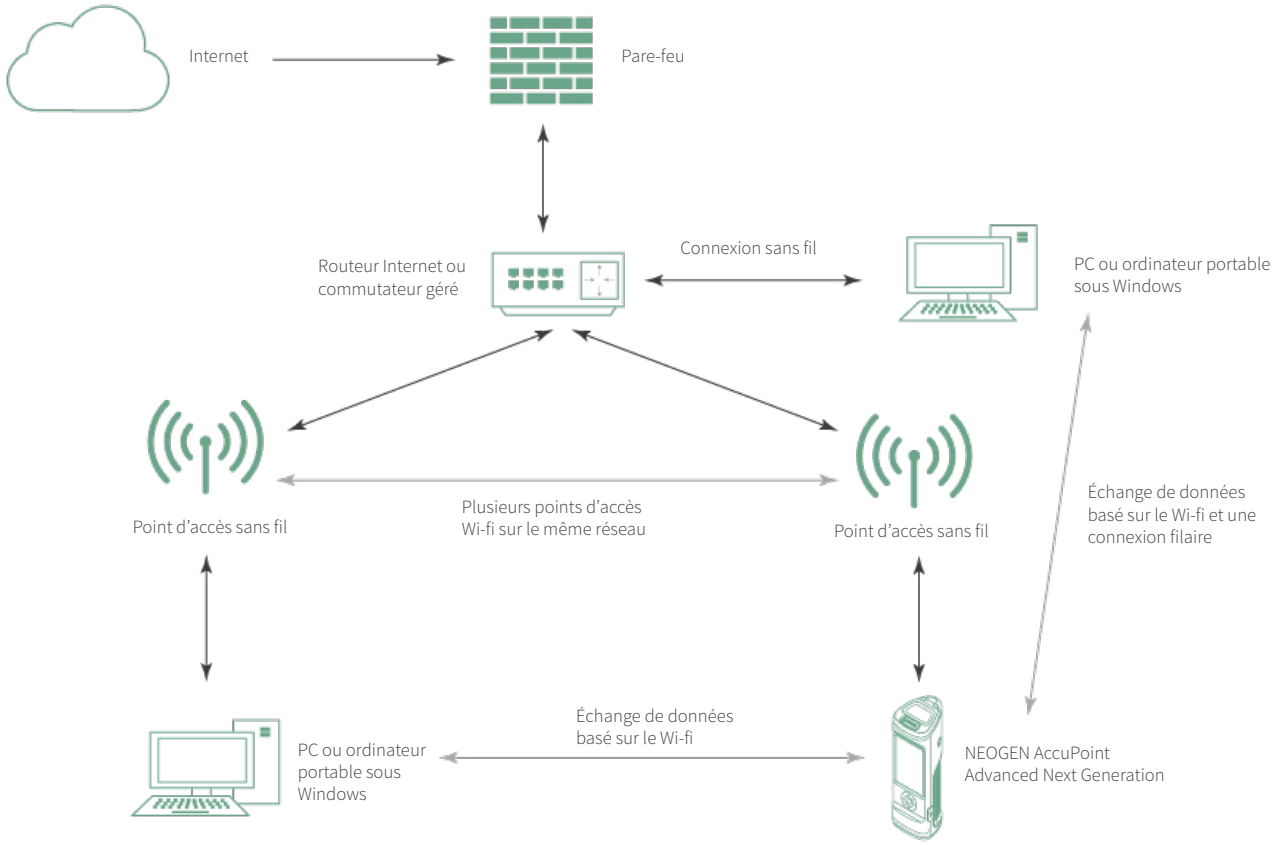
Un site de réseau simple est présent dans de nombreuses entreprises individuelles ou espaces de travail isolés. Il se compose généralement d'une connexion Internet et d'un seul point d'accès sans fil, comme le suivant :



Dans cette configuration réseau plate, les principaux problèmes consistent à s'assurer de la bonne configuration du point d'accès sans fil (WAP) pour permettre au dispositif AccuPoint® Advanced NG de se connecter au réseau local. Le guide de dépannage présente les différentes façons de modifier le WAP pour permettre de nouvelles connexions. Sur le PC ou l'ordinateur portable, la principale difficulté sera de veiller à ce que la connexion sans fil locale, le pare-feu et le logiciel de sécurité autorisent les connexions entrantes.

Organisation

Le site d'une organisation peut disposer de pare-feux et de logiciels de sécurité plus perfectionnés disposant de plusieurs points d'accès sans fil, comme le montre ce schéma :



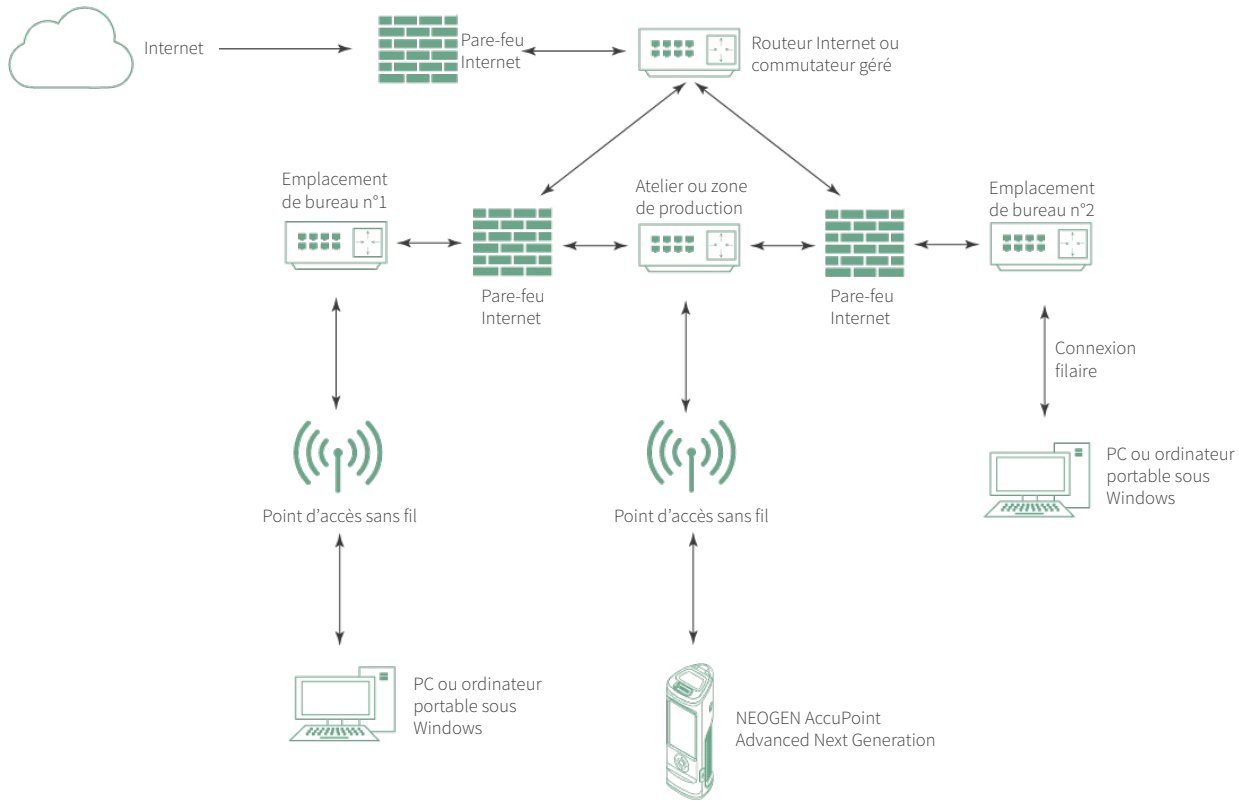
La plupart des utilisateurs possédant ce type de configuration réseau auront besoin de l'aide de leur équipe de services informatiques locale pour configurer correctement le dispositif et le PC hébergeant le logiciel Data Manager. Les tâches sont les suivantes :

1. Veiller à ce que AccuPoint® Advanced NG puisse accéder au réseau Wi-Fi.
2. Faire en sorte que le PC du gestionnaire de données et le dispositif AccuPoint Advanced NG puissent se voir sur le réseau.
3. S'assurer que le logiciel de contrôle de la sécurité autorise le trafic d'échange de données entre le dispositif AccuPoint Advanced NG et le PC du gestionnaire de données.

Le guide de dépannage explique en détail comment identifier les problèmes et les informations à partager avec l'équipe de services informatiques, en veillant à ce que tous les composants soient correctement configurés.

Entreprise

Un site d'entreprise dispose généralement d'une segmentation réseau, de configurations Wi-Fi avancées et de restrictions relatives aux dispositifs autorisés sur ses réseaux. Plusieurs pare-feu et commutateurs peuvent s'ajouter. L'exemple suivant représente un réseau d'entreprise très simplifié.



Dans un environnement réseau aussi complexe que celui-ci, la connexion Wi-Fi entre le dispositif AccuPoint® Advanced NG et le PC du gestionnaire de données peut nécessiter l'envoi de plusieurs tickets à l'équipe de services informatiques, et en particulier :

1. Modifications des stratégies de groupe de Windows qui autoriseront les connexions réseau entrantes, ainsi que des modifications du pare-feu local et du logiciel de sécurité sur le PC où est installé le gestionnaire de données.
2. Autorisations d'installer le logiciel Data Manager et de modifier la configuration du PC local.
3. Définition d'exceptions aux règles d'accès au réseau pour permettre au dispositif AccuPoint Advanced NG d'accéder au réseau Wi-Fi.
4. Modifications des règles relatives au pare-feu interne pour autoriser le trafic réseau entre le PC du gestionnaire de données et AccuPoint Advanced NG.
5. Mises à jour des règles du logiciel de sécurité pour permettre l'échange de données avec le dispositif AccuPoint Advanced NG.

Les environnements hautement sécurisés peuvent nécessiter la mise en place d'un nouveau SSID Wi-Fi, uniquement pour les communications AccuPoint Advanced NG.

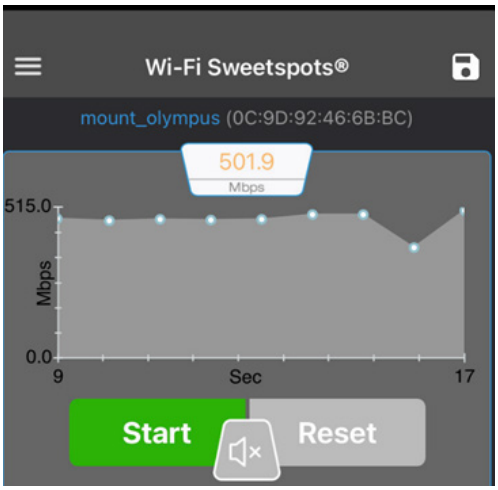
Vérification de la puissance du signal Wi-Fi

Les interférences Wi-Fi ou la faiblesse du signal pendant le fonctionnement du dispositif AccuPoint Advanced NG constituent l'un des problèmes les plus difficiles à résoudre. Comme indiqué, le dispositif est doté d'une radio Wi-Fi de plus faible puissance afin d'améliorer l'autonomie de la batterie et de préserver la portabilité. Malheureusement, cela signifie que le dispositif peut être plus sensible à la perte de signal dans les zones opérationnelles touchées par une faiblesse ou des interférences du signal Wi-Fi. Pour identifier à l'avance les problèmes de connexion Wi-Fi, la meilleure façon de procéder est de demander une étude du signal Wi-Fi dans les zones opérationnelles où vous prévoyez de collecter et de transmettre des données d'essai. Cependant, pour certaines organisations, cette procédure peut s'avérer trop difficile ou trop longue à mettre en œuvre.

Heureusement, il existe des outils de test de la connexion Wi-Fi qui permettent à la plupart des utilisateurs de mener une enquête très simple basée sur le débit de transmission du réseau. Pour tout utilisateur disposant d'un smartphone ou d'une tablette avec connectivité Wi-Fi, il est possible de charger des applications qui vérifieront la puissance du signal. Voici les applications disponibles sur iOS (Apple) et Android :

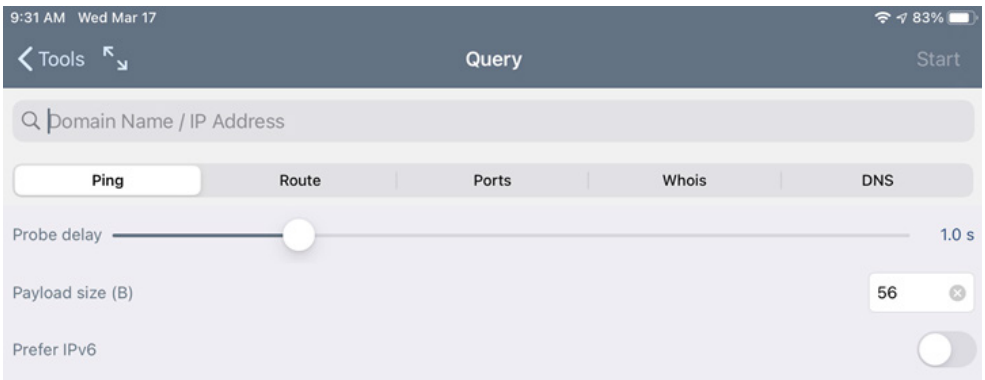
- Wi-Fi SweetSpots (conseillé, gratuit)
- Network Analyzer (également gratuit, mais plus complexe)
- Network Analyzer Pro (frais réduits pour un bel ensemble de fonctionnalités)

Veuillez consulter la capture d'écran de l'application Wi-Fi SweetSpots :



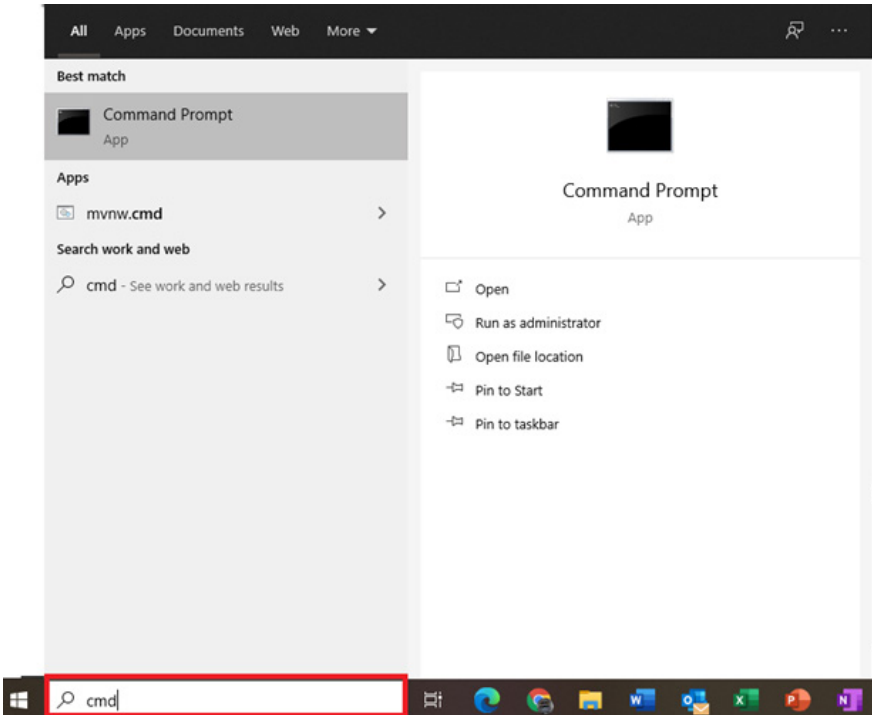
Wi-Fi SweetSpots effectue un suivi du débit Wi-Fi. Lorsque le taux de transfert du réseau chute, vous entrez dans un endroit où le signal Wi-Fi est plus faible, ou les niveaux d'interférence plus élevés. Si le débit du réseau chute de plus de 50 %, il est probable que le dispositif AccuPoint® Advanced NG connaisse des problèmes de communication réseau.

Network Analyzer est destiné aux utilisateurs possédant une expérience plus pointue des réseaux et souhaitant effectuer des diagnostics supplémentaires tels que le traçage des chemins, la vérification des DNS, les pings réseau, etc. À titre d'exemple, veuillez consulter la capture d'écran suivante de Network Analyzer Pro :



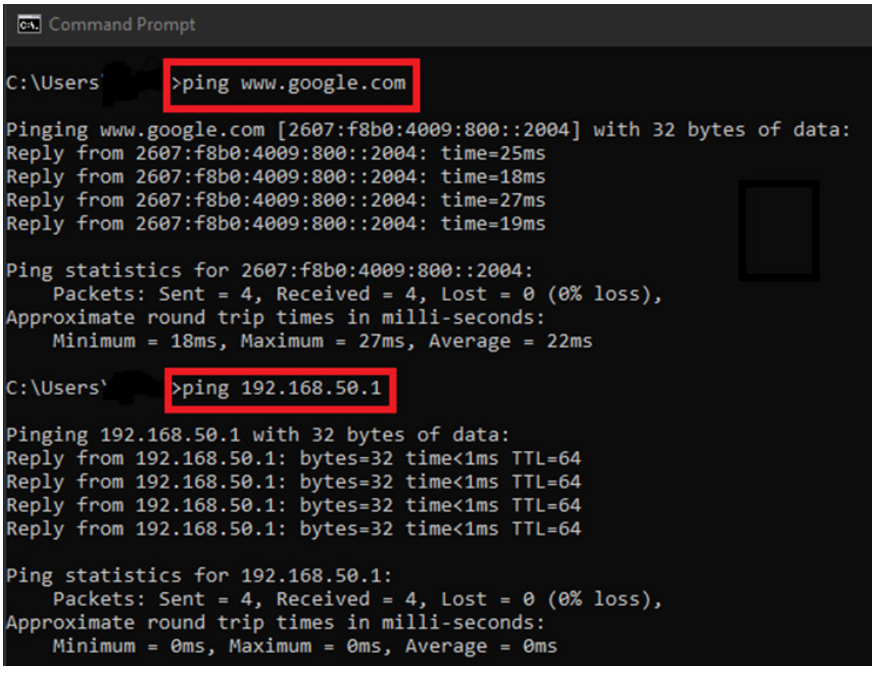
Outils de diagnostic réseau pour les utilisateurs

Windows 10 fournit aux utilisateurs plusieurs commandes très utiles qui peuvent être exécutées à partir du bureau de l'utilisateur. Pour ceux qui ne savent pas comment lancer une fenêtre d'invite de commande, veuillez consulter la capture d'écran suivante. Si vous tapez CMD dans la zone de recherche de Windows, vous verrez : Ping

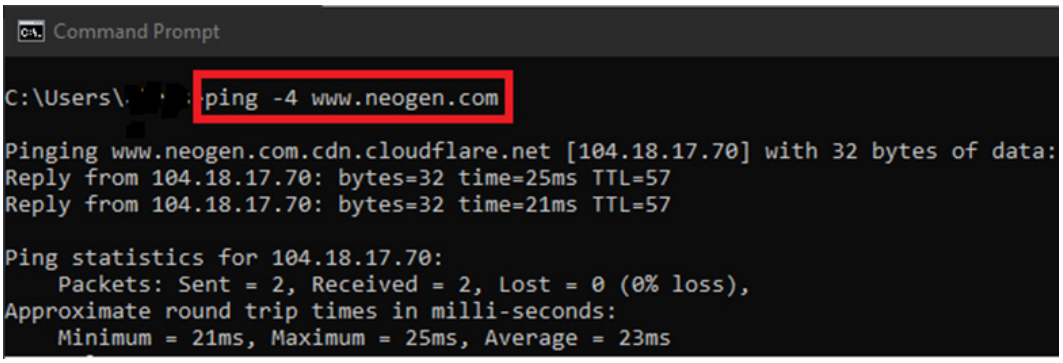


Ping

Cette commande simple est l'une des plus utiles pour déterminer si le PC du gestionnaire de données peut accéder au dispositif AccuPoint® Advanced NG. Cependant, certaines nuances sont à prendre en considération. La commande de base est tout simplement ping <some host> ou un numéro IP :



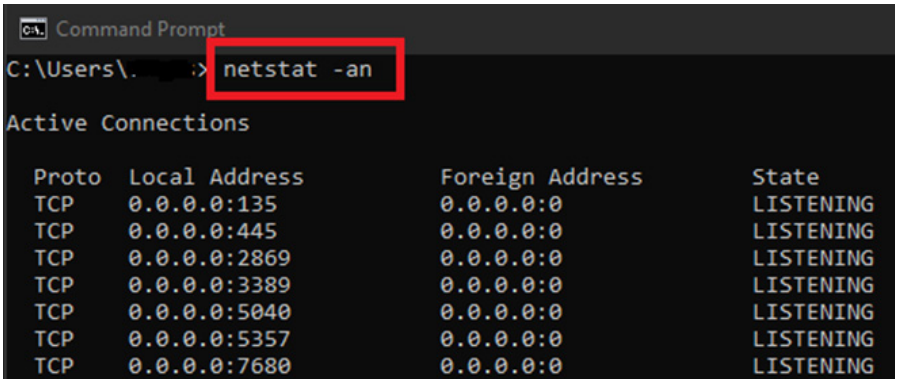
La première commande est utilisée pour envoyer une demande ping au site www.google.com. La seconde est utilisée pour envoyer une demande ping à une adresse sur le même réseau. Sachez que les adresses utilisées lors de la première demande ping sont IPv6. Pour contraindre une demande ping à utiliser IPv4, vous devrez peut-être modifier la commande en ajoutant -4, comme dans l'exemple suivant :



Les délais d'envoi de la demande Ping comptent ! Sur un réseau local, le temps nécessaire pour atteindre un hôte ne doit pas dépasser 10 ms. Tout délai supérieur doit être géré par votre équipe de services informatiques locale. Pour les adresses sur internet, le délai des demandes ping doit être égal ou inférieur à 120 ms. Les demandes Ping peuvent présenter un délai supérieur lorsque les hôtes sont géographiquement éloignés. Cependant, la survenue de délais lors de l'envoi d'une demande Ping vers des services courants comme Google ou Amazon peut indiquer un ralentissement de la connexion Internet. Étant donné que AccuPoint® Advanced NG et le PC sur lequel est installé le gestionnaire de données communiquent sur le même réseau, une connexion internet lente n'entravera pas le fonctionnement du dispositif et la transmission des données. Toutefois, une connexion Internet lente peut empêcher le téléchargement des mises à jour du gestionnaire de données ou du micrologiciel du dispositif.

Netstat

Cette commande présente les ports écoutés par un PC et ceux auxquels il est activement connecté. Pour AccuPoint Advanced NG, le PC du gestionnaire de données doit écouter le port 443. La commande et la sortie sont les suivantes:



L'adresse locale et le port sont importants :

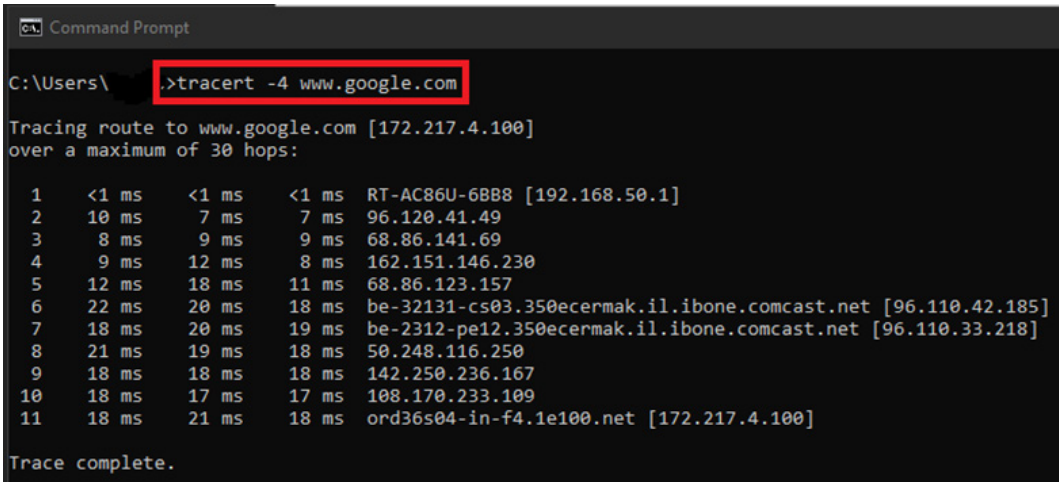
Adresse : ###.###.###.### :<Port : ###>

Il peut y avoir plusieurs dizaines d'entrées, selon les logiciels et les services en cours d'exécution sur un PC.

La sortie dans la capture d'écran pour l'adresse 0.0.0.0:445 montre que ce PC accepte les connexions sur le port 445 pour tous ses adaptateurs réseau. Cette commande contribuera à déterminer si le service Data Manager s'exécute et s'il est prêt à accepter les connexions du dispositif AccuPoint Advanced NG.

TRACERT

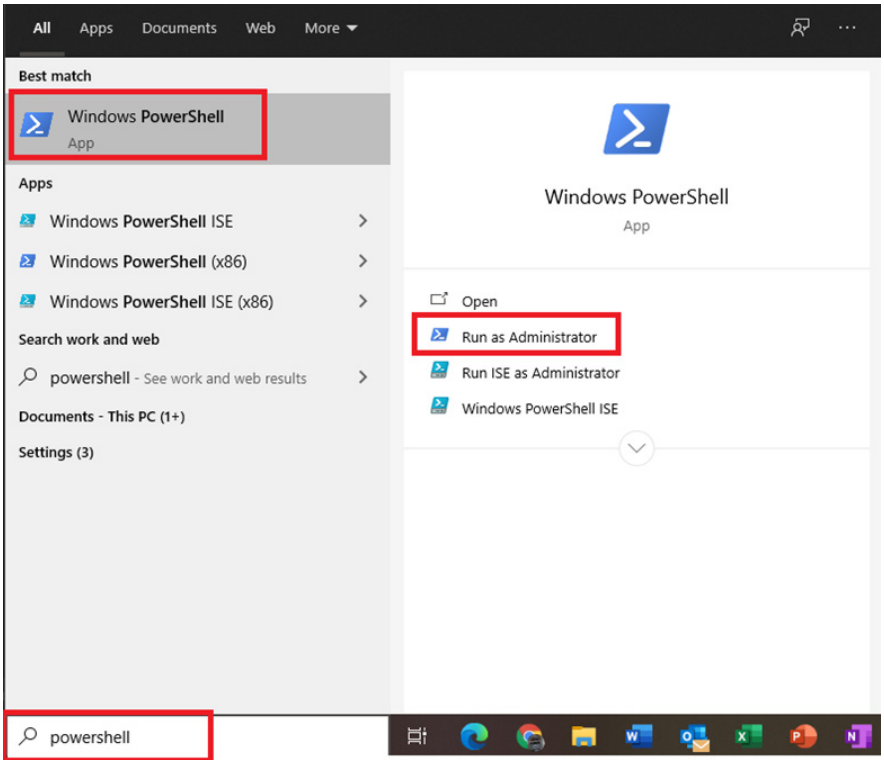
Le TRACERT montre le chemin d'un hôte vers un autre au sein d'un réseau. Chaque adresse intermédiaire constitue un bon sur le réseau. Cette commande permettra d'identifier les commutateurs, les pare-feux et les périphériques réseau devant être franchis par le trafic entre le PC du gestionnaire de données et le dispositif AccuPoint® Advanced NG. L'exemple suivant montre le chemin d'accès entre ce PC et l'hôte www.google.com. Sur un réseau local, le nombre de bonds doit être compris entre 1 et 6.



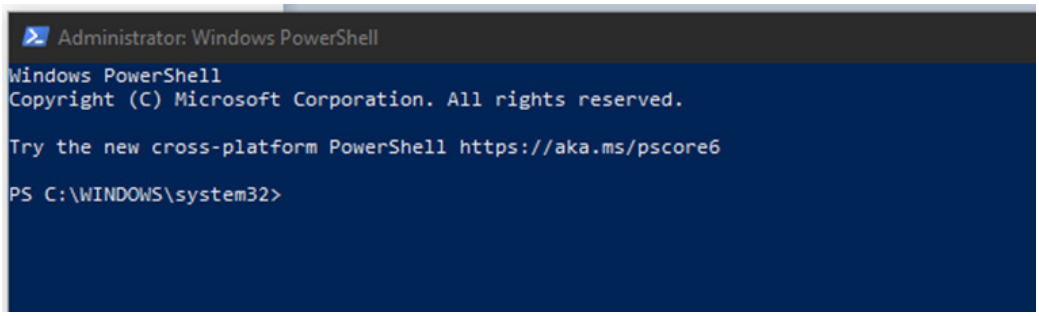
Le bond n°1 est le point d'accès sans fil local. Chaque bond qui suit est un routeur, un commutateur ou un parefeu que le trafic réseau doit franchir avant d'atteindre son objectif, à savoir l'adresse 172.217.4.100. Le paramètre -4 garantit l'utilisation par le trafic du protocole IPv4.

PowerShell

Dans le guide de dépannage, plusieurs commandes PowerShell sont répertoriées pour faciliter à la fois la configuration du PC du gestionnaire de données et le diagnostic des problèmes de communication. On accède à PowerShell de la même manière qu'à l'invite CMD. En général, l'interpréteur de commandes PowerShell s'exécute en mode administrateur.

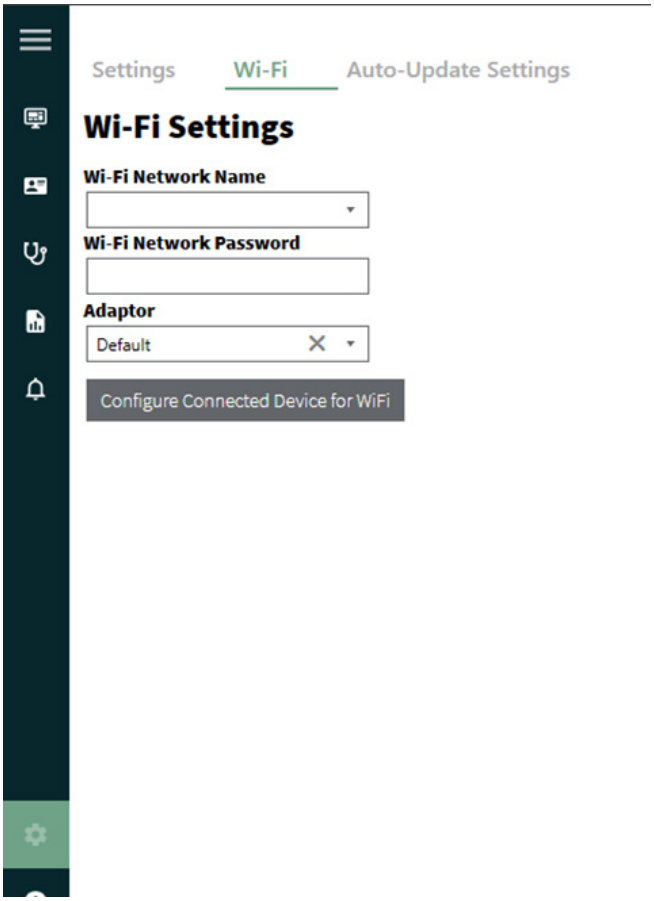


À l'invite, répondez en cliquant sur « Yes » (Oui) pour lancer PowerShell.



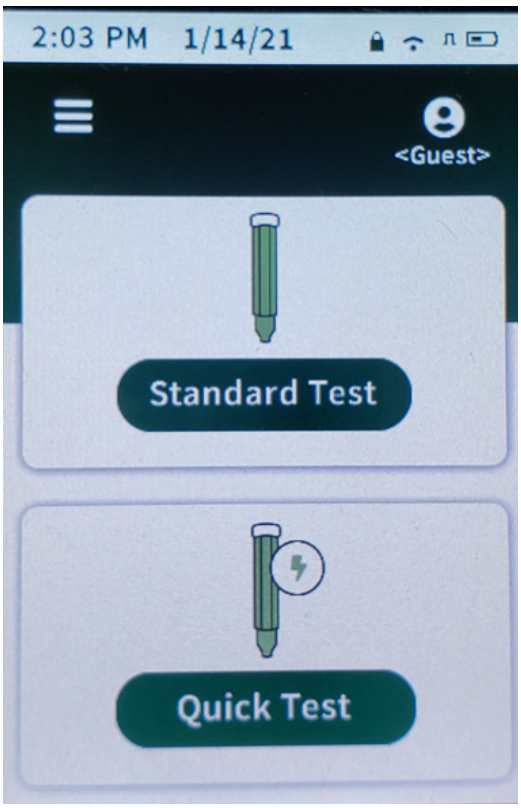
Configuration du dispositif pour le Wi-Fi

Pour configurer le dispositif AccuPoint® Advanced NG pour le Wi-Fi, accédez à l'écran Settings (Paramètres) en cliquant sur l'icône en forme d'engrenage en bas à gauche du Data Manager, puis sélectionnez l'onglet Wi-Fi. Les champs ne seront activés que si le dispositif AccuPoint Advanced NG est connecté au PC via un câble USB et est sous tension.



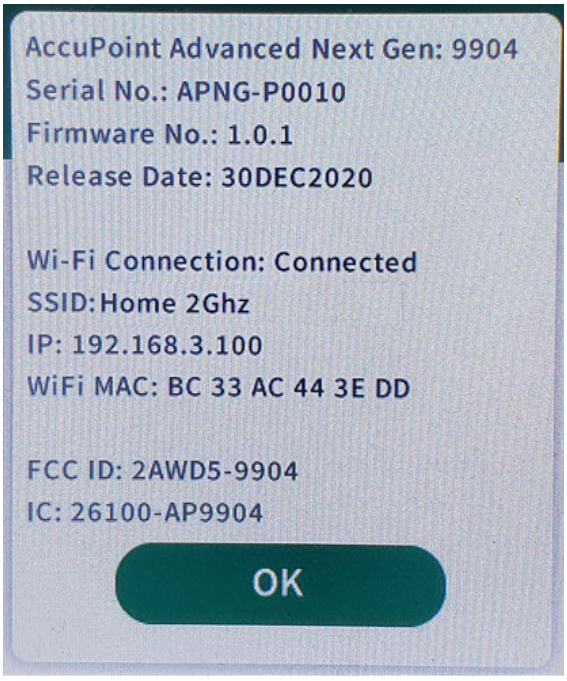
Une fois les champs Wi-Fi network name (Nom du réseau Wi-Fi) et Wi-Fi network password (Mot de passe du réseau Wi-Fi) sélectionnez, cliquez sur le bouton Configure connected device for Wi-Fi (Configurer le périphérique connecté pour le Wi-Fi).

Au bout de quelques secondes, le dispositif doit afficher à la fois une icône Wi-Fi et une icône de verrouillage en haut de l'écran.



Si tel n'est pas le cas, quelques opérations de dépannage sont à effectuer pour tenter de se connecter au dispositif.

Si la connectivité Wi-Fi reste défaillante, consultez l'écran About (À propos) du dispositif pour connaître son adresse IP.



Pour déterminer si le PC s'est connecté via le protocole de contrôle de transmission (TCP), ouvrez une invite de commande et essayez d'envoyer une demande ping au dispositif en utilisant l'adresse IP figurant sur l'écran About de ce dernier :

ping 192.168.3.100

Vous devriez recevoir une réponse semblable à celle ci-dessous, laquelle signifie que le PC peut voir le dispositif :

```
C:\Users>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=3ms TTL=255
Reply from 192.168.3.100: bytes=32 time=4ms TTL=255
Reply from 192.168.3.100: bytes=32 time=6ms TTL=255
Reply from 192.168.3.100: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

Une réponse hors délai à la demande ping signifie que le PC ne peut pas communiquer avec le dispositif.

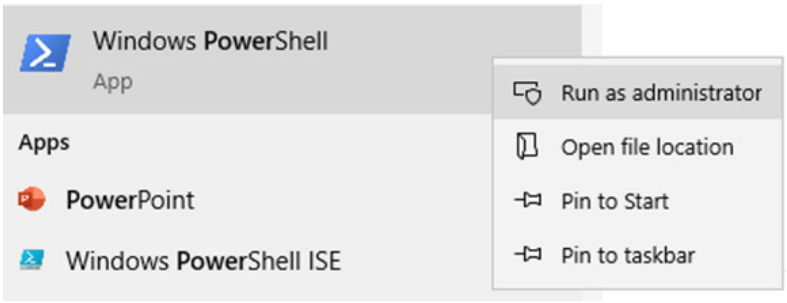
```
Pinging 192.68.3.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.68.3.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Vous devrez peut-être travailler avec votre équipe de services informatiques pour résoudre ce problème. Des étapes supplémentaires de dépannage sont indiquées plus loin dans ce document

Ouverture du port 443

Pour que le PC et le dispositif AccuPoint® Advanced NG puissent communiquer, le port 443 doit permettre la communication entre ces points finaux. Si un pare-feu est installé en local sur le PC, la règle d'accès entrant doit être ajoutée pour autoriser le trafic sur le port TCP 443. Des règles doivent également être ajoutées à tout logiciel anti-espions ou antivirus installé. Un script PowerShell a été fourni, lequel ajoutera automatiquement ces règles et polices locales. Si son exécution a échoué lors de l'installation, il peut être exécuté manuellement en observant les étapes suivantes.

Exécutez l'application Windows PowerShell avec des autorisations renforcées :



Une fois la fenêtre de commande PowerShell ouverte, naviguez vers le dossier d'installation du logiciel Data Manager d'AccuPoint®. Il s'agit par défaut du dossier C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0 :

Lancez la commande CD C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0

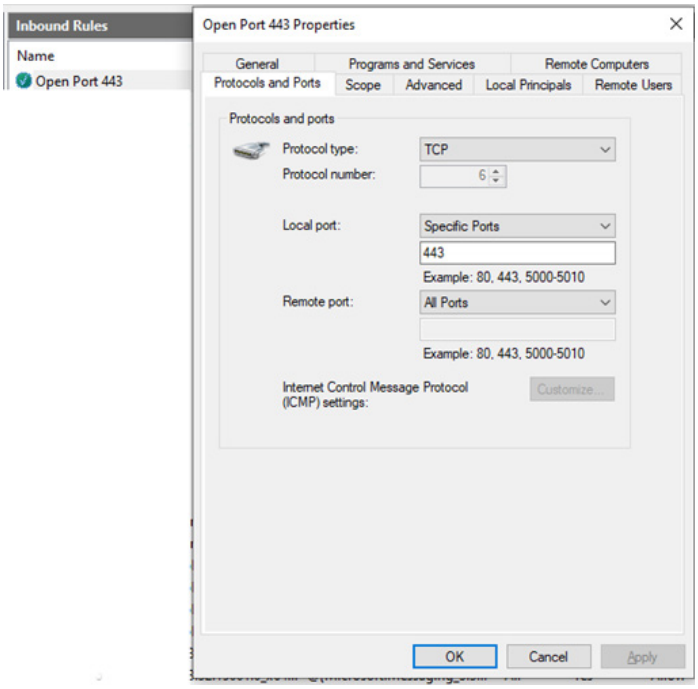
Exécutez le script securityConfig.ps1 PowerShell:

.\securityConfig.ps1

Le script tentera ensuite de mettre en œuvre les modifications de sécurité constatées, et produira un rapport une fois l'opération terminée. Essayez de configurer à nouveau le dispositif à l'aide du logiciel Data Manager, comme décrit dans la section Configuration du dispositif pour le Wi-Fi. Si vous ne parvenez pas à établir une connexion sécurisée avec le dispositif (l'icône de verrouillage n'apparaît pas), vérifiez manuellement les exclusions.

Examen des paramètres du pare-feu

Le script PowerShell devrait avoir installé les paramètres appropriés du pare-feu. Pour effectuer l'examen, ouvrez le programme de pare-feu installé sur le PC, vérifiez la section des règles d'entrée et recherchez la règle d'ouverture du port 443. Pour Windows Defender, double-cliquez sur la règle et basculez vers l'onglet Protocols and ports (Protocoles et ports).



Si cette règle ne figure pas dans l'application du pare-feu, elle peut être ajoutée manuellement, en utilisant l'interface utilisateur graphique (GUI) du pare-feu, ou en exécutant la commande suivante à partir d'une invite de commande avec des droits renforcés :

netsh advfirewall firewall add rule name="Open Port 443" dir=in action=allow protocol=TCP localport=443

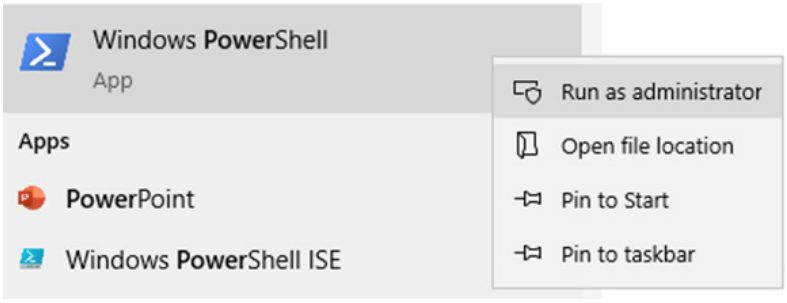
En cas d'échec, veuillez consulter la section de dépannage supplémentaire ci-dessous.

Dépannage supplémentaire

Le trafic réseau entre votre PC et le dispositif NEOGEN® AccuPoint® Advanced NG peut être bloqué pour de nombreuses raisons, lesquelles ne sont pas immédiatement évidentes. Il peut entre autres s'agir de la configuration de routeurs sans fil, de logiciels de sécurité s'exécutant sur le même réseau, de pare-feux locaux et de dispositifs de mise en réseau, ainsi que de règles relatives au réseau d'applications dans le cadre des réseaux avancés de fournisseurs tels que Cisco et VMWare.

Le script PowerShell précédemment mentionné répertorie les logiciels antivirus et de sécurité qui s'exécutent sur le PC du gestionnaire de données, mais il ne détecte pas tout et ne révèle pas les logiciels en cours de fonctionnement dans l'ensemble du réseau. Pour l'appeler, il convient de suivre les instructions précédentes.

Exécutez l'application Windows PowerShell avec des autorisations renforcées.



Une fois la fenêtre de commande PowerShell ouverte, naviguez vers le dossier d'installation du logiciel Data Manager d'AccuPoint. Il s'agit par défaut du dossier C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0.

Lancez la commande CD C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0

Exécutez le script securityConfig.ps1 PowerShell.

.\securityConfig.ps1

Un fichier texte contenant les informations éventuellement découvertes par le script PowerShell s'affiche. Cela vous aidera à modifier la configuration locale de votre logiciel de sécurité et à fournir des demandes plus détaillées à votre équipe de services informatiques.

Veuillez enregistrer les résultats pour les partager avec votre équipe de services informatiques, le cas échéant.

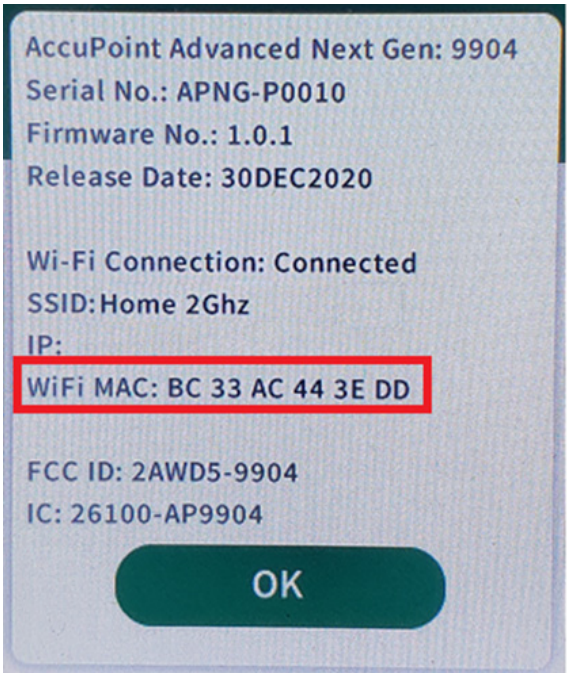
Les points suivants se rapportent à des problèmes courants et aux étapes permettant de les résoudre.

Le dispositif AccuPoint Advanced NG ne peut se connecter au Wi-Fi

Si, après avoir configuré le dispositif pour le Wi-Fi et l'avoir éteint puis rallumé, ce dernier ne parvient toujours pas à se connecter au Wi-Fi, il est fort probable qu'il soit bloqué par un élément de votre réseau. Les étapes de dépannage suivantes devraient permettre de résoudre les problèmes et de fournir des informations pouvant être utilisées par votre équipe de services informatiques.

Enregistrez le dispositif avec votre équipe de services informatiques ou un routeur local

Certains réseaux autorisent seulement les dispositifs reconnus à se connecter à eux en mode Wi-Fi. En d'autres termes, votre organisation doit enregistrer le dispositif comme un hôte autorisé. Cela s'effectue généralement en fournissant l'adresse MAC du dispositif. L'adresse MAC est répertoriée sur l'écran About (À propos) du dispositif. La capture d'écran suivante provient d'un dispositif AccuPoint® Advanced NG :

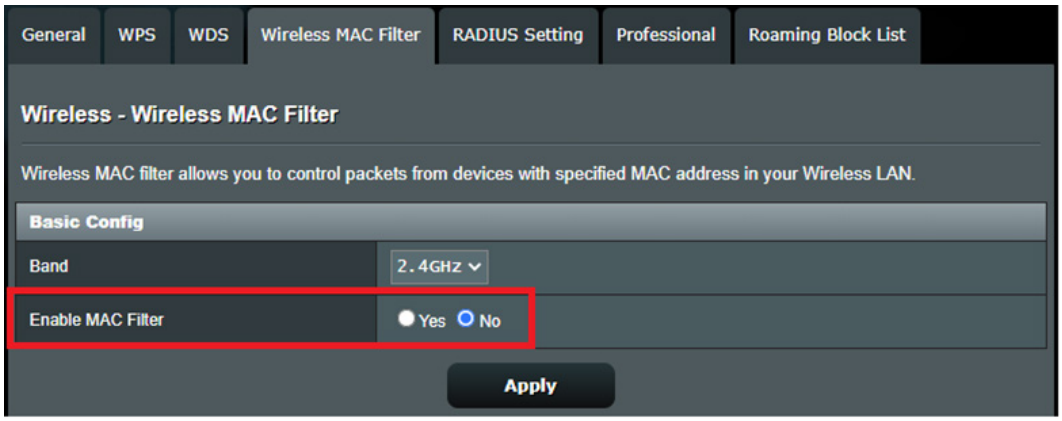


Consultez l'équipe des services informatiques de votre organisation si vous devez enregistrer votre dispositif, puis fournissez-lui l'adresse MAC figurant sur ce dernier.

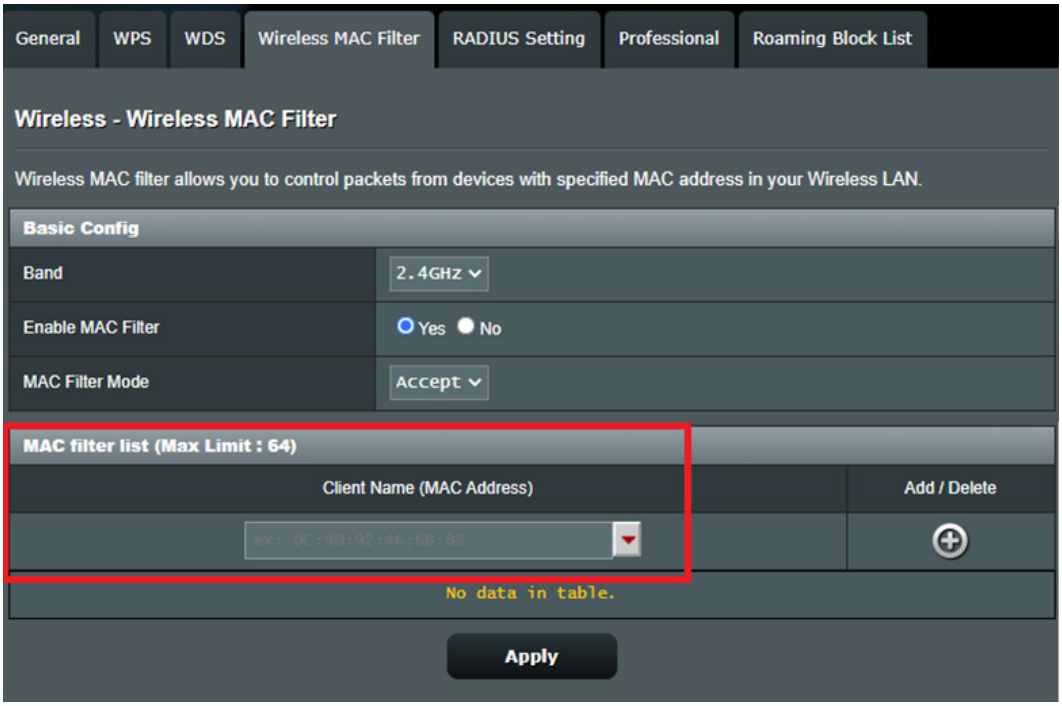
Si vous gérez votre propre routeur Wi-Fi, vous devez confirmer le fait que votre routeur local ne nécessite pas d'hôtes enregistrés. Cela dépendra de la marque et du type de votre routeur. Si possible, vous devez désactiver le filtrage des hôtes en fonction de l'adresse MAC sur votre routeur Wi-Fi.

Veuillez consulter la documentation de votre routeur avant d'effectuer des modifications.

Voici un exemple de capture d'écran d'un routeur Wi-Fi Asus :



Si un filtrage basé sur l'adresse MAC est nécessaire, assurez-vous que l'adresse de votre dispositif AccuPoint® Advanced NG est répertoriée ou ajoutez-la à la liste des hôtes autorisés.



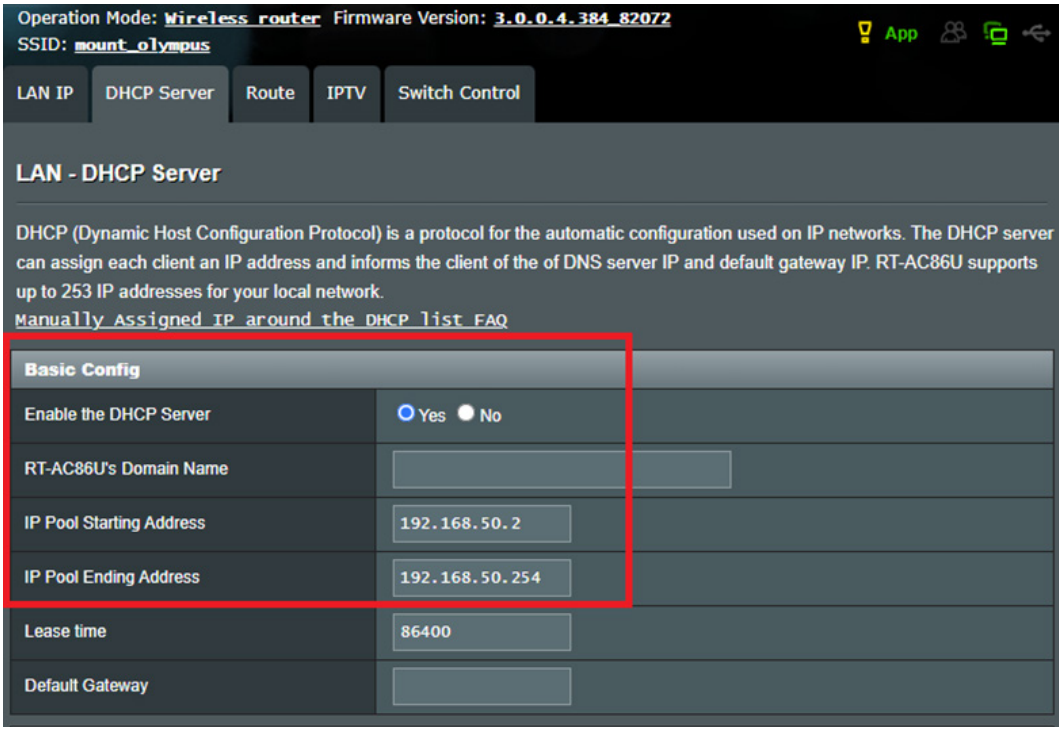
Vérifiez que les services DHCP sont disponibles

Dans la plupart des environnements réseau câblés et sans fil, les services DHCP (Dynamic Host Configuration Protocol) attribuent automatiquement une configuration réseau spécifique à tout hôte qui ne nécessite pas d'adresse réseau fixe. Si le protocole DHCP est désactivé, les PC et autres dispositifs ne pourront pas se connecter à la plupart des réseaux.

Le dispositif AccuPoint Advanced NG doit avoir accès aux services DHCP.

Dans un environnement d'entreprise, vous devez vérifier auprès de votre équipe de services informatiques que les services DHCP sont disponibles et activés pour le réseau sans fil auquel vous tentez de vous connecter avec le dispositif AccuPoint Advanced NG.

Si vous utilisez un point d'accès sans fil local, consultez la documentation de votre routeur pour vous assurer que le protocole DHCP est configuré. Dans l'écran suivant de configuration du routeur Asus, vous pouvez voir que le protocole DHCP est activé et que la plage d'adresses est attribuée aux hôtes connectés :



Si l'écran About (À propos) de votre dispositif AccuPoint® Advanced NG n'indique pas d'adresse IP dans la plage affichée sur votre routeur, le dispositif n'a pas pu communiquer correctement avec le service DHCP. Un échec du protocole DHCP se traduira par l'affichage d'une adresse 0.0.0.0 ou commençant par le chiffre 169. Essayez de redémarrer et/ou d'éteindre et de rallumer votre routeur avant de tenter de vous reconnecter à votre dispositif AccuPoint Advanced NG.

Si ces paramètres sont vierges sur votre routeur, veuillez consulter votre équipe de services informatiques pour obtenir les paramètres appropriés. Dans la mesure du possible, votre PC et votre dispositif doivent figurer dans la même plage d'adresses. Un mauvais paramétrage de cette plage peut générer des conflits d'adresses sur l'ensemble de votre réseau.

Vérifiez que le logiciel de sécurité du réseau autorise votre dispositif sur le réseau

Certaines organisations utilisent un logiciel de sécurité qui empêchent les dispositifs étrangers de se connecter au réseau local. Vous pouvez vérifier si le problème se pose en essayant de vous connecter avec un dispositif personnel qui ne s'est jamais connecté au réseau sans fil concerné, par exemple un téléphone ou une tablette. Si ces dispositifs ne parviennent pas à se connecter, vous devrez probablement demander à votre groupe de sécurité ou de services informatiques de créer une exception pour permettre au dispositif AccuPoint Advanced NG de se connecter au réseau.

Dans un environnement d'entreprise dans lequel vous devez saisir un nom d'utilisateur et un mot de passe pour accéder au réseau, vous aurez besoin d'une exception pour connecter votre dispositif AccuPoint Advanced NG, car ce dernier ne peut pas utiliser de compte séparé pour accéder à un réseau Wi-Fi. Veuillez consulter votre groupe local de services informatiques pour créer une exception.

Le filtrage du logiciel de sécurité est différent du filtrage basé sur l'adresse MAC/l'hôte qui se produit sur le routeur local ou le point d'accès sans fil.

Le dispositif AccuPoint® Advanced NG ne peut être atteint par une demande Ping émanant du PC

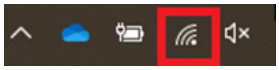
Si le dispositif se connecte avec succès, mais que votre PC ne peut pas envoyer de demande ping au dispositif, plusieurs raisons à cela sont possibles.

Vérifiez que votre PC est connecté au réseau en tant que réseau privé

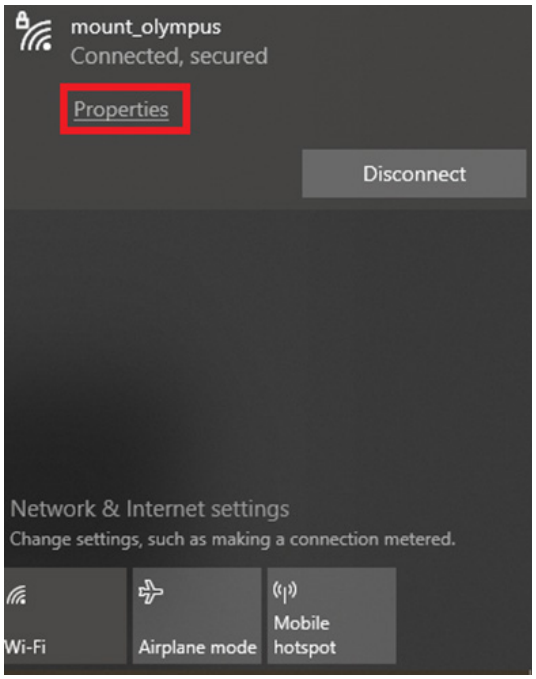
Si votre PC s'est connecté à un réseau public sans fil ou câblé, Windows 10 mettra en œuvre des protocoles de sécurité qui interféreront dans la communication entre le PC et le dispositif AccuPoint Advanced NG. Vous devrez vérifier que votre connexion réseau actuelle est considérée comme un réseau privé. Recherchez l'icône de mise en réseau dans l'angle inférieur droit de votre barre de tâches.

Un réseau câblé s'affichera comme suit :

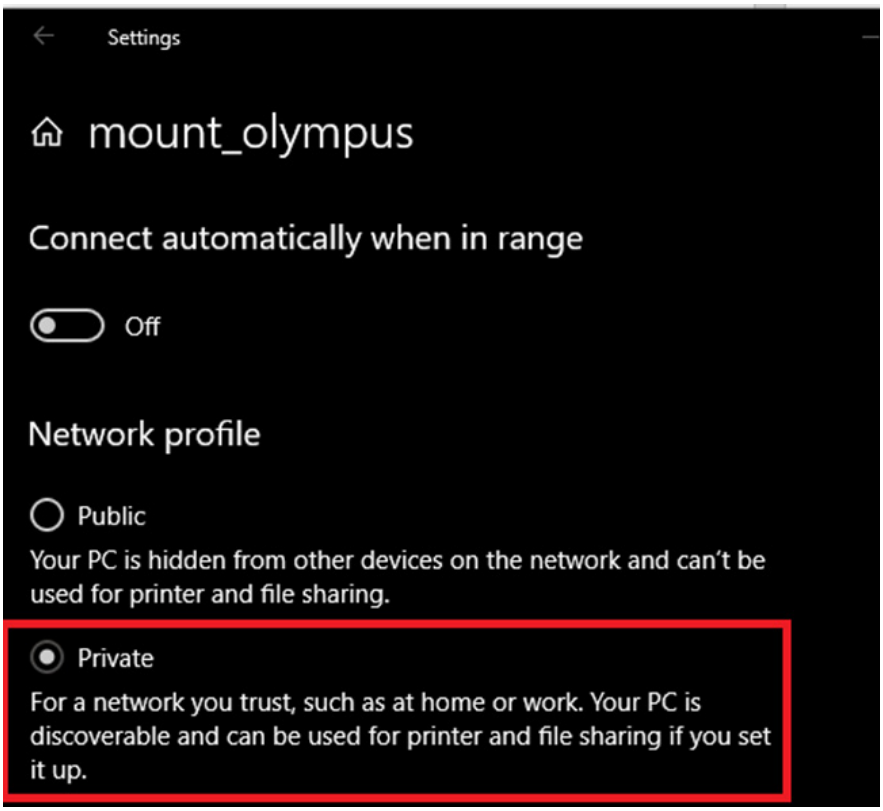
Un réseau sans fil s'affichera avec l'icône suivante :



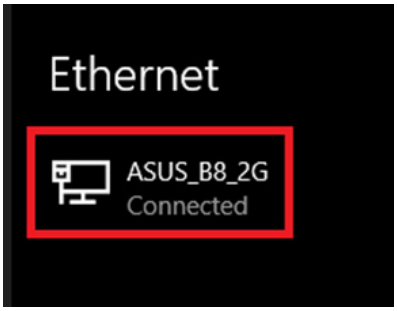
Cliquez sur l'icône de mise en réseau, puis sur Properties (Propriétés).



Dans l’écran qui s’affiche, assurez-vous que l’option Private (Privé) est sélectionnée.



Pour un réseau câblé, il se peut que vous aperceviez un écran intitulé Ethernet. Cliquez sur le nom de votre réseau câblé pour vérifier qu’il est défini comme privé.

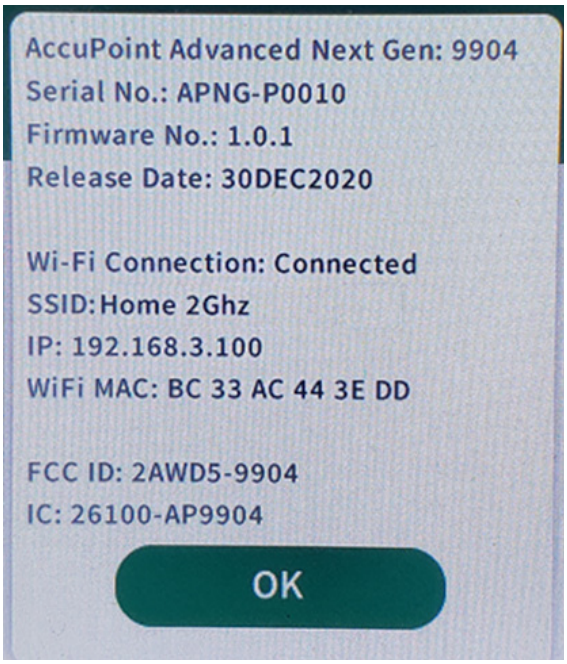


Vous ne devez utiliser un réseau câblé que si votre PC et le dispositif AccuPoint® Advanced NG sont considérés comme faisant partie du même segment de réseau local ou si l’ensemble de votre réseau permet aux dispositifs de se connecter via les segments de réseau. Vous devrez peut-être collaborer avec votre équipe de services informatiques pour autoriser les connexions entre les segments de réseau. Consultez la section suivante pour savoir comment procéder pour que le PC et le dispositif AccuPoint Advanced NG soient localisés sur le même segment de réseau.

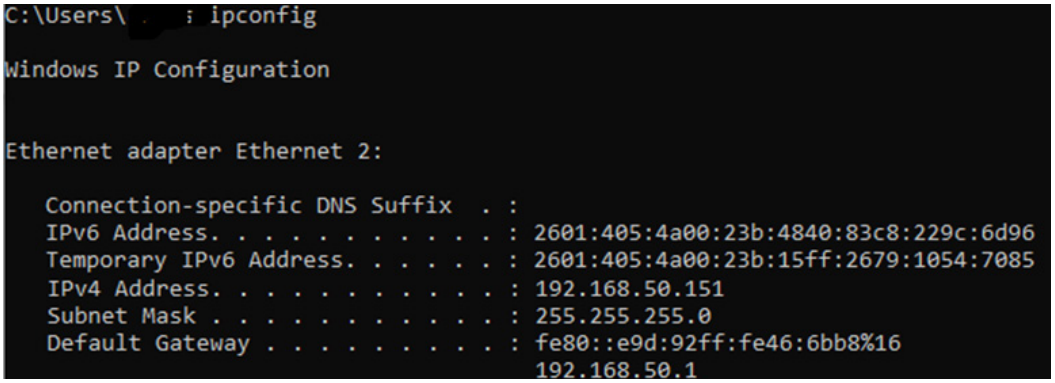
Vérifiez que le PC sur lequel est installé le logiciel Data Manager et le dispositif AccuPoint® Advanced NG se trouvent sur le même segment de réseau

Cela est nécessaire uniquement si votre organisation ne permet pas aux dispositifs de communiquer sur votre réseau.

Sur l'écran About (À propos), votre dispositif aura une adresse IP spécifique.



Dans ce cas, l'adresse réseau est 192.168.3.x. Les dispositifs appartenant à une plage d'adresses réseau différente peuvent ne pas être en mesure de détecter le dispositif AccuPoint Advanced NG. Depuis votre PC, vous devrez vérifier votre adresse réseau dans une fenêtre DOS ou CMD accessible via la commande IPCONFIG.



L'adresse répertoriée ici est 192.168.50.x. Dans de nombreux environnements d'entreprise, le PC et le dispositif AccuPoint Advanced NG ne pourraient pas partager le trafic réseau et les connexions.

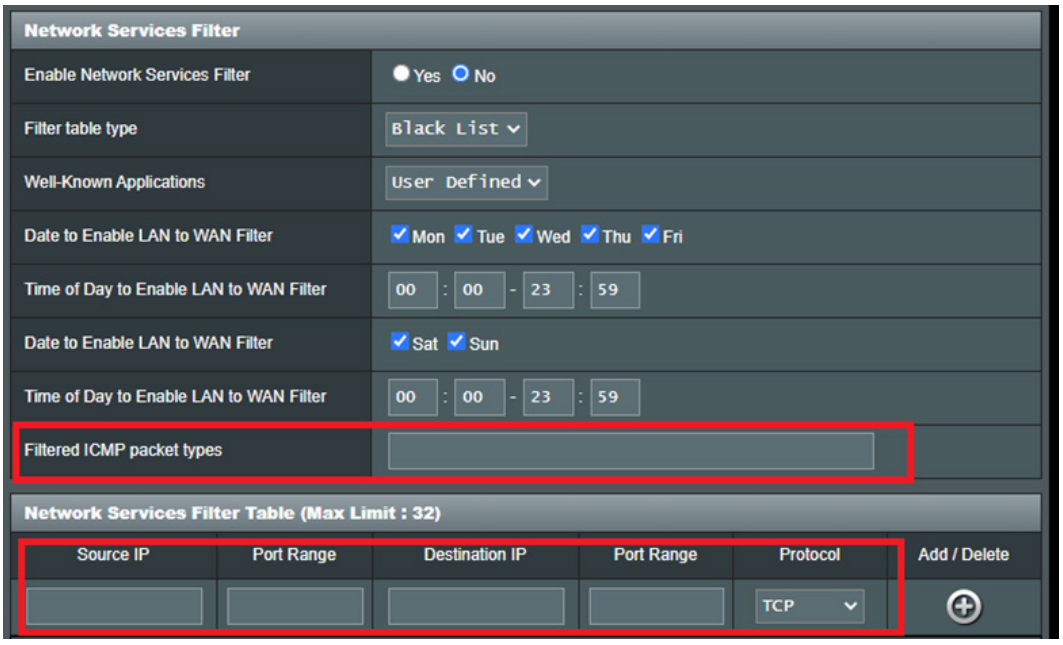
Vous devrez vérifier auprès de votre équipe de services informatiques quelles sont les restrictions en place pour que les dispositifs soient visibles les uns des autres sur le réseau, et ce sur l'ensemble des segments du réseau. La connexion de votre PC au même réseau sans fil que le dispositif AccuPoint Advanced NG peut offrir une solution rapide. Toutefois, cette connexion échouera si le PC ou le dispositif AccuPoint Advanced NG changent d'emplacement et se connectent à des points d'accès sans fil différents.

Vérifiez que votre réseau local autorise le trafic Ping

Certains réseaux bloquent tout trafic ping entre les hôtes. Ping utilise le protocole ICMP (Internet Control Message Protocol). De nombreux réseaux bloqueront tout trafic via ICMP en provenance d'un PC.

Veuillez consulter votre équipe de services informatiques pour vous assurer que le trafic ping ou ICMP entre hôtes est autorisé. Si tel n'est pas le cas, veuillez demander une exception. Cela rendra le dépannage de votre dispositif AccuPoint® Advanced NG plus simple et plus transparent.

Si vous gérez votre propre point d'accès sans fil, veuillez consulter votre documentation et vérifier que le trafic ping ou ICMP est autorisé. Vous devrez peut-être activer explicitement la méthode ping ou le protocole ICMP, ou supprimer les filtres de protocole.



Vérifiez que le logiciel de sécurité local ne bloque pas les demandes Ping sortantes

Certains logiciels de sécurité d'entreprise bloquent explicitement les demandes ping sortantes. Vous pouvez le confirmer en essayant d'envoyer une demande ping à des hôtes connus tels que www.google.com ou www.NEOGEN.com

```
C:\Users\    >ping www.neogen.com -4

Pinging www.neogen.com.cdn.cloudflare.net [104.18.16.70] with 32 bytes of data:
Reply from 104.18.16.70: bytes=32 time=28ms TTL=57
Request timed out.
Reply from 104.18.16.70: bytes=32 time=20ms TTL=57
Reply from 104.18.16.70: bytes=32 time=20ms TTL=57

Ping statistics for 104.18.16.70:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 28ms, Average = 22ms
```

Si cela fonctionne, recommencez avec un autre hôte ou PC sur votre réseau que vous savez connecté. La méthode la plus simple consiste à envoyer une demande ping à votre routeur. Lorsque vous lancez une commande ipconfig, celle-ci est listée comme la passerelle par défaut.

```
   Default Gateway . . . . . . . . . : fe80::e9d:92ff:fe46:6bb8%16
                                       192.168.50.1
```

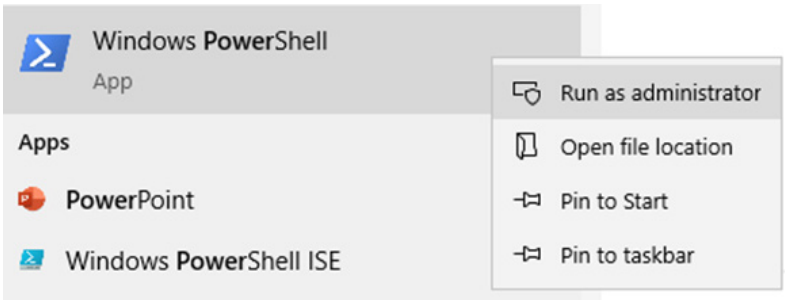
Vous devriez toujours pouvoir envoyer une demande ping à la passerelle.

```
C:\Users\      ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time<1ms TTL=64
Reply from 192.168.50.1: bytes=32 time<1ms TTL=64
Reply from 192.168.50.1: bytes=32 time<1ms TTL=64
Reply from 192.168.50.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Si vous ne pouvez pas envoyer de demande ping au routeur, le trafic ICMP est probablement bloqué. Vous devez alors vérifier que votre logiciel de sécurité autorise le trafic ICMP sortant.

Ajout de règles pour débloquer le trafic ICMP

Si vous avez mis en place une règle qui bloque le trafic ICMP, vous pouvez la débloquer en créant une règle en tant qu'administrateur sur le PC du gestionnaire de données. Exécutez l'application Windows PowerShell avec des autorisations renforcées.



Une fois que vous avez ouvert PowerShell, entrez le texte suivant pour activer le trafic ICMP Ipv4 et appuyez ensuite sur la touche Entrée.

```
netsh advFirewall Firewall add rule name="Allow PING IPv4" protocol=icmpv4:8,any dir=in action=allow
```

En option, si vous souhaitez activer le trafic ICMP Ipv6, saisissez le texte suivant et appuyez ensuite sur la touche Entrée.

```
netsh advFirewall Firewall add rule name="Allow PING IPv6" protocol=icmpv6:8,any dir=in action=allow
```

Veillez à ce que la sécurité de l'entreprise et le logiciel réseau autorisent le trafic entre votre PC et le dispositif AccuPoint® Advanced NG

De nombreux packs commerciaux de sécurité réseau bloquent le trafic entre les dispositifs du réseau, sauf autorisation expresse. Les tâches sont les suivantes :

1. CISCO Application Centric Infrastructure (ACI), qui peut disposer de règles visant à bloquer le trafic entre des hôtes non autorisés. Une nouvelle règle peut être nécessaire.
2. CrowdStrike, qui s'exécute localement en tant qu'agent et accepte les règles d'un serveur central, peut passer outre les modifications apportées au pare-feu Windows, bloquant ainsi le trafic ICMP et sécurisé vers le dispositif AccuPoint. Votre équipe de services informatiques devra peut-être ajouter des exceptions.
3. Rapid7, qui est semblable à CrowdStrike, peut nécessiter des dérogations aux règles pour autoriser le trafic.

Votre équipe de services informatiques peut émettre des règles Windows qui bloquent la communication entre le PC et le dispositif AccuPoint Advanced NG, notamment en empêchant les mises à jour des règles du pare-feu.

Vous pouvez utiliser la commande TRACERT, décrite précédemment dans ce document, pour identifier le chemin entre le PC du gestionnaire de données et le dispositif AccuPoint Advanced NG. Si la requête TRACERT échoue, le trafic est bloqué. Si la requête TRACERT réussit, mais que le PC et le dispositif AccuPoint Advanced NG ne peuvent pas communiquer, les ports utilisés par le dispositif et le PC sont bloqués. Une défaillance se manifeste de la façon suivante :

Tracing route to nosferatu [192.168.50.219]
over a maximum of 30 hops:

1 buho [192.168.50.151] reports: Destination host unreachable.

Trace complete.

Veillez à ce que les pare-feux du réseau ne bloquent pas le trafic réseau

Certains réseaux sont scindés par des pare-feux internes afin de protéger les zones sensibles, telles que les laboratoires et les espaces de production. Des règles ou des exceptions de pare-feux peuvent être nécessaires si le trafic réseau entre votre PC et le dispositif AccuPoint Advanced NG doit traverser un ou plusieurs pare-feux. La commande TRACERT permet également de diagnostiquer un problème de pare-feu.

Veuillez consulter votre équipe de services informatiques pour savoir si votre PC et le dispositif AccuPoint Advanced NG doivent franchir un ou plusieurs pare-feu pour communiquer.

Les transferts ne peuvent pas être initiés vers le dispositif AccuPoint Advanced NG

Les causes les plus probables de ce problème sont le blocage du trafic sur le port 80 vers le dispositif AccuPoint Advanced NG, ou le blocage du trafic sur le port 443 entre le dispositif et le PC.

Pour lancer un transfert depuis le PC vers le dispositif AccuPoint Advanced NG, le gestionnaire de données envoie un message au dispositif AccuPoint Advanced NG sur le port 80. Le dispositif se connecte ensuite au PC via le port 443, et transfère en toute sécurité les informations via TLS. Le blocage du trafic sur l'un de ces ports perturbera la synchronisation des données, y compris la transmission de plans du site par la technologie push.

Le trafic sur le port 80 est interrompu entre le PC et le dispositif AccuPoint® Advanced NG

La plupart des solutions utilisées pour résoudre les problèmes de ping évoqués ci-dessus peuvent également être utilisées entre le PC et le dispositif. Le PC établit le contact avec le dispositif sur le port 80. Ce type de trafic est souvent signalé par les logiciels et les dispositifs de sécurité.

Des interférences supplémentaires peuvent être provoquées par des agents de sécurité Internet qui font en sorte de tout simplement bloquer le trafic sortant sur le port 80. Bien qu'aucune donnée sensible ne soit transférée sur ce port, il est généralement considéré comme un port non sécurisé.

Le dispositif AccuPoint Advanced NG doit recevoir un message d'activation lui indiquant de lancer des communications sécurisées avec le PC sur le port 80.

Effectuez la première vérification indiquée dans la section Le dispositif AccuPoint Advanced NG ne peut être atteint par une demande Ping émanant du PC pour vous assurer que votre PC est connecté à son réseau local en tant que réseau privé. En l'absence de problème, veuillez continuer avec les étapes suivantes.

Pour vérifier la survenue d'un problème, la meilleure façon de procéder est d'utiliser la commande PowerShell Test-NetConnection. L'exemple suivant montre comment tester Google.com pour le port 443 :

```
Pinging www.google.com [172.217.6.4] with 32 bytes of data:
Reply from 172.217.6.4: bytes=32 time=21ms TTL=116
Reply from 172.217.6.4: bytes=32 time=21ms TTL=116

Ping statistics for 172.217.6.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 21ms, Average = 21ms
Control-C
PS C:\WINDOWS\system32> Test-NetConnection 172.217.6.4 -Port 443


ComputerName     : 172.217.6.4
RemoteAddress    : 172.217.6.4
RemotePort       : 443
InterfaceAlias   : Ethernet 2
SourceAddress    : 192.168.50.151
TcpTestSucceeded : True
```

La commande pour tester le dispositif AccuPoint Advanced NG serait la suivante :

Test-NetConnection <ip of device> -Port 80

Si vous constatez un échec, alors le port 80 est bloqué. Travaillez avec votre équipe de services informatiques pour résoudre ce problème. Vous pouvez avoir besoin d'exceptions pour le PC du gestionnaire de données ou le dispositif AccuPoint Advanced NG.

Le trafic sur le port 443 ne parvient pas à passer du dispositif AccuPoint Advanced NG au PC

Le PC du gestionnaire de données utilise le logiciel Data Manager pour héberger un service léger sur le port 443 via TLS.

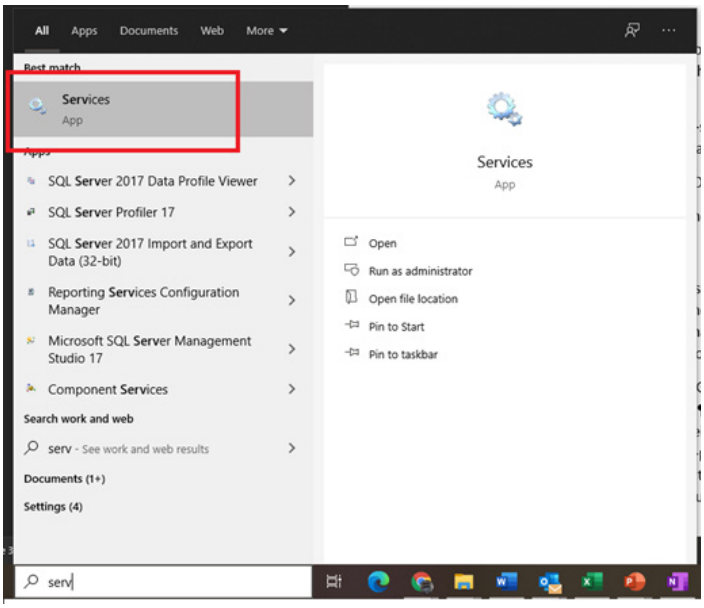
La plupart des problèmes entravant le trafic du port 443 sont résolus en mettant en œuvre les solutions énumérées ci-dessus dans la section consacrée au blocage des demandes ping. Cependant, les règles seraient configurées différemment. Autoriser le trafic SSL entrant sur le port 443 vers votre PC peut nécessiter un ou plusieurs des éléments suivants :

- Ajuster les règles de pare-feu du réseau interne.
- Ajuster les règles du logiciel de sécurité de l'entreprise.
- Ajout de règles ou d'exceptions d'assouplissement du contrôle réseau, comme ACI.
- Ajout de règles de groupe Windows pour autoriser les modifications du pare-feu local.

Vous devez également vérifier que le PC du gestionnaire de données est en situation d'écoute sur le port 443 en utilisant la commande :

netstat -an

Si le port 443 n'apparaît pas en écoute dans le résultat de cette commande, veuillez redémarrer le PC et recommencer le test. Si le problème persiste, consultez la liste des services du PC et vérifiez que le logiciel Data Manager est en cours d'exécution sur le PC.



Si le service est en cours d'exécution et que la commande netstat montre que le PC du gestionnaire de données est en situation d'écoute sur le port 443, vous aurez besoin d'un deuxième PC pour tester l'accès à ce port. Veuillez émettre la commande suivante depuis un autre PC en utilisant PowerShell vers le PC du gestionnaire de données :

Test-NetConnection <ip of Data Manager PC> -Port 443

Si cette commande échoue, suivez les recommandations de dépannage précédentes.

Résumé

Lorsqu'ils sont correctement configurés, sans interférence de signal, les transferts de données entre le PC du gestionnaire de données et le dispositif AccuPoint® Advanced NG doivent être rapides et fiables. Cependant, lors de l'arrivée d'un nouveau dispositif dans un réseau d'entreprise, le trafic peut être bloqué de plusieurs façons. Veuillez vous rappeler ce qui suit et vous référer aux sections précédentes de ce guide pour dépanner ou résoudre ces problèmes :

1. Configurez correctement le dispositif AccuPoint Advanced NG pour mettre en place la connectivité Wi-Fi, en utilisant une connexion USB entre le dispositif et le PC de gestion des données.
2. Exécutez le script PowerShell fourni, qui configurera le pare-feu local et le logiciel de sécurité sur le PC du gestionnaire de données, ou faites des recommandations à votre équipe de services informatiques.
3. Si le dispositif ne peut pas se connecter à votre réseau Wi-Fi, cela signifie que le point d'accès sans fil, les pare-feux internes, les logiciels de sécurité ou d'autres applications de sécurité le bloquent.
4. Si le dispositif peut se connecter au Wi-Fi, mais que l'icône de verrouillage ne s'affiche pas, cela signifie que votre PC ne peut pas accepter les connexions entrantes sur le port 443.
    a. Vérifiez que le logiciel Data Manager est en cours d'exécution sur votre PC et qu'il est en situation d'écoute sur le port 443.
    b. Exécutez les autres étapes de dépannage.
5. Si le dispositif peut obtenir une icône de verrouillage et que les transferts de données (synchronisations) peuvent être initiés depuis le dispositif mais pas depuis le PC, le trafic réseau entre le port 80 du PC et le dispositif AccuPoint Advanced NG est bloqué.

Ce guide sera mis à jour en fonction des besoins. C'est le cas notamment lorsque des informations de configuration nouvelles ou mises à jour sont disponibles, ou des conseils de dépannage supplémentaires seraient utiles.