Version 5.0.0 r3

Q-Net Quick Start Guide

Q-Net Security

Document Copyright Notice

Q-Net Security Patents

This product is covered by one or more U.S. patents or patent applications. For details, see https://qnetsecurity.com/patent.

Open Source Software

Following industry standard practice, Q-Net Security uses various common open source software libraries in its products. These libraries are distinct and separated by common interfaces from Q-Net Security's proprietary code and technologies. The open source software libraries that are delivered with the product are listed here: http://qnetsecurity.com/.

Table of Contents

1 What is a Q-Net?

Q-Net is a system designed to protect in-flight data between endpoints using patented, quantum resistant encryption running directly on hardware. A Q-Net is capable of designating a unique encryption/decryption key for every packet transmitted over the Q-Net. A Q-Net consists of two main components: The Q-Net Policy Manager (QPM) and Q-Net devices (e.g., Q-Boxes).

A Q-Box is the hardware device that performs the encryption/decryption that protects the data. It connects to the endpoint being protected via one port and your existing network on the other port. An endpoint connected to a Q-Box can only communicate with another endpoint that is also connected to a Q-Box (unless the endpoint has another NIC directly connected to the network).

The QPM is a rack mount unit that is connected to a network containing the Q-Net system. It is the centralized unit for registering, configuring, and monitoring a Q-Net via a web-based GUI.

Q-Net devices work on the transport layer to encrypt/decrypt the following protocols:

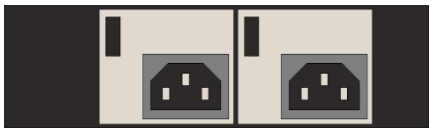
- UDP
- TCP

Q-Net will not pass any data that is not on one of the transport layer protocols listed. All data and protocols above the transport layer (e.g. HTTP, SSH, etc.) will work with Q-Net (i.e., is encrypted/decrypted).

2 Getting Started

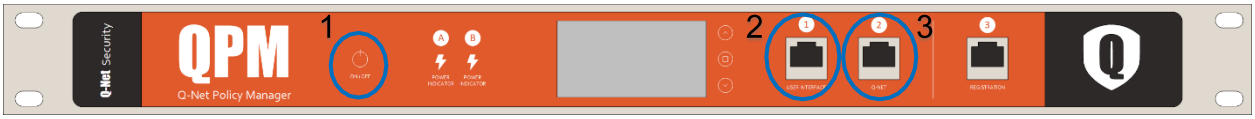
2.1 Connect the QPM

Plug one or both included power cords into the power supply connectors on the back of the unit.



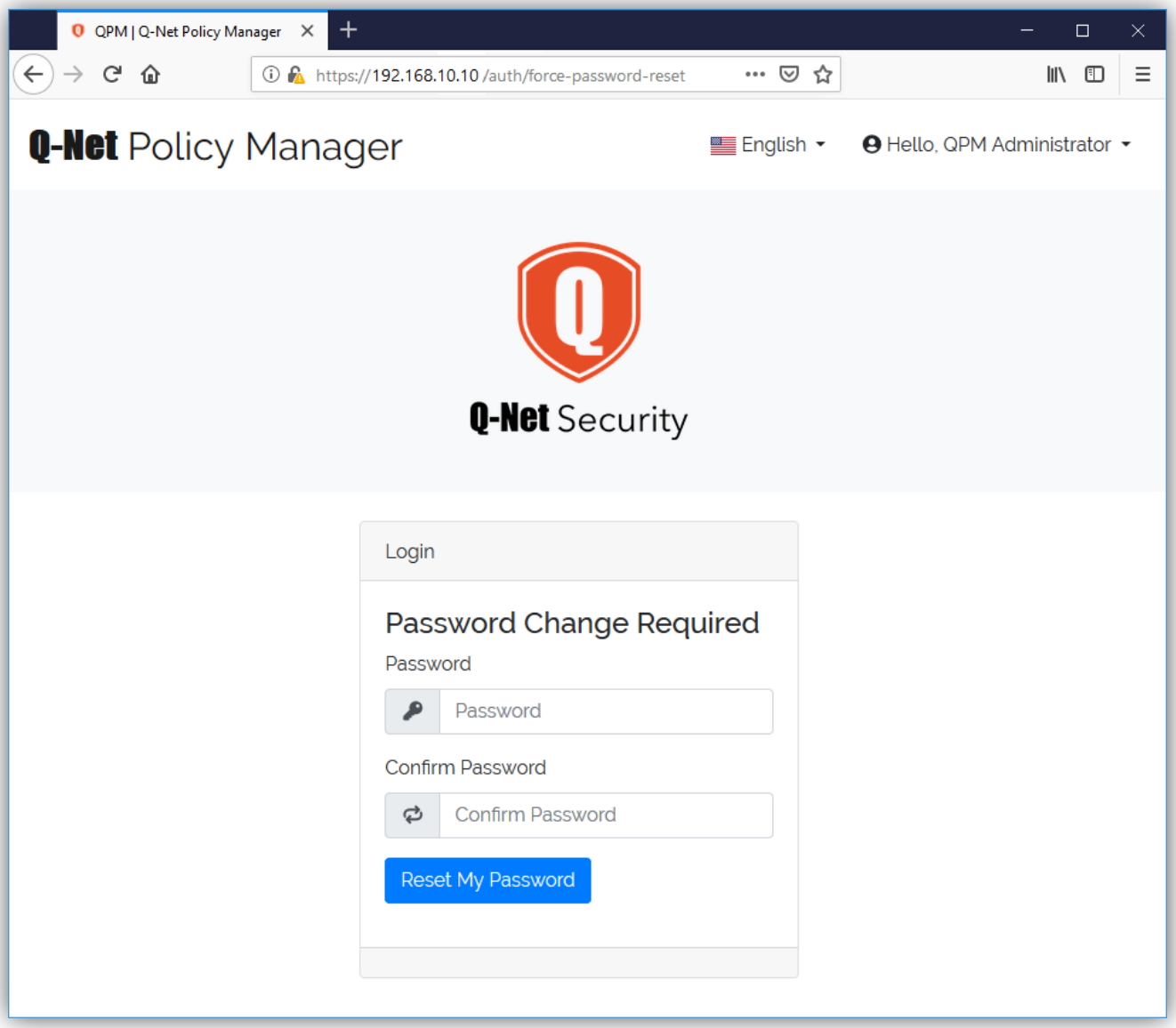
Power and connect the QPM to the Network, as follows:

1. Press the Power button on the QPM.
2. Plug an Ethernet cable into the Console port that is on a network with access to the QPM (typically an internal network). The default IP address of the QPM Console port is 192.168.10.10, however, your QPM may be configured to the address specified in your proof-of-concept (POC) questionnaire.
3. Plug an Ethernet cable into the Q-Net port that is on a network with access to the Q-Boxes. This can be the same network as the QPM Console port or any other network, for example, a VPN or leased line network.



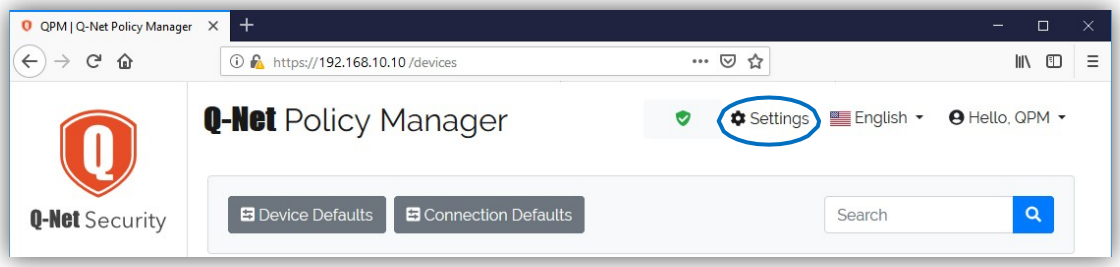
2.2 Log in and Configure the QPM

Access the QPM at the default IP 192.168.10.10. Note that the username and password will be provided to you during your scheduled setup call with the Q-Net team. After this call, you may change the default username and password.

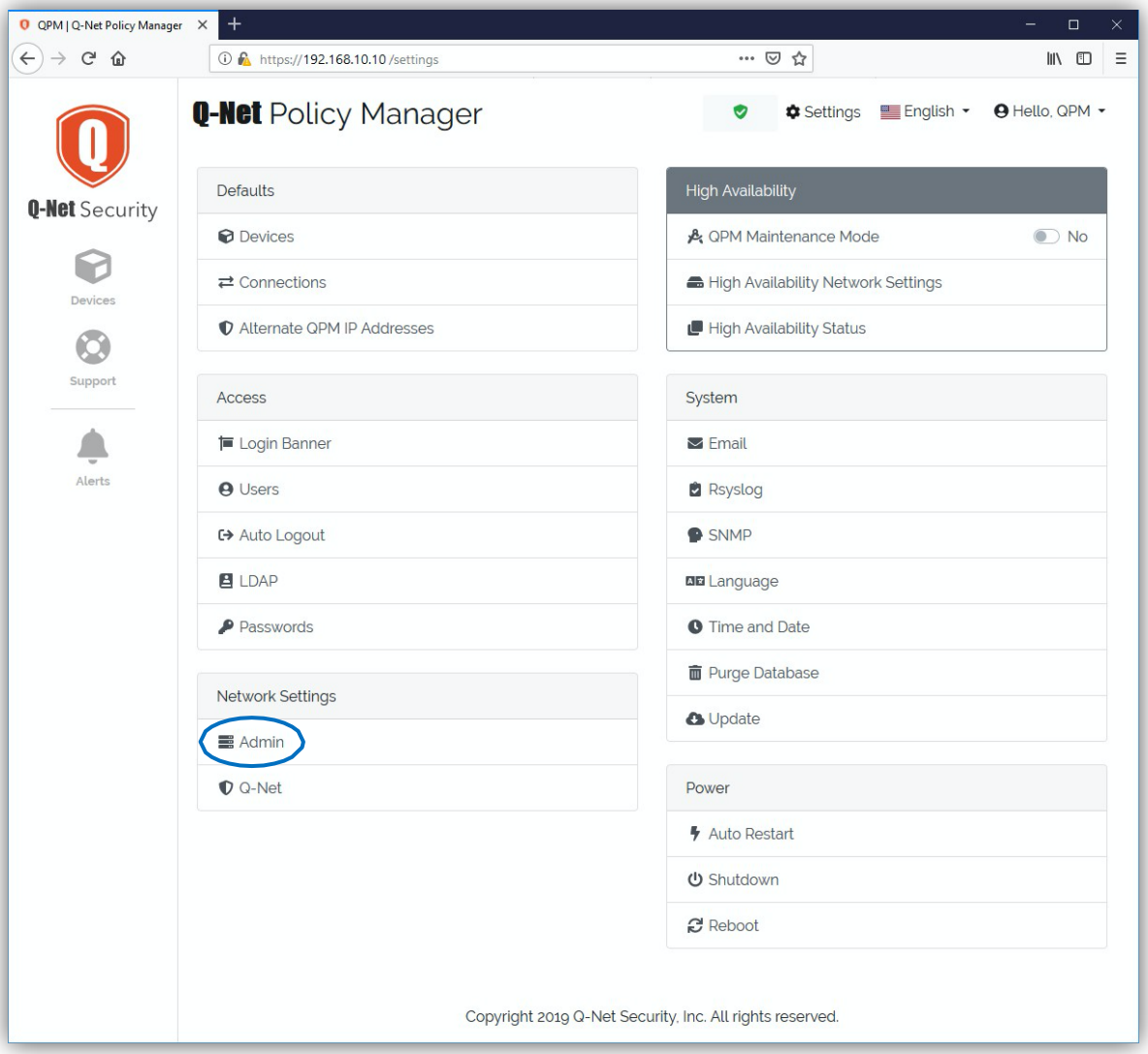


Setup the QPM GUI to be accessed by users on your network as follows:

1. Access Settings



2. Open the Admin Settings

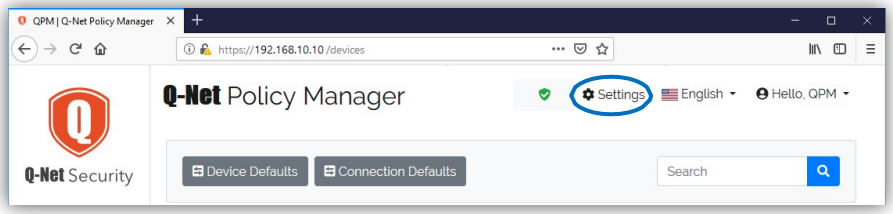


3. Set up the Admin Network Settings so the GUI can be accessed on your Network. In general, the QPM should be accessed on a static IP of an internal network. Assure the Gateway and Network Mask are compatible with the IP Address and enter DNS addresses used by your network (if needed). Click “Save” to have the QPM accessible at the desired IP Address. **Note:** After clicking save, you will have to navigate to the new QPM IP address in the web browser.

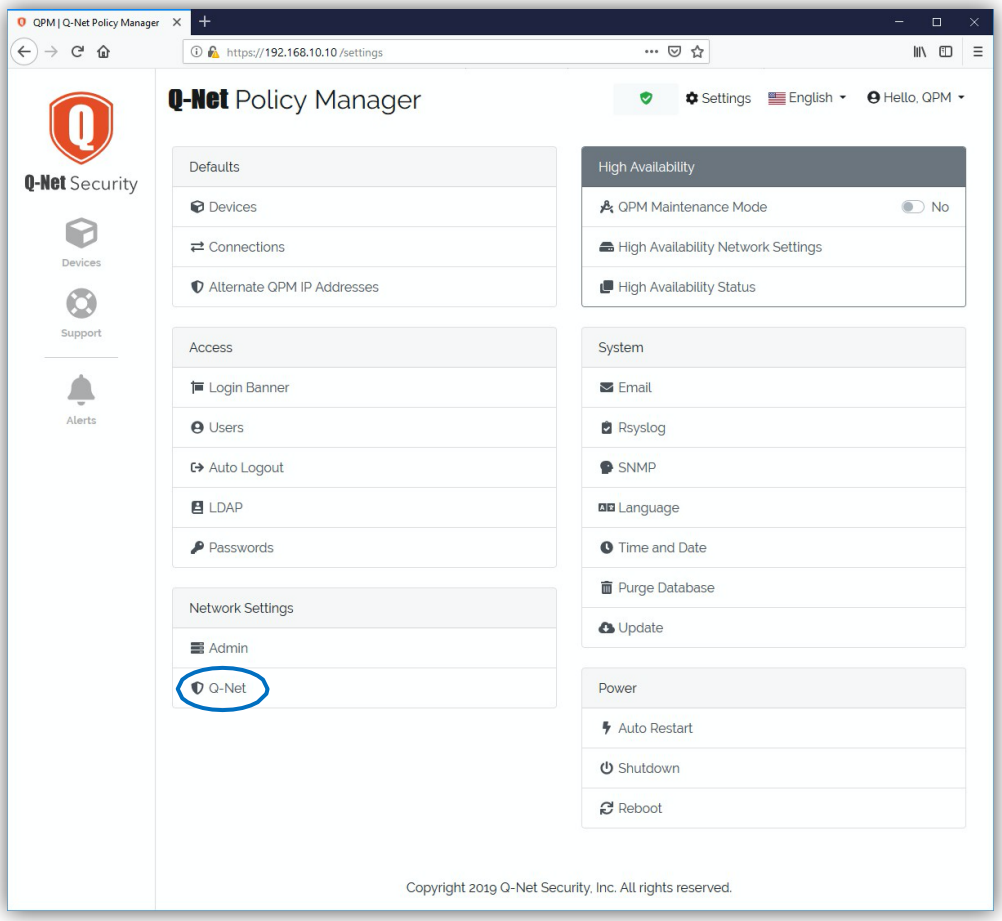
Set up the Q-Net Network settings to allow access to Q-Net devices, as follows:

1. Access Settings

Getting Started



2. Open the Q-Net Network Settings



3. Set up the Q-Net Network Settings so Q-Net devices can be accessed on your Network. The Local IP address is required to allow Q-Net devices to reach the QPM. The External IP is optional but is needed if the Q-Net devices are behind a NAT or Proxy server. Make sure the Network Mask is correct for the Local IP Address and set the Enrollment and Admin Ports. These ports can be set to any valid port value but need to be configured to allow UDP on the firewall, NAT, or Proxy if Q-Net devices are behind any such network services. Click "Save" to have the QPM accessible to Q-Net devices.

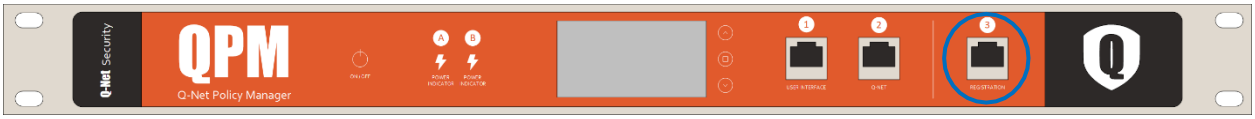
   Note: Q-Net also supports Alternate IP Addresses to accommodate more advanced NAT configurations. Alternate IP Addresses are managed under Settings/Defaults/Alternate QPM IP Addresses.

2.3 Register Devices

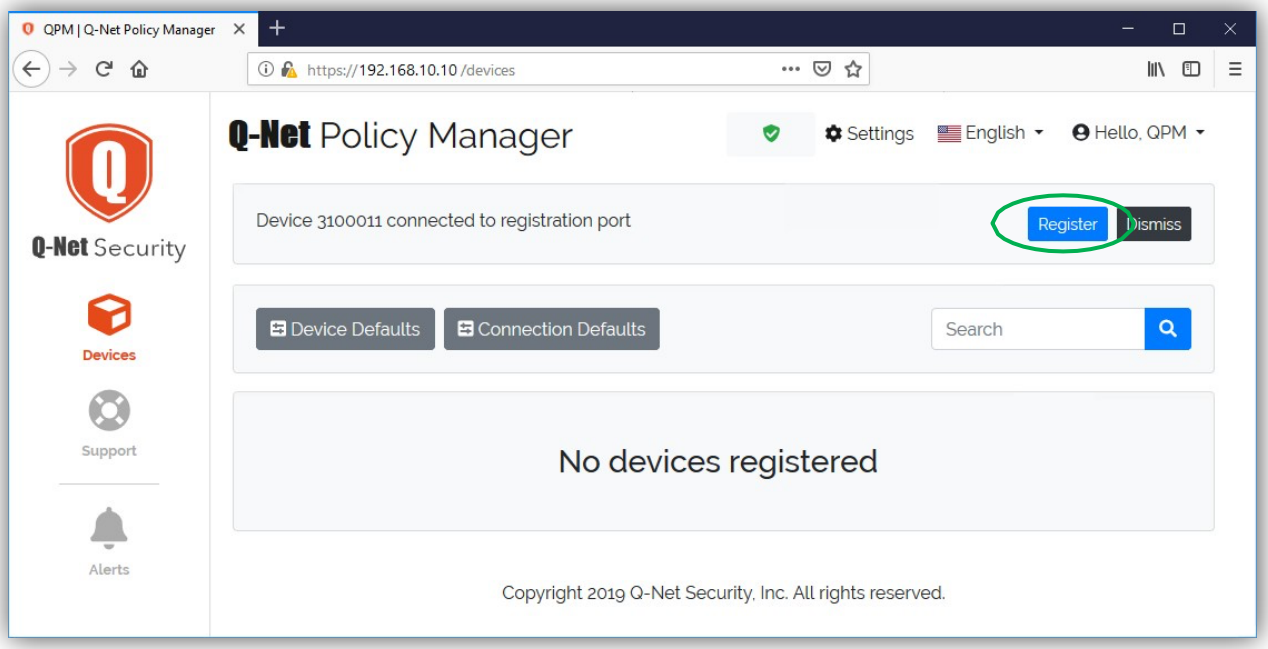
Devices must be registered to the QPM to allow Q-Net devices to connect to each other and exchange information with the QPM. Each Q-Net device must be registered using the following procedure:

1. Plug the included power cord into a wall socket and then into the power port on the Q-Box.

2. Plug one end of an Ethernet cable into the “Endpoint” port on the Q-Box and the other into the QPM registration port.



3. Go to the QPM GUI and wait for the “Registration” button to appear. Click “Register” to open the device registration page.

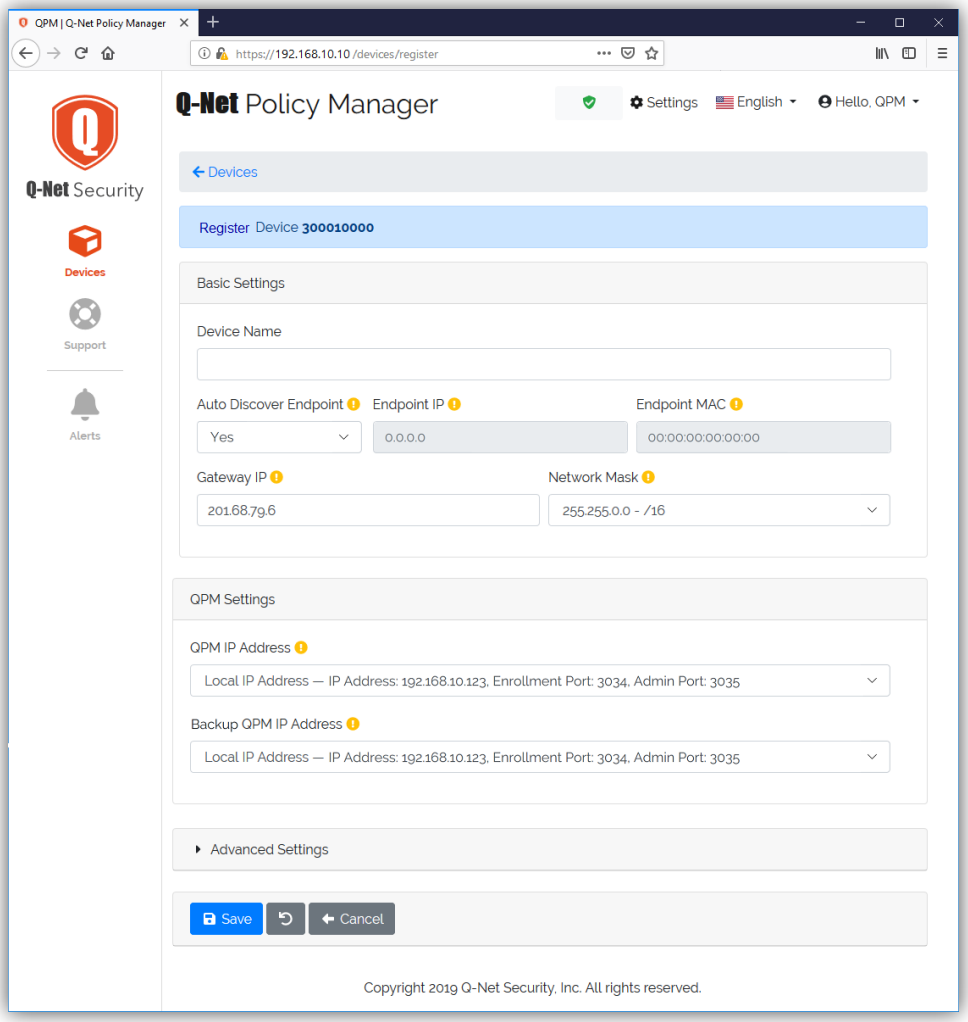


4. Enter following Basic Settings to register a device:

    a. Device Name – A descriptive name up to 100 characters

    b. Auto Discover Endpoint – The Q-Box can auto discover the IP and MAC addresses of the connected endpoint. If this option is chosen, the address fields will fill in as soon as the device is enrolled and can be viewed on the Device page. If Auto- discover is set to no, the user must manually enter the endpoint IP and MAC addresses.

    c. Gateway IP –The user must enter a Gateway IP appropriate for the IP Address of the endpoint.



5. Enter the QPM Settings to register a device:

6. Choose the QPM IP Address and ports from the drop-down list. This may be the Local, External, or Alternate IP Address configured earlier in Q-Net settings and/or Alternate QPM IP Addresses.

7. If configured for High Availability, the user must also enter the IP Address of the Secondary QPM, otherwise None should be chosen.

8. Click “Save” to complete device registration. The user will receive a confirmation the device was registered successfully or a failed message with an error if there was a problem.

2.4 Q-Net Topology

It is recommended that the Q-Net topology be designed before fielding Q-Net devices. Although there is no explicit step to lay out the Q-Net topology in the QPM, there are helpful tools to make it easier. Before we discuss topology, it is important to know how we define communication between Q-Net devices and limitations of the system. Q-Net devices must be configured to communicate with each other by configuring connections and associated properties. A connection has two connection parameters; 1) MTU and 2) Key Use. The MTU defines the Maximum Transmission Unit for all communication between devices (on that connection) and Key Use defines how many packets each key encrypts/decrypts.

A connection must have at least one property that consists of a destination Port Type, the port(s) it will travel on, and the protocol(s) supported (TCP and/or UDP). A single Q-Net device can have up to 2000 total properties in any combination. For example, one device can communicate with 2000 other devices that each have a connection with one associated property, or it could have one connection to one other device with 2000 associated properties. If a property is unidirectional, dynamic connections will be made and will figure into the equation of total properties allowed. Please refer to the User Manual for more information. This understanding can help lay out the topology of your Q-Net.

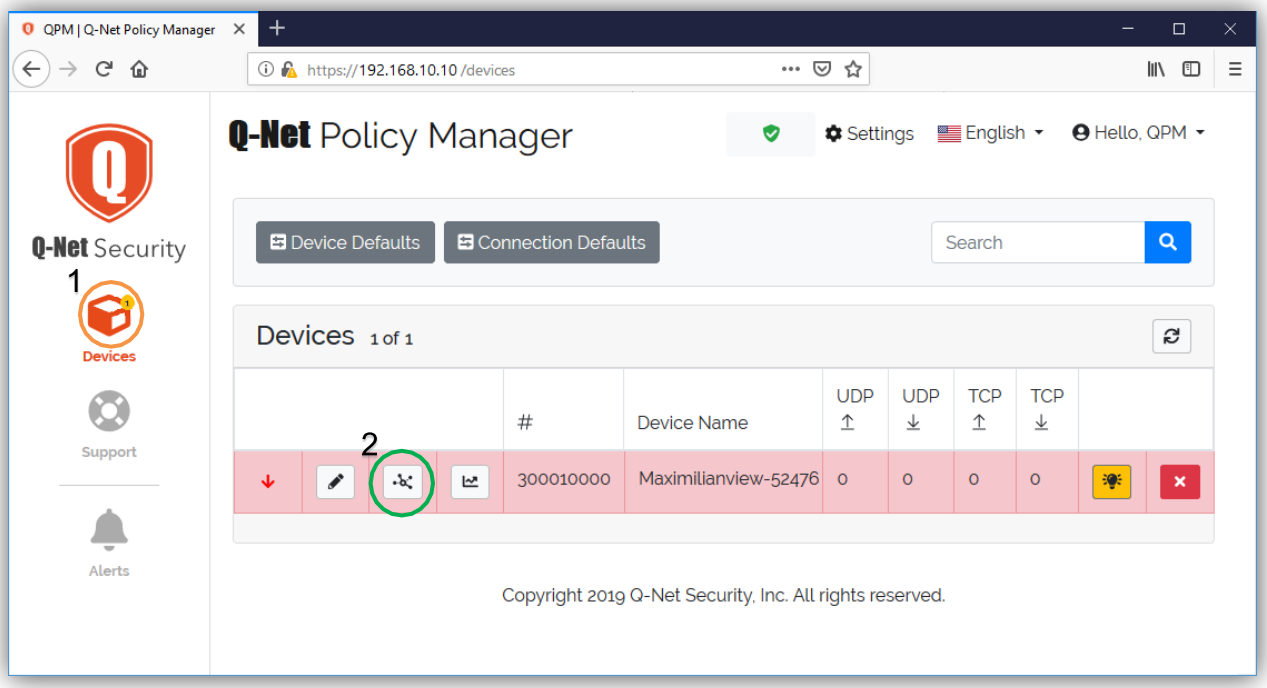
Q-Net does not dictate network topology and is designed to work with existing networks. A simple topology where every Q-Net device can talk to any other Q-Net device may be desirable (with the limit of 2000 properties per device). A company may want one to centralize communication by having one device talk to many devices, much like a hub and spoke network. It also may be helpful to have the central device in one hub and spoke talk to a hub in another hub and spoke. In this case, each device that is the hub like device can only have 1999 devices in its network, so it has one property available to communicate with the other hub like device. Carefully thinking out the Q-Net topology before deployment can be very helpful in saving time reconfiguring Q-Net connections and properties in the future.

2.5 Make Direct Connections

After registering devices and thinking about topology, you are ready to make connections and install devices. A device does not need to be fielded to allow connections, although it can be. Therefore, you can make connections before or after devices are deployed in the field.

To enter the connections page for a device:

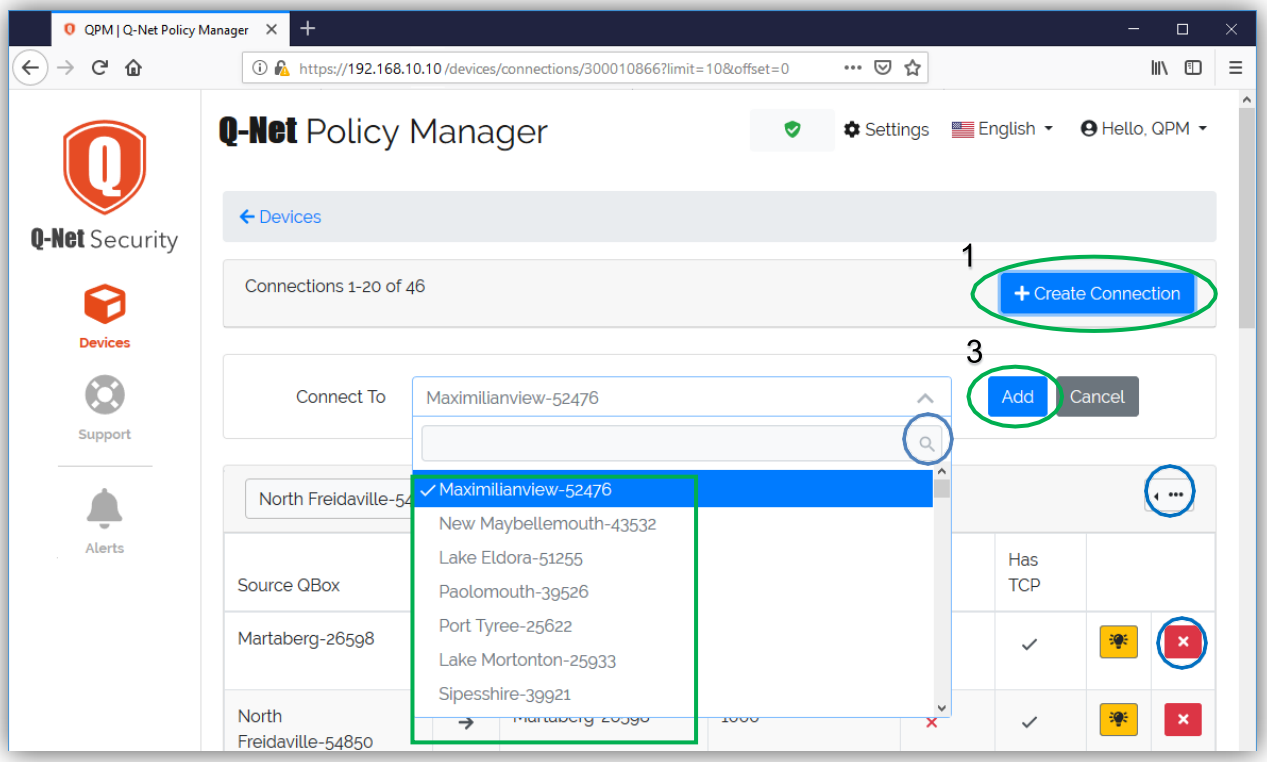
1. Click the Devices Icon.
2. Click the Connections Icon.



To create a connection:

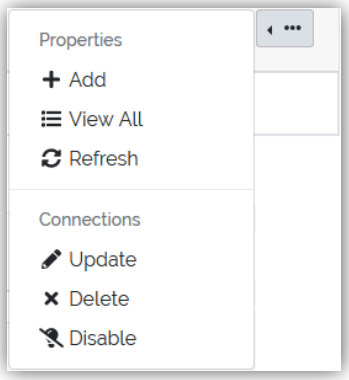
1. Click Create Connection at the top right.
2. Choose the device to connect to from the drop-down list.
3. Click Add.

Note: If there are a lot of devices in the system, you can limit the devices in the list by using the search built into the list.



The added connection appears at the bottom of the connections list displaying the two devices in the connection and information for the properties created. The connection automatically creates two properties (one for each direction of traffic flow) using the default connection properties managed in **Settings**. If the desired behavior is for traffic to only be initiated in one direction, the user can delete the property by clicking the red x next to the property.

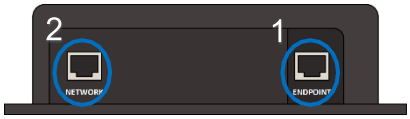
Connections and associated properties can be modified by the clicking the icon with an arrowhead followed by an ellipsis at the top of the connection to display the following options:



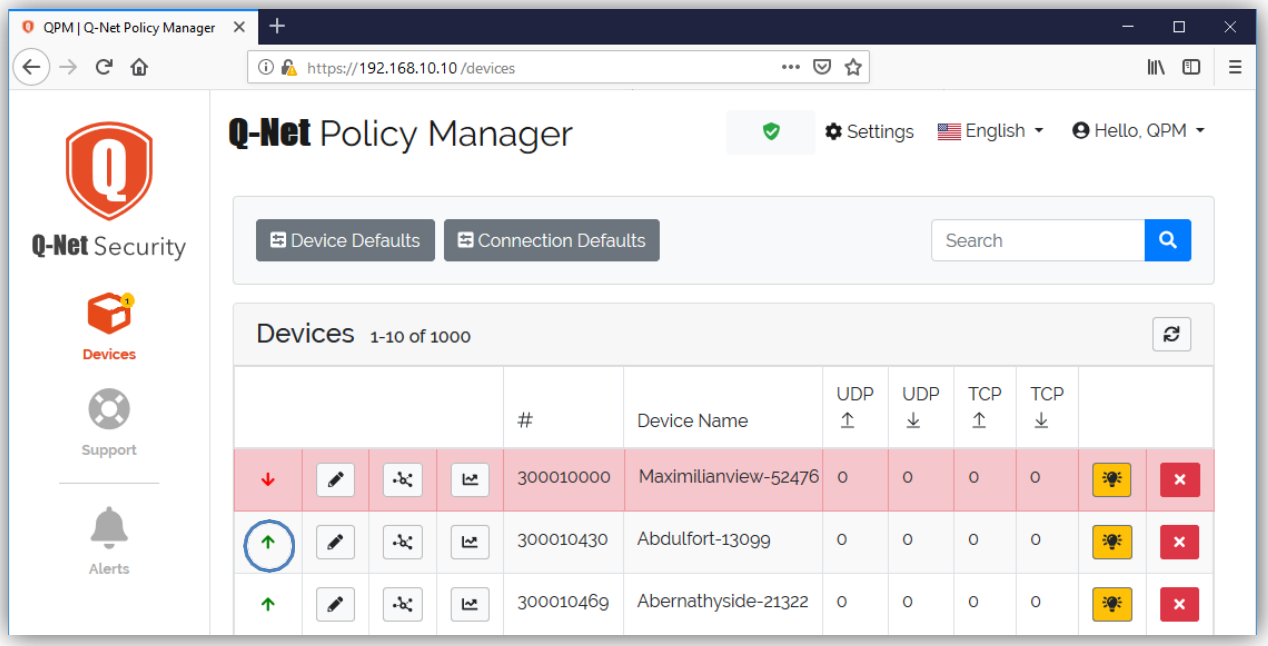
2.6 Install Devices in the Field

If you've already made your connections via the QPM, all you need to do is plug in the power to a wall socket and the Q-Box power port and connect to the Endpoint and Network as follows:

1. Plug an Ethernet cable from the computer you're connecting to into the Endpoint portof the Q-Box.
2. Plug an Ethernet cable from your network connection to the Network port of the Q-Box.

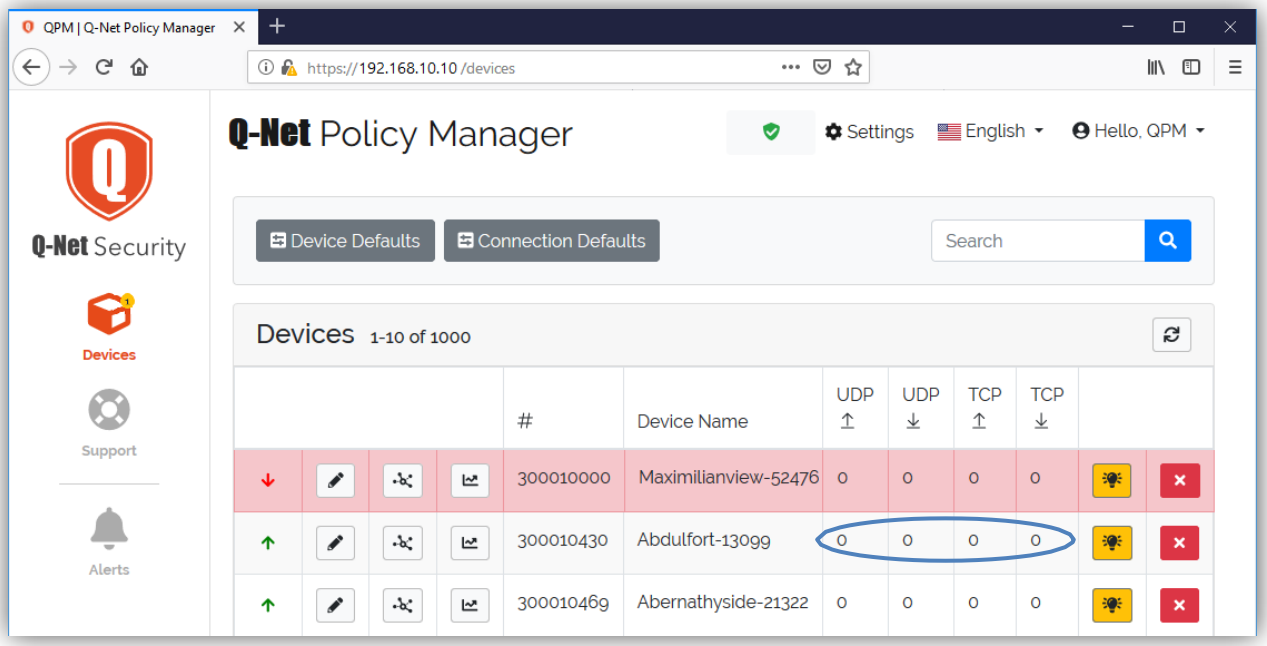


Once the Q-Box receives an identifying message from the endpoint (like an ARP) it will automatically enroll with the QPM and the device will indicate it is online with an upward green arrow in the Devices view of the QPM. Upon installation of two or more Devices with configured connections in the QPM, traffic will start to flow encrypted to and from the endpoints.



2.7 Make Sure It's Working

A user can confirm Q-Net devices are communicating with each other by viewing the Devices table and observing that at least one of the transmission/reception values is greater than 0.

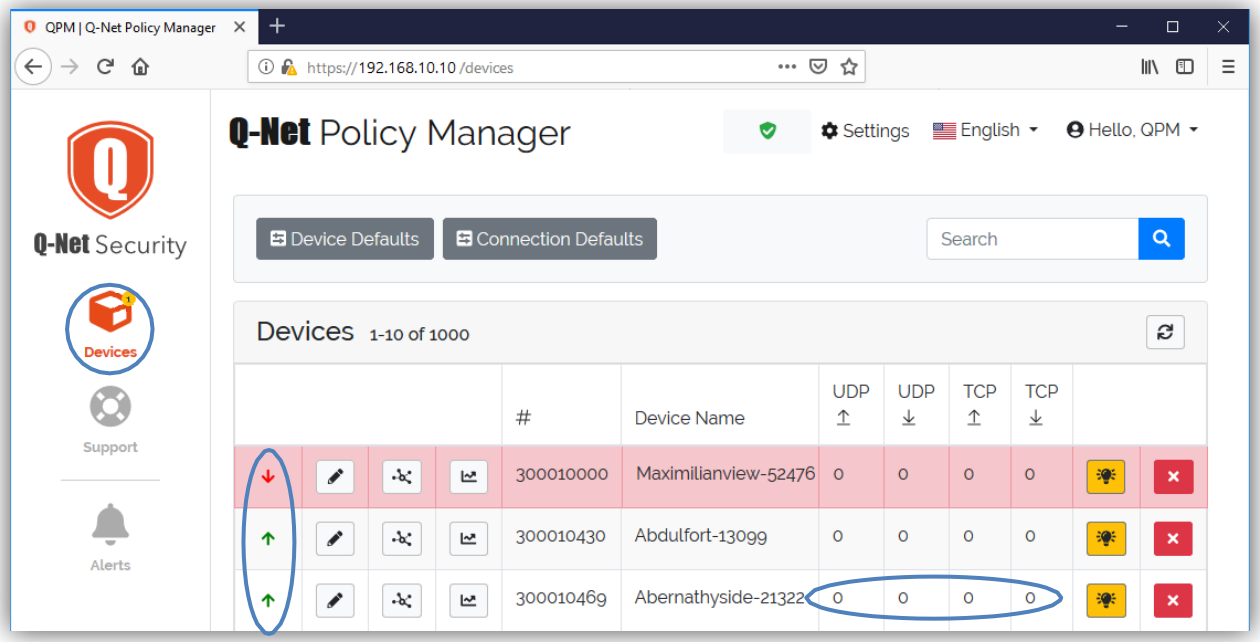


That's it, your Q-Net is now up and running.

2.8 Monitoring

Simple monitoring of the system can be done through the Devices view main page. Through this view you can quickly see

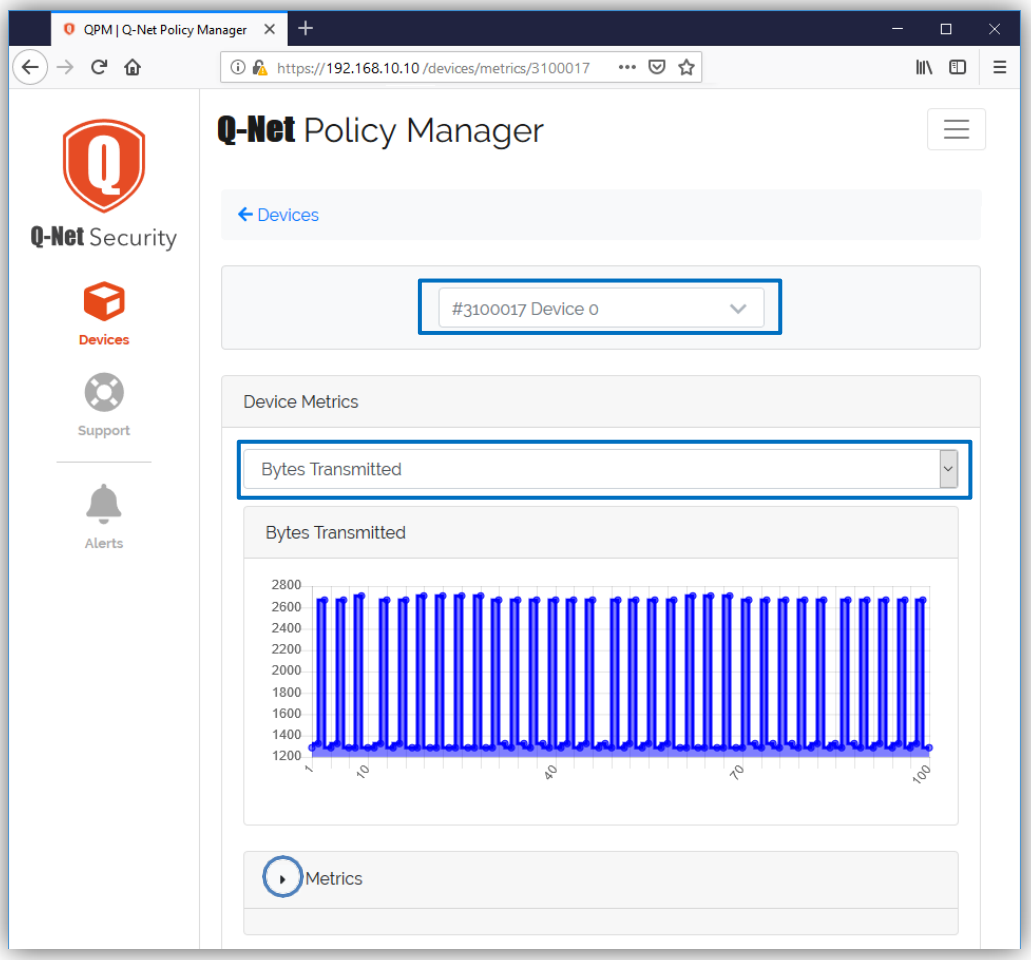
1. how many devices are not connected,
2. which devices are connected/not connected, and
3. overall transmission of UDP and TCP transmitted and received data in bytes.



More advanced traffic monitoring can be performed through the metrics view of each device. Click the graph icon of the device to view Bytes Transmitted and Bytes Received graphs of up to the last 100 data points.

The data being viewed can be changed via the dropdown above the graph and datapoint values can be viewed by clicking the arrow next to metrics. The device can also be changed with the dropdown at the top of the page.

Getting Started



3 Best Practices

3.1 Network Topology

The QPM is designed to be placed in a server rack with the normal security, access control, and UPS backup typically provided in a server room.

The QPM administration port (from which you access the web portal), should itself be protected by a Q-Box, to ensure malicious access to the whitelist is not permitted.

Warning: A Q-Box cannot be placed in front of the network port of the QPM, as this will disrupt communication. All traffic on the network port is already encrypted with the Q-Net protocol.

Warning: The IP address of the network port and admin ports on the QPM should never be set to the same address.

The QPM and Q-Boxes are designed to work with your existing network switches and routers. In particular, a firewall with attack protection, anti-virus, anti-spam, and Intrusion Detection and Prevention is highly recommended. Q-Net has been verified to work with some of the most common enterprise and small business network equipment. However, capability and default settings vary greatly from device to device and these can affect compatibility with Q-Net. Here a few Q-Net design parameters worth noting:

- The network must support fragments. This is because a Q-Net device adds 38 bytes of overhead to UDP and TCP packets. If fragments are not desired, the endpoint's MTU setting can be configured to send slightly smaller packets to avoid fragmentation.
- IP options are not supported and the packets containing them will be dropped.
- Q-Net does not allow outgoing pings or any other ICMP messages.
- Q-Net traffic may conflict with advanced threat tools like IDP or IPS. It may be necessary to modify existing rules or create exceptions to make these tools compatible with Q-Net traffic. Payload is encrypted, so inspection of payload above layer 4 cannot be performed by these tools.

It is recommended to run Q-Net on a high-speed, high reliability network. Q-Net is designed to work under relatively harsh network conditions; however, the key use parameter may need to be set to 255 to assure the best experience.

3.2 Q-Net Topology and Settings

Q-Net devices are designed to protect a single endpoint IP for maximum security; however, multiple endpoints may be secured by a single Q-Net device if a network aggregation point, such as a NAT, is used.

Protocol configuration:

- Direction – This is typically set to bi-directional. However, setting it in one direction to ensure only one endpoint can initialize communication is supported.
- Ports – This should be setup to accommodate the existing network.

Connection configuration:

- MTU – It is recommended to keep this at 1500.
- Encryption Key Use – It is recommended that this be set to the max value of 255 to start, as this will accommodate almost any network conditions. Please note that this does not affect the security of Q-Net.

Device outage detection should be tuned for a customer's specific needs and network conditions. On a poor connection between Q-Net devices and the QPM it is recommended to keep the Heartbeat Interval at the minimum 5 second setting and set the Re-enroll heartbeat count to a higher value. This will ensure device disconnections are detected quickly and accurately. On a high-quality network, setting the Heartbeat Interval to a higher value and the Heartbeat count to a low value is acceptable to save bandwidth.

Keeping the Metric Interval at a multiple of 60 seconds is recommended, as it makes the built-in Device charts and metric data easy to interpret. Dynamic Timeouts are only applicable to connections that are unidirectional. Typical values are 300 seconds for UDP and 86,400 second and are designed to match typical NAT values. If you expect UDP or TCP replies to always be slower or faster than this, these values can be changed to match your needs.

3.3 Users

For security reasons, only a limited number of Admin users should be setup and credentials for these users shall be strictly controlled.

3.4 High Availability

It is suggested that customers implement Q-Net High Availability to assure devices always have connectivity to a QPM for administrative and monitoring tasks. The QPMs should be placed in geographically isolated areas and be backed up with a UPS. They should also have a high reliability network between them to avoid unnecessary failover events.

3.5 Auto Restart

It is recommended to set Auto Restart to "Yes", to limit the amount of time the QPM is out of contact with Q-Net Devices in case of power loss.

4 Troubleshooting

4.1 General Issues

Problem	Resolution
Traffic is not going through Q-Net	• Make sure Q-Net devices are enrolled • Make sure Q-Net connections and properties have been configured for the devices • Make sure you are passing TCP or UDP traffic • Check Firewall configuration on the ports being used to make sure the traffic is allowed
Very little traffic is going through Q-Net	Increase key use
Device is going up and down frequently	Increase key use
All devices are down	• Make sure the QPM is not in Maintenance Mode • Check connections to the QPM Console and Network Ports
An individual Q-Net device is not working	• Check that the device is powered • Check connections on the Q-Net devices to the network and endpoint • Make sure the endpoint or network is sending ARPs
QPM is not powered	• Make sure the unit is plugged into the power connection. If it is and still not working, plug into the other power supply. • Hit the power button on the front panel

Troubleshooting

Problem	Resolution
The QPM is not reachable	• Check that the QPM is powered (green LEDabove button is illuminated) • Check the front display and make sure the IP Address is correct • Make sure the Gateway IP and P Mask are correct

4.2 HA Issues

Problem	Resolution
HA is not working	Check all the HA Settings. A common mistake is to set the Backup Q-Net address to be the same as the Admin address of the Primary or Secondary QPM.
HA is configured properly, but not working	Make sure the following ports are open for TCP traffic on the console side of each QPM; 443, 3306, 3000, 3300, and 3030. Make sure the Q-Net Admin port (1035) is open for UDP traffic on the Q-Net side of each QPM.
Neither of the QPMs indicate they are Primary	Make sure at least one QPM is out of Maintenance Mode
Replication isn't occurring on the Secondary HA QPM	Restart Replication
Data is different on the Primary and Secondary QPM	Synchronize the database on the Secondary QPM
QPMs are registered to each other, but Replication is not working	Enable Database Replication in HA Network Settings and configure both QPMs for HA mode

5 Related Documents

This document is a quick-start guide for the Q-Net Policy Manager. Further documentation is available, including:

- **Q-Net Policy Manual User's Guide:** Detailed guidance on how to install, deploy, and manage a Q-Net

Please contact our support team with any questions or feedback regarding this guide. Support can be contacted through https://qnetsecurity/tpondemand.com/helpdesk.