FAQ Manual

Version 1.0.2 Sep 2022

NMC-9181

Network Management Controller

Table of Contents

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

Trademark

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

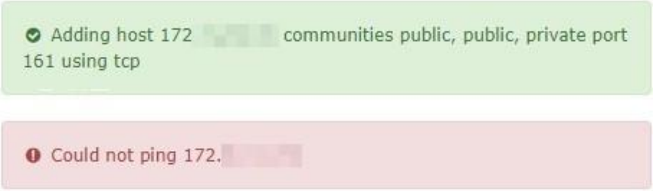
Contact us

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

Email: service@icpdas.com

1. FAQ

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



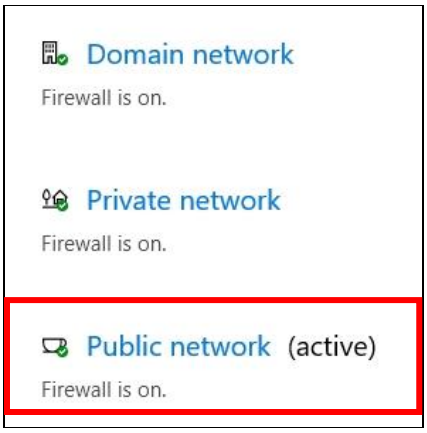
✔ Adding host 172 [redacted] communities public, public, private port 161 using tcp

❶ Could not ping 172.[redacted]

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

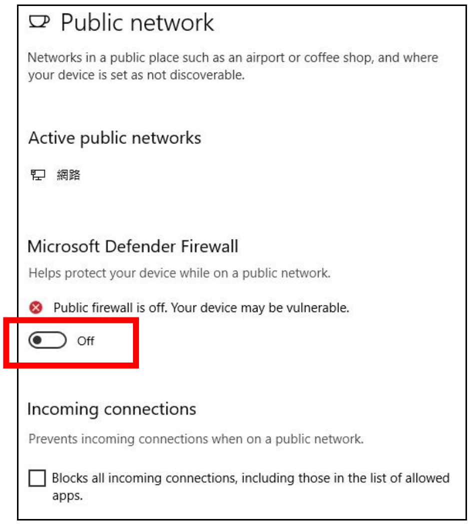


Domain network
Firewall is on.

Private network
Firewall is on.

Public network (active)
Firewall is on.

Step2



Public network

Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.

Active public networks

網路

Microsoft Defender Firewall

Helps protect your device while on a public network.

Public firewall is off. Your device may be vulnerable.

Off

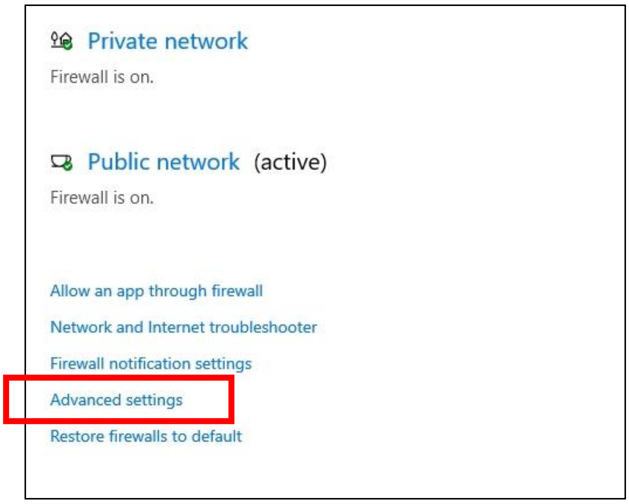
Incoming connections

Prevents incoming connections when on a public network.

□ Blocks all incoming connections, including those in the list of allowed apps.

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

Step1:



Private network

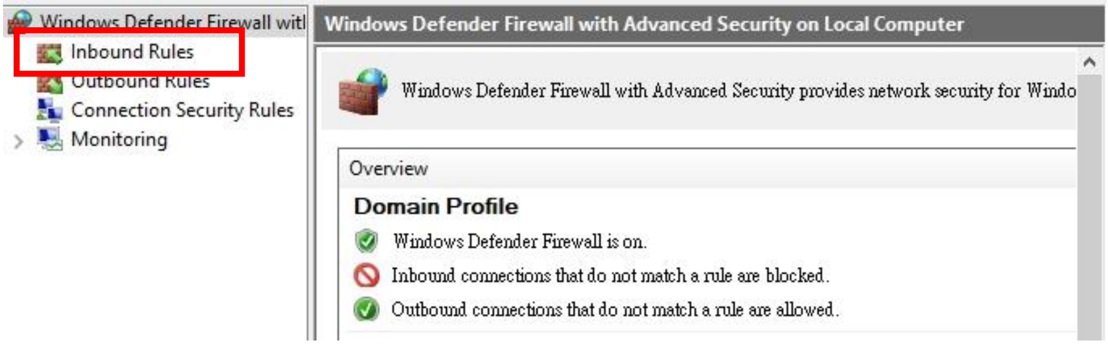
Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Step2



Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

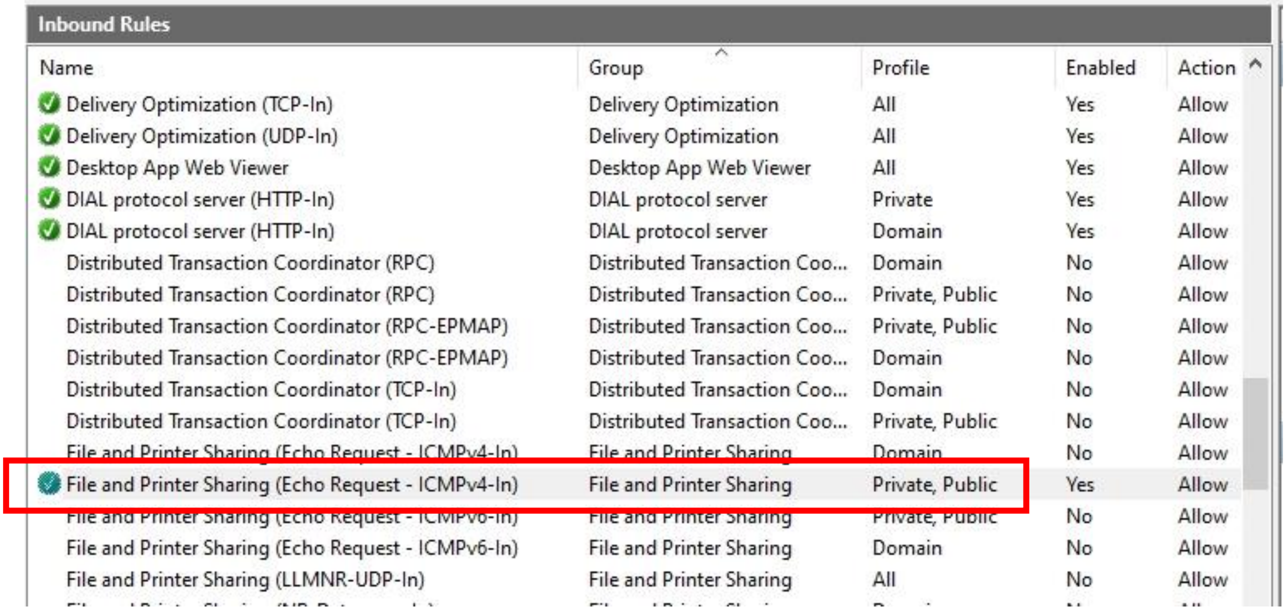
Domain Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

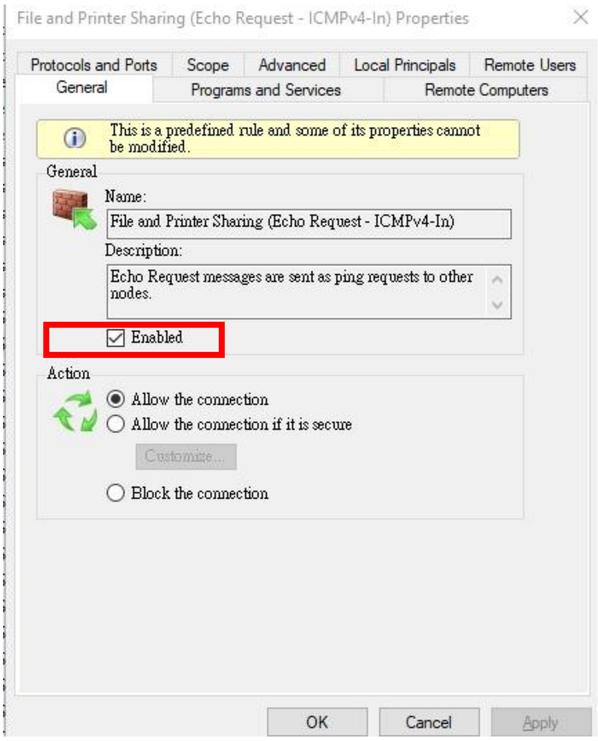
Step3



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 Coo...	Domain	No	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private, Public	No	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private, Public	No	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No	Allow
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No	Allow
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	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



File and Printer Sharing (Echo Request - ICMPv4-In) Properties

This is a predefined rule and some of its properties cannot be modified.

General

Name: File and Printer Sharing (Echo Request - ICMPv4-In)

Description: Echo Request messages are sent as ping requests to other nodes.

☑ Enabled

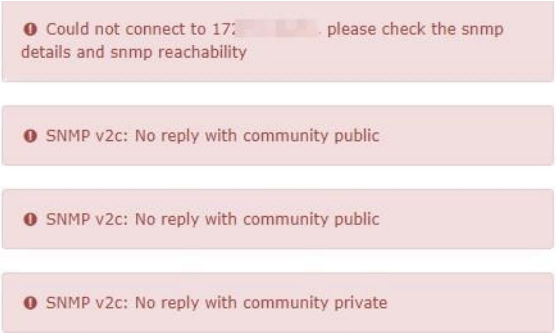
Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

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



Could not connect to 17[redacted], please check the snmp details and snmp reachability

SNMP v2c: No reply with community public

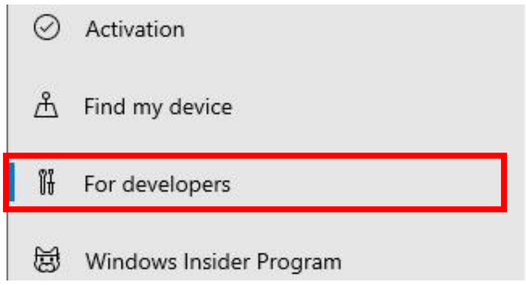
SNMP v2c: No reply with community public

SNMP v2c: No reply with community private

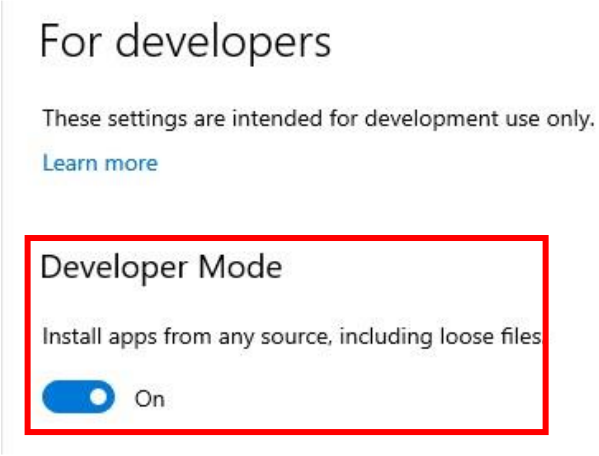
A02: The common cause is that the device is not installed with SNMP or the SNMP setting is wrong. The user must confirm the detailed SNMP setting, the exclusion method is based on the example of windows 10 OS operation, please refer to the following instructions to set.

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

Step1



Step2



For developers

These settings are intended for development use only.

Learn more

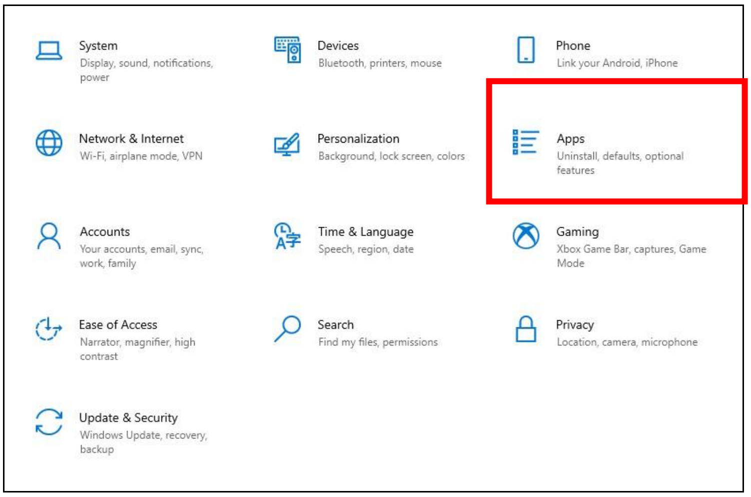
Developer Mode

Install apps from any source, including loose files

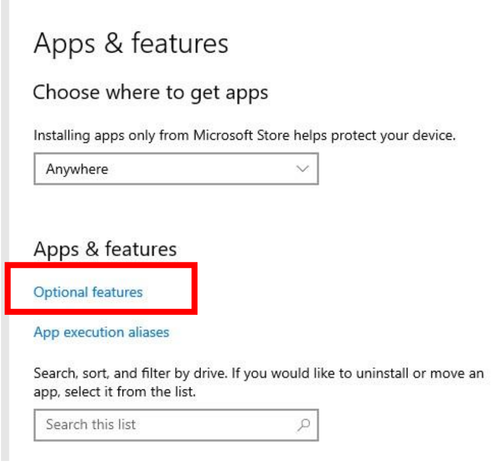
On

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

Step1


System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

Step2



Apps & features

Choose where to get apps

Installing apps only from Microsoft Store helps protect your device.

Anywhere

Apps & features

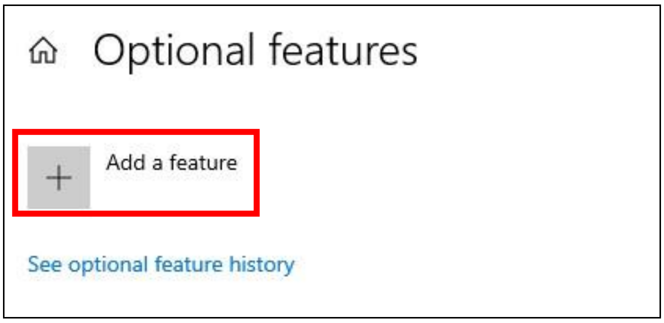
Optional features

App execution aliases

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

Search this list

Step3

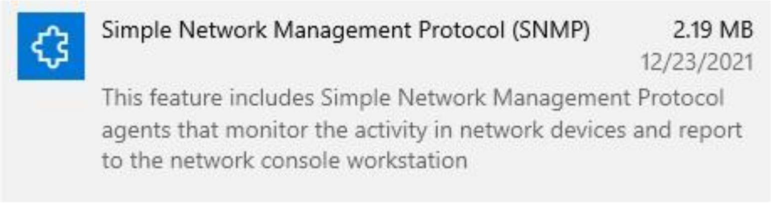


Optional features

Add a feature

See optional feature history

Step4

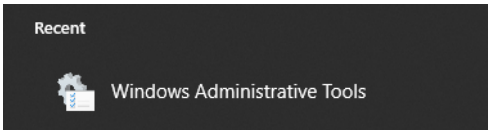


Simple Network Management Protocol (SNMP) 2.19 MB 12/23/2021

This feature includes Simple Network Management Protocol agents that monitor the activity in network devices and report to the network console workstation

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

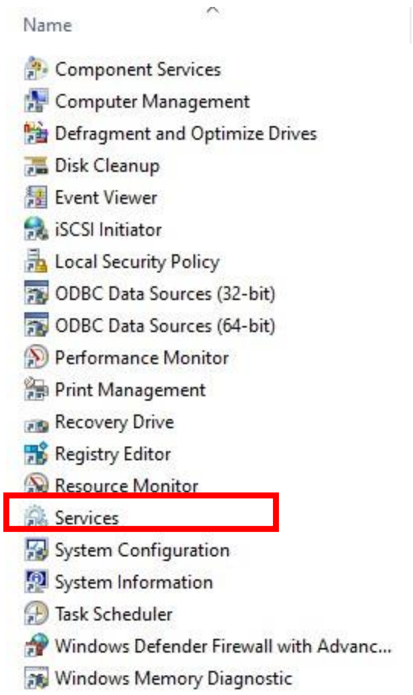
Step1



Recent

Windows Administrative Tools

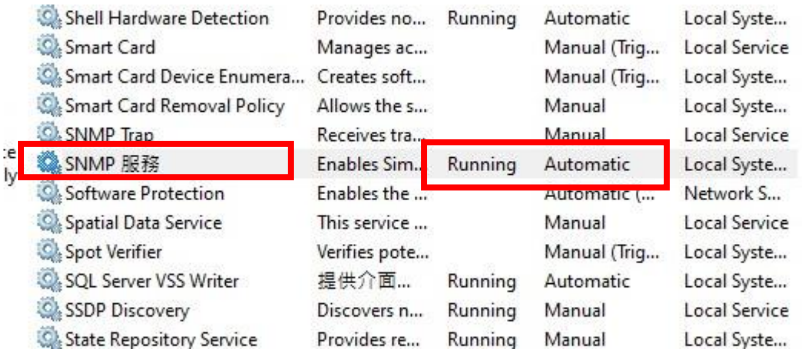
Step2



Name

- Component Services
- Computer Management
- Defragment and Optimize Drives
- Disk Cleanup
- Event Viewer
- iSCSI Initiator
- Local Security Policy
- ODBC Data Sources (32-bit)
- ODBC Data Sources (64-bit)
- Performance Monitor
- Print Management
- Recovery Drive
- Registry Editor
- Resource Monitor
- Services
- System Configuration
- System Information
- Task Scheduler
- Windows Defender Firewall with Advanc...
- Windows Memory Diagnostic

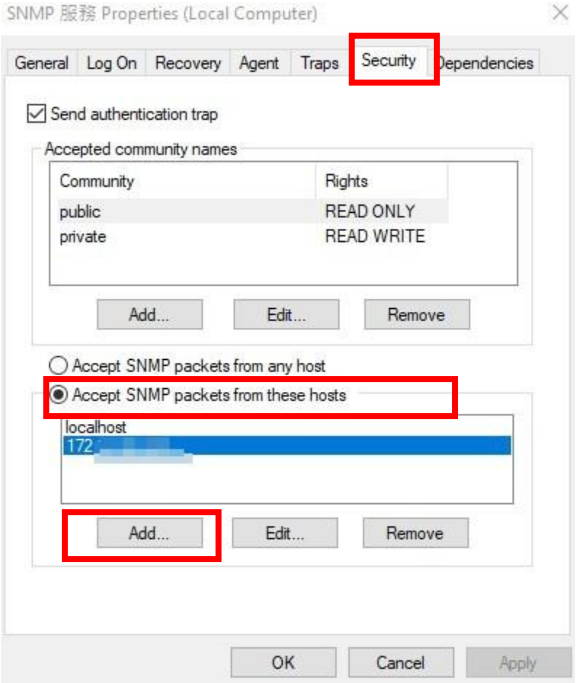
Step3



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



☑ Send authentication trap

Accepted community names

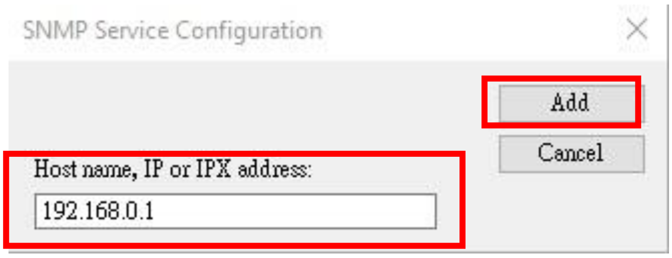
Community	Rights
public	READ ONLY
private	READ WRITE

○ Accept SNMP packets from any host

● Accept SNMP packets from these hosts

localhost
172[redacted]

Step2: Add NMC-9181 IP

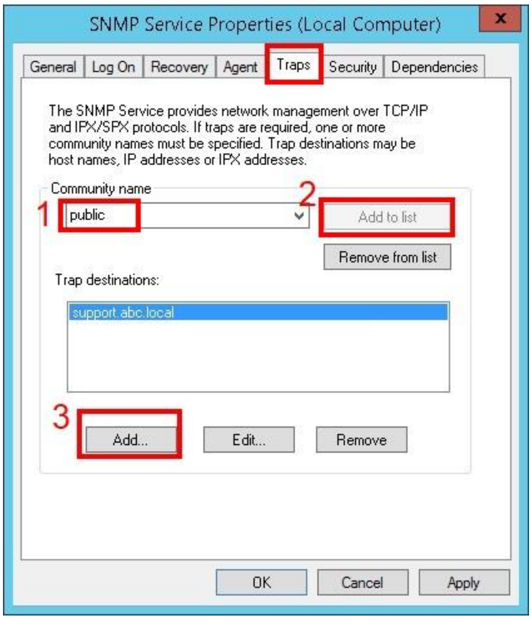


Host name, IP or IPX address:

192.168.0.1

5. Click [SNMP Service] > Click [Traps] tab > enter [Community name] > Click [Add to list] > Trap destinations [Add IP of NMC-9181].

Step1:



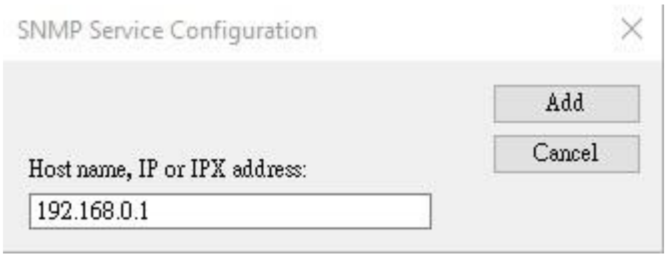
SNMP Service Properties (Local Computer)

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations: support.abc.local

Step2: Add NMC-9181 IP



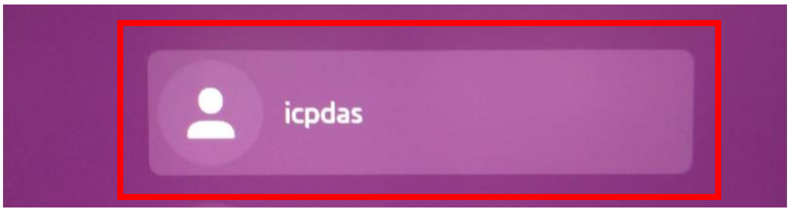
SNMP Service Configuration

Host name, IP or IPX address: 192.168.0.1

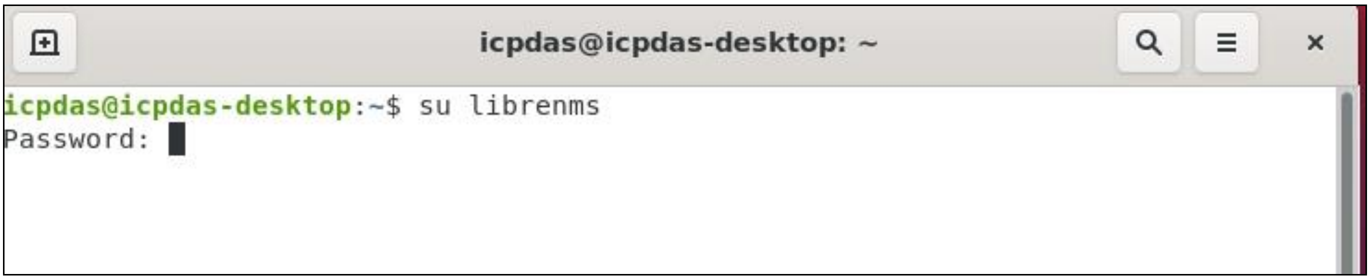
Q03: How to import SNMP MIB files?

A03: Please follow the instructions below to set up

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

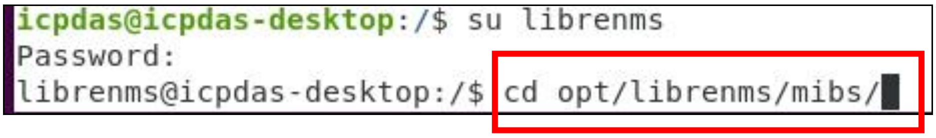


Step2: Open the terminal and enter [su librenms] , the default password is [D32fwefwef]

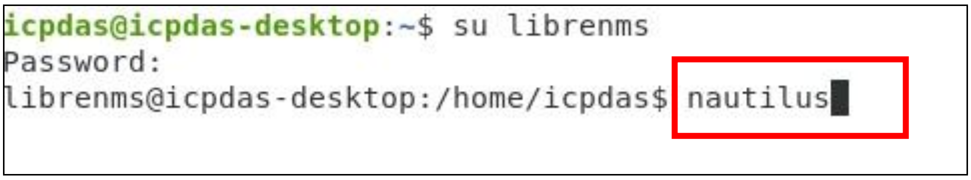


```
icpdas@icpdas-desktop:~$ su librenms
Password: 
```

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.

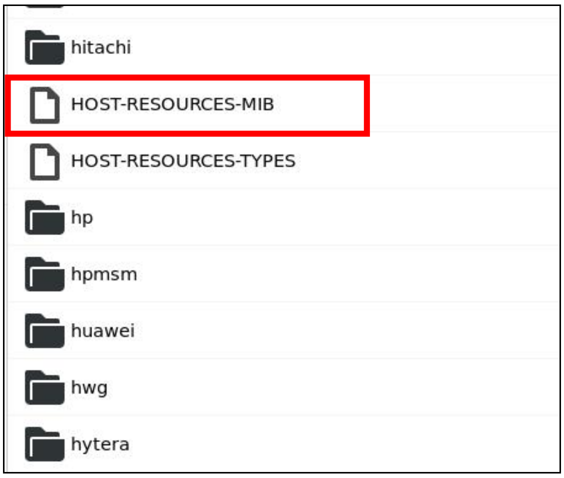


```
icpdas@icpdas-desktop:/$ su librenms
Password:
librenms@icpdas-desktop:/$ cd opt/librenms/mibs/
```



```
icpdas@icpdas-desktop:~$ su librenms
Password:
librenms@icpdas-desktop:/home/icpdas$ nautilus
```

Step4: Copy the .MIB file to the mibs folder

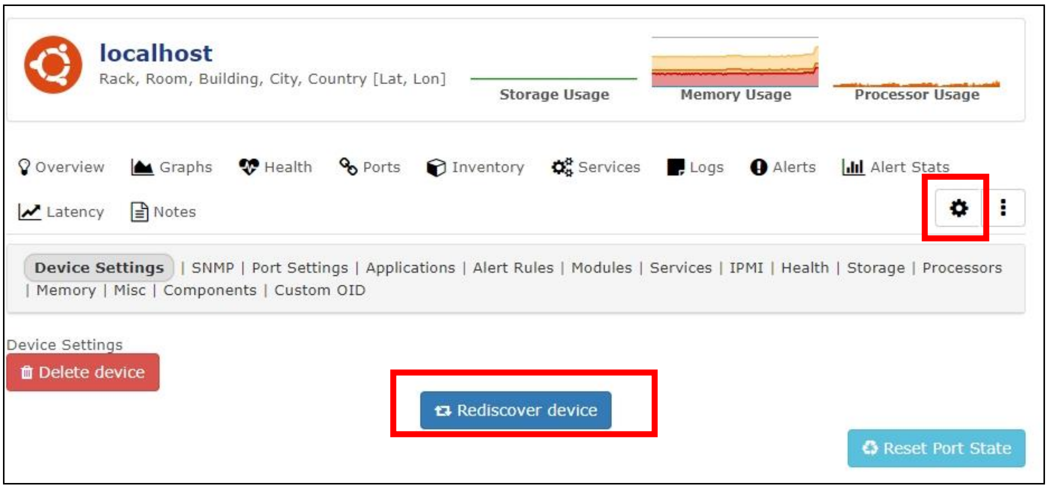


***Note:**

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.


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
Device Settings | SNMP | Port Settings | Applications | Alert Rules | Modules | Services | IPMI | Health | Storage | Processors | Memory | Misc | Components | Custom OID
Device Settings
Delete device
Rediscover device
Reset Port State

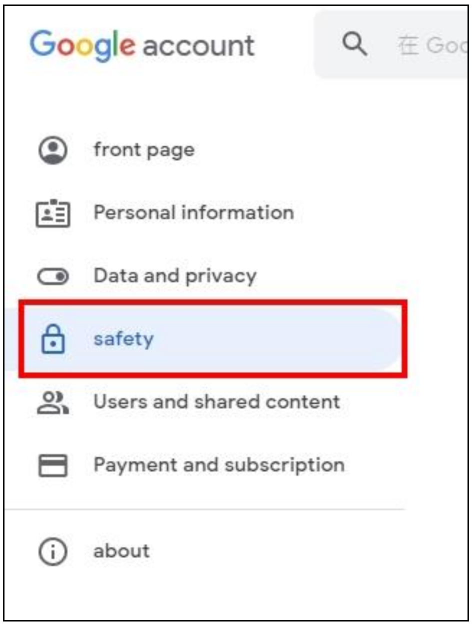
***Note:**

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/

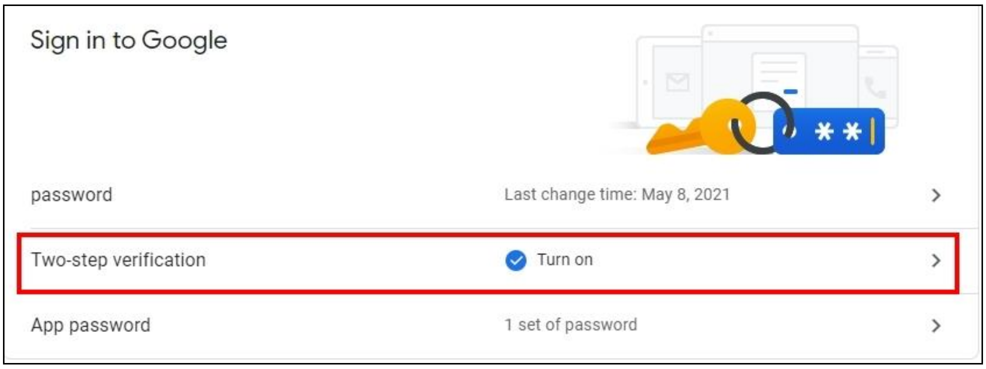
Q04: How to use Google SMTP to send a letter?

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]


Sign in to Google

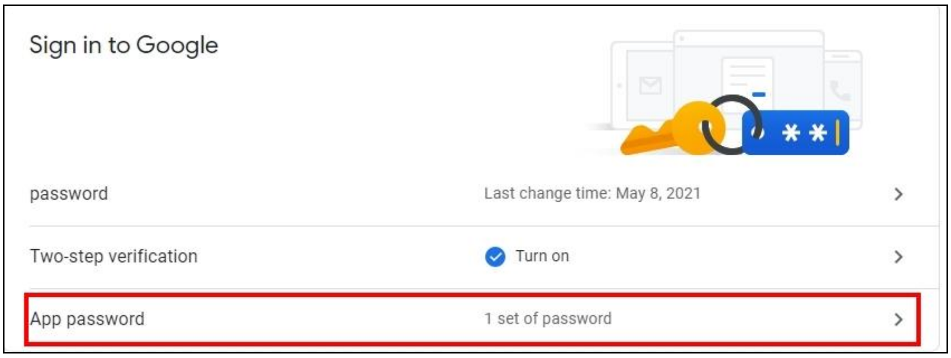
password Last change time: May 8, 2021

Two-step verification Turn on

App password 1 set of password

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

Step3: Set [Application Password]


Sign in to Google

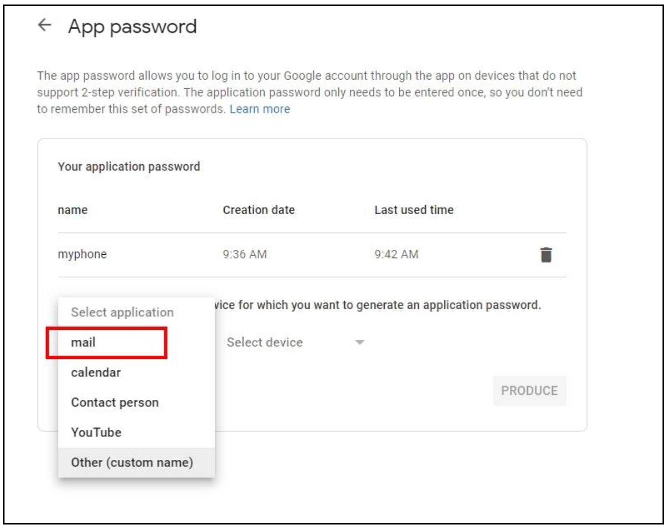
password Last change time: May 8, 2021

Two-step verification Turn on

App password 1 set of password

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

password, and then press [Produce].



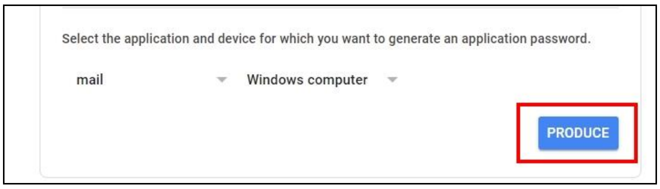
← App password

The app password allows you to log in to your Google account through the app on devices that do not support 2-step verification. The application password only needs to be entered once, so you don't need to remember this set of passwords. Learn more

Your application password

name	Creation date	Last used time
myphone	9:36 AM	9:42 AM

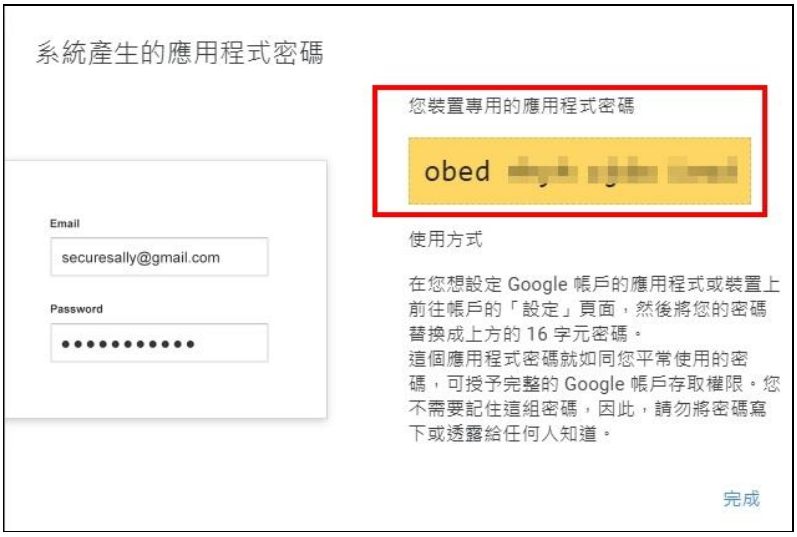
vice for which you want to generate an application password.



Select the application and device for which you want to generate an application password.

mail ▾ Windows computer ▾

Step5: Get the application password generated by the system.



系統產生的應用程式密碼

您裝置專用的應用程式密碼

obed [redacted]

使用方式

在您想設定 Google 帳戶的應用程式或裝置上前往帳戶的「設定」頁面，然後將您的密碼替換成上方的 16 字元密碼。

這個應用程式密碼就如同您平常使用的密碼，可授予完整的 Google 帳戶存取權限。您不需要記住這組密碼，因此，請勿將密碼寫下或透露給任何人知道。

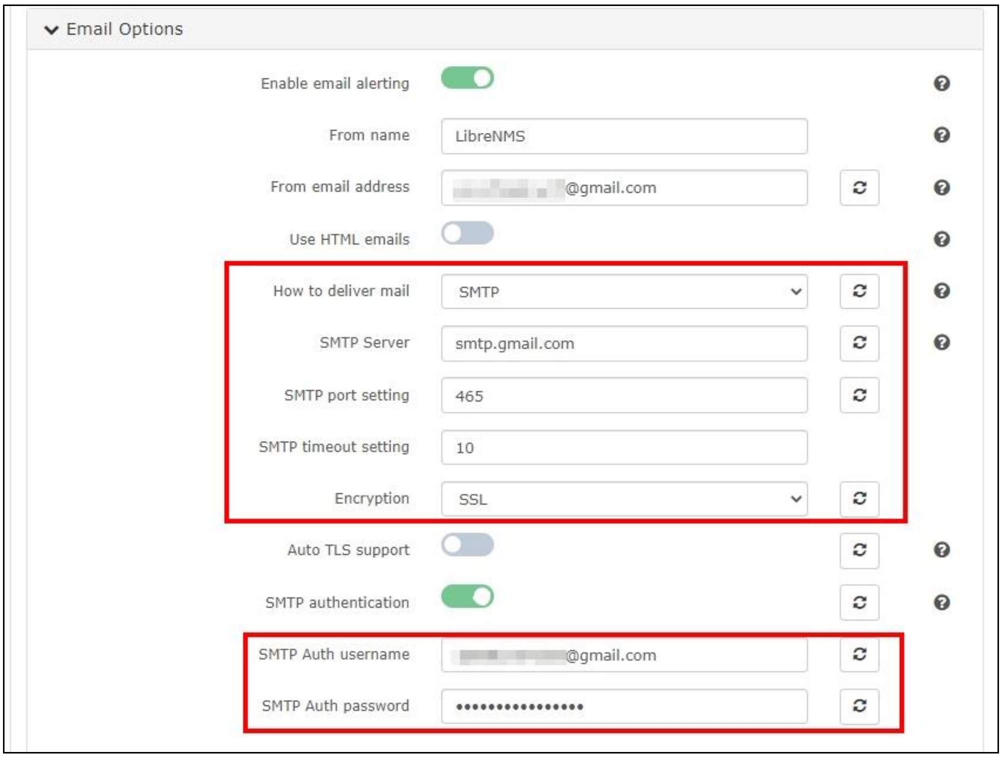
Email: securesally@gmail.com

Password: ●●●●●●●●●●●●

***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: On

From name: LibreNMS

From email address: [redacted]@gmail.com

Use HTML emails: Off

How to deliver mail: SMTP

SMTP Server: smtp.gmail.com

SMTP port setting: 465

SMTP timeout setting: 10

Encryption: SSL

Auto TLS support: Off

SMTP authentication: On

SMTP Auth username: [redacted]@gmail.com

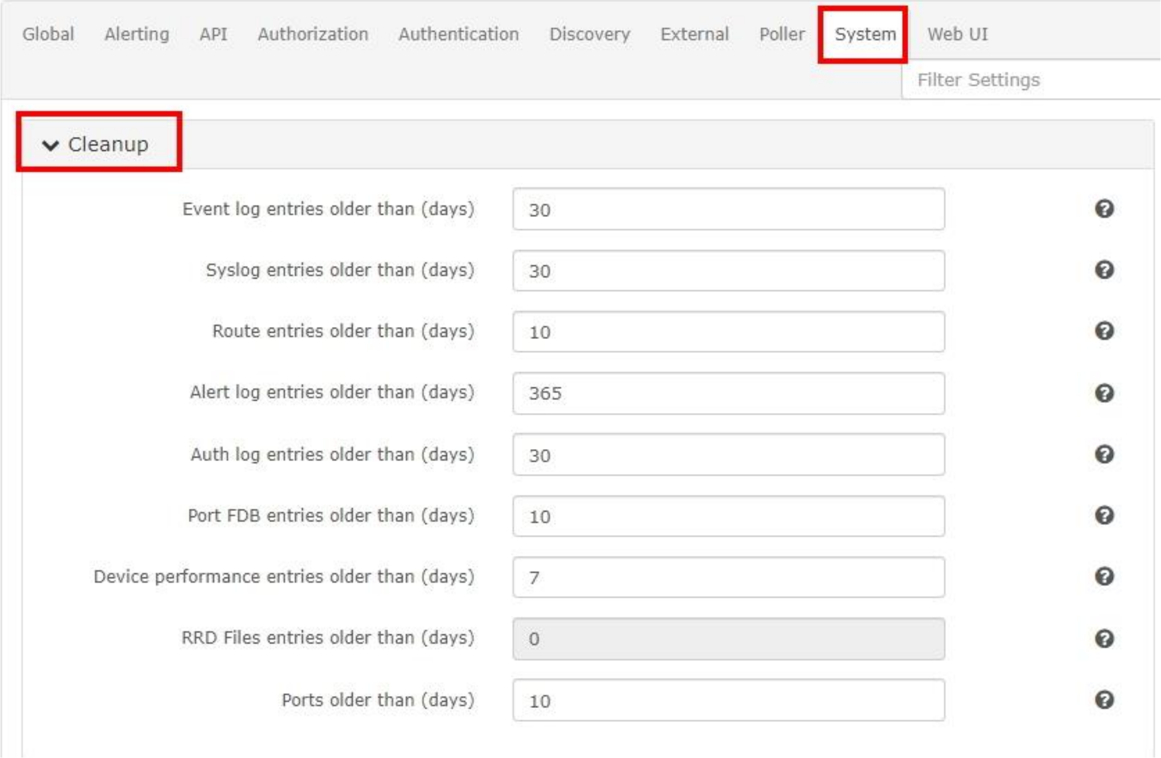
SMTP Auth password: ••••••••••••••••

- 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.



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**

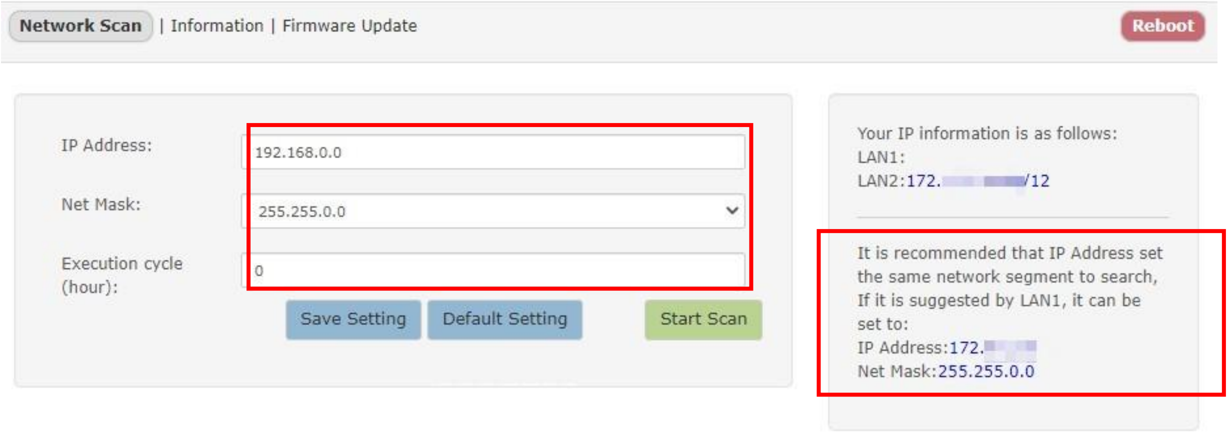
Please be aware that [**RRD Files**] is **NOT** set by default. This option will remove any RRD files that have not been updated for the set amount of days automatically - **only enable** this if you are comfortable with that happening. (All active RRD files are updated every polling period.)

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: Plugins Network Scan

Step 1: To [Plugins] > [ICPDAS] > [Network Scan] Input your network segment, netmask and excution cycle.



IP Address: 192.168.0.0

Net Mask: 255.255.0.0

Execution cycle (hour): 0

Your IP information is as follows:
LAN1:
LAN2:172.[redacted]/12

It is recommended that IP Address set the same network segment to search, If it is suggested by LAN1, it can be set to:
IP Address:172.[redacted]
Net Mask:255.255.0.0

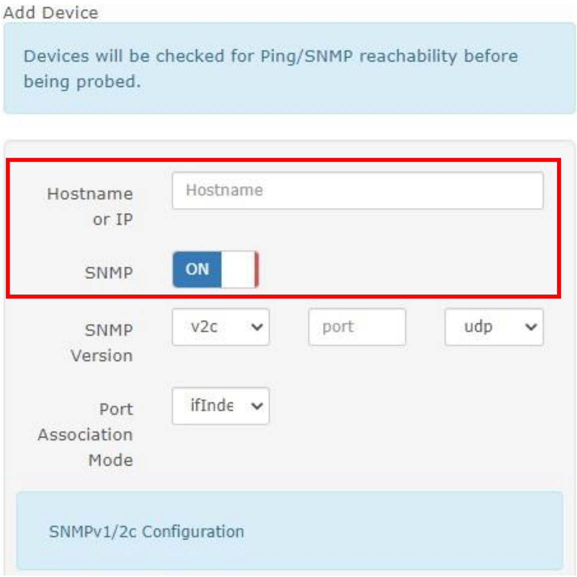
Note:

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

Step 2: Click Save Setting **and** Start Scan **to start automatic search.**

Method 2: Add Device

Step 1: To [Device] > [Add Device] Input Hostname or IP address, and on the ON **SNMP button.**



Add Device

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

Hostname or IP: Hostname

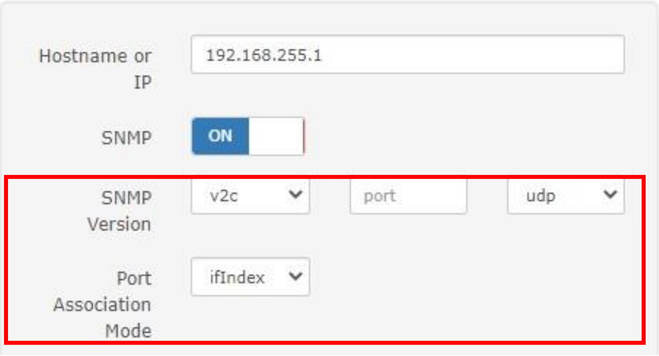
SNMP: ON

SNMP Version: v2c | port | udp

Port Association Mode: ifInde

SNMPv1/2c Configuration

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



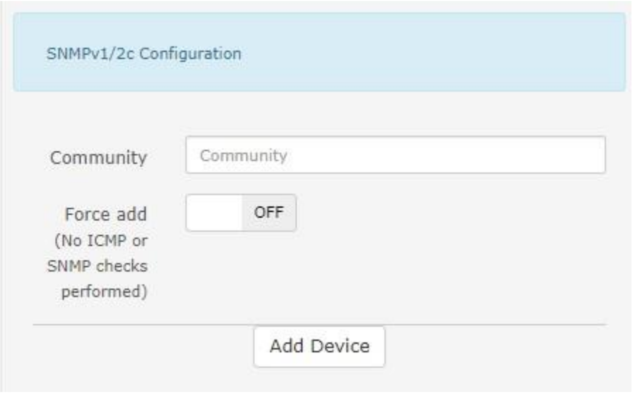
Hostname or IP: 192.168.255.1

SNMP: ON

SNMP Version: v2c | port | udp

Port Association Mode: ifIndex

Step 3: Fill in the following information according to the selected version, and then press the Add Device 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: Community

Force add (No ICMP or SNMP checks performed): OFF

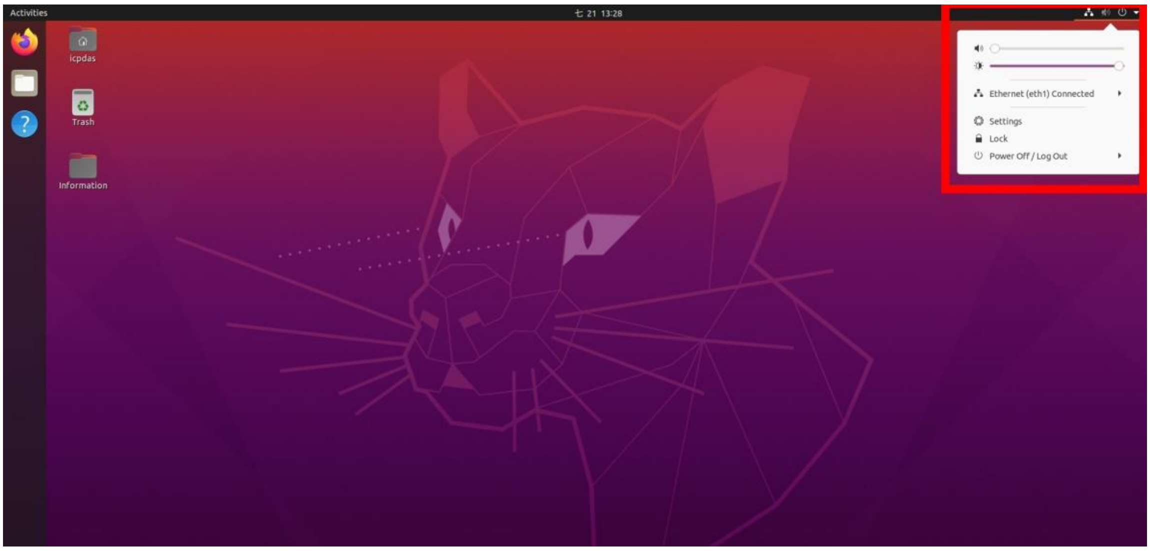
Note：

- 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.

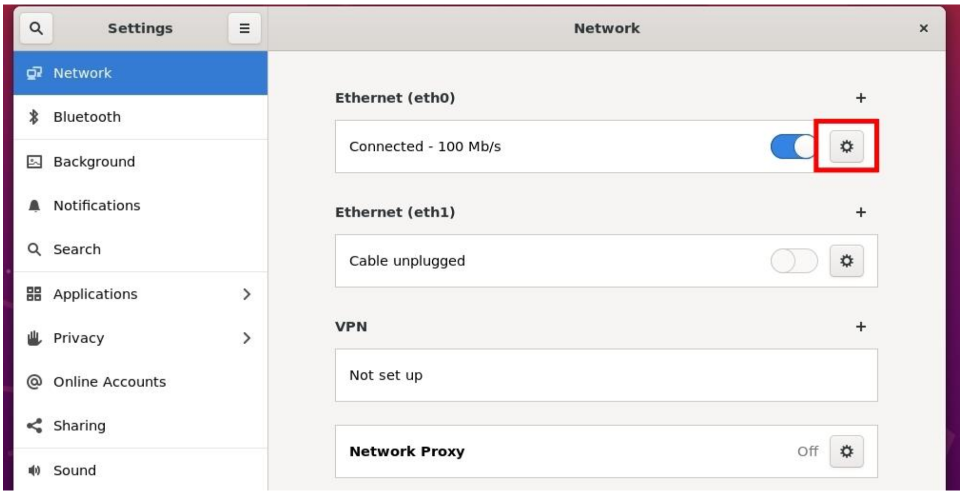
Q07: How to Change Your IP Address on Linux?

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]

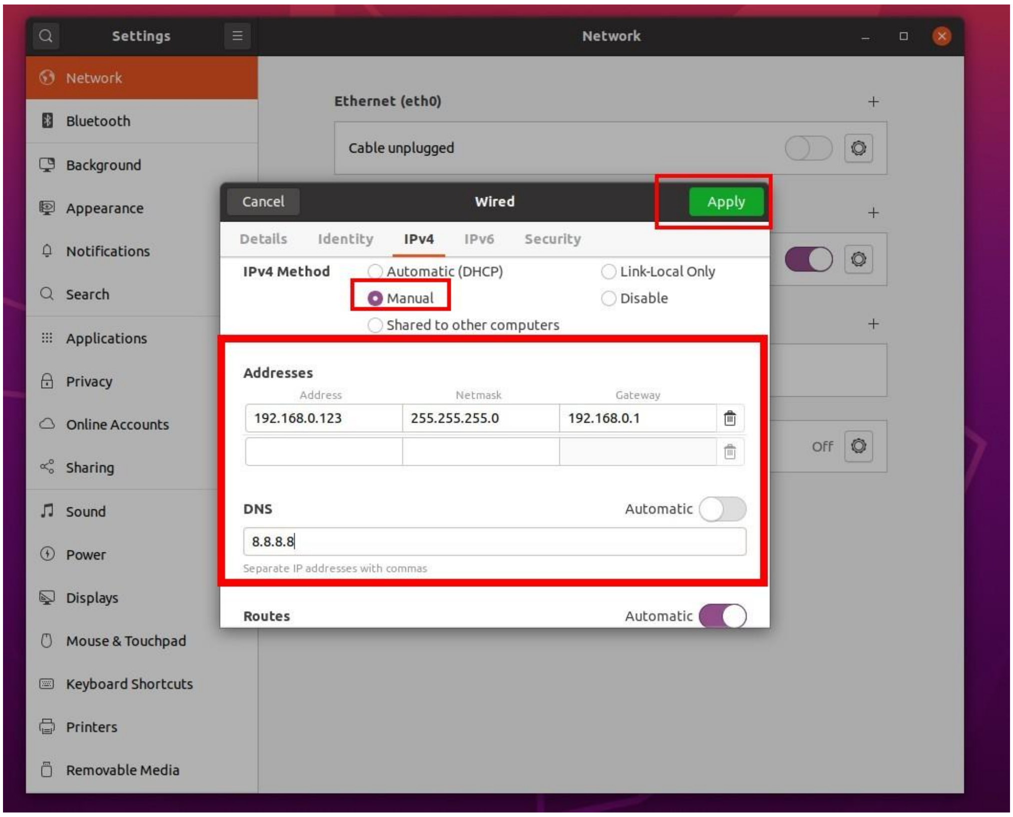


Step2: To [Setting] > [Network] > Click on the ⚙ icon of the interface you would like to set an IP address.



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].



IPv4 Method: ○ Automatic (DHCP) ● Manual ○ Shared to other computers ○ Link-Local Only ○ Disable

Addresses

Address	Netmask	Gateway
192.168.0.123	255.255.255.0	192.168.0.1

DNS Automatic: off

8.8.8.8

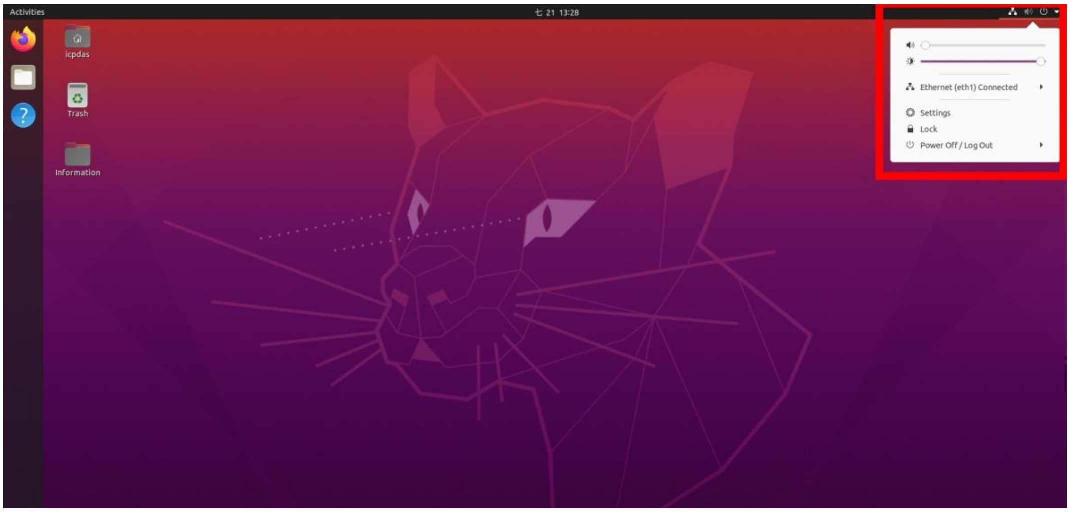
Separate IP addresses with commas

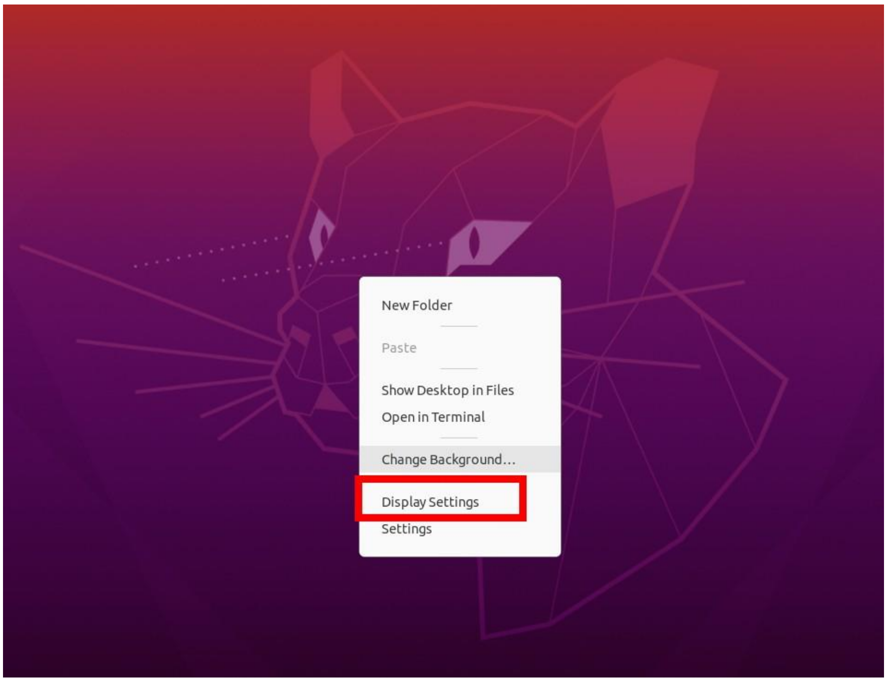
Routes Automatic: on

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.

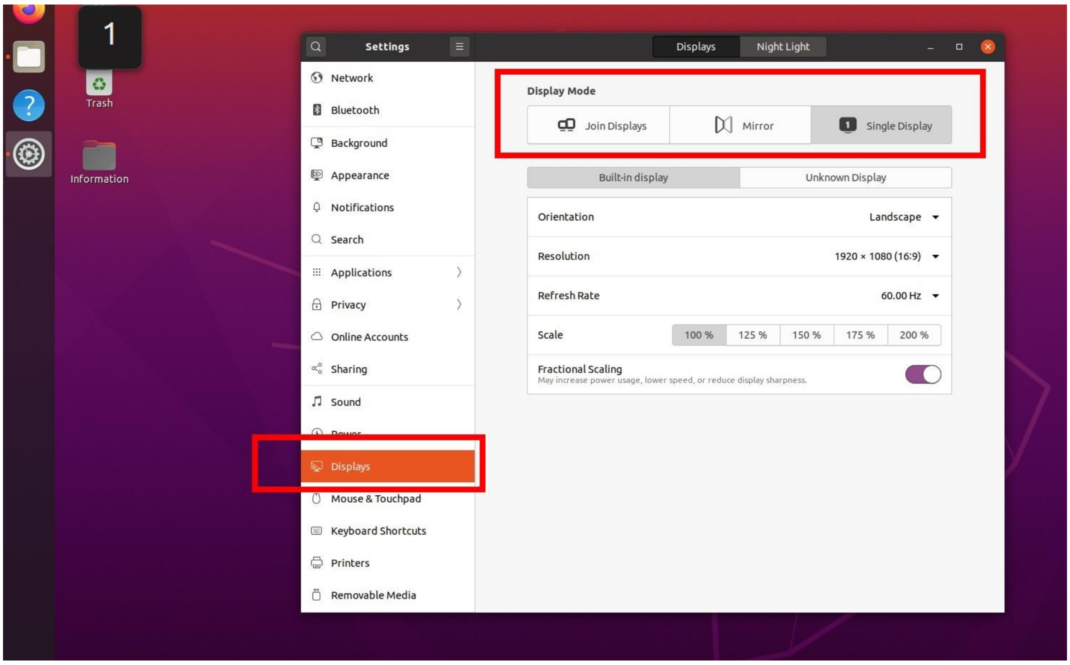
Step1: To Click the icon in the upper right corner and select [Setting] or click the right mouse button > select [Display Settings]





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

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



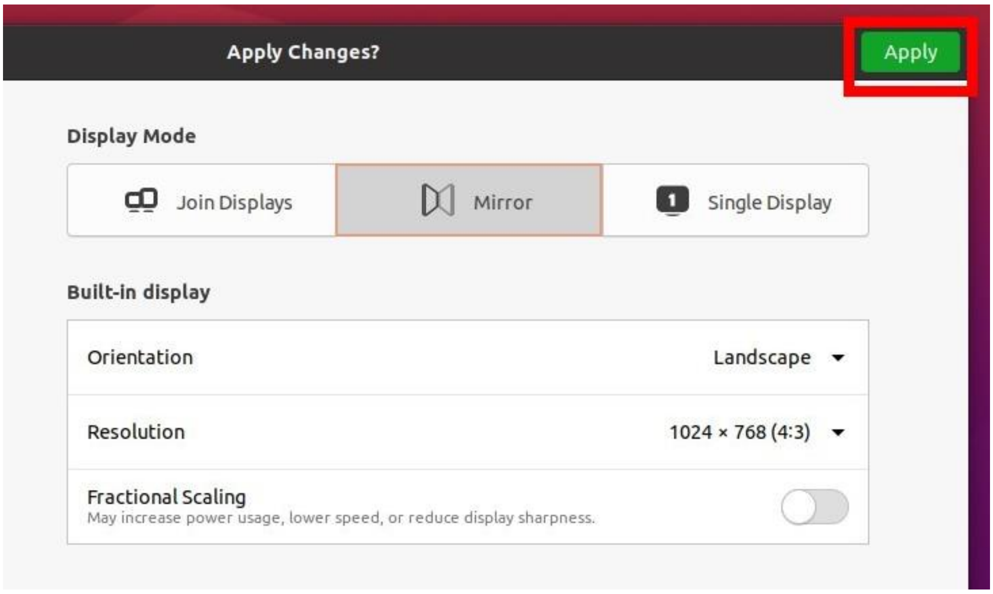
Orientation: Landscape

Resolution: 1920 × 1080 (16:9)

Refresh Rate: 60.00 Hz

Scale: 100 %

Fractional Scaling
May increase power usage, lower speed, or reduce display sharpness.



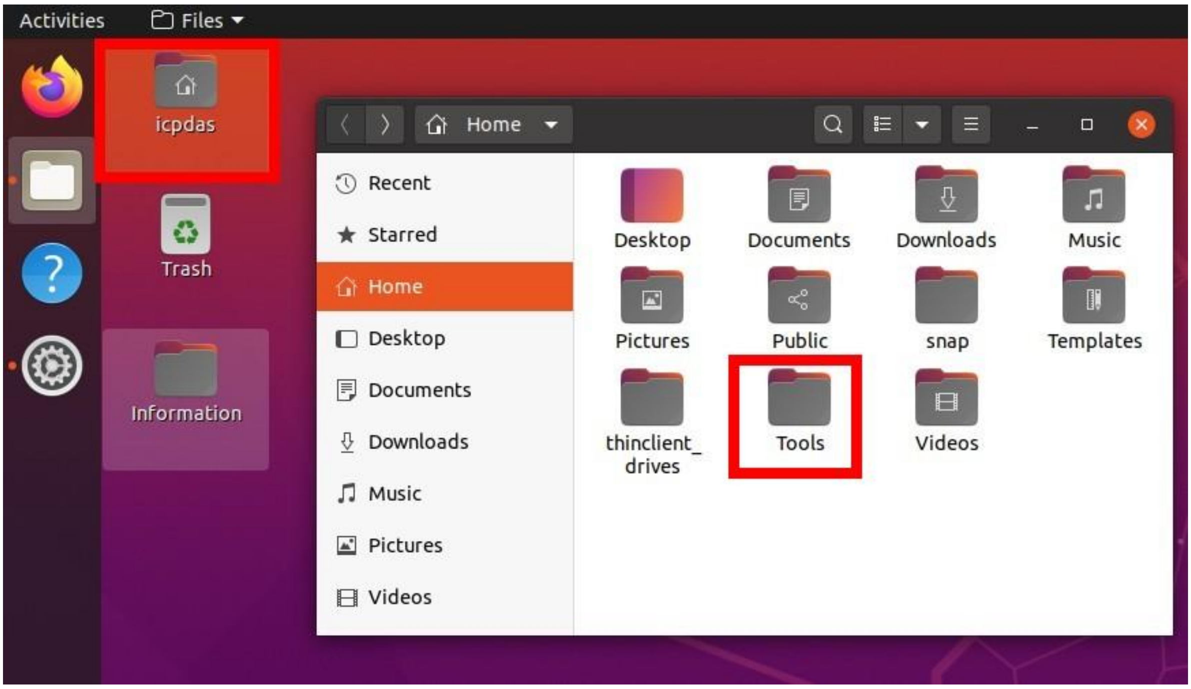
Display Mode

Join Displays | Mirror | Single Display

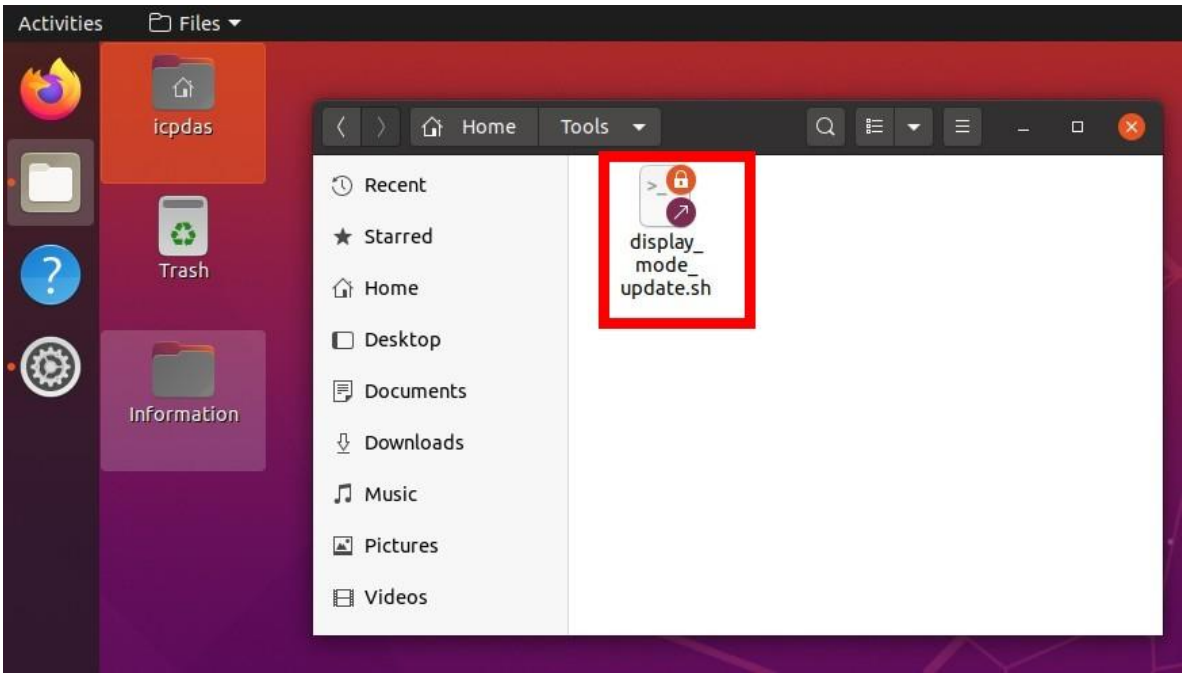
Built-in display

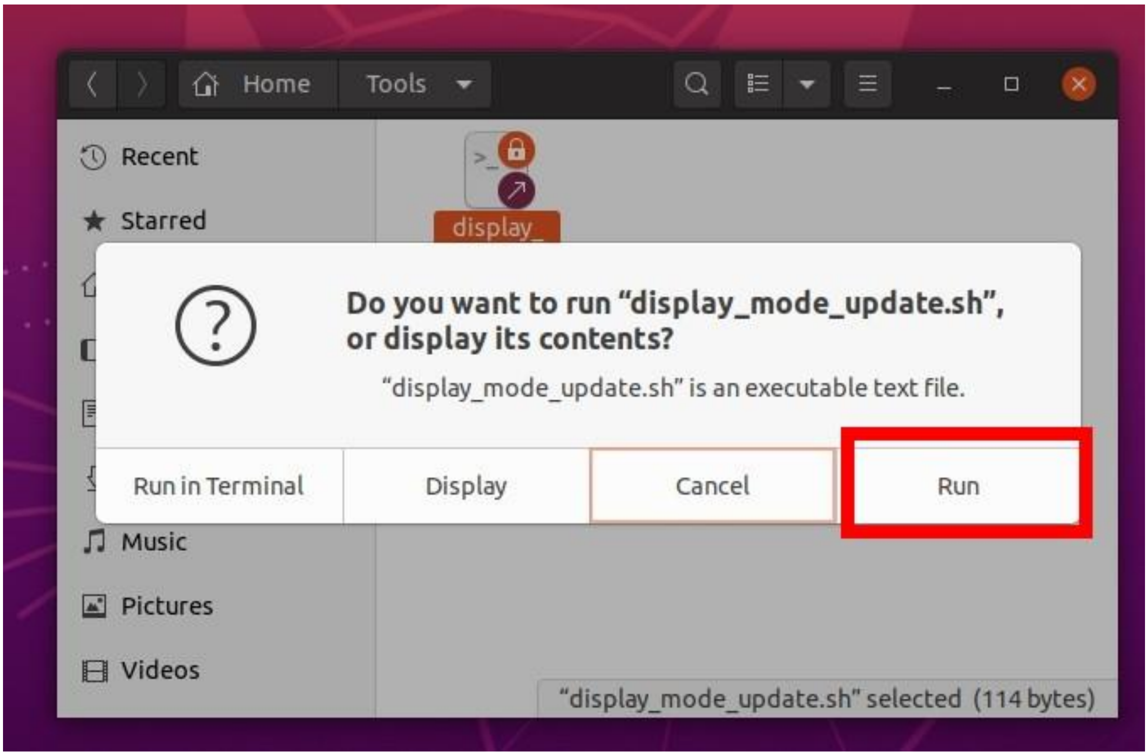
Orientation	Landscape
Resolution	1024 × 768 (4:3)
Fractional Scaling May increase power usage, lower speed, or reduce display sharpness.	

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]





Do you want to run “display_mode_update.sh”, or display its contents?

“display_mode_update.sh” is an executable text file.

“display_mode_update.sh” selected (114 bytes)

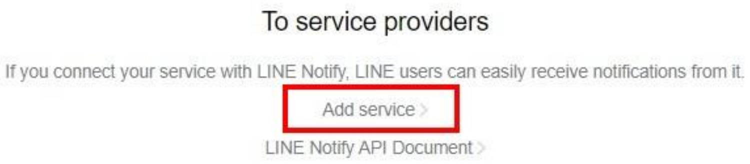
Q09: How to set up LINE Notify for alert transmission and rules ?

A09: Before setting up, you need to apply for a token at the Line Notify website.

If you already have a LINE Notify token, you can skip to Step7.

● Add new LINE Notify service

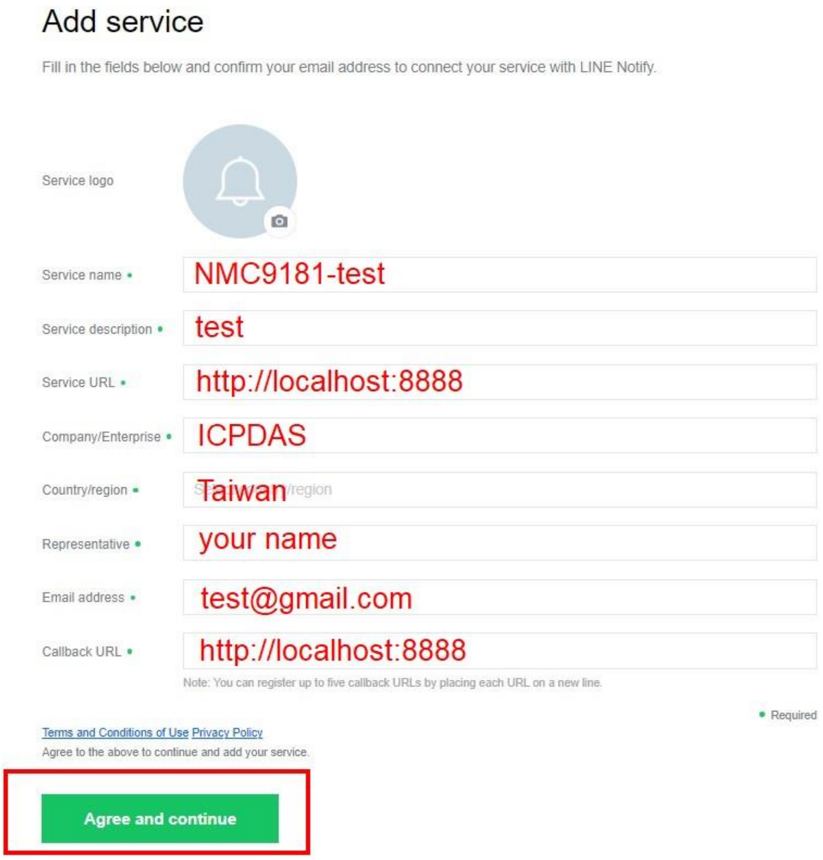
Step1: Go to Line Notify website https://notify-bot.line.me/en/ , and click [Add Service]



To service providers

If you connect your service with LINE Notify, LINE users can easily receive notifications from it.

Step2: Please complete the following information and refer to the example below, and click [Agree and continue]



Add service

Fill in the fields below and confirm your email address to connect your service with LINE Notify.

Service logo	
Service name •	NMC9181-test
Service description •	test
Service URL •	http://localhost:8888
Company/Enterprise •	ICPDAS
Country/region •	Taiwan
Representative •	your name
Email address •	test@gmail.com
Callback URL •	http://localhost:8888

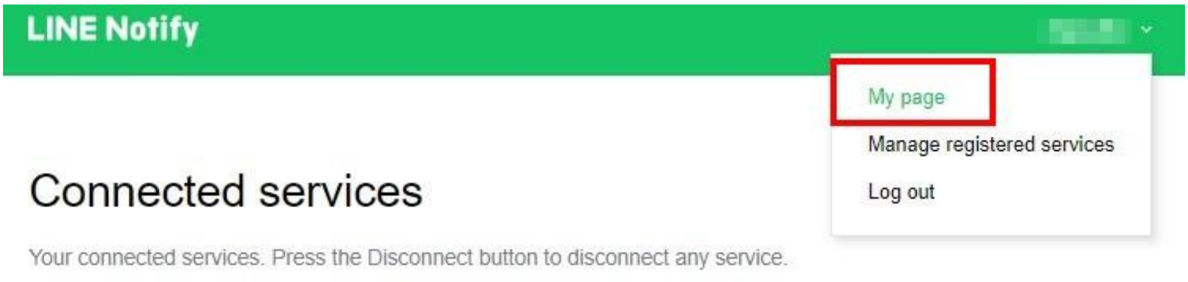
Note: You can register up to five callback URLs by placing each URL on a new line.

• Required

Terms and Conditions of Use Privacy Policy

Agree to the above to continue and add your service.

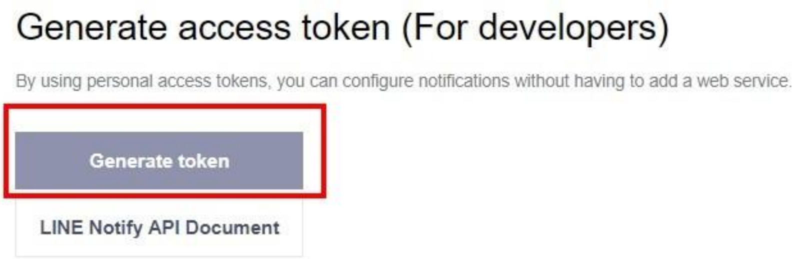
Step3: Find your personal information in the upper right corner and click [My Page].



Connected services

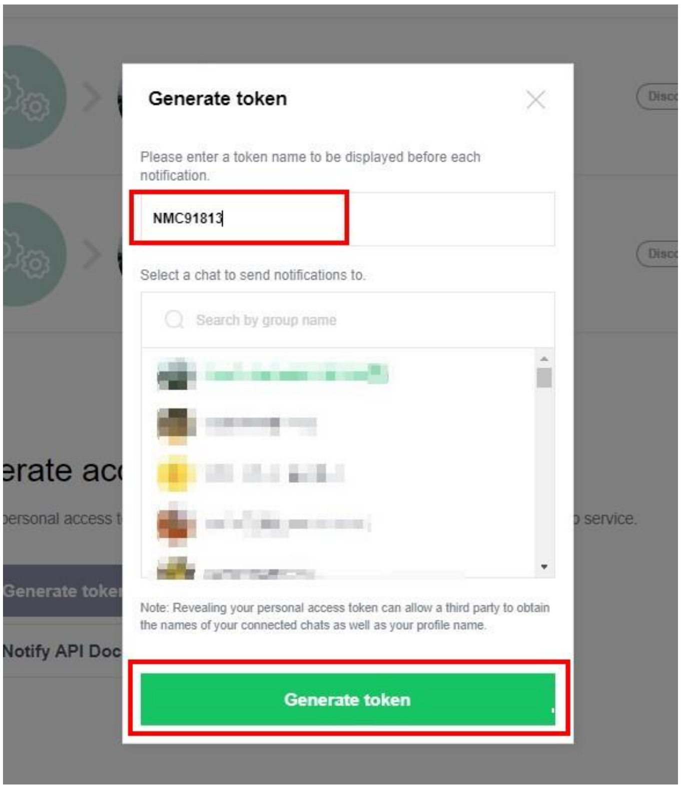
Your connected services. Press the Disconnect button to disconnect any service.

Step4: Click [Generate token], enter the name of the token displayed before each notification and select a chat to send the notification to.



Generate access token (For developers)

By using personal access tokens, you can configure notifications without having to add a web service.



Generate token

Please enter a token name to be displayed before each notification.

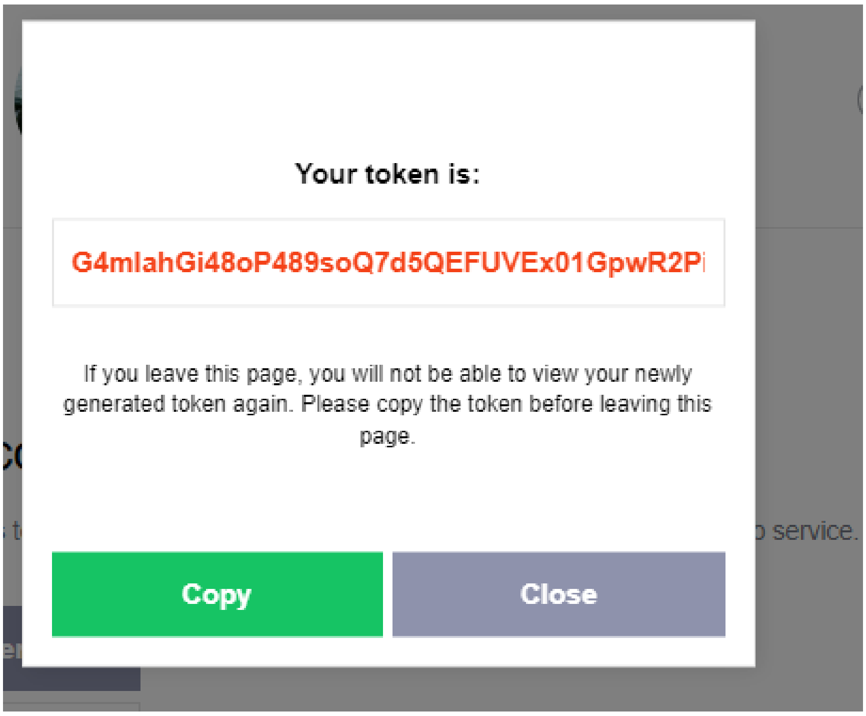
NMC91813

Select a chat to send notifications to.

Note: Revealing your personal access token can allow a third party to obtain the names of your connected chats as well as your profile name.

Step5: Copy and back up your token.

※ Note: Please copy the token before leaving this page.

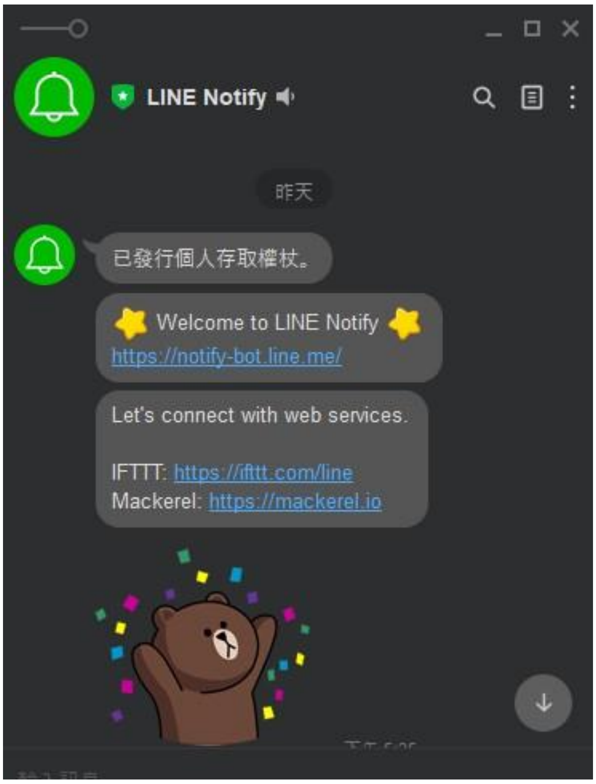


Your token is:

G4mlahGi48oP489soQ7d5QEFUVEx01GpwR2Pi

If you leave this page, you will not be able to view your newly generated token again. Please copy the token before leaving this page.

Step6: After completion, you can go to the Line app to check if there is a Line Notify message.



已發行個人存取權杖。

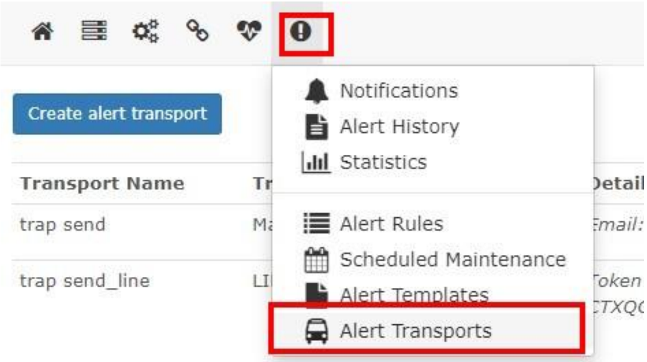
Welcome to LINE Notify
https://notify-bot.line.me/

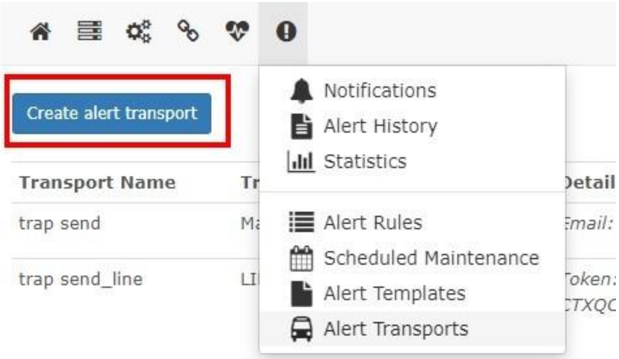
Let's connect with web services.

IFTTT: https://ifttt.com/line
Mackerel: https://mackerel.io

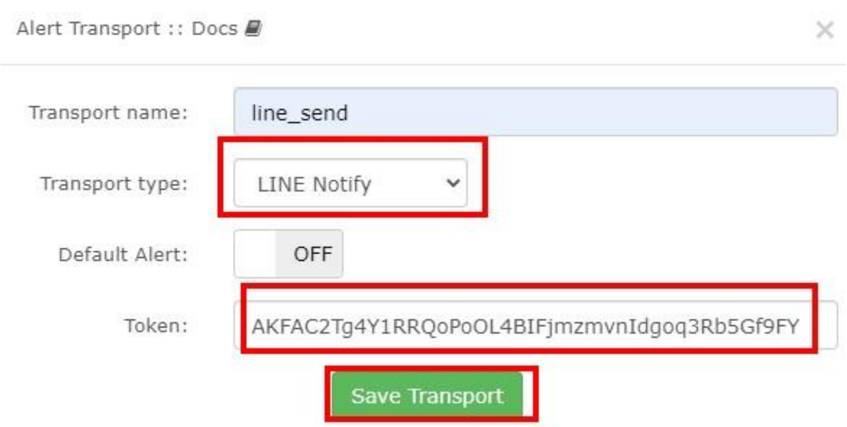
● Add new Alert Transport

Step7: To [Alert] > [Alert Transports], click [Create alert transport]





Step8: Transport name select [Line Notify] and paste your [Line Notify Token], then click [Save Transport]


Alert Transport :: Docs

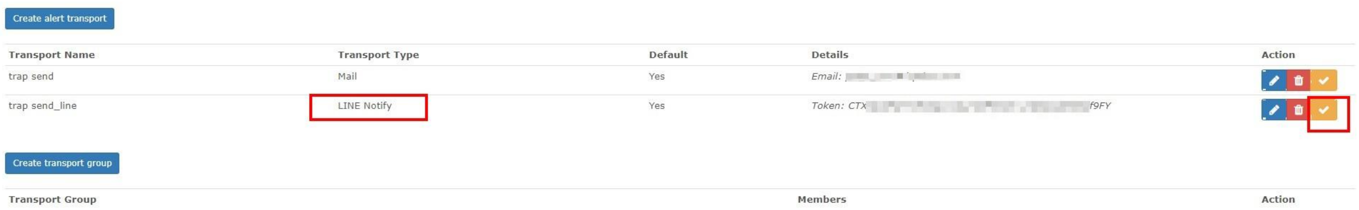
Transport name: line_send

Transport type: LINE Notify

Default Alert: OFF

Token: AKFAC2Tg4Y1RRQoPoOL4BIFjmzmvnIdgoq3Rb5Gf9FY

Step9: To [Alert] > [Alert Transports] and click ✓ test send.



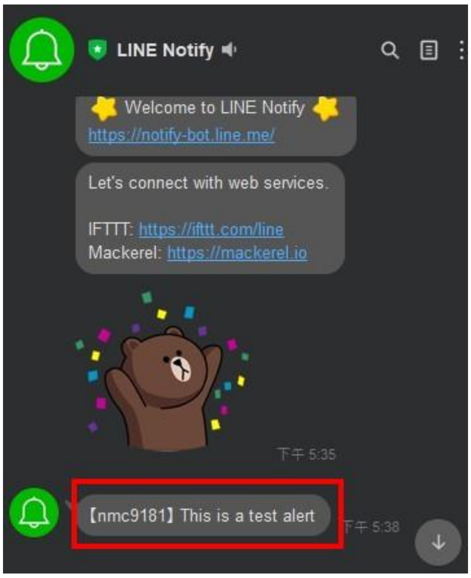
Create alert transport

Transport Name	Transport Type	Default	Details	Action
trap send	Mail	Yes	Email: [redacted]	✎ 🗑 ✓
trap send_line	LINE Notify	Yes	Token: CTX[redacted]f9FY	✎ 🗑 ✓

Create transport group

Transport Group	Members	Action

Check your line message.



Welcome to LINE Notify
https://notify-bot.line.me/

Let's connect with web services.

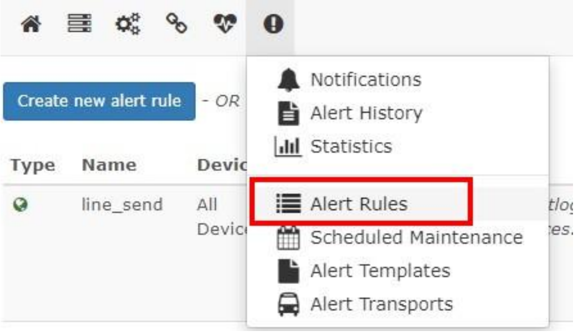
IFTTT: https://ifttt.com/line
Mackerel: https://mackerel.io

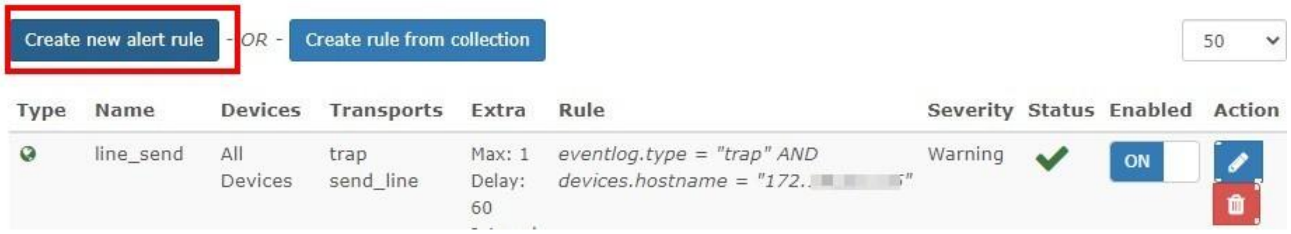
下午 5:35

【nmc9181】This is a test alert

下午 5:38

Step10: To [Alert] > [Alert Rules] and click [Create new alert rule].



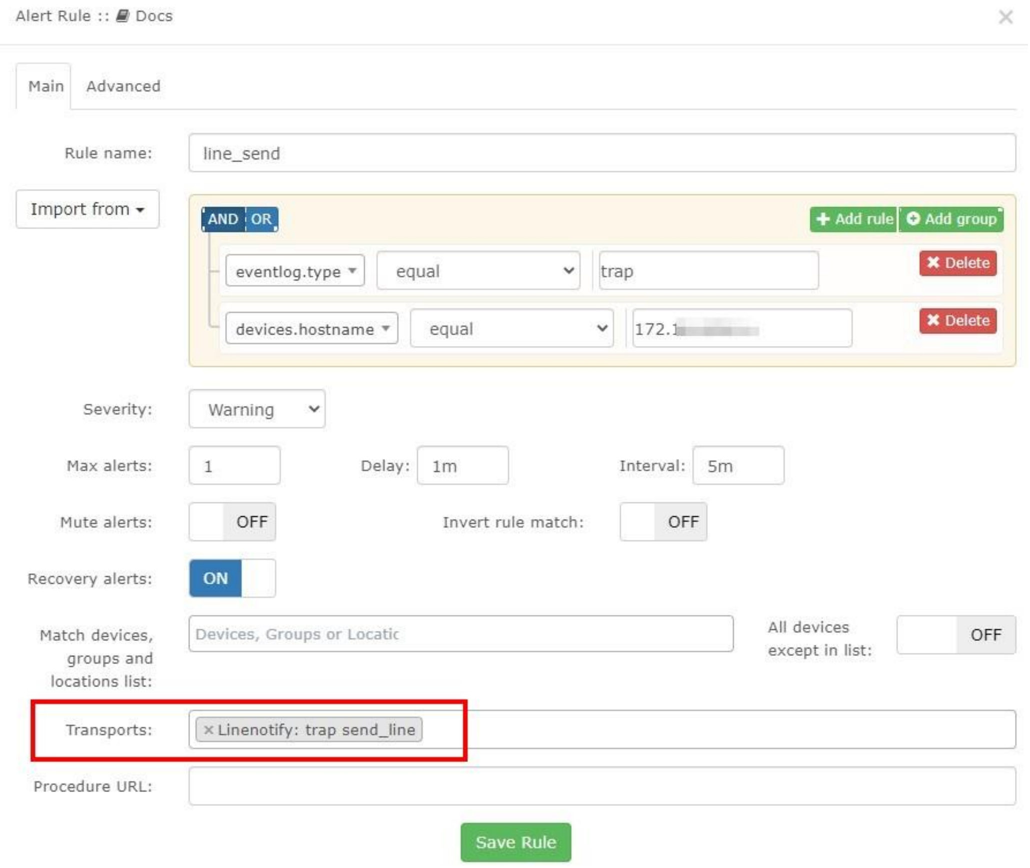


Create new alert rule - OR - Create rule from collection

50

Type	Name	Devices	Transports	Extra	Rule	Severity	Status	Enabled	Action
●	line_send	All Devices	trap send_line	Max: 1 Delay: 60	*eventlog.type = "trap" AND devices.hostname = "172.[redacted]"*	Warning	✓	ON	✎ 🗑

Step11: Fill in the alarm rules you want to set, and select the alert transport you set in [Transports] > [Save Rule]



Rule name: line_send

eventlog.type ▾ | equal | trap

devices.hostname ▾ | equal | 172.1[redacted]

Severity: Warning

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

Mute alerts: OFF Invert rule match: OFF

Recovery alerts: ON

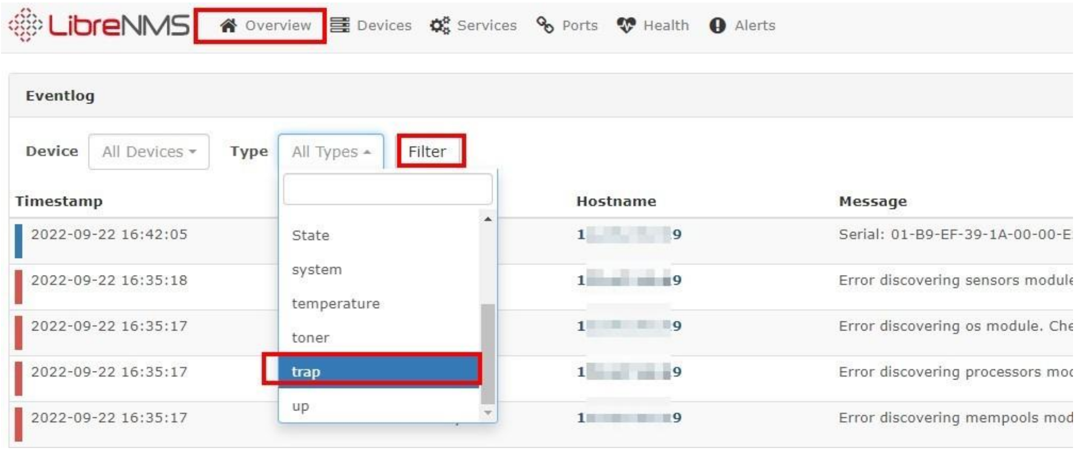
Match devices, groups and locations list: Devices, Groups or Locatic All devices except in list: OFF

Transports: × Linenotify: trap send_line

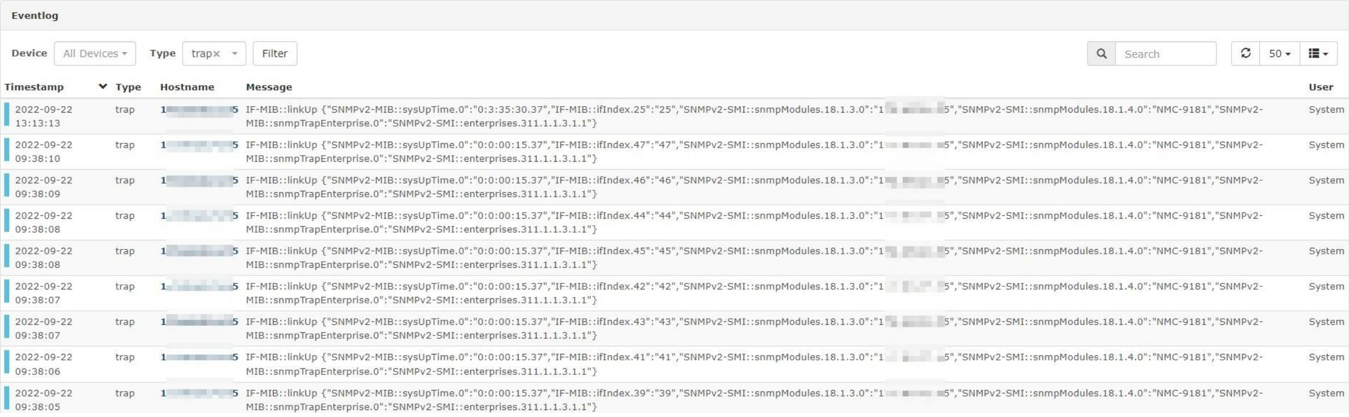
Procedure URL:

Q10: How to set the alarm rules for SNMP Trap ?

A10: The SNMP traps received by the NMC-9181 can be viewed at [Overview] > [Event log]. Set up the alarm rules can refer to the following steps



```
Timestamp             Hostname        Message
2022-09-22 16:42:05   1[redacted]9    Serial: 01-B9-EF-39-1A-00-00-E
2022-09-22 16:35:18   1[redacted]9    Error discovering sensors module
2022-09-22 16:35:17   1[redacted]9    Error discovering os module. Che
2022-09-22 16:35:17   1[redacted]9    Error discovering processors moc
2022-09-22 16:35:17   1[redacted]9    Error discovering mempools mod
```



Eventlog

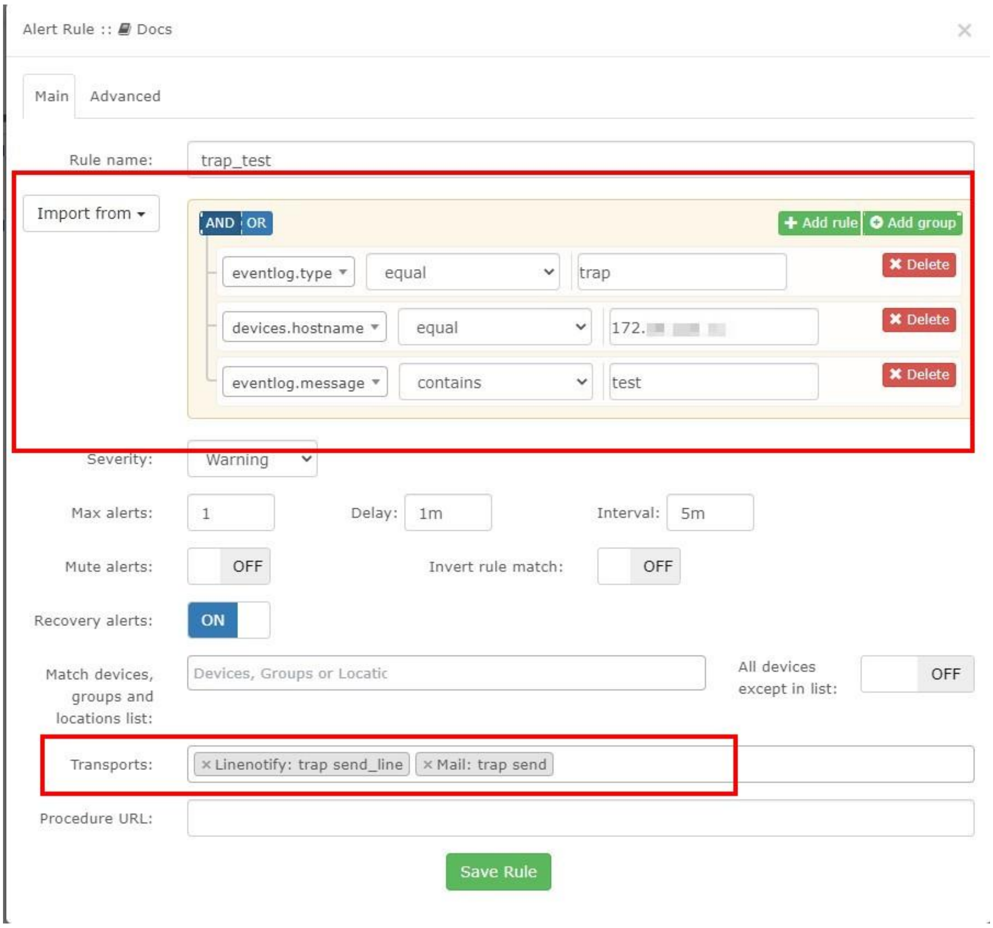
Device: All Devices | Type: trap× | Filter | Search | 50

Timestamp	Type	Hostname	Message	User
2022-09-22 13:13:13	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:3:35:30.37","IF-MIB::ifIndex.25":"25","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:10	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.47":"47","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:09	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.46":"46","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:08	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.44":"44","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:08	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.45":"45","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:07	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.42":"42","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:07	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.43":"43","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:06	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.41":"41","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System
2022-09-22 09:38:05	trap	1[redacted]5	IF-MIB::linkUp {"SNMPv2-MIB::sysUpTime.0":"0:0:00:15.37","IF-MIB::ifIndex.39":"39","SNMPv2-SMI::snmpModules.18.1.3.0":"1[redacted]5","SNMPv2-SMI::snmpModules.18.1.4.0":"NMC-9181","SNMPv2-MIB::snmpTrapEnterprise.0":"SNMPv2-SMI::enterprises.311.1.1.3.1.1"}	System

Step1: To [Alert] > [Alert Rules] and click [Create new alert rule].

Step2: Click [Add rule] > enter [eventlog.type] > [equal] > [trap].

If you want to set more detailed rule conditions, you can set [devices.hostname], [eventlog.message] , etc. and if you have [Alert Transports] set up, you can choose to add them, the example is shown below



Alert Rule :: Docs

Main | Advanced

Rule name: trap_test

Import from

AND | OR — Add rule | Add group

- eventlog.type — equal — trap — Delete
- devices.hostname — equal — 172.[redacted] — Delete
- eventlog.message — contains — test — Delete

Severity: Warning

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

Mute alerts: OFF | Invert rule match: OFF

Recovery alerts: ON

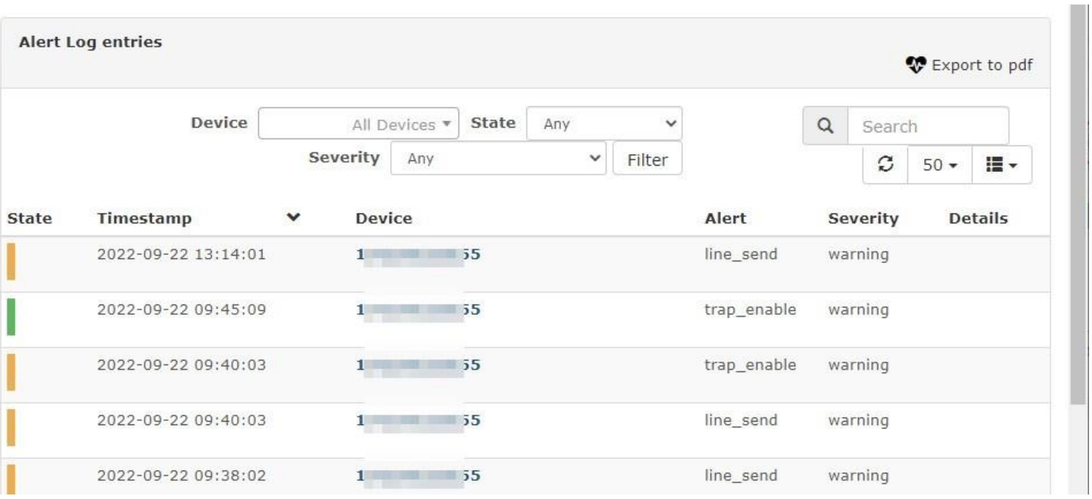
Match devices, groups and locations list: Devices, Groups or Locatic | All devices except in list: OFF

Transports: × Linenotify: trap send_line | × Mail: trap send

Procedure URL:

Save Rule

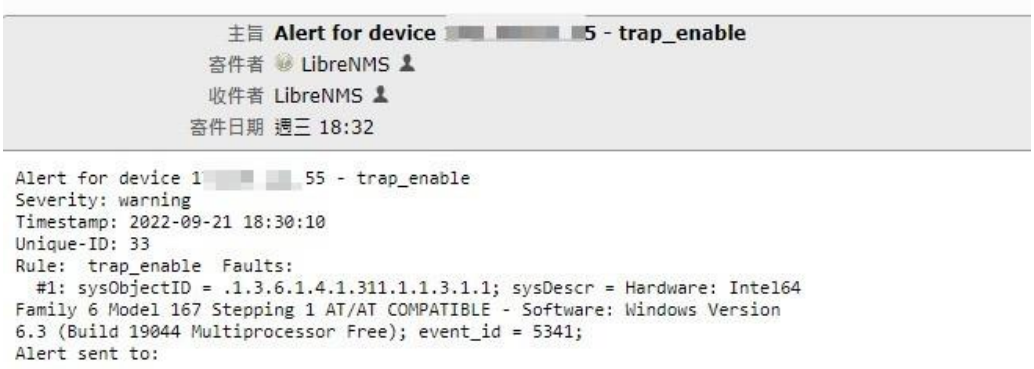
Step3: When the set alarm is triggered, you can go to [Alert] > [Alert History] to view it.



Alert Log entries

State	Timestamp	Device	Alert	Severity	Details
🟧	2022-09-22 13:14:01	1[redacted]55	line_send	warning	
🟩	2022-09-22 09:45:09	1[redacted]55	trap_enable	warning	
🟧	2022-09-22 09:40:03	1[redacted]55	trap_enable	warning	
🟧	2022-09-22 09:40:03	1[redacted]55	line_send	warning	
🟧	2022-09-22 09:38:02	1[redacted]55	line_send	warning	

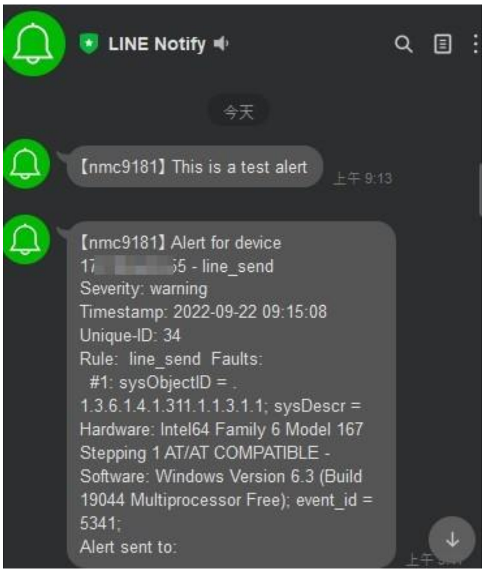
- **Go to the MAIL you have set up to check the alert message**



主旨 **Alert for device [redacted]5 - trap_enable**
寄件者 LibreNMS
收件者 LibreNMS
寄件日期 週三 18:32

```
Alert for device 1[redacted]55 - trap_enable
Severity: warning
Timestamp: 2022-09-21 18:30:10
Unique-ID: 33
Rule:  trap_enable  Faults:
  #1: sysObjectID = .1.3.6.1.4.1.311.1.1.3.1.1; sysDescr = Hardware: Intel64
Family 6 Model 167 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version
6.3 (Build 19044 Multiprocessor Free); event_id = 5341;
Alert sent to:
```

- **Go to the LINE you have set up to check the alert message**



【nmc9181】This is a test alert 上午 9:13

```
【nmc9181】Alert for device
17[redacted]55 - line_send
Severity: warning
Timestamp: 2022-09-22 09:15:08
Unique-ID: 34
Rule:  line_send  Faults:
  #1: sysObjectID = .
1.3.6.1.4.1.311.1.1.3.1.1; sysDescr =
Hardware: Intel64 Family 6 Model 167
Stepping 1 AT/AT COMPATIBLE -
Software: Windows Version 6.3 (Build
19044 Multiprocessor Free); event_id =
5341;
Alert sent to:
```

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
1.0.2	2022-09-22	Add FAQ Q09、Q10