AccuPoint® Advanced Next Generation Wi-Fi Networking Guide

Configuration and Troubleshooting

NEOGEN
NEOGEN.com

Contents

AccuPoint® Advanced NG Networking Requirements Overview

The AccuPoint® Advanced NG can support the following for Wi-Fi connectivity:

- 802.11 b/g/n
- WPA2/WPA Personal and Enterprise
- WEP
- IPV4
- Network throughput of up to 72 MBs
- Signal range of up to 450 m, which is affected by building superstructures, physical obstructions, and other signal interference.

The device is unable to support RADIUS Authentication or other forms of network authentication. In corporate environments that require host or user-based authentication, it is recommended that MAC address filtering be used instead for the AccuPoint Advanced NG devices. The device's MAC address is available on the about screen of each AccuPoint Advanced NG device. In some environments, MAC filtering may require a new SSID or a separate Wi-Fi network.

It is strongly recommended that DHCP host registration (DNS) be enabled on the network where both the data manager PC and the AccuPoint Advanced NG device will connect. When Wi-Fi is enabled, the device and the PC running the Data Manager software must be able to communicate with each other over the network, with either host initiating a connection. Since both the PC and the device may move between network segments or access points, changing IP addresses as a result, the ability to connect using the PC and the device hostname will be an essential capability, in order to accommodate dynamic IP address changes. If the PC and the AccuPoint Advanced NG device cannot use hostnames to connect and the IP address of either the PC or the device changes, it is very likely they will lose the ability to communicate until the AccuPoint Advanced NG device is reconfigured through a USB connection.

The AccuPoint Advanced NG device communicates securely with the PC running the Data Manager software using a self-signed TLS certificate. The TLS connection is hosted on the PC using the Data Manager service software component. This connection is established when the device is sending or receiving data from the Data Manager software, but it is not maintained continuously. After a brief period of inactivity, the connection is dropped by the device to avoid idle connection stability issues.

When a connection is initiated by the AccuPoint Advanced NG device, all communications will be over TLS on PC port 443. However, when the user wishes to push a site plan or otherwise initiate network communications with the AccuPoint Advanced NG device, the PC must first send a signal to the device over port 80 to a web service that is running on the AccuPoint Advanced NG. When the device receives this web service request, it will shut down the web service and initiate a secure connection to the data manager PC. When the secure connection has been dropped, the device will make the HTTP-based web service available again.

For corporate environments, it may be necessary to create network policy exceptions that allow traffic over port 80 to the AccuPoint® Advanced NG device from the data manager PC, and over port 443 from the device to the PC. Both the PC and device may use ICMP requests to ping each other as well, so ICMP traffic between the AccuPoint Advanced NG device and the PC must be enabled as well.

Within Windows on the data manager PC, the Data Manager software will attempt to reconfigure the local firewall and security settings at the time of installation in order to accommodate its access requirements. This is not always successful, based on the group policies and software on the PC where the software is installed.
The core network requirements include:

1. The network connection on the PC used to connect to the AccuPoint Advanced NG must be configured to be private. On Windows, all incoming traffic initiated by an external device is blocked on a public connection.
2. The local firewall on the data manager PC must be configured to allow:
    a. Incoming traffic on port 443
    b. Outgoing traffic on port 80 (standard HTTP).
    c. Outgoing and incoming ICMP traffic
3. The security software running on the PC and Windows group polices must allow the following executables to access the network:
    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 L◡cation}\HID_UART.exe

Additional exceptions may be required when the Data Manager software is updated. Technical bulletins will be provided when these changes occur.

Many corporate environments rely on endpoint protection and centralized security software — such as CrowdStrike — which require specific policy exceptions. Similarly, Windows group policies can interfere with device and PC connectivity as well.

These configuration requirements should be tested after the Data Manager software has been installed and an AccuPoint Advanced NG device has been configured for Wi-Fi access. Please see the directions and troubleshooting recommendations that follow.

If NEOGEN® Analytics is also in use, local traffic (on the data manager PC only) must be allowed on port 8080. However, this port does not need to be exposed to the network at large. Please see NEOGEN Analytics documentation for additional network access requirements.

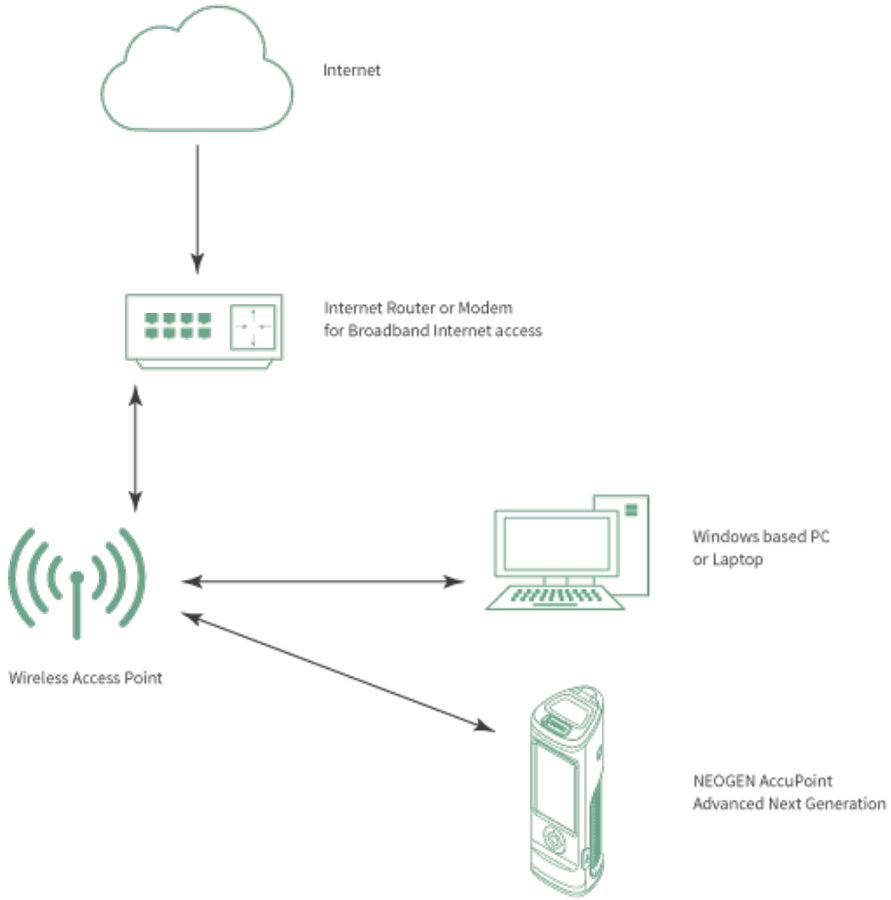
When altering configurations on the PC running the Data Manager software, the user making these changes must have administrator rights. This can be a temporary elevation, if required. Some organizations may be able to push changes down to local PCs. However, debugging connection issues is difficult without local administrator rights. One of the tools provided with the Data Manager software is a PowerShell script, which will provide some diagnostic information.

Before Getting Started

Understand Your Network Environment

Simple

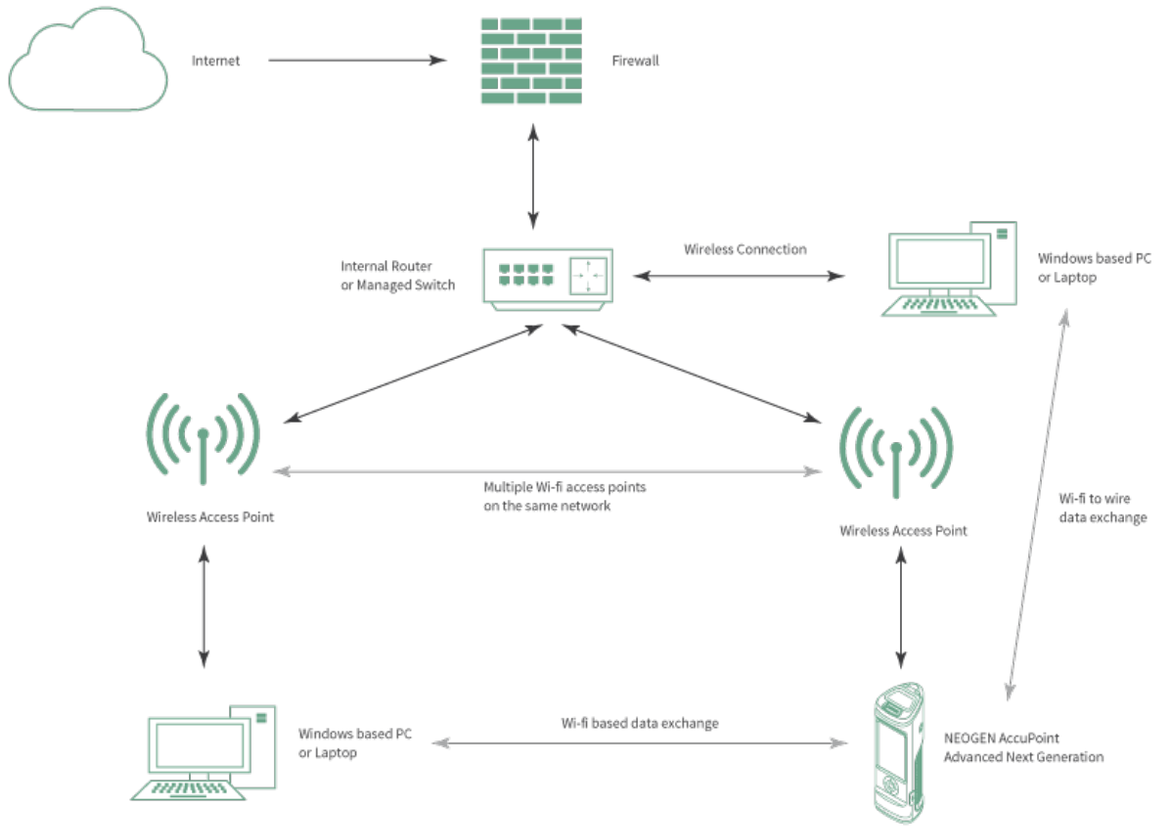
A simple network site is found in many single businesses or isolated workspaces. It typically consists of an internet connection and a single wireless access point such as the following:



In this flat network configuration, the primary issues will be ensuring that the wireless access point (WAP) is configured to allow the AccuPoint® Advanced NG device to connect to the local network. The troubleshooting guide discusses different ways to modify the WAP to allow new connections. On the PC or laptop, the primary issues will be ensuring the local wireless connection, firewall, and security software allow incoming connections.

Organization

An organization-level site may have firewalls and more advanced security software with multiple wireless access points, as seen in this diagram:



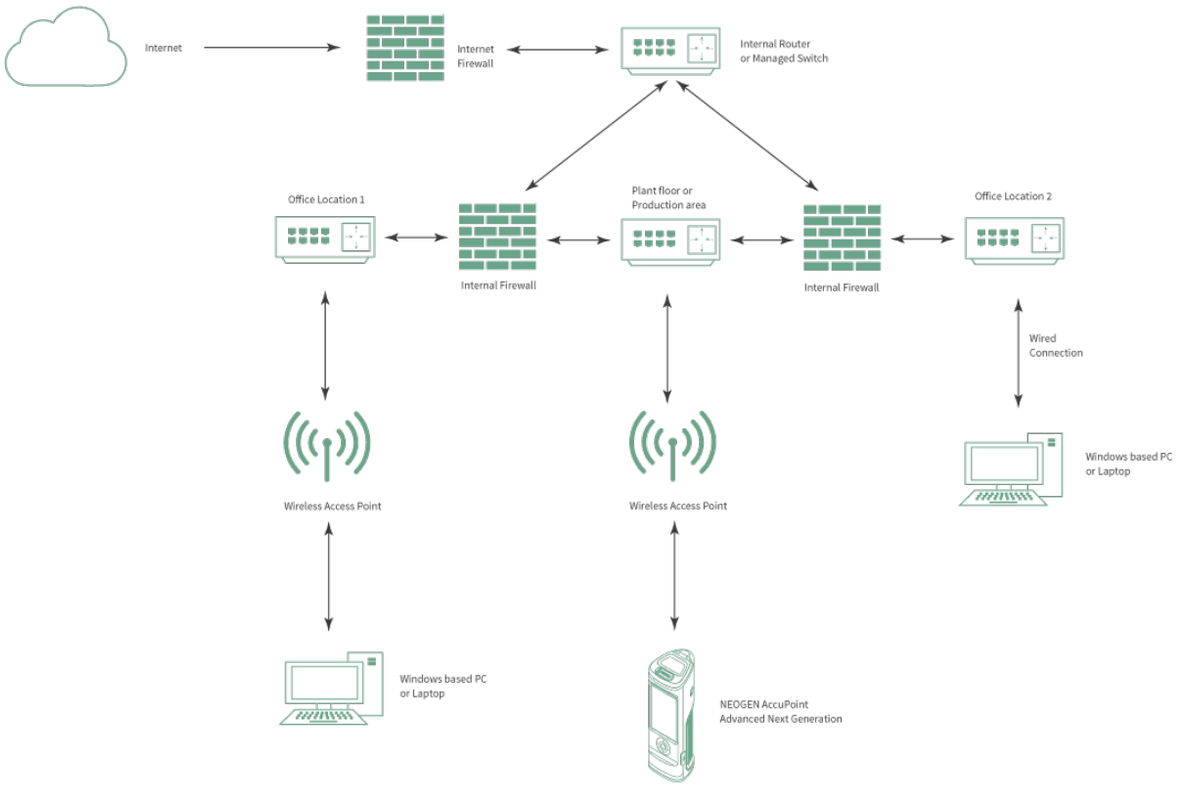
Most users with this type of network configuration will need assistance from their local IT services group to properly configure the device and the PC hosting the Data Manager software. This includes:

1. Ensuring the AccuPoint® Advanced NG can access the Wi-Fi network.
2. Ensuring that the data manager PC and the AccuPoint Advanced NG device can see each other on the network.
3. Ensuring security monitoring software allows the data exchange traffic between the AccuPoint Advanced NG and data manager PC.

The troubleshooting guide goes into detail on how to identify issues and what to share with the IT services group, with respect to ensuring all the components are properly configured.

Enterprise

An enterprise site typically has network segmentation, advanced Wi-Fi configurations, and device restrictions on what is allowed on its networks. This may include multiple firewalls and switches. The following is a highly simplified example of an enterprise network.



In a complex networking environment such as this, connecting the AccuPoint® Advanced NG device over Wi-Fi to the data manager PC may require several tickets with the IT services group, including:

1. Modifications to Windows group policies that will allow incoming networking connections, as well as changes to the local firewall and security software of the data manager PC.
2. Permissions to install the Data Manager software and to modify the local PC configuration.
3. Exceptions to network access rules to allow the AccuPoint Advanced NG device to access the Wi-Fi network.
4. Modifications to the internal firewall rules to allow network traffic between the data manager PC and AccuPoint Advanced NG.
5. Updates to security software policies to allow data exchange between the AccuPoint Advanced NG.

Highly secure environments may require a new Wi-Fi SSID to be established only for AccuPoint Advanced NG communications.

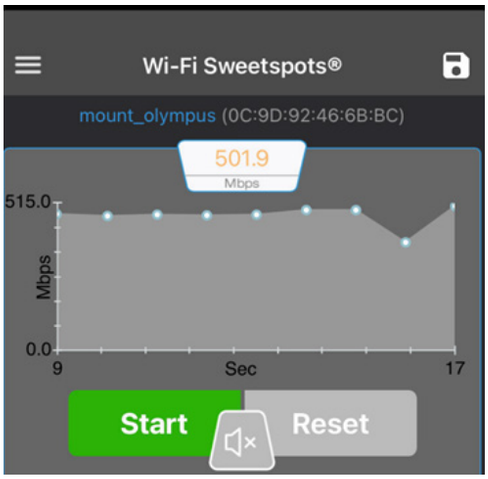
Checking Wi-Fi signal strength

One of the most difficult issues to resolve is Wi-Fi interference or weak signal strength during the operation of the AccuPoint Advanced NG device. As mentioned, the device has a lower-power Wi-Fi radio to improve battery life and maintain portability. Unfortunately, this means the device may be more susceptible to signal loss in operational areas that experience a weak Wi-Fi signal or Wi-Fi interference. The best way to identify Wi-Fi issues in advance is to request a Wi-Fi signal survey in your operational areas where you expect to collect and transmit test data. However, this may be too difficult or time consuming a request for some organizations.

Fortunately, there are Wi-Fi testing tools that will allow most users to perform a very simple Wi-Fi survey based on network transmission throughput. For any user with a smart phone or tablet with a Wi-Fi connection, users can load apps that will check signal strength. The following are apps available on both iOS (Apple) and Android:

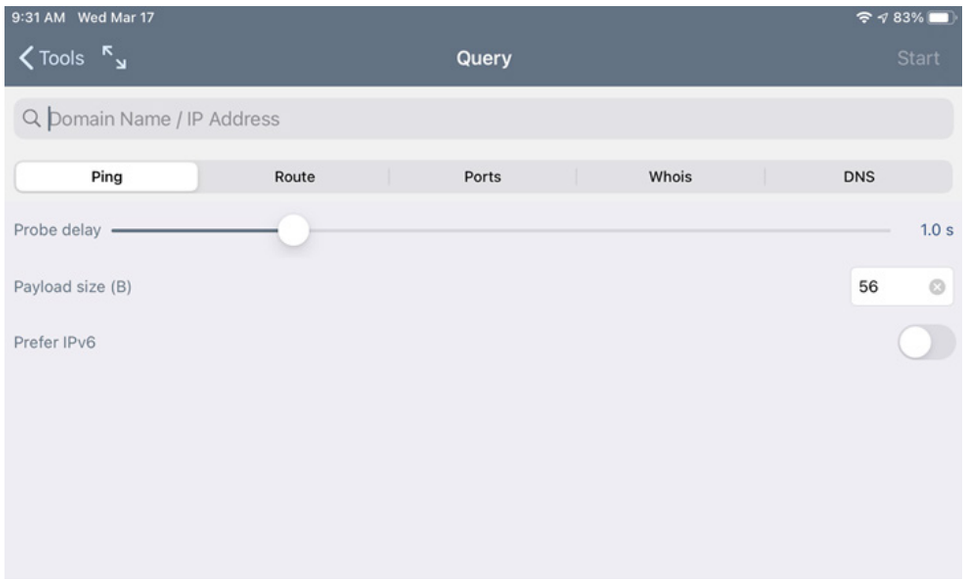
- Wi-Fi SweetSpots (recommended, free)
- Network Analyzer (also free, but more complex)
- Network Analyzer Pro (small fee with good features set)

Please see the application screenshot for Wi-Fi SweetSpots:



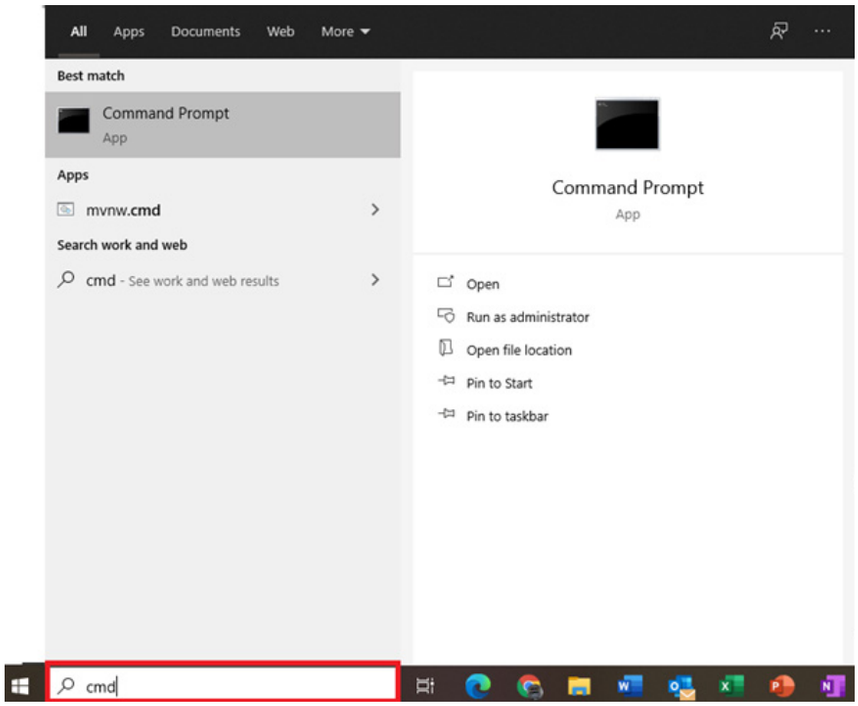
Wi-Fi SweetSpots tracks Wi-Fi throughput. When the network transfer rate drops, you are entering a spot with weaker Wi-Fi signal or higher levels of interference. If the network throughput drops by more than 50%, it is likely the AccuPoint® Advanced NG will experience network communication issues.

Network Analyzer is for users with more advanced network experience who would like to run additional diagnostics such as route tracing, DNS verification, network pings, etc. Please see the following screenshot from Network Analyzer Pro as an example:



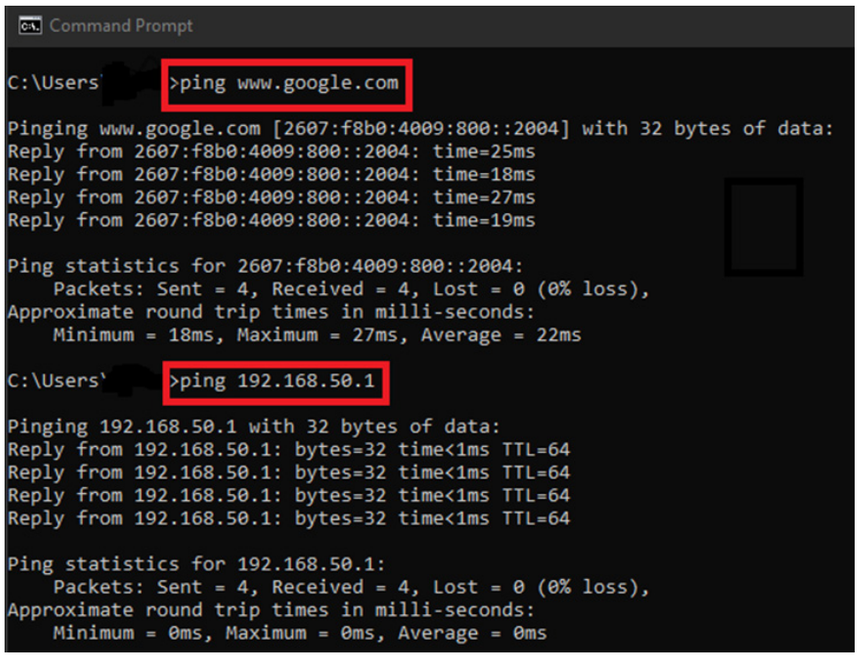
Network Diagnostic Tools for Users

Windows 10 provides users with several very useful commands that can be executed from the user's desktop. For those unfamiliar with how to launch a command prompt window, please see the following screenshot. If you type CMD in the Windows search box, you will see: Ping

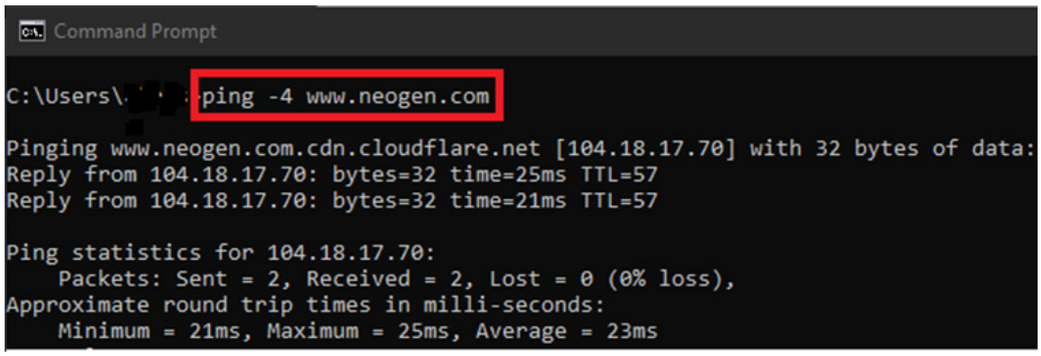


Ping

This simple command is one of the most useful for identifying if the data manager PC may access the AccuPoint® Advanced NG device. However, there are some nuances. The basic command is simply ping <some host> or IP:



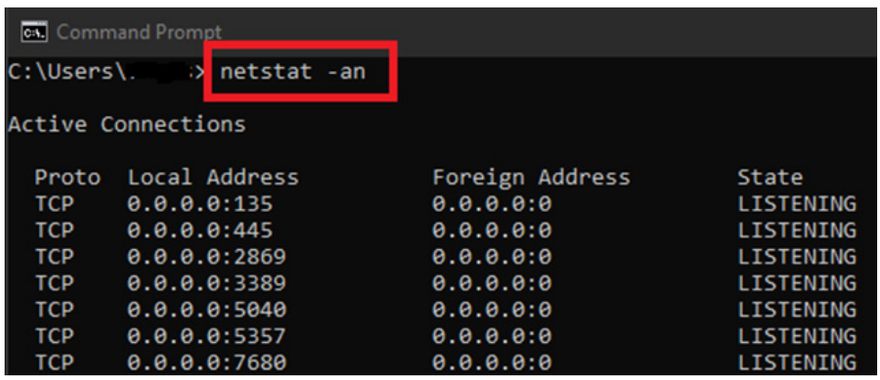
The first command is used to ping www.google.com. The second is used to ping an address on the same network. Notice that the addresses on the first ping request are IPv6. To force a ping to use IPv4 you may have to modify the command by including -4, such as in the following:



Ping times matter! On a local network, the time it takes to reach a host should be no more than 10 ms. Anything slower should be addressed by your local IT services group. For addresses on the internet, ping times should be 120 ms or less. Ping times higher than this may occur for hosts that are geographically distant. However, slow ping times to common services such as Google or Amazon may indicate a slow internet connection. Since the AccuPoint® Advanced NG and the data manager PC are communicating on the same network, a slow internet connection will not be a factor in device operation and data transmission. However, a slow internet connection may inhibit the ability to download updates to the data manager or the device firmware.

Netstat

This command will show what ports a PC is listening to and what ports it is actively connected to. For the AccuPoint Advanced NG, the data manager PC must be listening on port 443. The command and the output are as follows:



The local address and port are important:

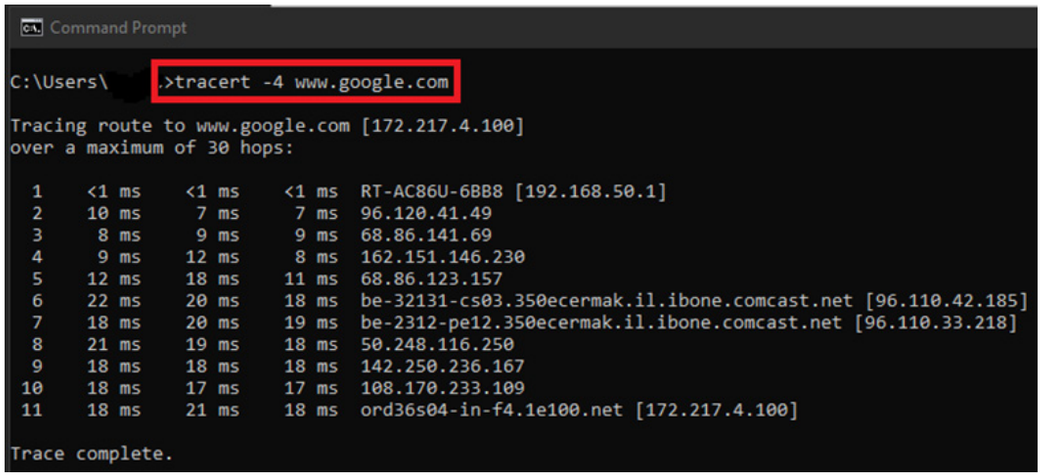
Address: ###.###.###.###:<Port: ###>

There could be several dozen entries, depending on what software and services are running on a PC.

The output in the screenshot for 0.0.0.0:445 shows that this PC is accepting connections on port 445 on all of its network adapters. This command will help to identify if the Data Manager service is running and ready to accept connections from the AccuPoint Advanced NG device.

TRACERT

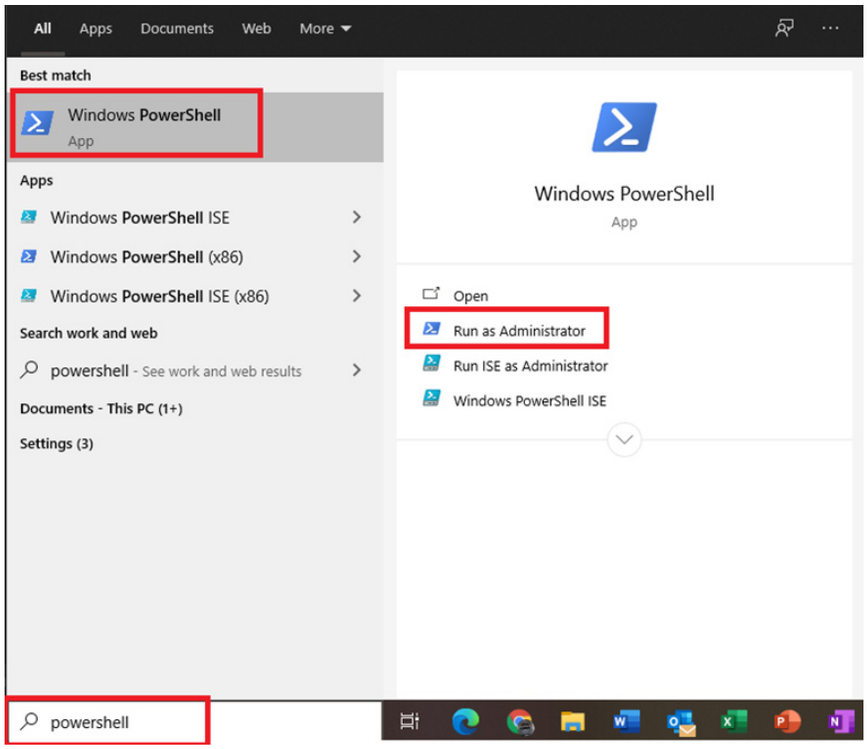
The TRACERT will show the path from one host to another through a network. Each intermediate address is a network hop. This command will help identify what switches, firewalls, and network devices traffic must traverse from the data manager PC to the AccuPoint® Advanced NG device. The following example shows the path between this PC and the host www.google.com. On a local network, there should be anywhere between 1 and 6 hops.



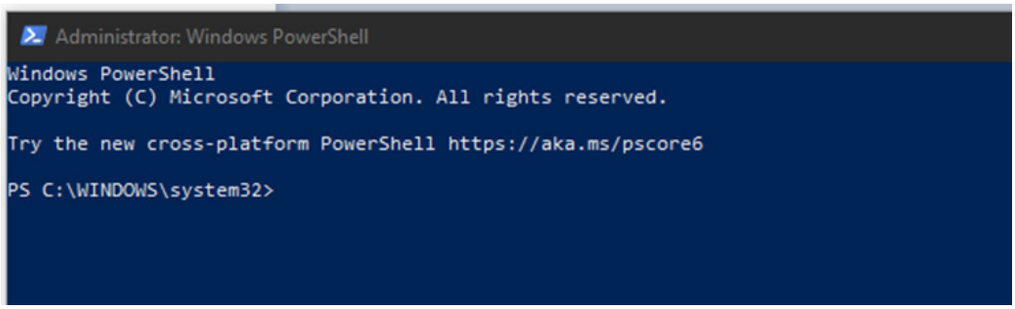
Hop #1 is the local wireless access point. Each hop that follows is a router, switch, or firewall that the network traffic must traverse before reaching its goal of 172.217.4.100. The parameter -4 ensures the traffic uses the IPv4 protocol.

PowerShell

In the troubleshooting guide, multiple PowerShell commands are listed in assisting both configuring the data manager PC as well as diagnosing communication issues. PowerShell is accessed the same way that the CMD prompt is accessed. In general, the PowerShell command shell should be run in administrator mode.

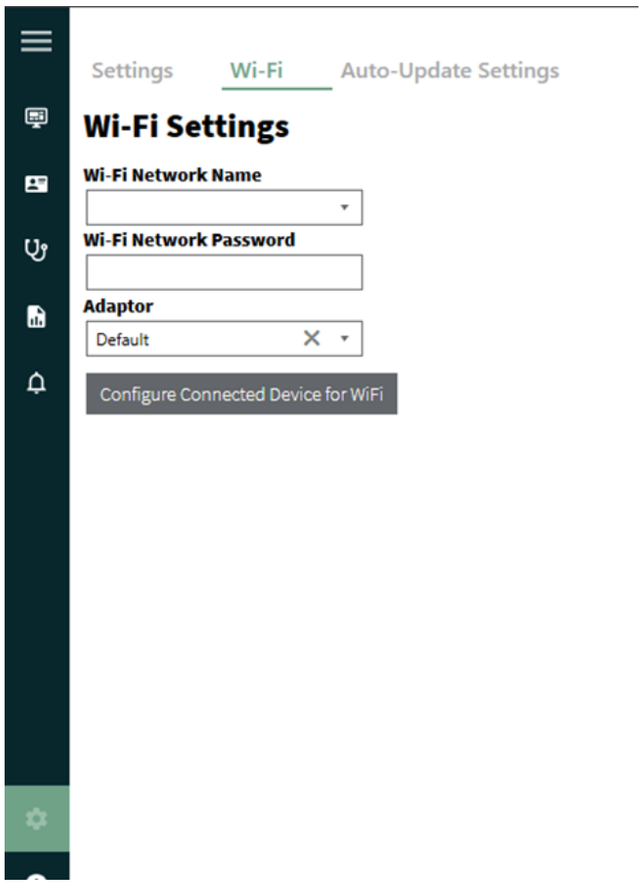


When prompted, respond by clicking yes to launch PowerShell.



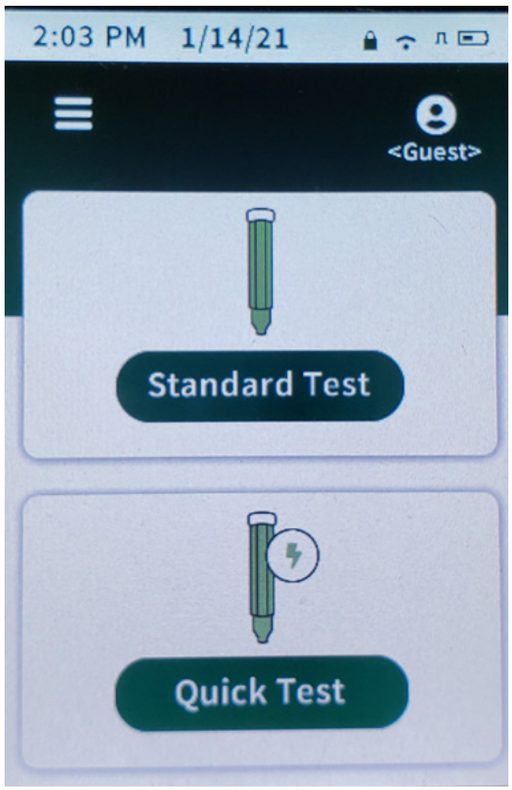
Configuring the Device for Wi-Fi

To set up the AccuPoint® Advanced NG device for Wi-Fi, go to the settings screen by clicking the gear icon on the bottom left of the Data Manager, then select the Wi-Fi tab. The fields will only be enabled if the AccuPoint Advanced NG device is connected to the PC with a USB cable and is powered on.



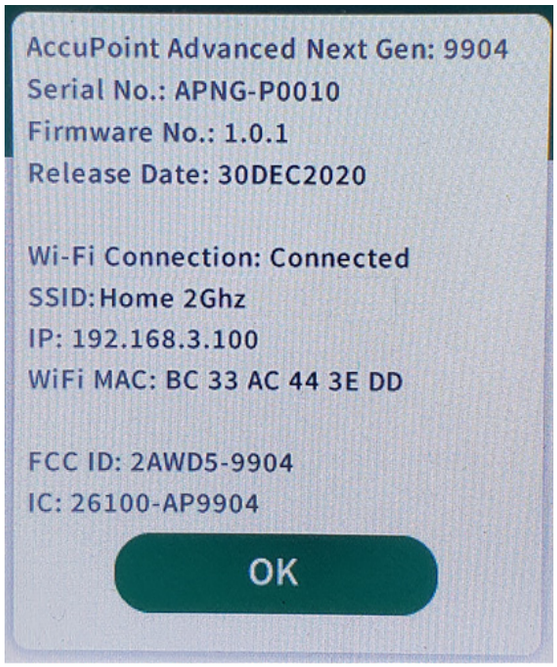
After selecting the Wi-Fi network name and Wi-Fi network password fields, click the configure connected device for Wi-Fi button.

After a few seconds, the device should display both a Wi-Fi icon and a lock icon on the top of the screen.



If this does not occur, then there are some troubleshooting steps to take to attempt to connect to the device.

If Wi-Fi connectivity continues to fail, view the about screen on the device to view the IP address of the device.



To determine if the PC has connected over Transmission Control Protocol (TCP), open a command prompt and attempt to ping the device by using the IP address from the device's about screen:

ping 192.168.3.100

You should receive a response like the one below, which signifies that the PC can see the device:

```
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
```

A ping response of request timed out signifies that the PC cannot communicate with the device.

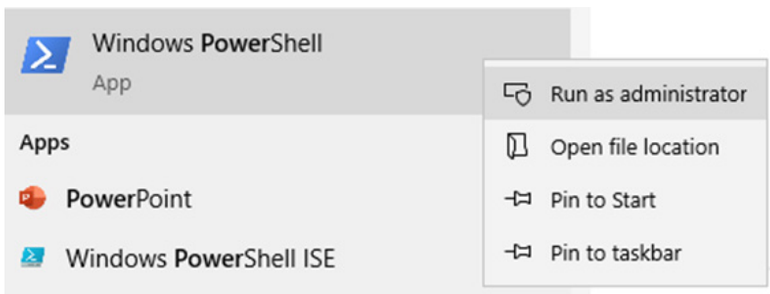
```
Pinging 192.68.3.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

You may need to work with your IT services group to resolve this. Additional troubleshooting steps are provided later in this document

Opening Port 443

Communication between the PC and the AccuPoint® Advanced NG device requires that port 443 allows communication between those endpoints. If there is a locally installed firewall on the PC, then the inbound rule must be added to allow traffic over TCP port 443. Policies must also be added to any installed antispyware or antivirus software as well. A PowerShell script has been provided that will automatically add these rules and local polices. If it failed to execute to during installation, it can be run manually in the steps that follow.

Run the Windows PowerShell application with elevated permissions:



Once the PowerShell command window is open, navigate to the installation folder of the AccuPoint® Data Manager. By default, this is the C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0 folder:

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

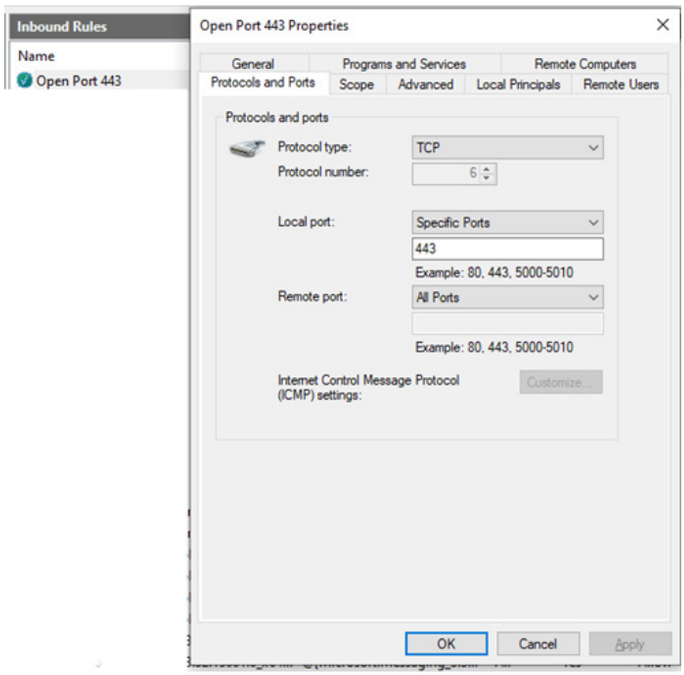
Run the securityConfig.ps1 PowerShell script:

.\securityConfig.ps1

The script will then attempt to implement the security changes it finds and will give a report when finished. Try to configure the device again using the Data Manager software as described in the configuring the device for Wi-Fi section. If this fails to securely connect to the device (the lock icon does not appear), review the exclusions manually.

Reviewing Firewall Settings

The PowerShell script should have installed the proper firewall settings. To review, open the firewall program installed on the PC and review the inbound rules section and look for the open port 443 rule. For Windows Defender, double-click on the rule and switch to the protocols and ports tab.



If this rule is not in the firewall application, then it can be added manually, either by using the graphical user interface (GUI) for the firewall, or running the following from an elevated command prompt:

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

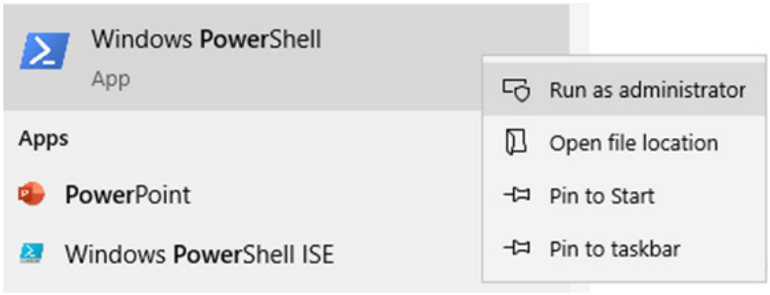
If this fails, please review the additional troubleshooting section below.

Additional Troubleshooting

Network traffic between your PC and the NEOGEN® AccuPoint® Advanced NG device can be blocked for many reasons, which would not be immediately obvious. This includes wireless router configuration, security software running on the same network, local firewalls and networking devices, and application network policies within advanced networking frameworks from vendors such as Cisco and VMWare.

The PowerShell script mentioned previously will list the antivirus and security software running on the data manager PC, but it will not catch everything, and it will not reveal software running on the network at large. This is invoked by following the previous directions.

Run the Windows PowerShell application with elevated permissions.



Once the PowerShell command window is open, navigate to the installation folder of the AccuPoint Data Manager. By default, this is the C:\Program Files (x86)\NEOGEN\AccuPoint Data Manager 4.0 folder.

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

Run the securityConfig.ps1 PowerShell script.

```
.\securityConfig.ps1
```

A text file will pop-up containing what the PowerShell script was able to discover. This will assist you in modifying the local configuration of your security software and providing more detailed requests to your IT services group.

Please save the results to share with your IT services group, if necessary.

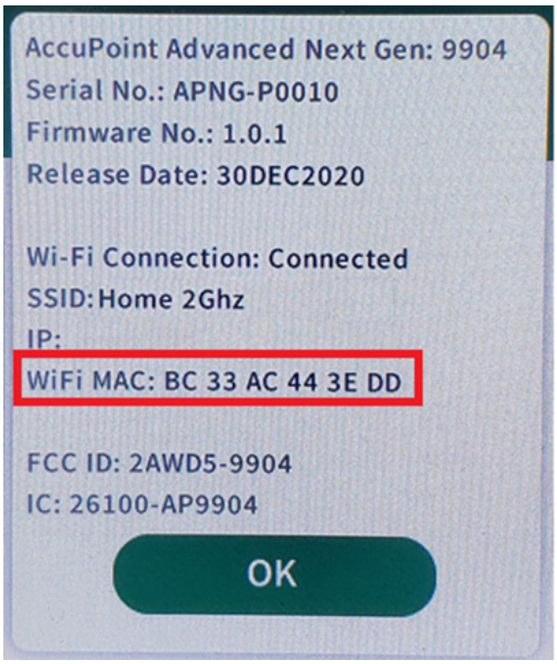
The items that follow are common problems and steps for their resolution.

AccuPoint Advanced NG Device Cannot Connect to Wi-Fi

If after configuring the device for Wi-Fi and powering it off and on, the device is still unable to connect to Wi-Fi, then there is most likely something on your network blocking the device. The following are troubleshooting steps which should help address problems and provide information that can be used by your IT services group.

Register the Device with Your IT Services Group or Local Router

Some networks will only allow recognized devices to connect to their Wi-Fi networks. This means that your organization must register the device as an allowed host. This is usually done by providing the device's MAC address. In the about screen of the device, the MAC address is listed. The following screenshot is from an AccuPoint® Advanced NG device:

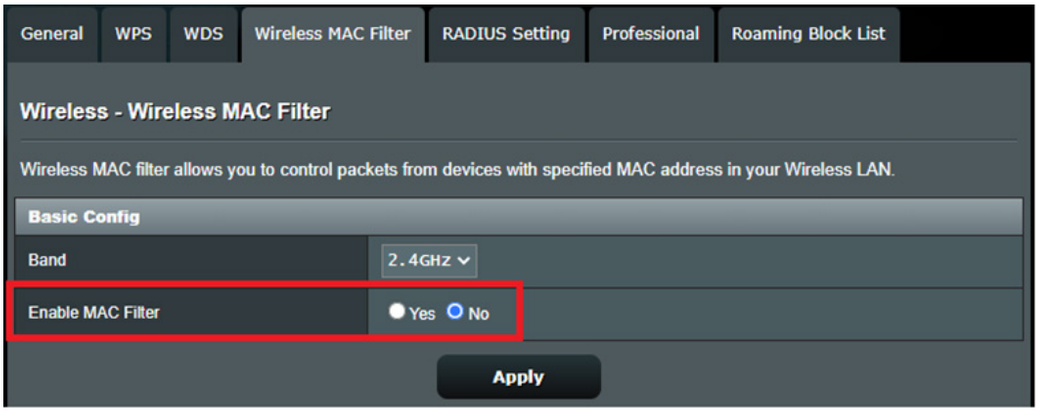


Consult with your organization's IT services team if you need to register your device, then provide them the MAC address listed on your device.

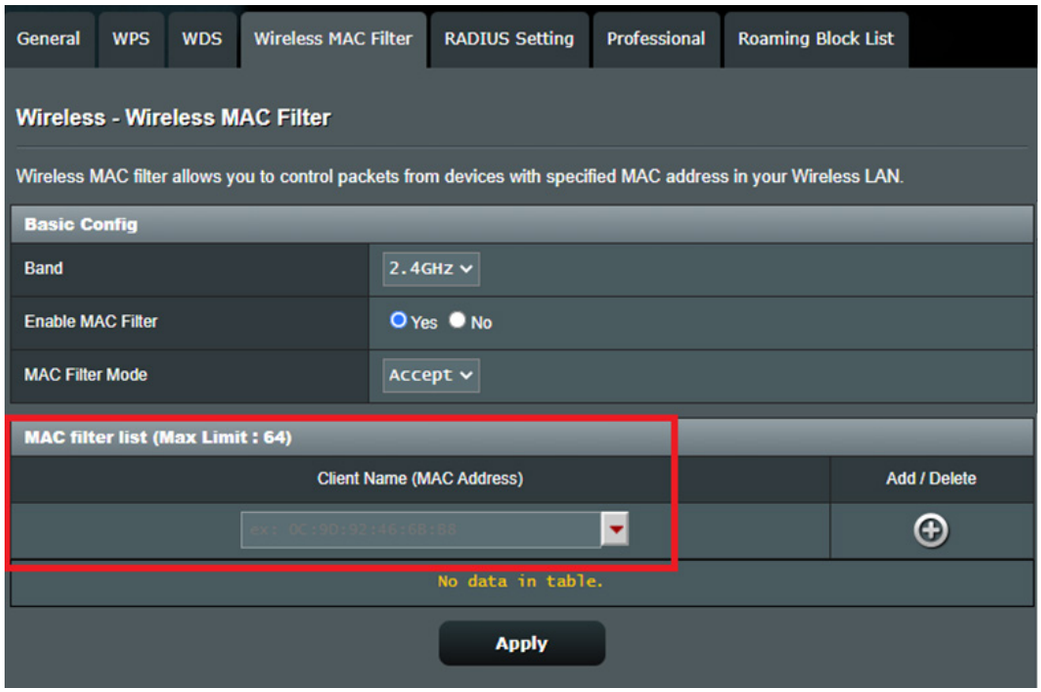
If you are managing your own Wi-Fi router, you need to confirm that your local router does not require registered hosts. This will vary by the brand and type of router. If possible, you should disable MAC-based host filtering on your Wi-Fi router.

Please consult the documentation on your router before making modifications.

The following is a sample screenshot from an Asus Wi-Fi router:



If MAC-based filtering is required, ensure that the MAC address of your AccuPoint® Advanced NG device is listed, or add it to the list of allowed hosts.



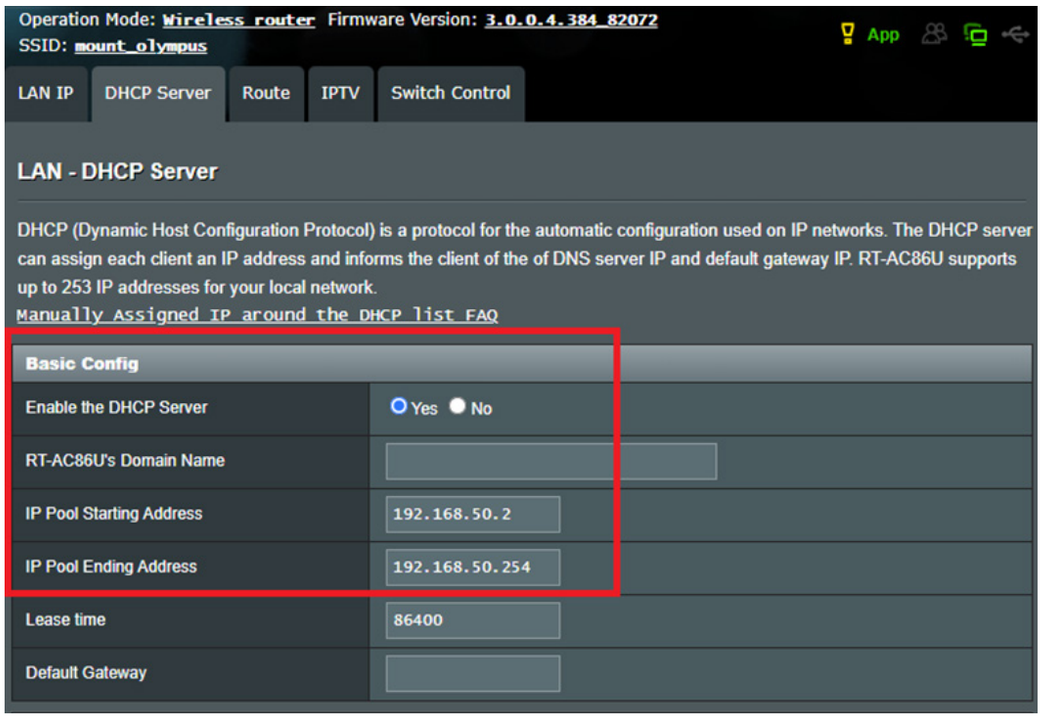
Verify That DHCP Services are Available

In most wireless and wired networking environments, Dynamic Host Configuration Protocol (DHCP) services automatically assign a specific network configuration to any host that does not require a fixed network address. If DHCP is disabled, PCs and other devices will be unable to connect to most networks.

The AccuPoint Advanced NG device requires access to DHCP services.

In a corporate environment, you must confirm with your IT services group if DHCP services are available and enabled for the wireless network you are attempting to connect to with the AccuPoint Advanced NG device.

If using a local wireless access point, consult the documentation on your router to ensure DHCP is configured. In the following Asus router configuration screen, you can see that DHCP is enabled and the address range is assigned to connected hosts:



If the About screen on your AccuPoint® Advanced NG device does not show an IP address in the range displayed on your router, the device was unable to properly communicate with the DHCP service. A DHCP failure will show as an address of 0.0.0.0 or an address that starts with the number 169. Try rebooting and/or powering your router off and on before attempting to reconnect with your AccuPoint Advanced NG device.

If these settings are blank on your router, please consult with your IT services group for the appropriate settings. Your PC and device should be in the same address range, if possible. Setting this range incorrectly can create address conflicts on your larger network.

Verify That the Network Security Software Allows Your Device on the Network

Some organizations run security software that blocks foreign devices from connecting to the local network. You can verify whether this is a problem by attempting to connect with a personally owned device that has not previously connected to the wireless network in question, such as a phone or tablet. If these devices are unable to connect, then you must most likely ask your security or IT services group for an exception to allow the AccuPoint Advanced NG device to connect to the network.

In a corporate environment in which you are required to enter a username and password to access the network, you will need an exception to connect your AccuPoint Advanced NG device, as the AccuPoint Advanced NG device lacks the ability to use a separate account to access a Wi-Fi network. Please consult with your local IT services group to create an exception.

Security software filtering is distinct from the MAC/host-based filtering that occurs on the local router or wireless access point.

AccuPoint® Advanced NG Device Cannot Be Reached with a Ping from the PC

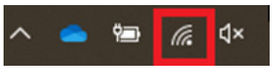
If the device successfully connects, but your PC cannot ping the device there are several possible causes.

Verify that Your PC is Connected to the Network as a Private Network

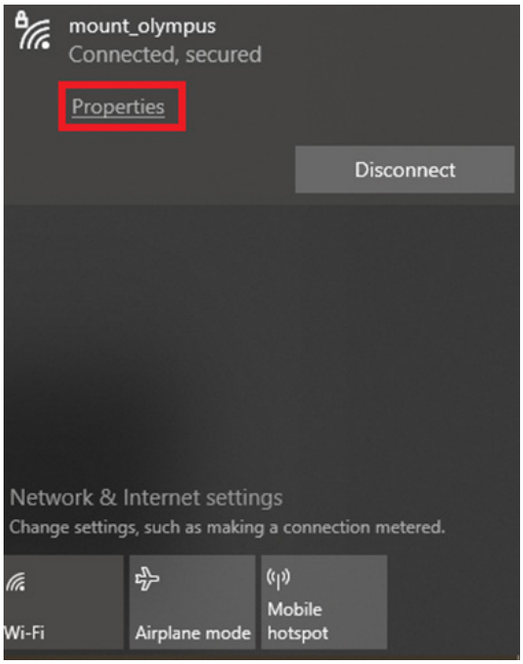
If your PC has connected to a public wireless or wired network, Windows 10 will implement security protocols that will interfere with the communication from the PC to the AccuPoint Advanced NG device. You will need to verify that your current network connection is considered a private network. Look on the lower right corner of your task bar for the networking icon.

A wired network this will appear as follows:

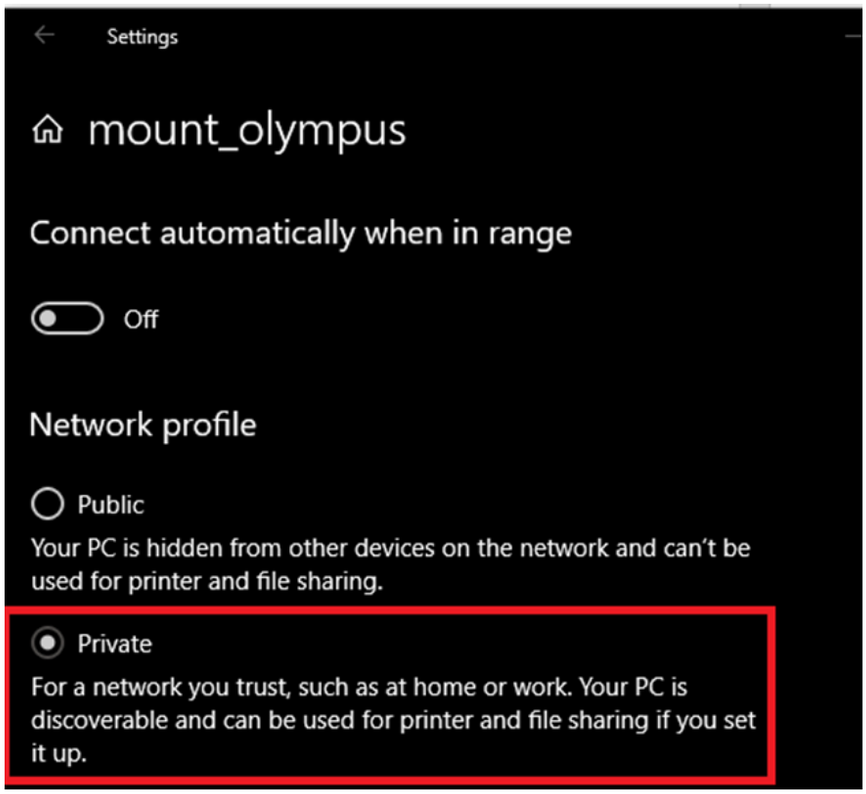
A wireless network, the Icon will appear as follow:



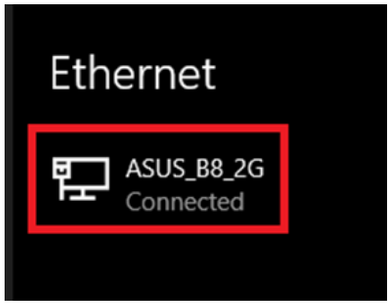
Click on the networking icon, and then click properties.



From the resulting screen, please make sure the private option is selected.



For a wired network, you may see a screen labeled ethernet. Click on the name of your wired network to verify it is set to private.

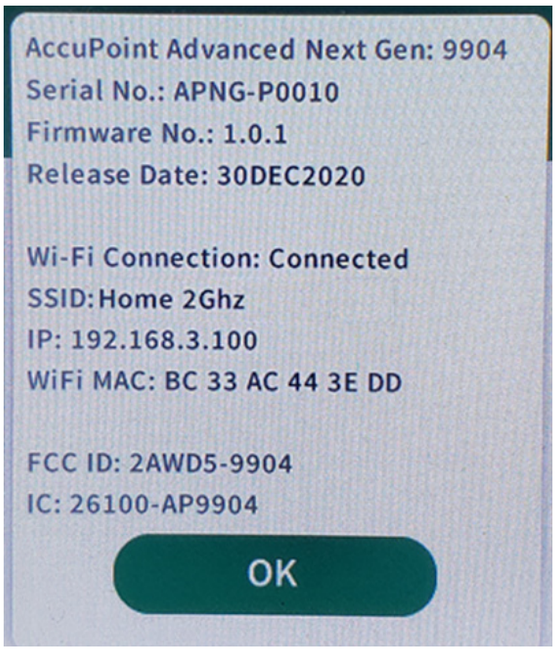


You should use a wired network only if your PC and the AccuPoint® Advanced NG device are considered part of the same local network segment or if your larger network allows devices to connect across network segments. You may need to work with your IT services group to allow connections across network segments. See the next section for how to ensure both the PC and the AccuPoint Advanced NG device are on the same network segment.

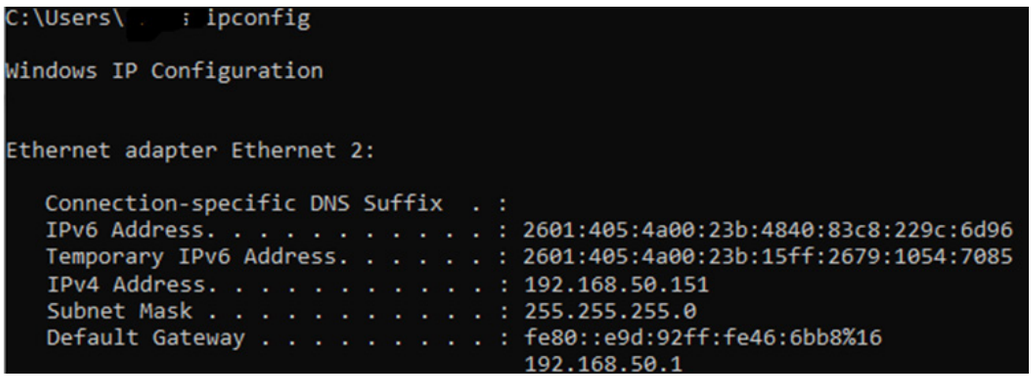
Verify the Data Manager PC and AccuPoint® Advanced NG Device are on the Same Network Segment

This is only necessary if your organization will not allow devices to communicate across your network.

On the about screen, your device will have a specific IP address.



In this case, the network is 192.168.3.x. Devices with a different network range may not be able to detect the AccuPoint Advanced NG device. From your PC, you will need to verify your network address by checking from a DOS or CMD window by using the command IPCONFIG.



The address listed here is 192.168.50.x. In many corporate environments, the PC and the AccuPoint Advanced NG device would not be able to exchange network traffic and connections.

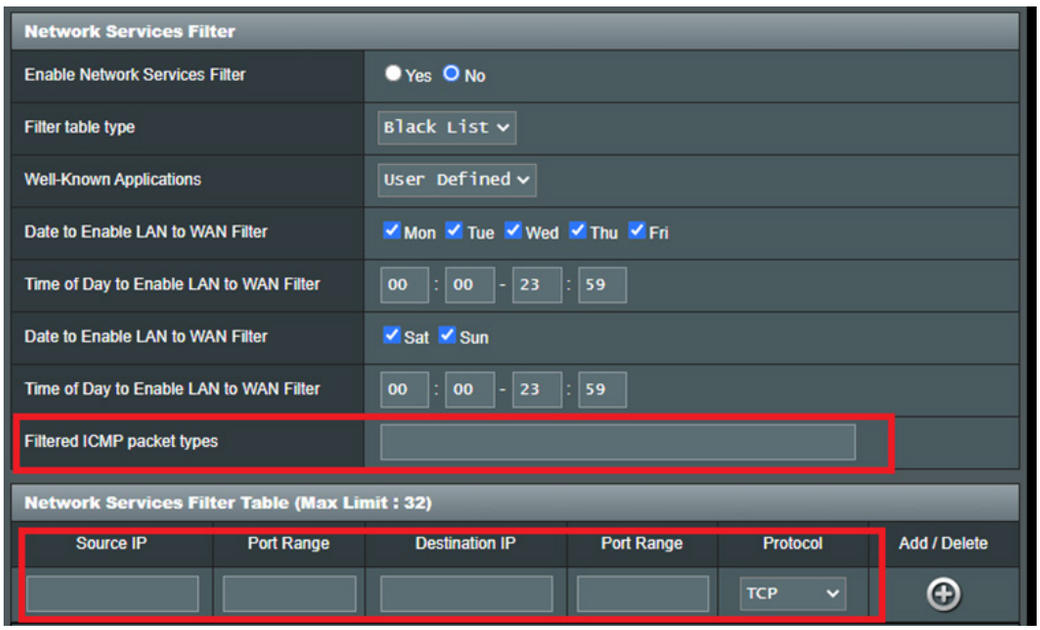
You will need to confirm with your IT services group what restrictions are in place in order for devices to be visible to each other on the network across network segments. A quick resolution may be to connect your PC to the same wireless network as the AccuPoint Advanced NG device. However, this connection will fail when either the PC or the AccuPoint Advanced NG device change locations and connect to different wireless access points.

Verify That Your Local Network Allows Ping Traffic

Some networks block all ping traffic between hosts. Ping uses the protocol Internet Control Message Protocol (ICMP). Many networks will block any traffic over ICMP originating from a PC.

Please consult with your IT services group to ensure host-to-host ping or ICMP traffic is allowed. If not, please ask for an exception. This will make troubleshooting your AccuPoint® Advanced NG device simpler and more transparent.

If you are managing your own wireless access point, please consult your documentation and verify that ping or ICMP traffic is allowed. You may have to explicitly enable ping or ICMP, or remove protocol filters.



Verify That Local Security Software is Not Blocking Outgoing Ping Requests

Some corporate security software will explicitly block outgoing ping requests. You can confirm this by attempting to ping well-known hosts such as www.google.com or 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
```

If this works, you try again with another host or PC on your network that you know is connected. The simplest way is to ping your router. When you issue an ipconfig command, this will be listed as the default gateway.

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

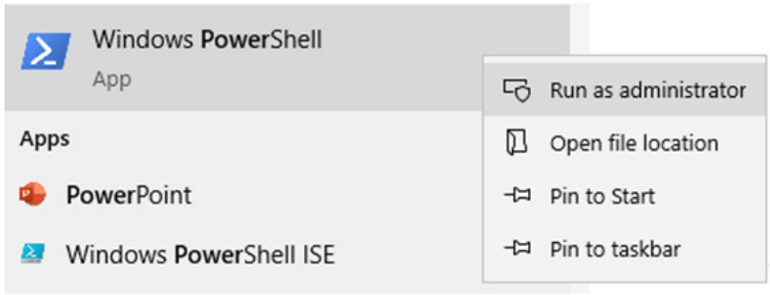
You should always be able to ping the gateway.

```
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
```

If you cannot ping the router, ICMP traffic is most likely blocked and you will need to ensure that your security software allows outgoing ICMP traffic.

Adding Rule to Unblock ICMP

If you have a rule in place that is blocking ICMP traffic, you can unblock it by creating a rule as an administrator on the data manager PC. Run the Windows PowerShell application with elevated permissions.



Once you have opened PowerShell, enter the following text to enable Ipv4 ICMP traffic and press enter afterward.

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

Optionally, if you wish to enable Ipv6 ICMP traffic, enter the following text and press enter afterward.

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

Ensure Enterprise Security and Network Software Allow Traffic Between Your PC and the AccuPoint® Advanced NG Device

Many commercial network security packages will block networking traffic between devices on the network unless explicitly allowed. This includes:

1. CISCO Application Centric Infrastructure (ACI), which may have policies to block traffic between unauthorized hosts. A new policy may be required.
2. CrowdStrike, which runs locally as an agent and accepts policies from a central server, may override changes to the windows firewall, blocking both ICMP and secure traffic to the AccuPoint device. Your IT services group may need to add exceptions.
3. Rapid7, which is similar to CrowdStrike, may require policy overrides to allow traffic.

Your IT services group may issue Windows policies that block communication between the PC and the AccuPoint Advanced NG device, including preventing updates to firewall rules.

You can use the TRACERT command, described earlier in this document, to identify the path from the data manager PC to the AccuPoint Advanced NG device. If the TRACERT request fails, traffic is being blocked. If the TRACERT succeeds, but the PC and AccuPoint Advanced NG device cannot communicate, the ports used by the device and the PC are being blocked. A failure will show as follows:

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.

Ensure Network Firewalls Are Not Blocking Network Traffic

Some networks are broken up by internal firewalls to protect sensitive areas, such as labs and production areas. Firewall rules or exceptions may be required if the network traffic between your PC and the AccuPoint Advanced NG device need to traverse one or more firewalls. The TRACERT command will assist in diagnosing a firewall problem as well.

Please consult with your IT services group to see if your PC and AccuPoint Advanced NG device must traverse one or more firewalls to communicate.

Transfers Cannot Be Initiated to the AccuPoint Advanced NG Device

The most likely root causes of this issue are the traffic on port 80 being blocked to the AccuPoint Advanced NG device, or the traffic over port 443 being blocked between the device and the PC.

To initiate a transfer from the PC to the AccuPoint Advanced NG device, the data manager sends a message to the AccuPoint Advanced NG device over port 80. The device then connects back to the PC over port 443, transferring information securely over TLS. Blocking traffic on either of these ports will interfere with data synchronization, including pushing site plans.

Traffic on Port 80 is Failing to Travel from the PC to the AccuPoint® Advanced NG Device

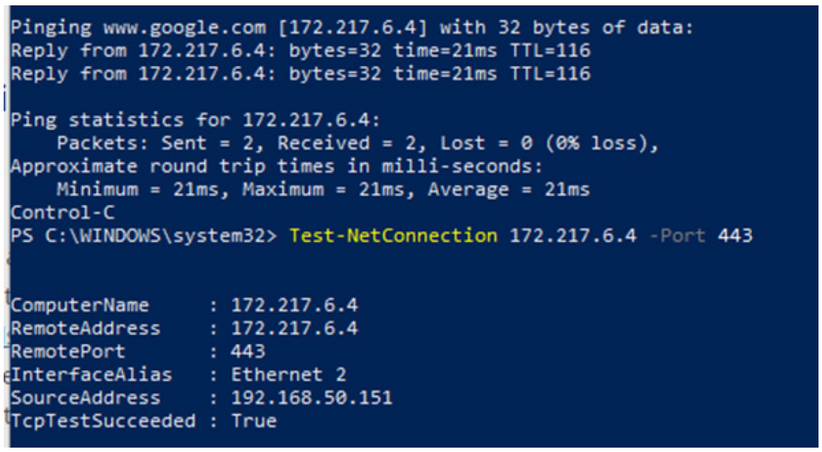
Most of the fixes used to resolve the ping issues listed above can be used for the same resolution between the PC and the device. The PC initiates contact with the device on port 80. Traffic of this sort is often flagged by security software and security devices.

Additional interference can be caused by web security agents that simply work to block outgoing traffic on port 80. While no sensitive data is transferred over port 80, port 80 is typically considered an insecure port.

The AccuPoint Advanced NG device must receive a wake-up message telling it to initiate secure communications with the PC over port 80.

Perform the first check listed under the AccuPoint Advanced NG device cannot be reached with a ping from the PC section to ensure that your PC is connected to its local network as a private network. If this is not issue, please continue with the steps listed below.

The best way to check to see if this is a problem is with the PowerShell command Test-NetConnection. The following example shows how to test Google.com for port 443:



The command to test the AccuPoint Advanced NG device would be:

Test-NetConnection <ip of device> -Port 80

If you do not see success, then port 80 is being blocked. Work with your IT services group to resolve this. You may need exceptions for the data manager PC or the AccuPoint Advanced NG device.

Traffic on Port 443 is Failing to Travel from the AccuPoint Advanced NG Device to the PC

The data manager PC uses the Data Manager software to host a lightweight service on port 443 over TLS.

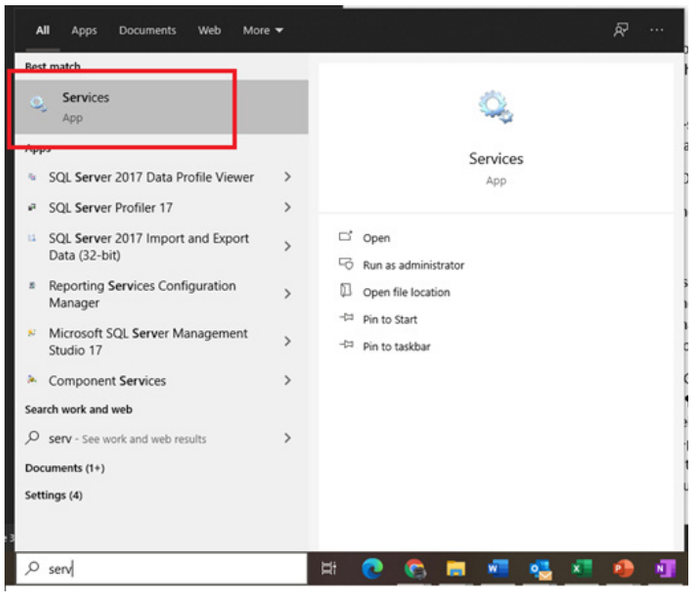
Most of the of issues blocking port 443 traffic are resolved by implementing the problem resolutions listed above blocking ping. However, the rules would be configured differently. Allowing incoming SSL traffic on port 443 to your PC may require one or more of the following:

- Adjusting internal network firewall rules.
- Adding policies to enterprise security software.
- Adding policies or exceptions to network control softer, such as ACI.
- Adding Windows group policies to allow local firewall changes.

You should also check that the data manager PC is listening on port 443 by using the command:

netstat -an

If port 443 does not appear on the output of this command as listening, please reboot the PC and test again. If it still fails, please look at the list of services on the PC and verify that the Data Manager software is running on the PC.



If the service is running, and the netstat command shows that the data manager PC is listening on port 443, then you will need a second PC to test access to port 443. Please issue the following command from another PC using PowerShell to the data manager PC:

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

If this command fails, follow the previous troubleshooting recommendations.

Summary

When properly configured with no signal interference, data transfers between the data manager PC and the AccuPoint® Advanced NG device should be quick and reliable. However, when bringing on a new device to a corporate network, traffic can be blocked in many ways. Please remember the following and refer to previous sections of this guide to troubleshoot or resolve these problems:

1. Properly configure the AccuPoint Advanced NG device for Wi-Fi connectivity using a USB connection to the device from the data manager PC.
2. Run the provided PowerShell script, which will configure the local firewall and security software on the data manager PC, or provide recommendations for your IT services group.
3. If the device cannot connect to your Wi-Fi network, then either the wireless access point, the internal firewalls or the security software, or other security appliances are blocking the device.
4. If the device can connect to the Wi-Fi, but the lock icon will not appear, then your PC cannot accept incoming connections on port 443.
    a. Verify that the Data Manager software is running on your PC and listening on port 443.
    b. Run the other troubleshooting steps.
5. If the device can get a lock icon, and data transfers (syncs) can be initiated from the device but not the PC, then network traffic on port 80 from the PC to the AccuPoint Advanced NG device is being blocked.

This guide will be updated as necessary. This includes when new or updated configuration information is available, or when additional troubleshooting guidance would be helpful.