



User Manual

Version 1.0.1 July 2022

NMC-9181

Network Management Controller



Table of Contents

1. Introduction	6
1.1 Features.....	6
1.2 Specifications.....	8
1.3 Application	9
2. Getting Started	10
2.1 Mounting the NMC-9181	11
2.2 Installing the RJ-45 waterproof connector assembly.....	15
2.3 Deploying a Basic NMC-9181 System.....	19
2.4 Using eSearch Utility to Connect the NMC-9181.....	21
3. Hardware.....	22
3.1 Appearances.....	22
3.2 Dimension	28
3.3 Rescue CF Card	29
4. LibreNMS	31
4.1 How to connect to LibreNMS.....	31
4.1.1 Use the eSearch Utility	31
4.1.2 Connect to LibreNMS from Ubuntu operation.....	33
4.2 Web Interface.....	35
4.2.1 Overview	35
(1) Dashboard.....	35
(2) Maps.....	38
(3) Plugins.....	39
(4) Tools	42
(5) Eventlog.....	43
4.2.2 Devices.....	43
(1) All Devices	43
(2) Geo Locations.....	45
(3) Manage Groups.....	46

(4) Device Dependencies	47
(5) Add Device	48
(6) Delete Device	50
4.2.3 Services	51
(1) All Services	51
(2) Services Templates	52
(3) Add Service	55
4.2.4 Ports	57
(1) All Ports	57
(2) Traffic Bills	58
(3) Interface Description Parsing	60
(4) Manage Groups	61
4.2.5 Health	62
4.2.6 Alerts	64
(1) How to setting alert transports and rule	64
(2) Notifications	68
(3) Alert History	69
(4) Statistics	69
(5) Scheduled Maintenance	70
(6) Alert Templates	70
4.2.7 User settings	71
4.2.8 Global settings	73
4.3 License	75
5. FAQ	76
Q01: An error message appears during [Add Device] [Cannot ping 192.168.xxx.xxx]	76
Q02: An error related to [SNMP] occurred during [Add Device].	78
Q03: How to import SNMP MIB files?	82
Q04: How to use Google SMTP to send a letter?	84
Q05: How to clean up LibreNMS log files?	87
Q06: How to Add Device?	88
Q07: How to Change Your IP Address on Linux?	89

Q08: How to Setting Display mode on Linux?	90
Appendix A. Revision History	94

Important Information

Warranty

All products manufactured by ICP DAS are under warranty regarding defective materials for a period of one year, beginning from the date of delivery to the original purchaser.

Warning

ICP DAS assumes no liability for any damage resulting from the use of this product. ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, not for any infringements of patents or other rights of third parties resulting from its use.

Copyright

Copyright © 2021 by ICP DAS Co., Ltd. All rights are reserved.

Trademark

Names are used for identification purpose only and may be registered trademarks of their respective companies.

Contact us

If you have any problem, please feel free to contact us. You can count on us for quick response.

Email: service@icpdas.com

1. Introduction

The NMC-9181 is a simple and easy-to-use network management controller that can be installed and operated without professional skills, and can manage network devices without additional software installation. It is equipped with an Intel E3845 CPU and a variety of connectives including dual Gigabit Ethernet, HDMI, VGA , USB port, RS-232 and RS-485 interface.

1.1 Features

The NMC-9181 built-in Ubuntu desktop operating system, users can easily use and complete the system required settings.

■ Ubuntu



Ubuntu is a Linux-based operating system. It is designed for computers, smartphones, and network servers. The system is developed by a UK based company called Canonical Ltd. All the principles used to develop the Ubuntu software are based on the principles of Open Source software development.

The features of the Ubuntu:

- The desktop version of Ubuntu supports all the normal software on Windows such as Firefox, Chrome, VLC, etc.
- It supports the office suite called **LibreOffice**.
- Ubuntu has an in-built email software called Thunderbird, which gives the user access to email such as Exchange, Gmail, Hotmail, etc.
- There are a host of free applications for users to view and edit photos.
- There are also applications to manage videos and it also allows the users to share videos.
- It is easy to find content on Ubuntu with the smart searching facility.

- The best feature is, it is a free operating system and is backed by a huge open source community.

The NMC-9181 built-in Librenms software package, users can easily complete network device management tasks through Librenms

■ LibreNMS



LibreNMS is an open source, powerful and feature-rich auto-discovering PHP based network monitoring system which uses the SNMP protocol. It supports a broad range of operating systems including Linux, FreeBSD, as well as network devices including Cisco, Juniper, Brocade, Foundry, HP and many more.

The features of the LibreNMS:

- It auto-discovers a whole network using these protocols: CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP.
- It has a mobile friendly Web UI, with customizable dashboards.
- Supports a Unix agent.
- Supports horizontal scaling to expand with your network.
- Supports a highly flexible and customizable alerting system; sends notifications through email.
- Supports an API for managing, graphing and retrieving data from your system.
- Offers a traffic billing system.
- Supports multiple authentication methods such as MySQL, HTTP, LDAP, Radius and Active Directory.
- Allows for auto updating and many other features.

1.2 Specifications

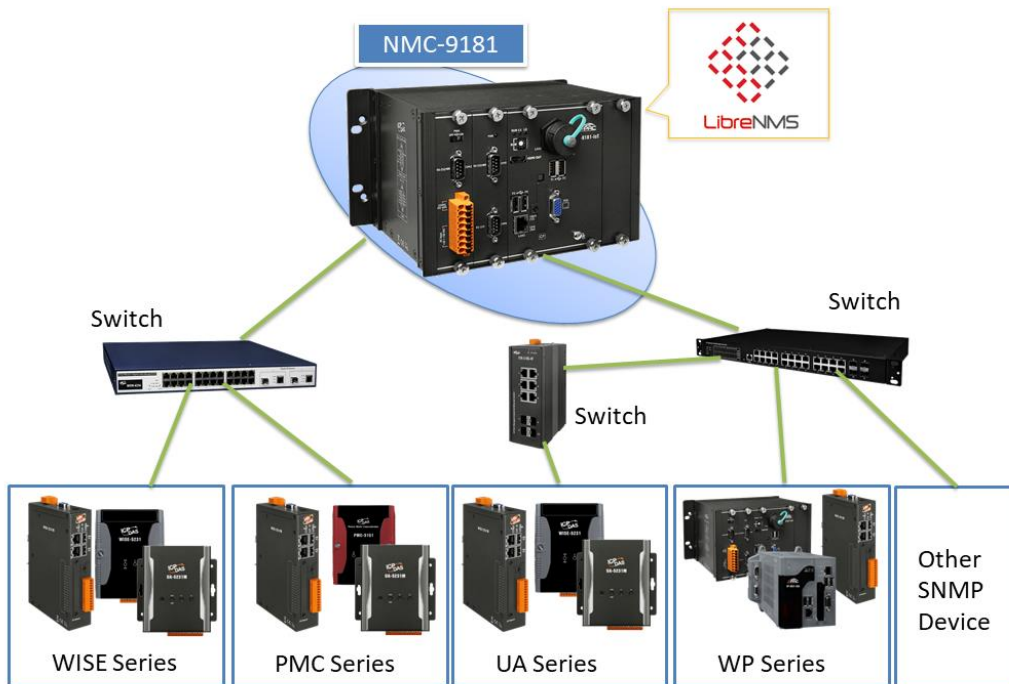
The table below summarizes the specifications of NMC-9181.

Models	NMC-9181
System Software	
OS	Ubuntu 20.04 LTS (64-bit)
Kernel	Linux Kernel 5.11.0-40
Service	SSH , XRDP, Web Server and LibreNMS
Main Unit	
CPU	E3845, 1.91 GHz, 64-bit quad core
System Memory	4 GB DDR3 SDRAM
Storage	64 GB SSD, 32 GB CF card
Flash(SSD)	mSATA slot with one 32 GB SSD
Non-Volatile Memory	128 KB MRAM, 16 KB EEPROM
64-bit Hardware Serial Number	Yes, for software copy protection
Real Time Clock	Provide seconds, minutes, hours, dates, day of week, month, year
Watchdog Timer	Dual Watchdog Timer
Display	
Signal	VGA, HDMI (2560 x 1600 @ 24bpp)
LED Indicators	
Status	PWR, RUN, L1, L2
I/O Expansion	
I/O Type	I-9K, I-97K series
I/O Expansion Slot	1
COM Ports	
Ports	1 x RS-232 (3000 VDC Isolated), 1 x RS-485 (3000 VDC Isolated), 2 x RS-232/RS-485 (3000 VDC Isolated)
HMI	
Buzzer	Yes
Rotary Switch	1 x 10 Position (0 ~ 9)
Ethernet	
Ports	2 x RJ-45, 10/100/1000 Base-TX
USB	
Ports	4 x USB 2.0
Mechanical	

Casing	Metal
Dimensions (W x L x H)	239 x 164 x 133 mm
Installation	DIN-Rail, Wall mounting
Environment	
Operating Temperature	-25 ~ +60°C
Storage Temperature	-30 ~ +80°C
Humidity	10 ~ 90% RH (Non-condensing)
Power	
Input Range	+10 ~ 30 VDC (1 kV Isolated)
Redundant Power Inputs	Yes
Consumption	18.5 W

1.3 Application

NMC-9181 is a network management controller, which can manage network devices in the LAN through SNMP protocol, including WP, XP, Wise, PMC, UA series controllers and other SNMP devices.



2. Getting Started

This chapter provides a guided tour of the NMC-9181 installation and configuration that describes the steps needed to download, install, configure, and run the basic procedures for user working with the NMC-9181 for the first time.

Before starting any task, please check the package contents. If any of the following package contents are missing or damaged, contact your dealer, distributor.

In addition to this guide, the package includes the following items:



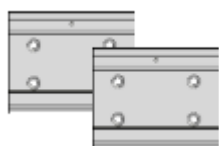
NMC-9181



CF slot with a CF card



Screw Driver



60 mm DIN-Rail Clip x 2



RJ-45 Waterproof Assembly



M3x6L Screw x 8

2.1 Mounting the NMC-9181

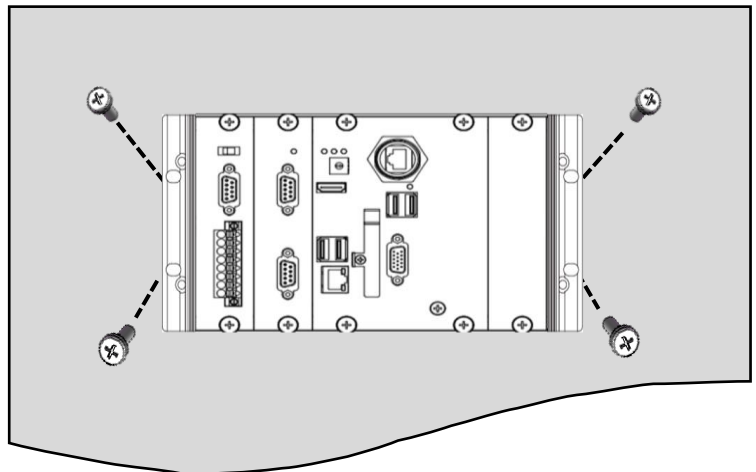
The NMC-9181 can be mounted either directly to a wall/panel, or onto a stainless 35mm DIN rail.

Wall/Panel mounting

Step 1:

Install the four mounting screws into the 4 keyhole mounting holes.

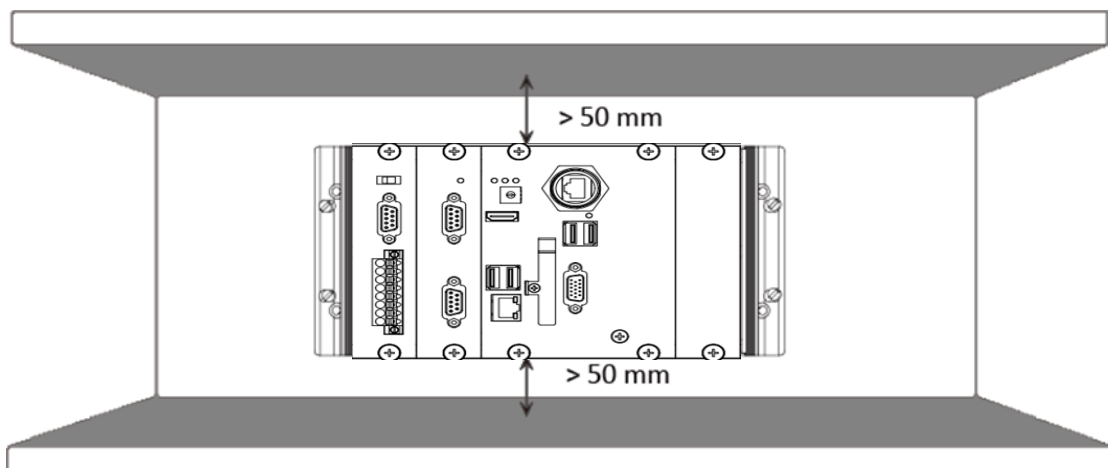
Step 2: Fasten the screws securely.



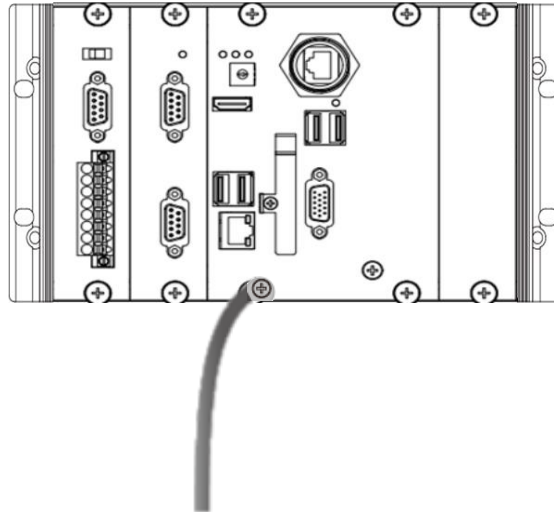
Tips & Warnings



There must be a minimum clearance of 50mm between the NMC-9181 and the top and bottom side of the enclosure panel.



Step 3: Connect the ground lead to the frame ground point.



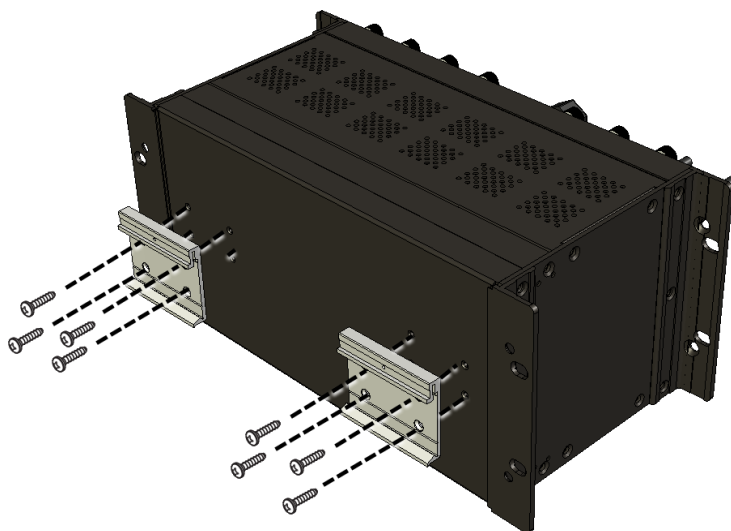
Tips & Warnings



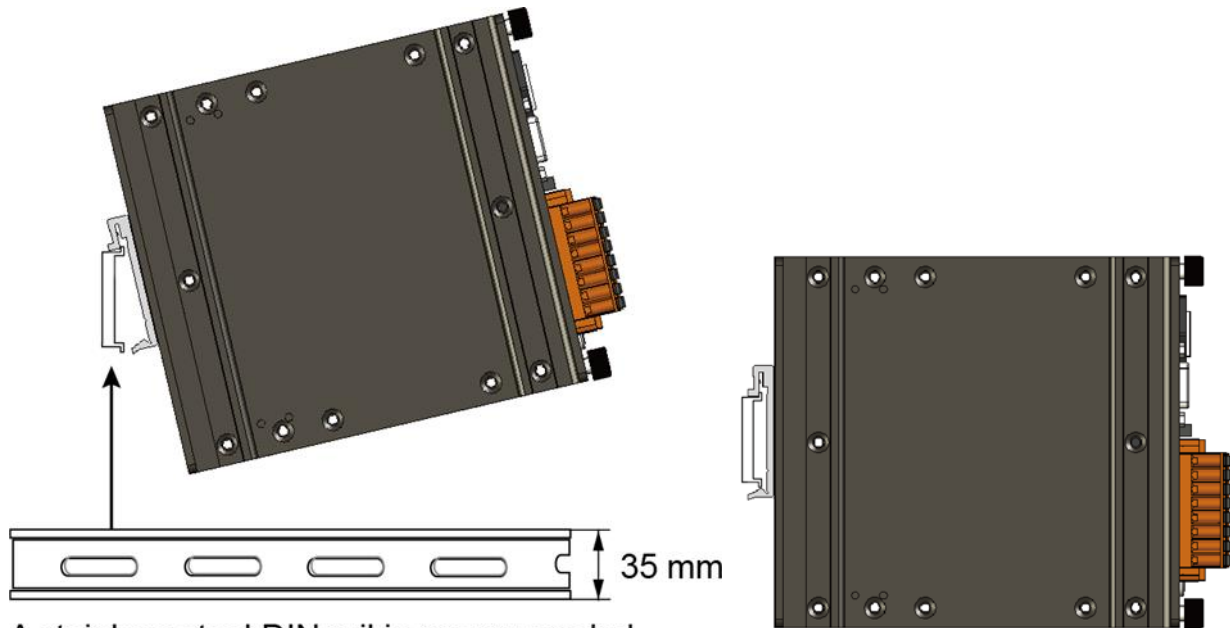
A good common ground reference (earth ground) is essential for proper operation of the NMC-9181. One side of all control circuits, power circuits and the ground lead must be properly connected to earth ground by either installing a ground rod in close proximity to the enclosure or by connecting to the incoming power system ground. There must be a single-point ground (i.e. copper bus bar) for all devices in the enclosure that require an earth ground.

DIN Rail mounting

Step 1: Fasten the DIN rail clip to the NMC-9181



Step 2: Clip the device onto a stainless DIN rail

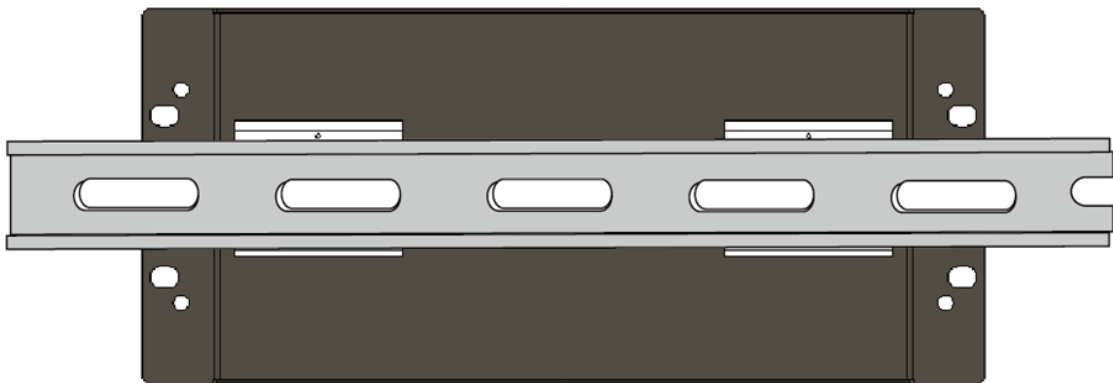


A stainless steel DIN rail is recommended.

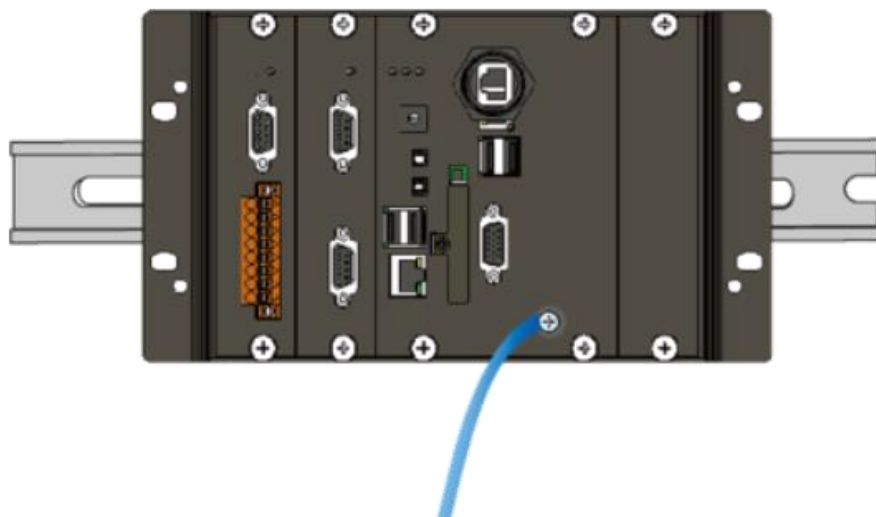
Tips & Warnings



For DIN rail mounting, it is strongly recommended that only a stainless steel DIN rail be used to support the weight of NMC-9181 system, providing stability and preventing NMC-9181 from leaning



Step 3: Connect the ground lead to the frame ground point



Tips & Warnings



A good common ground reference (earth ground) is essential for proper operation of the NMC-9181. One side of all control circuits, power circuits and the ground lead must be properly connected to earth ground by either installing a ground rod in close proximity to the enclosure or by connecting to the incoming power system ground. There must be a single-point ground (i.e. copper bus bar) for all devices in the enclosure that require an earth ground.

2.2 Installing the RJ-45 waterproof connector assembly

The NMC-9181 is equipped with an RJ-45 waterproof connector to protect the connection in vibrate environment.

The RJ-45 waterproof connector is optional for use with LAN1 port. If you do not need the RJ-45 waterproof connector, you can remove the cap and just plug in a regular Ethernet cable.

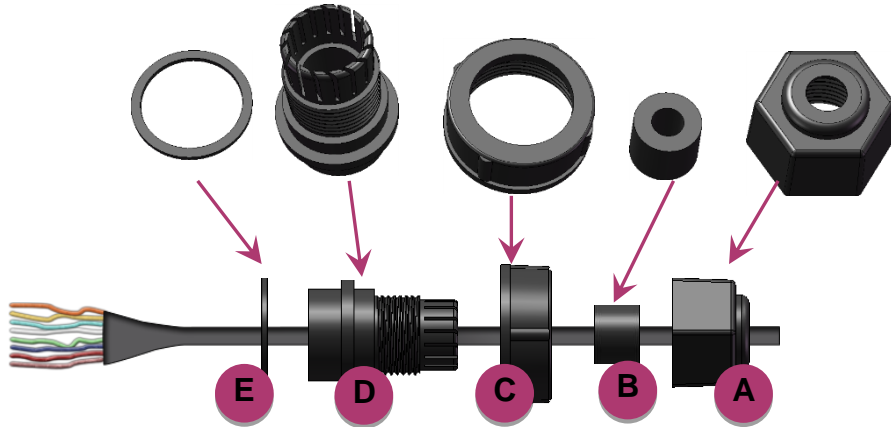


If you want to use the RJ-45 waterproof connector for protecting the connection, follow the instructions below.

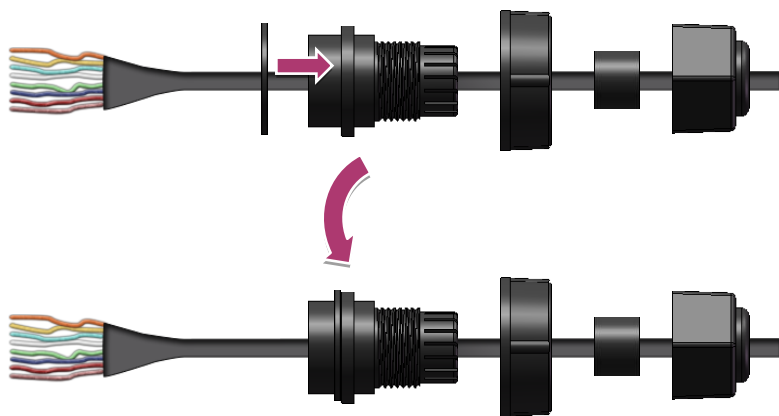
Step 1: Remove the RJ-45 connector from the RJ-45 cable



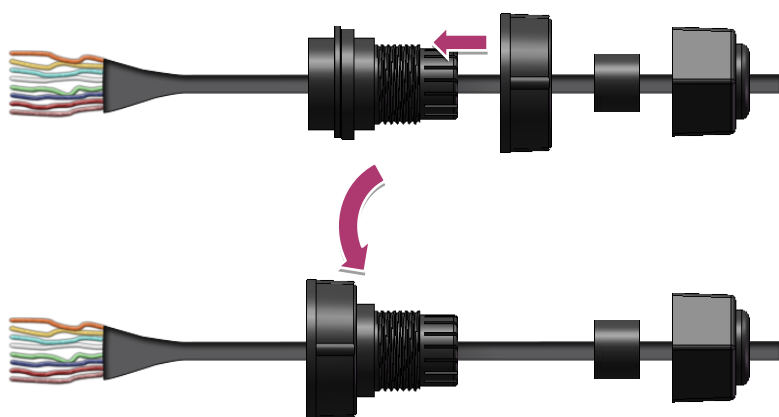
Step 2: Feed the end of the RJ-45 cable through the (A) sealing nut, (B) rubber sealing insert, (C) cable gland base, (D) clamping ring and (E) panel gasket



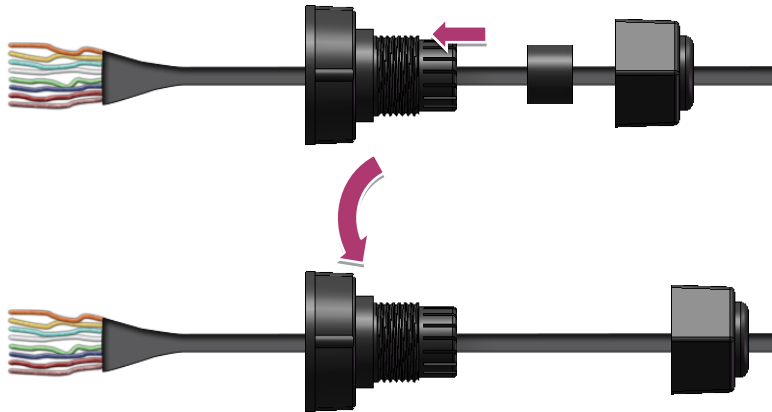
Step 3: Wrap the (E) panel gasket around the (D) clamping ring



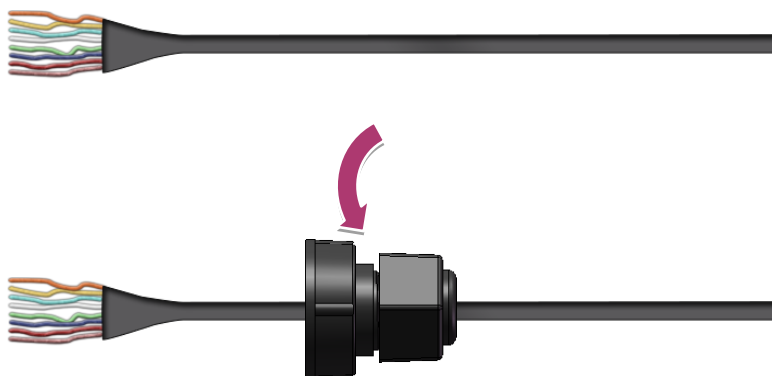
Step 4: Wrap the (C) cable gland base around the (D) clamping ring



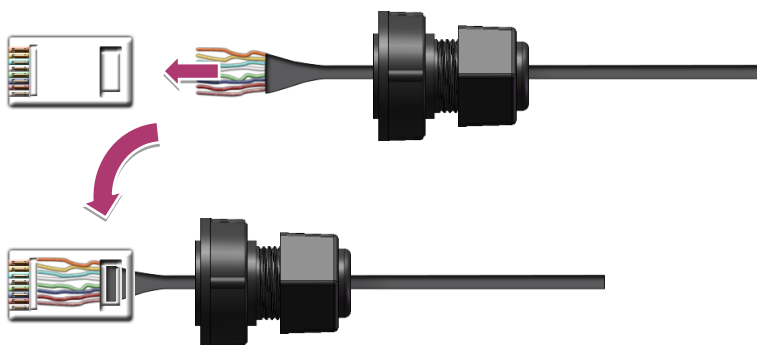
Step 5: Insert the (B) rubber sealing insert into the (D) clamping ring



Step 6: Push the (E) sealing nut forward and Hand-tighten it to seal the assembly



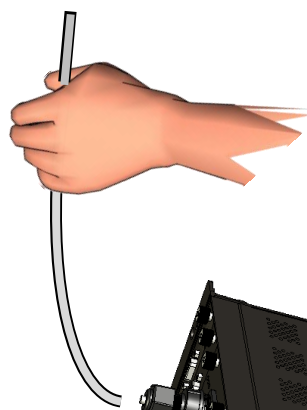
Step 7: Insert the RJ-45 cable into the RJ-45 connector



Step 8: Push the RJ-45 waterproof connector ass grabembly forward



Step 9: Insert the Ethernet cable and screw the RJ-45 waterproof into the receptacle



The Ethernet cable is secured tightly in the connector.



2.3 Deploying a Basic NMC-9181 System

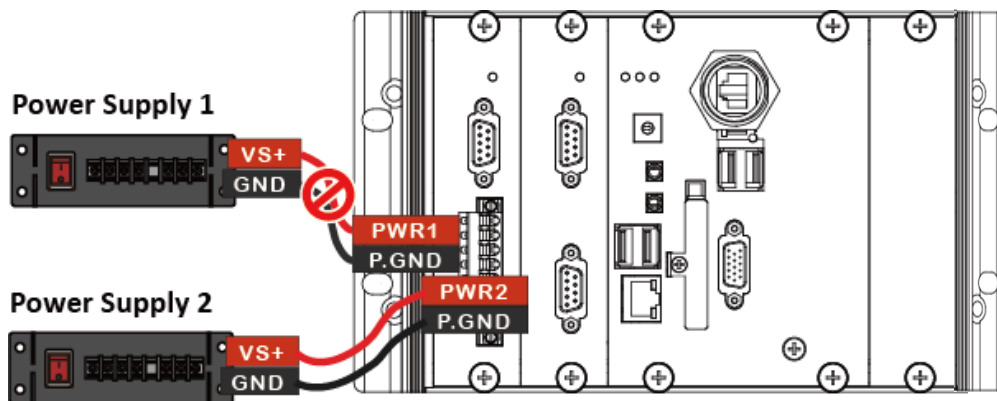
The NMC-9181 provides a variety of communication interface to suit a range of application. Here is a simple application for using the NMC -9181.

Step 1: Connect the positive terminal (+) of the power supply to the terminal PWR1/2 and the negative terminal (-) of the power supply to the P.GND

Tips & Warnings



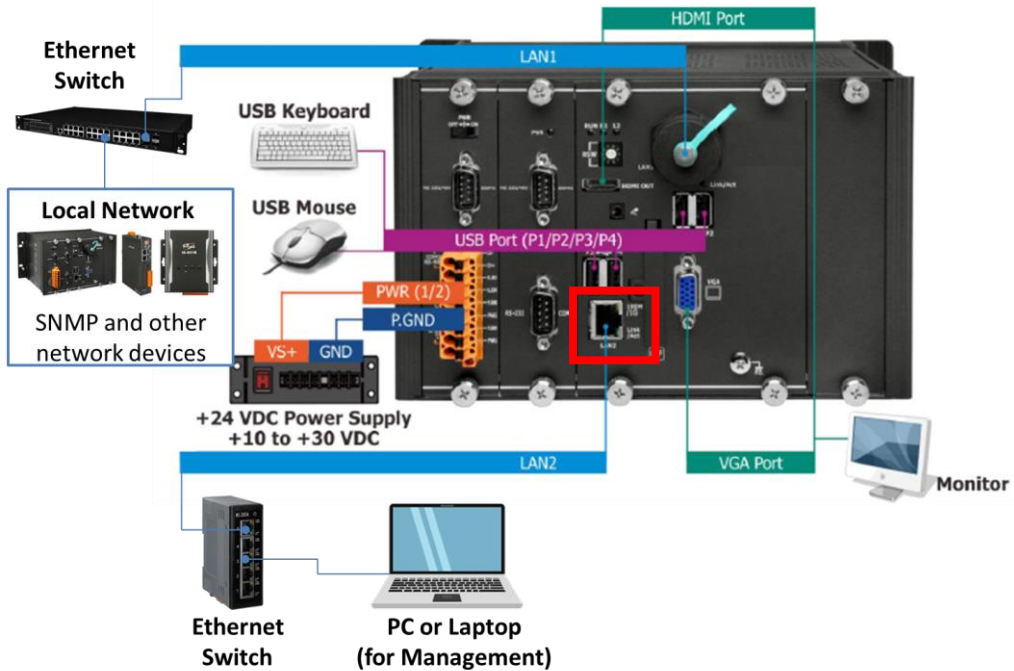
1. The input range of power supply is +10 to +30 V_{DC}.
2. The NMC -9181 have two power inputs that can be connected simultaneously to the two independent power sources. If one power source fails, the other source takes over automatically. Redundant power input help assure non-stop operation of the NMC -9181.



Step 2: Connect the USB mouse or the USB keyboard to the USB port

Step 3: Connect the monitor to the VGA port

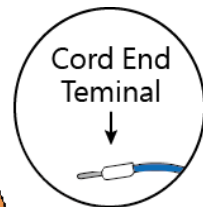
Step 4: Connect PC to the LAN2 through an Ethernet switch.



Tips & Warnings

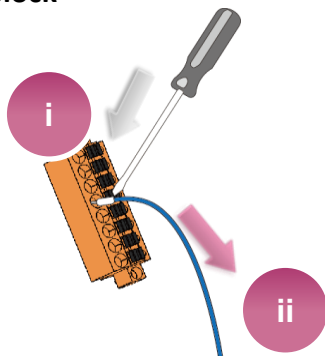


The metal part of the cord end terminal on the wire can be direct wired to the terminal.



Remove the wiring from the terminal block

- i. Use the screwdriver to push the black clip in
- ii. Remove the wiring



2.4 Using eSearch Utility to Connect the NMC-9181

eSearch Utility is a portable application under Linux and all the most popular Windows OS. It supports tDS-700/tGW-700, tM-752N, tSH-700 series modules and most of the ICP DAS Ethernet I/O devices for getting network configuration information such as IP address, gateway, subnet mask, MAC address and alias, and configuring those network settings for modules joining the network.

Please Installing the eSearch Utility

<http://www.icpdas.com/en/product/guide+Software+Utility+Driver+eSearch+Utility>

Step 1: Searching the ethernet device connected on the network

Step 2: Select NMC-9181

Step 3: Connect to the web pages (The default login name is [librenms], password is [D32fwefwef]).

The screenshot shows the LibreNMS web interface. The 'Device Summary' table is as follows:

Summary	Devices	Ports	Services
Up	1	58	0
Down	10	14	0
Ignored tag	0	0	0
Alert disabled	0	NA	NA
Disabled/Shutdown	0	1	0
Total	11	72	0

The 'Eventlog' table shows the following entries:

Timestamp	Type	Hostname
2021-12-07 18:15:07	down	172.17.12.27
2021-12-07 18:15:07	down	172.17.12.30
2021-12-07 18:15:07	down	172.17.12.31
2021-12-07 18:15:07	down	172.17.13.13
2021-12-07 18:15:07	down	172.17.13.94

The 'Top Devices' section lists the following devices and their traffic:

Device	Traffic
172.18.0.248	[Traffic Graph]
172.17.12.26	[Traffic Graph]
localhost	[Traffic Graph]
172.17.12.27	[Traffic Graph]
172.18.0.10	[Traffic Graph]

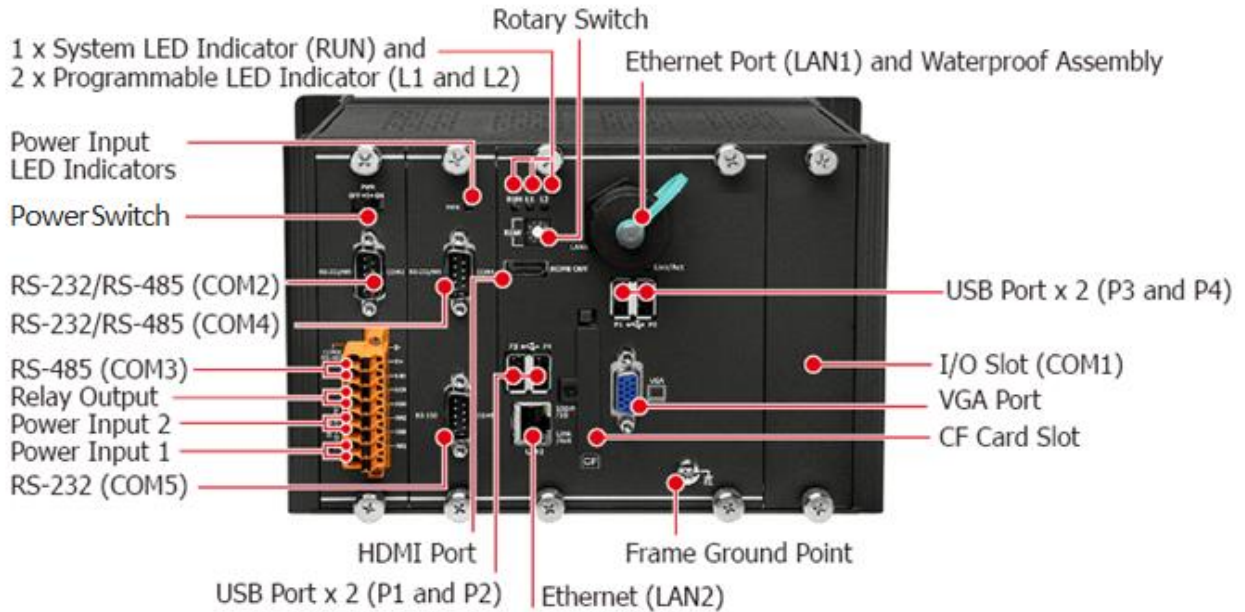
The 'Eventlog' table also includes a detailed view for the selected device 'NMC-9181':

Name	Alias	IP Address	Sub-net Mask	Gateway	MAC Address
NMC-9181	N/A	192.168.255.1	255.255.0.0		00:0D:E0:6E:...

The bottom toolbar contains buttons for 'Search Server', 'Configuration (UDP)', and 'Web'. A red arrow points from the 'Web' button to the 'NMC-9181' entry in the 'Eventlog' table.

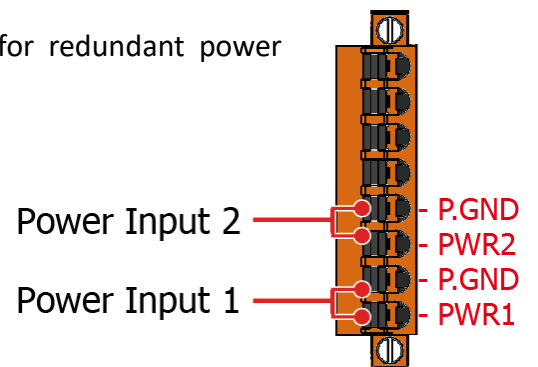
3. Hardware

3.1 Appearances

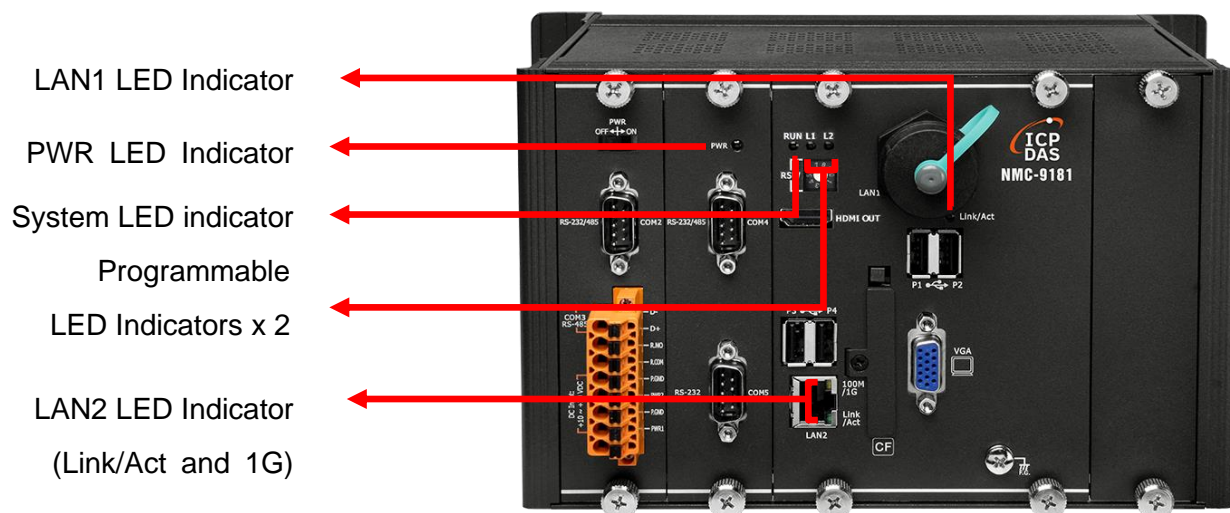


Redundant Power (PWR1 and PWR2)

The NMC-9181 has a terminal with 8-wire; there are 4-wire for redundant power inputs, the details of the redundant power are shown to the side.

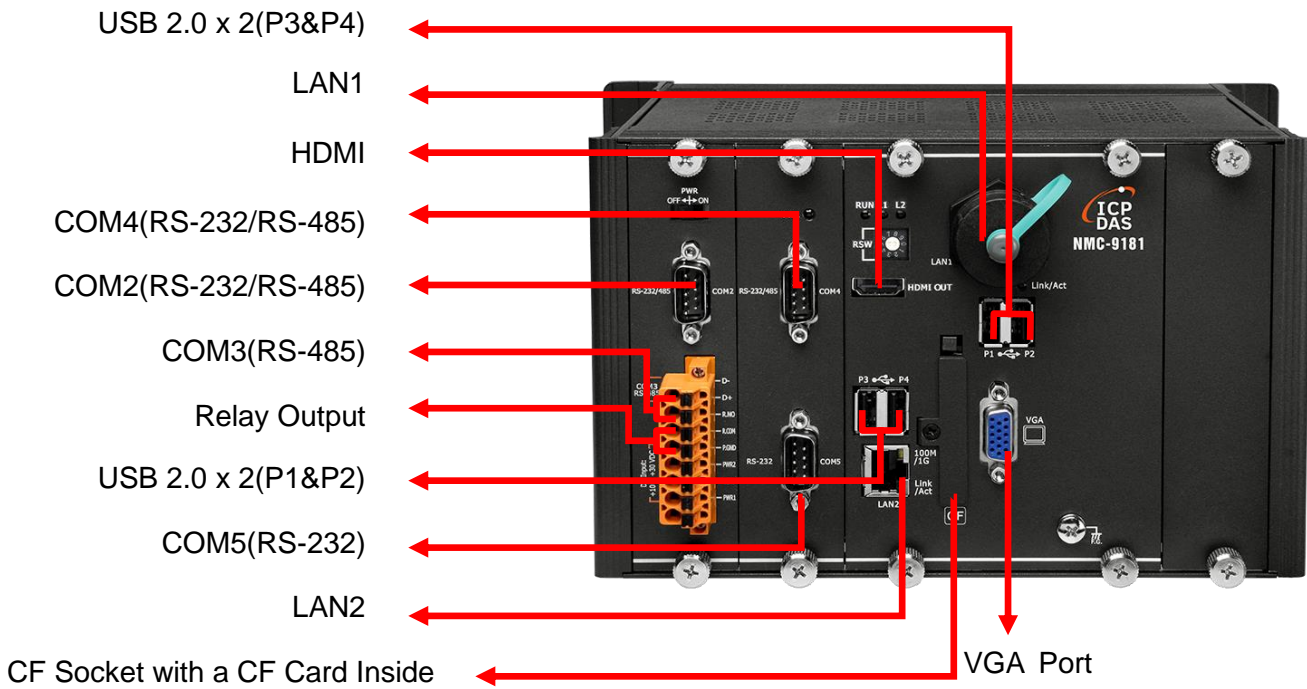


LED Indicators



LED Indicator	Label	State (Color)	Meaning
Programmable LED Indicators	L1 and L2	-	Programmable LED indicators
System LED indicator	RUN	Orange	OS is running
PWR LED Indicator	PWR	Green	Power is on
LAN1 LED indicator	Link/Act	Green	The Link is active
		Blinking	Network activity
LAN2 LED indicator	Link/Act	Green	The Link is active
		Blinking	Network activity
	1G	Orange	The network speed is 1 G

Communication Ports



● CF Socket with a CF Card Inside

The NMC-9181 comes with a CF card inside the CF socket. The CF card can be used to restore the NMC-9181 system and expand the memory up to 32 GB.

● LAN Ports, LAN1 and LAN2

The NMC-9181 has two Ethernet ports that can be used to connect the router to the Internet or to other devices.

● USB 2.0 Ports, P1, P2, P3 and P4

The NMC-9181 has four USB 2.0 ports that can be used to connect the USB devices such as mouse, keyboard or an external USB hard drive.

● VGA Port

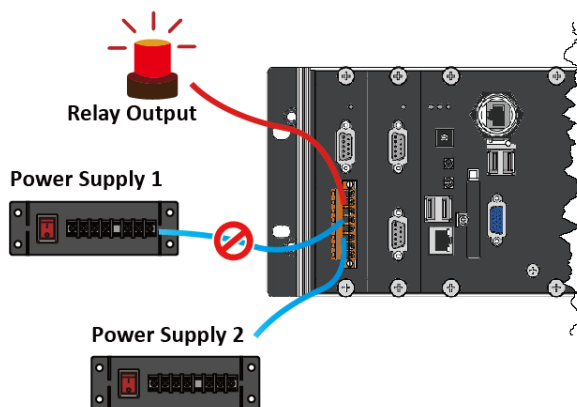
The NMC-9181 has a VGA port that can be used with a variety of supported VGA resolutions, and the output resolution covers, 640 x 480, 800 x 600, 1024 x 768.

● HDMI Port

NMC-9181 has an HDMI port that can be used to connect to a monitor and supports 2560 x 1600 @ 24bpp.

● Relay Output

The NMC-9181 has a relay output that can be used to control a light, siren, or other low voltage device when an alarm occurs.



● COM2 (RS-232/RS-485)

The COM2 port is a 9-pins RS-232/RS-485 connector that can be configured as either RS-232 or RS-485, that only can select one at a time and its configuration depends on the pin connections as follows:

RS-232 (RXD, TXD and GND)

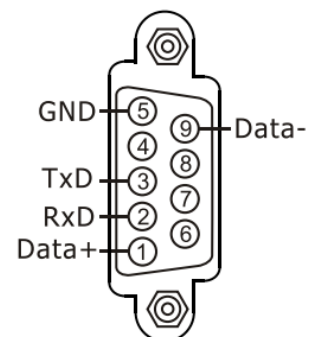
RS-485 (Data+ and Data-)

There is no software configuration or hardware jumper needed.

The details of the COM2 port specifications are shown to the side.

Warning: The LibreNMS software function does not support this hardware interface.

Note: 16C550 compatible



Port Type: Male

Baud Rate: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200 bps

Data Bits: 5, 6, 7, 8

Parity: None, Even, Odd, Mark (Always 1), Space (Always 0)

Stop Bits: 1, 2

FIFO: 64 bytes

● COM3 (2-wire RS-485)

Note: 16C550 compatible

Port Type: Terminals

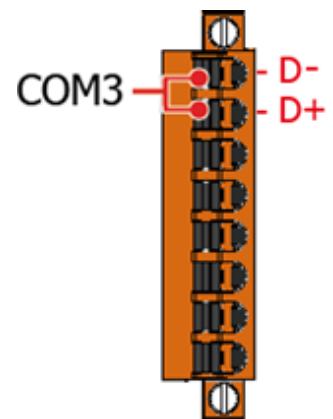
Baud Rate: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200 bps

Data Bits: 5, 6, 7, 8

Parity: None, Even, Odd, Mark (Always 1), Space (Always 0)

Stop Bits: 1, 2

FIFO: 128 bytes



Warning: The LibreNMS software function does not support this hardware interface.

● COM4 (RS-232/RS-485)

The COM4 port is a 9-pins RS-232/RS-485 connector that can be configured as either RS-232 or RS-485, that only can select one at a time and its configuration depends on the pin connections as follows:

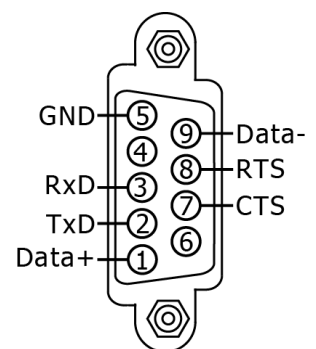
RS-232 (RXD, TXD, RTS, CTS and GND)

RS-485 (Data+ and Data-)

There is no software configuration or hardware jumper needed.

The details of the COM4 port specifications are shown to the side.

Note: 16C550 compatible



Port Type: Male

Baud Rate: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200 bps

Data Bits: 5, 6, 7, 8

Parity: None, Even, Odd, Mark (Always 1), Space (Always 0)

Stop Bits: 1, 2

FIFO: 128 bytes

Warning: The LibreNMS software function does not support this hardware interface.

● COM5 (RS-232)

The COM5 port is a 9-pins RS-232 connector. The details of the COM5 port specifications are shown to the side.

Note: 16C550 compatible

Port Type: Male

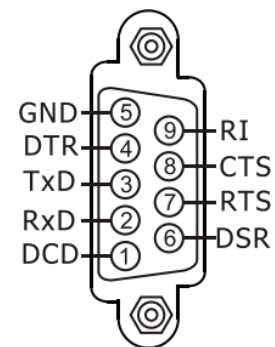
Baud Rate: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200 bps

Data Bits: 5, 6, 7, 8

Parity: None, Even, Odd, Mark (Always 1), Space (Always 0)

Stop Bits: 1, 2

FIFO: 128 bytes



Warning: The LibreNMS software function does not support this hardware interface.

Tips & Warnings

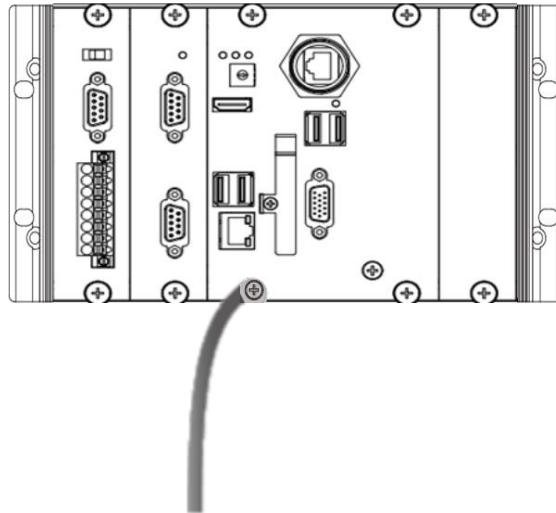


The table below shows the data bit and their corresponding stop bit for COM2, COM3, COM4 and COM5.

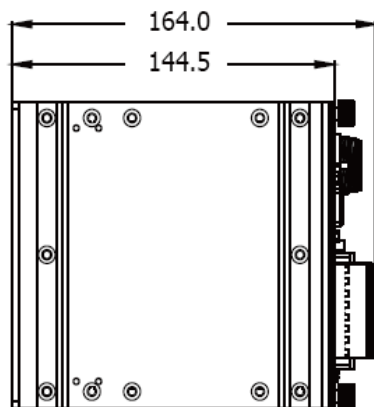
Word Length	Number of Stop Bits
5, 6, 7, 8	1
5	1.5
6, 7, 8	2

Frame Ground Point

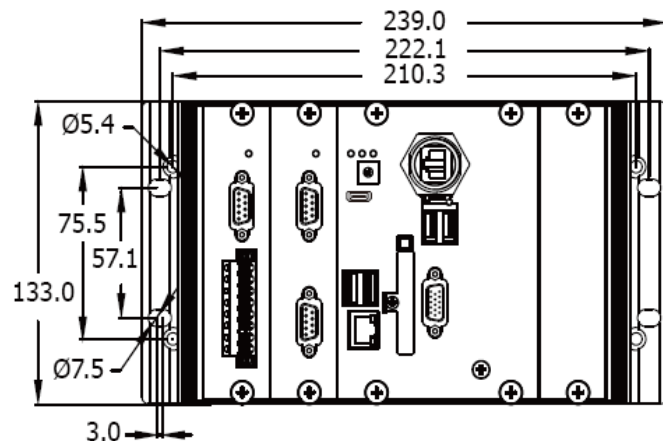
The frame ground point is a small piece of metal that can be used to terminate the shield.



3.2 Dimension



Left Side View

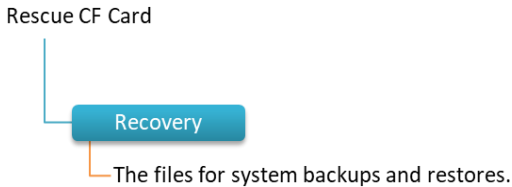


Front View

(Units: mm)

3.3 Rescue CF Card

The NMC-9181 comes with a rescue compact flash card that supports rescue mechanism for the NMC-9181.

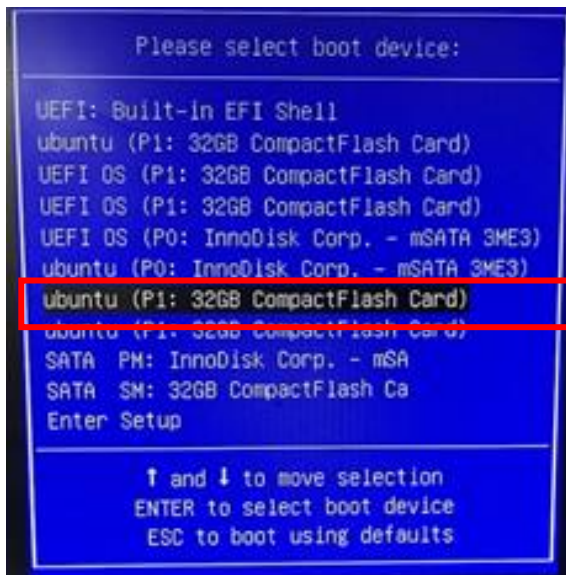


Restore NMC-9181 system

When the firmware file and the system are damaged, you can refill the system with a cf card.

Step 1: NMC-9181 reboots, powers on and enters the BIOS interface.

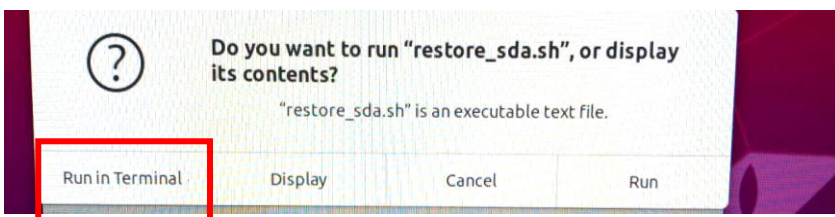
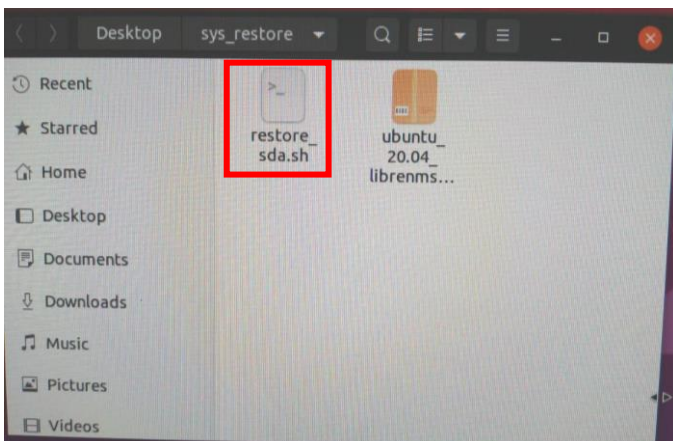
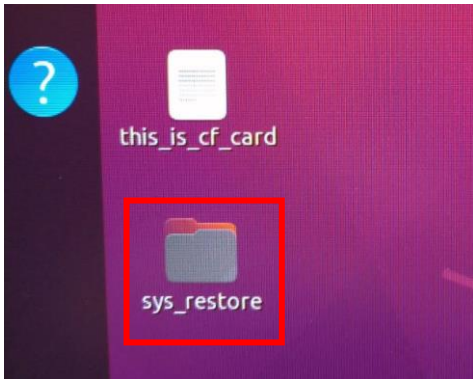
Step 2: After booting, press F7 on the BIOS boot screen. After the startup option appears, move to the [Ubuntu (P1: 32GB CompactFlash Card)] option, and press Enter to enter



Note:

Login [icpdas] and the default password is [icpdas].

Step 3: After rebooting, there is a [sys_restore] folder on the desktop screen, double click into it and then click [restore_sda.sh] to run.

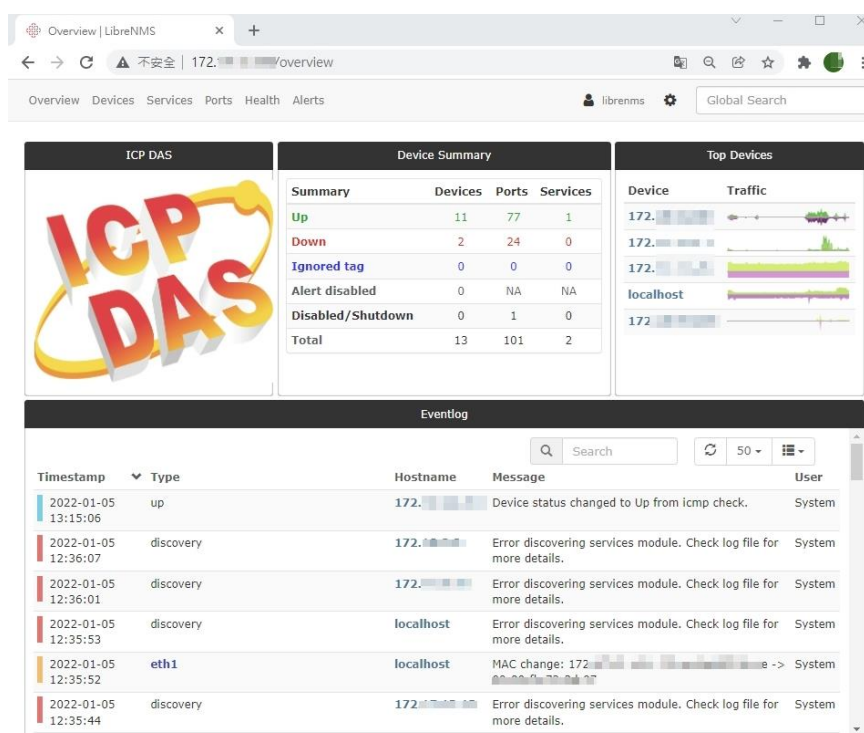


Note :

Please note that the loading process takes a long time, please do not turn off the power during this process.

4. LibreNMS

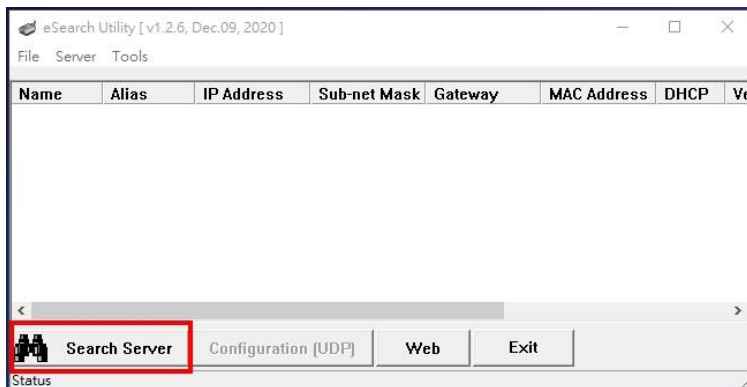
The LibreNMS is an auto-discovering network monitoring platform supporting a wide range of hardware platforms and operating systems including Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, F5, Brocade, Citrix Netscaler, NetApp and many more. Please refer to the following link for details.



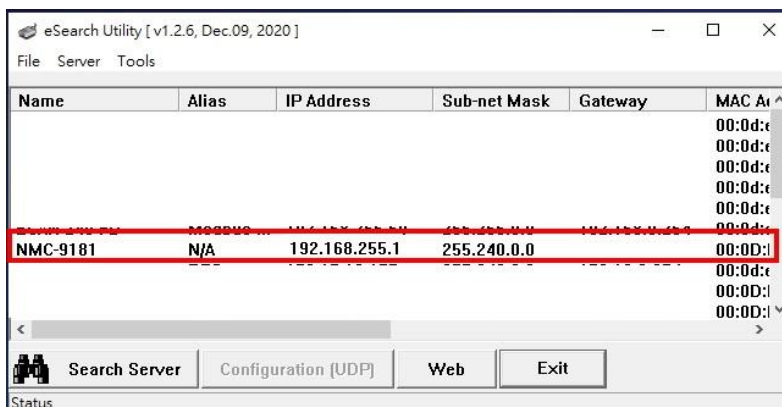
4.1 How to connect to LibreNMS

4.1.1 Use the eSearch Utility

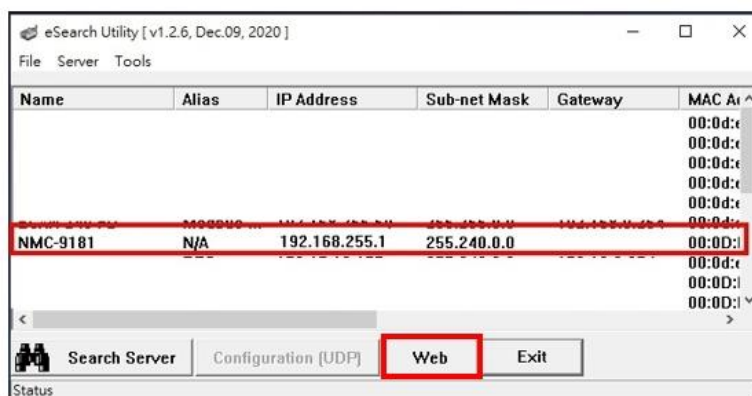
Step 1: Searching the ethernet device connected on the network



Step 2: Select NMC-9181



Step 3: Connect to the web pages.

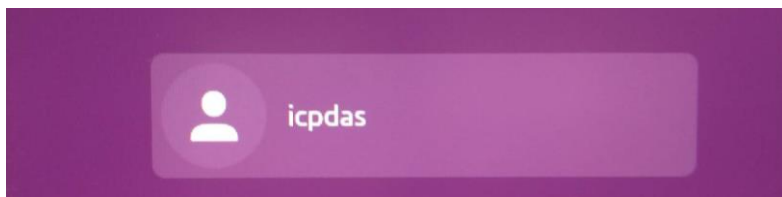


Step 4: The default login name is [**librenms**], password is [**D32fwefwef**].

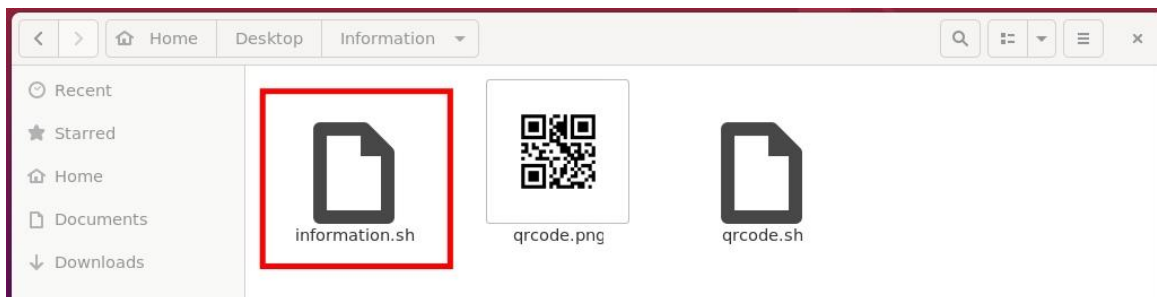


4.1.2 Connect to LibreNMS from Ubuntu operation

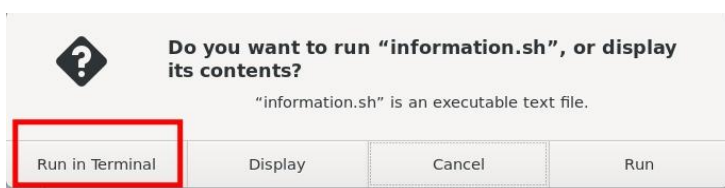
Step 1: Login [**icpdas**] and the default password is [**icpdas**].



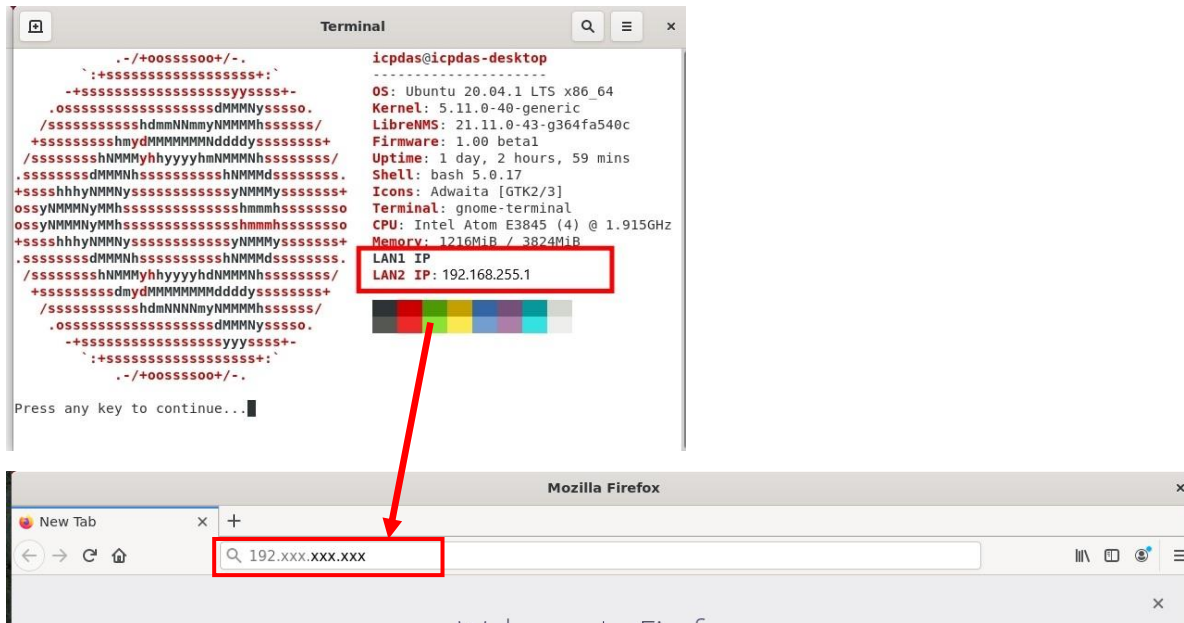
Step 2: Into the [Desktop/Information], Select [Information.sh]



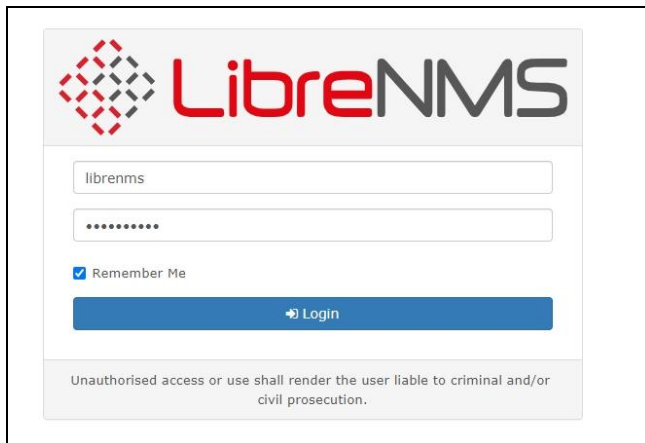
Step 3: Select [Run in Terminal]



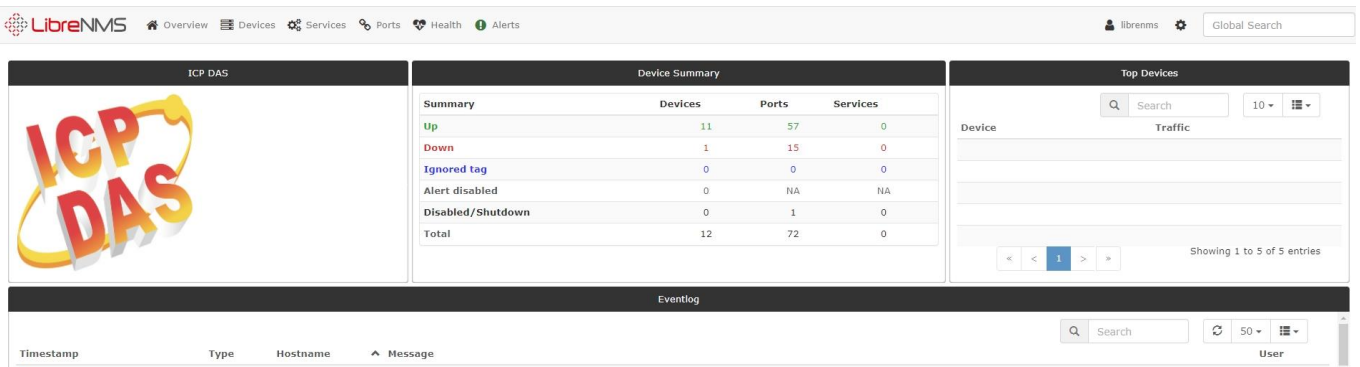
Step 4: Copy [LAN1 IP] or [LAN2 IP] to the web page



Step 5: The default login name is [librenms], password is [D32fwefwef].



4.2 Web Interface



4.2 Web home page

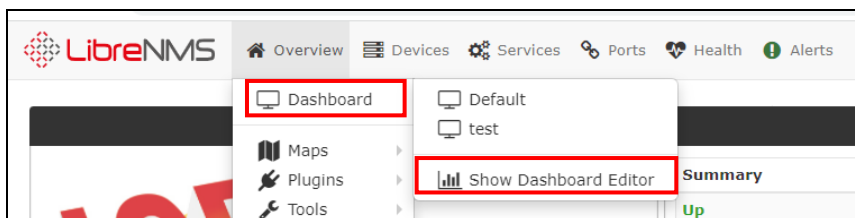
4.2.1 Overview

(1) Dashboard

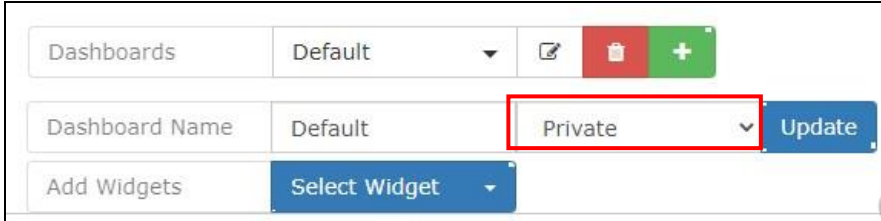
Create customised dashboards in LibreNMS per user. You can share dashboards with other users. You can also make a custom dashboard and default it for all users in LibreNMS.






Setting a global default dashboard

Step 1: Then go to Overview → [Dashboard] → [Show Dashboard Editor] and set the global default dashboard.




Step 2: Set the dashboard permissions to either [shared read] 、 [shared] or [Private], depending on what you want the users access to change. The following is an example.








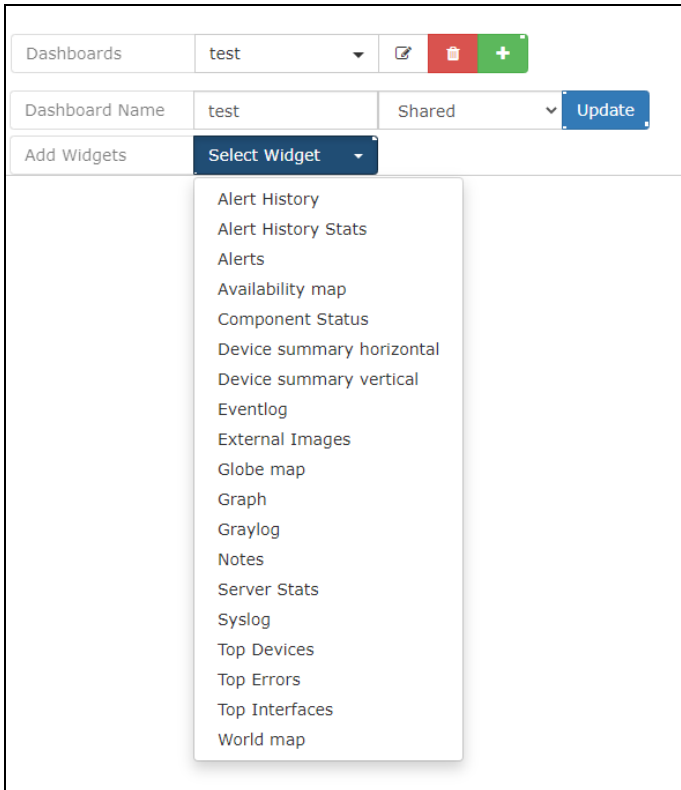
Dashboards	Default	  
Dashboard Name	Default	Private 
Add Widgets	Select Widget 	

- **Private** : Sets the dashboard to only the user that created the dashboard can view and edit.
- **Shared Read** : Sets the dashboard to allow other users to view the dashboard, but cant make changes to the dashboard.
- **Shared** : Allows all users to view the dashboard and make changes.

Step 3: LibreNMS has a whole list of Widgets to select from, Users can choose which widgets they want to add. Please refer to the following instructions.



Dashboards	Default	  
Dashboard Name	Default	Private 
Add Widgets	Select Widget 	

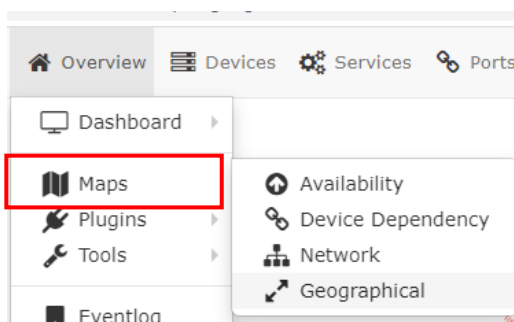


- **Alerts Widget** : Displays all alert notifications.
- **Availability Map** : Displays all devices with colored tiles, green up, yellow for warning (device has been restarted in last 24 hours), red for down. You can also list all services and ignored/disabled devices in this widget.
- **Components Status** : List all components Ok state, Warning state, Critical state.
- **Device Summary horizontal** : List device totals, up, down, ignored, disabled. Same for ports and services.
- **Device Summary vertical** : List device totals, up, down, ignored, disabled. Same for ports and services.
- **Eventlog** : Displays all events with your devices and LibreNMS.
- **External Image**: can be used to show external images on your dashboard. Or images from inside LibreNMS.
- **Globe Map** : Will display map of the globe.
- **Graph** : Can be used to display graphs from devices.

- **Graylog** : Displays all Graylog's syslog entries.
- **Notes** : Use for html tags, embed links and external web pages. Or just notes in general.
- **Server Stats** : Will display gauges for CPU, Memory, Storage usage. Note the device type has to be listed as "Server".
- **Syslog** : Displays all syslog entries.
- **Top Devices** : By Traffic, or Uptime, or Response time, or Poller Duration, or Processor load, or Memory Usage, or Storage Usage.
- **Top Interfaces** : Lists top interfaces by traffic utilization.
- **World Map** : displays all your devices locations. From syslocation or from override sysLocation.

(2) Maps

A global map will be drawn from the information in the database, it is worth noting that this could lead to a large network map. Network maps for individual devices are available showing the relationship with other devices. Also you can Build Device Groups and those Device Groups can be drawn with Network Map..



- **Availability:** List available devices.
- **Device Dependency:** Provide a network map of a single device, showing the parent relationship with other devices.
- **Network:** Network maps for individual devices are available showing the relationship with other devices.
- **Geographical:** Geographical will mark your device location on the map.

(3) Plugins

A variety of extended functions are provided here. ICP DAS provides ICPDAS plugins to simplify user operations. The ICPDAS plugins function includes Network Scan, Firmware Update, The detailed setting operations are described below.


Network Scan

Search for devices in the same area network, set IP, Mask, Execution cycle, and then start automatic search

Step 1: Input your network segment, netmask and execution cycle.

Note:

For IP Address and Net Mask settings, please refer to the suggestions on the right.

Step 2: Click  and  to start automatic search.

Information

Display basic information of NMC-9181



The screenshot shows the 'Information' tab of the NMC-9181 web interface. The page has a header with 'Network Scan | Information | Firmware Update' and a 'Reboot' button. A red box highlights a table of system information.

OS:	Ubuntu 20.04.1 LTS
Kernel:	5.11.0-40-generic
LibrNMS:	21.11.0-43-g364fa540c
Firmware:	1.00 beta1
LAN 1:	
LAN 2:	192.168.255.1

Reboot

reboot system

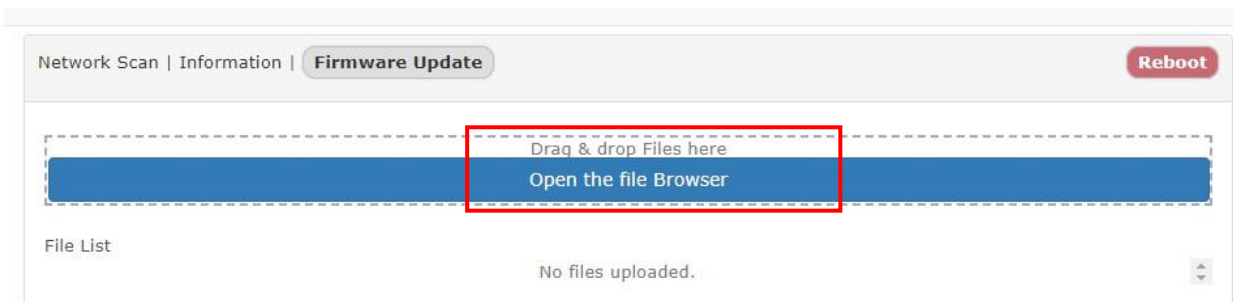


The screenshot shows the same 'Information' tab as above, but with a red box highlighting the 'Reboot' button in the top right corner of the header.

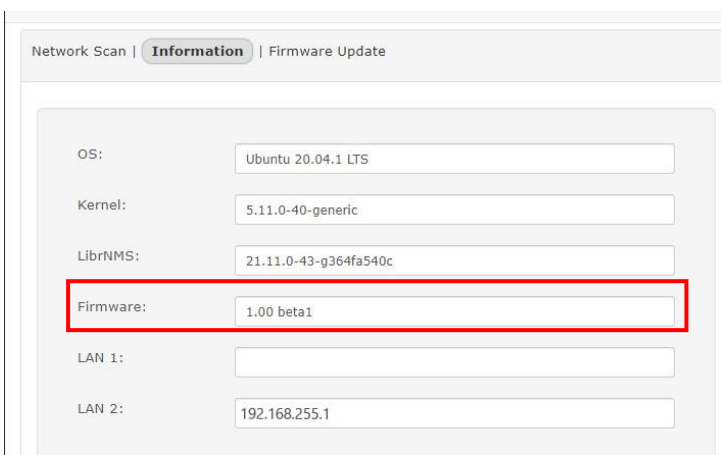
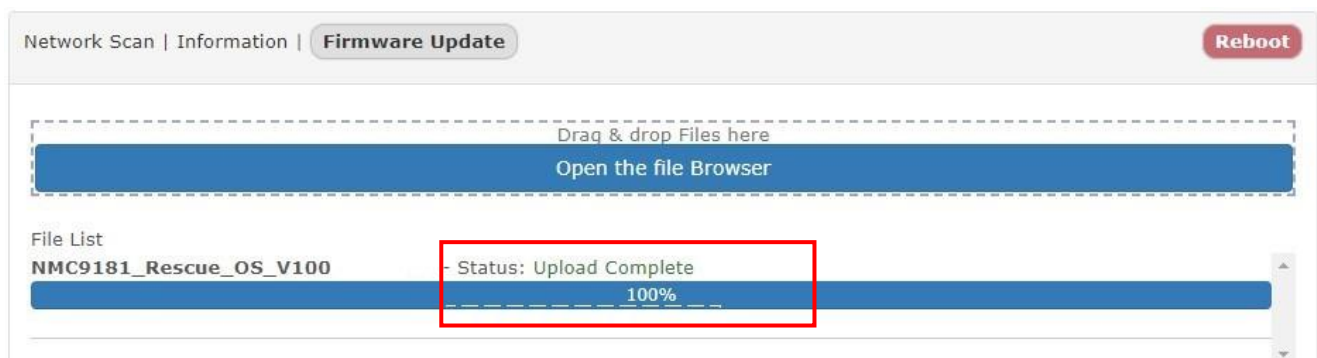
Firmware Update

Step 1: To icpdas.com search for [nmc-9181], click the [download center] to download the latest firmware

Step 2: Open the file Browser, you can select or drag files to update the firmware.



Step 3: Successful update will display [Upload Complete], you can go to the [information] to check whether the [firmware version] has changed.



(4) Tools

RIPE NCC API

RIPE NCC is responsible for the allocation and management of IP address resources throughout Europe. This API is provided by RIPE NCC

- **Abuse Contact Finder** : The Abuse Contact Finder may be able to help you find the email address that should be used to report network abuse originating from a particular IP address.

RIPE NCC API Tools

Abuse Contact Finder
 Whois

10745 Query

abuse@arin.net

- **Whois** : WHOIS is a transmission protocol used to query the IP and owner of domain names in the Internet. You can use netname, ip or ASN to query.

RIPE NCC API Tools

Abuse Contact Finder
 Whois

193.0.24.0 Query

```
inetnum = 193.0.24.0-193.0.30.255
netname = RIPENCC-MEETING-PUBLIC
descr = Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
remarks = RIPE NCC Training Services & RIPE Meetings
remarks = This space is used as public space during RIPE meetings
country = NL
admin-c = BRD-RIPE
tech-c = OPS4-RIPE
status = ASSIGNED PA
mnt-by = RIPE-NCC-MNT
mnt-routes = RIPE-NCC-MNT
mnt-domains = RIPE-NCC-MNT
created = 2013-10-09T14:42:14Z
last-modified = 2017-12-04T14:40:12Z
source = RIPE
```

(5) Eventlog

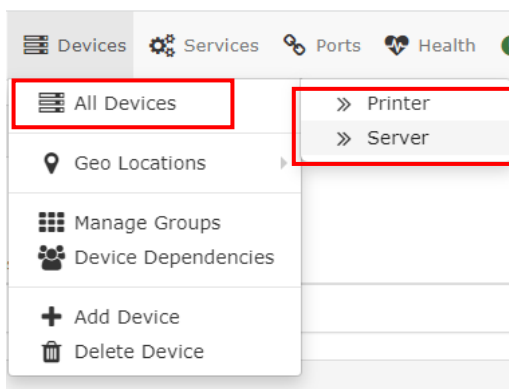
Detailed records will list all equipment changes and event handling information

Eventlog				
Device	All Devices ▾	Type	All Types ▾	Filter
		Q Search		↻ 50 ▾
Timestamp	Type	Hostname ^	Message	User
2021-11-25 15:27:02	system		Device 127.0.0.1 has been removed	librenms
2021-11-25 16:59:21	system		Device localhost has been removed	librenms
2021-11-26 10:30:57	system		Device 172.17.0.1 has been removed	librenms
2021-12-21 16:13:31	system		Device 172.17.0.1 has been removed	librenms
2021-12-22 14:55:02	service	localhost	Service " changed status from Unknown to Critical - -	System
2021-12-17 10:05:05	reboot	localhost	Device rebooted after 23 hours 37 minutes 5 seconds -> 40s	System
2021-12-17 10:05:08	eth0	localhost	ifOperStatus: up -> down	System
2021-12-17 10:05:08	eth0	localhost	ifSpeed: 1 Gbps -> 0 bps	System

4.2.2 Devices

(1) All Devices

There are two types of devices, Printer and Server, which can be selected to list different device information, graphs information and control the operation of the device.



- **Lists** : The list is divided into [Detail] and [Basic].

Lists: Basic | **Detail** | Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature
Agent Remove Search | Remove Header

Refresh 50 List Icon

Search All All OS All Versions All Platforms All Featuresets

All Locations Serverx **Search** Update URL Reset

S.	Id	M.	Vendor	Device	Metrics	Platform	Operating System	Up/Down Time	Location	Actions
5				172.507 controller	6		Microsoft Windows	21d 4h 40m 33s	Your Location Here	
6				172.pmc-5231	6		Microsoft Windows	46d 2h 57m 2s	Your Location Here	

Lists: **Basic** | Detail | Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature
Agent Remove Search | Remove Header

Refresh 50 List Icon

Search All All OS All Versions All Platforms All Featuresets All Locations

Serverx **Search** Update URL Reset

Status	Device	Platform	Operating System	Up/Down Time	Actions
	172.		Microsoft Windows	22d 2h 15m 36s	
	172.		Microsoft Windows	47d 32m 3s	

- **Graphs** : List the chart information of all devices by selection.

Lists: Basic | Detail | Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | **Poller** | Ping | Temperature

From Poller Perf Remove Search | Remove Header

To **Update**

- **Actions** : Can be operated and set the device.

Lists: Basic | **Detail** | Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature
Agent

Refresh 50 List

Search All All OS All Versions All Platforms All Featuresets

All Locations Serverx Search Update URL Reset

S.	Id	M.	Vendor	Device	Metrics	Platform	Operating System	Up/Down Time	Location	Actions
5			172.507	controler	6		Microsoft Windows	21d 4h 40m 33s	Your Location Here	
6			172.pmc-5231		6		Microsoft Windows	46d 2h 57m 2s	Your Location Here	
8			172.wise-5231		6		Microsoft Windows	30d 21h 52s	Your Location Here	

(2)Geo Locations

Sort by location, you can change the location and show the chart. The page is as below:

- **Actions** : Can change the location.

Locations

Search Refresh 25 List

Location	Coordinates	Devices	Network	Servers	Firewalls	Down	Actions
Your Location Here	N/A	6	0	6	0	0	
taiwan	N/A	1	0	1	0	0	
Rack, Room, Building, City, Country [Lat, Lon]	N/A	1	0	1	0	0	

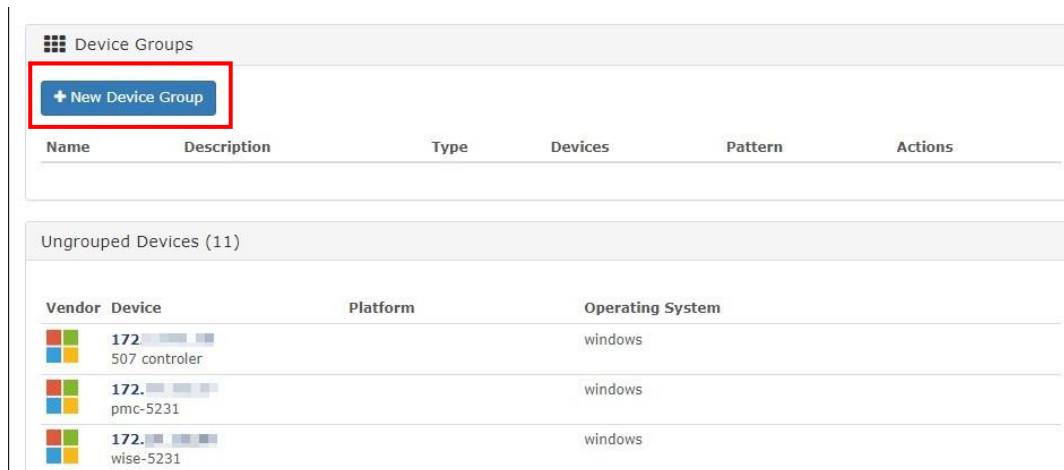
Showing 1 to 3 of 3 entries

(3)Manage Groups

Add New Device Group

Users can set and add device groups.

Step 1: Click [+New Device Group] button.



Step 2: Input the group name, description, type and device or rules. The detailed description is as follows.

Create Device Group

Name:

Description:

Type:

Define Rules: AND OR + Add rule + Add group Delete

Save Cancel

- **Type Static** : Select Devices.

Type Static

Select Devices localhost

● **Type Dynamic** : Set the rule

Define Rules

AND OR + Add rule + Add group

devices.type equal server Delete

devices.timeout
 devices.transport
devices.type
 devices.uptime
 devices.version
 devices_attribs.attrib_id

Step 3: Input Save button, if successfully added as shown below:

Device Groups

+ New Device Group

Name	Description	Type	Devices	Pattern	Actions
printer		Static	2		edit add delete

(4)Device Dependencies

Can manage the parent device of Device, after editing, it will be displayed in "Parent Device(s)".

Step 1: Select parent and child host, the default is "None".

Device Dependency for Multiple Devices
✕

Bulk Add Clear All

Here you can modify multiple device dependencies. Setting the parent device to "None" will clear the dependency.

Parent Host:

✕ localhost (icpdas-desktop)

Child Hosts:

✕ 172. [redacted] (507 controler)
✕ 172. [redacted] (pmc-5231)

✕ 172. [redacted] (icpdas main switch)

Cancel
Save


Step 2: Input Save button, if successfully added as shown below:

Id	Hostname	Parent Device(s)	Actions
	172. [redacted] 507 controler	localhost	✎ ✖

(5)Add Device

SNMP


Simple Network Management Protocol (SNMP) is an application layer protocol defined by the Internet Architecture Board (IAB) in RFC1157, which is used to exchange management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol combination.

Step 1: Input Hostname or IP address, and on the  SNMP button.

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname or IP

SNMP 


SNMP Version

Port Association Mode

SNMPv1/2c Configuration


Step 2: Input the SNMP Version, port and Communication protocols, Port Association Mode choose “ifIndex”.

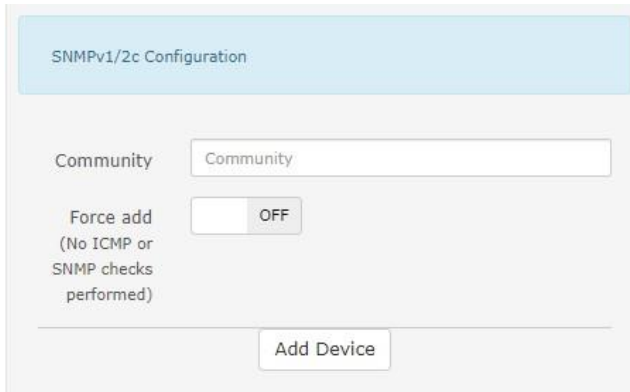
Hostname or IP

SNMP 

SNMP Version

Port Association Mode

Step 3: Fill in the following information according to the selected version, and then press the  button, all the added devices will be in the device list. After clicking [Devices] -> [All Devices] in the menu, you can view all the device objects in your control.



SNMPv1/2c Configuration

Community

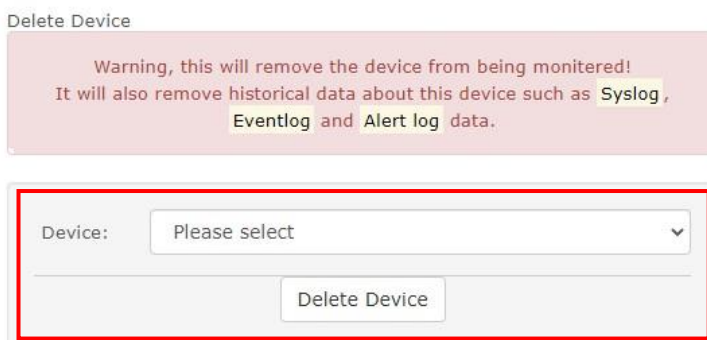
Force add
(No ICMP or
SNMP checks
performed) OFF

Note :

- If you “Force add” button choose “OFF”, will perform ICMP or SNMP check, whether the device supports ICMP or SNMP protocol
- If the check fails, please check whether the device is installed or enabled with SNMP.

(6)Delete Device

Step 1: Select the device to remove and click button.



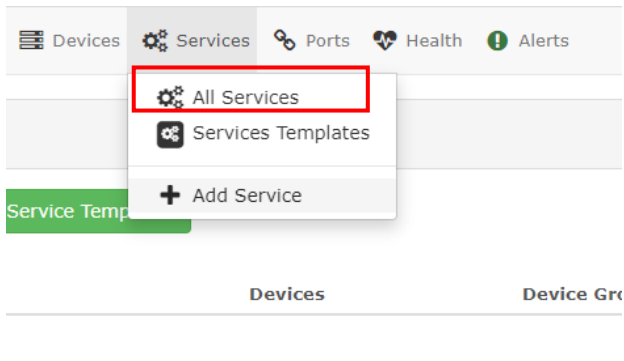
Delete Device

Warning, this will remove the device from being monitored!
It will also remove historical data about this device such as Syslog ,
Eventlog and Alert log data.

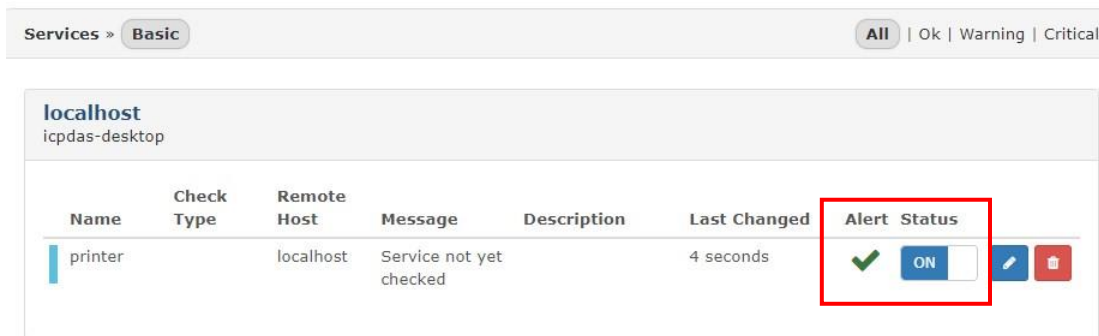
Device:

4.2.3 Services

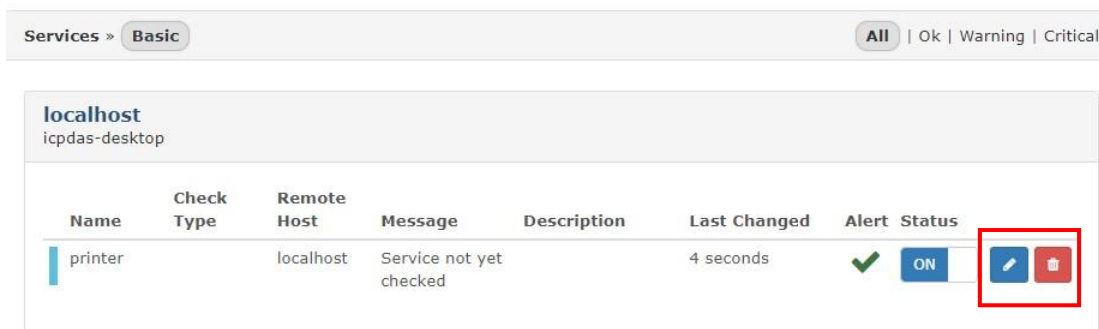
(1) All Services



- **Status :** You can turn off or turn on the alert.



- **Delete / Edit Service :** Service will modified for the specified Device.

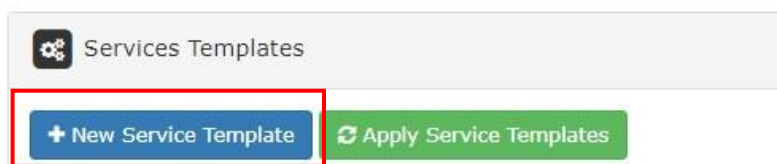


(2) Services Templates

Service Templates within LibreNMS provides the same ability as Nagios does with Host Groups. Known as Device Groups in LibreNMS. They are applied devices that belong to the specified Device Group.

Create Service Template

Step 1: Click  button.



Step 2: Fill in according to the field settings, the detailed settings are as follows.

Create Service Template

Service Template will created for the specified Device Group.

Name

Device Type

Select Devices

Device Groups

Check Type

Description

Remote Host

Parameters

Parameters may be required and will be different depending on the service check.

Ignore alert tag OFF





Disable polling and alerting OFF

- **Device Type:** Divided into static and dynamic two choices, and dynamic can customize the device rules.
- **Select Devices:** Service Template will created for the specified Device Group.
- **Device Groups:** Can select the created device group.
- **Check Type:** Choose to check services, such as http, tcp, snmp, etc.
- **Description:** It is recommended to add a description to facilitate user management.
- **Remote Host:** Monitor remote service via LibreNMS.
- **Ignore alert tag:** Enable to make the alert tag unavailable.

Step 3: Users can apply, edit, and delete Services Templates.





Services Templates

+ New Service Template Apply Service Templates

Name	Description	Devices	Device Groups	Device Type	Device Rules	Actions
Template_TEST	test	1	0	Static		   

localhost

Name	Check Type	Parameters	Remote Host	Description	Modified	Ignored	Disabled
Template_TEST	apt			test	2021-12-29 13:14:38	0	0

- Apply Services for this Service Template 
- Remove Services for this Service Template 
- Edit Service Template 
- Delete Service Template 

Step 4: After pressing apply , the content will appear in [all device]

172 
desktop-ptk4rog

Name	Check Type	Remote Host	Message	Description	Last Changed	Alert	Status
Template_TEST	apt		Usage: check_apt [[-d	test	1 minute 57 seconds		  

(3)Add Service

Step 1: Fill in according to the field settings and click  , the detailed settings are as follows.

Add Service

Service will created for the specified Device.

Name:

Device:

Check Type:

Description:

Remote Host:

Parameters:

Parameters may be required and will be different depending on the service check.

Ignore Alert Tag:

Disable Polling and Alerting:

- **Device:** Service will created for the specified Device.
- **Check Type:** Choose to check services, such as http, tcp, snmp, etc.
- **Remote Host:** Monitor remote service via LibreNMS.

Step 2: If successfully added as shown below:

✔ Device Settings Saved

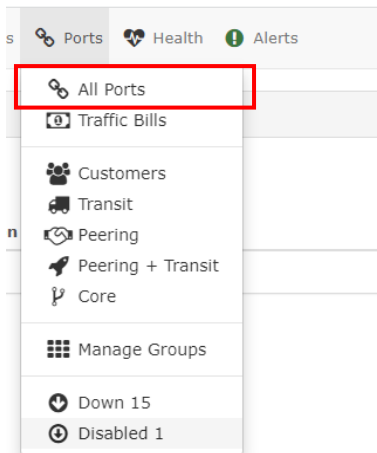
Note :

- Service Templates are tied into Device Groups, you need at least one Device Group to be able to add Service Templates - You can define a dummy one. The Device Group does not need members to add Service Templates.

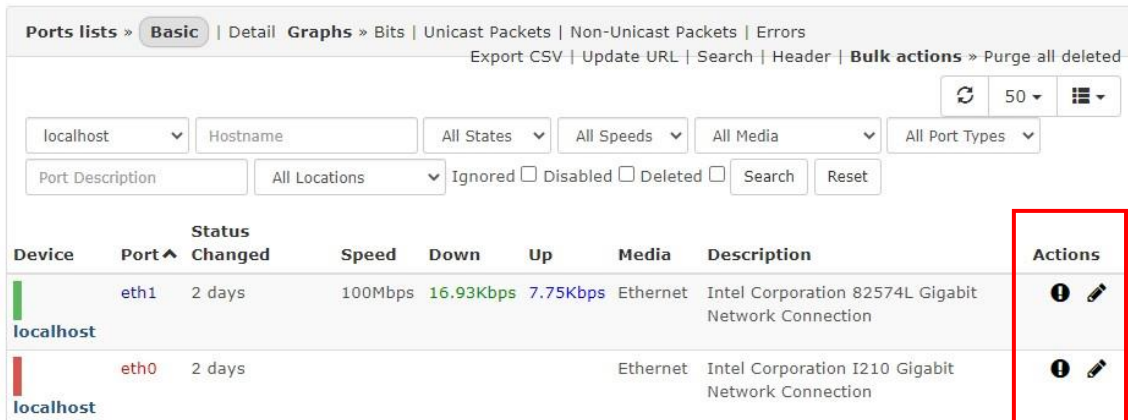
4.2.4 Ports

(1) All Ports





Get info for all ports on all devices and list all device ports information.



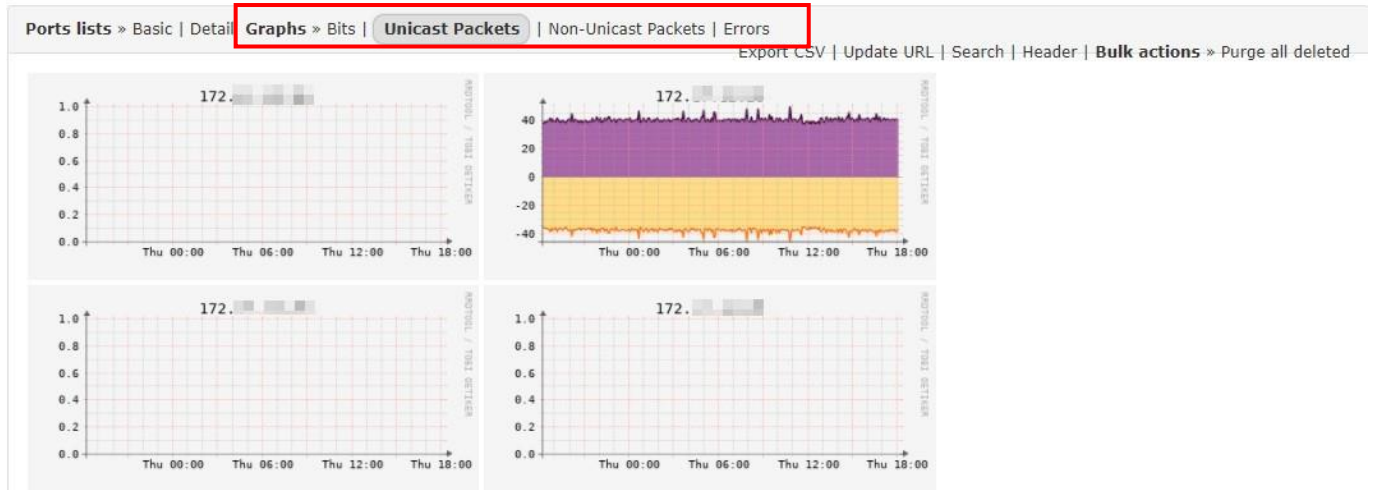
- **Actions :** You can “View alerts” and “Edit ports”.



A screenshot of the 'Ports lists' page in a web application. The page has a breadcrumb trail: 'Ports lists » Basic | Detail Graphs » Bits | Unicast Packets | Non-Unicast Packets | Errors'. Below the breadcrumb, there are filters for 'localhost', 'Hostname', 'All States', 'All Speeds', 'All Media', and 'All Port Types'. There are also checkboxes for 'Ignored', 'Disabled', and 'Deleted', along with 'Search' and 'Reset' buttons. The main content is a table with the following columns: 'Device', 'Port', 'Status Changed', 'Speed', 'Down', 'Up', 'Media', 'Description', and 'Actions'. The 'Actions' column is highlighted with a red rectangular box. The table contains two rows of data for 'localhost'.

Device	Port	Status Changed	Speed	Down	Up	Media	Description	Actions
localhost	eth1	2 days	100Mbps	16.93Kbps	7.75Kbps	Ethernet	Intel Corporation 82574L Gigabit Network Connection	 
localhost	eth0	2 days				Ethernet	Intel Corporation I210 Gigabit Network Connection	 

- **Graphs** : List the chart information of all devices by selection.



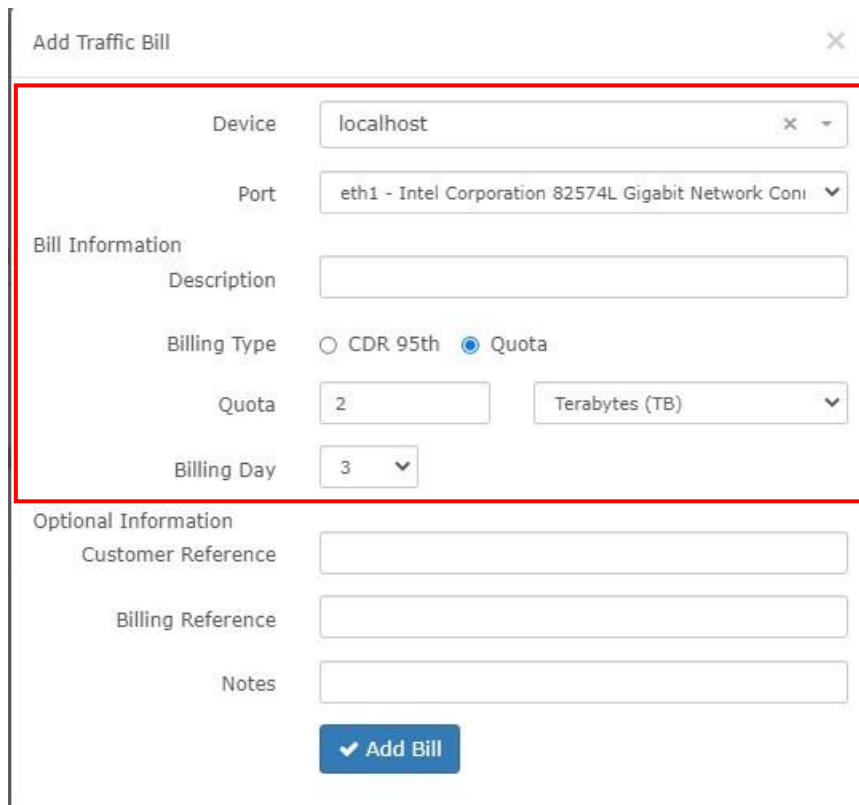
(2)Traffic Bills

Using the billing module, you can create traffic bills, assign quotas to them, and add ports to them. It then tracks port usage and shows you traffic usage in the bill, including any excesses.

Step 1: Click  button.

Billing name	Type	Allowed	Inbound	Outbound	Total	95th Percentile	Overusage	Predicted
2021-12-02 to 2022-01-	Quota	500 GB	29.57 MB	72.93 MB	102.5 MB	25.93 Kbps	-	139.78 MB

Step 2: Fill in according to the field settings and click  button, the detailed settings are as follows.



Add Traffic Bill

Device localhost

Port eth1 - Intel Corporation 82574L Gigabit Network Coni

Bill Information

Description

Billing Type CDR 95th Quota

Quota 2 Terabytes (TB)


Billing Day 3

Optional Information

Customer Reference

Billing Reference

Notes



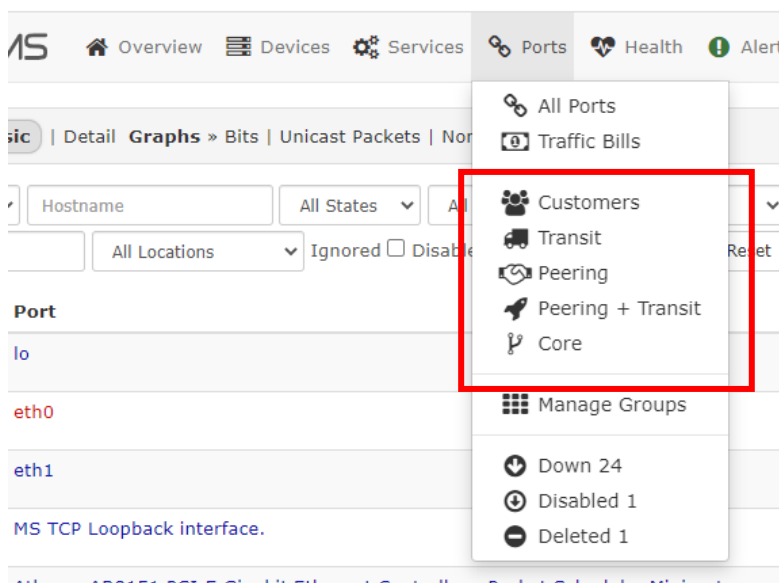
- **Device:** You have to select the device where the port is located
- **Port:** The port you actually want to have billed. You can always change that later or even add multiple ports into one bill.
- **Billing Type “Quota”:** just looks at the total traffic used by the port
- **Biling Type “CDR 95th”:** “CDR 95th” looks at the 95% average (to put it simple), which will monitor the total bandwidth used, throw away the top 5% and then calculate the average for the remaining “low”-95%.
- **Billing Day:** The billing day is the day of the month at which the current billing-period starts and ends.

(3)Interface Description Parsing

Librenms can interpret, display and group certain additional information on ports. This is done based on the format that the port description is written although it's possible to customise the parser to be specific for your setup.

Interface description tags are divided into Customers, Transit, Peering, Peering+Transit, Core.

This function will automatically search your device for keywords, and you can search for the device in the corresponding category.



Note:

- For relevant examples of keywords, please refer to the following links.

<https://docs.librenms.org/Extensions/Interface-Description-Parsing/>

(4)Manage Groups

Step 1: Click  button.



Port Groups

+ New Port Group

Name	Description	Ports	Actions
------	-------------	-------	---------

Step 2: Input group name, description and Click “Save” button.

Create Port Group

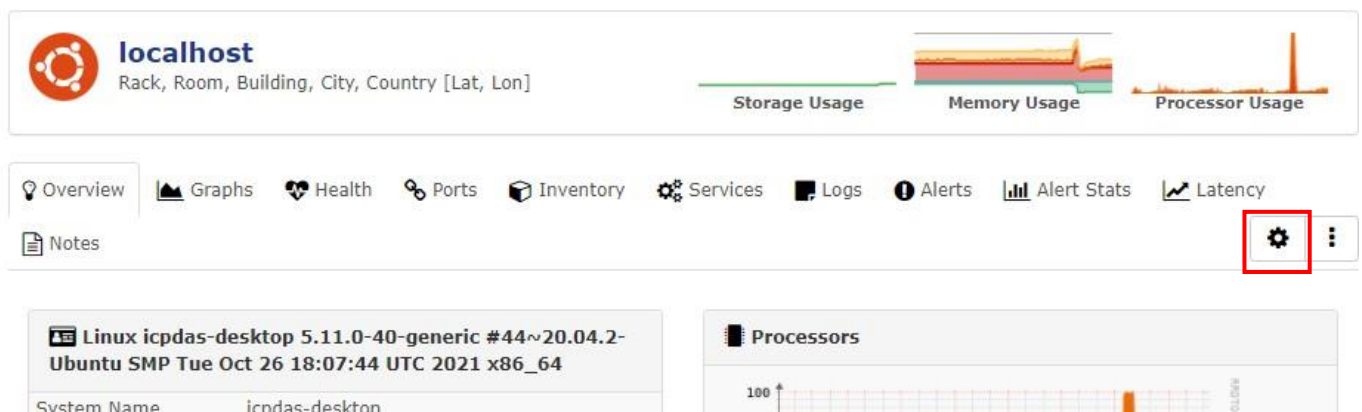


Name

Description

Save **Cancel**


Step 3: Go to the device interface you want to configure, click  button



localhost
Rack, Room, Building, City, Country [Lat, Lon]

Storage Usage Memory Usage Processor Usage

Overview Graphs Health Ports Inventory Services Logs Alerts Alert Stats Latency

Notes 

Linux icpdas-desktop 5.11.0-40-generic #44~20.04.2-Ubuntu SMP Tue Oct 26 18:07:44 UTC 2021 x86_64

System Name icpdas-desktop

Processors

100

Step 4: To [Port Settings] > [Port Group] input [group name]

Index	Name	Admin	Operational	Disable polling	Ignore alert tag	ifSpeed (bits/s)	Port Group	RRD Time	Description
1	lo	up	up	OFF	OFF	10000000	x my_test	OFF	lo
2	eth0	up	down	OFF	OFF	0	No Group	OFF	Intel Corporation I210 Gig
3	eth1	up	up	OFF	OFF	100000000	No Group	OFF	Intel Corporation 82574L

4.2.5 Health

“Health” provides various indicators about how the device is performing in terms of hardware - if this information is available - such as temperature, voltage, fan speed, etc... Notice that some of this information is already shown in the overview page for the device (which you get when you click on the name of the device).

Used	Count
1.58 GiB / 3.73 GiB	2
3.04 GiB / 5.73 GiB	
299.43 MiB / 3.73 GiB	3
1.16 GiB / 3.73 GiB	2

- **Memory:** Display memory types, charts and usage status of all devices.

Device	Memory	Used	Usage
localhost	Physical memory	1.6 GiB / 3.73 GiB	2.13 GiB 43%
localhost	Virtual memory	3.21 GiB / 5.73 GiB	2.53 GiB 56%

- **Processor:** Display processor types, diagrams and usage status of all devices.

Device	Processor	Usage
localhost	Intel Atom E3845 @ 1.91GHz	5% 95%
localhost	Intel Atom E3845 @ 1.91GHz	5% 95%

- **Storage:** Display all device storage locations, charts and usage status.

Device	Storage	Used	Usage
localhost	/run	1.91 MiB / 382.41 MiB	380.5 MiB 1%
localhost	/	9.7 GiB / 57.95 GiB	48.25 GiB 17%

- **Temperature:** Display the maximum and minimum values and current values of Temperature Sensors, graphs, and temperatures of all devices

Device	Sensor	Current	Low Limit	High Limit
localhost	acpitz-acpi-0:temp1	26.8 °C	16.8 °C	46.8 °C
localhost	Core 0	59 °C	48 °C	78 °C




- **Count:** Display counters, graphs, maximum and minimum counts and current values of all devices

Device	Sensor	Current	Low Limit	High Limit
172	Impressions since powered on	222	-	-
172	Life time impressions	88.13 K	-	-
172	Impressions since powered on	0	-	-
172	Life time impressions	28.88 K	-	-

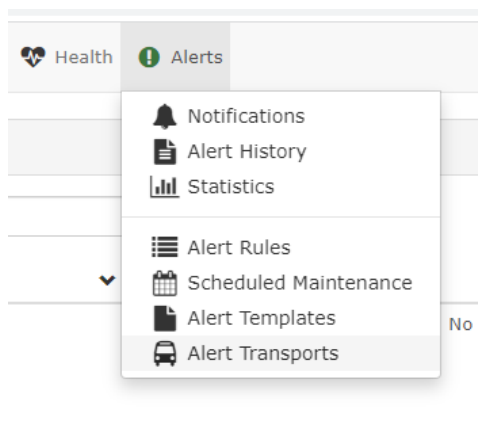
- **State:** Display the printer state, chart, and current state of the Sensor for all devices.

Device	Sensor	Current	Low Limit	High Limit
172.17.0.1	Printer Device Status	 Running	-	-
172.17.0.1	Printer Error Status	 Normal	-	-
172.17.0.2	Printer Device Status	 Running	-	-
172.17.0.2	Printer Error Status	 Normal	-	-

- **Toner:** Display toner types, diagrams and usage conditions of all printer devices.

Device	Toner	Type	Used	Usage
172.17.0.1	Black Cartridge HP CE255X	Toner Cartridge	 51%	51%
172.17.0.1	TRAY 1	Input	 0%	0%
172.17.0.1	TRAY 2	Input	 50%	50%

4.2.6 Alerts



(1) How to setting alert transports and rule

Step 1: To [Global Setting] > [Alerting] > [Email Options] > setting send mail, detailed description and

examples are shown below

gmail configuration example

SMTP host	smtp.gmail.com
SMTP port number	465
SMTP security mode	SSL/TLS
SMTP authentication	yes
SMTP account	[your gmail account]
SMTP password	[google application password]

- **From email address:** your mail
- **How to deliver mail:**SMTP
- **SMTP Server:** smtp.gmail.com(for gmail) or other
- **SMTP port setting:**The default is 25,if use gmail the port is "465".
- **SMTP timeout setting:**The default is 10
- **Encryption:** Encryption is the process of disguising the content of your email messages to protect them from being read by unwanted parties, the default is disabled.
- **Auto TLS support:** The default is disabled
- **SMTP authentication:** Please select enable, and enter your email account and password.

Step 2: To [Alerts] > [Alert Transports] > [Create alert transport], detailed description and examples are shown below

Alert Transport :: Docs ×

Transport name:

Transport type:

Default Alert: OFF

Email:

[Save Transport](#)

- **Transport Type:** The object to which the alert will be sent, please select mail or other
- **Email:** Please enter the email account (receiving).

Step 3: To [Alerts] > [Alert Rules] > click [Create rule from collection] or [Creat new alert rule], it is recommended to select [Alert rule collection], select the desired rule, and then change the setting value

[Create new alert rule](#) - OR - [Create rule from collection](#)

50 ▼

Type	Name	Devices	Transports	Extra	Rule	Severity	Status	Enabled	Action
+ Click here to create the default alert rules!									

Alert rule collection ×

10 ▼
☰ ▼

Name	Rule	
Devices up/down	macros.device_down = "1"	Select
Device Down! Due to no ICMP response.	macros.device_down = "1" && devices.status_reason = "icmp"	Select
SNMP not responding on Device - Check on SNMP Service - Device marked Down!	macros.device_down = "1" && devices.status_reason = "snmp"	Select

Step 4: Modify or add rule settings, detailed description and examples are shown below.

Alert Rule :: Docs

Main Advanced

Rule name: Devices up/down

Import from

AND OR + Add rule + Add group

macros.device_down equal No Yes Delete

Severity: Critical

Max alerts: 1 Delay: 1m Interval: 5m

Mute alerts: OFF Invert rule match: OFF

Recovery alerts: ON

Match devices, groups and locations list: Devices, Groups or Locati All devices except in list: OFF

Transports: Transport/Group Name

Procedure URL:

Save Rule

- **Rule name:** The description of this alert rule.
- **Severity:** How to display the alert. OK: green, Warning: yellow , Critical: red.
- **Max alerts:** How many notifications to issue while active before stopping. -1 means no limit . If interval is 0, this has no effect.
- **Delay:** How long to wait before issuing a notification. If the alert clears before the delay, no notification will be issued. (s, m, h, d)
- **Interval:** How often to re-issue notifications while this alert is active. 0 means notify once. This is affected by the poller interval. (s, m, h, d)
- **Invert rule match:** Alert when this rule doesn't match.
- **Recovery alerts:** Issue recovery notifications
- **All devices except in list:** If ON, alert rule check will run on all devices except the selected devices and groups.
- **Transports:** Restricts this alert rule to specified transports.
- **Procedure URL:** a link to some documentation on how to handle this alert. This will be included in notifications.

Step 5: After adding, it will be displayed in [Alert Rules], and you can turn on or off the alert rules at any time

Create new alert rule - OR - Create rule from collection 50 ▾

Type	Name	Devices	Transports	Extra	Rule	Severity	Status	Enabled	Action
	Devices up/down	taiwan	alert_test	Max: 1 Delay: 60 Interval: 300	macros.device_down = 1	Critical		<input checked="" type="checkbox"/>	

Step 6: You can go to [Alerts]> [Alert Transports] to test sending an alert send.

Transport Name	Transport Type	Default	Details	Action
alert_test	Mail	No	Email: account@gmail.com	

Note:

- If an error message pops up from the test sending an alert, please reconfirm whether the content of the above steps is filled in correctly.

(2) Notifications

The user will be notified of the device whose alarm status is [active], and the rule and time point will be listed. The user can view the action and take notes.

Alerts						
<input type="text" value="Search"/> 50 ▾ 						
Timestamp	Rule	Hostname	Location	ACK	Notes	Details
	2021-12-27 12:05:06	Devices up/down	172			
<pre>#1: last_polled => '2021-12-27 12:00:08' last_polled_timetaken => '3.07' last_discovered_timetaken => '4.33' last_discovered => '2021-12-24 18:37:11' last_ping_timetaken => '0.6'</pre>						

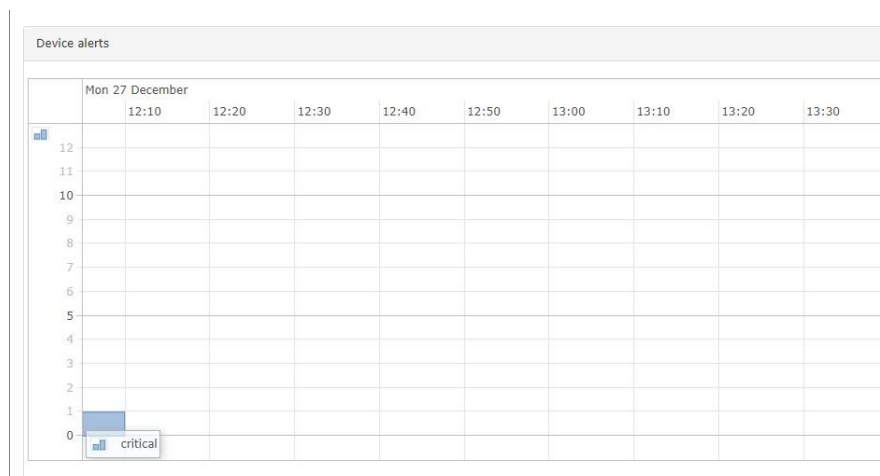
(3) Alert History

You can view the history of alerts as follows. Red statue: active, Green statue: recovered.

	2021-12-27 13:40:08	localhost	Devices up/down	critical
	2021-12-27 13:40:08	172.17.0.1	Devices up/down	critical
	2021-12-27 13:40:08	172.17.0.2	Devices up/down	critical
	2021-12-27 13:25:08	172.17.0.1	Devices up/down	critical
	2021-12-27 12:05:06	172.17.0.1	Devices up/down	critical
	2021-12-27 11:50:20	172.17.0.1	Devices up/down	critical
	2021-12-27 11:50:20	172.17.0.2	Devices up/down	critical
	2021-12-27 11:50:18	172.17.0.1	Devices up/down	critical
	2021-12-27 11:50:16	172.17.0.2	Devices up/down	critical

(4) Statistics

This function will unify the alarm data and plot it into a chart.



(5) Scheduled Maintenance

Provide users to set and schedule maintenance time.

Create Schedule
✕

Title *:

Notes:

Recurring *: No

Start *:

End *:

Map To *:

Schedule maintenance

Schedule maintenance

↻ 50 ▾
☰ ▾

Title	Recurring	Start (no recurring)	End (no recurring)	Start recurring dt	End recurring dt	Start recurring hr	End recurring hr	Recurring on days	Actions	Status
test	No	2021-12-27 14:01	2021-12-27 15:01						✎ 🗑	Current

« < 1 > »

Showing 1 to 1 of 1 entries

(6) Alert Templates

This feature allows users to define their own alarm templates if the generally provided example alarm rules do not meet their needs.

Create new alert template

↻ 50 ▾
☰ ▾

#	Name	Alert Rules	Action
1	BGP Sessions.		✎ 🗑
0	Default Alert Template	Devices up/down	✎ 🗑
2	Ports		✎ 🗑
3	Temperature		✎ 🗑

Alert Template :: Docs ✕

Template name:

Template:

```

{{ $alert->title }}
Severity: {{ $alert->severity }}
@if ($alert->state == 0) Time elapsed: {{ $alert->elapsed }} @endif
Timestamp: {{ $alert->timestamp }}
Unique-ID: {{ $alert->uid }}
Rule: @if ($alert->name) {{ $alert->name }} @else {{ $alert->rule }} @endif
@if ($alert->faults) Faults:
@foreach ($alert->faults as $key => $value)
  #{{ $key }}: {{ $value['string'] }}
@endforeach
@endif
Alert sent to:
@foreach ($alert->contacts as $key => $value)
  {{ $value }} <{{ $key }}>
@endforeach

```

Attach template to rules:

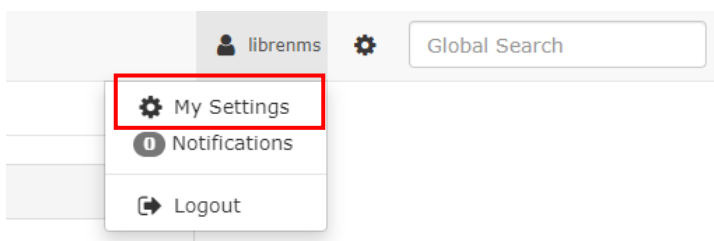
Alert title:

Recovery title:

[Update template](#)

4.2.7 User settings

The user can change the password and preferences.



Change Password

User Preferences

Push Notifications

To enable browser notifications, there must be an alert transport referencing this user

Change Password

Current Password	<input type="password"/>
New Password	<input type="password"/>
Verify New Password	<input type="password"/>
<input type="button" value="Change Password"/>	

Preferences

Preferences

Dashboard	<input type="text" value="librenms:Default"/>	▼
CSS Style	<input type="text" value="Default (Light)"/>	▼
Language	<input type="text" value="Default (English)"/>	▼
Add schedule notes to devices notes		<input type="checkbox"/> OFF

* Translation not fully supported

Note:

- Translation not fully supported.

Two-Factor Authentication

Two-factor authentication is an extra layer of security designed to ensure that you are the only person who can access your account, even if someone knows your password.

Preferences

Dashboard: librenms:Default

CSS Style: Default (Light)

Language: Default (English) * Translation not fully supported

Add schedule notes to devices notes: OFF

Two-Factor Authentication

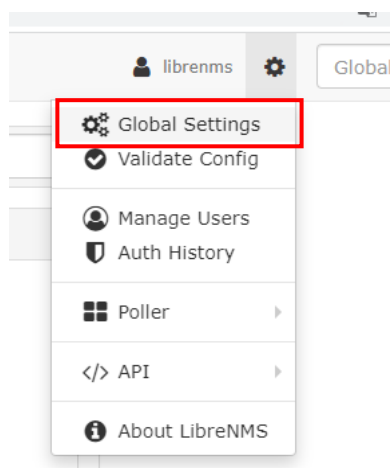
TwoFactor Type: Time Based (TOTP)

Generate TwoFactor Secret Key

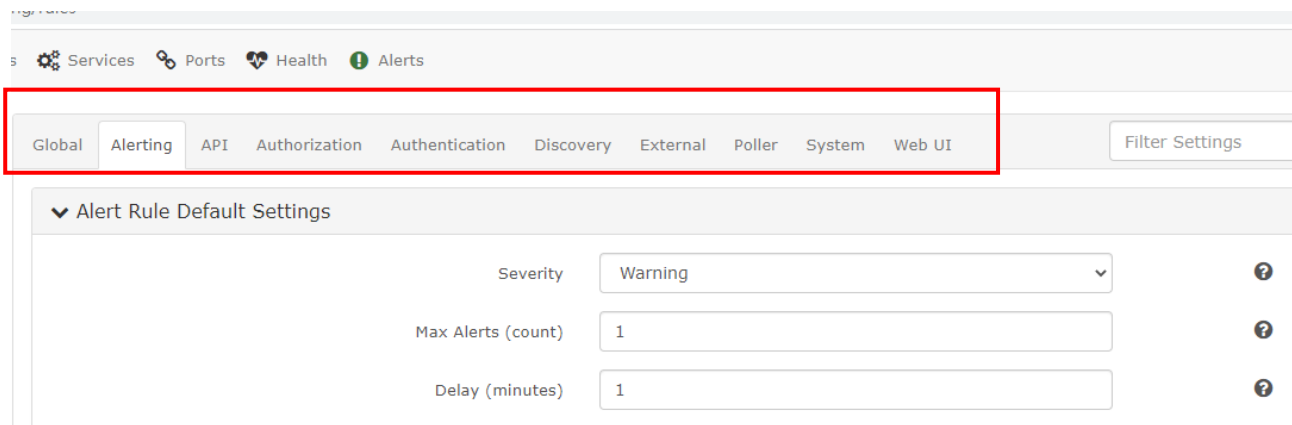
- **Time based(TOTP):** Time-based One-time Password (TOTP) is a time-based OTP.
- **Counter based(HOTP):** Each time the HOTP is requested and validated, the moving factor is incremented based on a counter.

Choosing between HOTP and TOTP purely from a security perspective is clearly beneficial to TOTP. It is important that the verification server must be able to cope with the possible time drift of TOTP tokens to minimize the impact on users.

4.2.8 Global settings



Global setting can set Alerting 、 API 、 Authorization 、 Authentication 、 Discovery 、 External 、 Poller 、 System 、 Web UI, the detailed description is as follows.



- **Alerting:** Set default alarm rules, email sent, general alarm settings.
- **API:** Cross-origin resource sharing (CORS) is a browser security feature that restricts cross-origin HTTP requests that are initiated from scripts running in the browser. If your REST API's resources receive non-simple cross-origin HTTP requests, you need to enable CORS support.
- **Authorization:** You can enable user access via dynamic Device Groups.
- **Authentication:** You can set up Active Directory, General Authentication, LDAP.
- **Discovery:** The module can be turned on or off, and the network IP and Mountpoints to be ignored can be set.
- **External:** Users can set Location and Integration, and Integration includes Graylog, Location, Mac OUI Lookup, NfSen, Oxidized, PeeringDB, Smokeping, SNMP Traps, Unix-Agent.
- **Poller:** Support for Graphite, InfluxDB, OpenTSDB, Prometheus, RRDTOOL can be enabled, and the POLLER module can be configured.
- **System:** You can set the time for automatic data clearing, proxy server, LibreNMS host name, and enable update.
- **Web UI:** Users can set and change Availability Map, Dashboard, Device, Graph, Style, Interface Description Parsing, max search and Display network links on the map.

4.3 License

Copyright (C) 2006-2012 Adam Armstrong adama@memetic.org

Copyright (C) 2013-2021 by individual LibreNMS contributors

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

5. FAQ

Q01: An error message appears during [Add Device] [Cannot ping 192.168.xxx.xxx]



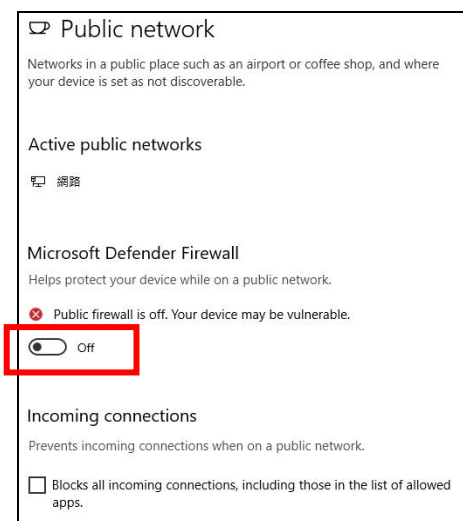
A01: Common reasons for the device to disable IPV6 or deny access to NMC-9181, the exclusion method is based on the example of windows 10 OS operation, there are two methods, please refer to the following instructions to set

1. Public network firewall is off.

Step1

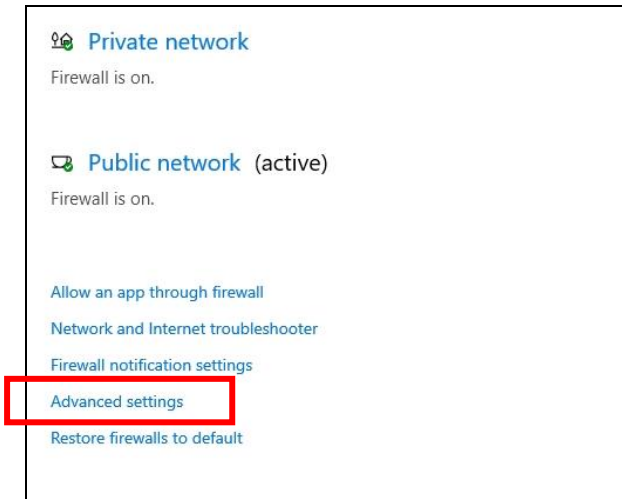


Step2



2. Go to [Advanced Settings] > [Inbound Rules] > [File and Printer Sharing(ICMP4-In)] > [Check Enable]

Step1:



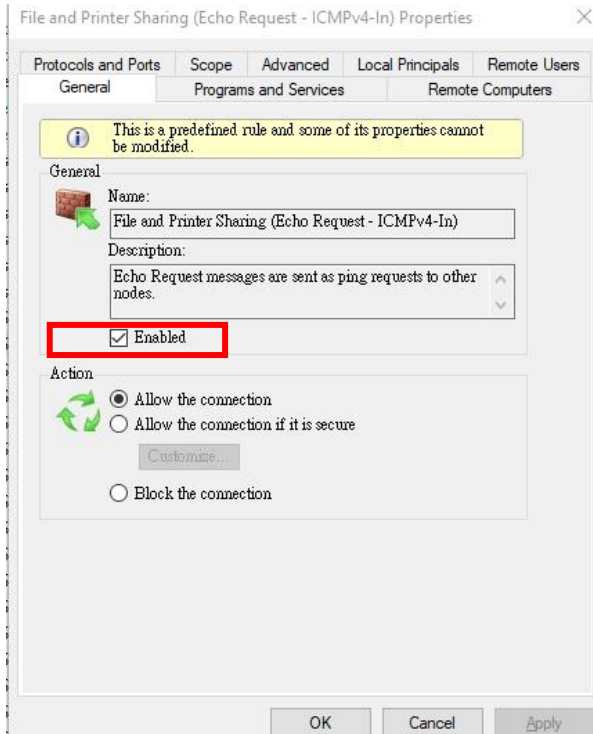
Step2



Step3

Inbound Rules				
Name	Group	Profile	Enabled	Action
✓ Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes	Allow
✓ Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes	Allow
✓ Desktop App Web Viewer	Desktop App Web Viewer	All	Yes	Allow
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes	Allow
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Co...	Domain	No	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Co...	Private, Public	No	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Co...	Private, Public	No	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Co...	Domain	No	Allow
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Co...	Domain	No	Allow
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Co...	Private, Public	No	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No	Allow
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private, Public	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private, Public	No	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow

Step4



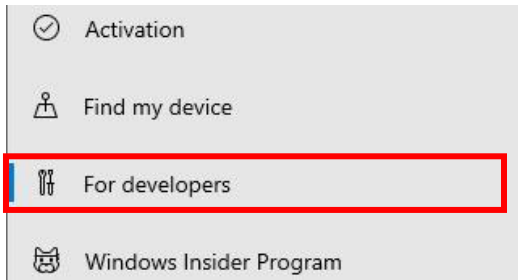
Q02: An error related to [SNMP] occurred during [Add Device].



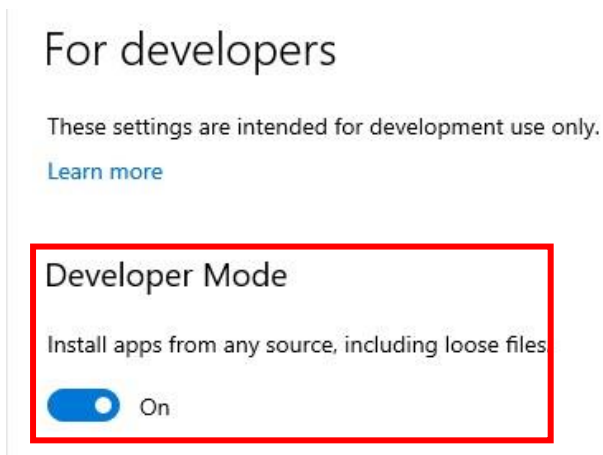
A02: The common cause is that the device is not installed with SNMP or the SNMP setting is wrong. The user must confirm the detailed SNMP setting, the exclusion method is based on the example of windows 10 OS operation, please refer to the following instructions to set.

1. [Settings] > [Update and Security] > [For Developers] > Developer Mode [On]

Step1

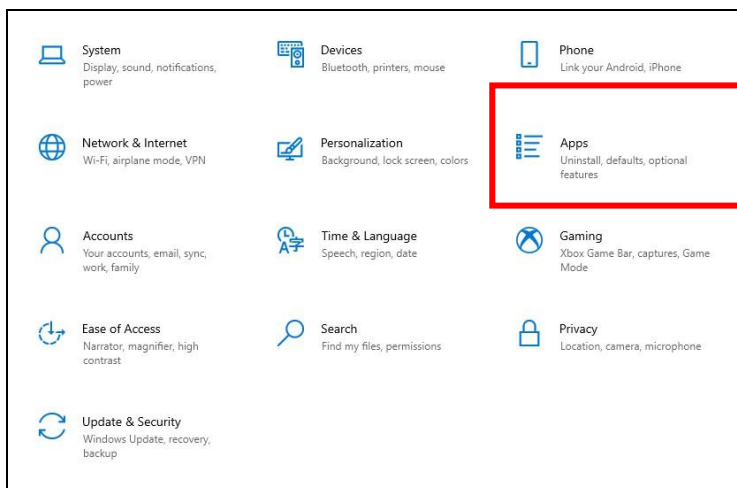


Step2

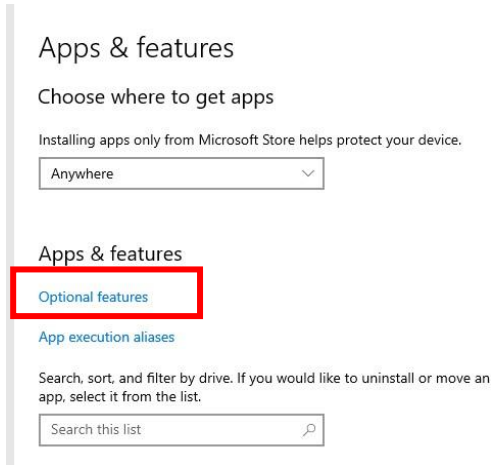


2. [Settings] > [Apps] > [Optional Features] > [New Features]> Find Simple Network Management Protocol (SNMP)> [Install]

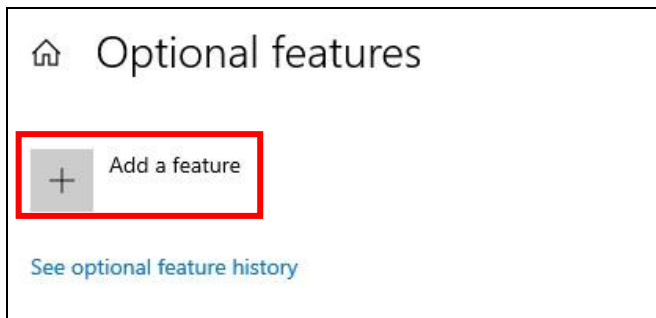
Step1



Step2



Step3

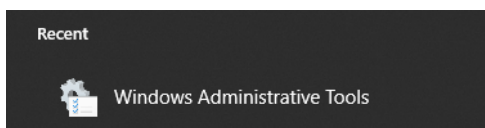


Step4

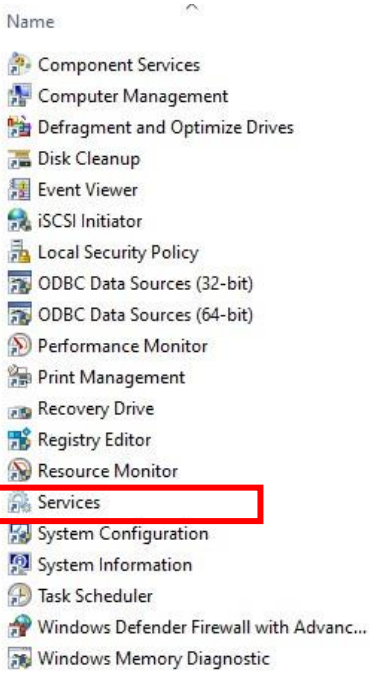


3. Please go to [Windows Administrative Tools] > [Services] > [SNMP Service] > Confirm whether to enable

Step1



Step2

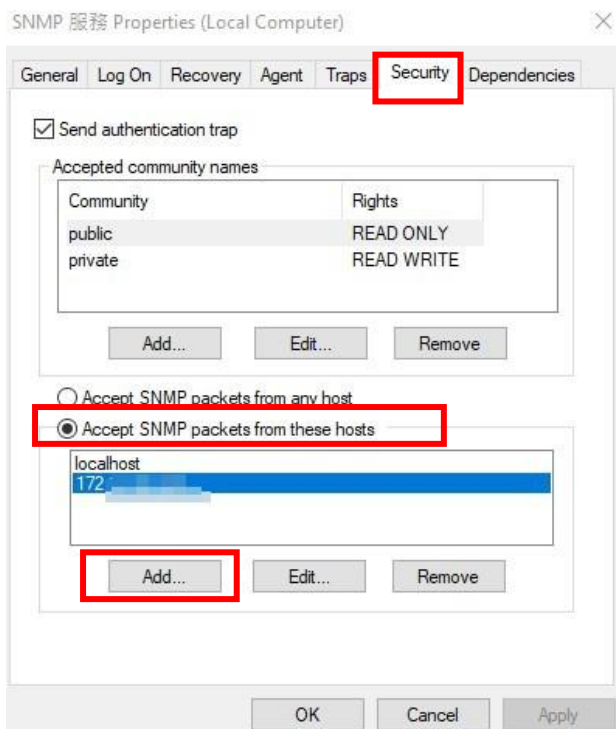


Step3

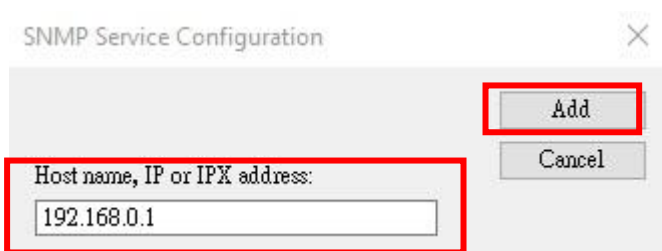
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...		Manual (Trig...	Local Service
Smart Card Device Enumera...	Creates soft...		Manual (Trig...	Local Syste...
Smart Card Removal Policy	Allows the s...		Manual	Local Syste...
SNMP Trap	Receives tra...		Manual	Local Service
SNMP 服務	Enables Sim...	Running	Automatic	Local Syste...
Software Protection	Enables the ...		Automatic (...	Network S...
Spatial Data Service	This service ...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trig...	Local Syste...
SQL Server VSS Writer	提供介面...	Running	Automatic	Local Syste...
SSDP Discovery	Discovers n...	Running	Manual	Local Service
State Repository Service	Provides re...	Running	Manual	Local Syste...

4. Click [SNMP Service] > Go to [Security] > [Accept SNMP packets from these hosts] > [Add IP of NMC-9181].

Step1



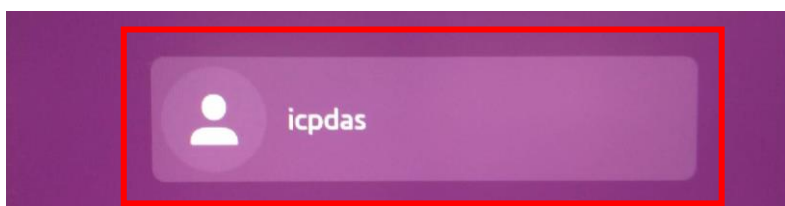
Step2: Add NMC-9181 IP



Q03: How to import SNMP MIB files?

A03: Please follow the instructions below to set up

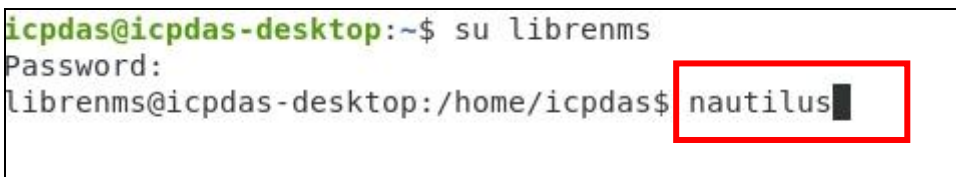
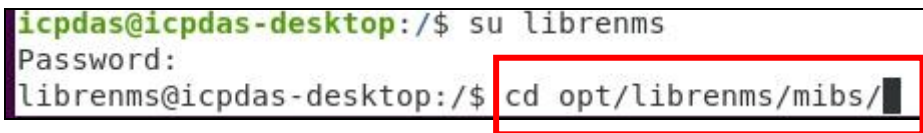
Step1: Login as [icpdas], the default password is [icpdas]



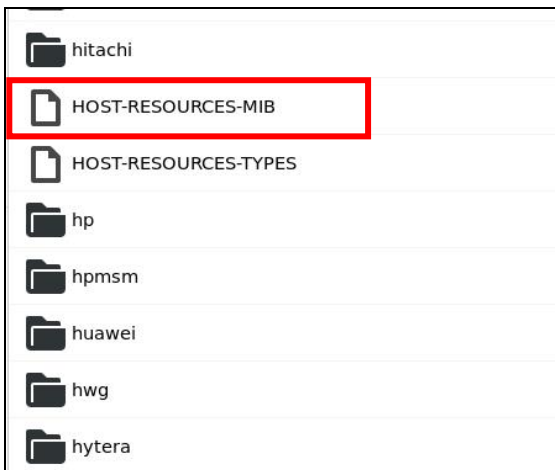
Step2: Open the **terminal** and enter [su librenms] , the default password is [D32fwefwef]



Step3: Users can type [cd opt/librenms/mibs] to go to the mibs folder, or type [nautilus] to open the file manager operation to access the mibs folder.



Step4: Copy the **.MIB** file to the **mibs** folder



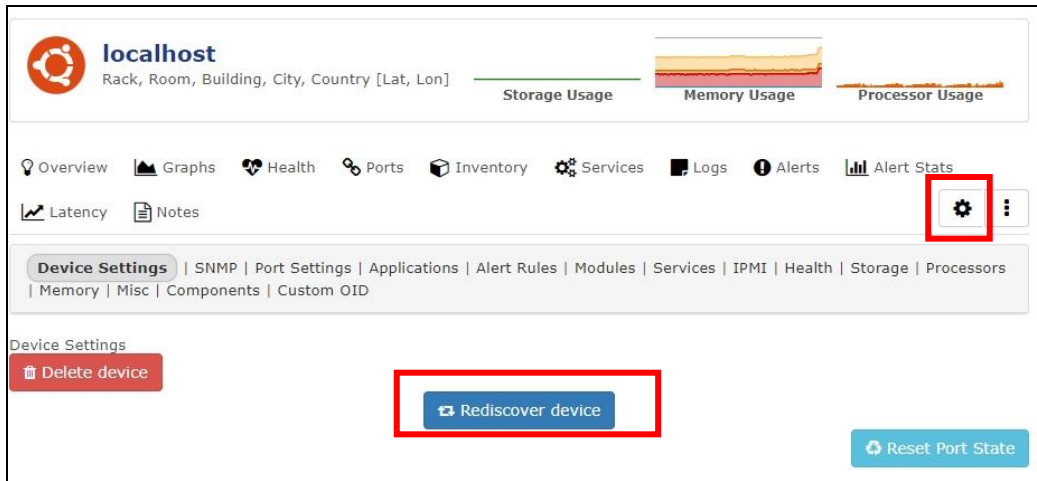
***Note:**

1.If the device has MIBs available and you use it in the detection then you can add these in. It is highly recommended that you **add mibs** to a **vendor specific directory**. For instance **HP mibs** are in

mibs/hp. Please ensure that these directories are specified in the yaml detection file, see mib_dir above.

2. Do not delete files randomly to avoid errors.

Step5: Then click the **gear icon** at the top right of the device and then click [**Rediscover Device**] to let LibreNMS scan again.



***Note:**

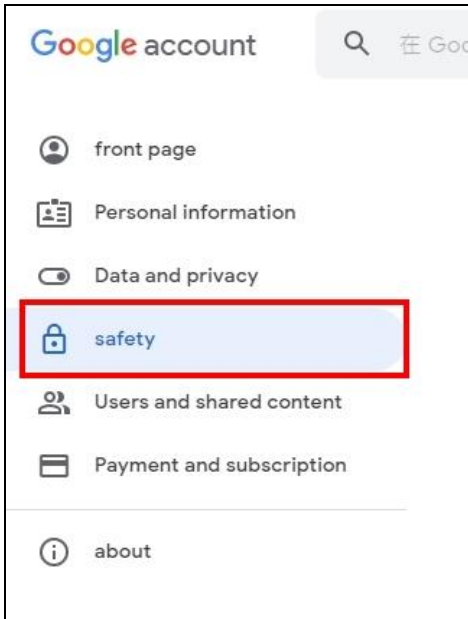
1. LibreNMS will grab the device information based on the **yaml file** in the [opt/ librenms /includes/definitions] directory and the **sysObjectID** in the specified folder in **mib_dir**.
2. mib_dir can **only** specify one folder.
3. For details, please refer to the link below

<https://docs.librenms.org/Developing/os/Initial-Detection/>

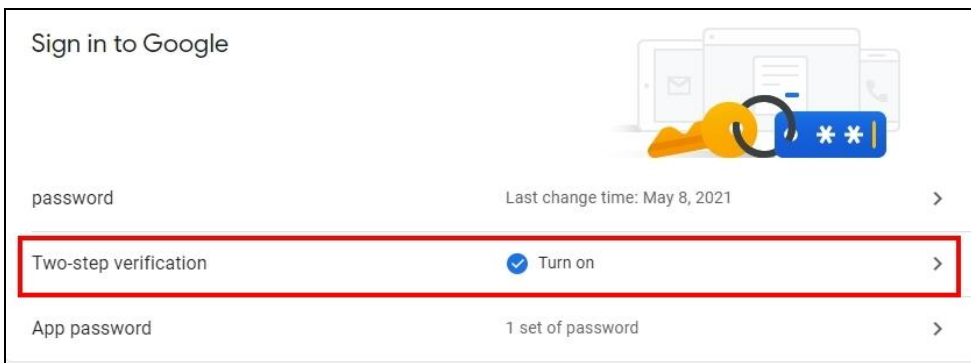
Q04: How to use Google SMTP to send a letter?

A04: Please follow the instructions below to set up.

Step1: Login to Google and go to Google **security settings** page.

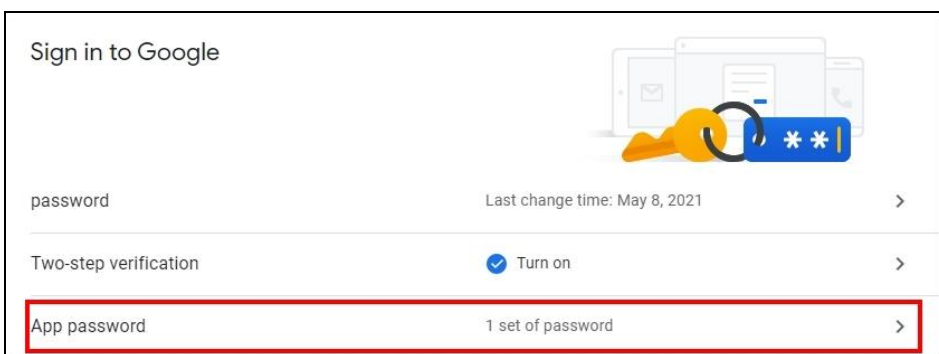


Step2: Enable [Two-step verification]



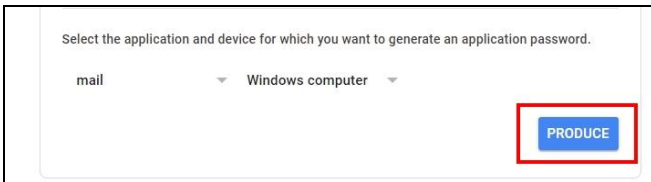
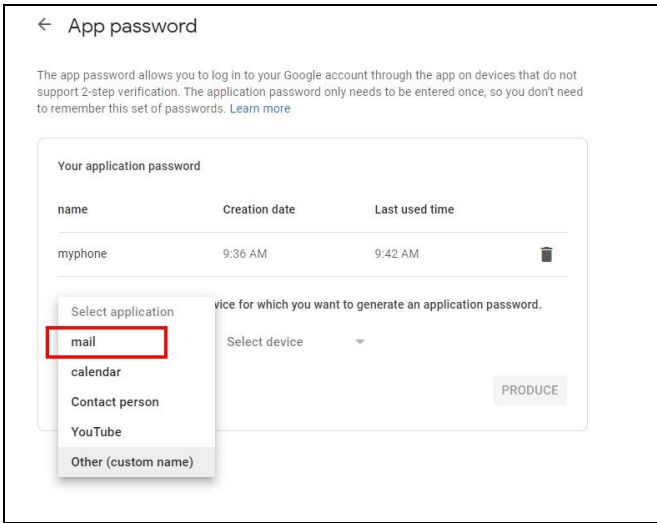
***Note:** In this process, you need to use your phone for verification.

Step3: Set [Application Password]



Step4: Select the application (MAIL) and device for which you want to generate an application

password, and then press **[Produce]**.



Step5: Get the application password generated by the system.



***Note**

This application password is just like your usual password, which grants full access to your Google account. You do not need to remember this set of passwords, so please do not write down or disclose the password to anyone who knows it.

Step6: To [Global Setting] > [Alerting] > [Email Options], Set up Google SMTP to send mail.

▼ Email Options

Enable email alerting

From name LibreNMS

From email address [redacted]@gmail.com

Use HTML emails

How to deliver mail SMTP

SMTP Server smtp.gmail.com

SMTP port setting 465

SMTP timeout setting 10

Encryption SSL

Auto TLS support

SMTP authentication

SMTP Auth username [redacted]@gmail.com

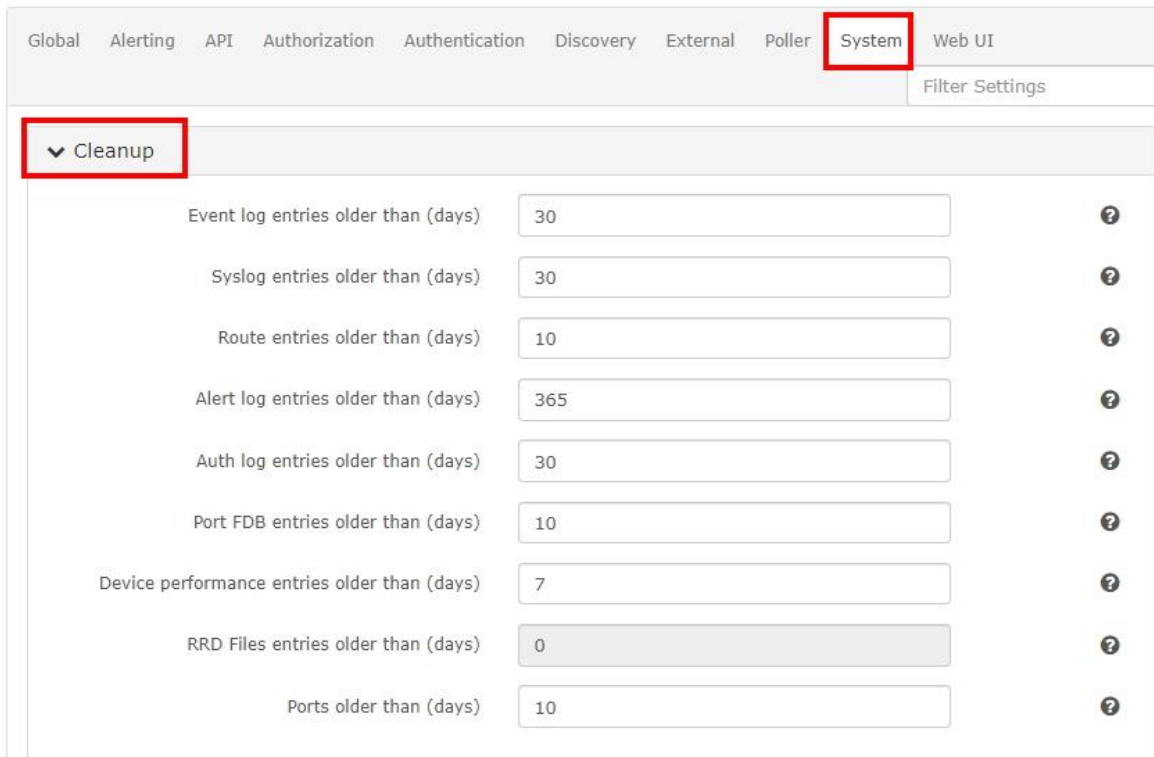
SMTP Auth password

- SMTP host: [smtp.gmail.com](#)
- SMTP port number: **465**
- SMTP security mode: **SSL/TLS**
- SMTP authentication: **Enable**
- SMTP account: [[your gmail account](#)]
- SMTP password: [[google application password](#)]

Q05: How to clean up LibreNMS log files?

A05: As the number of devices starts to grow in your LibreNMS install, so will things such as the RRD files, MySQL database containing eventlogs, Syslogs and performance data etc. Your LibreNMS install could become quite large so it becomes necessary to clean up those entries. With Cleanup Options, you can stay in control.

Step1: To [Global Setting] > [System] > [Cleanup], these options will ensure data within LibreNMS over X days old is automatically purged. You can alter these individually, values are in days.



Setting	Value	Help
Event log entries older than (days)	30	?
Syslog entries older than (days)	30	?
Route entries older than (days)	10	?
Alert log entries older than (days)	365	?
Auth log entries older than (days)	30	?
Port FDB entries older than (days)	10	?
Device performance entries older than (days)	7	?
RRD Files entries older than (days)	0	?
Ports older than (days)	10	?

***Note**

Please be aware that [RRD Files] is **NOT** set by default. This option will remove any RRD files that have not been updated for the set amount of days automatically - **only enable** this if you are comfortable with that happening. (All active RRD files are updated every polling period.)

Q06: How to Add Device?

A06: To use this software, you must add a new device, please refer to the following link to add a device.

Method 1:

[4.2.1 Overview\(3\) Plugins Network Scan](#)

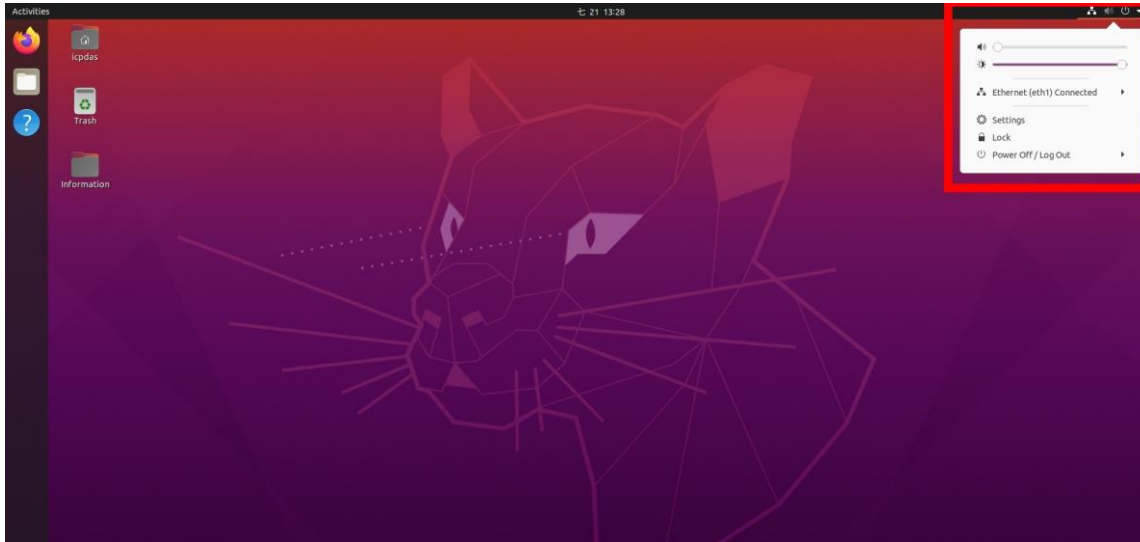
Method 2:


[4.2.2 Devices \(5\) Add Device](#)

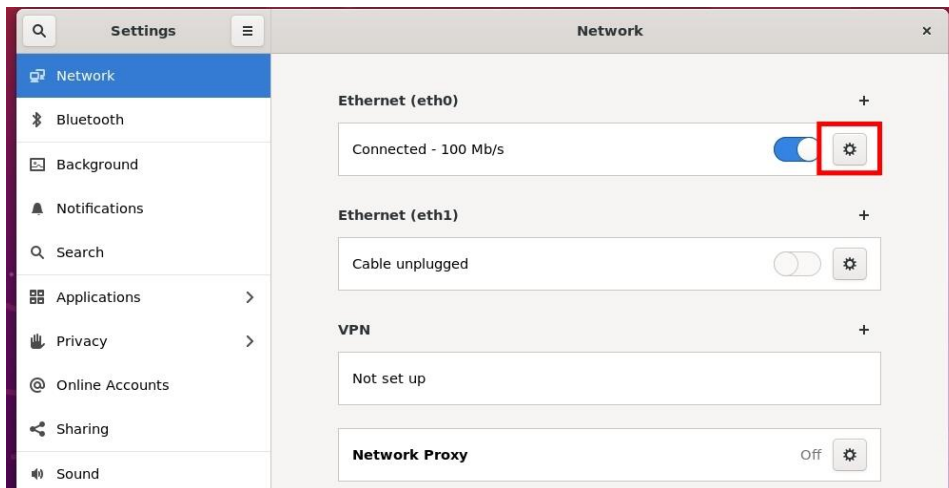
Q07: How to Change Your IP Address on Linux?

A07: Please Login Linux and follow the instructions below to set up.

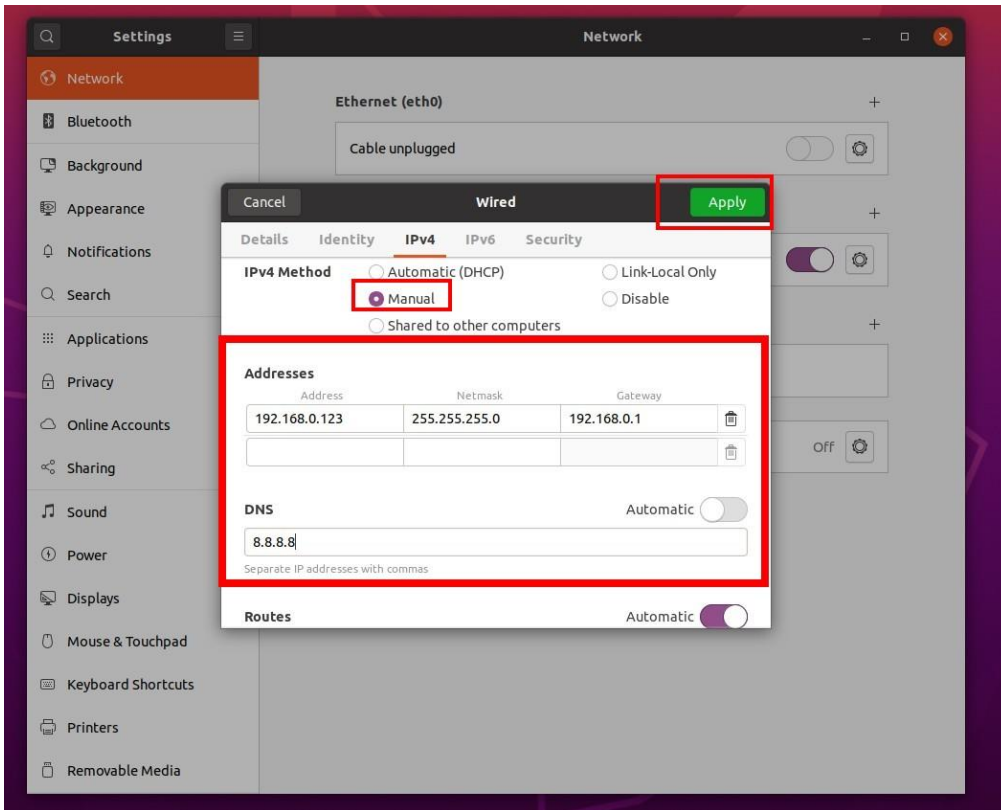
Step1: To Click the icon in the upper right corner and select [Setting]



Step2: To [Setting] > [Network] > Click on the  icon of the interface you would like to set an IP address.



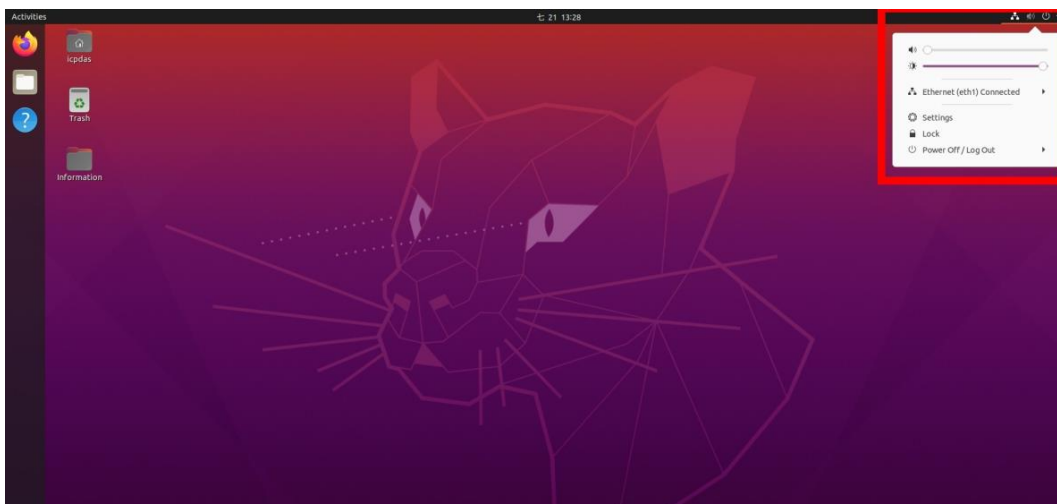
Step3: You will need to select Manual on the IPv4 tab in order to enter your settings. Select [IPv4] > [Manual] > Update the IP address to what you want it to be > [Apply].

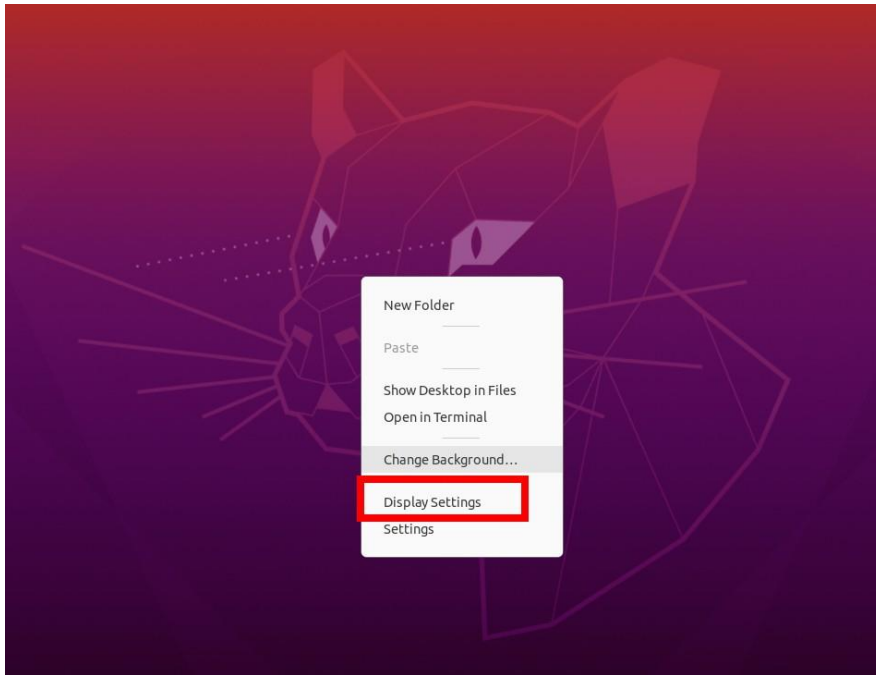


Q08: How to Setting Display mode on Linux?

A08: If an external monitor is connected using VGA or HDMI, the Login controls not displayed on all screens, You can set the display mode to solve the problem, Please follow the instructions below to set up.

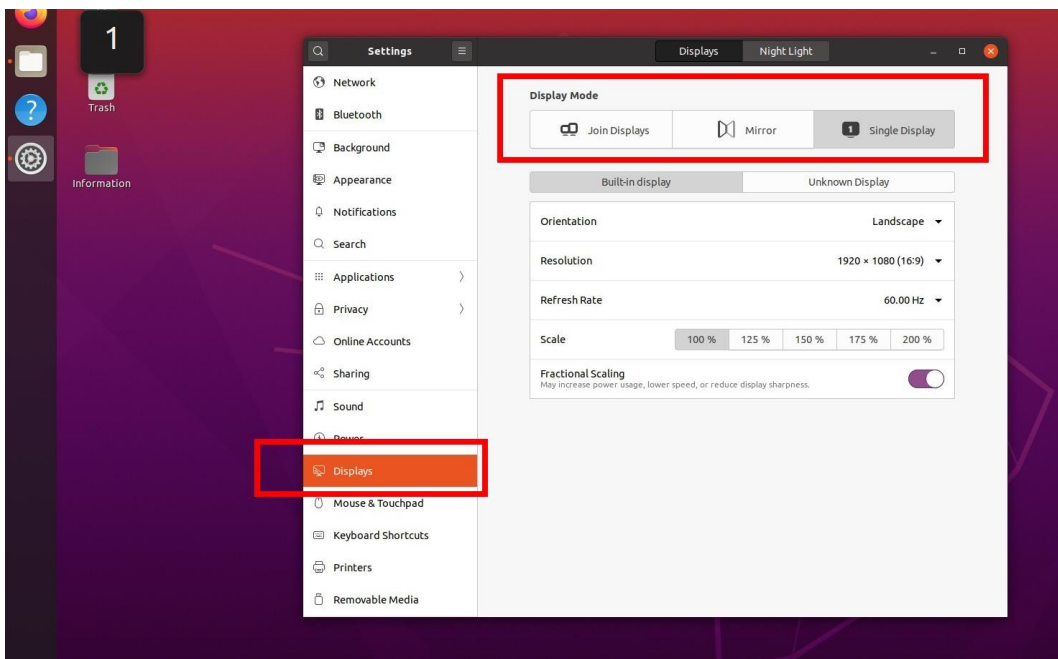
Step1: To Click the icon in the upper right corner and select [Setting] or click the right mouse button > select [Display Settings]

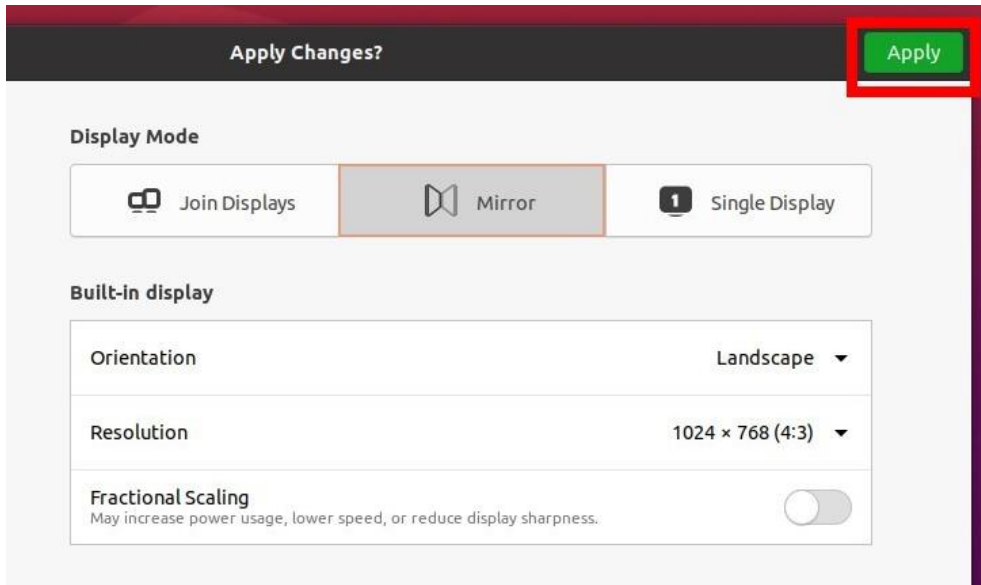




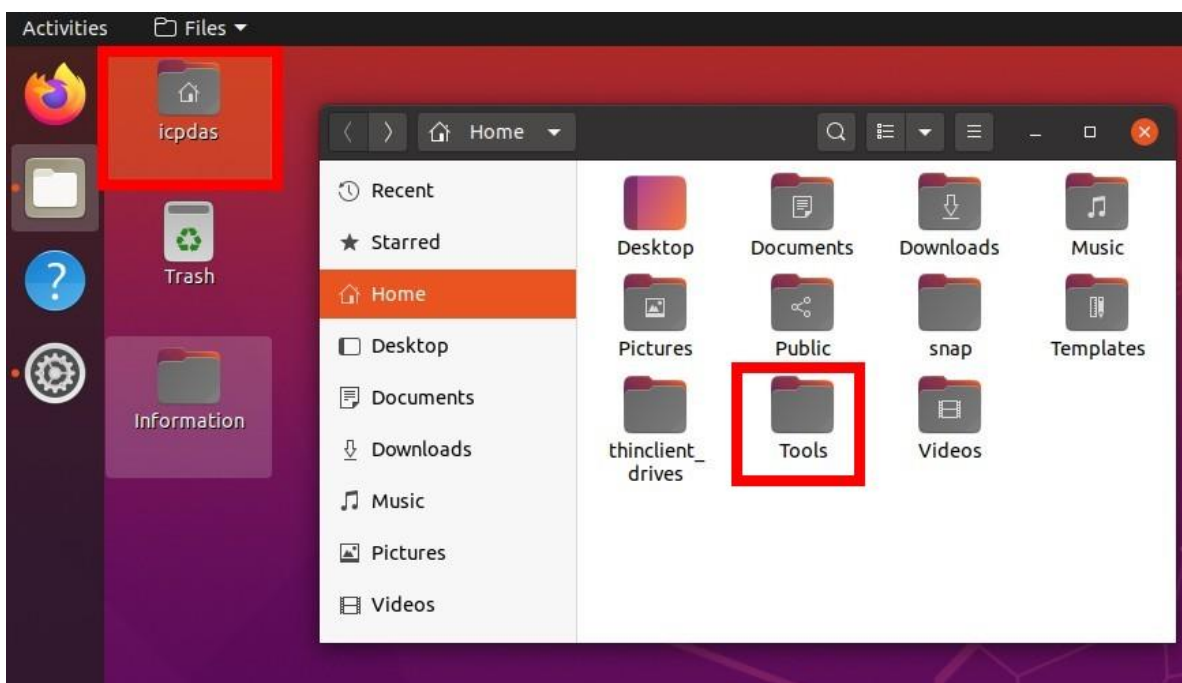
Step2: To [Setting] > [Displays] > Select a display mode to what you want it to be > [Apply].

***Note: It is recommended to select [Mirror mode]**

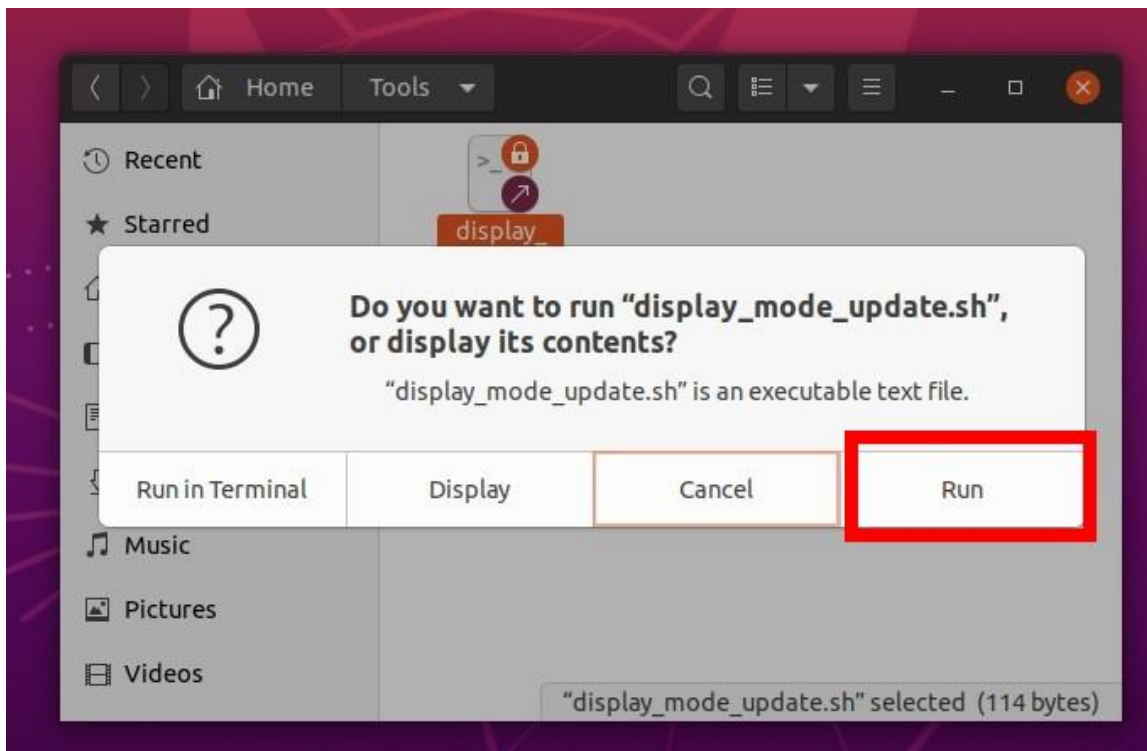
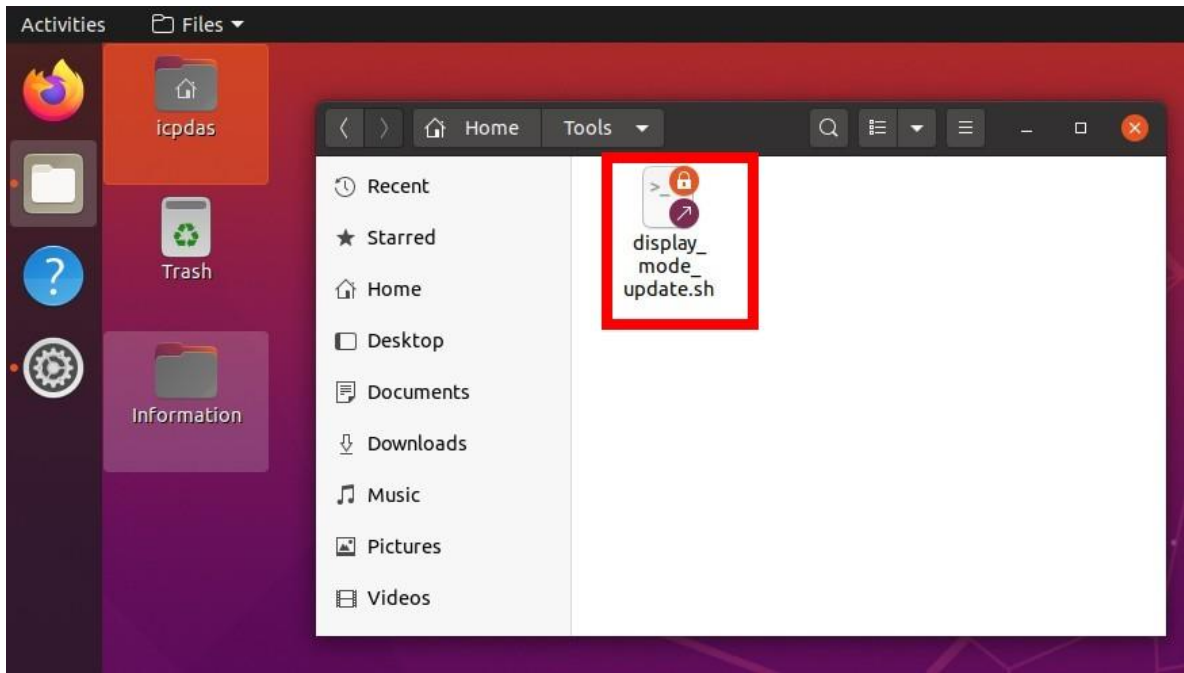




Step3: After setting the display mode, go back to the **Desktop** > Select [**icpdas**] file > Click [**Tools**] file



Step4: Double click [**display_mode_update.sh**] file > Select [**Run**]



Appendix A. Revision History

This chapter provides revision history information to this document.

The table below shows the revision history.

Version	Date	Description of changes
1.0.0	2021-12-08	The First Release Revision
1.0.1	2022-07-21	Add FAQ Q07 、 Q08