Device Search Utility v3.x User Manual

Version 1.1, November 2025

www.moxa.com/products

Device Search Utility v3.x User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

Device Search Utility v3.x (**DSU**) is a handy tool that helps you easily discover Moxa's NPort and MGate, as well as provide functions for single and mass device deployment. **DSU** v3.x now functions as a web-based application that works on Chrome, Firefox, and Microsoft Edges.

Supporting OS:

- Windows 11 and Arm, 10, 8.1, 8 and 7

  Windows 7 with the following packages installed, taking into consideration the TLS v1.2 and .NET 6 compatibility
  - Service Pack 1 (SP1)
  - Microsoft Visual C++ 2015-2022 Redistributable
  - Security Update Pack KB3063858
  - Microsoft Root Certificate Authority 2011
- Windows Server 2025, 2022, 2019, 2016, 2012 R2, 2012 and 2008 R2

  Windows Server 2008 R2 with the following packages installed, taking into consideration the TLS v1.2 and .NET 6 compatibility
  - Service Pack 1 (SP1)
  - Microsoft Visual C++ 2015-2022 Redistributable
  - Security Update Pack KB3063858
  - Microsoft Root Certificate Authority 2011

Supporting browser type and compatible versions:

<table>
<tr><th></th><th>Chrome</th><th>Firefox</th><th>Microsoft Edge</th></tr>
<tr><td>Windows 11 and Arm</td><td rowspan="6">Version 128.0.6613.85 and later</td><td rowspan="6">Version 129.0.2 and later</td><td rowspan="6">Version 126.0.2592.87 and later</td></tr>
<tr><td>Windows 10</td></tr>
<tr><td>Windows Server 2025</td></tr>
<tr><td>Windows Server 2022</td></tr>
<tr><td>Windows Server 2019</td></tr>
<tr><td>Windows Server 2016</td></tr>
<tr><td>Windows 8.1</td><td rowspan="6">Version 109.0.5414.120 and later</td><td rowspan="6">Version 115.14.0 and later</td><td rowspan="6">Not available</td></tr>
<tr><td>Windows 8</td></tr>
<tr><td>Windows 7</td></tr>
<tr><td>Windows Server 2012 R2</td></tr>
<tr><td>Windows Server 2012</td></tr>
<tr><td>Windows Server 2008 R2</td></tr>
</table>

NOTE

1. Starting from v3.1, **DSU** adopted the Progressive Web Application (PWA) format, which is supported by Chrome and Microsoft Edge. If your browser is not supporting PWA yet, you should still be able to use **DSU** with the browser interface.
2. Also, starting from v3.1, **DSU** has become a web application. If you encounter any trouble with **DSU**, we advise you to close or clear cookies and then relaunch it.
3. If your OS version is older or can only support an older browser, e.g., Internet Explorer, use **DSU** version 2.x.

Supporting Models:

See **Release Note** in the **About** section to learn which products are supported by **DSU** v3.x.

2. How to Use Device Search Utility

Installation and Launch

The installation of the application has two options:

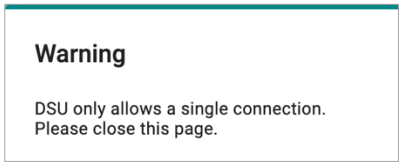
- Full installation: Follow the installer steps to complete the installation:
  - Silent installation: DeviceSearchUtility.exe /silent

  Launch the application by selecting the Device Search Utility shortcut on your desktop.
- Portable/standalone version: Some customers may have security restrictions that prevent them from installing a new application on their computers. Copy the "DeviceSearchUtility" folder from the zip file. Run the download from Moxa's website and place it on your desktop. Follow the instructions below.
  - Run InstallCertificate.bat as administrator
  - Run DeviceSearchUtility.exe as administrator

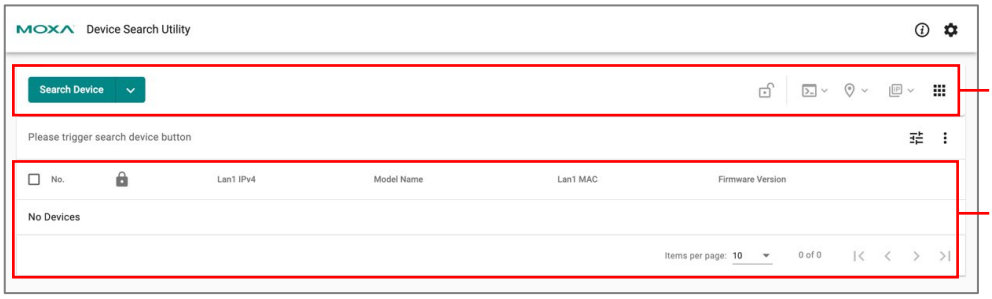
  If you wish to uninstall the Root CA certificate, run UninstallCertificate.bat.

NOTE

1. The default port number for DSU is **5005**. If you prefer to use another port, you may edit "**Program Files\Moxa\Device Search Utility\DeviceSearchUtility.xml**" and modify the line "**localhost:5005**" to your preferred port number.
2. You can run only one instance of DSU per computer. Accessing DSU through a new browser tab, another browser, or remote means will deny this action and show an error message.



Working Pane and User Interface



Function icon	Function name	Brief introduction
Search Device	Search	Searching devices by broadcast, unicast, or IP range
	Unlock	Unlocking selected devices of the same model type
	Console	Using the web console
	Locate	Locating the device by triggering the buzzer or indicating by LED.
	Assign IP	Assigning IP address of device(s)

Function icon	Function name		Brief introduction
	More functions		Advanced functions
		Import Configuration	Importing configuration to the same model device(s)
		Export Configuration	Exporting configuration from the same model device(s)
		Firmware Upgrade	Firmware upgrade for the same model device(s)
		Import Certificate	Importing certificates to the device(s)
		Allowlist	Setting the list of allowed IP addresses that have access to the device
		Restart	Restarting device(s)
		Reset	Resetting device(s) to factory default
	Filter		Searching the list, table filter
	Application Information		About and User Manual sections
	Preferences		Utility settings, language selection

Search Result Table Column Name	Brief Introduction	Default to Display
Device Name	The alias name of the device	N
Model Name	The model type of the device	Y
Unlock Status	The lock status by DSU	Y
LAN1 IPv4	IPv4 address of LAN1	Y
LAN1 MAC	MAC address of LAN1	Y
LAN2 IPv4	IPv4 address of LAN2	N
LAN2 MAC	MAC address of LAN2	N
LAN1 IPv6	IPv6 address of LAN1	N
LAN2 IPv6	IPv6 address of LAN2	N
Firmware Version	Current loaded firmware version of the device	Y

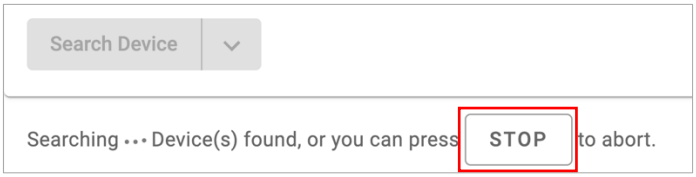
Function

The availability of functions in **DSU** depends on how your device supports the function. If the function is disabled in your device firmware, DSU will display the function as being in a disabled state. Or if the function is not supported by your device, then the function will not be shown in **DSU**.

Search Device

Search Device provides three ways of searching. Select the pull-down menu to see the options:

Broadcast search	Default button action. It would search for the devices by broadcasting.
Search by IP	Searching the device by a specific IP
Search by IP range	Searching the device in a certain IP range, e.g., 192.168.127.1 to 192.168.127.255.



It's possible to stop the search at any stage of the process. A **STOP** button appears on top of the table; select it to halt the search and keep the already searched devices on the list.

The default search time is 10 seconds. DSU will continue searching until the time is up. If your device(s) does not appear, you may change the search timeout limit in **Preferences > Device Search > Timeout limit for device searching**, to give the network a bit more time to respond.

NOTE

1. When launching DSU, it will broadcast a search for the devices. If you wish not to search when launching, you can uncheck the option in **Preferences > Device Search > Automatically search devices** after launching DSU.
2. When searching by IP or IP range, the search results will only display the corresponding IP type. For example, if you search by IPv4, only IPv4 values will be displayed.

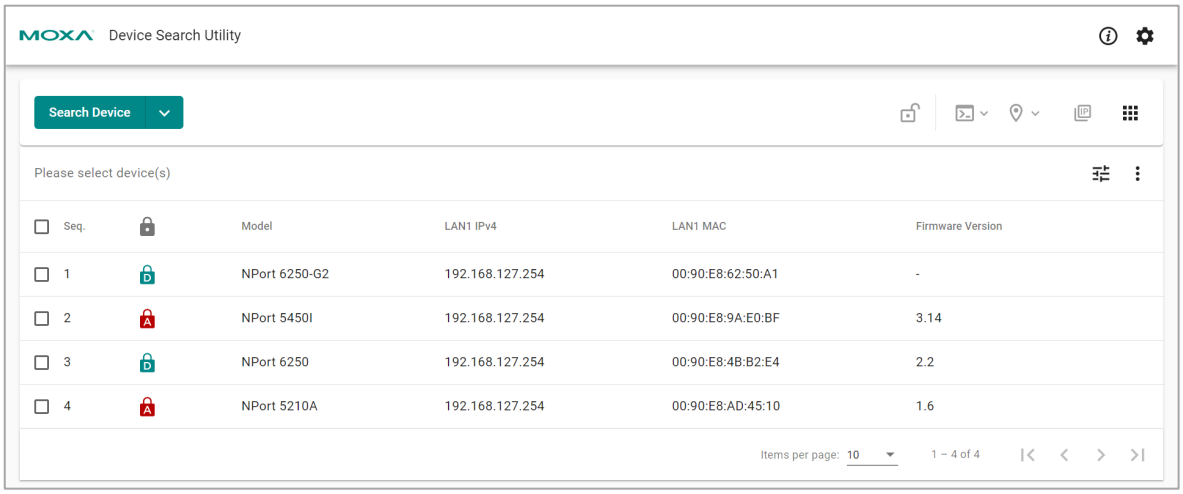
Unlock

The NPort and MGate security design has made great strides over decades. Now, they have four different types of login permissions. See the lock type of your device from the Search list table and refer to the table below for the corresponding unlocking method.

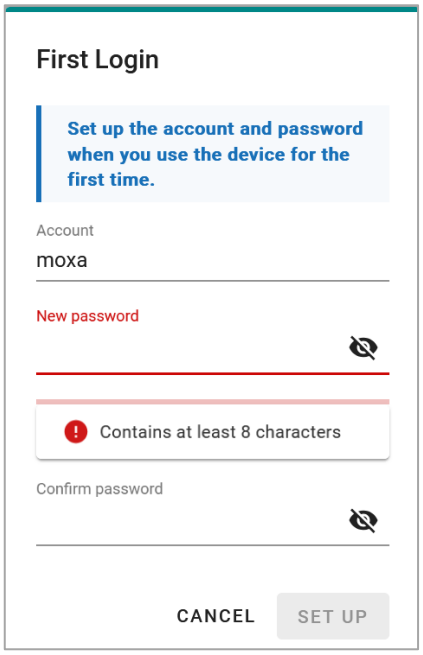
	Login Permission Type	Definition
	Default	First-time login requires creating an account and password
	Basic	Login requires to input password only
	Advanced	Login requires inputting account and password
	Legacy/Unlocked	The device is unlocked, or does not require login

First-time Login

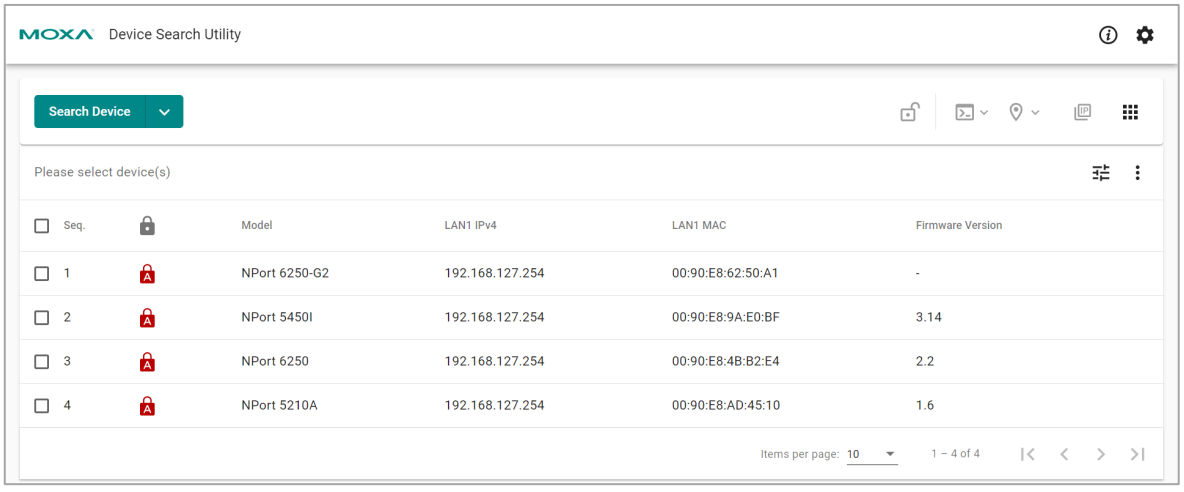
For newer versions of the NPort or MGate, the device may be required to set up an account and password when logging in for the first time.



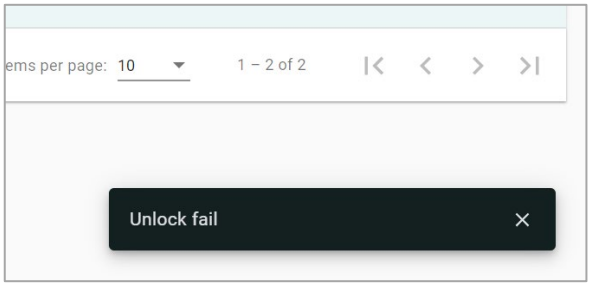
When you try to unlock the device, the login window will remind you to set up the account and password, and it will show the password minimum requirement as tips below the password field.



Once you create the default account and password successfully, the device may restart. After completing **START NEW TASK**, the lock icon will change to **Advance** type:



If an error occurs while unlocking, such as entering the incorrect password, the system will notify you by displaying an error message at the bottom right side of the screen.



NOTE

1. You can only unlock the same model devices.
2. If you need to change the account and password, go into the web console, and find **User Account** function.

An auto-lockout mechanism locks the device after a period of inactivity (default period of three minutes), requiring you to unlock it again. The auto lockout option is in **Preference > Unlock Timeout**.

Console

The device's Web console contains all settings. Selecting the button reveals the options to access it.

- HTTP (IPv4)
- HTTPS (IPv4)
- Telnet

NOTE

For later released products, certain insecure connection methods are disabled by default, such as HTTP, Telnet, and SSH. If you need to access the device by one of these methods, enable them through the web console first: **Basic Settings > Console Settings**.

Locate

Unlock the device before you can use the function.

This is to locate the device by triggering the buzzer. Selecting the button will show all options of **Locate**. If your device does not support certain options, they will be disabled:

- Locate (IPv4)
- Locate (IPv6)

Assign IP

The device(s) needs to be unlocked before the function can be used.

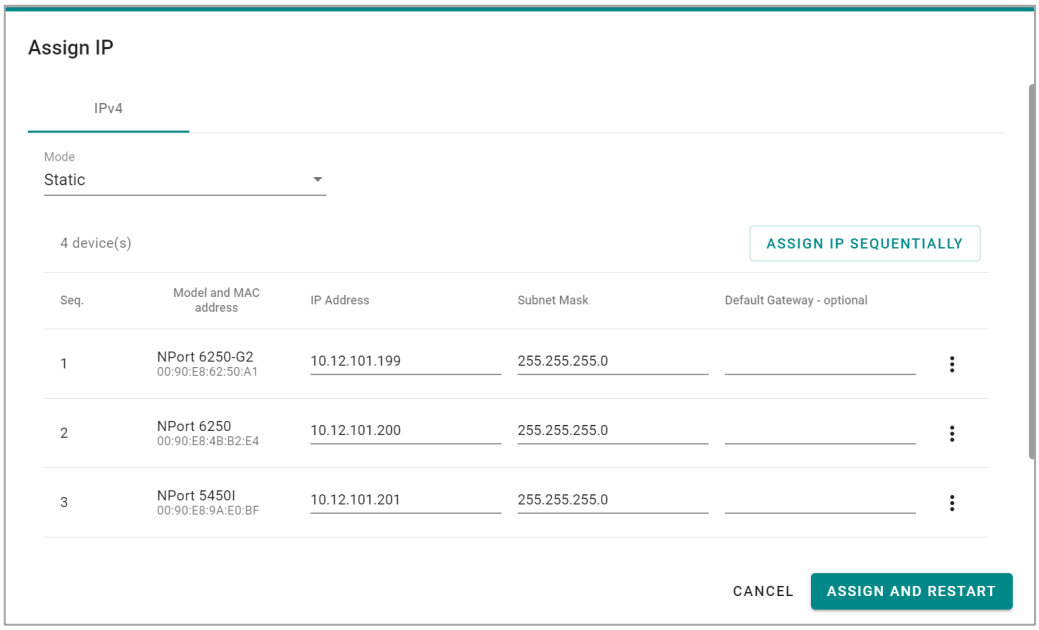
Select to assign IPv4 or IPv6. If the selected devices(s) support IPv6, then the IPv6 tab will appear. Otherwise, DSU will only show the IPv4 tab.

Assign IPv4

Mode: Static or DHCP

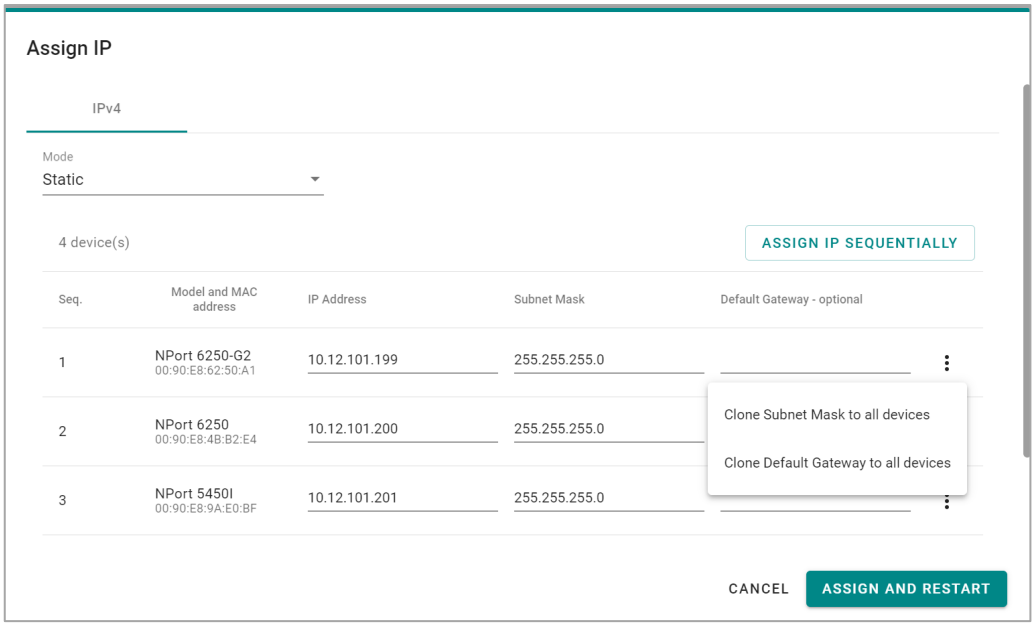
Select on the fields of **IP Address, Subnet Mask, Default Gateway – optional,** to manually key in the values.

If you have selected multiple devices and the specific IP is not required for each device, you may consider using **ASSIGN IP SEQUENTIALLY** to set up IP quickly. The function will be based on the IP value of the No. 1 device in the list to increment the IP address.



Clone "Network Mask"/"Default Gateway" to all devices

This is a quick way to copy and paste Netmask or gateway values to all the selected devices. Edit **Subnet Mask** and **Default Gateway – optional** of any device first, and find the options in the menu icon at the end of the list and apply:

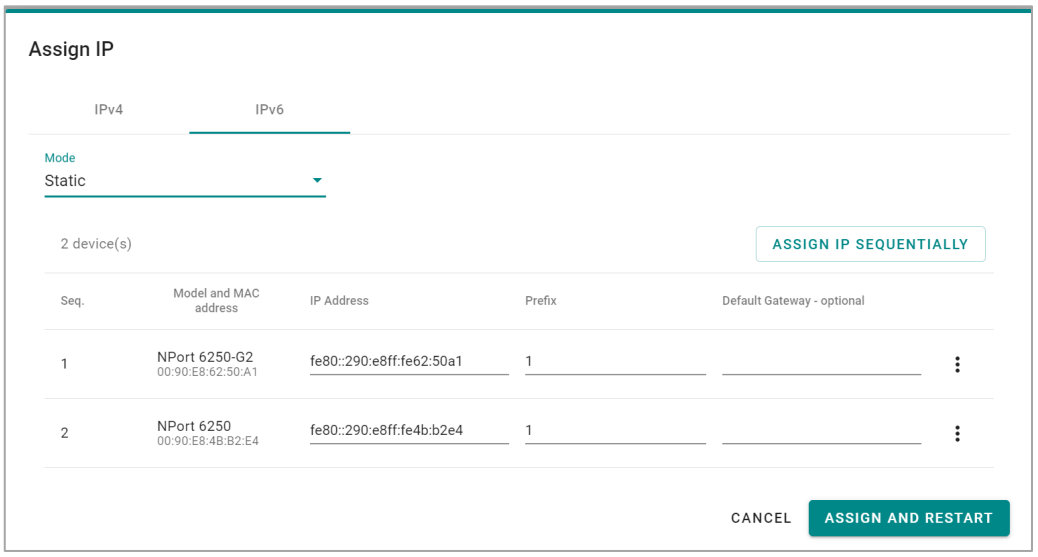


Assign IPv6

Mode: Static, Auto or Disable

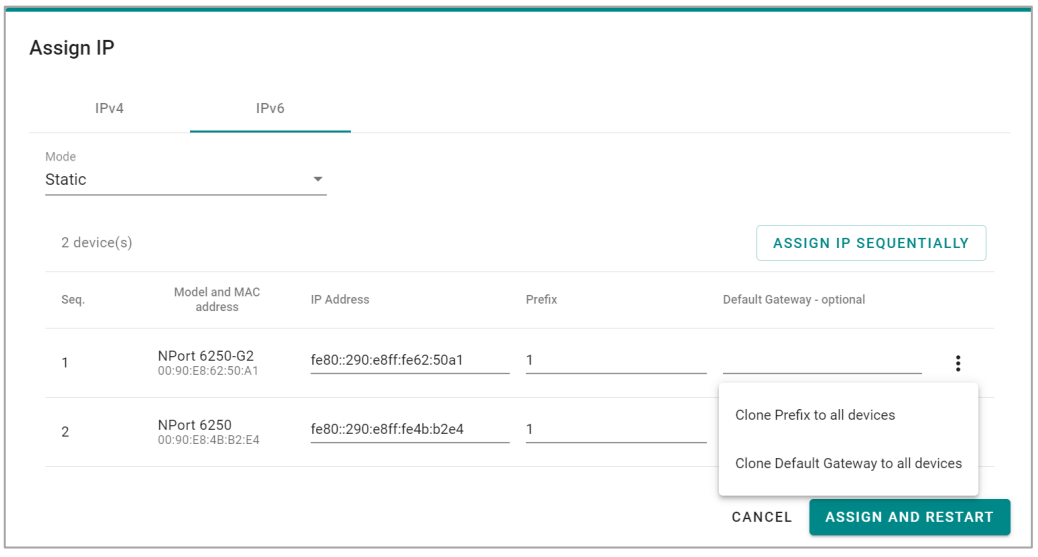
Select on the fields of **IP Address, Prefix, Default Gateway – optional,** to manually key in the values.

If you have selected multiple devices and specific IP is not required for each device, you may consider using **ASSIGN IP SEQUENTIALLY** to set up IP quickly. The function will be based on the IP value of the No. 1 device in the list to increment the IP address.



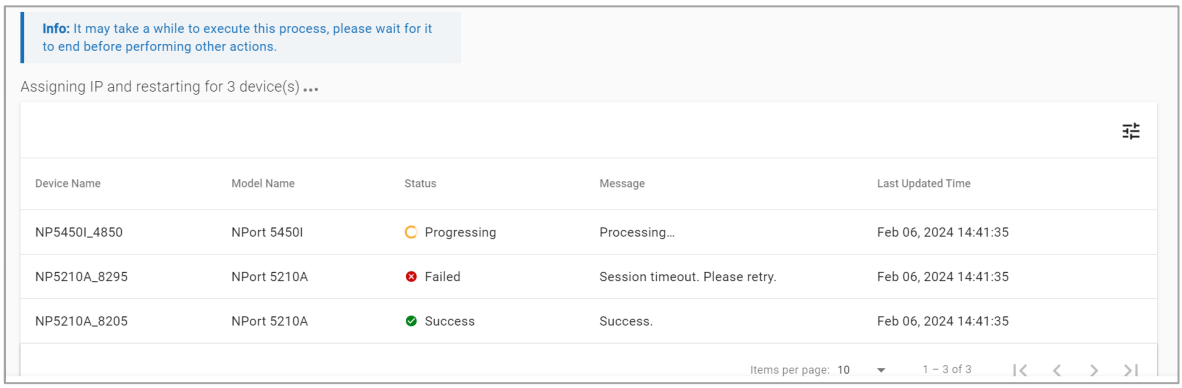
Clone "Prefix"/"Default Gateway" to All Devices

This is a quick way to copy and paste Prefix or gateway values to all the selected devices. Edit **Prefix** and **Default Gateway—optional** of any device first, and find the options in the menu icon at the end of the list and apply:



Apply the Changes

After you have set everything, select **ASSIGN & RESTART** to restart your device(s) and set up a new IP. DSU will display the result, whether it is successful or failed, in the **Status** and **Message** columns of each device.

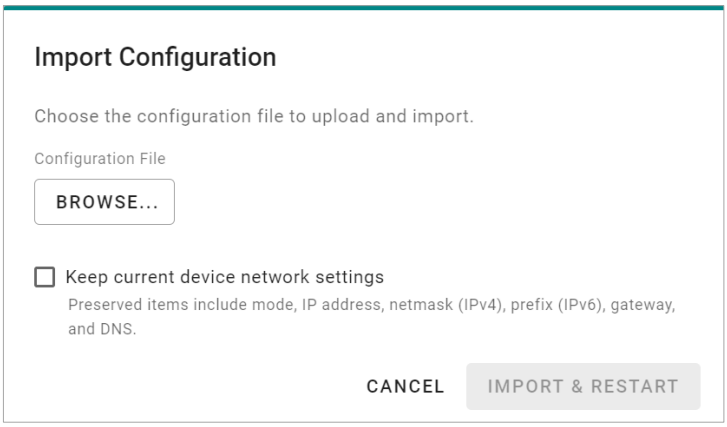


More Functions

Import Configuration

The device(s) needs to be unlocked before the function can be used.

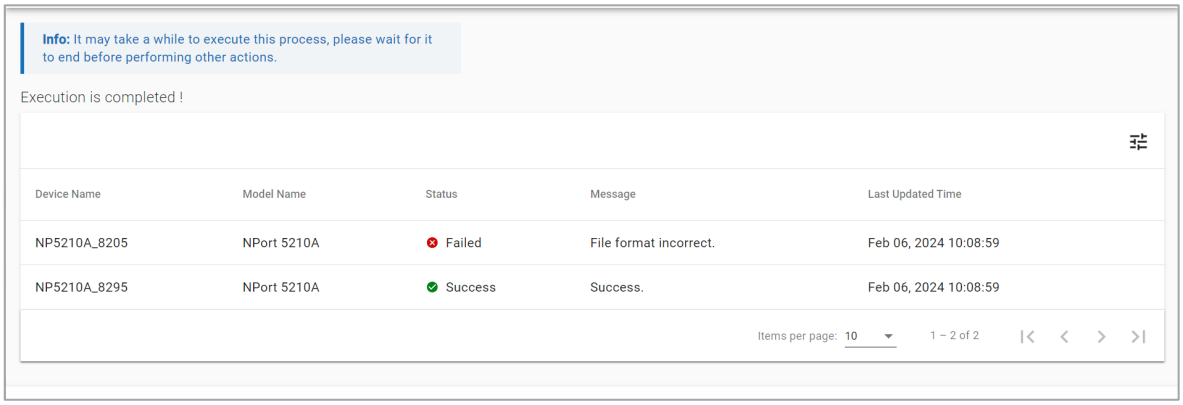
Import Configuration is to import one configuration file to one or more devices with the same model name.



Keep the Current Device Network Settings

If you wish to keep the existing network settings for the device(s), check the option.

After importing the configuration, DSU should display the success or failure in the **Status & Message** columns for each device.



Your device may restart again to make the configuration effective, and your work in progress will be stopped.

NOTE

For the possible cause of failure, refer to Appendix: Error Messages.

Select **START NEW TASK** to go back to the main console pane, and it will re-search again.

Export Configuration

The device(s) needs to be unlocked before the function can be used.

Export Configuration is to export the configuration file from one or more devices with the same model name. When exporting one device only, the file format may be *.ini, *.dat, *.txt, *.cfg, *.dec. The filename will be [ModelName] - [IP] _ [Date] .xxx, e.g, NPort6150-10.123.10.1_220724.ini.

When exporting multiple devices, the system will zip the configuration files.

Firmware Upgrade

The device(s) needs to be unlocked before the function can be used.

Firmware Upgrade allows sending one firmware file to one or more devices with the same model name. The firmware file extension normally ends in .ROM.

Step 1: Select the same models

Step 2: Import firmware file

Step 3: Import and Restart

CAUTION

When upgrading the firmware, do not pull out the power adapter plug of the device, nor restart/reset the device, as it could brick the device.

Import Certificate

The device(s) needs to be unlocked before the function can be used.

Import Certificate allows exchanging certificate files to one or more devices to establish secure command/data transfers.

Step 1: Select suitable models, e.g., NPort 6000-G2

Step 2: Import certificate

Step 3: Save and restart

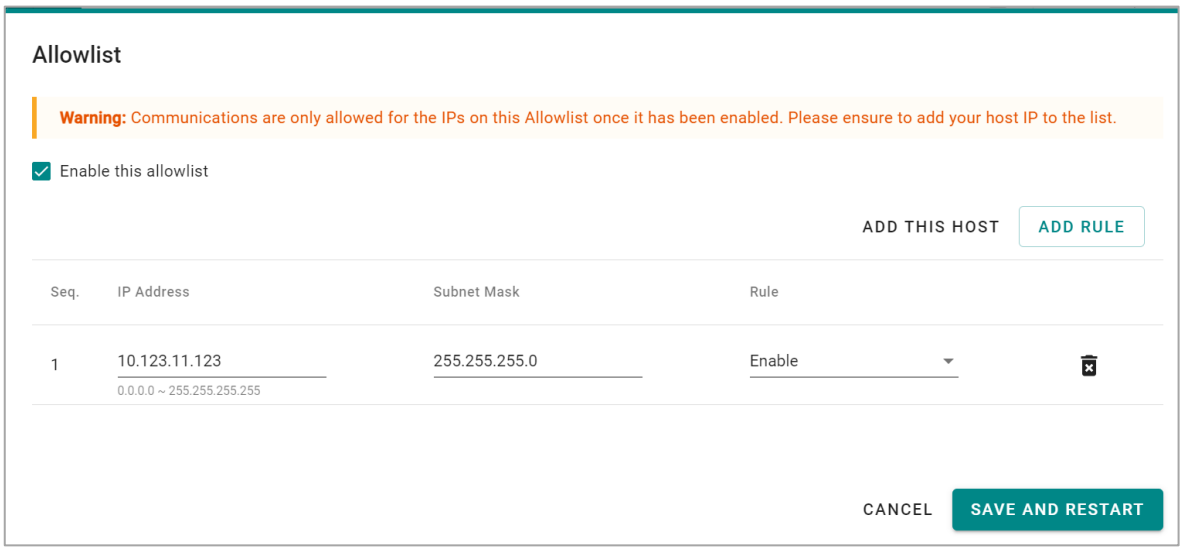
NOTE

1. Import certificates are only available for certain models, e.g., the NPort 6000-G2 Series
2. Certificates can only be imported when ports are closed, and data is not being transferred. You will receive a notification to close all open ports before importing the certificate file.

Allowlist

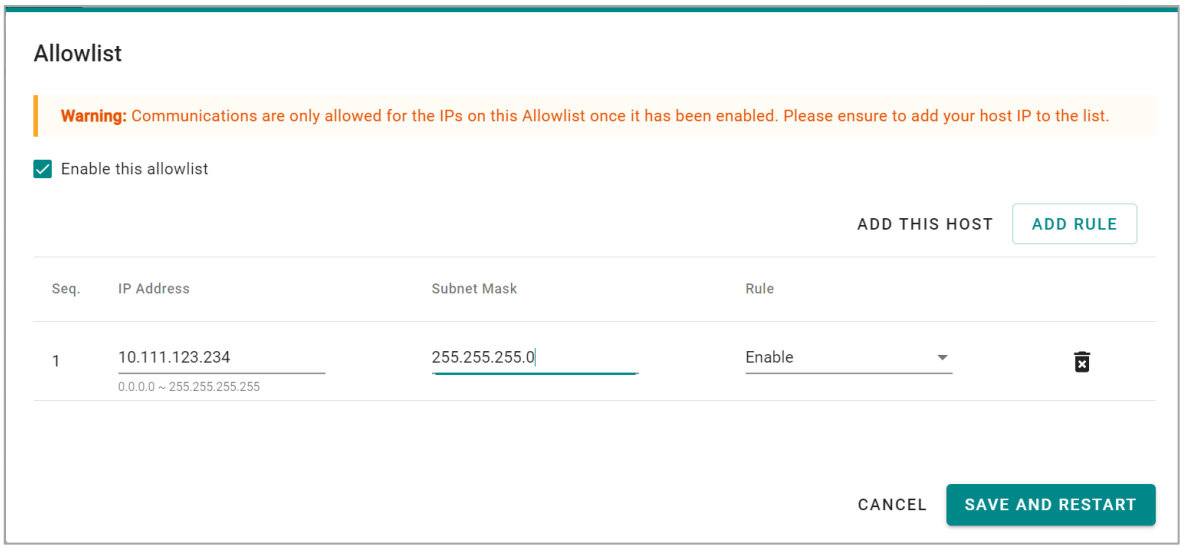
The device(s) needs to be unlocked before the function can be used.

The allowlist provides access permission to the device by granting IPs to the access list. Select **ADD RULE** or **ADD THIS HOST** to create a new rule for the allowlist.



ADD RULE

This grants access permission to a specific IP.



IP Address	The IP address of the allow to access computer
Subnet Mask	The subnet mask of the allow to access computer
Rule	Enable/Disable the allowlist rule
	Delete the allowlist rule

Enable This Allowlist

This is to enable the entire allowlist function, and this option would only be activated when there is a rule in the list. The access restriction will only be activated when this option is checked.

ADD THIS HOST

To add the current computer, which is operating **DSU** to the allowlist.

NOTE

If the computer operating **DSU** serves as the host computer for your device, it is crucial to include the host computer in the access list by selecting **ADD THIS HOST**. Otherwise, if you enable the **Allowlist** without adding the host computer's IP, the device will block the host computer from accessing it again.

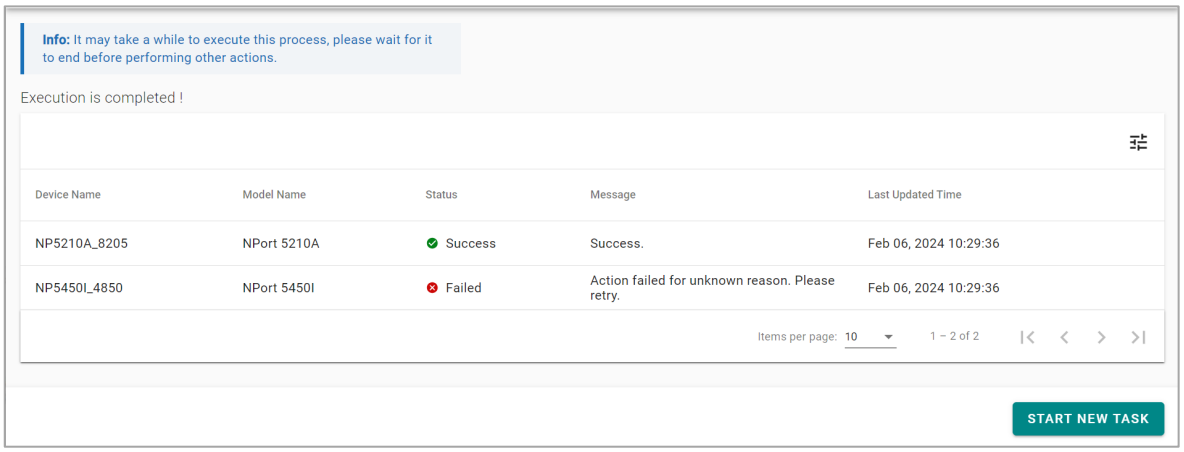
After completing the allowlist editing, select the **Save & Restart** button. Note the device may need to restart, and your work in progress will be terminated.

Restart

The device(s) needs to be unlocked before the function can be used.

Restart may apply to one or more devices. Select the devices that you need to restart and hit the **Restart** button.

After **Restart** has completed, DSU should show the result, whether successful or fail in the **Status** and **Message** columns of each device:



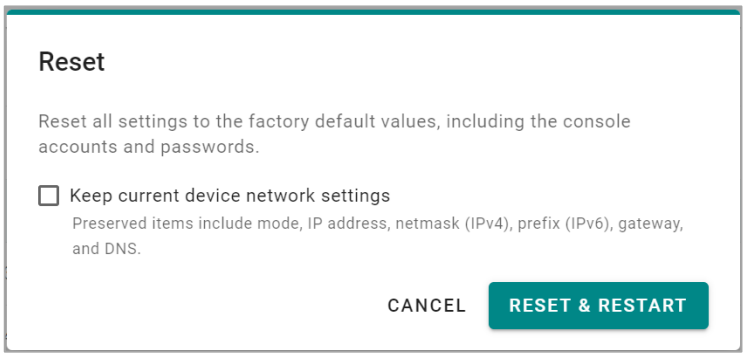
Your device may restart again to make the configuration effective, and your work in progress will be stopped.

> **NOTE**
>
> For the cause of failure, refer to Appendix: Error Messages.

Reset

The device(s) needs to be unlocked before the function can be used.

Reset may apply to one or more devices. Select the devices that you need to reset and then select the **Reset** button.



Keep Current the Device Network Settings

If you wish to keep the existing network settings for the device(s), check the options.

COM Mapping

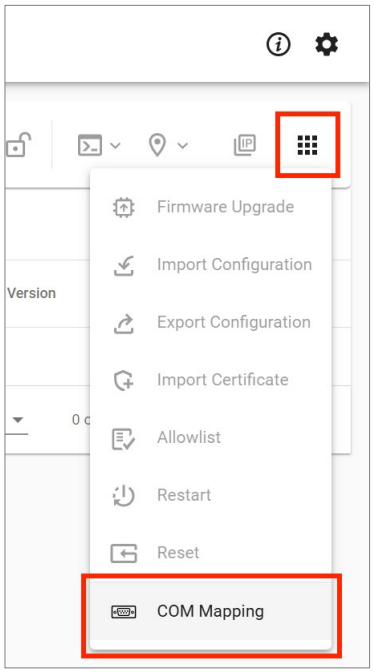
Real COM Mode

Set up the NPort's or MGate's serial ports as remote COM ports for your PC host. For the NPort, set the serial port(s) to Real COM mode when mapping COM ports with the Moxa Windows Driver Manager.

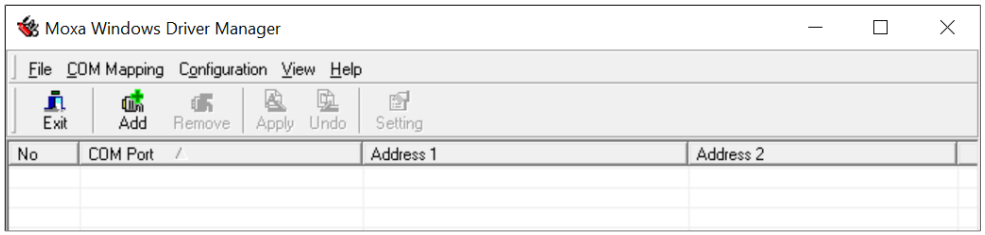
NOTE

1. At this moment, COM mapping only supports the **NPorts** and the **MGate MB3x70-G2**.
2. COM mapping requires Moxa Windows Driver Manager. If your computer does not have Moxa Windows Driver Manager installed, re-run the DSU installer to include Moxa Windows Driver Manager installation or download it from Moxa.com/Support.
3. To run COM mapping, your computer must have the latest Visual C++ Redistributable installed. It may be necessary to restart your computer after installing Visual C++ Redistributable.

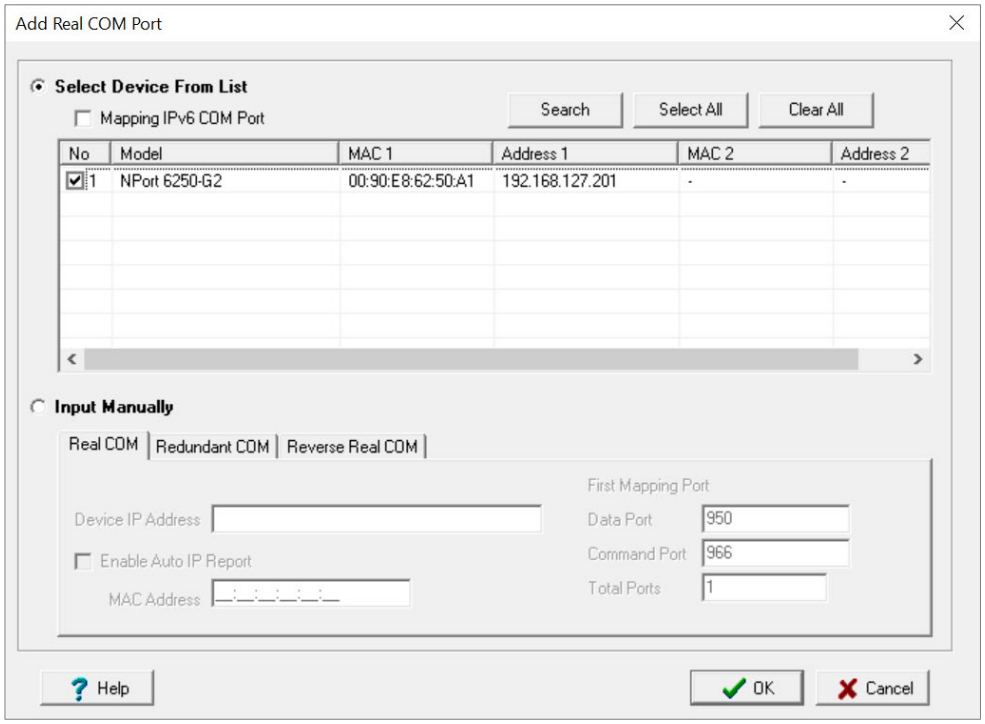
1. Select **COM Mapping** in the **More Functions**.



2. Select the **Add** icon in **Moxa Windows Driver Manager**. For the MGate MB3x70-G2 Series, you may jump to step 4.



3. Select **Search** to search for NPort device servers. From the list that is generated, select the server to which you will map COM ports, and then select **OK**. The default IPv4 address will be changed to the IPv6 address when **Mapping IPv6 COM Port** is checked.



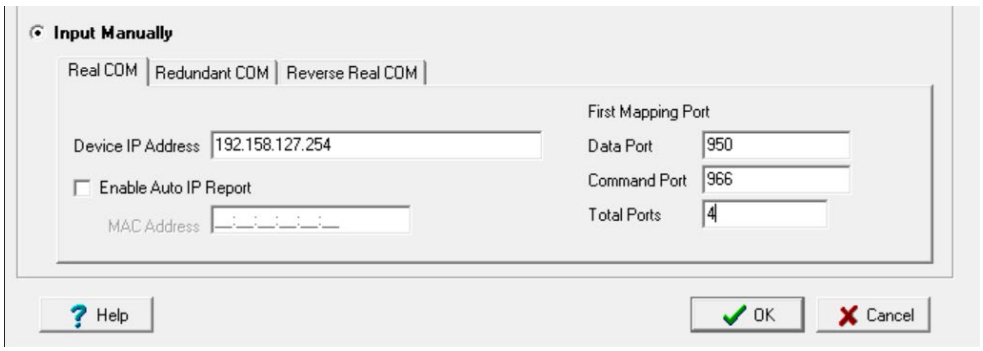
NOTE

Only the NPort 6000 and NPort 6000-G2 models support IPv6.

4. For the **NPort**, alternatively, you can select **Input Manually** and then manually enter the NPort **Device IP Address**, first **Data Port**, first **Command Port**, and **Total Ports** to map the COM ports. Note that the Add Real COM Port page supports Fully Qualified Domain Name (FQDN), in which case the IP address will be filled in automatically.

   For the **MGate MB3x70-G2 Series** supporting up to 4 Real COM, you are only required to enter the MGate **Device IP Address** and **Total Ports** set to 4 to which the COM ports will be mapped. **Neither Data Port and Command Port are required to change**.

   Select **OK** to proceed to the next step.



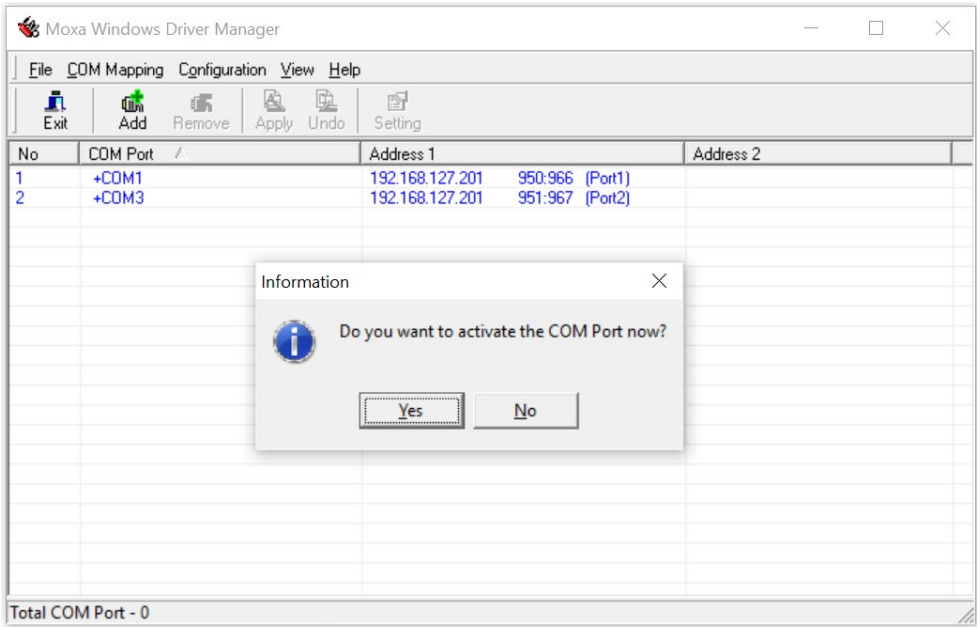
NOTE

For NPort's **Real COM mode**, the Data Port number and Command Port number are fixed. The Data Port number starts at **950** for your device's serial port 1, **951** for serial port 2, and so on. The Command Port number starts at **966** for serial port 1, **967** for serial port 2, and so on.

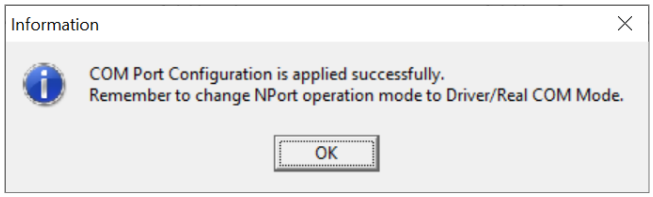
For example, if your device has eight serial ports and you only want to map **ports 3 to 5**, set **Total Ports** to **3**. The first mapped port will have a Data Port number of **952** and a Command Port number of **968**.

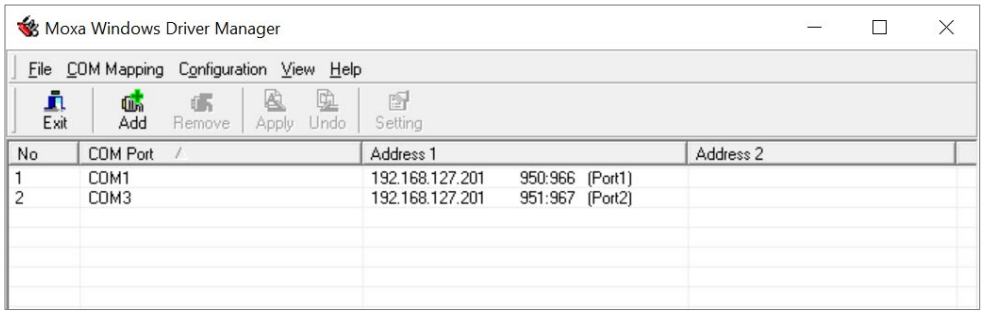
If you need to map serial ports **non-sequentially** (e.g., port 3 and port 5), you must add each port **separately**.

5. COM ports and their mappings will appear in blue until activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not use the COM port until it is activated. Select **Yes** to activate the COM ports or **No** to activate the COM ports later.



6. Upon successful activation, a confirmation dialogue will appear, and all activated ports will change to black.



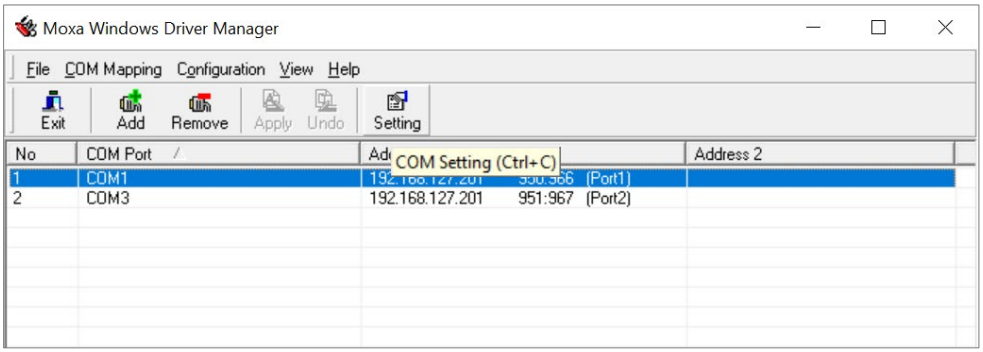


NOTE

1. The **Redundant COM** mode is available for CN2600 models and the NPort 6600-G2 only; **Redundant COM** mode encryption is only available on the NPort 6600-G2 models.
2. The **Reverse Real COM** mode is available for the NPort 6000 and 6000-G2 only.

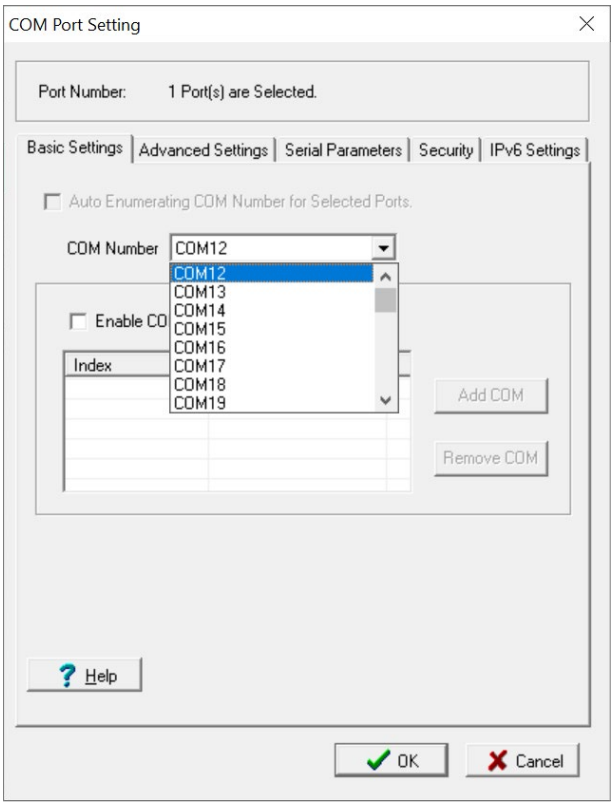
Configuring the Mapped COM Ports

To reconfigure the settings for a specific serial port on the NPort in Real COM mode, choose the corresponding row and select the **Setting** icon.



Basic Setting

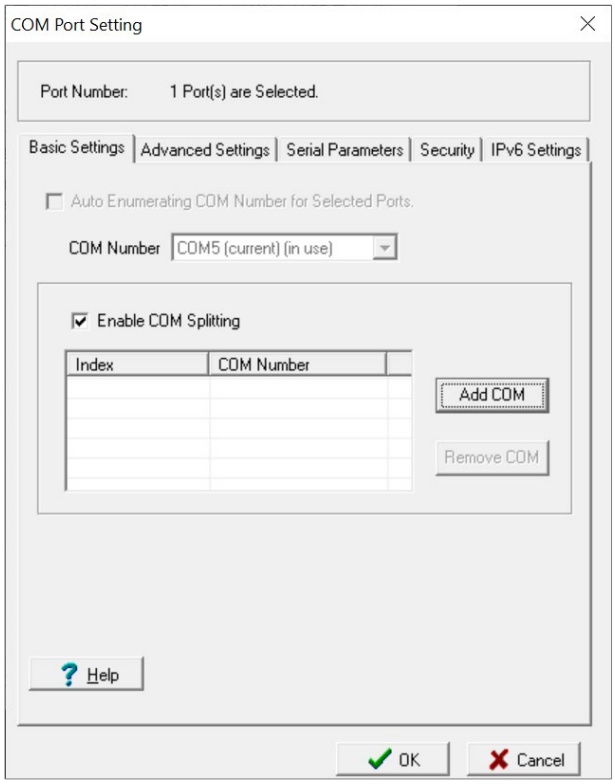
Under the **Basic Setting** window, use the **COM Number** drop-down list to select a COM number to be assigned to the serial port that is being configured. If you have selected multiple ports, you may select the **Auto Enumerating COM Number for Selected Ports** option to assign available COM numbers in sequence to selected serial ports. Note that it will label ports that are "in use" accordingly.



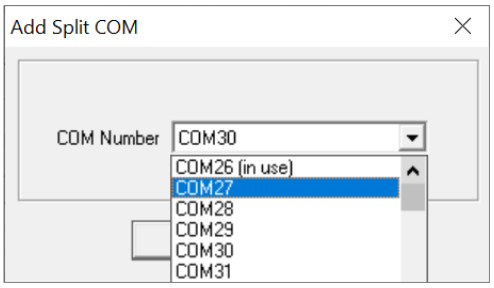
COM Splitting

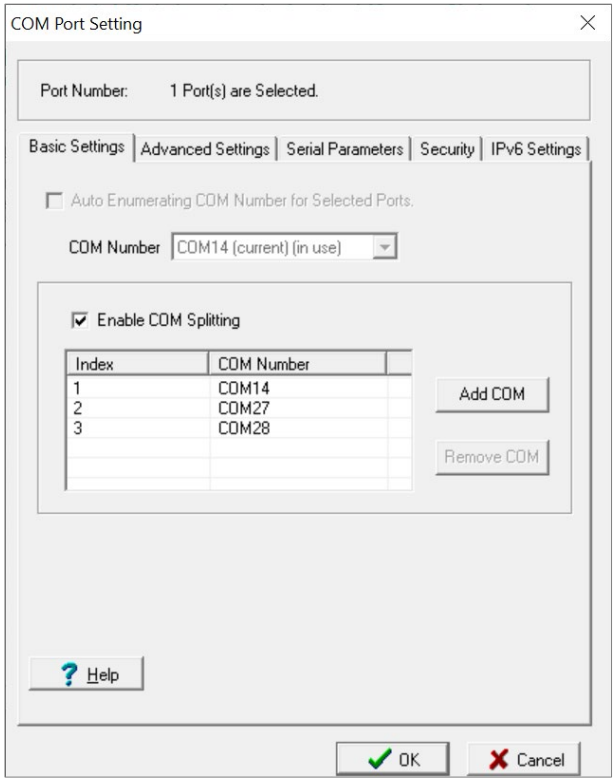
COM **Splitting** allows you to redirect data from the same serial port to several virtual COM ports on your computer. Remember, you need to adjust **Max Connection** in your NPort. For example, if you split into two COM ports, **Max Connection** needs to be adjusted to 2. Refer to the **Max Connection** introduction in the NPort User Manual regarding configuration and number limitation.

1. **Enabling COM Splitting**

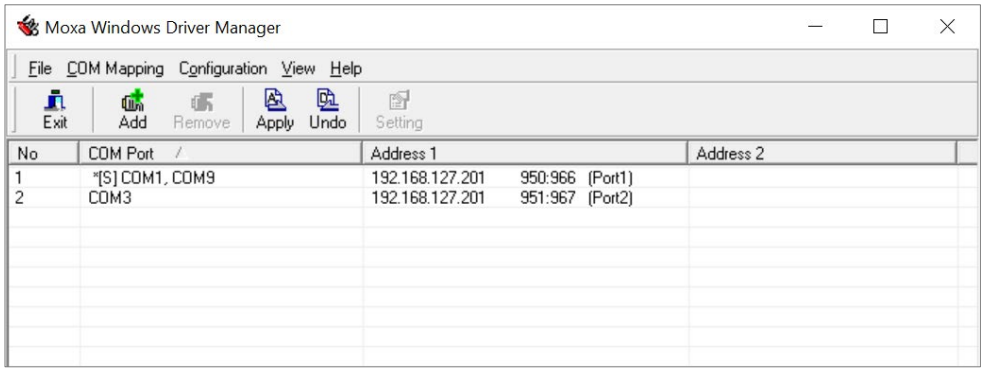


2. **Add COM** to select target COM ports for splitting; the COM port must be available.

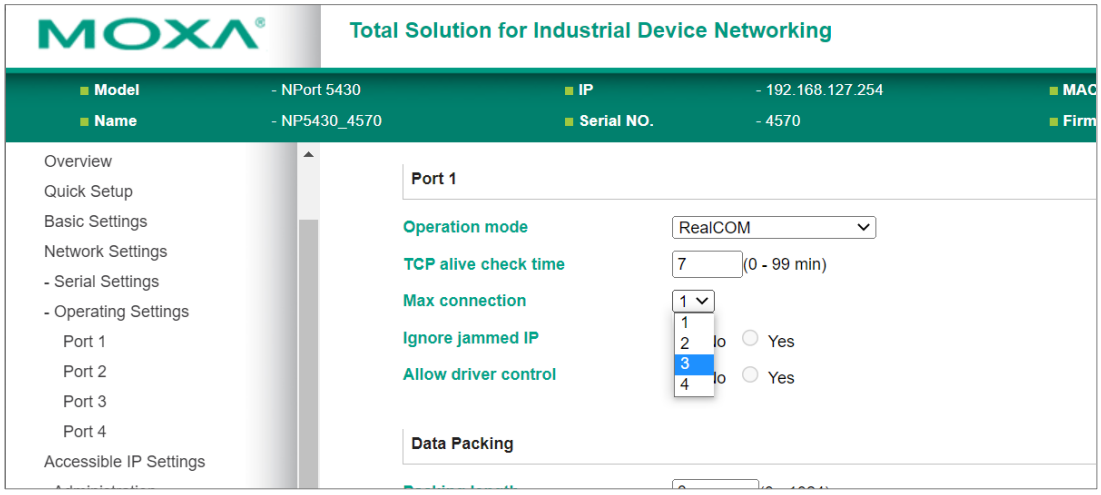




3. After pressing OK, make sure that you have grouped together the COM ports you just selected. Then, select **Apply** to save the change.

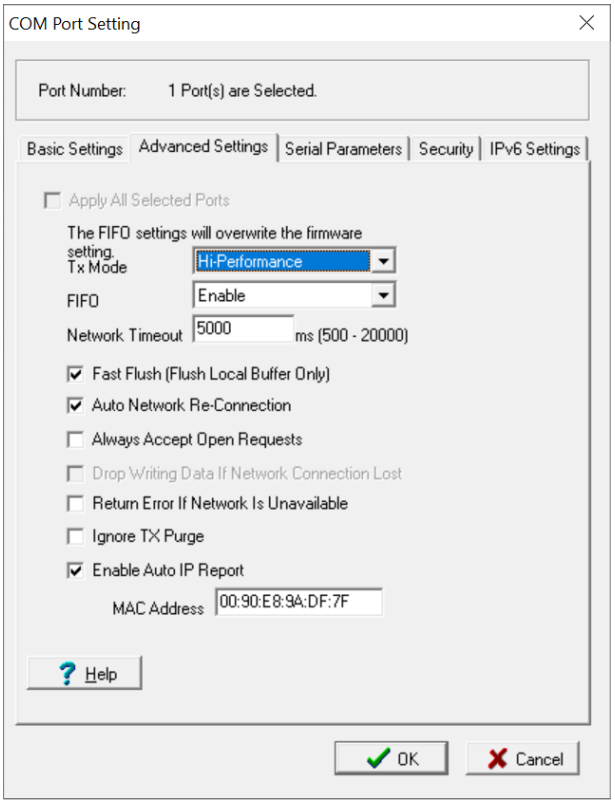


4. In the NPort's **Operating Settings**, adjust the number in the **Max Connection** drop-down menu to match the unit's number in the **Com Splitting** Group



Advanced Setting

Select the **Advanced Setting** tab to change **Tx Mode**, **FIFO**, and **Flash Flush**.



Tx Mode

Hi-Performance is the default for **Tx Mode**. After the driver sends data to the NPort, the driver immediately issues a "Tx Empty" response to the program. Under **Classical** mode, the driver waits to send the "Tx Empty" response until it receives confirmation from the NPort's serial port. This causes lower throughput. If you want to ensure that all data is sent out before further processing, we recommend using **Classical** mode.

FIFO

If **FIFO** is disabled, the NPort will transmit one byte each time until the Tx FIFO becomes empty, and it will generate a Rx interrupt for each incoming byte. This will cause a faster response and lower throughput.

Network Timeout

Use this option to prevent blocking if the target NPort is unavailable.

Fast Flush (only flushes the local buffer)

For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. After a program uses the PurgeComm() function, the NPort driver actively queries the NPort's firmware multiple times to ensure there is no queued data in the NPort's firmware buffer, instead of simply flushing the local buffer. This design is used to satisfy some special considerations. However, it may take more time (about several hundred milliseconds) than a native COM1, because of the additional time spent communicating across the Ethernet. Therefore, PurgeComm() works much faster with native COM ports on the PC than with mapped COM ports on the NPort. To accommodate other applications that require a faster response time, the NPort driver implements a **Fast Flush** option. This function is enabled by default.

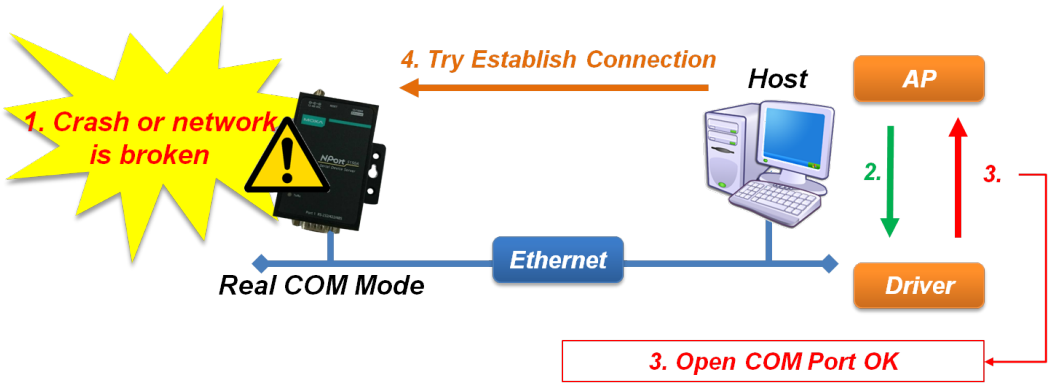
If you have disabled **Fast Flush** and find that COM ports mapped to the NPort perform markedly slower than when using a native COM port, check if your application uses "PurgeComm()" functions. If so, try enabling the **Fast Flush** function and see if there is a significant improvement in the **Performance.**

Network Reconnection

With this option enabled, the driver will repeatedly attempt to re-establish the TCP connection if the NPort does not respond to background "check-alive" packets.

Always Accept Open Requests

When the driver cannot establish a connection with the NPort, the user's software can still open the mapped COM port, just like an onboard COM port.



Return Error If the Network Is Unavailable

Disabling this option will prevent the driver from returning any errors even where a connection to the NPort cannot be established. Enabling this option will cause the Win32 Comm function to return the error code "STATUS_NETWORK_UNREACHABLE" when a connection cannot be established to the NPort. Typically, this shows that your host's network connection is offline, likely because of a disconnected cable. If you can access other network devices, it could show that the NPort is not currently powered or is not properly connected. To use this function, make sure **Auto Network Re-Connection** is enabled.

Drop Writing Data If Network Connection Lost

If the network connection between Windows and the NPort device is lost, the enabled NPort driver will drop the writing data. The writing data will not be sent out after the network reconnects.

Ignore TX Purge

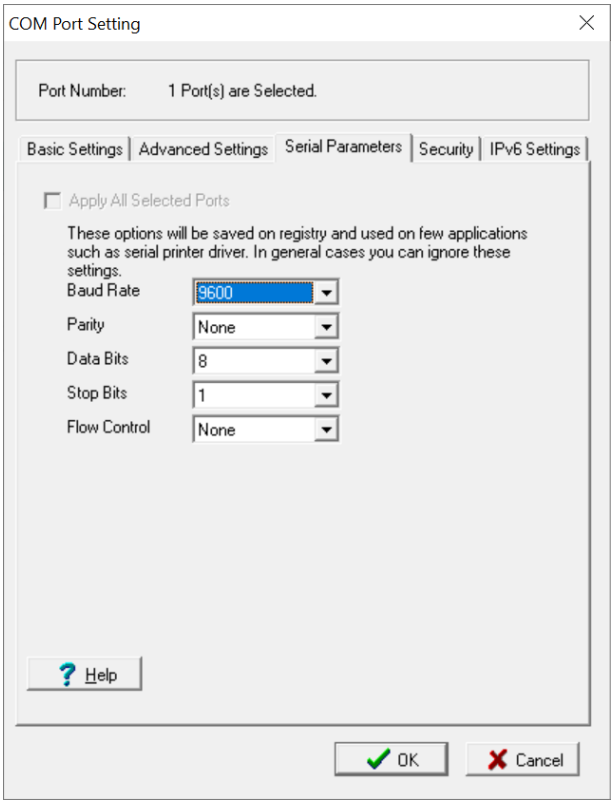
Applications can use the Win32 API PurgeComm to clear the output buffer. The application will end outstanding overlapping write operations. Select the **Ignore TX Purge** checkbox to ignore the effect on output data.

NOTE

Starting **Windows Driver Manager** v1.19 supports certain **Moxa OnCell** models; the **Enable Auto IP Report** function in the **Advance Settings** only supports OnCell products.

Serial Parameters

Once the NPort is powered on, the **Serial Parameters** window in the following figure displays the default settings. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



Security (NPort 6000 and NPort G2 models)

Enable Encryption

Enable the SSL encryption for data and command transmission of the selected COM port.

- **Data only**

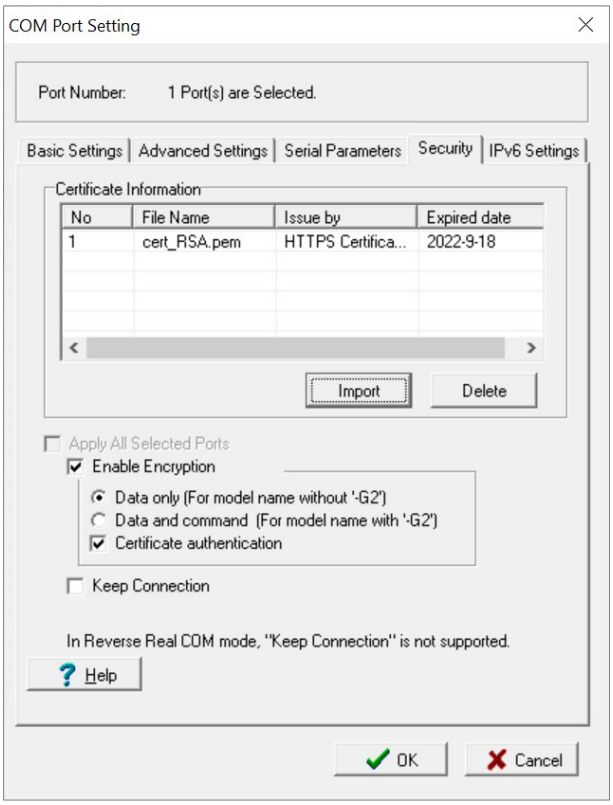
  Older models of NPort support data encryption only. Select this option if you are using older NPort
- **Data and command**

  NPort G2 supports both data and command encryption. Select this option if you are using NPort G2 models.
- **Enable certification authentication**

  Supports the NPort G2 and NPort 6000 models only. This is a security enhancement that provides you with a mechanism to check if the Certificate Authority (CA) has certified an imported certificate. Select the Import button above to import certification of your own.

Keep Connection

If you frequently open/close your COM port (with data encryption enabled), and if the NPort is used by only one host, we recommend enabling this option for quicker operations. A COM port with encryption enabled will take a short time (300 to 500ms) while opening because of the SSL protocol. Enabling these options will ensure that the COM port connection (SSL) remains connected. Here, opening/closing the COM port will be quicker.



NOTE

In **Reverse Real COM** mode, **Keep Connection** is not supported.

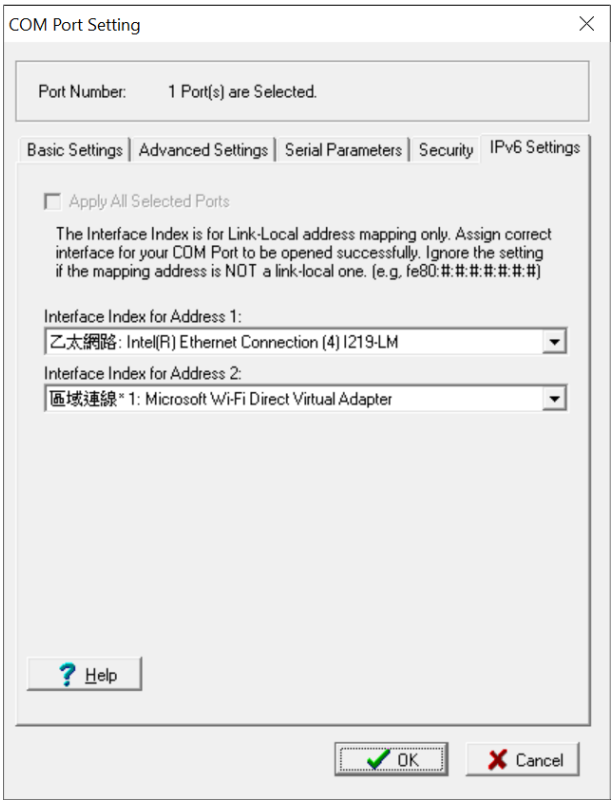
IPv6 Settings (NPort 6000 and NPort 6000-G2 models)

Interface Index

The **Interface Index** is for Link-Local address mapping only. Ignore the setting if the mapping address is not a Link-Local (e.g., fe80: 0/64) one. Assign the **Interface Index** for routing issues when the COM port is mapped with a link-local address. This setting tells the Windows system which interface to route the data to.

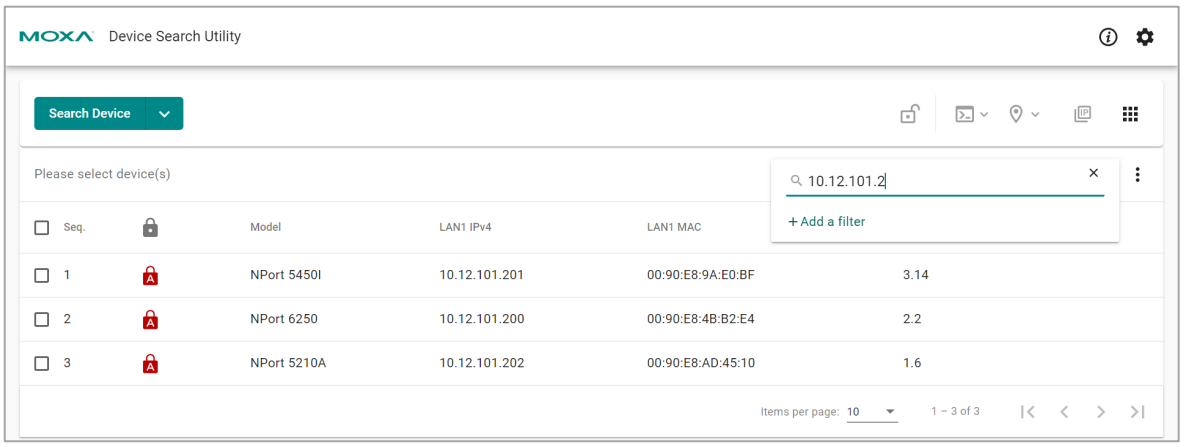
NOTE

1. Security supports the NPort 6000 and NPort G2 models only.
2. IPv6 settings support the NPort 6000 and NPort 6000-G2 models only.

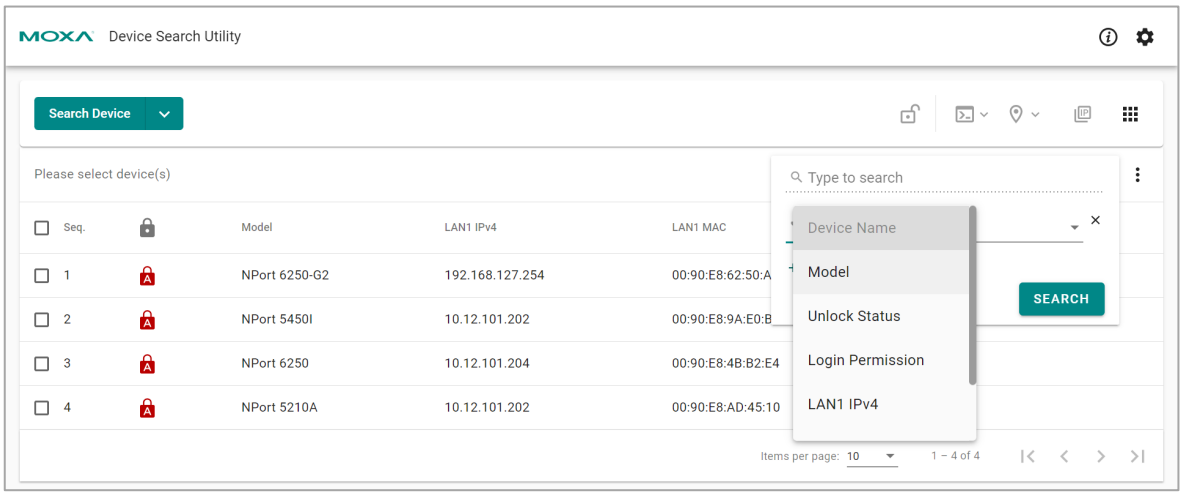


Filter

Filter is to help you quickly find the device(s) that you are looking for from a long list. Enter any value in the **Type to search** field, and it will quickly search for matching device attributes.



Or, you can use **Add a filter** to use single or combined conditions to help you find specific devices.



The **Filter** function will also search for the character(s) in the hidden columns.

Filter Options

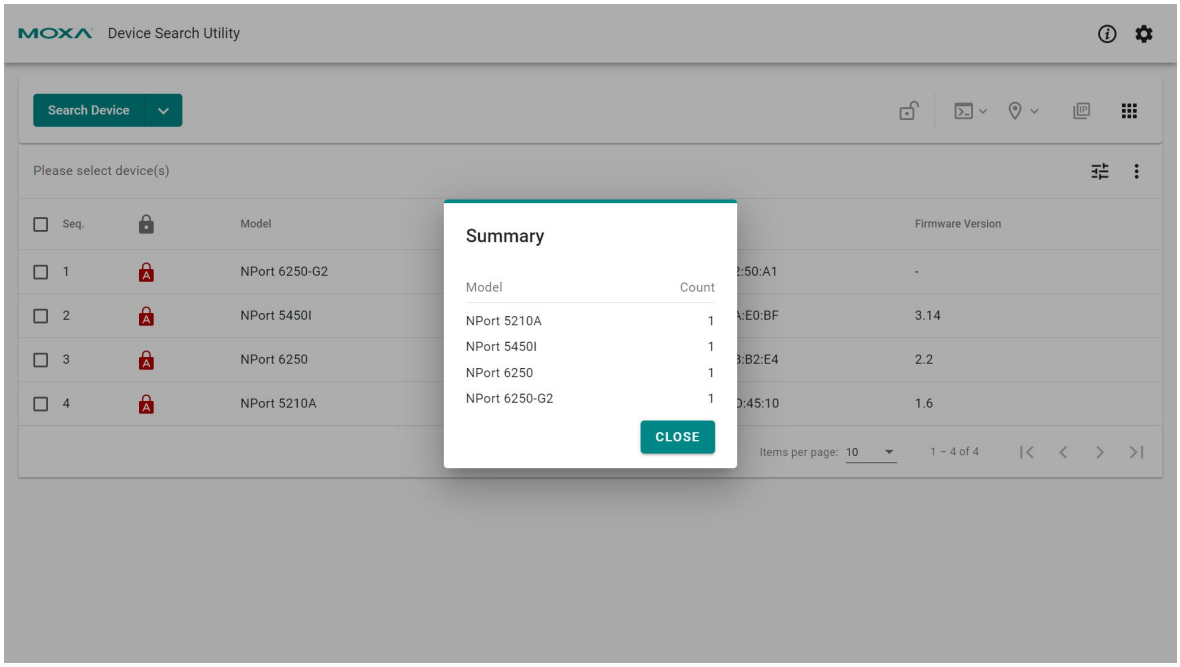
Filter Value	Filter Criteria
Device Name	Searching input value in the Device Name field
Model Name	Searching input value in the Model Name field
Unlock Status	Searching for locked or unlock devices
Login Permission	Search for devices with Advanced, Legacy, Default or Normal login. (Refer to the **Unlock** section for detailed permission definition)
LAN1 IPv4	Searching for the IP value in the IPv4 field
LAN1 MAC	Searching for the MAC address value in the LAN1 MAC field
Firmware Version	Search for device firmware version in the Firmware Version field

NOTE

Filter value is case sensitive.

Summary View

The Summary View offers a straightforward display of the total count for each model in the search table list.



Save List to File

Save List to File saves the device(s) showing in the current view to a local file. View the saved file in CSV format by using editing software like Microsoft Excel or macOS Numbers.

The saved file looks like this:

B9

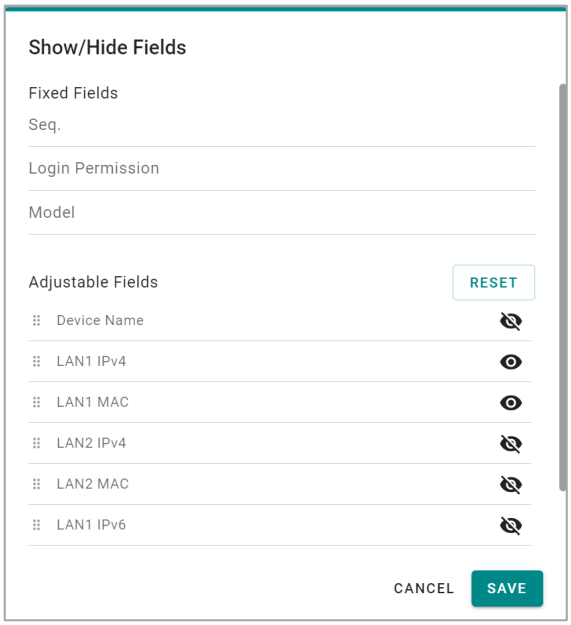
	A	B	C	D	E	F	G
1	Seq.	Login Permission	Model	LAN1 IPv4	LAN1 MAC	Firmware Version	
2	1	Advanced	NPort 6250-G2	10.12.101.199	00:90:E8:62:50:A1	1.0.0	
3	2	Advanced	NPort 5450I	10.12.101.201	00:90:E8:9A:E0:BF	3.14	
4	3	Advanced	NPort 6250	10.12.101.200	00:90:E8:4B:B2:E4	2.2	
5	4	Advanced	NPort 5210A	10.12.101.202	00:90:E8:AD:45:10	1.6	

NOTE

1. If you wish to include more fields in the file, you need to make the field visible in **Show/Hide Columns**.
2. For security reasons, there may be information on certain fields that are hidden. Unlock those devices first to have all data shown in the list.

Show/Hide Columns

Default settings do not display all the device's attributes. If you need to have those fields available, show the columns as visible:



: Visible

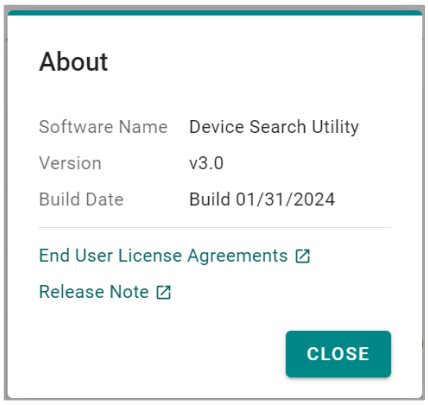
: Invisible

> **NOTE**
>
> Only the options under **Adjustable Columns** can be shown. The options under **Fixed Columns** will always be shown by default.

Application Information

About

Find End **User License Agreements** and **Release Notes** here.

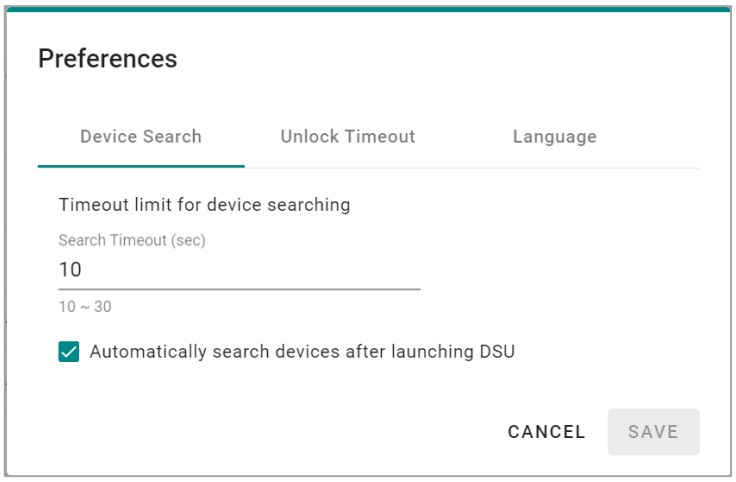


User Manual

Here you can find the User Manual of **DSU**. If you need to read the user manual in other languages, switch the language in **Preference > Languages**, or find the PDF file in **Program files\Moxa\Device Search Utility\wwwroot\assets**.

Preference

Device Search



Timeout Limit for Searching Devices

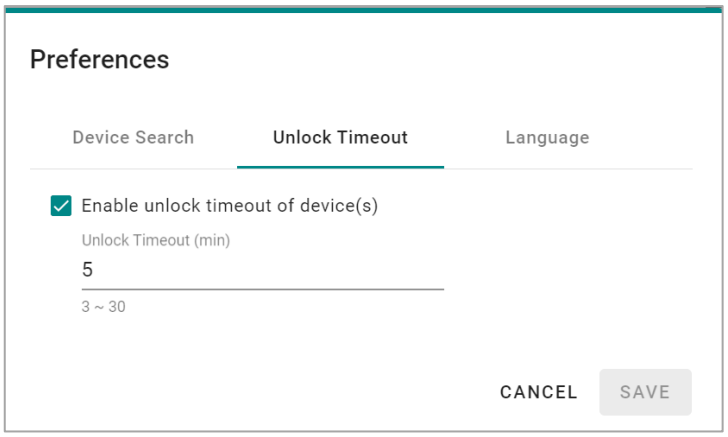
When a device is discovered, the timer for each search restarts and continues searching until no more devices are found.

The default time limit is 10 seconds.

Automatically Searching Devices After Launching DSU

When the application is launched, the search will trigger. The default is set to On.

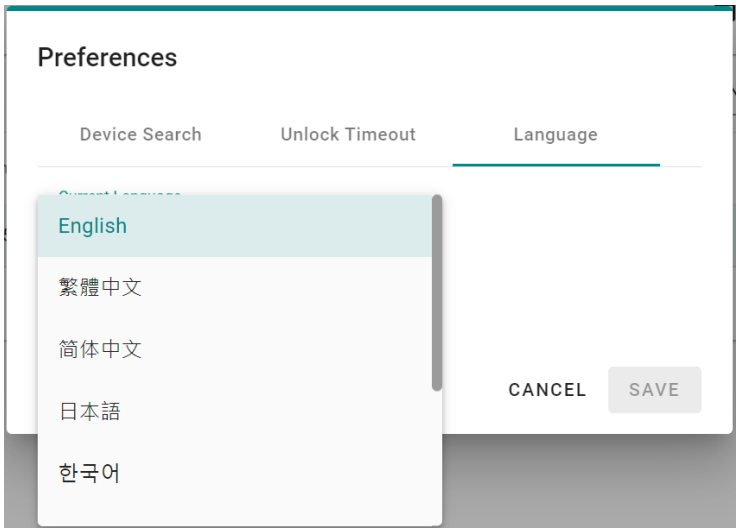
Unlock Timeout



In **DSU**, this value determines the unlock timeout. If the timer expires or the **DSU** application is closed, the device will lock again, and you will need to unlock it again.

> **NOTE**
>
> This is not the same as **Session Timeout** of **Session Control** on the web console.

Language



DSU provides a user interface in a variety of languages: English, Traditional Chinese, Simplified Chinese, Japanese, Korean, German, French, Russian, and Spanish.

3. Usage Scenario Tips

Mass Deployment

DSU is a useful tool for mass deployment when your devices (same model) share a common configuration.

Step 1: Set up configuration in one device in the web console

Step 2: Export configuration file from the device in **DSU**; the configuration is the main configuration file

Step 3: Assign IP for all the devices

Step 4: Import configuration to all the devices (Keep the current device network settings)

A. Error Message

Error Message	Possible Cause	Possible Resolution
The account or password does not comply with the device policy. Check the input values and retry.	The entered account and password do not match the security requirement.	Refer to the security requirement and try again.
Error with the IPv4 address in the configuration file. Check and retry importing.	The IPv4 address value in the configuration file is not correct.	Check the IPv4 address value in the configuration file and try again.
Error with the IPv4 gateway in the configuration file. Check and retry importing.	The IPv4 gateway value in the configuration file is not correct.	Check the IPv4 gateway value in the configuration file and try again.
Error with the IPv4 netmask in the configuration file. Check and retry importing.	The IPv4 netmask value in the configuration file is not correct.	Check the IPv4 netmask value in the configuration file and try again.
Error with the IPv6 address in the configuration file. Check and retry importing.	The IPv6 address value in the configuration file is not correct.	Check the IPv6 address value in the configuration file and try again.
Error with the IPv6 gateway in the configuration file. Check and retry importing.	The IPv6 gateway value in the configuration file is not correct.	Check the IPv6 gateway value in the configuration file and try again.
Error with the IPv6 prefix in the configuration file. Check and retry importing.	The IPv6 prefix value in the configuration file is not correct.	Check the IPv6 prefix value in the configuration file and try again.
Failed to {action}. Retry.	The command initiation or the process has been terminated.	Try again. If failure persists, try the following: • Close the browser page and launch **DSU** again. • Or short press device's reset button once and try again. Then try again.
File format incorrect.	The format of the file is not the correct type.	Check the file format and try again.
Input value does not comply. Check and retry.	Due to the incorrect value, you cannot execute the command.	Check the value and try again.
Insufficient permission.	The login account does not have permission for the action.	Change to another login account with sufficient permission or contact your administrator.
The IPv4 address value does not comply. Check and retry.	The value entered for the IPv4 address does not comply with the requirement.	Check the value and try again.
The IPv4 gateway value does not comply. Check and retry.	The value entered for the IPv4 gateway does not comply with the requirement.	Check the value and try again.
The IPv4 netmask value does not comply. Check and retry.	The value entered for the IPv4 netmask does not comply with the requirement.	Check the value and try again.
The IPv6 address value does not comply. Check and retry.	The value entered for the IPv6 address does not comply with the requirement.	Check the value and try again.
The IPv6 gateway value does not comply. Check and retry.	The value entered for the IPv6 gateway does not comply with the requirement.	Check the value and try again.

Error Message	Possible Cause	Possible Resolution
The IPv6 prefix value does not comply. Check and retry.	The value entered for the IPv6IPv6 prefix does not comply with the requirement.	Check the value and try again.
The marked device(s) may possibly be in a different network segment with your computer, or there may be an issue with the networking. It is recommended to check before proceeding further.	The device is not in the same network segment as DSU.	Relocate both the device and DSU to the same network segment.
Selected file cannot be opened.	The file cannot be imported, possibly the file is accessed by another application or being moved or does not exist.	Check the file status and try again
Session timed out while performing Keep IP. Check the IP configuration in the device before processing further.	Timeout when trying to keep IPv4 or IPv6.	Check if the IPv4 or IPv6 value stays the same before continuing.
Session timed out while trying to restart. Restart the device manually.	The device is not responding after restarting.	• Search the device again after 1 minute. • Check the network. • Check if the device is still powered on. If it is, short press the reset button once; if not, check the power source or power cable and power up the device again. Then search again and check if the intended action has been achieved or not.
Session timed out. Retry.	The device is not responding.	• Check the networking. • Check if the device is still powered on
The device does not support the feature.	The command is not accepted.	The device may not support this function.
Unable to connect while performing **Keep current the device network settings**. Check the IP configuration in the device before processing further.	The connection dropped when trying to keep IP.	Check if the IPv4 or IPv6 value stays the same before continuing.
Unable to connect while trying to restart. Restart the device manually.	The device is not reachable after restarting.	• Search the device again after 1 minute. • Check the network. • Check if the device is still powered on. If it is, short press the reset button once; if not, check the power source or power cable and power up the device again. Then, search again and check if the intended action has been achieved or not.
Unable to connect. Check the network.	The network may be experiencing a link failure.	Check the networking.
Unable to {Action}. Retry.	Failed to execute the command, possibly the command initiation or the process having been terminated.	Try again. If failure persists, try the following: • Close the browser page and launch **DSU** again. • Or short press the reset button once. Then, try again
An unknown error occurred while trying to restart. Restart the device manually.	An unknown error occurred.	• Search the device again after 1 minute. • Check the network. • Check if the device is still powered on. If it is, short press the reset button once; if not, check the power source or power cable and power up the device again. Search again and check if the intended action has been achieved or not.

Error Message	Possible Cause	Possible Resolution
An unknown error occurred. Retry.	An unknown error occurred.	Try again. If failure persists, try following: • Close the browser page and launch **DSU** again. • Or short press device's reset button once. Then, try again.
You have not logged in or the login session timed out.	You have not unlocked the device or the device's unlock function timed out.	Unlock the device again.
The Telnet service is not available on your computer. Check your Windows settings and try again.	The Telent application is not available to be called.	Install the application if it has not been installed yet. To enable the service, go to **Windows settings** and enable **Telnet Client**.
The search range cannot span across network segments.	Out of range for Search by IP range.	Keep the first three fields constant, and only change the fourth field, e.g., 192.168.127.1 to 192.168.127.255.