AccuPoint® Advanced Next Generation: guía de redes de wifi

Configuración y solución de problemas

NEOGEN®
NEOGEN.com

Contenido

AccuPoint® Advanced NG: resumen de requisitos de red

Para conectarse a una red de wifi, el AccuPoint® Advanced NG es compatible con:

- 802.11 b/g/n
- WPA2/WPA Personal y Enterprise
- WEP
- IPV4
- Rendimiento de red de hasta 72 MBs
- Alcance de señal de hasta 450 m, que se ve afectado por las superestructuras de los edificios, los obstáculos físicos y otras interferencias de la señal.

El dispositivo no es compatible con la autenticación RADIUS u otras formas de autenticación de red. En los entornos corporativos que requieren autenticación basada en el host o en el usuario, se recomienda utilizar el filtrado de direcciones MAC en lugar de los dispositivos AccuPoint Advanced NG. La dirección MAC del dispositivo está disponible en la pantalla sobre cada dispositivo AccuPoint Advanced NG. En algunos entornos, el filtrado MAC puede requerir un nuevo SSID o una red de wifi independiente.

Se recomienda encarecidamente que se habilite el registro de host DHCP (DNS) en la red a la que se conectarán la PC gestora de datos y el dispositivo AccuPoint Advanced NG. Cuando el wifi está activado, el dispositivo y la PC donde se ejecuta el software Data Manager deben poder comunicarse entre sí a través de la red, con cualquiera de los dos host al iniciar una conexión. Dado que la PC y el dispositivo pueden moverse entre segmentos de red o puntos de acceso, lo cual puede resultar en un cambio de direcciones IP, la capacidad de conectarse usando la PC y el nombre de sistema host del dispositivo será una capacidad esencial, a fin de acomodar los cambios dinámicos de dirección IP. Si la PC y el dispositivo AccuPoint Advanced NG no pueden utilizar nombres de sistema host para conectarse y la dirección IP de la PC o del dispositivo cambia, es muy probable que pierdan la capacidad de comunicarse hasta que el dispositivo AccuPoint Advanced NG se vuelva a configurar a través de una conexión USB.

El dispositivo AccuPoint Advanced NG se comunica de forma segura con la PC donde se ejecuta el software Data Manager mediante un certificado TLS autofirmado. La conexión TLS se aloja en la PC mediante el componente de software del servicio Data Manager. Esta conexión se establece cuando el dispositivo envía o recibe datos del software Data Manager, pero no se mantiene de forma constante. Tras un breve periodo de inactividad, el dispositivo abandona la conexión para evitar problemas de estabilidad en ella.

Cuando el dispositivo AccuPoint Advanced NG inicia una conexión, todas las comunicaciones se realizarán a través de TLS en el puerto 443 de la PC. Sin embargo, cuando el usuario desea enviar un plan de sitio o iniciar de otro modo las comunicaciones de red con el dispositivo AccuPoint Advanced NG, la PC debe enviar primero una señal al dispositivo a través del puerto 80 a un servicio web que se está ejecutando en el AccuPoint Advanced NG. Cuando el dispositivo reciba esta solicitud de servicio web, cerrará el mismo e iniciará una conexión segura con la PC gestora de datos. Cuando la conexión segura se haya interrumpido, el dispositivo volverá a poner a disposición el servicio web basado en HTTP.

Para los entornos corporativos, puede que sea necesario crear excepciones de política de red que permitan el tráfico a través del puerto 80 hacia el dispositivo AccuPoint® Advanced NG desde la PC gestora de datos, y a través del puerto 443 desde el dispositivo hacia la PC. Tanto la PC como el dispositivo pueden utilizar solicitudes ICMP para hacer ping entre sí, por lo que el tráfico ICMP entre el dispositivo AccuPoint Advanced NG y la PC también debe estar habilitado.

Dentro de Windows, en la PC del gestor de datos, el software Data Manager intentará reconfigurar el firewall local y la configuración de seguridad en el momento de la instalación para adaptarse a sus requisitos de acceso. Esto no siempre tiene éxito, depende de las políticas de grupo y el software en la PC donde se instala el software.
Los requisitos básicos de la red incluyen los siguientes:

1. La conexión de red en la PC que se use para conectarse a AccuPoint Advanced NG debe configurarse para que sea privada. En Windows, todo el tráfico entrante que inicia un dispositivo externo se bloquea en una conexión pública.
2. El firewall local en la PC del administrador de datos debe estar configurado para admitir:
    a. Tráfico entrante en el puerto 443
    b. Tráfico saliente en el puerto 80 (HTTP estándar).
    c. Tráfico de ICMP saliente y entrante
3. El software de seguridad que se ejecuta en la PC y las políticas de grupo de Windows deben permitir que los siguientes ejecutables accedan a la red:
    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

Es posible que se requieran excepciones adicionales cuando se actualice el software de Data Manager. Se brindarán boletines técnicos cuando se produzcan estos cambios.

Muchos entornos corporativos dependen de una protección de terminales y softwares de seguridad centralizado, como CrowdStrike, que requieren excepciones de políticas específicas. Del mismo modo, las políticas de grupo de Windows también pueden interferir con la conectividad de los dispositivos y las PC.

Estos requisitos de configuración deben probarse después de que se haya instalado el software Data Manager y se haya configurado un dispositivo AccuPoint Advanced NG para el acceso a wifi. Consulte las instrucciones y recomendaciones para la solución de problemas a continuación.

Si también se utiliza NEOGEN® Analytics, se debe permitir el tráfico local (solo en la PC del gestor de datos) en el puerto 80. Sin embargo, este puerto no necesita estar expuesto a la red en general. Consulte la documentación de NEOGEN Analytics para conocer los requisitos adicionales de acceso a la red.

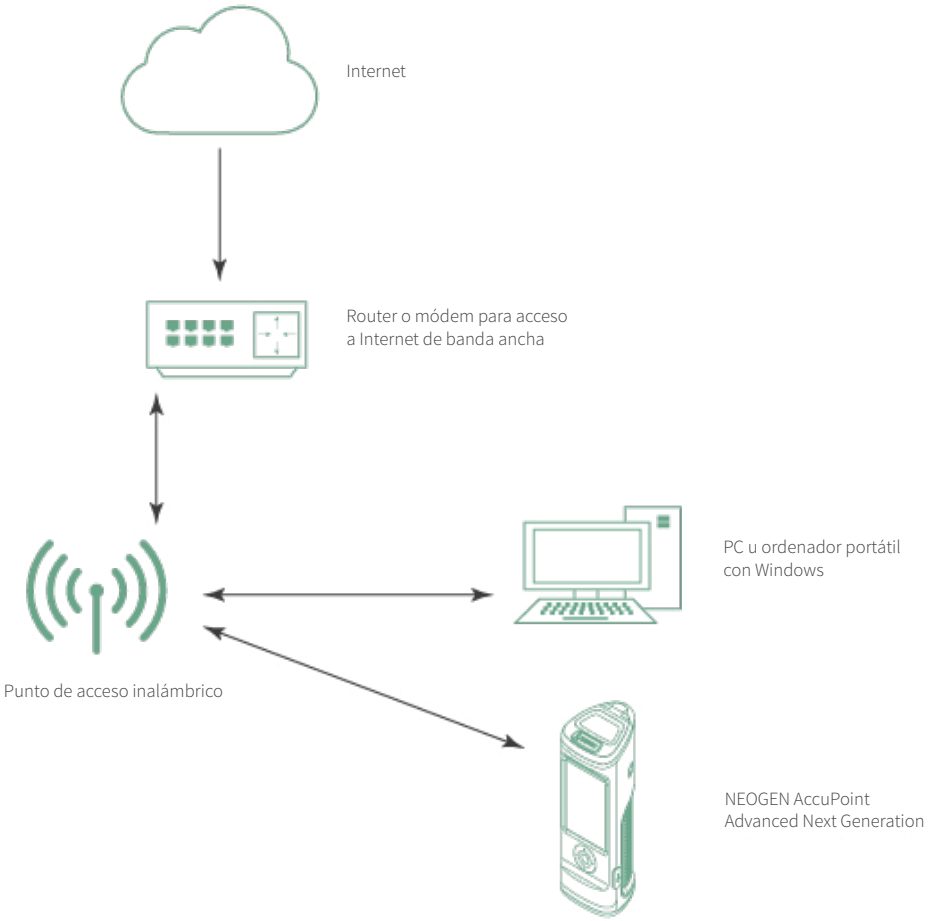
Para modificar las configuraciones en la PC que ejecuta el software Data Manager, el usuario que realiza estos cambios debe tener derechos de administrador. Esto puede ser una autorización temporal, si es necesario. Algunas organizaciones pueden trasladar los cambios a las PC locales. Sin embargo, depurar los problemas de conexión es difícil si no se tienen derechos de administrador local. Una de las herramientas proporcionadas junto con el software Data Manager es un script de PowerShell, que proporcionará cierta información de diagnóstico.

Antes de comenzar

Conozca su entorno de red

Simple

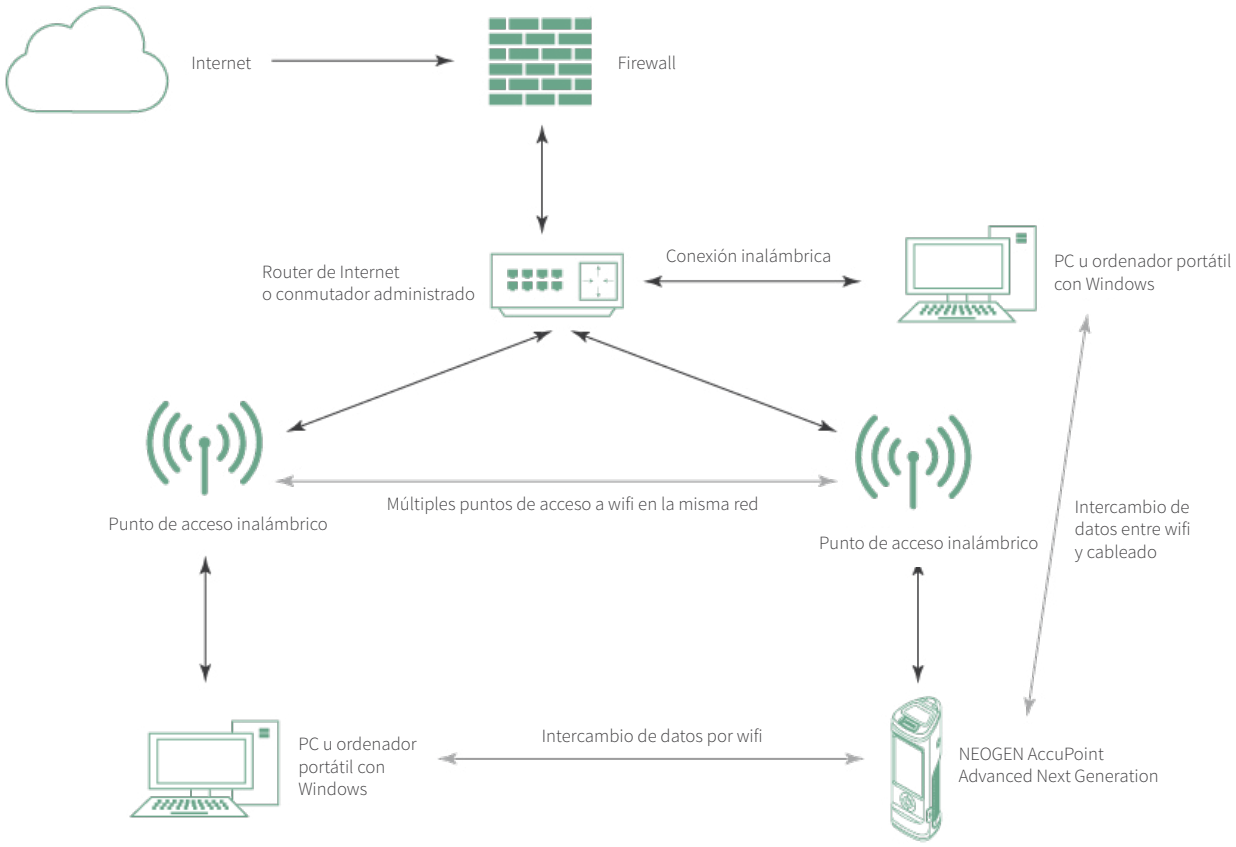
Hay sitios de red simples en muchas empresas individuales o espacios de trabajo aislados. En general, se conforma de una conexión a Internet y un único punto de acceso inalámbrico como el siguiente:



En esta configuración de red simple, lo principal será asegurarse de que el punto de acceso inalámbrico (WAP) esté configurado para permitir que el dispositivo AccuPoint® Advanced NG se conecte a la red local. En la guía de resolución de problemas, se analizan diferentes formas de modificar el WAP para permitir nuevas conexiones. En la PC o el ordenador portátil, las cuestiones principales serán garantizar que la conexión inalámbrica local, el firewall y el software de seguridad permitan las conexiones entrantes.

Organización

Un sitio a nivel de organización puede tener firewalls y un software de seguridad más avanzado con múltiples puntos de acceso inalámbricos, como se ve en este diagrama:



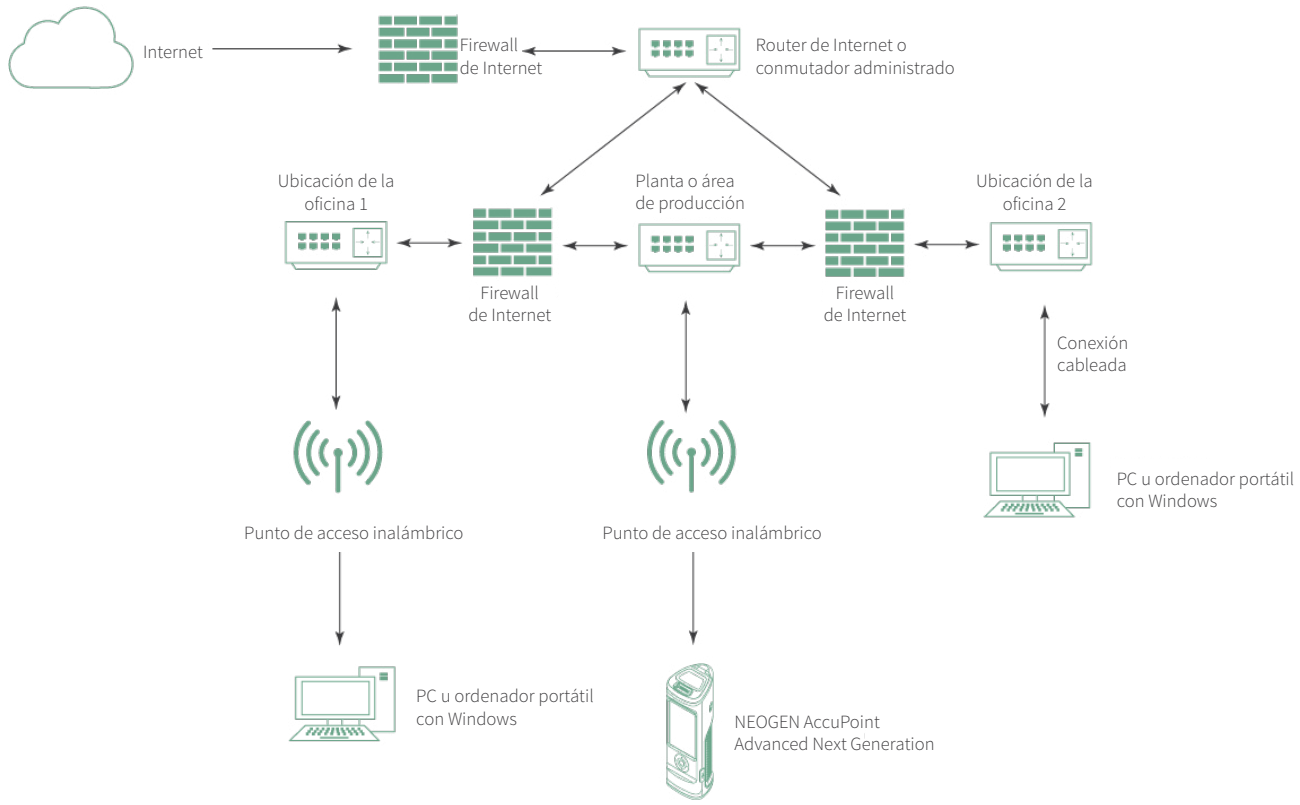
La mayoría de los usuarios con este tipo de configuración de red necesitarán la ayuda de su grupo local de servicios informáticos para configurar correctamente el dispositivo y la PC que aloja el software Data Manager. Esto incluye lo siguiente:

1. Garantizar que el AccuPoint® Advanced NG pueda acceder a la red de wifi.
2. Garantizar que la PC gestora de datos y el dispositivo AccuPoint Advanced NG puedan verse mutuamente en la red.
3. El software de supervisión de seguridad permite el intercambio de datos entre el AccuPoint Advanced NG y la PC gestora de datos.

La guía de resolución de problemas detalla cómo identificar los problemas y qué compartir con el grupo de servicios de TI para garantizar que todos los componentes estén bien configurados.

Empresa

Un sitio empresarial suele tener segmentación de red, configuraciones avanzadas de wifi y restricciones en los dispositivos para lo que se permite en sus redes. Esto puede incluir múltiples firewalls y conmutadores. A continuación, se presenta un ejemplo muy simplificado de una red empresarial.



En un entorno de red complejo como este, la conexión del dispositivo AccuPoint® Advanced NG a través de wifi a la PC del gestor de datos puede requerir varias tareas con el grupo de servicios de TI, las cuales incluyen las siguientes:

1. Modificaciones en las políticas de grupo de Windows que permitirán las conexiones de red entrantes, así como cambios en el firewall local y en el software de seguridad de la PC del gestor de datos.
2. Permisos para instalar el software Data Manager y para modificar la configuración de la PC local.
3. Excepciones a las reglas de acceso a la red para permitir que el dispositivo AccuPoint Advanced NG acceda a la red de wifi.
4. Modificación de las reglas del firewall interno para permitir el tráfico de red entre la PC del gestor de datos y el AccuPoint Advanced NG.
5. Actualizaciones de las políticas del software de seguridad para permitir el intercambio de datos con el AccuPoint Advanced NG.

Los entornos de alta seguridad pueden requerir que se establezca un nuevo SSID de wifi solo para las comunicaciones de AccuPoint Advanced NG.

Comprobación de la intensidad de la señal wifi

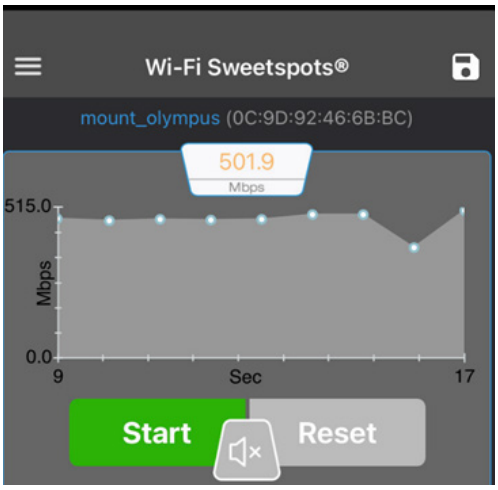
Uno de los problemas más difíciles de resolver durante el funcionamiento del dispositivo AccuPoint Advanced NG es la interferencia del wifi o una intensidad de señal débil. Como ya se ha mencionado, el dispositivo tiene una radio de wifi de menor potencia para mejorar la duración de la batería y mantener la portabilidad. Desafortunadamente, esto significa que el dispositivo puede ser más susceptible a la pérdida de señal en áreas operativas con una señal

de wifi débil o interferencias. La mejor manera de identificar los problemas de wifi por adelantado es solicitar un estudio de la señal de wifi en las zonas operativas en las que se espera recoger
y transmitir datos de prueba. Sin embargo, para algunas organizaciones, esta puede ser una petición difícil o que lleve demasiado tiempo.

Por suerte, existen herramientas de prueba de wifi que permitirán que la mayoría de los usuarios realicen un análisis muy sencillo del wifi, que se basa en el rendimiento de la transmisión de la red. Cualquier usuario con un teléfono inteligente o una tableta con conexión de wifi puede instalar aplicaciones que comprueben la intensidad de la señal. Las siguientes aplicaciones están disponibles para iOS (Apple) y para Android:

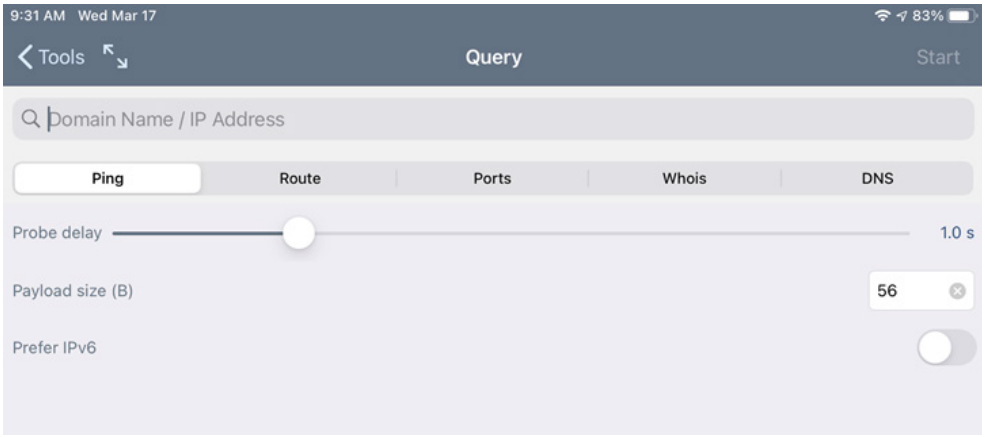
- Wi-Fi SweetSpots (recomendada, gratuita)
- Network Analyzer (también gratuita, pero más compleja)
- Network Analyzer Pro (pequeña comisión, con buenas características)

Consulte la captura de pantalla de la aplicación Wi-Fi SweetSpots:



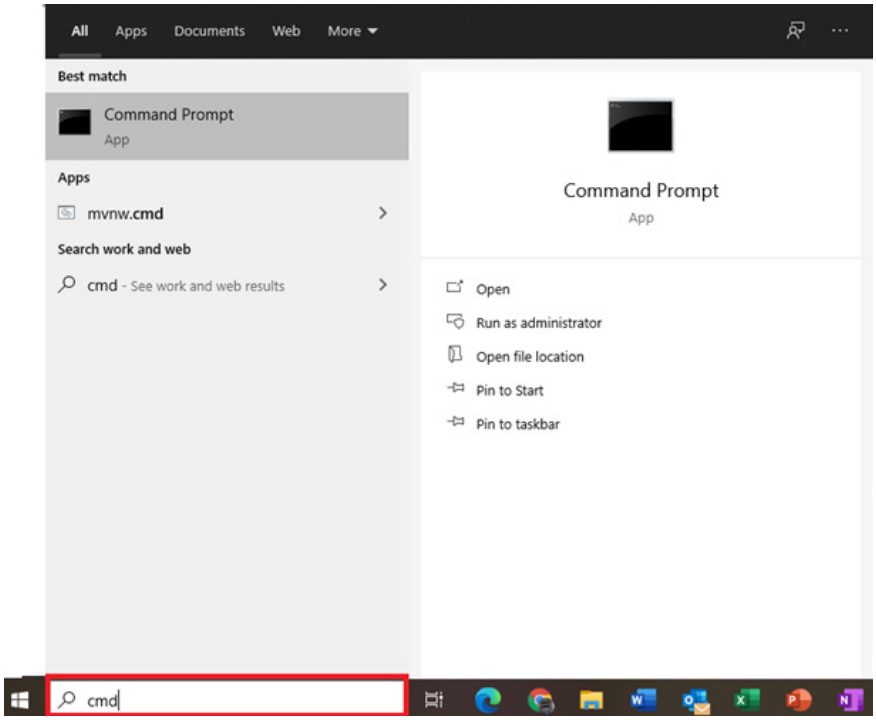
Wi-Fi SweetSpots hace un seguimiento del rendimiento del wifi. Cuando la tasa de transferencia de la red disminuye, quiere decir que está entrando en un lugar con una señal de wifi más débil o con mayores niveles de interferencia. Si el rendimiento de la red disminuye más del 50 %, es probable que el AccuPoint® Advanced NG experimente problemas de comunicación en la red.

Network Analyzer es para los usuarios con más experiencia en redes que deseen ejecutar diagnósticos adicionales, como el rastreo de rutas, la verificación de DNS, los pings de red, etc. Vea la siguiente captura de pantalla de Network Analyzer Pro como ejemplo:



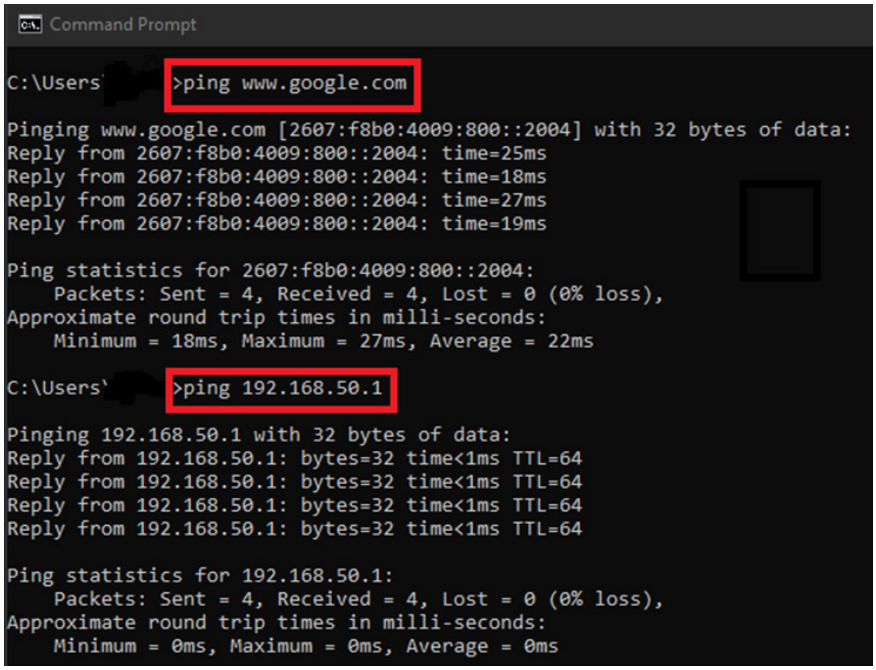
Herramientas de diagnóstico de red para usuarios

Windows 10 les proporciona a los usuarios varios comandos útiles que se pueden ejecutar desde el escritorio del usuario. Aquellos que no estén familiarizados con cómo lanzar una ventana de petición de comando encontrarán más información en la siguiente captura de pantalla. Si escribe CMD en el cuadro de búsqueda de Windows, verá: Ping

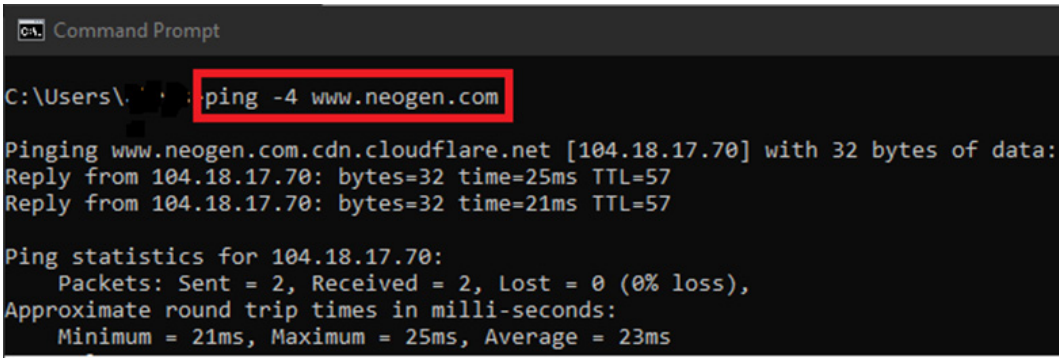


Ping

Este comando sencillo es uno de los más útiles para identificar si la PC gestora de datos puede acceder al dispositivo AccuPoint® Advanced NG. Sin embargo, hay algunos matices. El comando básico es simplemente ping <some host> o IP:



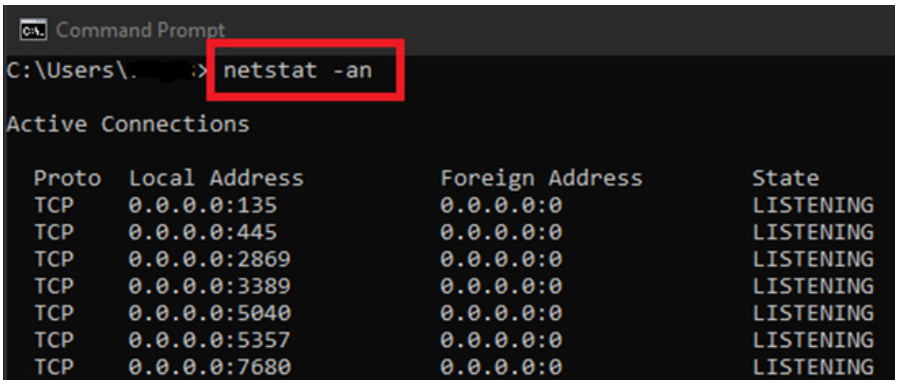
El primer comando se utiliza para hacer ping a www.google.com. El segundo se utiliza para hacer ping a una dirección en la misma red. Tenga en cuenta que las direcciones de la primera petición de ping son IPv6. Para forzar un ping a usar IPv4, puede que tenga que modificar el comando e incluir -4, como se muestra a continuación:



Los tiempos de ping son importantes. En una red local, el tiempo que se tarda en llegar a un host no debería ser superior a 10 ms. El grupo de servicios IT local debe abordar todo lo que tarde más. Para las direcciones en Internet, los tiempos de ping deben ser de 120 ms o menos. Los tiempos de ping superiores pueden ocurrir con hosts que se encuentren geográficamente distantes. Sin embargo, los tiempos de ping lentos con servicios comunes como Google o Amazon pueden indicar una conexión a Internet lenta. Dado que el AccuPoint® Advanced NG y la PC gestora de datos se comunican en la misma red, una conexión a Internet lenta no será un factor que afecte el funcionamiento del dispositivo ni a la transmisión de datos. Sin embargo, una conexión a Internet lenta puede inhibir la posibilidad de descargar actualizaciones del gestor de datos o del firmware del dispositivo.

Netstat

Este comando mostrará qué puertos están asociados con una PC y a qué puertos está conectada activamente. Para el AccuPoint Advanced NG, la PC gestora de datos debe estar asociada al puerto 443. El comando y la salida son los siguientes:



La dirección local y el puerto son importantes:

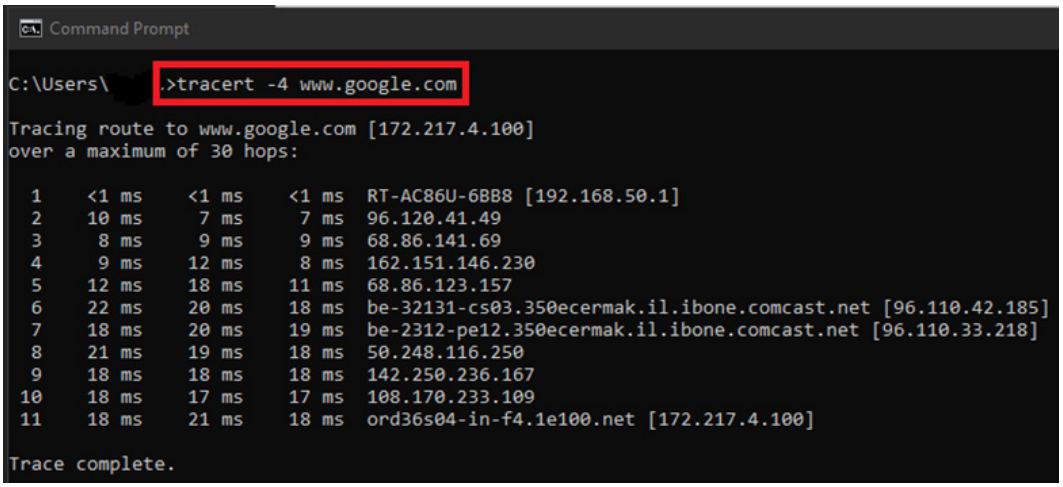
Dirección: ###.###.###.###:<Puerto: ###>

Puede haber varias decenas de entradas, según el software y los servicios que se ejecuten en una PC.

La salida en la captura de pantalla para 0.0.0.0:445 muestra que esta PC está aceptando conexiones en el puerto 445 en todos sus adaptadores de red. Este comando ayudará a identificar si el servicio Data Manager se está ejecutando y está listo para aceptar conexiones desde el dispositivo AccuPoint Advanced NG.

TRACERT

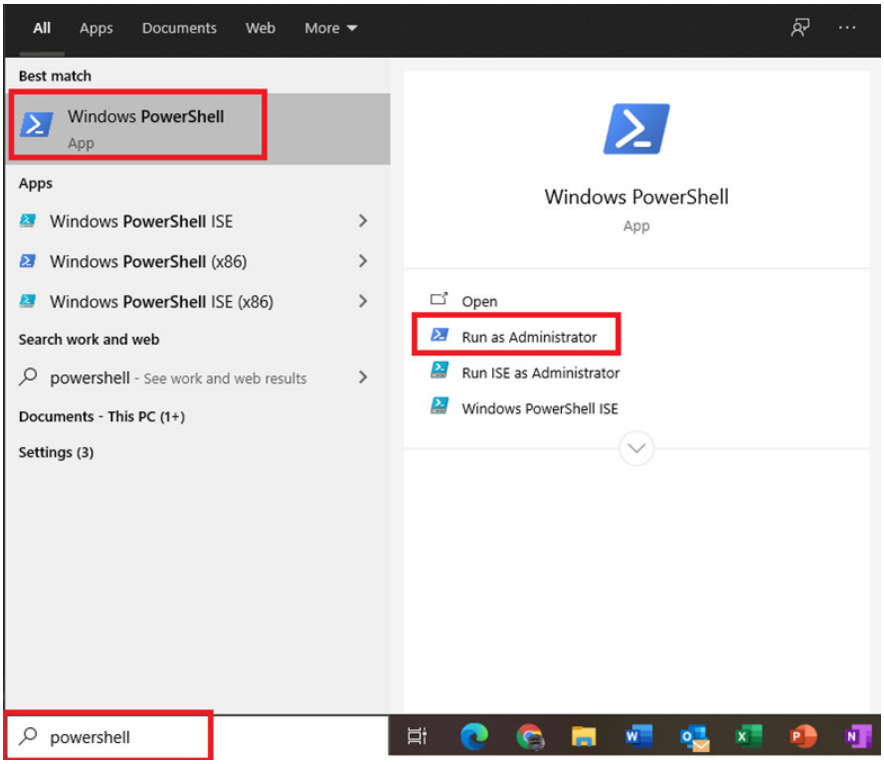
El TRACERT mostrará la ruta de un host a otro a través de una red. Cada dirección intermedia es un salto de red. Este comando ayudará a identificar qué conmutadores, firewalls y dispositivos de red debe atravesar el tráfico desde la PC gestora de datos hasta el dispositivo AccuPoint® Advanced NG. El siguiente ejemplo muestra la ruta entre esta PC y el host www.google.com. En una red local, debería haber entre 1 y 6 saltos.



Hop #1 es el punto de acceso inalámbrico local. Cada salto que sigue es un enrutador, un conmutador o un firewall que el tráfico de la red debe atravesar antes de alcanzar su objetivo de 172.217.4.100. El parámetro 4 garantiza que el tráfico utilice el protocolo IPv4.

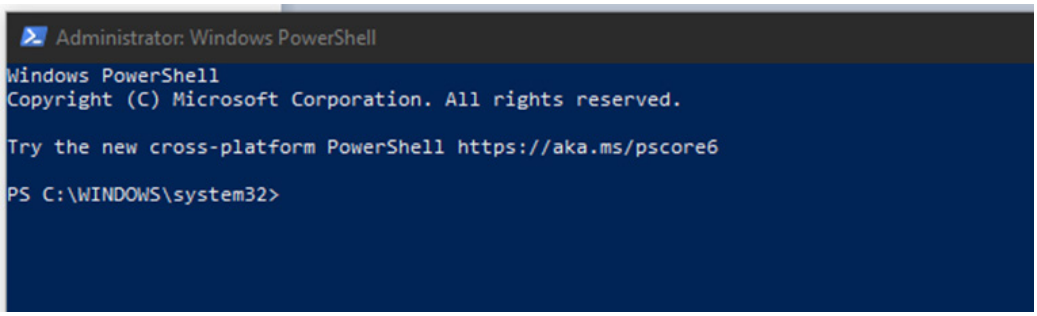
PowerShell

En la guía de solución de problemas, se enumeran varios comandos de PowerShell para ayudar tanto a configurar la PC del gestor de datos como a diagnosticar problemas de comunicación. A PowerShell se accede de la misma manera que se accede al indicador de CMD. En general, el shell de comandos de PowerShell debe ejecutarse en modo de administrador.



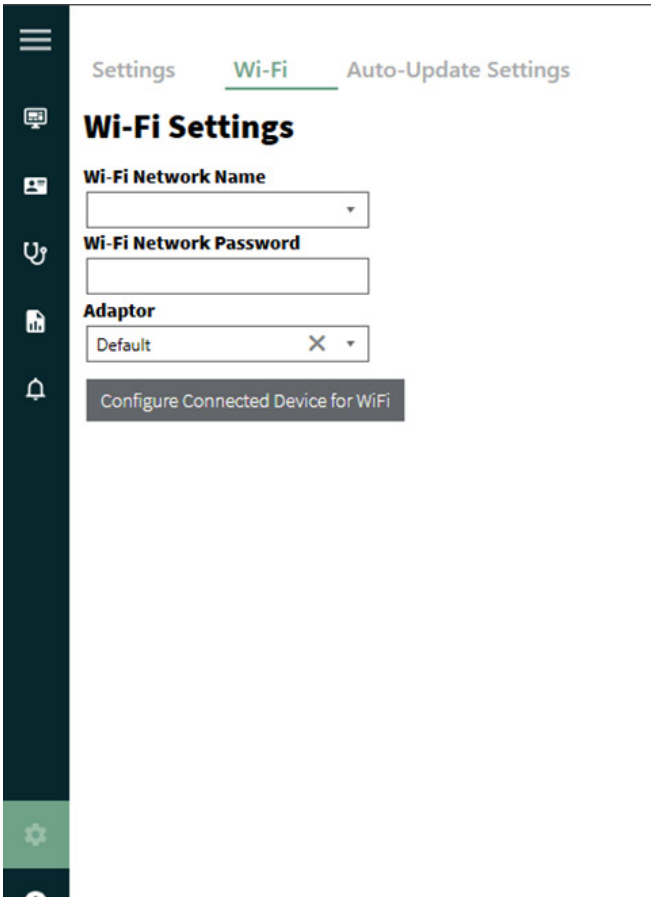
NEOGEN.com

Cuando se le solicite, responda haciendo clic en sí para iniciar PowerShell.



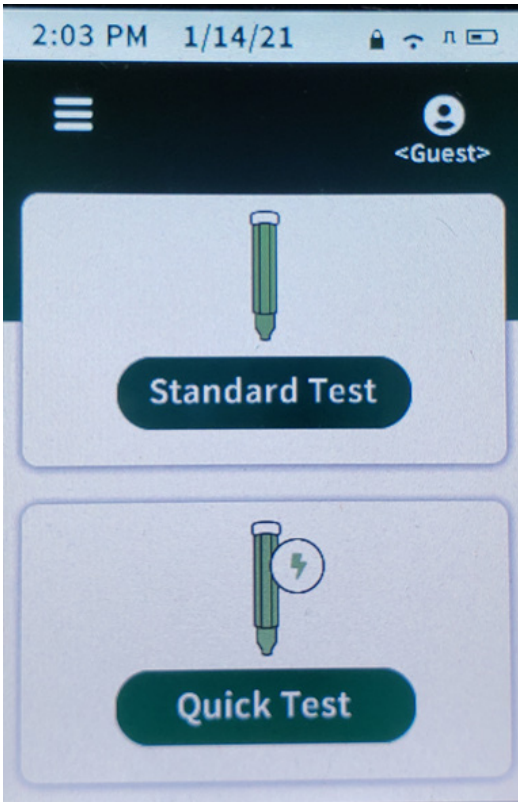
Configuración del dispositivo para wifi

Para configurar el dispositivo AccuPoint® Advanced NG para wifi, vaya a la pantalla de configuración haciendo clic en el icono de engranaje situado en la parte inferior izquierda del Data Manager y, a continuación, seleccione la pestaña wifi. Los campos solo se activarán si el dispositivo AccuPoint Advanced NG está conectado a la PC con un cable USB y está encendido.



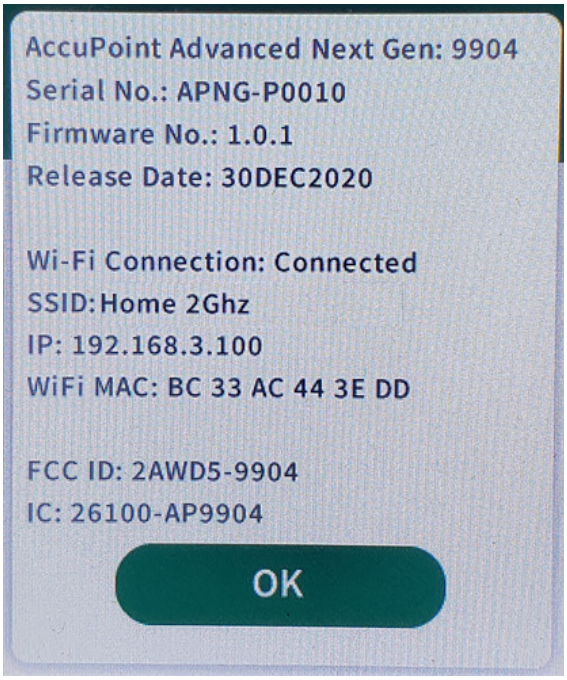
Después de seleccionar los campos de nombre de la red de wifi y contraseña de la red de wifi, haga clic en el botón para configurar el dispositivo conectado para wifi.

Después de unos segundos, el dispositivo debería mostrar un icono de wifi y un icono de candado en la parte superior de la pantalla.



Si esto no ocurre, hay algunos pasos de solución de problemas que se pueden seguir para intentar conectarse al dispositivo.

Si la conexión al wifi sigue fallando, consulte la pantalla del dispositivo para ver la dirección IP de este.



Para determinar si la PC se ha conectado a través del Protocolo de Control de Transmisión (TCP), abra una petición de comandos e intente hacer un ping al dispositivo utilizando la dirección IP de la pantalla sobre el dispositivo:

ping 192.168.3.100

Debería recibir una respuesta como la siguiente, que significa que la PC puede ver el dispositivo:

```
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
```

Una respuesta ping de que caducó la solicitud significa que la PC no puede comunicarse con el dispositivo.

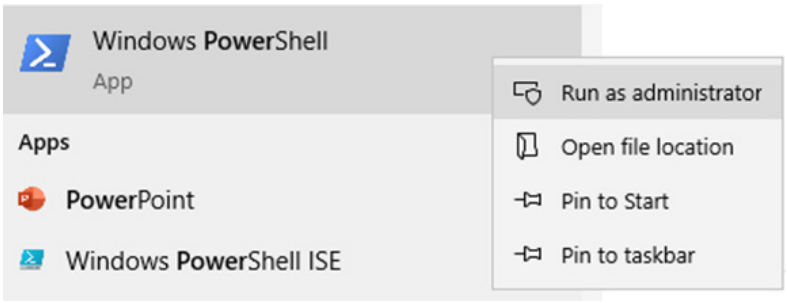
```
Pinging 192.68.3.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

Es posible que tenga que trabajar con su grupo de servicios de TI para resolverlo. Más adelante en este documento, se ofrecen otros pasos para la solución de problemas

Apertura del puerto 443

La comunicación entre la PC y el dispositivo AccuPoint® Advanced NG requiere que el puerto 443 permita la comunicación entre esas terminales. Si hay un firewall instalado localmente en la PC, se debe añadir la regla de entrada para permitir el tráfico a través del puerto TCP 443. También deben añadirse políticas a cualquier software antispyware o antivirus instalado. Se ha incluido un script de PowerShell que añadirá estas reglas y políticas locales de forma automática. Si no se ejecuta durante la instalación, se puede ejecutar manualmente en los pasos que siguen.

Ejecute la aplicación Windows PowerShell con permisos avanzados:



Una vez abierta la ventana de comandos de PowerShell, navegue hasta la carpeta de instalación de AccuPoint® Data Manager. Por defecto, se trata de la carpeta C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0:

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

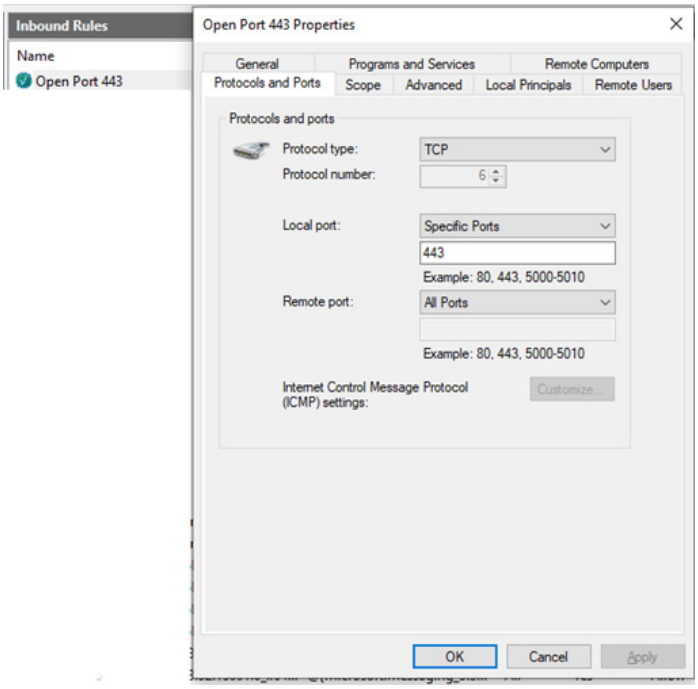
Ejecute el script PowerShell securityConfig.ps1:

.\securityConfig.ps1

El script intentará implementar los cambios de seguridad que encuentre y hará un informe cuando haya terminado. Intente configurar el dispositivo de nuevo mediante el software Data Manager como se describe en la sección de configuración del dispositivo para wifi. Si no se consigue conectar de forma segura con el dispositivo (no aparece el icono del candado), revise las exclusiones manualmente.

Revisión de la configuración del firewall

Se supone que el script de PowerShell instaló la configuración adecuada del firewall. Para comprobarlo, abra el programa de firewall instalado en la PC y revise la sección de reglas de entrada y busque la regla del puerto abierto 443. Para Windows Defender, haga doble clic en la regla y cambie a la pestaña de protocolos y puertos.



Si esta regla no está en la aplicación del firewall, puede añadirse de modo manual, ya sea a través de la interfaz gráfica de usuario (GUI) del firewall, o al ejecutar lo siguiente desde un indicativo de comando avanzado:

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

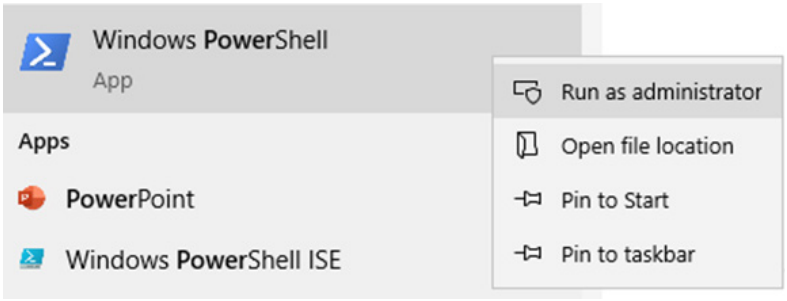
Si esto falla, revise la sección adicional de solución de problemas a continuación.

Más soluciones a problemas

El tráfico de red entre su PC y el dispositivo NEOGEN® AccuPoint® Advanced NG puede ser bloqueado por muchas razones, que pueden no ser obvias inmediatamente. Esto incluye la configuración del router inalámbrico, el software de seguridad que se ejecuta en la misma red, los firewalls locales y los dispositivos de red, así como las políticas de red de aplicaciones dentro de los marcos de red avanzados de proveedores como Cisco y VMWare.

El script de PowerShell que se mencionó antes enumerará el software del antivirus y de seguridad que se ejecuta en la PC del gestor de datos, pero no lo detectará todo, y no revelará el software que se ejecuta en la red en general. Se invoca siguiendo las indicaciones antes mencionadas.

Ejecute la aplicación Windows PowerShell con permisos avanzados.



Una vez abierta la ventana de comandos de PowerShell, navegue hasta la carpeta de instalación de AccuPoint Data Manager. Por defecto, se trata de la carpeta C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0.

```
CD C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0
```

Ejecute el script PowerShell securityConfig.ps1.

```
.\securityConfig.ps1
```

Aparecerá un archivo de texto con la descripción de lo que el script de PowerShell ha podido encontrar. Esto le ayudará a modificar la configuración local de su software de seguridad y a realizar solicitudes más detalladas a su grupo de servicios de IT.

Guarde los resultados para compartirlos con su grupo de servicios de IT de ser necesario.

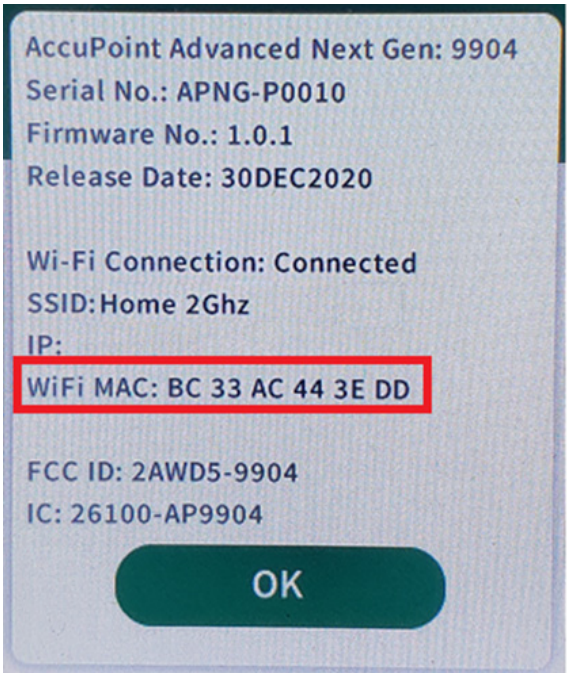
Los siguientes puntos son problemas comunes y los pasos para su resolución.

El dispositivo AccuPoint Advanced NG no puede conectarse al wifi

Si después de configurar el dispositivo para wifi, apagarlo y encenderlo, el dispositivo sigue sin poder conectarse al wifi, lo más probable es que haya algo en su red que esté bloqueando el dispositivo. A continuación, se presentan los pasos que deberían ayudar a resolver los problemas y proporcionar información que puede ser utilizada por su grupo de servicios de IT.

Registre el dispositivo en su grupo de servicios de IT o en el router local

Algunas redes solo permiten que los dispositivos reconocidos se conecten a sus redes wifi. Esto significa que su organización debe registrar el dispositivo como un host permitido. Por lo general, esto se logra al proporcionar la dirección MAC del dispositivo. La dirección MAC aparece en la pantalla “Acerca de” del dispositivo. La siguiente captura de pantalla es de un dispositivo AccuPoint® Advanced NG:

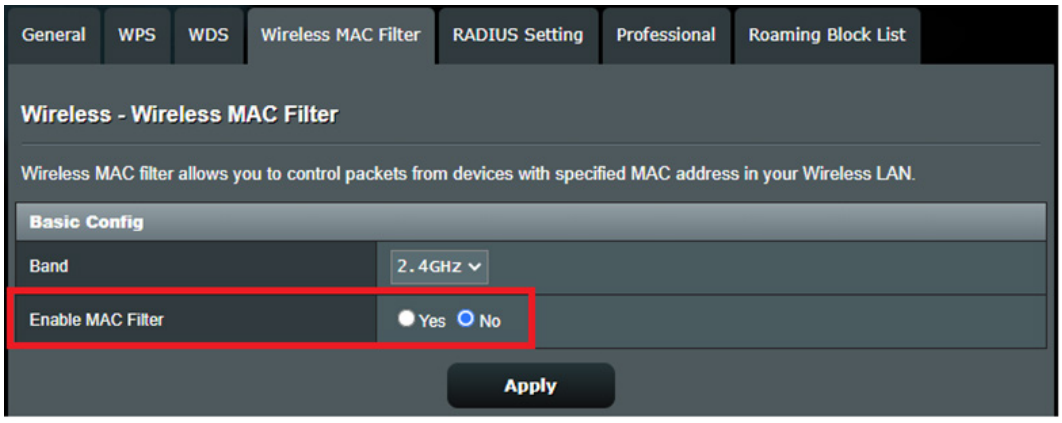


Consulte con el equipo de servicios de IT de su organización si necesita registrar su dispositivo, y brinde la dirección MAC que aparece en este.

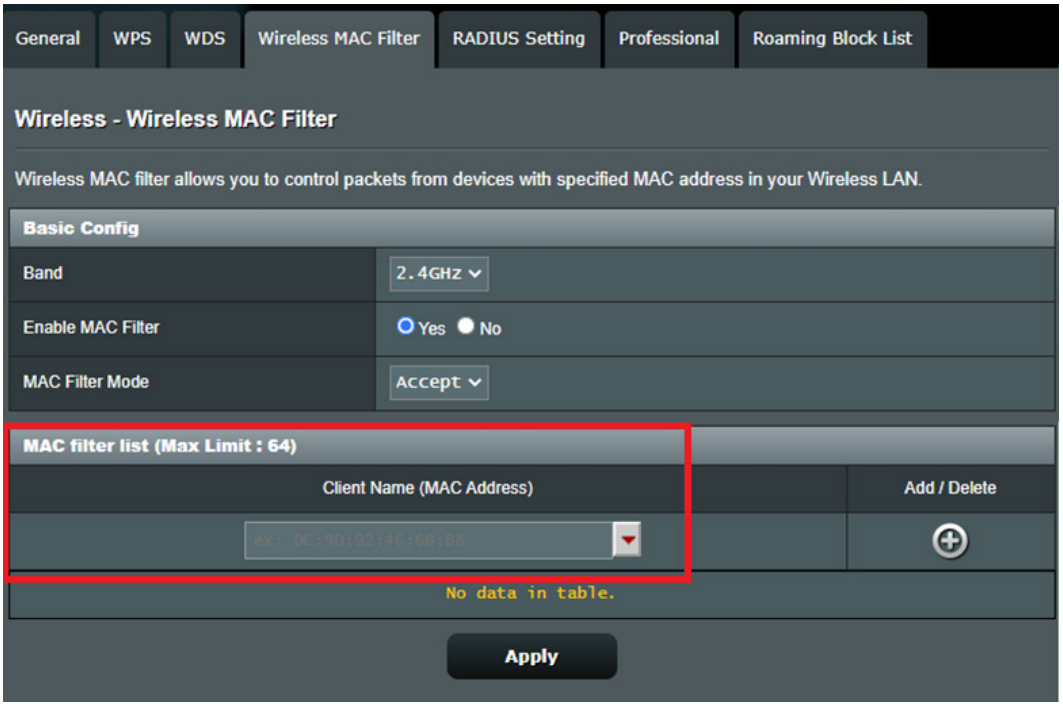
Si está gestionando su propio router de wifi, debe confirmar que su router local no requiere hosts registrados. Esto variará según la marca y el tipo de router. Si es posible, debería desactivar el filtrado de hosts basado en MAC en su router de wifi.

Consulte la documentación de su router antes de realizar modificaciones.

La siguiente es una captura de pantalla de ejemplo de un router de wifi marca Asus:



Si se requiere un filtrado basado en MAC, asegúrese de que la dirección MAC de su dispositivo AccuPoint® Advanced NG esté en la lista, o añádala a la lista de hosts permitidos.



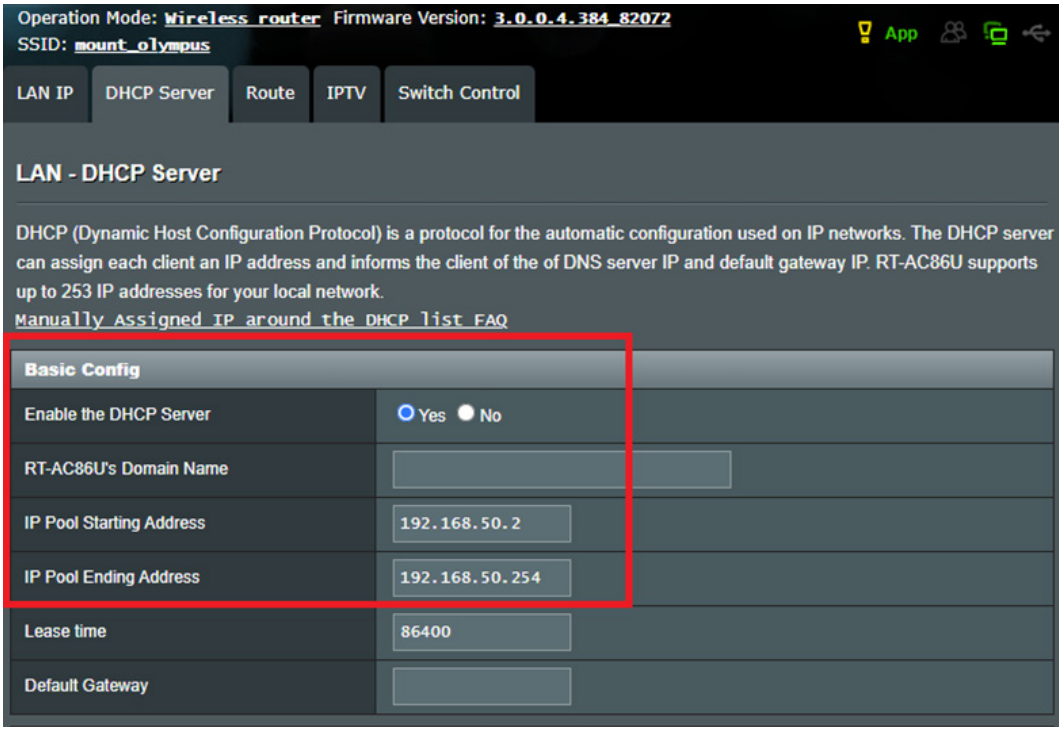
Verifique que los servicios del DHCP estén disponibles

En la mayoría de los entornos de red inalámbricos y cableados, los servicios del Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) asignan automáticamente una configuración de red específica a cualquier host que no requiera una dirección de red fija. Si se desactiva el DHCP, las PC y otros dispositivos no podrán conectarse a la mayoría de las redes.

El dispositivo AccuPoint Advanced NG requiere acceso a los servicios del DHCP.

En un entorno corporativo, debe confirmar con su grupo de servicios de IT si los servicios del DHCP están disponibles y habilitados para la red inalámbrica a la que intenta conectarse con el dispositivo AccuPoint Advanced NG.

Si utiliza un punto de acceso inalámbrico local, consulte la documentación de su router para asegurarse de que el DHCP está configurado. En la siguiente pantalla de configuración del router Asus, puede ver que el DHCP está habilitado y el rango de direcciones está asignado a los hosts conectados:



Si la pantalla “Acerca de” de su dispositivo AccuPoint® Advanced NG no muestra una dirección IP en el rango que se muestra en su router, significa que el dispositivo no pudo comunicarse correctamente con el servicio del DHCP. Un fallo del DHCP se mostrará como una dirección de 0.0.0.0 o una dirección que comienza con el número 169. Intente reiniciar o apagar y encender su router antes de intentar volver a conectarse con su dispositivo AccuPoint Advanced NG.

Si estos ajustes están en blanco en su router, consulte con su grupo de servicios de IT para configurarlo correctamente. De ser posible, su PC y el dispositivo deben estar en el mismo rango de direcciones. Una configuración incorrecta de este rango puede crear conflictos en las direcciones en su red más amplia.

Compruebe que el software de seguridad de la red permita que su dispositivo ingrese en la red

Algunas organizaciones utilizan un software de seguridad que bloquea la conexión de dispositivos desconocidos a la red local. Para comprobar si se trata de un problema, intente conectar un dispositivo propio que no se haya conectado previamente a la red inalámbrica en cuestión, como un teléfono o una tableta. Si estos dispositivos no pueden conectarse, lo más probable es que deba solicitarle a su grupo de seguridad o de servicios de IT una excepción para permitir que el dispositivo AccuPoint Advanced NG se conecte a la red.

En un entorno corporativo en el que se requiera introducir un nombre de usuario y una contraseña para acceder a la red, necesitará una excepción para conectar su dispositivo AccuPoint Advanced NG, ya que el dispositivo AccuPoint Advanced NG carece de la capacidad de utilizar una cuenta independiente para acceder a una red wifi. Consulte con su grupo local de servicios de IT para crear una excepción.

El filtrado por software de seguridad es distinto del filtrado MAC o del basado en un host que se produce en el router local o en el punto de acceso inalámbrico.

No se puede llegar al dispositivo AccuPoint® Advanced NG con un ping desde la PC

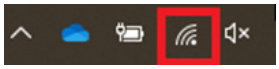
Si el dispositivo se conecta con éxito, pero su PC no puede hacerle ping al dispositivo, puede haber varias causas posibles.

Verifique que su PC está conectada a la red como una red privada

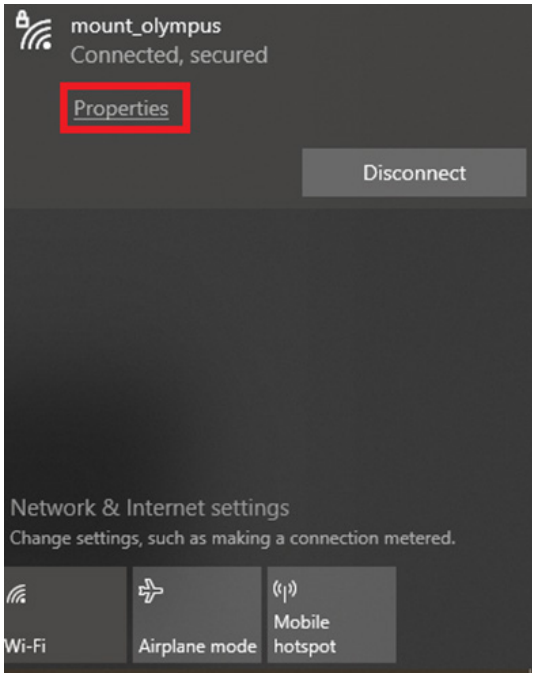
Si su PC se ha conectado a una red pública inalámbrica o cableada, Windows 10 implementará protocolos de seguridad que interferirán en la comunicación de la PC con el dispositivo AccuPoint Advanced NG. Deberá verificar que su conexión de red actual se considere una red privada. Busque en la esquina inferior derecha de su barra de tareas el icono de red.

En una red cableada, esto aparecerá de la siguiente manera:

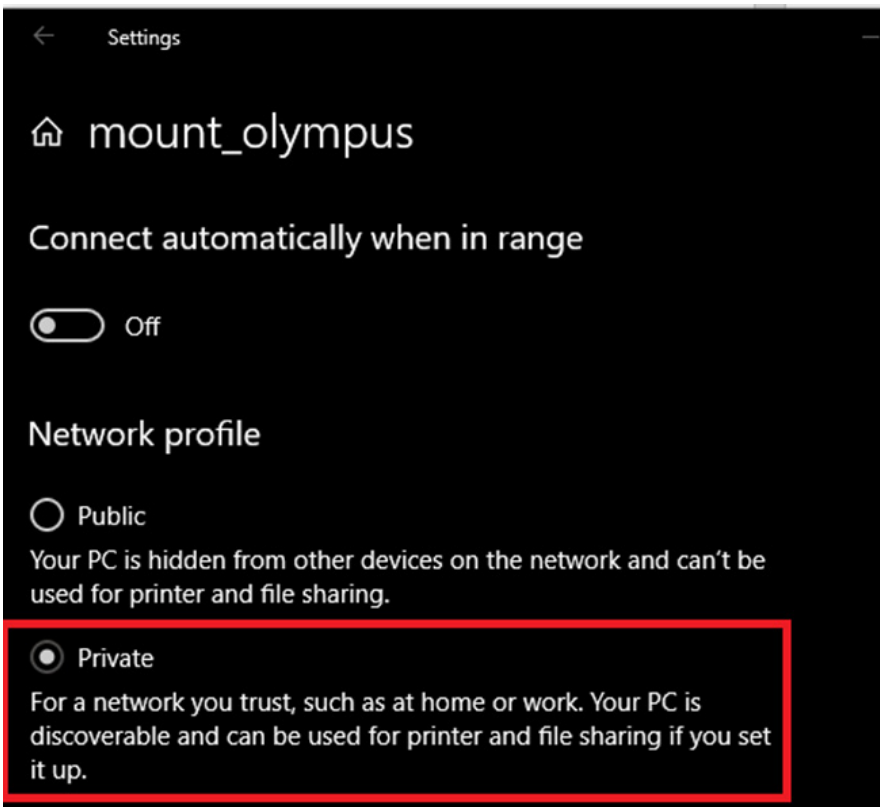
Una red inalámbrica, el icono aparecerá de la siguiente manera:



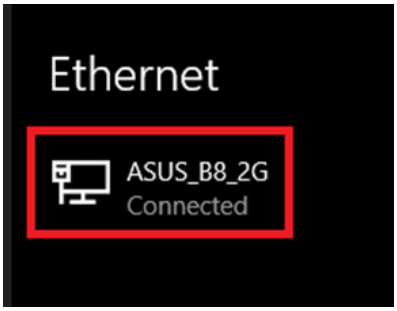
Haga clic en el icono de red y, a continuación, en propiedades.



En la pantalla resultante, asegúrese de que la opción privada está seleccionada.



En el caso de una red cableada, es posible que vea una pantalla con la etiqueta ethernet. Haga clic en el nombre de su red cableada para comprobar que está configurada como privada.

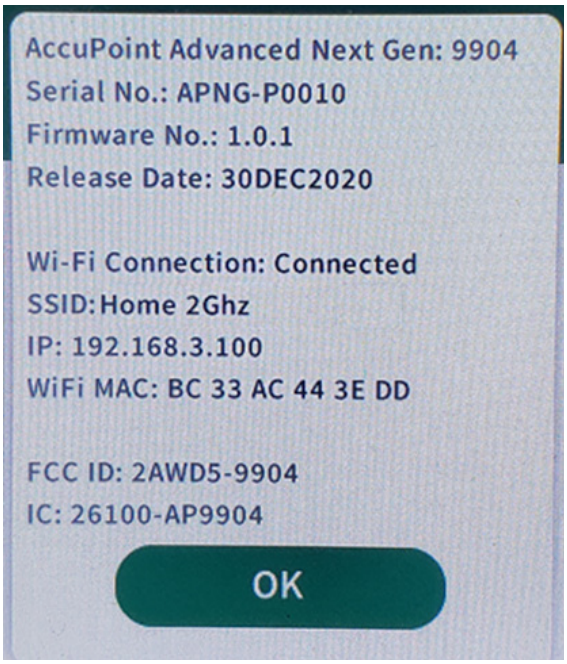


Debe utilizar una red cableada solo si su PC y el dispositivo AccuPoint® Advanced NG se consideran parte del mismo segmento de red local o si su red más amplia permite que los dispositivos se conecten a través de segmentos de red. Es posible que tenga que trabajar con su grupo de servicios de IT para permitir las conexiones a través de los segmentos de red. Consulte la siguiente sección para saber cómo asegurarse de que la PC y el dispositivo AccuPoint Advanced NG están en el mismo segmento de red.

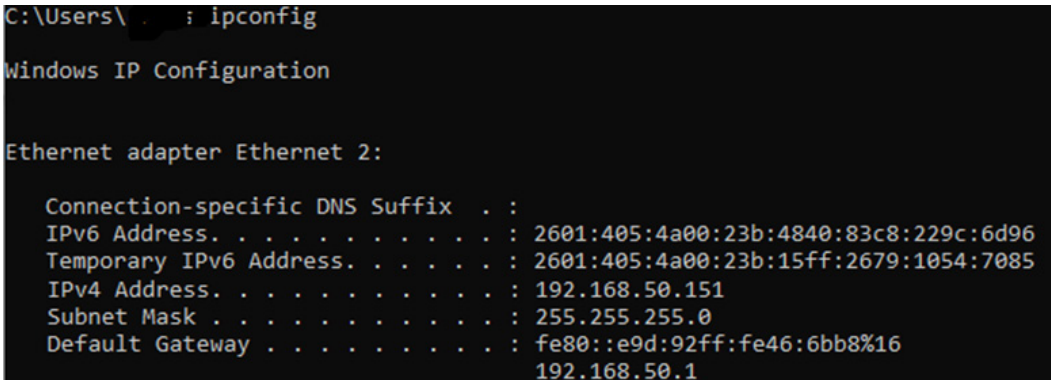
Verifique que la PC de gestión de datos y el dispositivo AccuPoint® Advanced NG están en el mismo segmento de red

Esto solo es necesario si su organización no permite que los dispositivos se comuniquen a través de su red.

En la pantalla “Acerca de”, su dispositivo tendrá una dirección de IP específica.



En este caso, la red es 192.168.3.x. Es posible que los dispositivos con un rango de red diferente no puedan detectar el dispositivo AccuPoint Advanced NG. Desde su PC, tendrá que verificar su dirección de red a través de una ventana DOS o CMD, mediante el comando IPCONFIG.



La dirección que aparece aquí es 192.168.50.x. En muchos entornos corporativos, la PC y el dispositivo AccuPoint Advanced NG no podrían intercambiar tráfico ni conexiones de red.

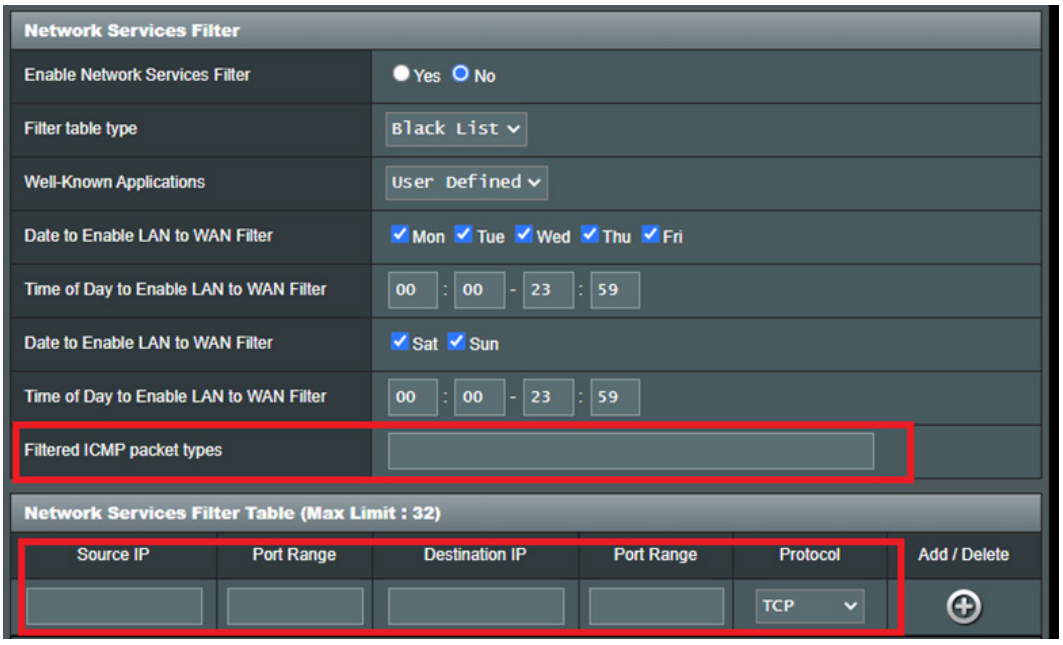
Deberá confirmar con su grupo de servicios de IT qué restricciones existen para que los dispositivos sean visibles entre sí en la red a través de los segmentos de la misma. Una solución rápida puede ser conectar su PC a la misma red inalámbrica que el dispositivo AccuPoint Advanced NG. Sin embargo, esta conexión fallará cuando la PC o el dispositivo AccuPoint Advanced NG cambien de ubicación y se conecten a diferentes puntos de acceso inalámbricos.

Compruebe que su red local permite el tráfico de ping

Algunas redes bloquean todo el tráfico de ping entre hosts. El comando ping utiliza el protocolo de control de mensajes de Internet (Internet Control Message Protocol, ICMP). Muchas redes bloquearán cualquier tráfico a través de ICMP originado en una PC.

Consulte con su grupo de servicios de IT para asegurarse de que el tráfico ping o ICMP de host a host está permitido. Si no es así, solicite una excepción. Esto hará que la resolución de problemas de su dispositivo AccuPoint® Advanced NG sea más sencilla y transparente.

Si gestiona su propio punto de acceso inalámbrico, consulte su documentación y verifique que el tráfico ping o ICMP esté permitido. Es posible que tenga que habilitar explícitamente el ping o el ICMP, o eliminar los filtros de protocolo.



Verifique que el software de seguridad local no esté bloqueando las solicitudes de ping salientes

Algunos programas de seguridad corporativos bloquearán explícitamente las solicitudes de ping salientes. Puede confirmarlo intentando hacer ping a hosts conocidos como www.google.com o 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 esto funciona, inténtelo de nuevo con otro host o PC de su red que sepa que está conectado. La forma más sencilla es hacer un ping al router. Cuando emita un comando ipconfig, este aparecerá como la puerta de enlace predeterminada.

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

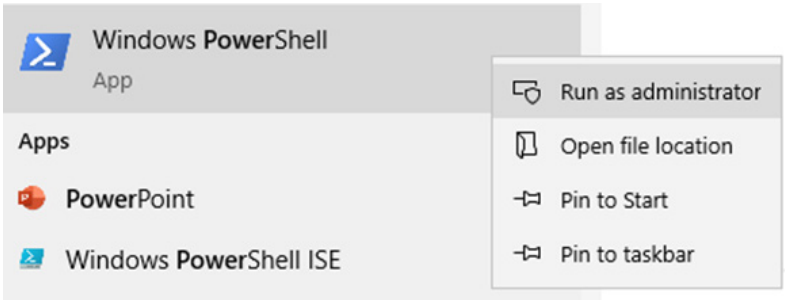
Debería poder hacer ping a la puerta de enlace en todo momento.

```
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 no puede hacer ping al router, lo más probable es que el tráfico ICMP esté bloqueado y tendrá que asegurarse de que su software de seguridad permita el tráfico ICMP saliente.

Añadir regla para desbloquear ICMP

Si tiene una regla que bloquea el tráfico ICMP, puede desbloquearla creando una regla como administrador en la PC del gestor de datos. Ejecute la aplicación Windows PowerShell con permisos avanzados.



Una vez que haya abierto PowerShell, introduzca el siguiente texto para habilitar el tráfico Ipv4 ICMP y luego pulse Intro.

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

Como opción, si desea habilitar el tráfico Ipv6 ICMP, introduzca el siguiente texto y luego pulse Intro.

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

Asegúrese de que la seguridad de la empresa y el software de red permitan el tráfico entre la PC y el dispositivo AccuPoint® Advanced NG

Muchos paquetes de seguridad de red comerciales bloquearán el tráfico de red entre los dispositivos de la red a menos que se permita de forma explícita. Esto incluye lo siguiente:

1. Infraestructura céntrica de aplicaciones CISCO (Application Centric Infrastructure, ACI), que puede tener políticas para bloquear el tráfico entre hosts no autorizados. Puede ser necesaria una nueva política.
2. CrowdStrike, que se ejecuta localmente como un agente y acepta las políticas de un servidor central, puede anular los cambios del firewall de Windows, bloqueando tanto el tráfico ICMP como el tráfico seguro hacia el dispositivo AccuPoint. Es posible que su grupo de servicios de IT tenga que añadir excepciones.
3. Rapid7, que es similar a CrowdStrike, puede requerir anulaciones de políticas para permitir el tráfico.

Su grupo de servicios de IT puede emitir políticas de Windows que bloqueen la comunicación entre la PC y el dispositivo AccuPoint Advanced NG, e incluso impedir las actualizaciones de las reglas del firewall.

Puede utilizar el comando TRACERT descrito antes para identificar la ruta desde la PC gestora de datos hasta el dispositivo AccuPoint Advanced NG. Si la solicitud de TRACERT falla, quiere decir que el tráfico está siendo bloqueado. Si el TRACERT tiene éxito, pero la PC y el dispositivo AccuPoint Advanced NG no pueden comunicarse, los puertos que utilizan el dispositivo y la PC están siendo bloqueados. Se mostrará un fallo de la siguiente manera:

Rastreo de la ruta hacia nosferatu [192.168.50.219]
en un máximo de 30 saltos:

1 buho [192.168.50.151] informa: Host de destino inalcanzable.

Rastreo completo.

Asegúrese de que los firewalls de la red no bloqueen el tráfico de la red

Algunas redes están divididas por firewalls internos para proteger áreas sensibles, como los laboratorios y las áreas de producción. Es posible que se necesiten reglas o excepciones de firewalls si el tráfico de red entre la PC y el dispositivo AccuPoint Advanced NG debe atravesar uno o más firewalls. El comando TRACERT también le ayudará a diagnosticar un problema de firewall.

Consulte con su grupo de servicios de IT para averiguar si la PC y el dispositivo AccuPoint Advanced NG deben atravesar uno o más firewalls para comunicarse.

No se pueden iniciar transferencias al dispositivo AccuPoint Advanced NG

Las causas más probables de este problema son el bloqueo del tráfico en el puerto 80 hacia el dispositivo AccuPoint Advanced NG, o el bloqueo del tráfico en el puerto 443 entre el dispositivo y la PC.

Para iniciar una transferencia desde la PC al dispositivo AccuPoint Advanced NG, el gestor de datos envía un mensaje al dispositivo AccuPoint Advanced NG a través del puerto 80. A continuación, el dispositivo se conecta de nuevo a la PC a través del puerto 443 y transfiere la información de forma segura a través de TLS. El bloqueo del tráfico en cualquiera de estos puertos interferirá con la sincronización de datos, incluso con el envío de planes de sitio.

El tráfico en el puerto 80 no viaja desde la PC al dispositivo AccuPoint® Advanced NG

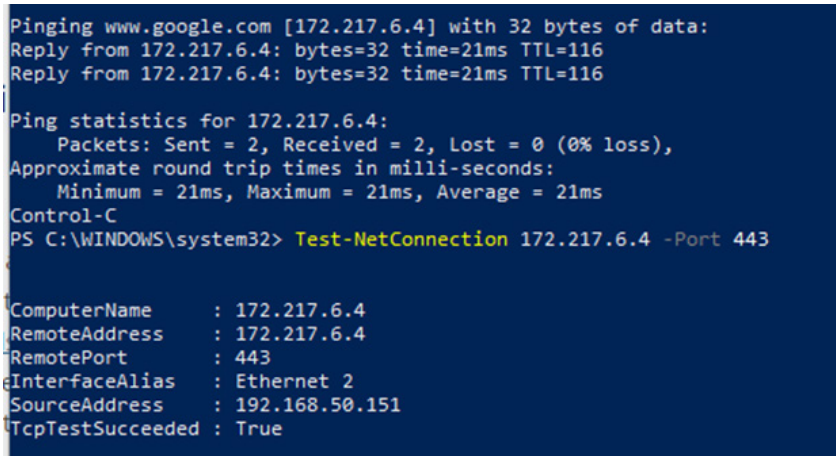
La mayoría de los arreglos utilizados para resolver los problemas de ping antes mencionados pueden utilizarse para resolver los mismo problemas entre la PC y el dispositivo. La PC inicia el contacto con el dispositivo en el puerto 80. El software de seguridad y los dispositivos de seguridad suelen identificar el tráfico de este tipo.

Los agentes de seguridad web que simplemente trabajan para bloquear el tráfico saliente en el puerto 80 pueden causar una interferencia adicional. Aunque no se transfieren datos sensibles a través del puerto 80, este suele considerarse un puerto inseguro.

El dispositivo AccuPoint Advanced NG debe recibir un mensaje de activación a través del puerto 80 que le indique que inicie las comunicaciones seguras con la PC.

Realice la primera comprobación indicada en la sección “No se puede acceder al dispositivo AccuPoint Advanced NG con un ping desde la PC” para asegurarse de que la PC esté conectada a su red local como una red privada. Si esto no es así, siga los pasos que se indican a continuación.

La mejor manera de comprobar si esto es un problema es con el comando de PowerShell Test-NetConnection. El siguiente ejemplo muestra cómo probar Google.com para el puerto 443:



El comando para probar el dispositivo AccuPoint Advanced NG sería:

Test-NetConnection <ip of device> -Port 80

Si no funciona, entonces el puerto 80 está siendo bloqueado. Trabaje con su grupo de servicios de TI para resolverlo. Es posible que necesite excepciones para la PC gestora de datos o para el dispositivo AccuPoint Advanced NG.

El tráfico en el puerto 443 no viaja desde el dispositivo AccuPoint Advanced NG a la PC

La PC gestora de datos utiliza el software Data Manager para alojar un servicio ligero en el puerto 443 a través de TLS.

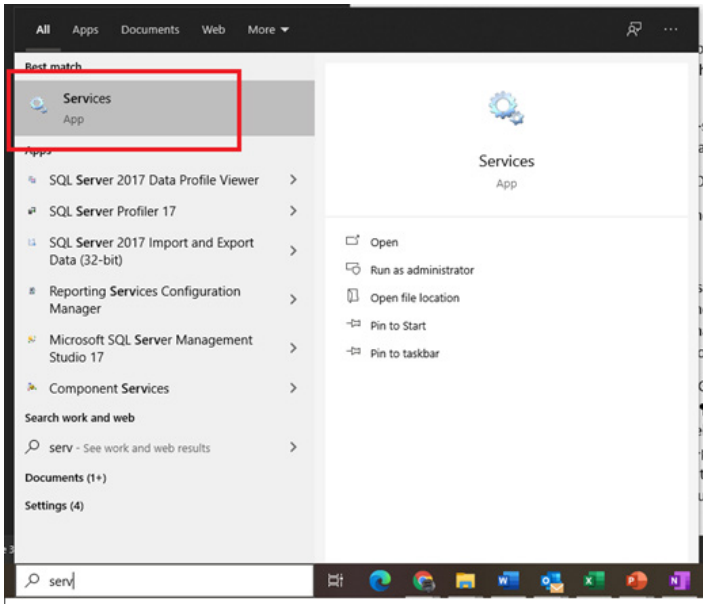
La mayoría de los problemas que bloquean el tráfico del puerto 443 se resuelven al implementar las soluciones de problemas para bloqueo de ping enumeradas anteriormente. Sin embargo, las normas se configurarían de forma diferente. Permitir el tráfico SSL entrante en el puerto 443 a la PC puede requerir uno o más de los siguientes:

- Ajuste de las reglas del firewall de la red interna.
- Añadir políticas al software de seguridad de la empresa.
- Añadir políticas o excepciones a los software de control de red, como ACI.
- Añadir políticas de grupo de Windows para permitir cambios en el firewall local.

También debe comprobar que la PC gestora de datos está asociada con el puerto 443 mediante el comando:

netstat -an

Si el puerto 443 no aparece como asociado en la salida de este comando, reinicie la PC y pruebe de nuevo. Si sigue fallando, mire la lista de servicios de la PC y compruebe que el software Data Manager se esté ejecutando en la PC.



Si el servicio se está ejecutando, y el comando netstat muestra que la PC del gestor de datos está asociada al puerto 443, entonces necesitará una segunda PC para probar el acceso al puerto 443. Emita el siguiente comando desde otra PC con PowerShell hacia la PC del gestor de datos:

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

Si este comando falla, siga las recomendaciones de solución de problemas mencionadas antes.

Resumen

Si se configura correctamente y sin interferencias de señal, las transferencias de datos entre la PC gestora de datos y el dispositivo AccuPoint® Advanced NG deberían ser rápidas y fiables. Sin embargo, al incorporar un nuevo dispositivo a una red corporativa, el tráfico puede bloquearse de muchas maneras. Recuerde lo siguiente y consulte las secciones anteriores de la guía para solucionar estos problemas:

1. Utilice una conexión USB desde la PC gestora de datos hacia el dispositivo para configurar correctamente la conexión de wifi del dispositivo AccuPoint Advanced NG.
2. Ejecute el script provisto de PowerShell, que configurará el firewall local y el software de seguridad en la PC del gestor de datos, o proporcionará recomendaciones para su grupo de servicios de IT.
3. Si el dispositivo no puede conectarse a su red de wifi, entonces el punto de acceso inalámbrico, los firewalls internos o el software de seguridad, u otros dispositivos de seguridad están bloqueando el dispositivo.
4. Si el dispositivo puede conectarse al wifi, pero el icono del candado no aparece, entonces la PC no puede aceptar conexiones entrantes en el puerto 443.
    a. Compruebe que el software Data Manager se está ejecutando en la PC y está asociado al puerto 443.
    b. Ejecute los demás pasos de solución de problemas.
5. Si el dispositivo muestra el icono de bloqueo, y las transferencias de datos (sincronizaciones) pueden iniciarse desde el dispositivo pero no desde la PC, entonces el tráfico de red en el puerto 80 desde la PC hacia el dispositivo AccuPoint Advanced NG está siendo bloqueado.

Esta guía se actualizará cuando sea necesario. Esto incluye información de configuración nueva o actualizada, o cuando una guía adicional para la resolución de problemas podría ser útil.

NEOGEN.com