

Monigear Network Equipment Discovery and Configuration Tool User Guide

1. Installation of Device Configuration Tool.....	2
2. Initial Configuration.....	5
2.1 Login Password.....	5
2.2 Certificate Authentication.....	5
3. Discovering/Connecting Devices.....	7
3.1 Discovering Devices in the LAN with One Click.....	7
3.2 Adding Devices Across Network Segments via IP.....	8
3.3 Connecting Devices via Serial Port.....	9
4. Configuring Devices.....	10
4.1 Basic Device Settings.....	11
4.2 IoT Settings.....	11
4.3 GNC Settings.....	12
4.4 Viewing Running Status.....	13
5. Device Group Classification Management.....	14
FAQ.....	15
1) System Error Solutions.....	15
2) Unable to Discover Devices via Network.....	15
3) Unable to Find Target Device/Crash During Connection.....	15

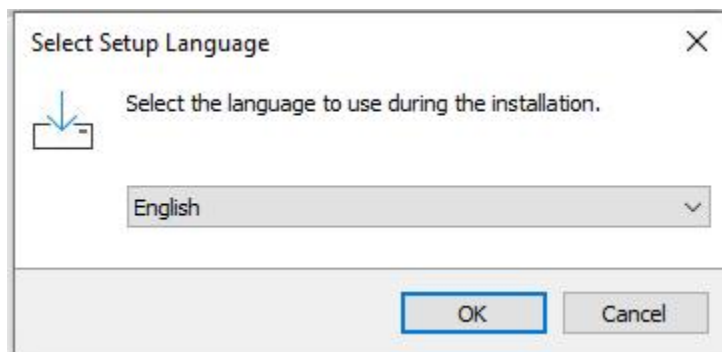
Monigear network equipment because of the powerful network related functions and the corresponding configuration items are more, this tool is developed to facilitate the configuration of equipment, in addition to the local equipment can also be used to use this tool to centrally manage the device. Due to the consideration of security, the communication between the device and the software of this tool uses TLS, and we provide a set of X509 self-signed certificates in the default installation package, and customers can also use openssl to issue their own certificates instead to ensure their own security.

1. Installation of Device Configuration Tool

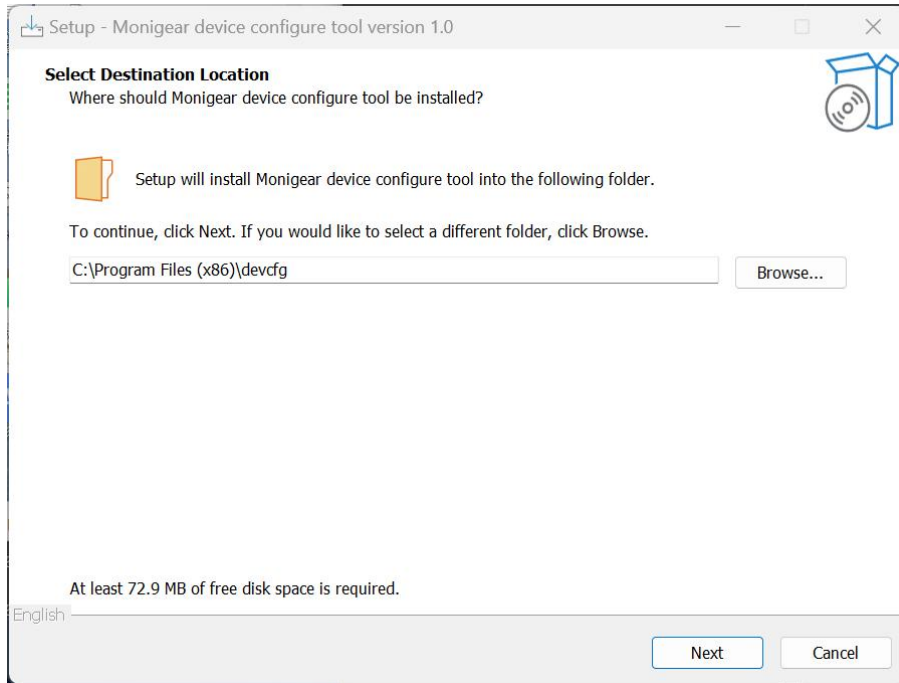
You can download the software here:

http://www.monigear.com/download/devcfg_setup.exe.

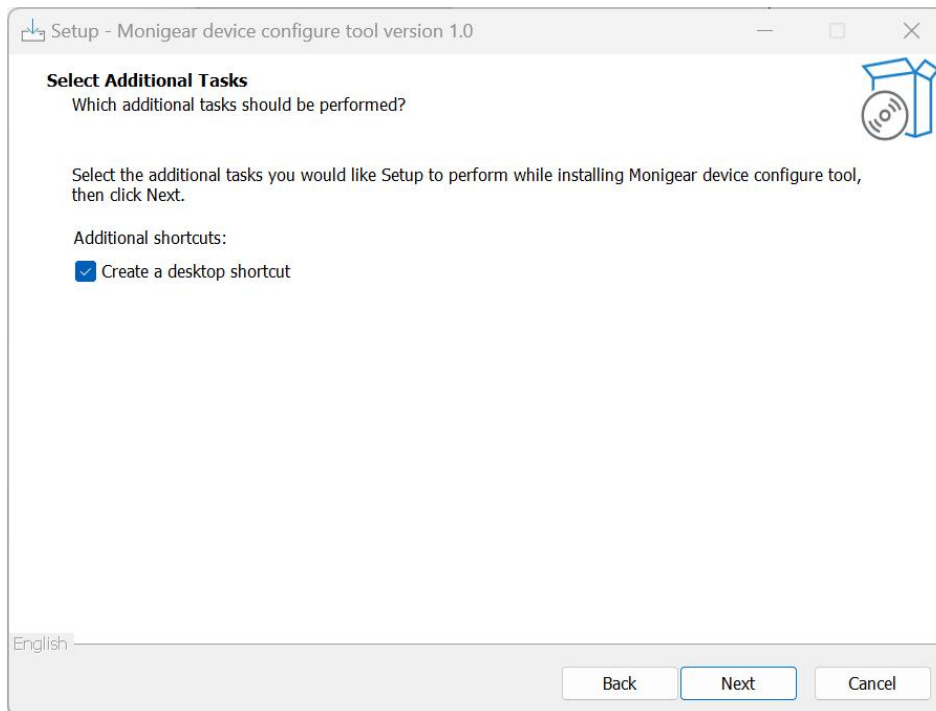
1. Run the installation software and select the installation language.

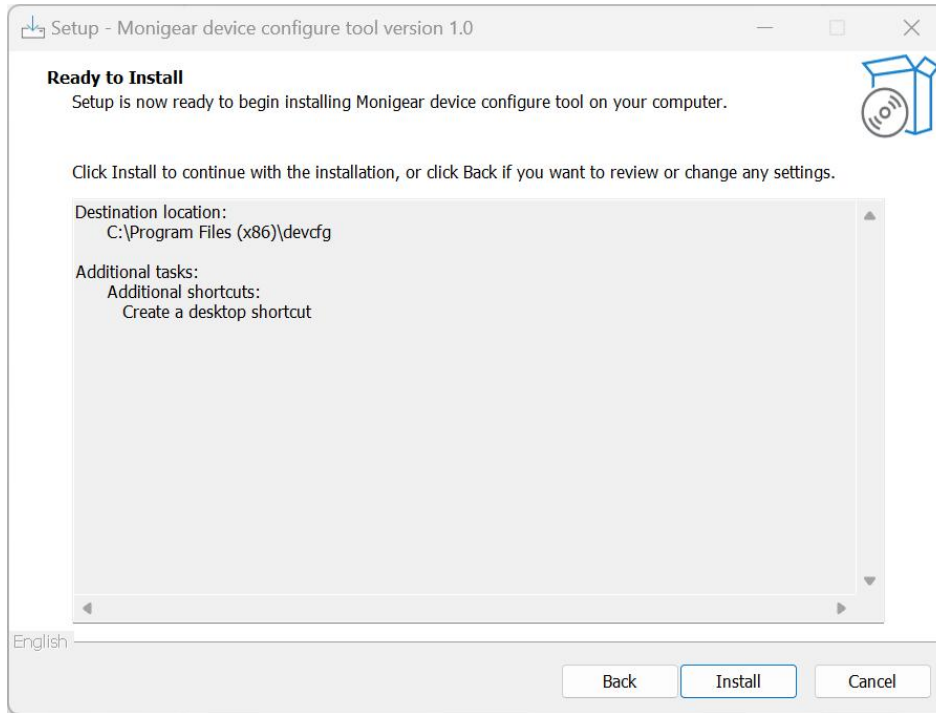


2. Choose the installation path.



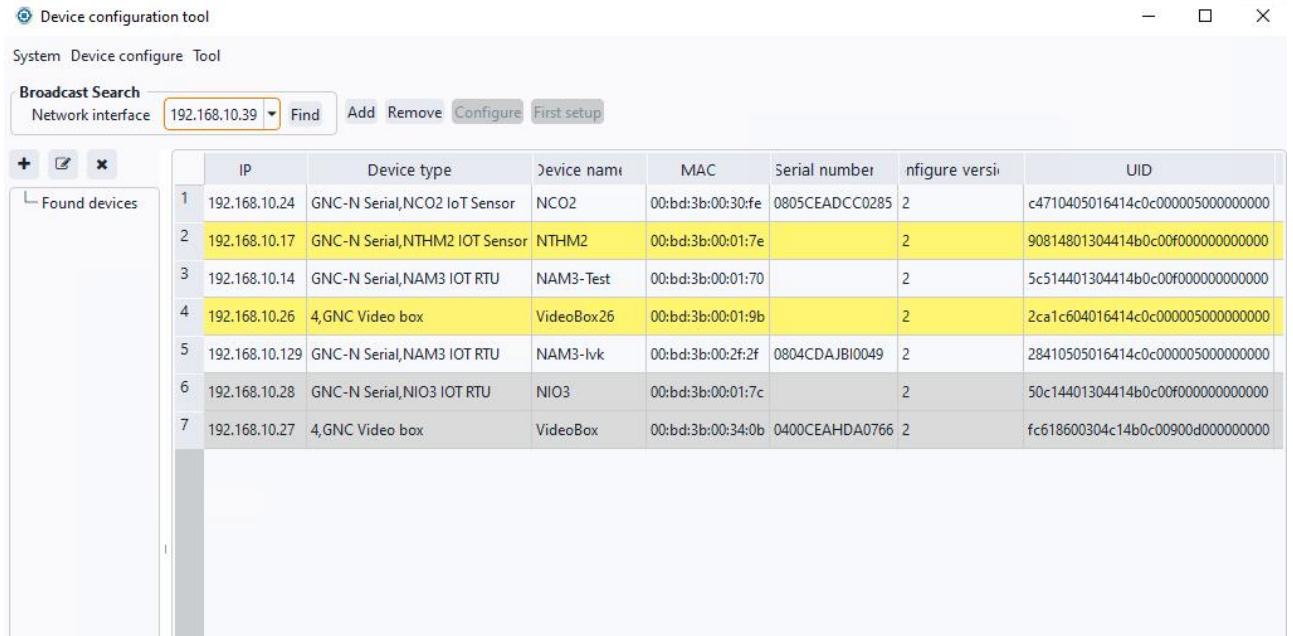
3. Follow the steps to complete the installation.





When the program is started for the first time, there will be a firewall prompt, at this time, you must accept it, let the firewall accept the network communication of the tool through, otherwise it will not work normally. For more details, refer to Appendix B - Common Issues: Unable to Discover Devices via Network.

After installation, the system interface will display as shown below. The top section contains system tools, the left side shows the device group node tree, and the right side displays the list of Monigear devices with corresponding brief information. If an error occurs when opening the program, refer to Appendix A - Common Issues: System Error Solutions or contact technical support.



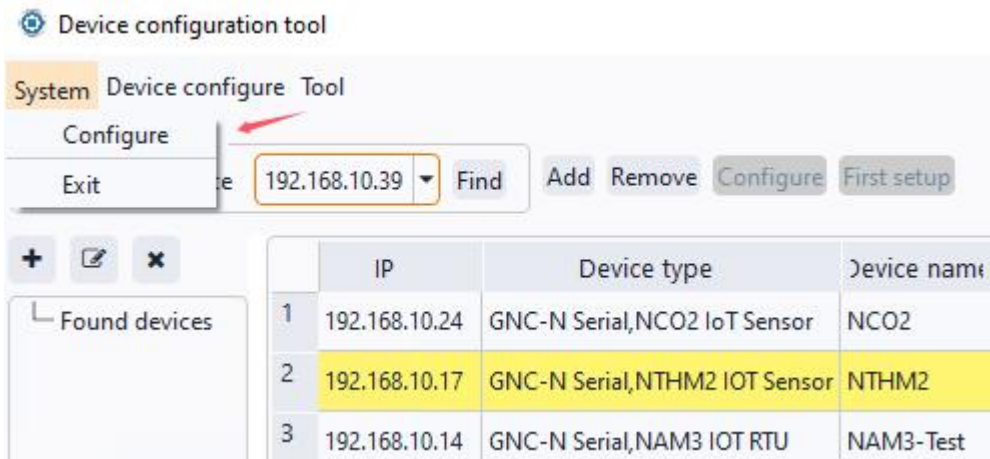
2. Initial Configuration

2.1 Login Password

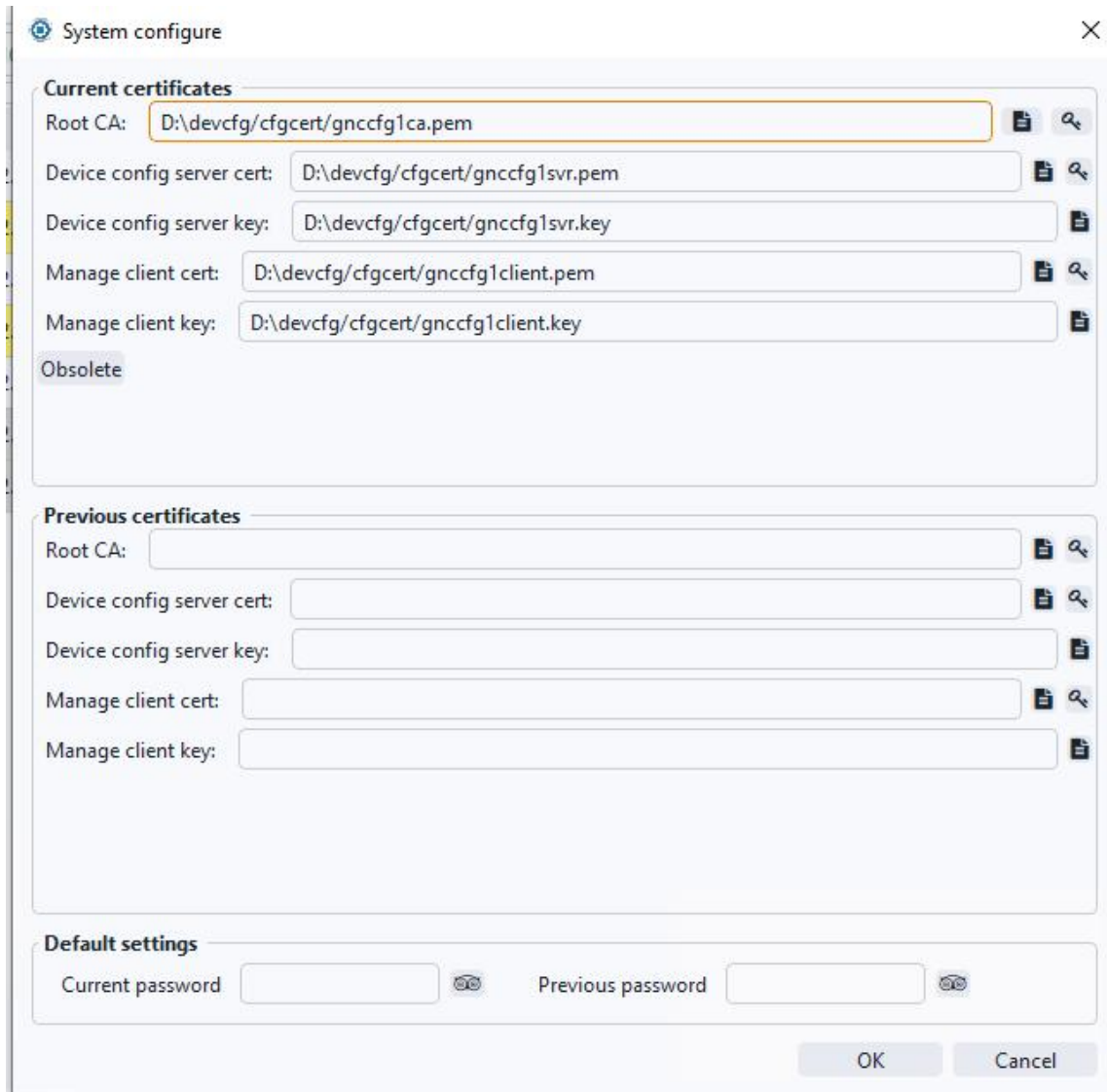
The first time you run the device configuration tool, you need to set a login password. Subsequent runs will require this password to log in.

2.2 Certificate Authentication

To connect Monigear devices and software, a certificate must be set for authentication. Open the configuration interface from the top left corner of the device configuration tool.



Specify the directory for the locally saved certificate file and key file.



The screenshot shows a 'System configure' dialog box with three main sections: 'Current certificates', 'Previous certificates', and 'Default settings'. The 'Current certificates' section has five text input fields with file selection icons to their right. The 'Previous certificates' section has five empty text input fields with similar icons. The 'Default settings' section has two password input fields with eye icons. At the bottom are 'OK' and 'Cancel' buttons.

Section	Field Name	Value
Current certificates	Root CA:	D:\devcfg/cfgcert/gnccfg1ca.pem
	Device config server cert:	D:\devcfg/cfgcert/gnccfg1svr.pem
	Device config server key:	D:\devcfg/cfgcert/gnccfg1svr.key
	Manage client cert:	D:\devcfg/cfgcert/gnccfg1client.pem
	Manage client key:	D:\devcfg/cfgcert/gnccfg1client.key
Previous certificates	Root CA:	
	Device config server cert:	
	Device config server key:	
	Manage client cert:	
	Manage client key:	
Default settings	Current password	
	Previous password	

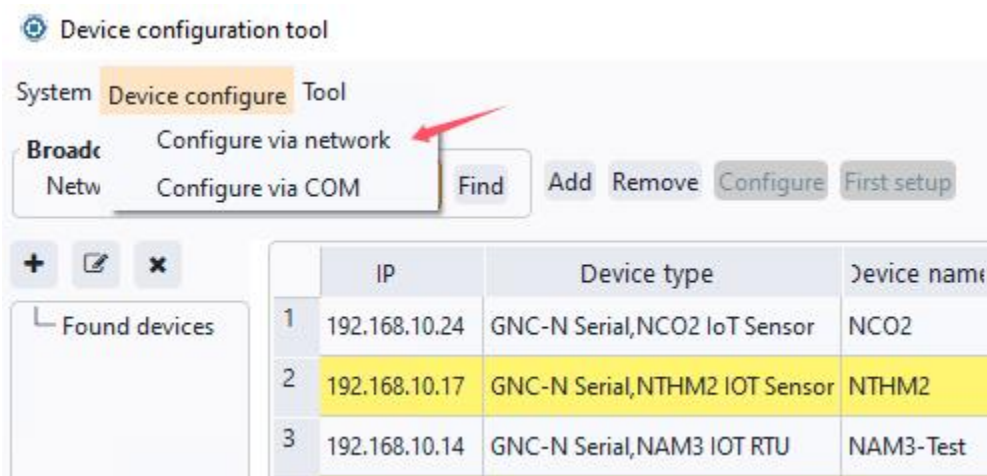
The above figure shows the digital certificate generated by us in the installation package after the initial installation, which is convenient for customers to use for testing immediately, and in actual application, customers can generate digital certificates by themselves, and how to generate digital certificates can refer to the OpenSSL documentation for related content.

After the current certificate is invalidated, do not delete the old certificate immediately, it will be displayed in the "Previously Used Certificate File" at the bottom. In this way, after enabling the new certificate, you can find the device, there is a special color in the device list to show the devices that are currently using the old certificate, the tool can connect to these devices with the old certificate, and then there is a special button to update the certificate on the interface to help customers quickly replace the certificate.

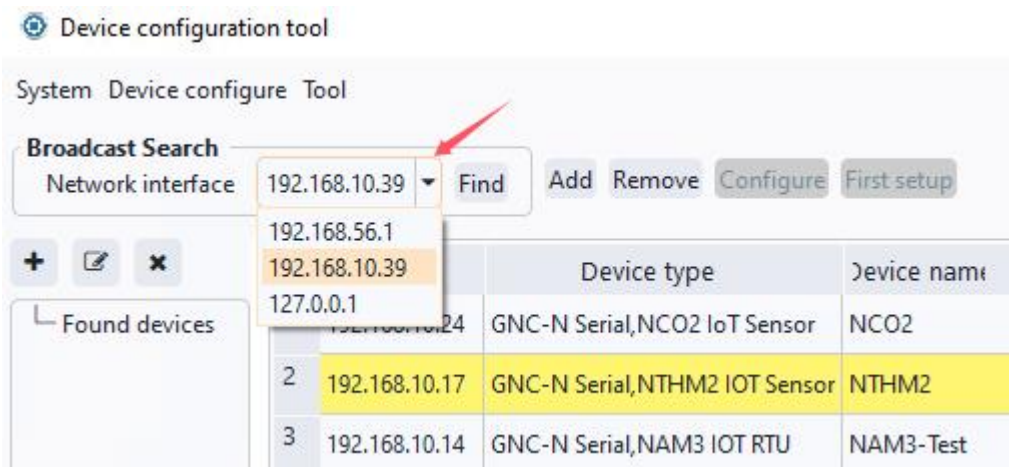
3. Discovering/Connecting Devices

3.1 Discovering Devices in the LAN with One Click

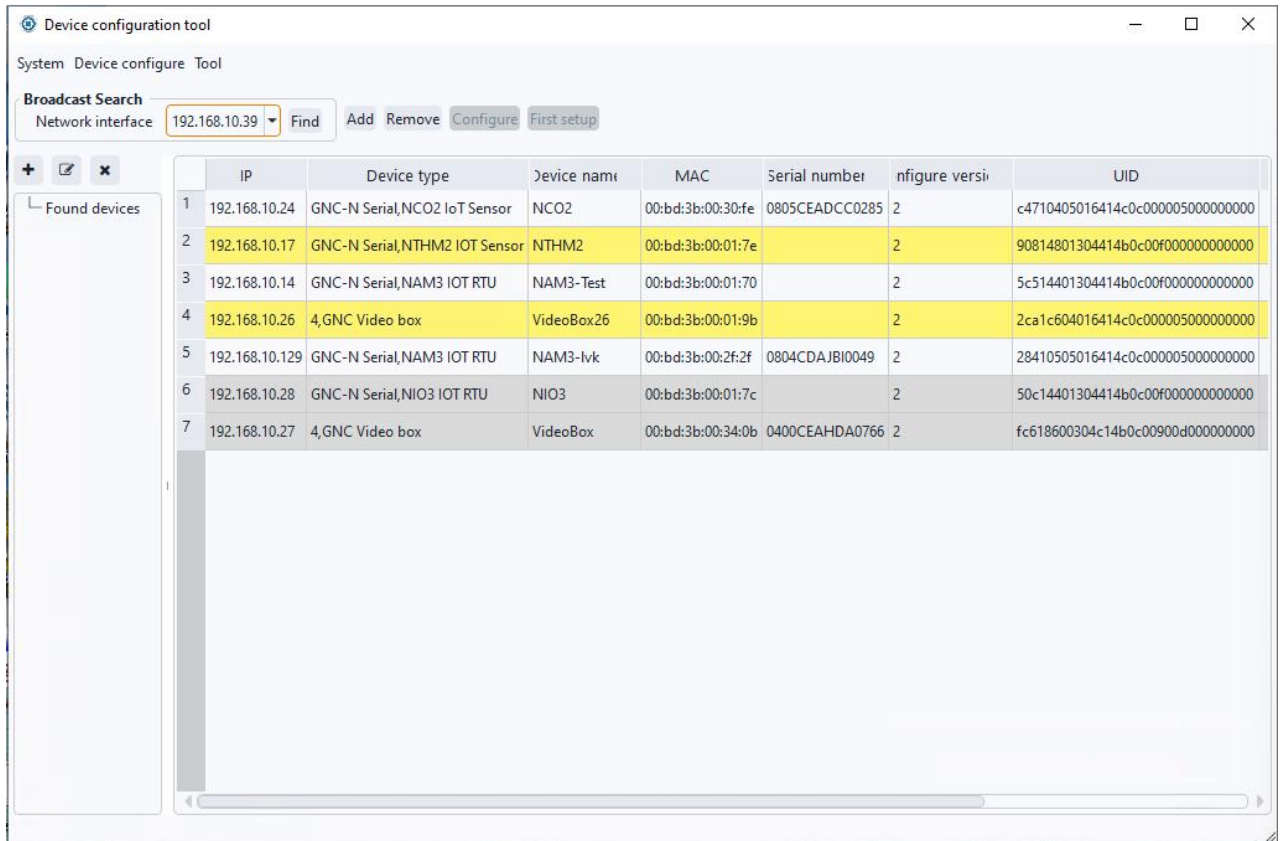
There are two ways to configure the device: over the network, or through the serial port. By default, the tool is configured through the network, or you can select the configuration method in the “Device configure” menu.



Select the network interface where the host and devices are located.



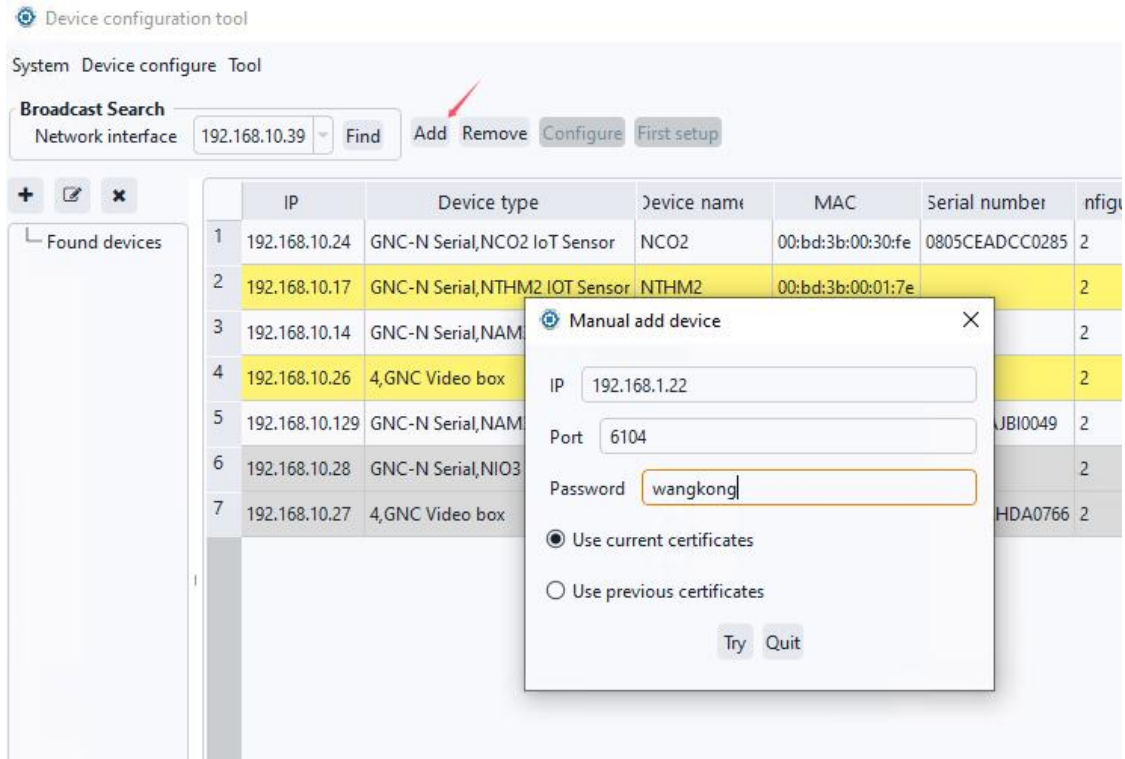
click “Find”, and devices within the same LAN segment will be discovered.



In the list of found devices, the background color of each device is different to indicate different device status, and you can see the current status information of the corresponding device by moving the mouse over the IP column in the first column. The dark gray color indicates that the product of our previous generation can be found but cannot be configured with this tool. The light gray color indicates that the device is configured with a digital certificate that is different from the current tool and cannot be configured. The green one indicates that it is a new device and has not yet been uploaded to the configuration certificate. The yellow one indicates that the factory password is being used, which has security risks. etc...

3.2 Adding Devices Across Network Segments via IP

If the device and the host are not in the same LAN, but can communicate through the router, it cannot be discovered in this case, but can be manually added through the device IP address. Select any device group node, click Add, enter the device IP, port number (default 6104), and device connection password. Ensure the input is correct, click Try to Connect. If connect successfully, the device will be added to the list.

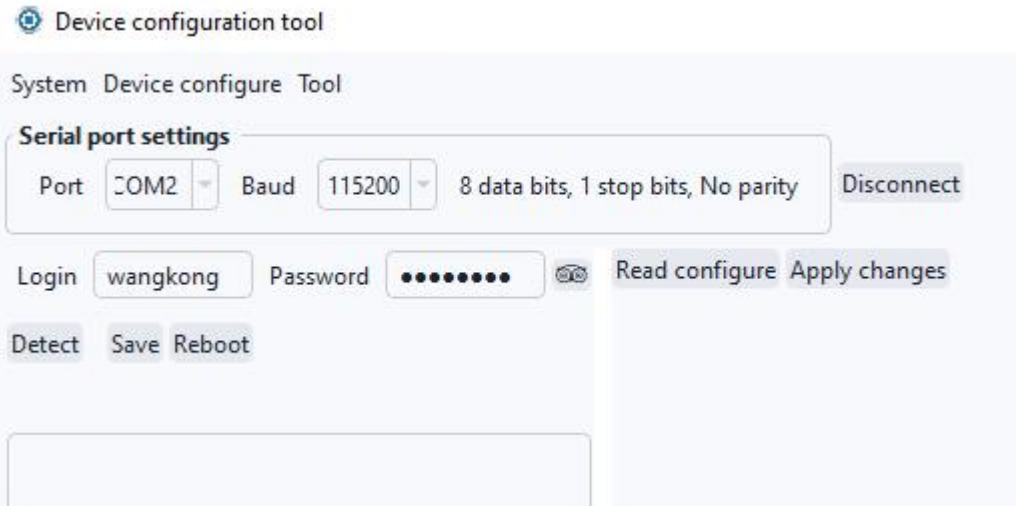


If the device already exists in another group, it cannot be added to the current group. Remove it from the existing group first. To delete a device, select the target device and click Delete in the top menu.

Devices discovered via LAN can also be added using this method. After deleting a device from any node in the LAN, clicking Search will rediscover the device in the system root node “Found devices”.

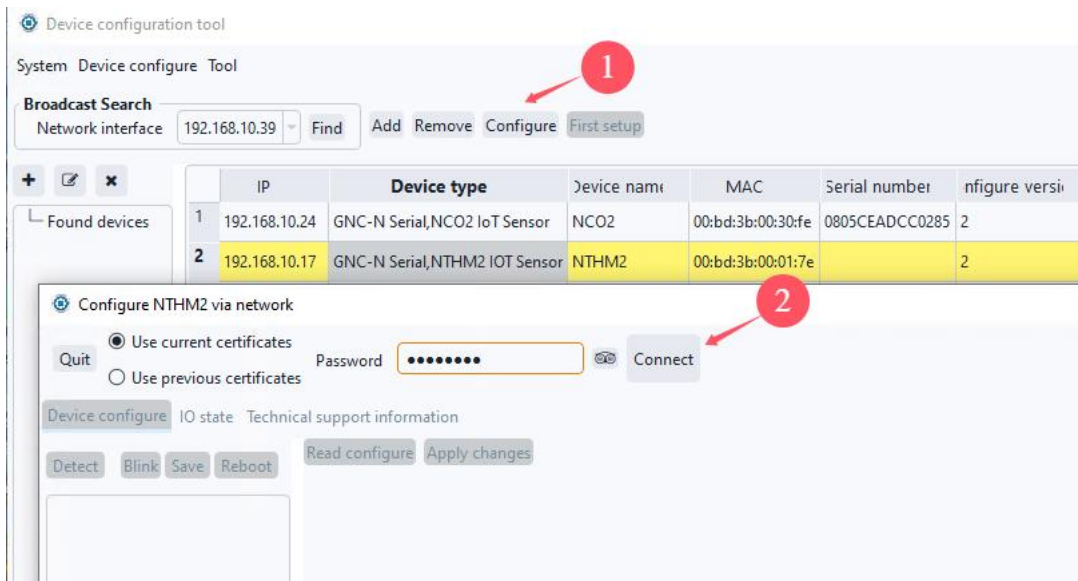
3.3 Connecting Devices via Serial Port

Select the configuration method from the top menu and choose to configure via serial port. Select the host's serial port. Monigear devices have a default baud rate of 115200. After clicking Connect and entering the username and password, you can connect to the device via serial port. Ensure the correct wiring of the serial port on the device for successful communication.

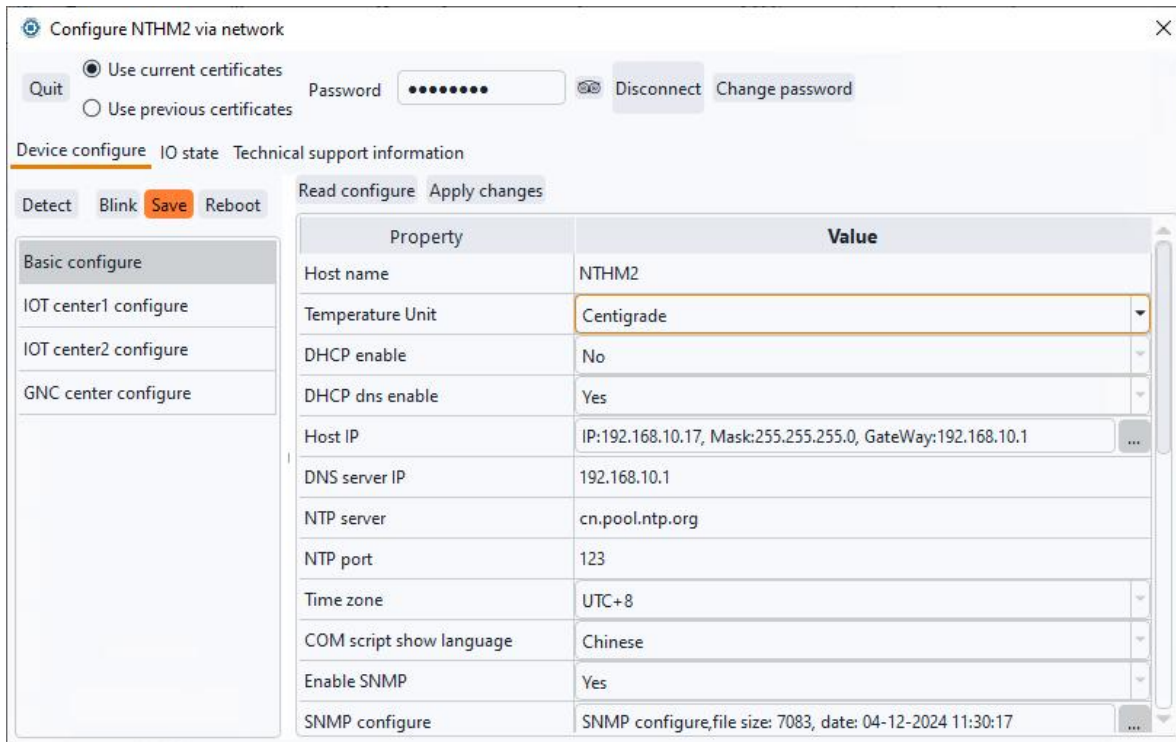


4. Configuring Devices

Devices discovered via network or added via IP can be configured in the network configuration interface. Select the device under the corresponding group and click Configure to enter the device interface. A device password is required to connect.



For new devices, use “Change password” button update the connection password to current used one. Click “Detect” button to access the configuration interface, left part is category, right part is configure item and value.



Devices connected via serial port can be configured similarly after connecting with username and password.

4.1 Basic Device Settings

Click Basic configure - Read Configuration to display the basic settings of the device, show as the above picture. Users can choose to enable or disable DHCP, DNS, BACNET, Modbus TCP etc., and make changes as needed. Click Apply Changes - Save - Restart for the new settings to take effect.

If DHCP is not enabled, you can configure a fixed IP address and click the button on the right to modify the static IP address. The IP address and the gateway must be set in the same subnet, otherwise the setting is invalid. It is worth mentioning that if DHCP is enabled, the IP address displayed on the setting interface does not represent the current IP of the device!

4.2 IoT Settings

Monigear devices can be connected to two independent IoT hubs at the same time to achieve hot data backup.

Click one IoT Center Settings - Read Configuration to display the IoT settings. Apply changes, save, and restart for the new settings to take effect.

Configure VideoBox26 via network

Use current certificates Password: Disconnect Change password
 Use previous certificates

[Device configure](#) [IO state](#) [Technical support information](#) [Script in device](#)

[Detect](#) [Blink](#) [Save](#) [Reboot](#) [Read configure](#) [Apply changes](#)

Property	Value
MQTT version	Default
QOS	Almost once
Keep alive time(sec)	60
Clean session	No
Retain publish	No
Enable will option	No
Will QOS	Almost once
Will retain	No

Center type: Standard MQTT

Property	Value
Center IP or c	192.168.10.151
Port	1883
Client ID	VideoBox
User name	gncdevice
Password	wangkong
Topic prefix	device
Password	up

In addition to the standard MQTT protocol support, such as Mosquitto, Emqx and other commonly used MQTT brokers that can build their own services, Monigear devices are also adapted to the connection of several major IoT cloud services, such as AWS/Azure/Ali, etc

4.3 GNC Settings

GNC-SCADA software is a powerful data acquisition and monitoring software developed by our company, and we have our own GNC protocol between the equipment and software, which is set up to connect with 2 active and standby GNC centers.

Click GNC Settings - Read Configuration to display the GNC settings. Apply changes, save, and restart for the new settings to take effect.

Configure VideoBox26 via network

Use current certificates
 Use previous certificates

Quit Password: ●●●●●● Disconnect Change password

Device configure IO state Technical support information Script in device

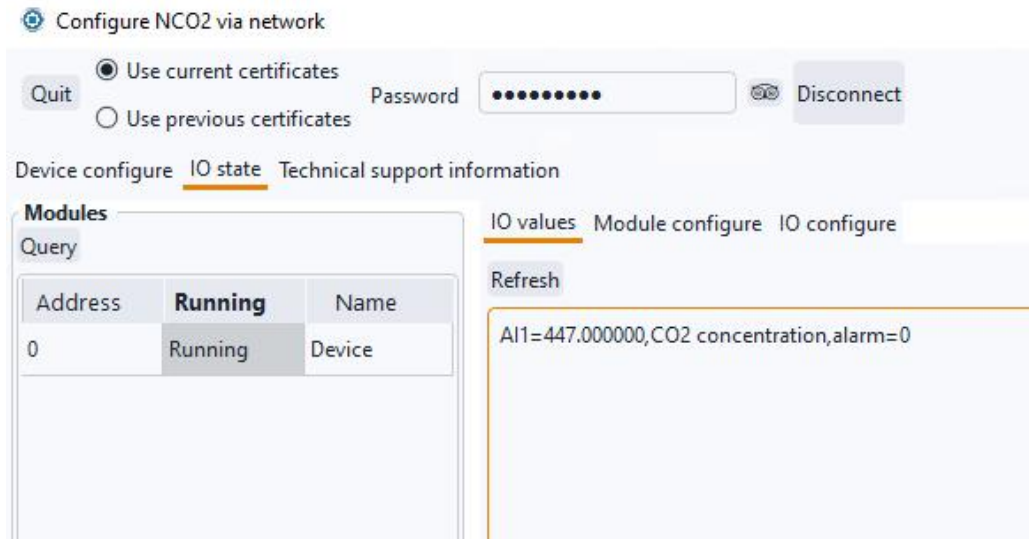
Detect Blink Save Reboot Read configure Apply changes

Property	Value
Center1 server	192.168.10.254
Center1 report port	6101
Center1 comm key	wangkong
Center1 connect type	TCP
Center1 force CA check	No
Center1 TLS verify type	CA only
Center1 root CA file	GNC center1 CA,file size: 0, date: 01-01-1970 08:00:00
Center1 client certificate	GNC center1 client certificate,file size: 0, date: 01-01-1970 08:00:00
Center1 client key	GNC center1 client key,file size: 0, date: 01-01-1970 08:00:00
Center1 key file password	
Center1 location comment	
Center2 server	192.168.10.125
Center2 report port	6101
Center2 comm key	wangkong
Center2 connect type	TCP
Center2 force CA check	No
Center2 TLS verify type	CA only
Center2 root CA file	GNC center2 CA file size: 0, date: 01-01-1970 08:00:00

The above are the configuration categories that all devices have, and each device has its own unique setting category, and the corresponding configuration refers to the description of the corresponding device, most of which are easy to understand and set up from the graphical interface.

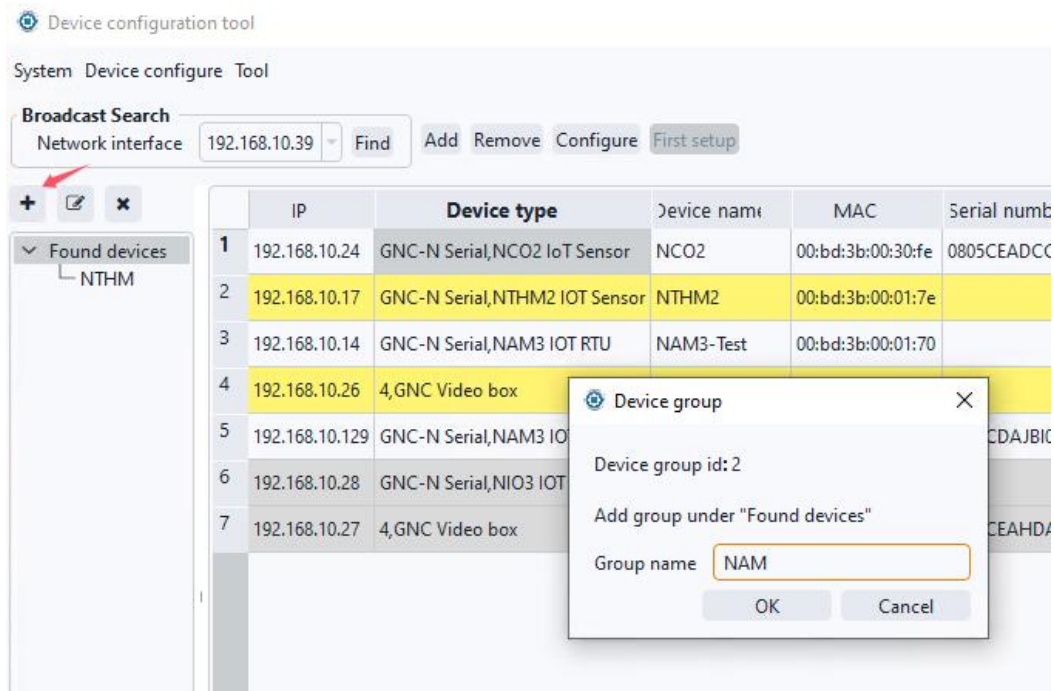
4.4 Viewing Running Status

The running status of the device can only be viewed and configured via network interface. Select the module to view, click “IO Value” tabs - click “Refresh” button to view all AIO and DIO information of the device.



5. Device Group Classification Management

In the network configuration interface, device groups can be added/deleted under any node path for bulk management.



To add a new device group node, click the + sign, enter the desired name, and click OK. To delete, click the × sign. If the group contains devices, it cannot be deleted.

To add devices to a group, use the Add button to add new device, or drag devices from Discovered Devices to the desired group node.

FAQ

1) System Error Solutions

If the configuration tool does not open normally and a system error occurs, prompt that VCRUNTIME140.dll missing. Install the VC 2015-2019 redistribute component package will fix it.

2) Unable to Discover Devices via Network

Ensure the firewall is set to a private network. If unable to discover Monigear devices, check if the firewall allows the software to communicate on the private network.

If the system exists another firewall, make sure UDP port 6104 is allowed.

3) Flash quit when connection

If you can't find a device in the Discovered Devices device group node when you find a device over the network, or if the connected device crashes in the device configuration interface. The reason is that the time of the device is abnormal, not the current time but the start time of Unix 1970, which is not within the validity period of the digital certificate, which caused the connection failure. At this time, the device should be restore to factory default, the IP assignment should be reset, and the time synchronization should be re-executed during the application of the new IP to the device, and the modification can be re-founded/connected to the device.