

User Manual : Neosoft NILRT Firewall Tools

Version 1.0

	Author	Auditor	Recipient
Name	Dany Baron		
Company	Neosoft Technologies	Neosoft Technologies	

Neosoft Technologies Inc.
4800 rue de Rouen, suite 230
Montréal, QC H1V 3T4

Toll-free: 1-866-636-7381
Phone: (418) 948-8324
Fax: (418) 948-8325
<https://www.neosoft.ca>

HISTORY

Version	Date	Author	Modification
1.0	2024-06-19	Dany Baron	Initial release

SUMMARY

1	Introduction	5
2	System Requirements	5
3	Licensing	5
4	Installation Instructions	6
4.1	Obtain the package	6
4.2	Install the package	6
4.2.1	If you have an .ipk file	6
4.2.2	If you have access to the Neosoft package repository	6
5	Using the software	7
5.1	Starting neofw	7
5.2	Configuring the firewall	7
5.2.1	Select applications	7
5.2.2	Specify TCP & UDP custom ports	8
5.2.3	Apply rules	9
6	Troubleshooting	9

FIGURES

Figure 1.	Neosoft license directory	5
Figure 2.	Installing neo-fw-tools from file.....	6
Figure 3.	Allowed applications list	7
Figure 4.	Custom allowed TCP ports	8
Figure 5.	Applied firewall rules.....	9

1 Introduction

Neosoft NILRT Firewall Tools (neo-fw-tools) is a software package designed for managing firewall configurations on National Instruments Linux Real-Time (NILRT) systems. This tool provides a user-friendly, graphical interface for configuring firewall rules to enhance the security of your NILRT devices.

2 System Requirements

- Target Hardware: National Instruments CompactRIO and PXI products
- Operating System: NI Linux Real-Time (NILRT)
- Prerequisites:
 - Root access to the target device
 - SSH client (e.g., PuTTY) for remote access

3 Licensing

The neo-fw-tools package requires a license from Neosoft Technologies specific to the unit's serial number.

1. Obtain a License:
Contact Neosoft Technologies to obtain a license file (<package>.lic) for your target device. You may contact Neosoft Technologies using the contact information at the start of this document. Be sure to provide the serial number of the target on which you wish to install the package.
2. Install the License:
Transfer the license file to the /etc/neosoft/licenses directory on the target device using a SFTP client. You may create the directory if it does not exist.

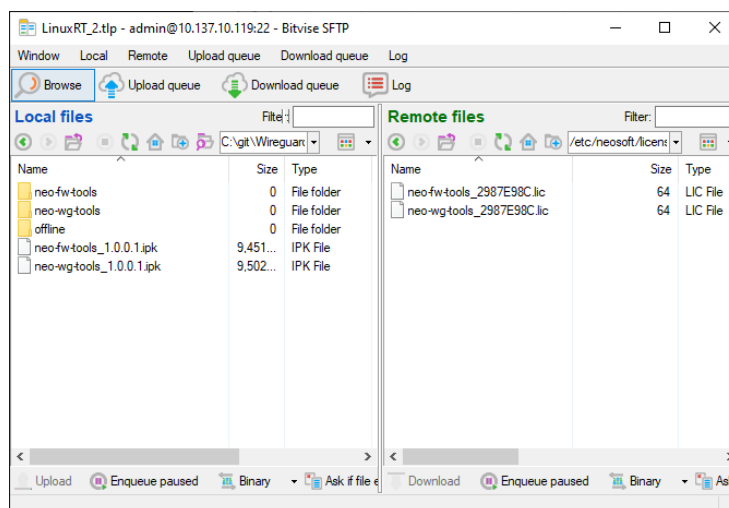


Figure 1. Neosoft license directory

4 Installation Instructions

4.1 Obtain the package

You may add the Neosoft package repository if you were provided an URL or obtain the package file directly from your Neosoft representative.

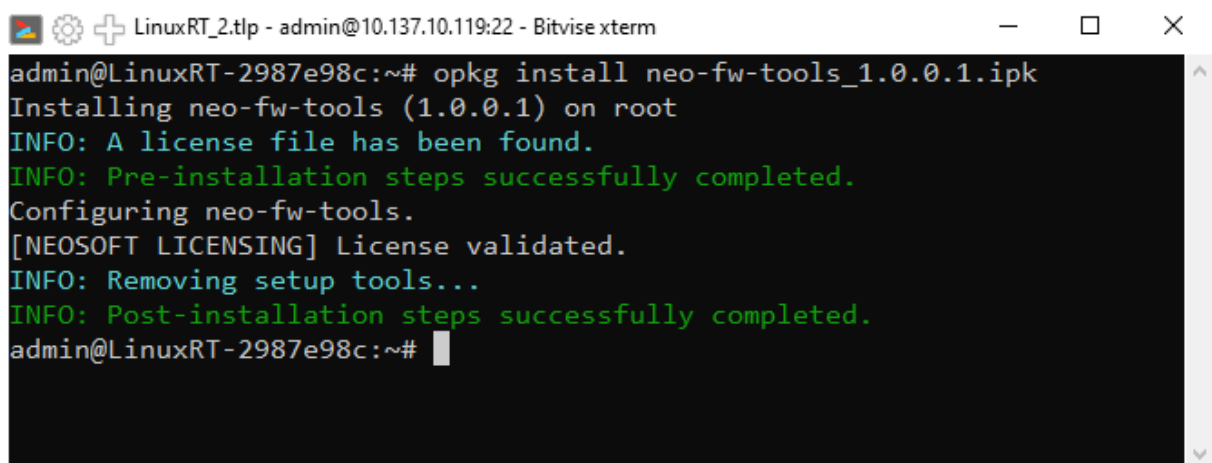
If you obtained the package file directly, use a SFTP client to transfer the package file (<package>_<version>.ipk) to the target device.

4.2 Install the package

4.2.1 If you have an .ipk file

Open an SSH terminal (e.g., PuTTY) and connect to the target device. Execute the following command to install the package (replace <package.ipk> with the actual name of the file you uploaded to the device):

```
opkg install <package.ipk>
```



```
LinuxRT_2.tlp - admin@10.137.10.119:22 - Bitvise xterm
admin@LinuxRT-2987e98c:~# opkg install neo-fw-tools_1.0.0.1.ipk
Installing neo-fw-tools (1.0.0.1) on root
INFO: A license file has been found.
INFO: Pre-installation steps successfully completed.
Configuring neo-fw-tools.
[NEOSOFT LICENSING] License validated.
INFO: Removing setup tools...
INFO: Post-installation steps successfully completed.
admin@LinuxRT-2987e98c:~#
```

Figure 2. Installing neo-fw-tools from file.

4.2.2 If you have access to the Neosoft package repository

Open an SSH terminal (e.g., PuTTY) and connect to the target device. Execute the following command to download and install the package:

```
opkg install neo-fw-tools
```

5 Using the software

5.1 Starting neofw

After installation, you can invoke neofw by simply using the “neofw” command, without arguments.

5.2 Configuring the firewall

After executing the command, the interface will start up, allowing you to configure the firewall.

5.2.1 Select applications

A checklist dialog will appear, allowing you to select the applications you want to allow through the firewall from a curated list. It includes common NI and system applications.

You can navigate the list using the arrow keys and select an application in the list to be allowed using the space key. You can navigate between the list and the main menu using the tab key.

Once the allowed applications have been selected, you can press enter to go to the next step.

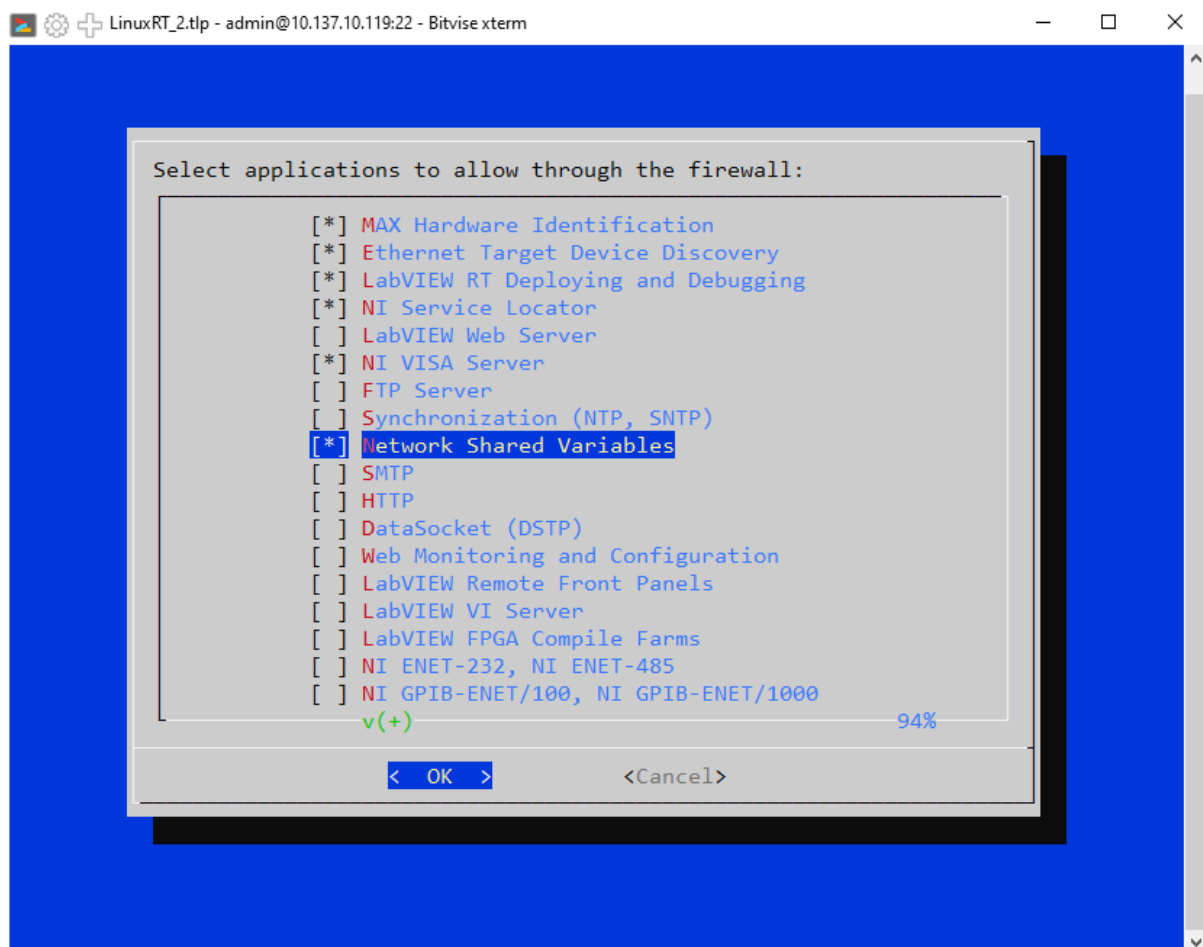


Figure 3. Allowed applications list

5.2.2 Specify TCP & UDP custom ports

The second and third screen will prompt you to add TCP and UDP custom ports, respectively.

If you use a custom application with a specific port or port range that is not listed in the app list on the first screen, this is where you will enter the ports it will use.

You can enter multiple ports or ranges of ports, separated by a comma. Port ranges are specified with a colon (:).

For example: "499, 5000:6000" will allow inbound port 499 and 5000 to 6000.

To validate the input and/or go to the next screen, press the enter key.

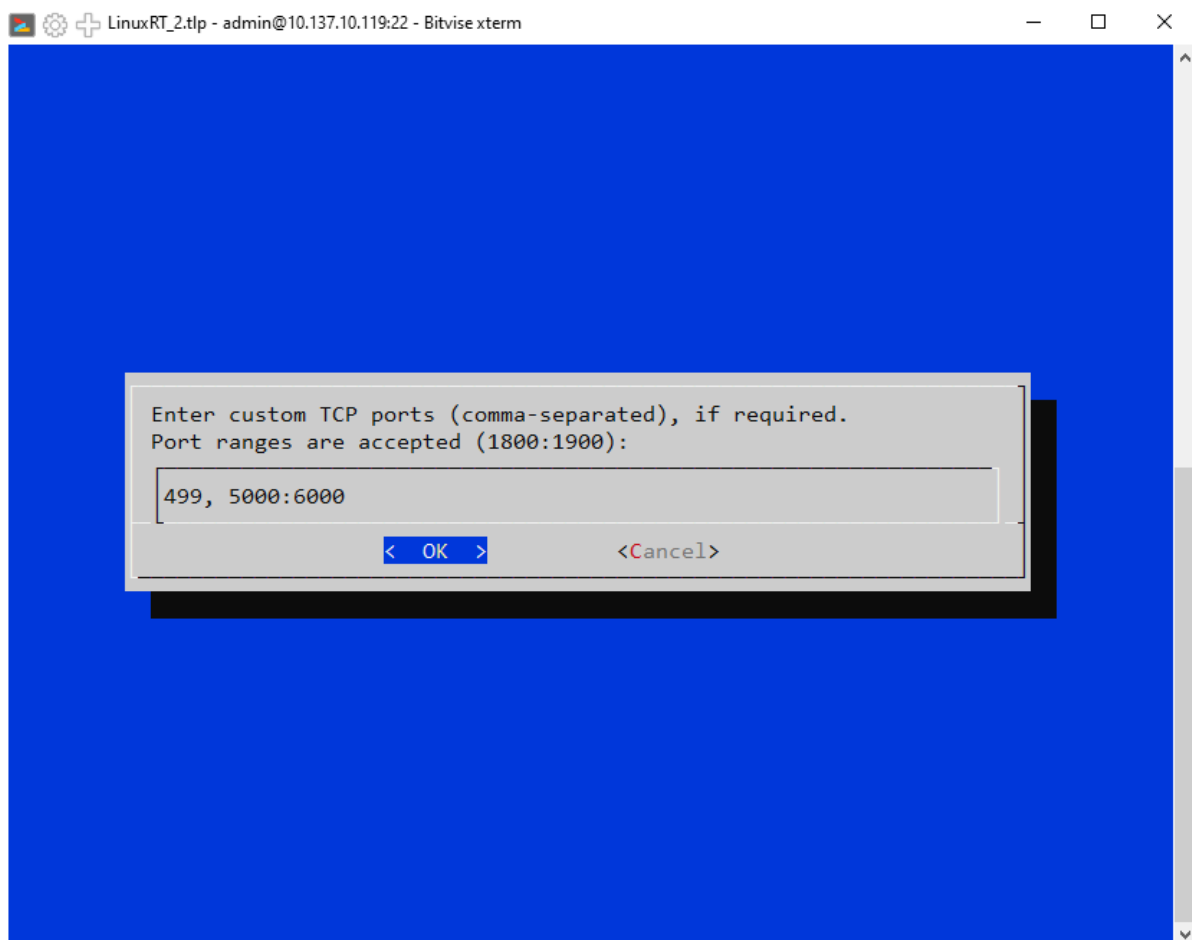
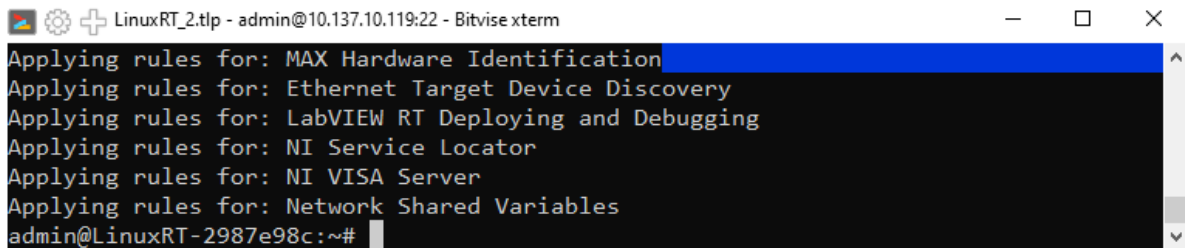


Figure 4. Custom allowed TCP ports

5.2.3 Apply rules

Once all screens have been validated, the firewall rules will automatically be generated and immediately be applied.



```
LinuxRT_2.tlp - admin@10.137.10.119:22 - Bitvise xterm
Applying rules for: MAX Hardware Identification
Applying rules for: Ethernet Target Device Discovery
Applying rules for: LabVIEW RT Deploying and Debugging
Applying rules for: NI Service Locator
Applying rules for: NI VISA Server
Applying rules for: Network Shared Variables
admin@LinuxRT-2987e98c:~#
```

Figure 5. Applied firewall rules

6 Troubleshooting

- **Permission Denied:** Ensure you are running the neofw utility with root privileges, as it is required to modify the firewall settings.
- **License validation issues:** Verify the license file is placed in the correct directory (/etc/neosoft/licenses) and corresponds to the target device's serial number.