# FMX Series

# Network Management User Manual

Copyright © 2009-2019 FS.COM All Rights Reserved.

# Contents

# Preface

## Overview

| Chapter Number | Description |
|---|---|
| Preface | This chapter introduces contents, version information and explanation of special symbols. |
| Chapter 1 NMS System Overview | This chapter introduces the functions of NMS system. |
| Chapter 2 NMS System Installation and Startup | This chapter describes how to install the NMS software and the startup, initialization and shutdown of the NMS system. |
| Chapter 3 Interface Operation of NMS System | This chapter introduces the user login, exit and password change in the NMS interface. |
| Chapter 4 System Management | This chapter introduces the system configuration of NMS system. |
| Chapter 5 Alarm Management | This chapter introduces management of current and history alarms. |
| Chapter 6 Performance Management | This chapter introduces management of current and history performances. |
| Chapter 7 Log Management | This chapter introduces log management. |
| Chapter 8 Security Management | This chapter introduces user and user group management. |
| Chapter 9 Routine Maintenance | This chapter introduces the routine maintenance of NMS system. |
| Chapter 10 Common Problem | This chapter introduces how to deal with common problems. |
| Abbreviation | This chapter introduces the specific meaning of abbreviations. |

## Product Version

| Product Number | Version Number |
|---|---|
| FMX-100G-CH2U | V1.0.0 |

## Content Introduction

This manual mainly introduces the general operation of the network management platform, including installation and startup of the NMS system, login, exit, password change, security management, system management of network element, alarm management, log management, performance management, routine maintenance of the NMS system, common problems and so on.

## Explanation of Special Symbols

The following symbols may appear in this manual, which respectively represent the following meanings:

| Symbol | Description |
|---|---|
| ⚡ | Special attention should be paid to the content. If the operation is improper, it may cause serious injury to the person. |
| ⚠ | It reminds the matters for attention. Improper operation may cause loss of data or damage to the device. |
| 💡 | It represents the operation or information that requires special attention to ensure the success of the operation or the normal work of the device. |
| 🔑 | A skill or a knack which helps to solve a problem and save time. |
| 📝 | The necessary supplement and explanation for the description of the text. |

1. It is not allowed to make modification if the input box or the drop-down box is grayed out.
2. The add, delete, modify and refresh buttons are all on the toolbar.
3. One and only one data in the table must be selected first while doing the modification operation.
4. At least one data in the table must be selected while doing the deletion operation.
5. The refresh button is used to refresh the table and the form. There are two refresh operations on the toolbar. When it shows "Refresh Table" on 🔄 icon, it will refresh the table. When it shows "Refresh Form" on 🔄 icon, it will refresh the form.

# Chapter 1 NMS System Overview

## 1.1. NMS System Introduction

FMX NMS adopts B/S architecture. Only server software needs to be deployed while installing. It uses the browser as the client. HTTP protocol is used for communication between server and client.

## 1.2. Functional Characteristics

FMX NMS system adopts advanced and mature network management architecture, which provides a whole set of Java-based cross platform development tools, modules and API. It can easily integrate with multiple third-party systems. It is an integrated network management system designed according to the bottom-up rule, which is highly user oriented, carrier-grade and cross-platform. Moreover, it provides a comprehensive solution for network management.

FMX NMS system can meet various needs of users:

- Telecom operators and manufacturers can establish network elements and network management systems.
- Service providers can establish network management and operation support systems.
- Enterprises and independent software developers can build application program management solutions.

The device managed by FMX NMS system includes all kinds of IP devices in backbone layer, convergence layer and access layer. At present, the management of softswitch, integrated access server, digital subscriber loop, Ethernet switch, router and ADSL device has been implemented.

FMX NMS system covers four layers of TMN management:

- Network Element Layer;
- Network Element Management Layer;
- Network Management Layer;
- Service Management Layer.

FMX NMS system adopts friendly and full graphical interface, which is simple and easy to operate.

FMX NMS system provides a powerful operation and management tool for network administrators. The network management system can visually display the network view, monitor and manage multiple network devices in the network, and ensure the reliable, safe and efficient operation of the network.

## 1.3. Hardware Requirements

Table 0-1 Hardware and Operating System Requirements

| | Server Configuration | Client Configuration (Browser) |
|---|---|---|
| Minimum Configuration | CPU: Frequency 2.0G<br>Memory: 4G<br>Hard Disk: >200G<br>Resolution: 1440x900<br>Operating System:<br>Windows Server 2008 | CPU: Frequency 2.0G<br>Memory: 4G<br>Hard Disk: >100G<br>Resolution: 1440x900<br>Operating System: Windows 7 |
| Recommended Configuration | CPU: Frequency 2.4GHz and above<br>Memory: >8G<br>Resolution: 1920x1080<br>Hard Disk: >500GB<br>Operating System:<br>Windows Server 2008, Windows Server 2012 | CPU: Frequency 2.4GHz and above<br>Memory: >8G<br>Resolution: >1920x1080<br>Hard Disk: >200GB<br>Operating System:<br>Windows 7, Windows 10 |

The FMX NMS system with B/S architecture does not request high requirements for the client; however, there is a certain requirement for the browser. It is recommended to adopt IE11.0 and above version or Google Chrome.

⚠ **FMX NMS management software is not available for Linux computer operation system now. But we can offer related MIB files for customers.**

## 1.4. Networking Mode

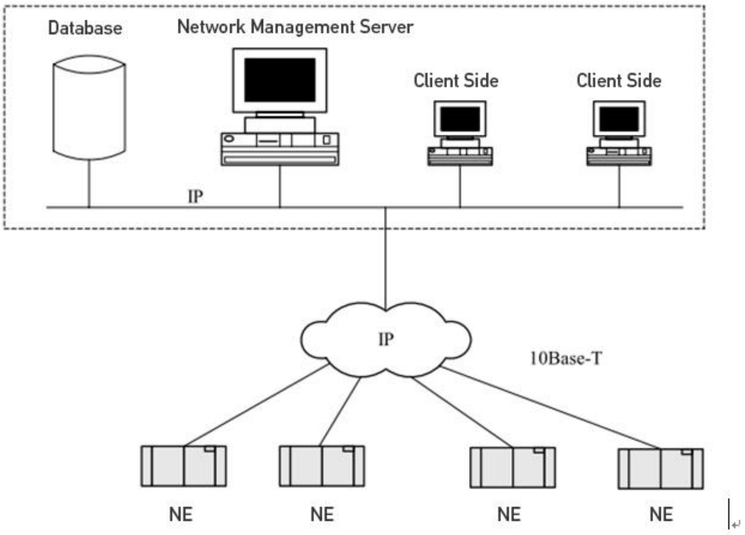


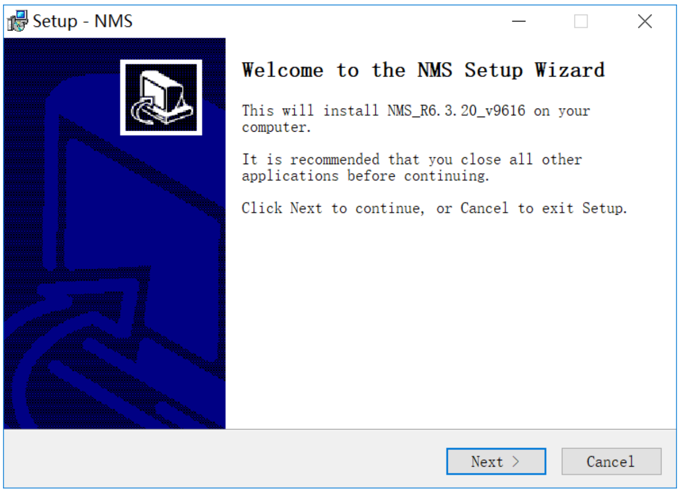
Figure 0-1 Network Diagram

# Chapter 2 NMS System Installation and Startup

## 2.1. NMS Software Installation

### Steps

1. Double click the installation program “NMS_Setup.exe” to enter the installation window. (Click OK when the welcome page pops up.)



Welcome to the NMS Setup Wizard

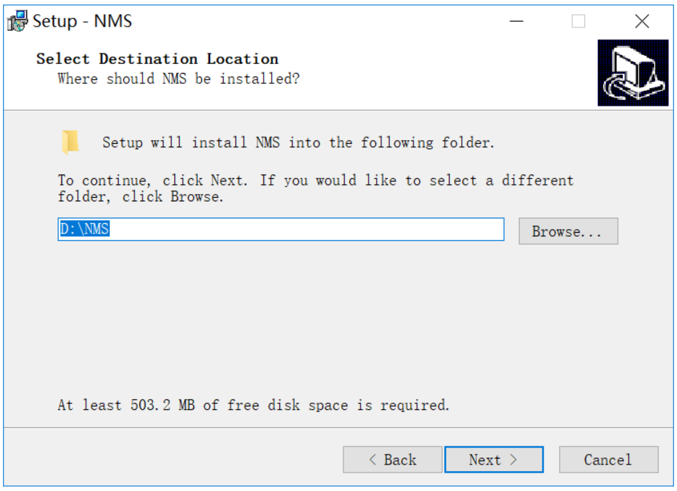
This will install NMS_R6.3.20_v9616 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 0-1 Software Installation - NMS Setup Wizard

2. Click*“Next”*to enter the next page to configure the installation path of the software. There should be no space, special or Chinese characters in the installation path. (It is not recommended to locate it in the roof directory or to install it in disks which need system management permission.)



Select Destination Location
Where should NMS be installed?

Setup will install NMS into the following folder.

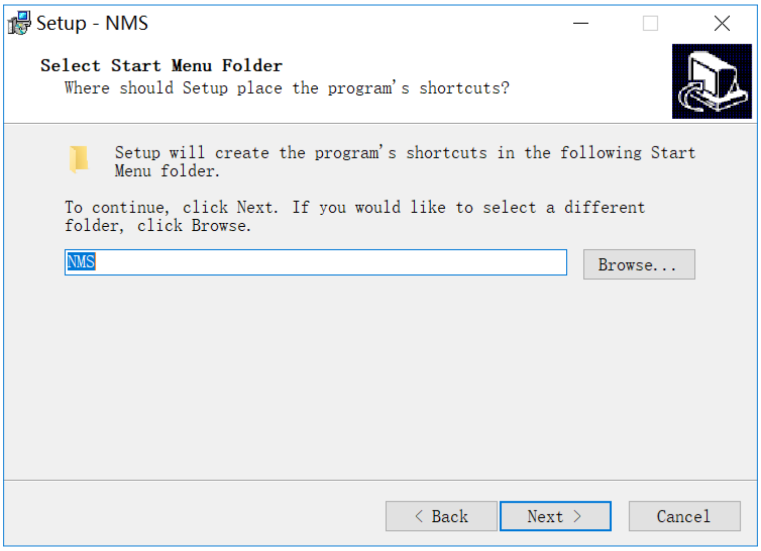
To continue, click Next. If you would like to select a different folder, click Browse.

D:\NMS

At least 503.2 MB of free disk space is required.

Figure 0-2 Software Installation-Destination Location

3. After selecting the installation path, click*“Next”.*



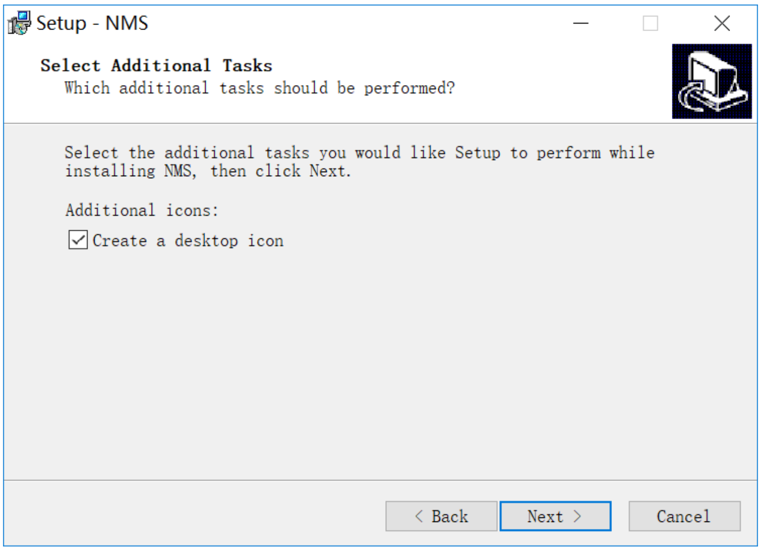
**Select Start Menu Folder**
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

NMS

Figure 0-3 Software Installation-Select Start Menu Folder



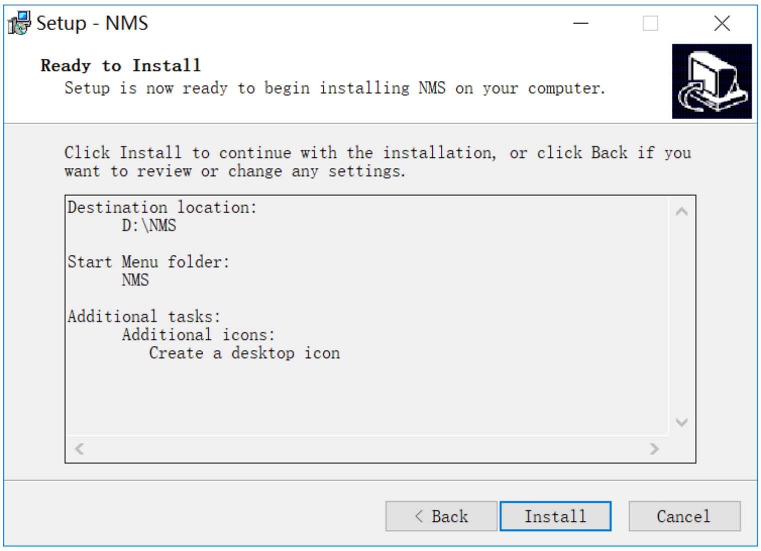
**Select Additional Tasks**
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing NMS, then click Next.

Additional icons:

☑ Create a desktop icon

Figure 0-4 Software Installation-Create A Desktop Icon



**Ready to Install**
Setup is now ready to begin installing NMS on your computer.

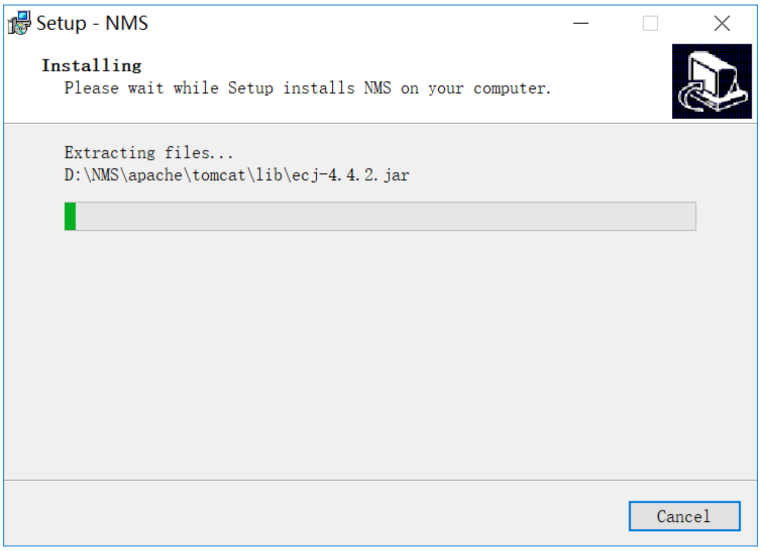
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      D:\NMS

Start Menu folder:
      NMS

Additional tasks:
      Additional icons:
         Create a desktop icon
```

Figure 0-5 Software Installation-Ready to Install

Click*"Install"*to install the software.

4. Start the installation.

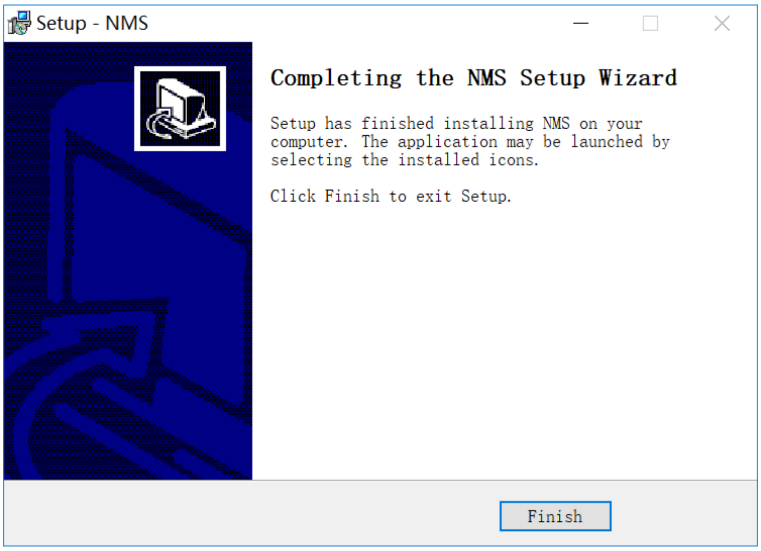


**Installing**
Please wait while Setup installs NMS on your computer.

Extracting files...
D:\NMS\apache\tomcat\lib\ecj-4.4.2.jar

Figure 0-6 Software Installation-Installing

5. The installation is successfully completed.



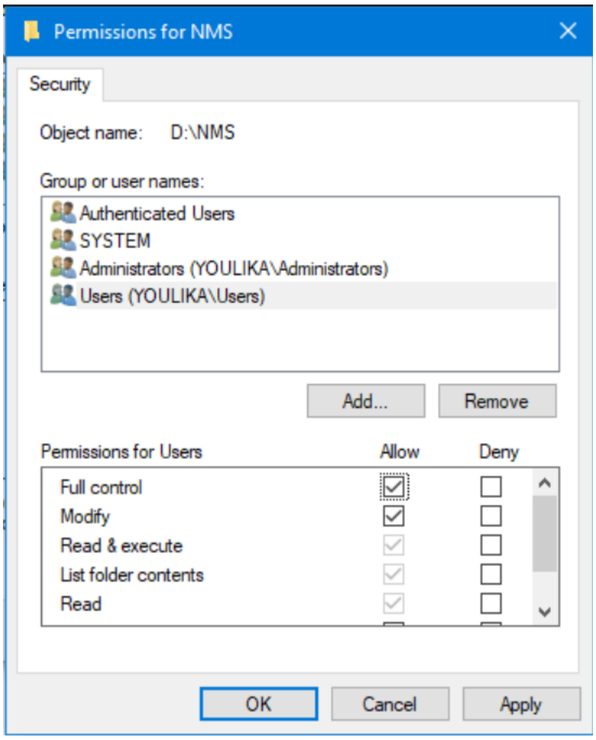
Completing the NMS Setup Wizard

Setup has finished installing NMS on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Figure 0-7 Software Installation-Completing the NMS Setup Wizard

6. If the server end software is installed in the operating system of Windows Server 2008 or Windows Server 2012, it also needs to configure the software permissions. Right click the software installation folder (e.g. D:\NMS), and select*"Properties"* menu item. Click*"Security"*tab, and select "Everyone" in the"Group or user names"list. Then click *"Edit"* and assign all the permissions (e.g. "modify", "read and execute" permissions) to "Everyone", as shown in the figure below:



Permissions for NMS

Security

Object name: D:\NMS

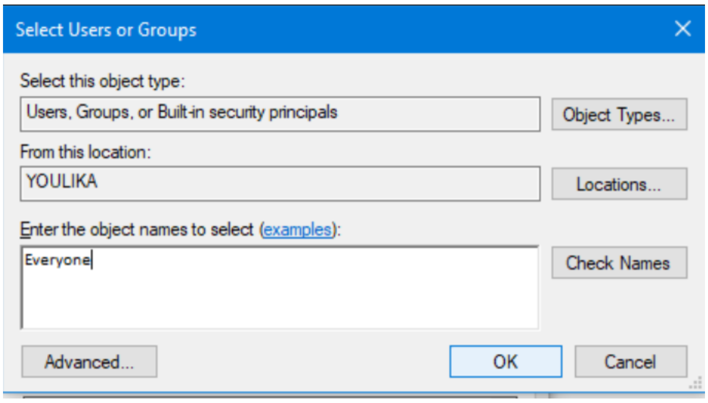
Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (YOULIKA\Administrators)
- Users (YOULIKA\Users)

| Permissions for Users | Allow | Deny |
|---|---|---|
| Full control | ☑ | □ |
| Modify | ☑ | □ |
| Read & execute | ☑ | □ |
| List folder contents | ☑ | □ |
| Read | ☑ | □ |

Figure 0-8 Software Installation-Permission Settings

7. If there is no “Everyone” in the“Group or user names”list, click *“Edit”* and*“Add”* to add“Everyone”and assign all the permissions to“Everyone”, as shown in the figure below:



Select Users or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

YOULIKA

Enter the object names to select (examples):

Everyone

Figure 0-9 Add User Permissions

8. If the server end software still has a running problem, then it needs to install the Microsoft Visual C++ runtime. The recommended installation steps are as follows:

(1) Uninstall FMX NMS network management software.

(2) Install Microsoft Visual C++ runtime vcredist.exe, and restart the equipment after successful installation.

After successful restart of the equipment, install FMX NMS network management software.

## 2.2. Key License Validation

### Steps

The key license validation is needed when you use the software for the first time. Please contact our engineer to get the software key.

1. Click “Start → Program → NMS → NMS Server”, the dialogue box of license validation will pop up when you run the server for the first time, as shown in the figure below:

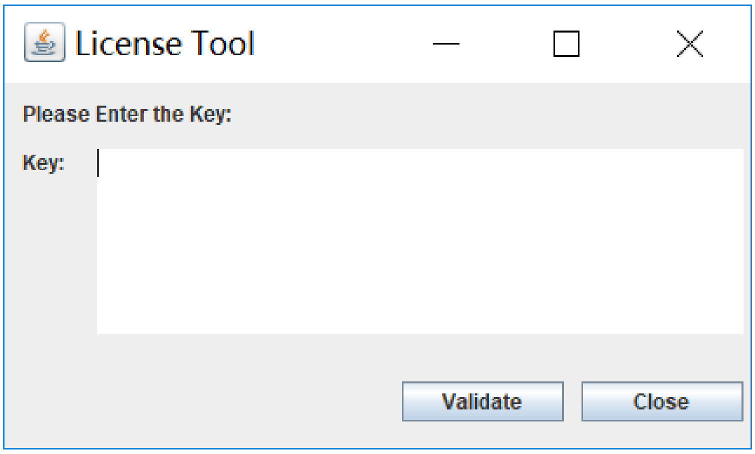


Figure 0-10 Key License Validation Interface

2. Input the correct key which you get from *FS Sales Manager*, and click*“Validate”*, you can enter the main interface of the server program if the validation is successful. (Before getting your license key, you should provide your IP address of your computer to our sales manager for debugging the NMS Sever.)

3. After the key license validation is successful, there is no need to verify it again when you restart the server. If the key license is out of validity, you need to reapply the key and verify it before you use the NMS software again.

4. If the entity server with NMS software is replaced or the key is out of validity, failure of key license validation may occur.

## 2.3. Reinitialize Database

### Prerequisite

The NMS server has been shut down.

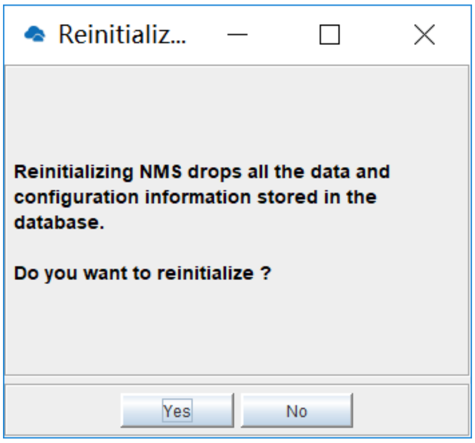
### Related Information

Clear the database and initialize the NMS server.

### Steps

After the server is shut down, click“*Reinitialize NMS*”.

After it displays a prompt message, click OK to clear all the data. Only the original default user name and password are retained. The user needs to add the data back.



Reinitializing NMS drops all the data and configuration information stored in the database.

Do you want to reinitialize ?

Figure 0-11 Server End Software-Reinitialize Database

## 2.4. Start Server End Program

### Steps

1. Click Start→Program→NMS→NMS Server, then the server interface pops up:

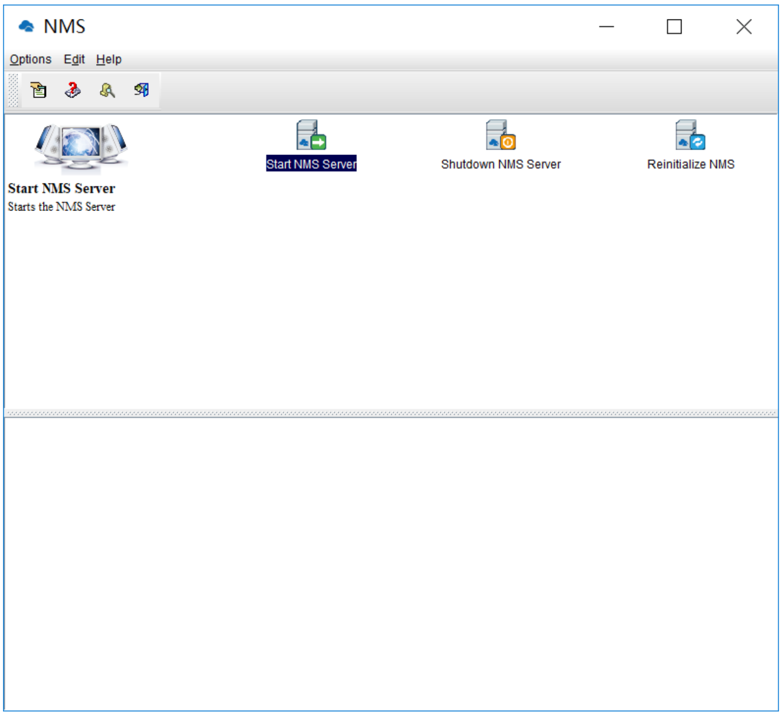
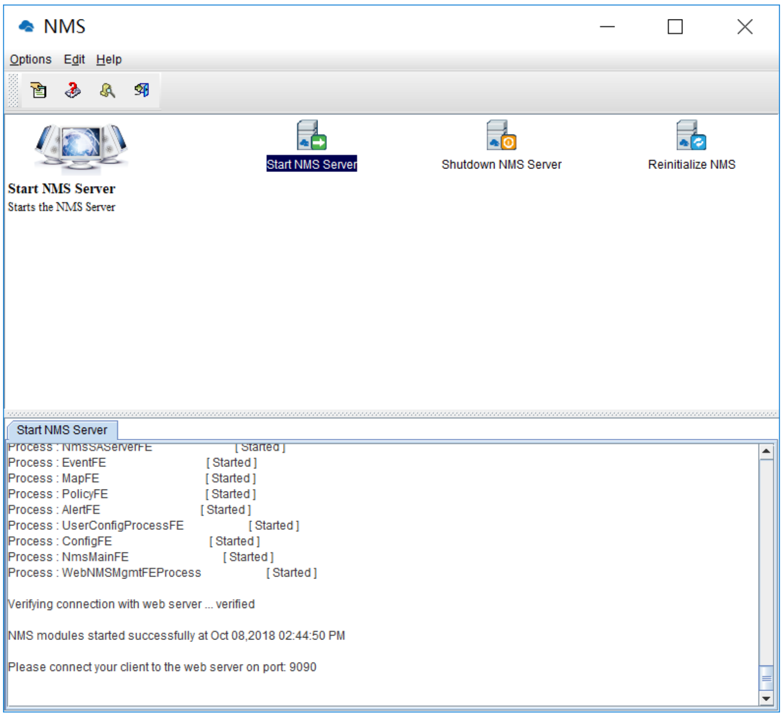


Figure 0-12 Server End Software-Main Interface

2. Double click*"Start NMS Server"* icon to run the server:



```
Process : NmsSAServerFE                 [ Started ]
Process : EventFE                 [ Started ]
Process : MapFE                 [ Started ]
Process : PolicyFE                 [ Started ]
Process : AlertFE                 [ Started ]
Process : UserConfigProcessFE                 [ Started ]
Process : ConfigFE                 [ Started ]
Process : NmsMainFE                 [ Started ]
Process : WebNMSMgmtFEProcess                 [ Started ]

Verifying connection with web server ... verified

NMS modules started successfully at Oct 08,2018 02:44:50 PM

Please connect your client to the web server on port: 9090
```

Figure 0-13 Server End Software-Start NMS Server

When it prompts*"Please connect your client to the web server on port: 9090"*, it means that you have successfully started the NMS server.

## 2.5. Log Into Client

### Steps

1. Open a browser.

2. Enter the server IP address XXX.XXX.XXX.XXX:9090. (It is the IP address of NMS server.)

3. Enter correct user name and password (For the administrator, the default login user name is "root", and the default password is "public"), as shown in the figure below:

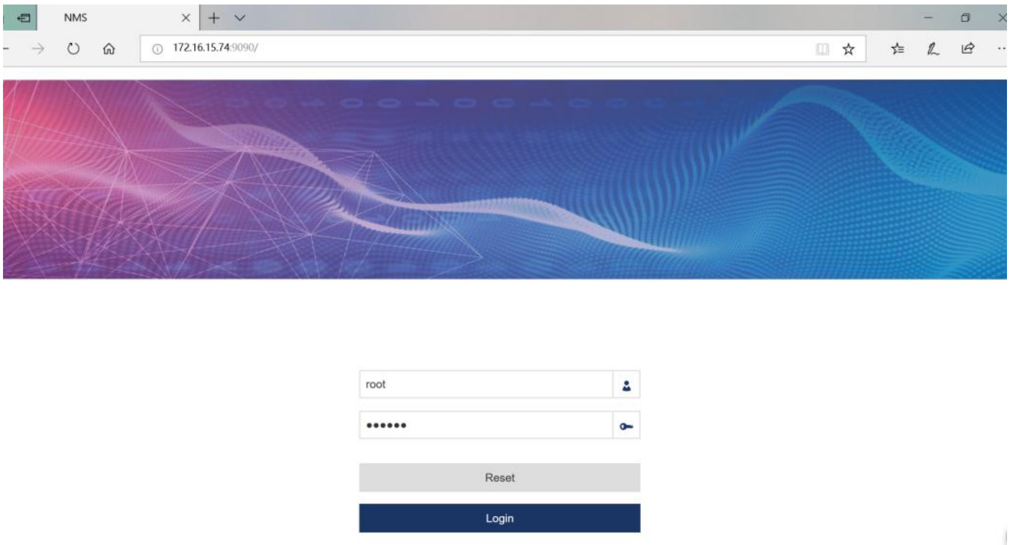


Figure 0-14 Login NMS - Login Interface

After login, the main interface appears, as shown in the figure below:

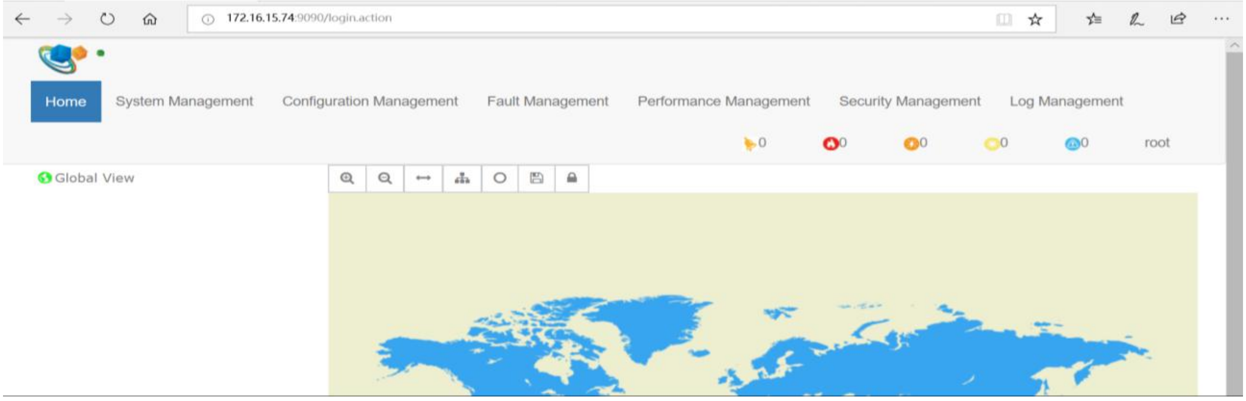


Figure 0-15 Login NMS - Home

## 2.6. Stop Server End Program

### Prerequisite

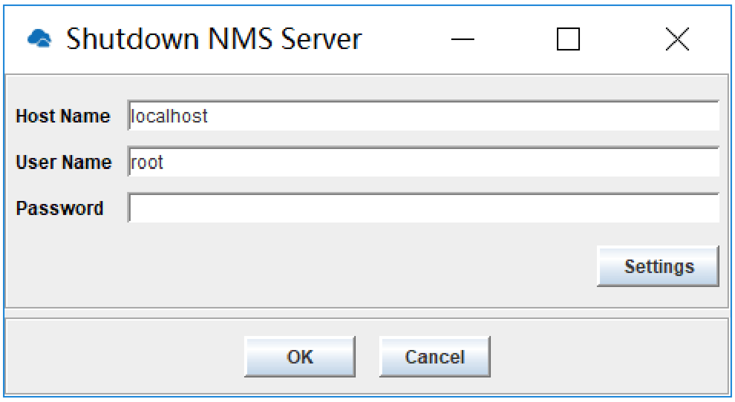
The NMS server has been successfully started.

### Related Information

Shut down the NMS server.

### Steps

Click*"Shutdown NMS Server"*, and the following window pops up:



Host Name localhost

User Name root

Password

Figure 0-16 Server End Software-Shutdown NMS Server

Enter the correct user name and password with administrative privileges (By default, the user name is "root", and the password is "public").

Click *"OK"*, the server will be shut down.

## 2.7. NMS Software Upgrade

### 2.7.1.Database Backup

#### Prerequisite

The NMS server has been shut down.

#### Related Information

After successful login of DB Tool, the NMS data can be stored in the database under two circumstances of shutting down the server and starting the server. Meanwhile, the data of the database can also be exported. After successful installation of NMS, select and double click"NMS" in "All Programs", then DB Tool interface pops up, as shown in the figure below:

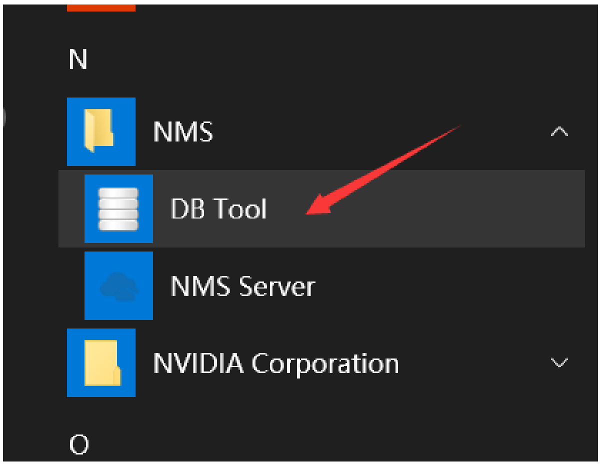


Figure 0-17 DB Tool Path

#### Steps

Double click*"DB TooL"*, the following interface pops up:

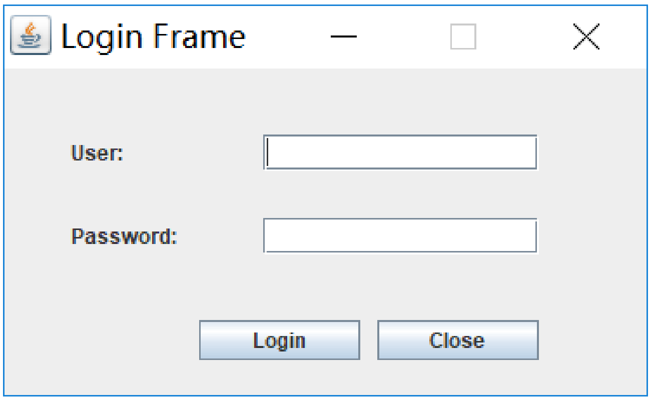


Figure 0-18 DB Tool Login Frame

The initial login account is "root", and the password is "public". The following figure shows the interface of successful login:

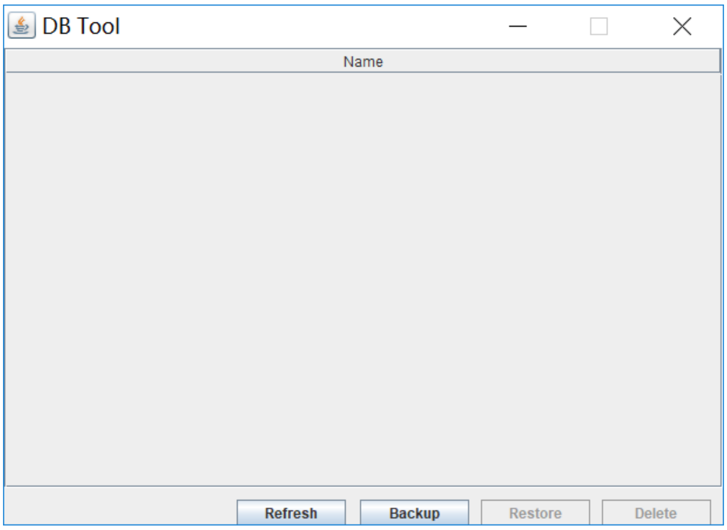
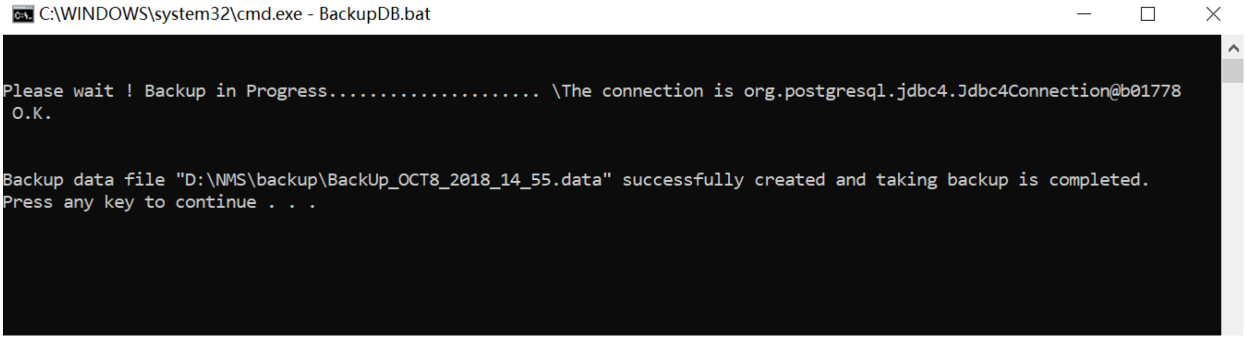


Figure 0-19 DB Tool Interface

The database backup can be realized by clicking*"Backup"* button. After the backup is successful, you can view the backup data by clicking *"Refresh"*button, as shown in the figure below:



```
Please wait ! Backup in Progress.................... \The connection is org.postgresql.jdbc4.Jdbc4Connection@b01778
 O.K.

Backup data file "D:\NMS\backup\BackUp_OCT8_2018_14_55.data" successfully created and taking backup is completed.
Press any key to continue . . .
```

Figure 0-20 Successful Database Backup

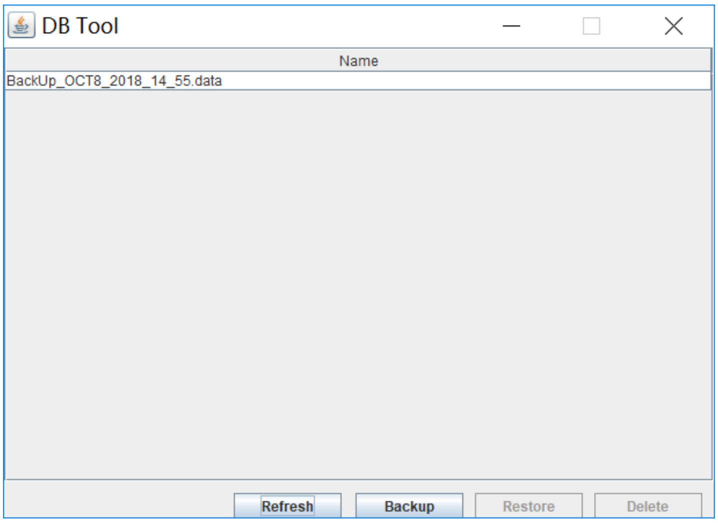


Figure 0-21 View Backup Data

In the NMS installation directory, copy the backup data for future use.

### 2.7.2.NMS Software Upgrade

#### Prerequisite

The NMS server has been shut down.

#### Related Information

Shutdown NMS server and uninstall the current NMS software.

#### Steps

Install new NMS software. The operation steps are the same as that described in 2.1.

### 2.7.3.Import NMS Data

#### Prerequisite

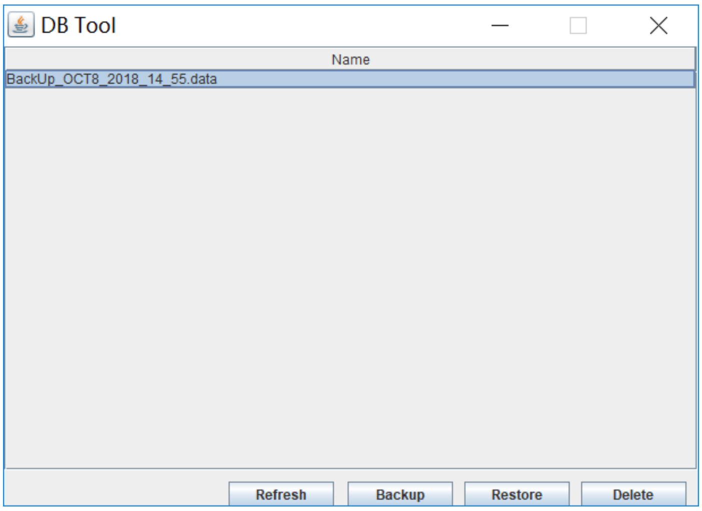
The NMS server has been shut down.

#### Related Information

Shutdown NMS server

#### Steps

Double click*"DB Tool"* to login DB Tool interface and click*"Refresh"* to view the data which needs to be restored. Click*"Restore"*to restore the database, then the following interface will pop up:



DB Tool

| Name |
|---|
| BackUp_OCT8_2018_14_55.data |

Figure 0-22 View Restored Data

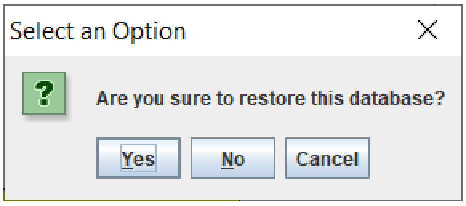
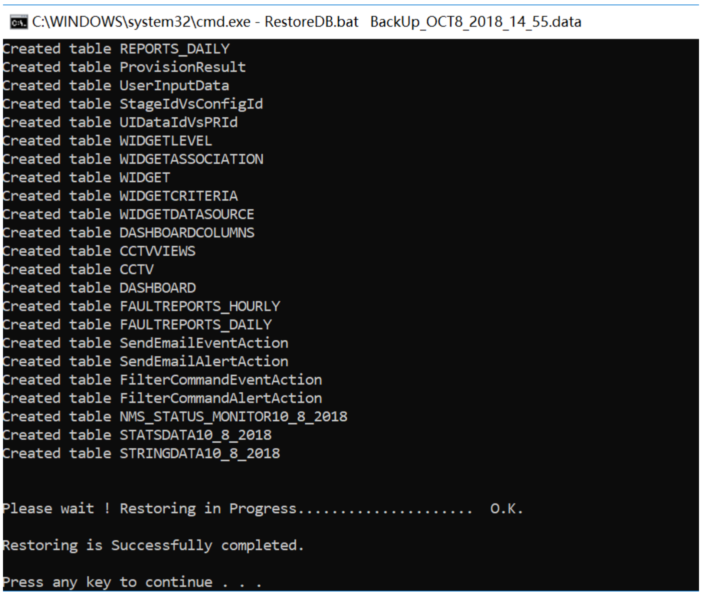


Figure 0-23 Confirm to Restore Database



C:\WINDOWS\system32\cmd.exe - RestoreDB.bat BackUp_OCT8_2018_14_55.data

```
Created table REPORTS_DAILY
Created table ProvisionResult
Created table UserInputData
Created table StageIdVsConfigId
Created table UIDataIdVsPRId
Created table WIDGETLEVEL
Created table WIDGETASSOCIATION
Created table WIDGET
Created table WIDGETCRITERIA
Created table WIDGETDATASOURCE
Created table DASHBOARDCOLUMNS
Created table CCTVVIEWS
Created table CCTV
Created table DASHBOARD
Created table FAULTREPORTS_HOURLY
Created table FAULTREPORTS_DAILY
Created table SendEmailEventAction
Created table SendEmailAlertAction
Created table FilterCommandEventAction
Created table FilterCommandAlertAction
Created table NMS_STATUS_MONITOR10_8_2018
Created table STATSDATA10_8_2018
Created table STRINGDATA10_8_2018


Please wait ! Restoring in Progress....................  O.K.

Restoring is Successfully completed.

Press any key to continue . . .
```

Figure 0-24 Successfully Restore Database

### 2.7.4.Clear Cache

Every time the NMS software is updated and upgraded, the data of the browser need to be emptied. The operation steps are as follows:

1. Enter the Google Chrome browser, and click the menu button on the right side of the toolbar.

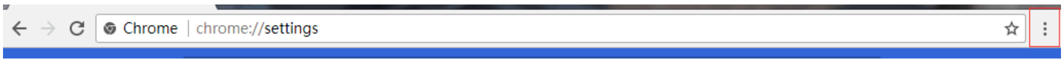


Figure 0-25 Chrome Settings

2. Open the menu and select “Settings”.

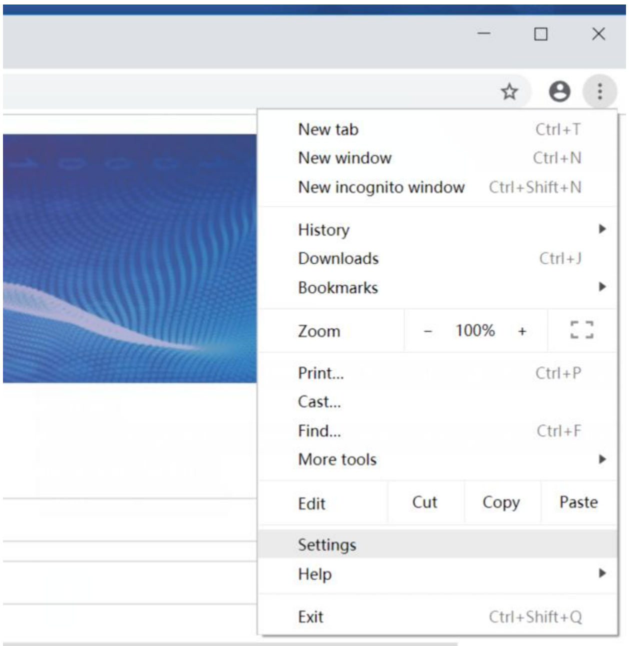
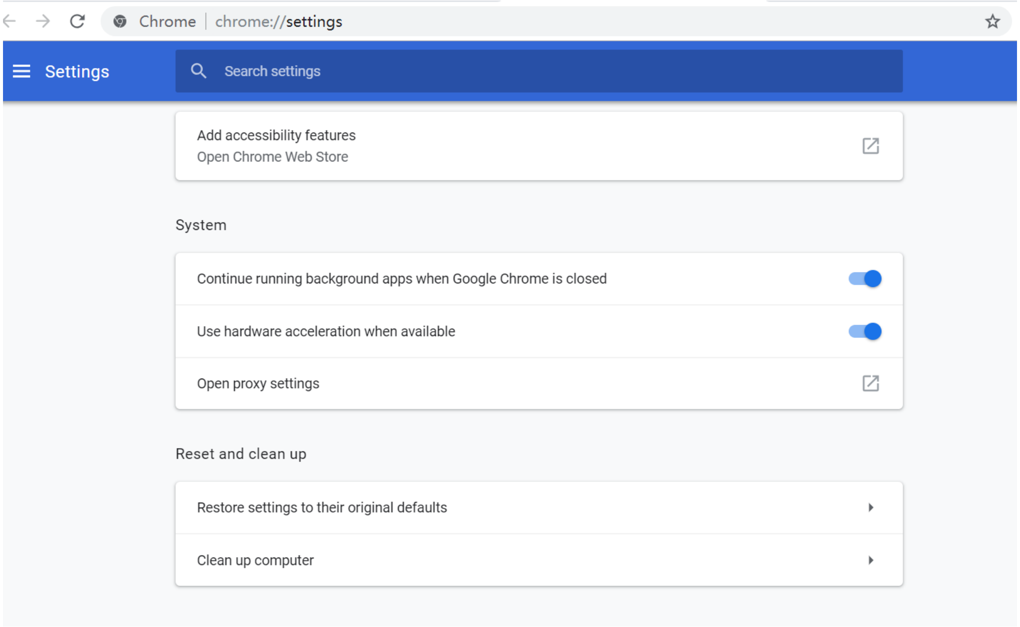


Figure 0-26 Menu Options

3. Enter the settings page, select the last option *"Reset"*to clear the browser cache.



Add accessibility features
Open Chrome Web Store

System

Continue running background apps when Google Chrome is closed ●

Use hardware acceleration when available ●

Open proxy settings

Reset and clean up

Restore settings to their original defaults

Clean up computer

Figure 0-27 Clear Cache

# Chapter 3 Interface Operation of NMS System

The area division of the main interface is shown in the following figure:

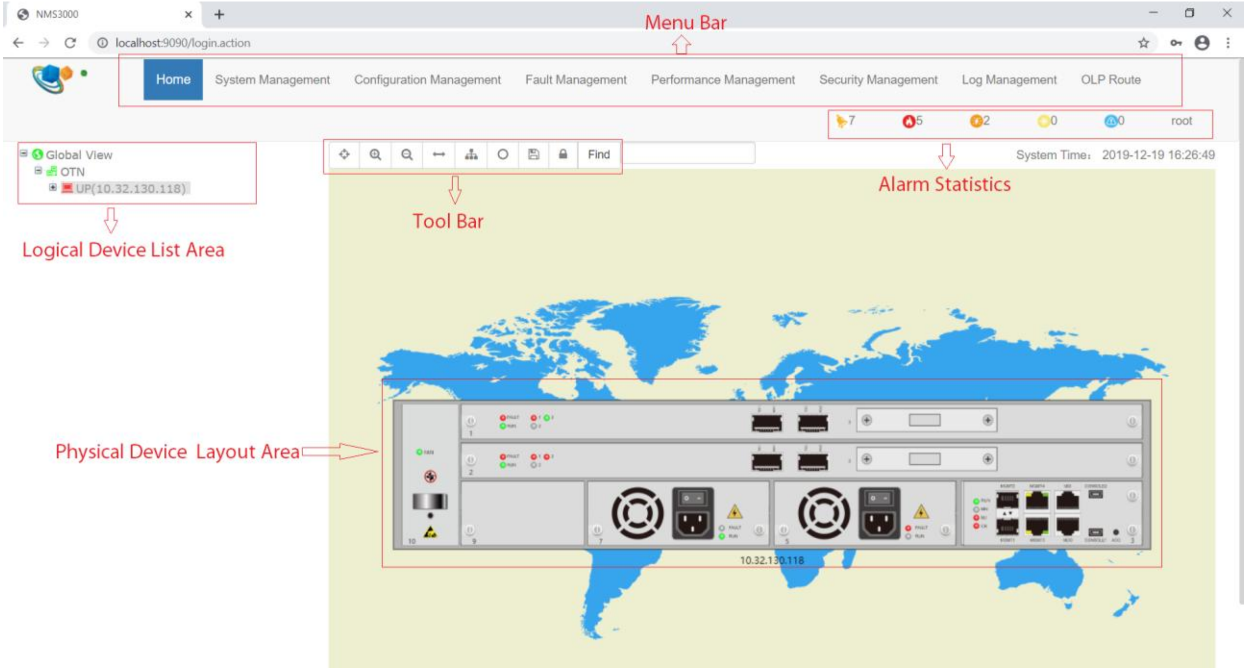


Figure 0-1 Logon Main Interface of NMS System

## 3.1.Interface Operation

### 3.1.1.Screen Lock

The main interface of the FMX NMS system provides the screen lock function which is similar like that of Windows system. The operation steps are as follows:

Click the user*"root"*in the main interface and select*"Screen Lock"*, then the screen of the FMX NMS system can be locked and the following window pops up:

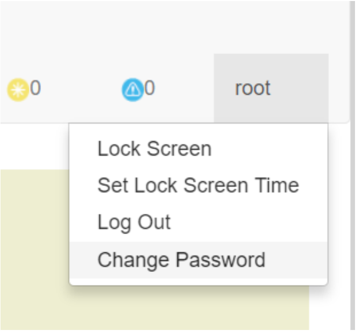


Figure 0-2 Root User Menu-Screen Lock

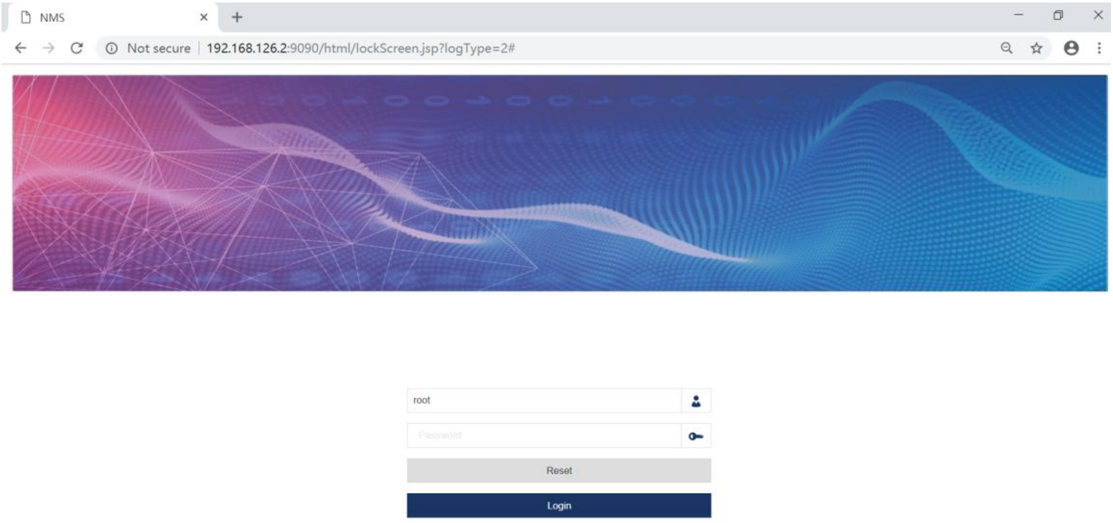
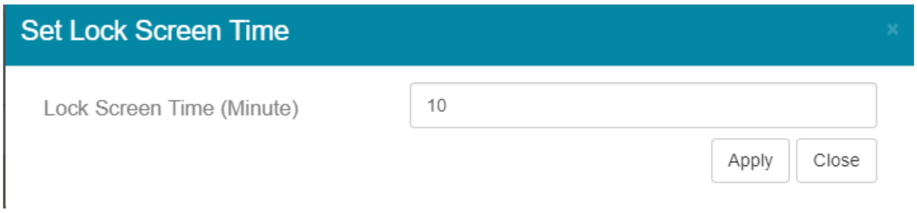


Figure 0-3 Screen Lock Interface

Set automatic screen lock time:

Click the user *"root"* in the main interface and select*"Set Screen Lock Time",* then the NMS screen can be locked and the following window pops up:


Set Lock Screen Time

Lock Screen Time (Minute): 10

Figure 0-4 Set Screen Lock Time

Note: The screen lock time is counted in minutes, and it should be set as not more than 30 minutes (≤30 minutes).

### 3.1.2.Exit Logon

Click the user*"root"*in the main interface and select *"Exit",* then you can exit logon and the following window pops up:

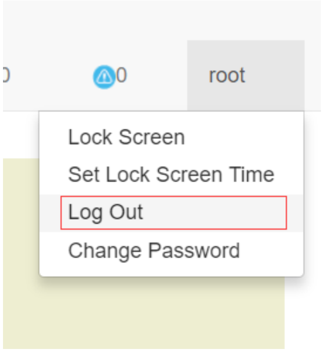


Figure 0-5 Root User Menu-Exit

### 3.1.3.Change Password

Click the user*"root"*in the main interface and select*"Change Password"*, then the following window pops up:

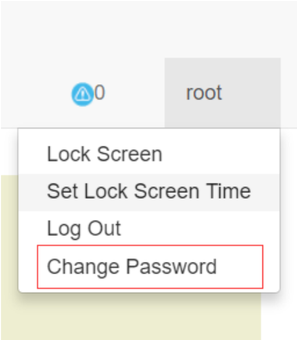
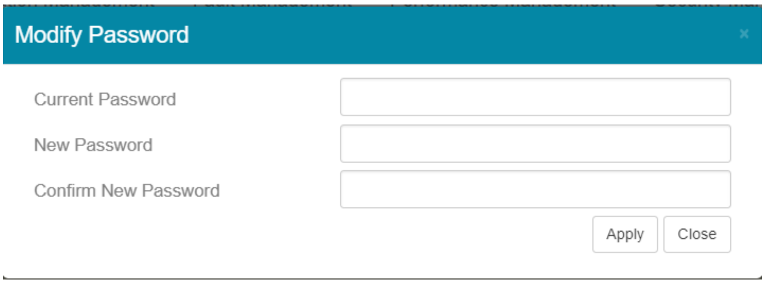


Figure 0-6 Root User Menu-Change Password


Modify Password

Current Password

New Password

Confirm New Password

Figure 0-7 Change Password

After the password is successfully changed, please login with the new password.

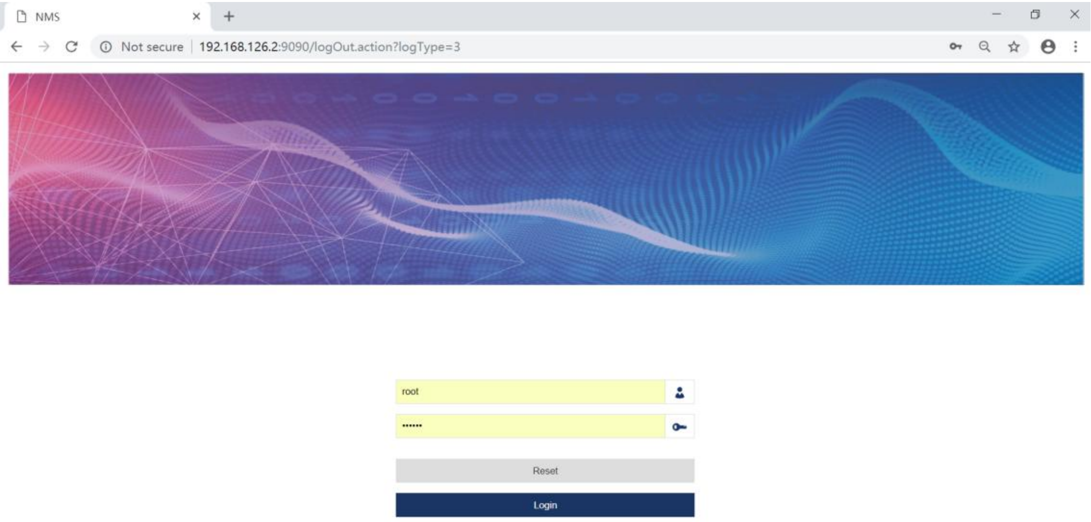


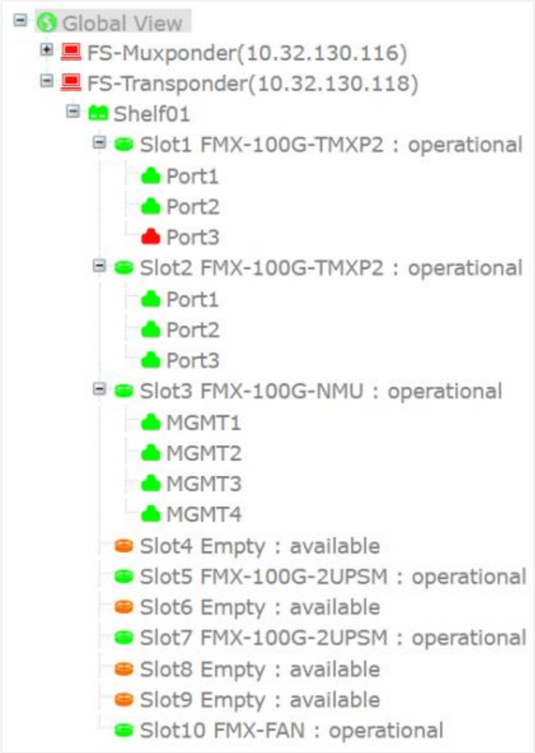
Figure 0-8 Login with New Password

# Chapter 4 System Management

## 4.1. NE(Network Element) Management

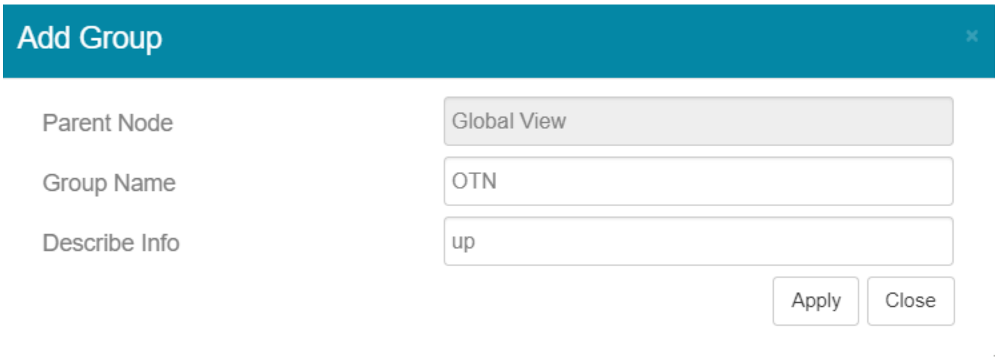
### 4.1.1. Add Group

Right click*"Global View"*→ *"Add Group"* , then you can add user groups. There is no limit to the number of groups. (The user can create multilevel group menus to distinguish equipment from different machine rooms.)



- Global View
  - FS-Muxponder(10.32.130.116)
  - FS-Transponder(10.32.130.118)
    - Shelf01
      - Slot1 FMX-100G-TMXP2 : operational
        - Port1
        - Port2
        - Port3
      - Slot2 FMX-100G-TMXP2 : operational
        - Port1
        - Port2
        - Port3
      - Slot3 FMX-100G-NMU : operational
        - MGMT1
        - MGMT2
        - MGMT3
        - MGMT4
      - Slot4 Empty : available
      - Slot5 FMX-100G-2UPSM : operational
      - Slot6 Empty : available
      - Slot7 FMX-100G-2UPSM : operational
      - Slot8 Empty : available
      - Slot9 Empty : available
      - Slot10 FMX-FAN : operational

Figure 0-1 NE Management-Global View



Add Group

| | |
|---|---|
| Parent Node | Global View |
| Group Name | OTN |
| Describe Info | up |

Figure 0-2 NE Management-Add Group

It is allowed to create new user group, modify and delete group information and add NE.

Modifying group information includes modifying group name and description of the group.

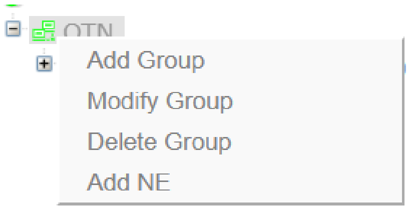
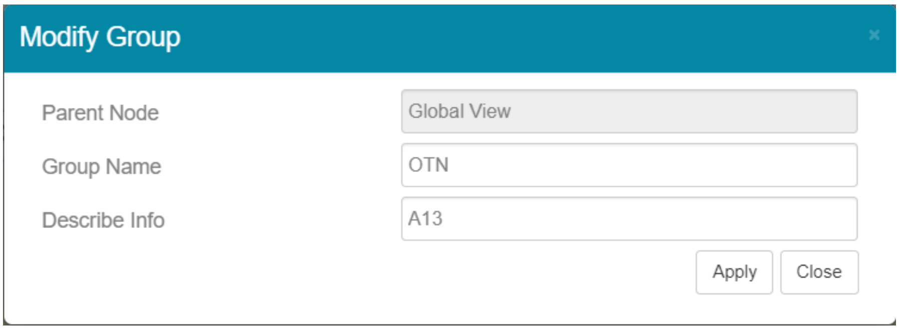


Figure 0-3 NE Management-Group Node


Modify Group

Parent Node: Global View

Group Name: OTN

Describe Info: A13

Figure 0-4 NE Management-Modify Group

All the network elements of the group will be deleted when the user group is deleted.

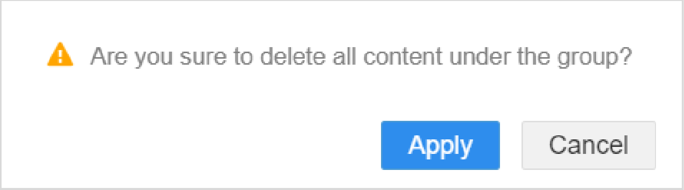

Are you sure to delete all content under the group?

Figure 0-5 NE Management-Delete Group

### 4.1.2. Add NE

#### Prerequisite

1. Run the NMS server, and login the browser.

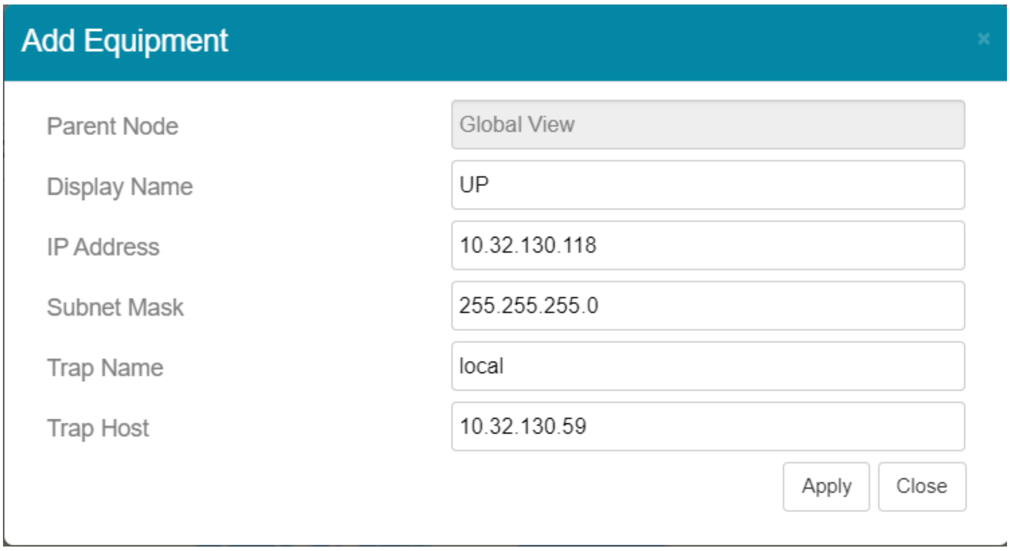
2. The NE has been physically connected with the NMS server.

3. The home page of the NMS has been successfully logged in.

#### Steps

1. Open the browser to enter the web page of NMS. Log in NMS and select *"Add Equipment"* on the right click menu of *"Global View"* ,  then the "Add Equipment" interface pops up.

2. Enter the NE name, IP address, subnet mask and Trap name, select Trap host, and click*"Apply"*to complete the creation (Display name refers to display name of NE, Trap name refers to the name of trap host), as shown in the figure below:



Add Equipment

| | |
|---|---|
| Parent Node | Global View |
| Display Name | UP |
| IP Address | 10.32.130.118 |
| Subnet Mask | 255.255.255.0 |
| Trap Name | local |
| Trap Host | 10.32.130.59 |

Figure 0-6 NE Management-Add Equipment

3. (Optional) If you want to modify the properties of NE which has been created, right click the NE to be modified, select *"Modify NE"* in the pop-up menu, and modify relevant properties in "Modify Equipment" interface.

4. (Optional) If you want to delete the NE which has been created, select *"Delete NE"* in the right click menu of the created NE, and click "Apply" in the prompt box.

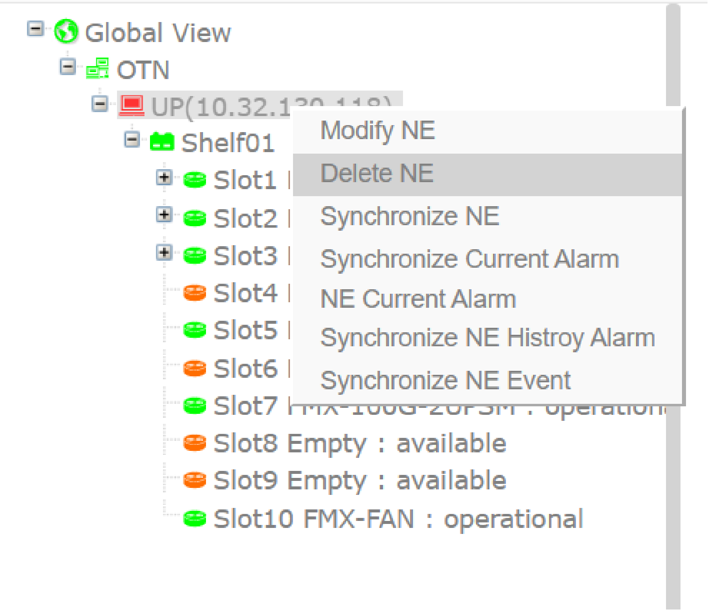
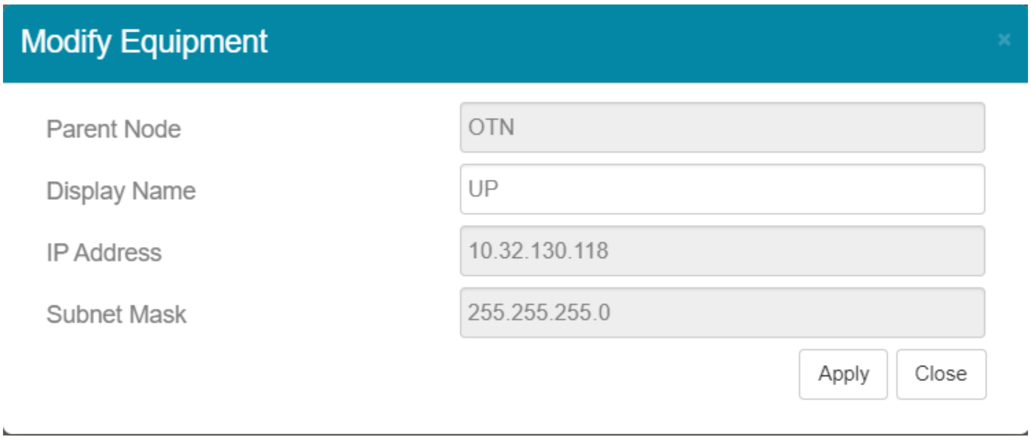


Figure 0-7 NE Management-NE Nodes

### 4.1.3. Modify NE

Right click *"Modify NE"*, you can modify the descriptions of NE.



Modify Equipment

| | |
|---|---|
| Parent Node | OTN |
| Display Name | UP |
| IP Address | 10.32.130.118 |
| Subnet Mask | 255.255.255.0 |

Figure 0-8 NE Management-Modify NE

### 4.1.4. Synchronize NE

Right click NE nodes, and then click *"Synchronize NE"* , you can synchronize the state of all NE boards.

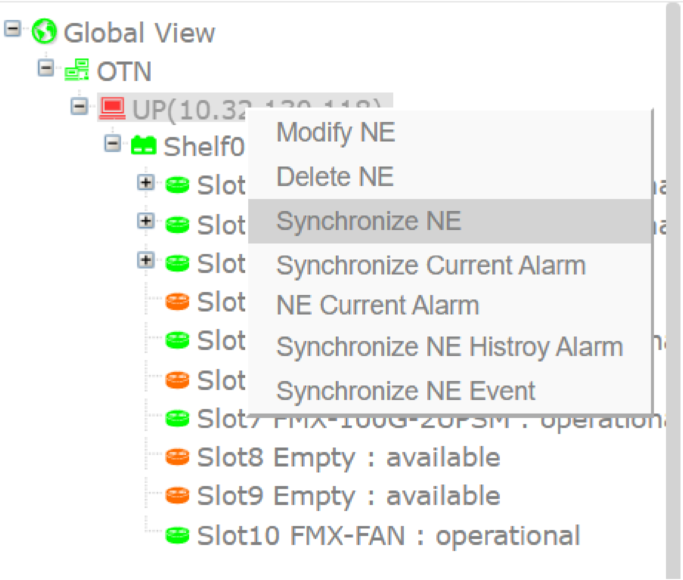


Figure 0-9 NE Management-Synchronize NE

Right click NE nodes, and then click *"Synchronize Current Alarm"*, you can synchronize the current alarm information of NE.

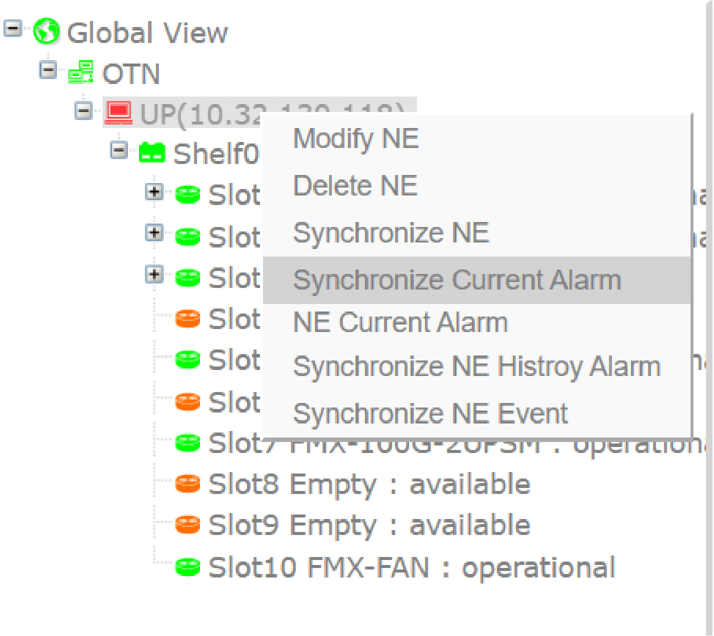


Figure 0-10 NE Management-Synchronize Current Alarm

## 4.2. FTP Server Configuration

### Prerequisite

1. The NMS server runs successfully, and the NMS interface has been successfully logged in.

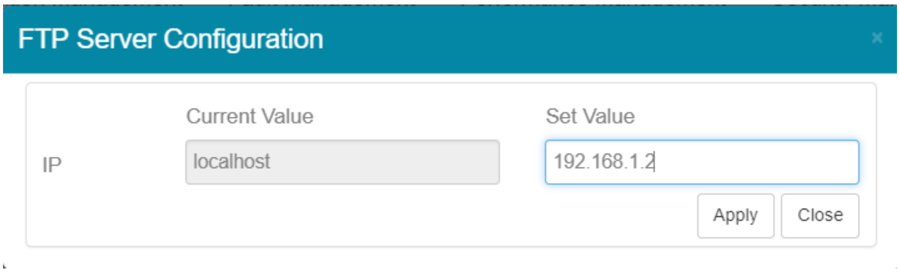
2. There is IP which can be connected with the external network.

### Purpose

It is used for saving, uploading, downloading, upgrading configurations of NE and collecting performance statistics. Each network element needs to be configured separately.

### Steps

Select NE, and click “System Management→FTP Server Configuration” on the navigation bar to enter FTP configuration interface.


FTP Server Configuration

| | Current Value | Set Value |
|---|---|---|
| IP | localhost | 192.168.1.2 |

Figure 0-11 FTP Server Configuration

### Parameter Description

The system directly assigns local-host to *"Current Value"*. The user needs to change it.

For setting values: The system shows the IP of local network card to the user. The user needs to select the IP connected with the communication of the equipment.

After selecting the appropriate*"Set Value"* IP, you can click*"Apply"* to assign the actual IP to*"Current Value"*.

## 4.3. SNMP Configuration

### Prerequisite

Run the NMS server, login NMS, and successfully add NE.

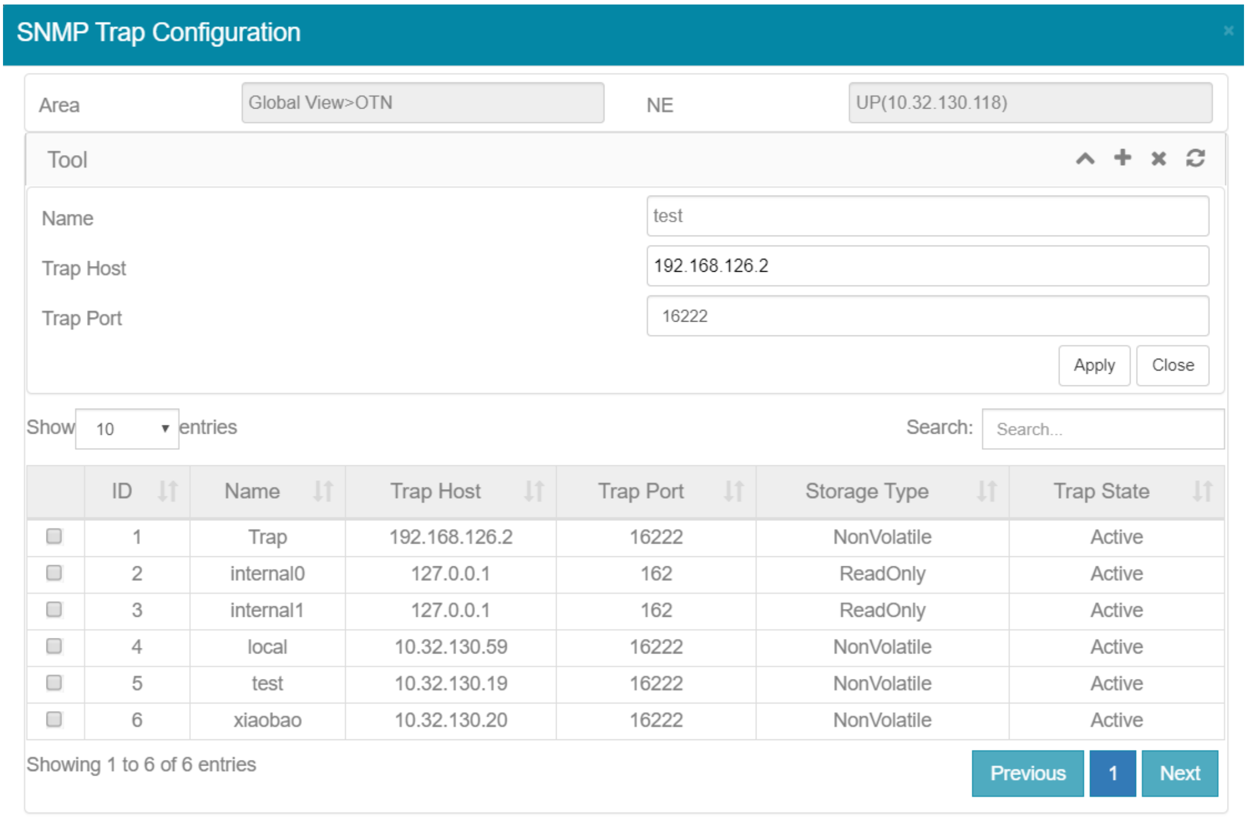
### Related Information

When a NE device is connected with multiple NMS servers, different Trap addresses need to be respectively configured for every NMS system.

The server is installed under windows. The user needs to turn off the firewall, or set 69 and 16222 ports to penetrate. Otherwise, the upload, download and alarm event report of SNMP trap may fail.

### Steps

Select the NE on the left menu, and click "System Management → SNMP Trap Configuration" on the navigation bar.



SNMP Trap Configuration

Area: Global View>OTN

NE: UP(10.32.130.118)

Tool

Name: test

Trap Host: 192.168.126.2

Trap Port: 16222

| | ID | Name | Trap Host | Trap Port | Storage Type | Trap State |
|---|---|---|---|---|---|---|
| □ | 1 | Trap | 192.168.126.2 | 16222 | NonVolatile | Active |
| □ | 2 | internal0 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 3 | internal1 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 4 | local | 10.32.130.59 | 16222 | NonVolatile | Active |
| □ | 5 | test | 10.32.130.19 | 16222 | NonVolatile | Active |
| □ | 6 | xiaobao | 10.32.130.20 | 16222 | NonVolatile | Active |

Showing 1 to 6 of 6 entries

Figure 0-12 SNMP Configuration

When the user needs to add new IP, click " ⌃ + × ⟳ " button in the toolbar, then the add page will pop up.

### Parameter Description

Name: entered by the user. There is no limitation.

Trap Host: IP address of the host to receive Trap information

Trap Port: The port number of the host to receive Trap information is 16222.

## 4.4. NE IP Configuration

### Prerequisite

1. Run the NMS server and login NMS.

2. NE has been successfully created.

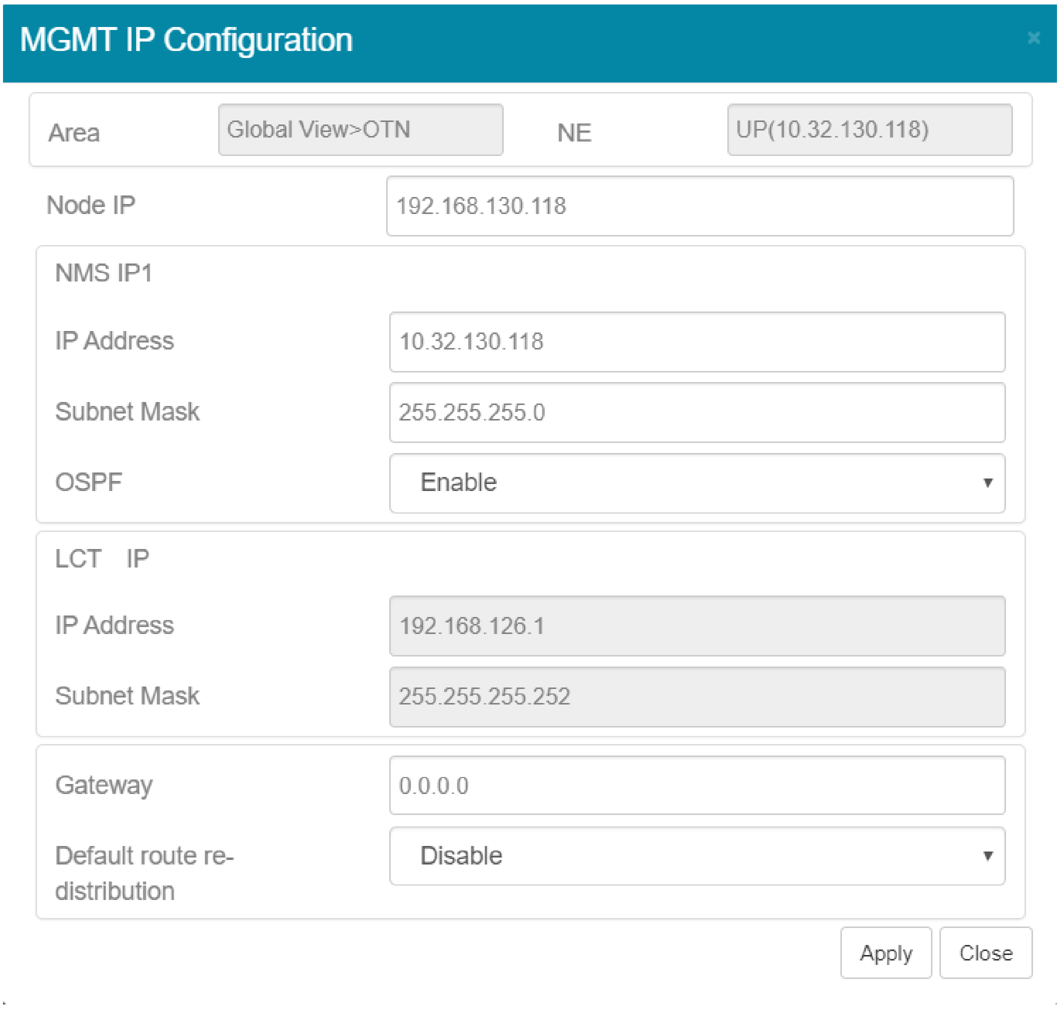
3. The physical configuration has been completed.

### Related Information

Configure IP address of the Ethernet port.

### Steps

Select NE on the left menu, and click "System Management→Manage IP Configuration" on the navigation bar.



MGMT IP Configuration

| | |
|---|---|
| Area | Global View>OTN |
| NE | UP(10.32.130.118) |
| Node IP | 192.168.130.118 |
| NMS IP1 | |
| IP Address | 10.32.130.118 |
| Subnet Mask | 255.255.255.0 |
| OSPF | Enable |
| LCT IP | |
| IP Address | 192.168.126.1 |
| Subnet Mask | 255.255.255.252 |
| Gateway | 0.0.0.0 |
| Default route re-distribution | Disable |

Figure 0-13 Manage IP Configure

### NE Management

1. The PC of local NMS is connected with the device NMU MGMT ports (The default IP address is 192.168.126.1 and the subnet mask is 255.255.255.252.)

2. The IP address of 192.168.126.2 needs to be configured for the PC of the local NMS. Ping the command*"ping 192.168.126.1"* for detection by using PC. If it can be successfully pinged, then the device can be managed and configured locally.

3. Plan to modify*" Node IP"* , *"NMS IP1"*and*"NMS IP2"*according to the IP address of the user's current network."Node IP"is the IP address to identify NE. "NMS IP1"and"NMS IP2"are IP addresses of MGMT ports on NE which are connected with NMS server. It is generally configured on gateway network element (It is not configured on non gateway network element).

## 4.5. Time Configuration

### 4.5.1 NTP Server Configuration

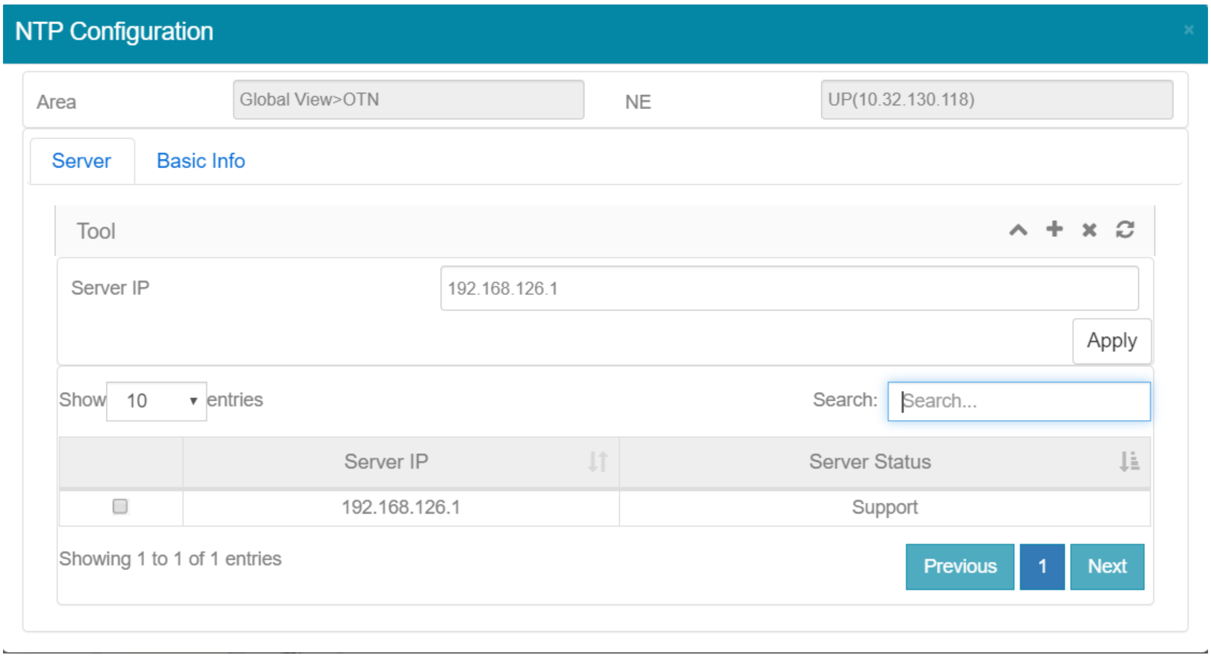
#### Related Information

Relevant configuration of NTP client helps to realize time synchronization of NE and NTP server.

#### Steps

Select the NE on the left menu, and click "System Management → NTP Configuration" on the navigation bar to enter the configuration screen.

NTP includes*"Server"* and *"Basic Information"*. The currently configured NTP server information can be shown on the server end. The user can add new NTP server by clicking "+"on the toolbar.



NTP Configuration

Area: Global View>OTN

NE: UP(10.32.130.118)

Server | Basic Info

Tool

Server IP: 192.168.126.1

Apply

Show 10 entries

Search: Search...

| | Server IP | Server Status |
|---|---|---|
| □ | 192.168.126.1 | Support |

Showing 1 to 1 of 1 entries

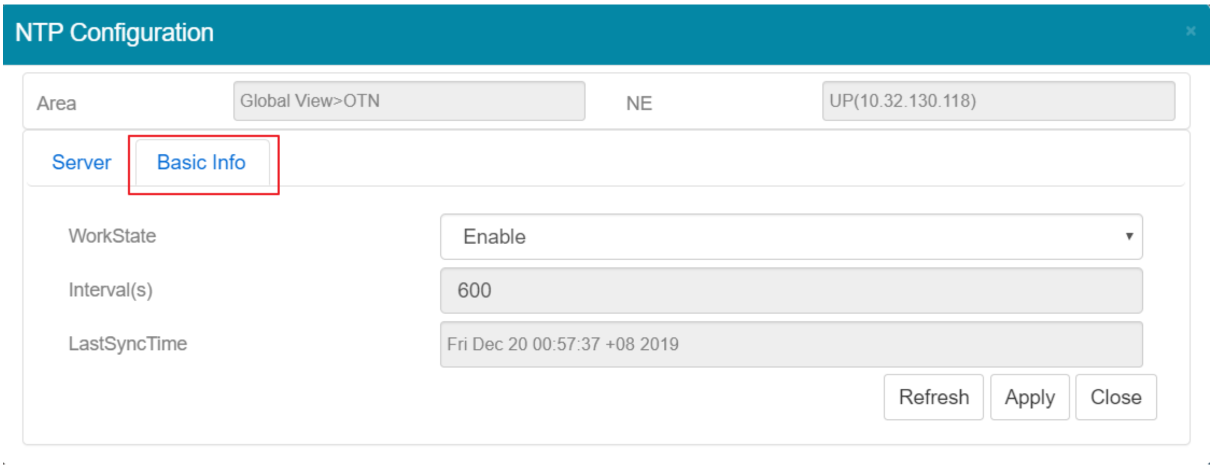
Previous 1 Next

Figure 0-14 NTP Configuration-Server

Enter the correct server IP, and click *"Apply"* to complete the adding operation.

The user can select one or multiple options in the check box of the table, and then click "X" button on the toolbar to complete the delete operation.

The user can choose whether to enable NTP server and can fix the time interval as "3600" with a unit of second in*"Basic Info"*.


NTP Configuration

Area: Global View>OTN
NE: UP(10.32.130.118)

WorkState: Enable
Interval(s): 600
LastSyncTime: Fri Dec 20 00:57:37 +08 2019

Figure 0-15 NTP Configuration-Basic Information

### 4.5.2 NE Time Configuration

#### Prerequisite

1. Run the NMS server and login the NMS.

2. NE has been successfully created.

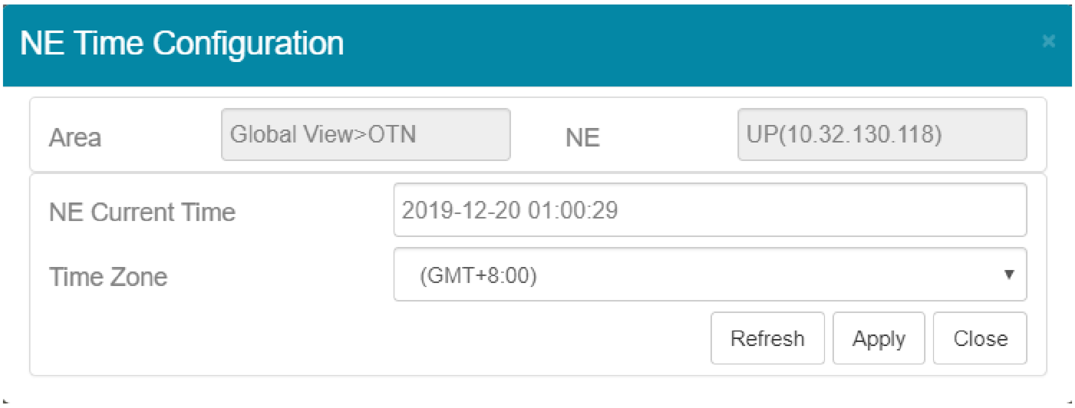
3. Physical configuration has been completed.

#### Related Information

Configure the time of NE system. By default, GMT is adopted as the standard time zone.

#### Steps

Select the NE on the left menu, and click “System Management → NE Time Configuration” on the navigation bar.


NE Time Configuration

Area: Global View>OTN
NE: UP(10.32.130.118)

NE Current Time: 2019-12-20 01:00:29
Time Zone: (GMT+8:00)

Figure 0-16 NE Time Configuration

Fill in the *"NE Current Time"* in the correct format (year-month-date hour:minute:second). Click*"Apply"*to complete the configuration. There is a prompt message whether it is successful or failed.

⚠ **The time zone is Greenwich time, which is eight hours later than Beijing Time. Eight hours needs to be reduced while making configuration.**

# 4.6.NE-Related Operation

## 4.6.1.NE Basic Information

### Prerequisite

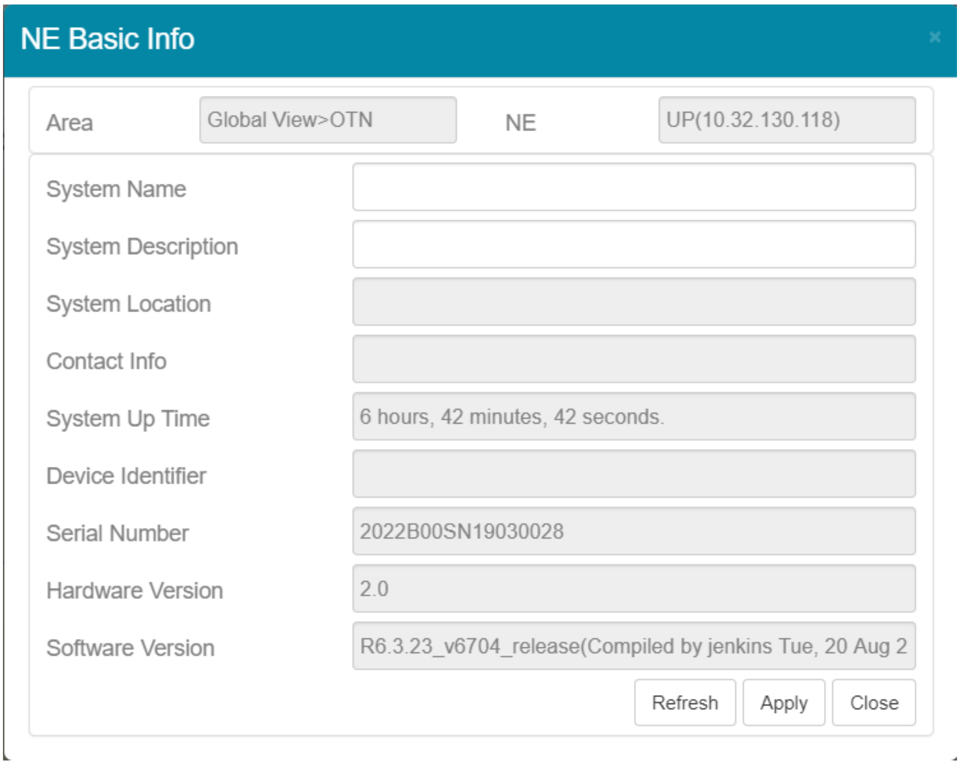
Run the NMS server, login NMS and NE is successfully added.

### Related Information

Show NE basic information

### Steps

Select NE on the left menu, and click "System Management → NE Basic Info" on the navigation bar. The user can modify information such as System Name, System Description, System Location and Contact Info etc.



NE Basic Info

| | | | |
|---|---|---|---|
| Area | Global View>OTN | NE | UP(10.32.130.118) |

| | |
|---|---|
| System Name | |
| System Description | |
| System Location | |
| Contact Info | |
| System Up Time | 6 hours, 42 minutes, 42 seconds. |
| Device Identifier | |
| Serial Number | 2022B00SN19030028 |
| Hardware Version | 2.0 |
| Software Version | R6.3.23_v6704_release(Compiled by jenkins Tue, 20 Aug 2 |

Figure 0-17 NE Basic Information

### 4.6.2.Configuration Data Saving

#### Prerequisite

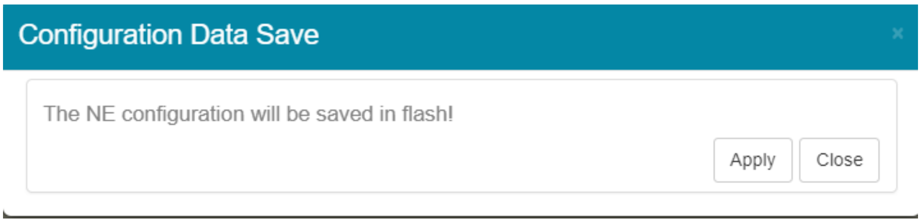
The NMS server has been opened and NMS has been logged in.

#### Related Information

After the NE configuration takes effect, the configuration data will be firstly stored in the NE memory. Every one minute, the NE will automatically save the changed configuration data to Flash (After reboot of NE, the user can restore the configuration data from Flash). If the user needs to save the configuration in advance, then he can use this command.

#### Steps

Select the NE on the left menu, and click "System Management → Configuration Data Saving" on the navigation bar. Click *"Apply"* to save the configuration data, and a prompt message will pop up to tell whether it is successfully saved.



Configuration Data Save

The NE configuration will be saved in flash!

Figure 0-18 Configuration Data Saving

## 4.6.3.Configuration Data Upload

### Prerequisite

1. Run the NMS server and login NMS.

2. FTP has been successfully configured.

### Related Information

Upload the current NE configuration to the NMS system.

### Steps

1. Select the NE on the left menu, and click “System Management → Configuration Data Upload” on the navigation bar, a window pops up.

2. The configuration file is automatically downloaded in the browser.

3. Put the configuration file to the following directory: “Server Installation Root NMS→ TFTP → configure” to finish configuration.

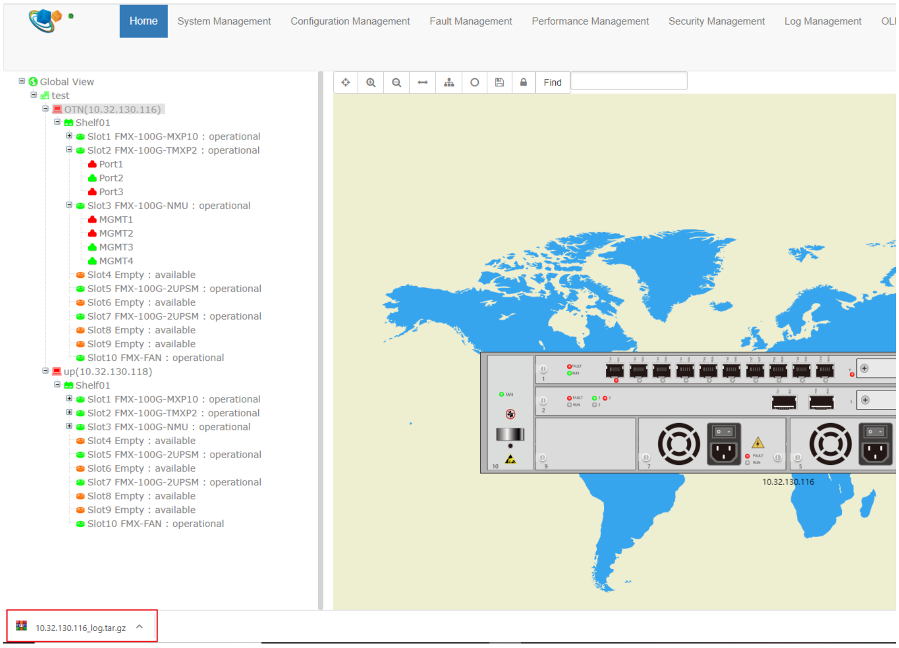


Figure 0-19 Configuration Data Upload

## 4.6.4.Configuration Data Download

### Prerequisite

1. Run the NMS server and login NMS.

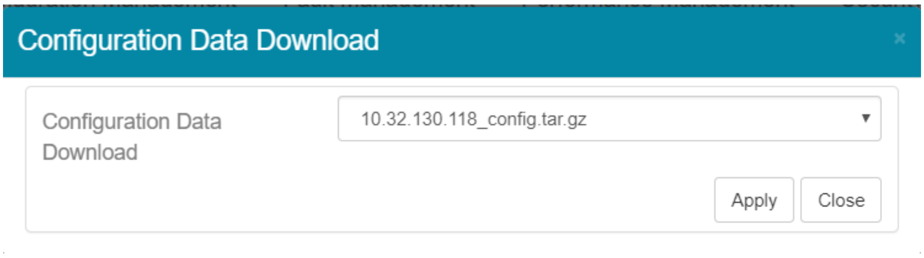
2. FTP has been successfully configured.

### Related Information

Download the current NE configuration to the NMS system.

### Steps

Select the NE on the left menu, and click "System Management -->Configuration Data Download" on the navigation bar, a download screen pops up. The user can select the file name which needs to be downloaded to NE. If there is no file, then this operation cannot be performed.


Configuration Data Download

Configuration Data Download: 10.32.130.118_config.tar.gz

Figure 0-20 Configuration Data Download

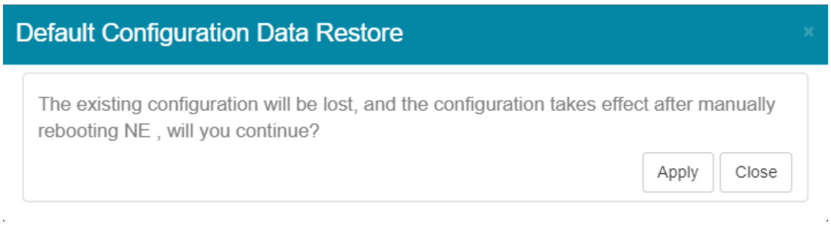
## 4.6.5.Restore the Default Configuration

### Related Information

Restore NE configuration to default configuration.

### Steps

Select the NE on the left menu, and click "System Management --> Default Configuration Data Restore" on the navigation bar to enter the interface. Click *"Apply"* button, a prompt message will appear to ask whether you are sure to restore the default configuration.


Default Configuration Data Restore

The existing configuration will be lost, and the configuration takes effect after manually rebooting NE , will you continue?

Figure 0-21 Default Configuration Data Restore

## 4.6.6.NE Log Upload

### Prerequisite

1. Run the NMS server and login the NMS.

2. FTP has been successfully configured.

### Related Information

Upload the log of current network element to the NMS system.

### Steps

1. Select the NE on the left menu, and click “System Management -->NE Log Upload” on the navigation bar, a screen pops up.

2. The log file is automatically downloaded in the browser.

3. Put the log file to the following directory: “Server Installation Root NMS→ TFTP→ log” to finish configuration.

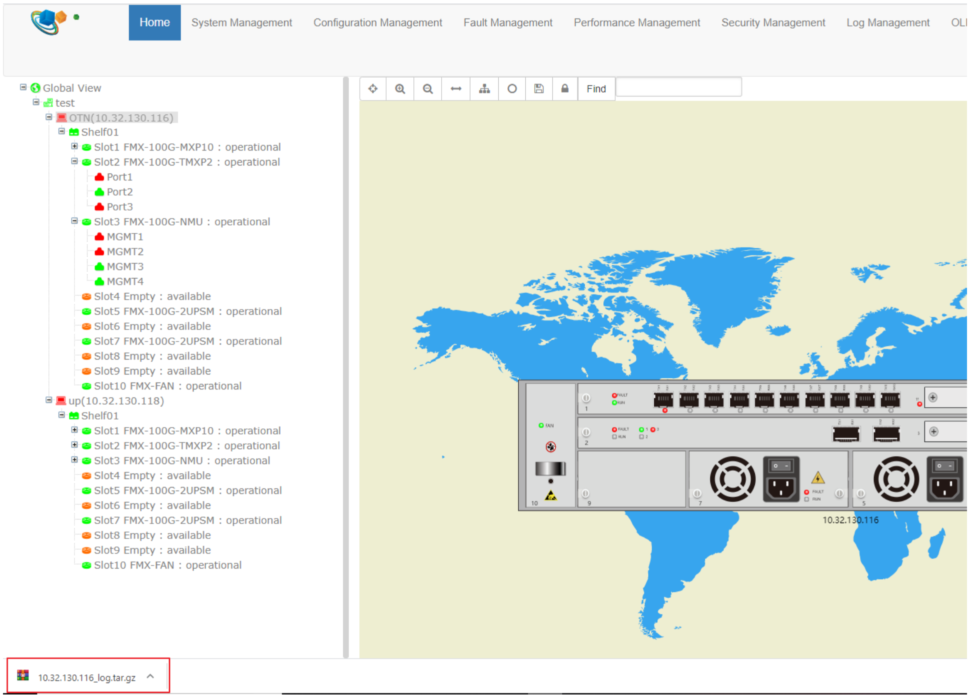


Figure 0-22 NE Log Upload

## 4.6.7.NE Software Upgrade

### Prerequisite

1. Run the NMS server and login NMS.

2. FTP has been successfully configured.

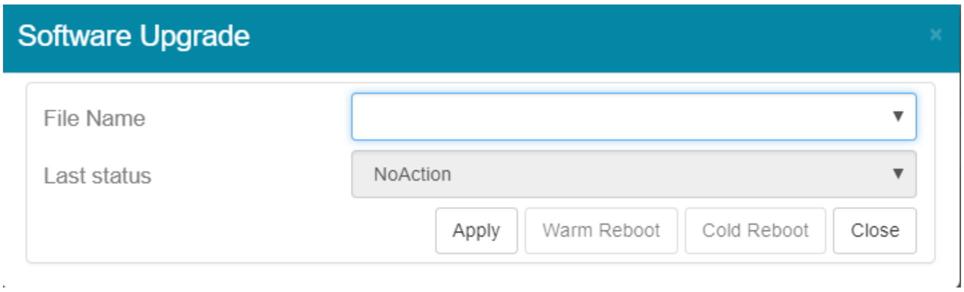
3. The software upgrade file and the MD5 validating file have been successfully imported to the following directory: Server Installation Root NMS→ TFTP → software. The user can modify the upgrade file name and the MD5 validating file name locally. The names of the two files must be consistent (except the suffix), and they cannot contain Chinese or special characters.

### Related Information

Download the upgraded file of NMS to the NE, so as to realize software upgrade of the NE.

### Steps

Select the NE on the left menu, and click *"System Management →Software Upgrade"* on the navigation bar, a software upgrade screen pops up. The user can select relevant file, and click*"Apply"* to perform the operation.



Software Upgrade

File Name

Last status: NoAction

Figure 0-23 Software Upgrade

The system reads the value of*"Last Status"*. When the value is "Success", the user can make the upgraded software take effect by clod start or warm start.

**tar.gz file needs to be selected while upgrading software. There is no need upgrading MD5 file. (If this file is upgraded, then the NMS system will prompt the failure.)**

## 4.6.8.NE Reboot

### Related Information

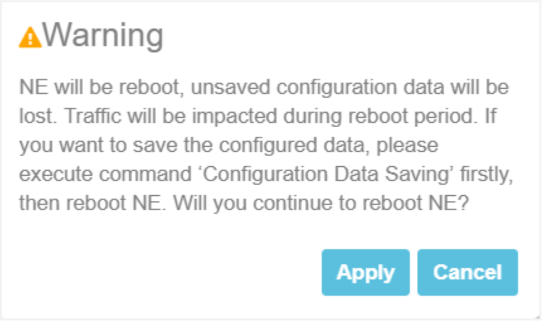
Remote reboot of NE can be realized by the NMS system.

For OTN network element, there are cold start and warm start.

### Steps

Select the NE on the left menu, and click *"System Management →NE Warm Start"* on the navigation bar. A prompt message that asks whether to reboot the equipment appears. Click "OK" to reboot the equipment. (Services will not be interrupted in the process of warm start.)

Select the NE on the left menu, and click *"System Management →NE Cold Start"* on the navigation bar. A prompt message that asks whether to reboot the equipment appears. Click *"OK"* to reboot the equipment. (Services will be interrupted in the process of cold start. After the startup of the equipment is completed, the services can be recovered.)



⚠Warning

NE will be reboot, unsaved configuration data will be lost. Traffic will be impacted during reboot period. If you want to save the configured data, please execute command 'Configuration Data Saving' firstly, then reboot NE. Will you continue to reboot NE?

Figure 0-24 NE Reboot

### 4.6.9.BSP Upgrade of SC Module(NMU Module)

#### Prerequisite

1. Run the NMS server and login NMS.

2. FTP has been successfully configured.

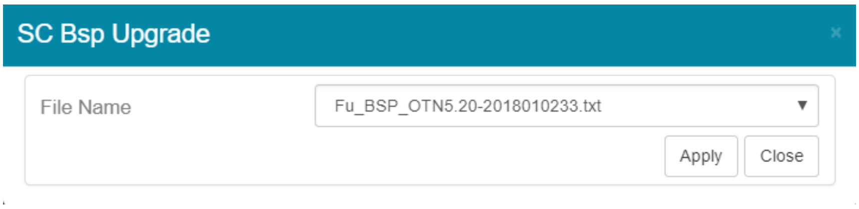
3. The BSP upgrade file and the MD5 validating file have been successfully imported to the following directory: Server Installation Root NMS → TFTP → BSP. (The firmware_update file needs to be simultaneously imported to this root directory.) The user can modify the upgrade file name and the MD5 validating file name locally. The names of the two files must be consistent (except the suffix), and they cannot contain Chinese or special characters.

#### Related Information

Download the BSP upgraded file of NMS to the NMU module, so as to realize BSP upgrade of the NMU module.

#### Steps

Select the NE on the left menu, and click *"System Management →BSP Upgrade of SC Module"* on the navigation bar, the BSP upgrade screen pops up. The user can select relevant file, and click*"Apply"*to perform the operation.



SC Bsp Upgrade

File Name: Fu_BSP_OTN5.20-2018010233.txt

Figure 0-25 BSP Upgrade of NMU Module

After it is successfully upgraded, the NE will automatically reboot. When the reboot is successful, the BSP upgrade will take effect.

### 4.6.10.BSP Upgrade of LC Module(Business Module)

#### Prerequisite

1. Run the NMS server and login NMS.

2. FTP has been successfully configured.

3. The BSP upgrade file and the MD5 validating file have been successfully imported to the following directory: Server Installation Root NMS → TFTP → LCBSP. (The firmware_update file needs to be simultaneously imported to this root directory.) The user can modify the upgrade file name and the MD5 validating file name locally. The names of the two files must be consistent (except the suffix), and they cannot contain Chinese or special characters.

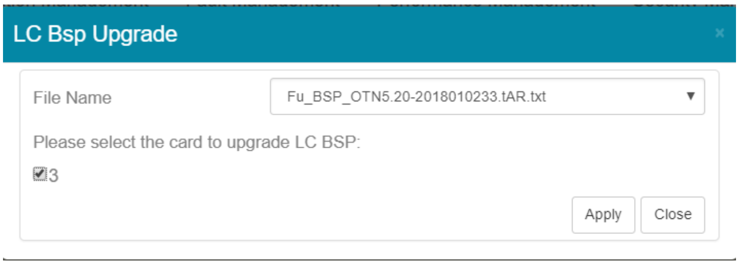
## Related Information

Download the BSP upgraded file of NMS to the LC module, so as to realize BSP upgrade of the LC module.

## Steps

Select the NE on the left menu, and click *"System Management →BSP Upgrade of LC module"* on the navigation bar, the BSP upgrade screen pops up. The user can select relevant file, and click*"Apply"*to perform the operation.

In the process of BSP upgrade of LC module, all the online LC modules will be displayed in the upgrade interface. It is allowed to select multiple LC modules or only one LC module.



LC Bsp Upgrade

File Name: Fu_BSP_OTN5.20-2018010233.tAR.txt

Please select the card to upgrade LC BSP:

☑3

Figure 0-26 BSP Upgrade of LC Module

After it is successfully upgraded, the business module will automatically reboot. When the reboot is successful, the BSP upgrade will take effect.

# Chapter 5 Alarm Management

## 5.1. Alarm Management Introduction

### 5.1.1. Alarm Management Overview

Alarm management function is a function group that manages the failures of all kinds of network equipment during the operation of the NMS system. This function group calls the fault that it manages as alarm.

There are two kinds of alarms—device alarm and background alarm.

■ Device alarm is the alarm issued directly by network devices.

■ Background alarm is a system alarm which is produced by the NMS system itself according to the threshold value of some pre-set operating parameters, such as performance alarm, system management alarm etc.

Alarm management can also monitor and manage events and notifications in the network.

The faults and events in the whole network can be centrally monitored and managed through alarm management function. Users can make real-time monitoring of the alarm in the network, can view and even filter the alarms that they do not need to see according to certain conditions. The alarm can be presented to the network maintenance personnel in the intuitive way of sound, light and so on.

After the alarm occurs, the user can confirm/counter-confirm the alarm. He can also clear the alarm, notify it to other person by mail or SMS, and can view the detailed information of the alarm and the events related to the alarm.

If the user sums up the processing mode of the alarms and puts it into the alarm processing suggestion library, when the similar alarm occurs again, the user can view the corresponding alarm processing suggestion and shorten the time to solve the problem.

In general, we can achieve the purpose of centralized management and monitoring of alarms, events and notifications in the network through alarm management function.

### 5.1.2.Alarm Management Interface

Click*"Fault Management"*in the menu of the main interface, the following window will pop up:

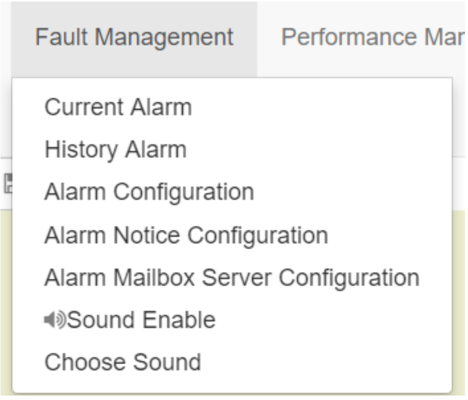


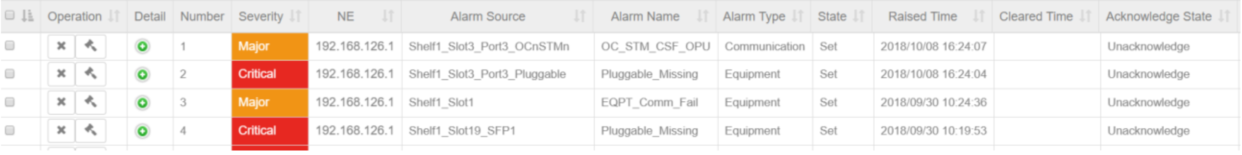
Figure 0-1 Alarm Management Menu

There are six items in the menu: current alarm, history alarm, alarm configuration, alarm notice configuration, alarm mailbox server configuration and sound enable.

### 5.1.3.Alarm Level

There are four alarm levels—emergency, main, secondary and warning.

Different colors are used to distinguish the different levels of alarms: emergency--red, main—orange, secondary—light yellow, warning—light blue.



| ☐ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | ✖ ⚒ | ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge |
| ☐ | ✖ ⚒ | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge |
| ☐ | ✖ ⚒ | ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge |
| ☐ | ✖ ⚒ | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Unacknowledge |

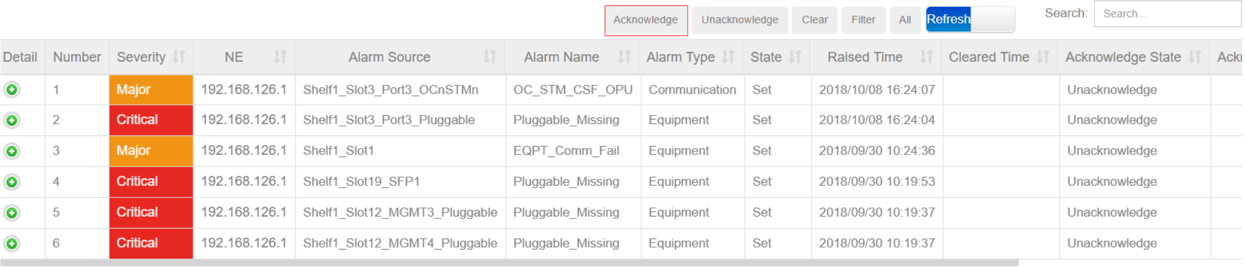
Figure 0-2 Alarm Level

## 5.2.Alarm Processing

### 5.2.1.Confirm Alarm

Alarm confirmation is to convert an alarm from unconfirmed state to confirmed state. For an unconfirmed alarm, the user can use this function to confirm it and only the current alarm has this function.

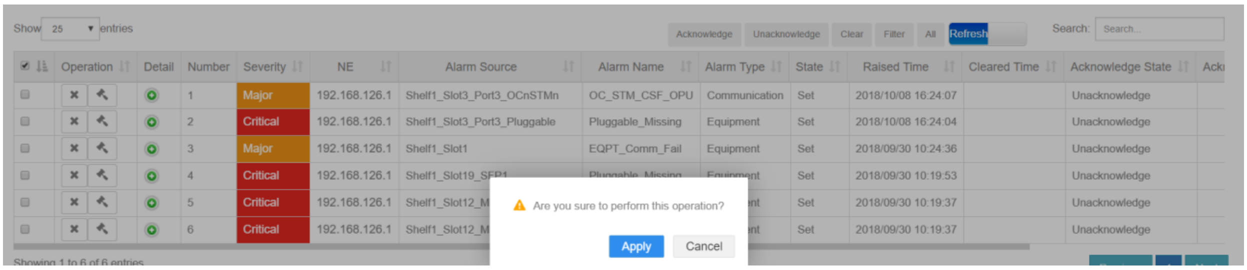
The operation steps are as follows: tick one or multiple alarms from the current alarms, then click "OK" in the main menu of current alarm to confirm the selected alarms.



| Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ack |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge | |
| ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge | |
| ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge | |
| ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Unacknowledge | |
| ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Unacknowledge | |
| ⊕ | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Unacknowledge | |

Figure 0-3 Alarm Confirm

Tick "Select All" box in the left upper corner, and click the corresponding operation buttons to perform operations such as batch confirmation, batch cancellation, batch removal and so on, as shown in the figure below:

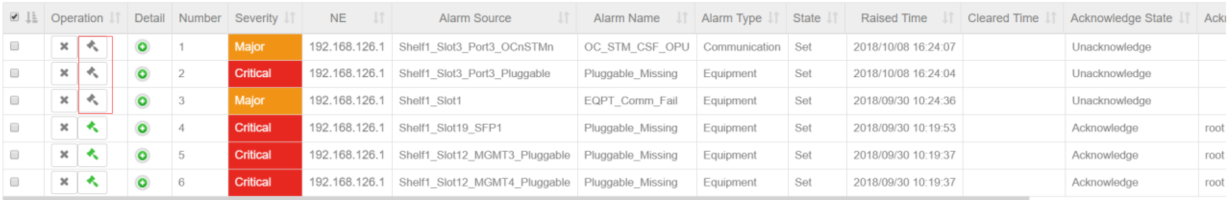


| ☑ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | ✖ ⚒ | ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge | |
| ☐ | ✖ ⚒ | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge | |
| ☐ | ✖ ⚒ | ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge | |
| ☐ | ✖ ⚒ | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Unacknowledge | |
| ☐ | ✖ ⚒ | ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_M | | nt | Set | 2018/09/30 10:19:37 | | Unacknowledge | |
| ☐ | ✖ ⚒ | ⊕ | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_M | | nt | Set | 2018/09/30 10:19:37 | | Unacknowledge | |

⚠ Are you sure to perform this operation?

Figure 0-4 Batch Alarm Confirmation

The columns of "confirmation person" and "confirmation time"in current alarm interface will display the user name and confirmation time of the login to the NMS system. Any current alarm can be confirmed by clicking the 🔨 button.



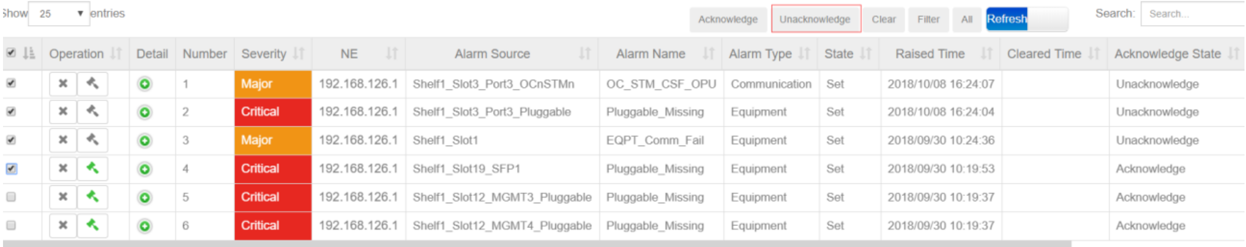
| ☑ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ 🔨 | ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge | |
| □ | ✖ 🔨 | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge | |
| □ | ✖ 🔨 | ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge | |
| □ | ✖ 🔨 | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Acknowledge | root |
| □ | ✖ 🔨 | ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge | root |
| □ | ✖ 🔨 | ⊕ | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge | root |

Figure 0-5 Confirm Current Alarm

## 5.2.2.Counter-Confirm Alarm

Counter-confirmation is to convert an alarm from confirmed state to unconfirmed state. For a confirmed alarm, the user can use this function to counter-confirm it.

The operation steps are as follows: tick one or multiple alarms from the current alarms, then click "Cancel Confirmation" in the main menu of current alarm to cancel the confirmation of the confirmed alarms.



| ☑ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ✖ 🔨 | ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge |
| ☑ | ✖ 🔨 | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge |
| ☑ | ✖ 🔨 | ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge |
| ☑ | ✖ 🔨 | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Acknowledge |
| □ | ✖ 🔨 | ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge |
| □ | ✖ 🔨 | ⊕ | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge |

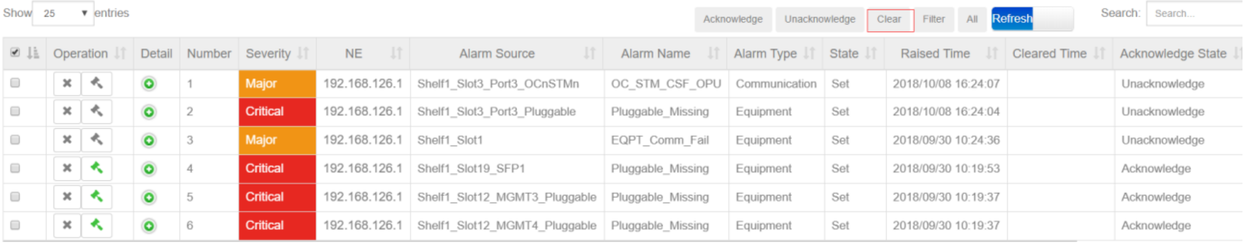
Figure 0-6 Cancel Confirmation

The confirmation of any current alarm can be canceled by clicking the 🔨 button.

## 5.2.3.Alarm Clear

This function is used to clear the current alarms. The steps are as follows:

Tick one or multiple alarms from the current alarms, and then click "Clear" in the main menu of current alarm to clear current alarms. (Only alarms that exist in the NMS system but do not exist in NE can be cleared.)



| ☑ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ 🔨 | ⊕ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge |
| □ | ✖ 🔨 | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge |
| □ | ✖ 🔨 | ⊕ | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 | | Unacknowledge |
| □ | ✖ 🔨 | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Acknowledge |
| □ | ✖ 🔨 | ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge |
| □ | ✖ 🔨 | ⊕ | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge |

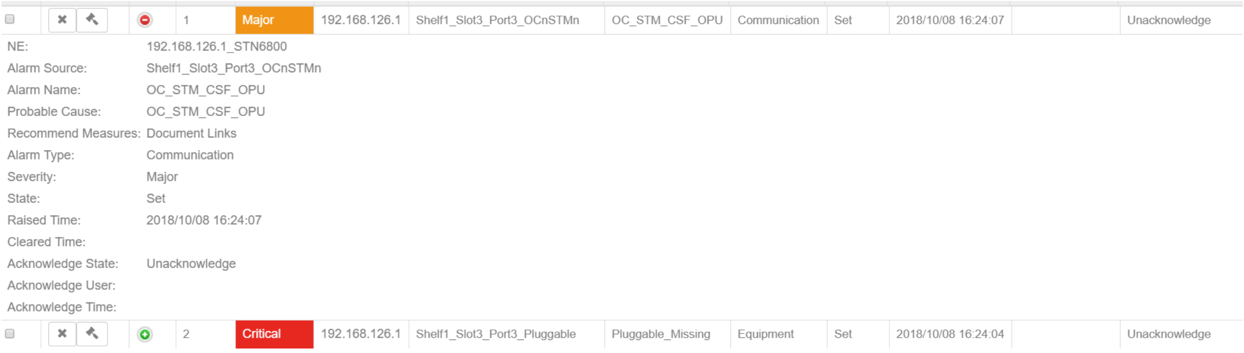
Figure 0-7 Clear Alarm

Any confirmed alarm can be cleared by clicking the ✖ button.

⚠ **This function is not available for customers now, only for internal debugging.**

### 5.2.4.Alarm Details

When the user needs to view the alarm details, he can click ⊕ button under "Details"and the details interface will pop up, as shown in the figure below:



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ 🔨 | ⊖ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge |

| | |
|---|---|
| NE: | 192.168.126.1_STN6800 |
| Alarm Source: | Shelf1_Slot3_Port3_OCnSTMn |
| Alarm Name: | OC_STM_CSF_OPU |
| Probable Cause: | OC_STM_CSF_OPU |
| Recommend Measures: | Document Links |
| Alarm Type: | Communication |
| Severity: | Major |
| State: | Set |
| Raised Time: | 2018/10/08 16:24:07 |
| Cleared Time: | |
| Acknowledge State: | Unacknowledge |
| Acknowledge User: | |
| Acknowledge Time: | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ 🔨 | ⊕ | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge |

Figure 0-8 Alarm Details

### 5.2.5.Alarm Synchronization

The alarm synchronization function can provide users with synchronous NE alarm. The user can select the NE location which needs to be synchronized.

When the user finds the alarm data of the NMS system is not consistent with that of the network equipment, he can use this function to synchronize the alarm data of specified location with that of the network equipment.

Select the NE which needs to achieve alarm synchronization, and right click *Synchronize Current Alarm*, then alarms of NE and NMS will keep the same.

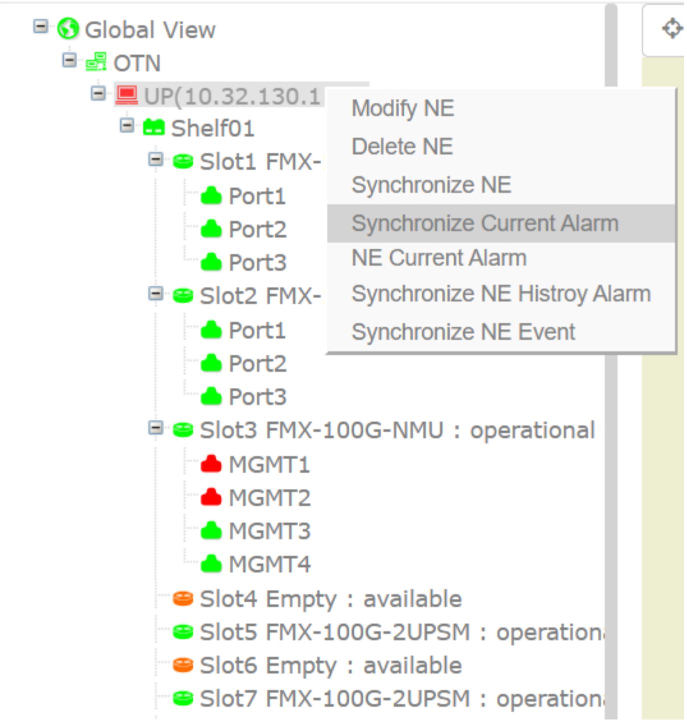


Figure 0-9 Synchronize Current Alarm

A prompt box which tells success will pop up. That means the alarm synchronization is completed.

## 5.3. Alarm Query

### 5.3.1. Current Alarm

#### Prerequisite

1. Start NMS server and successfully login the NMS system.

2. SNMP is successfully configured.

#### Related Information

Obtain real-time alarm of NE.

#### Steps

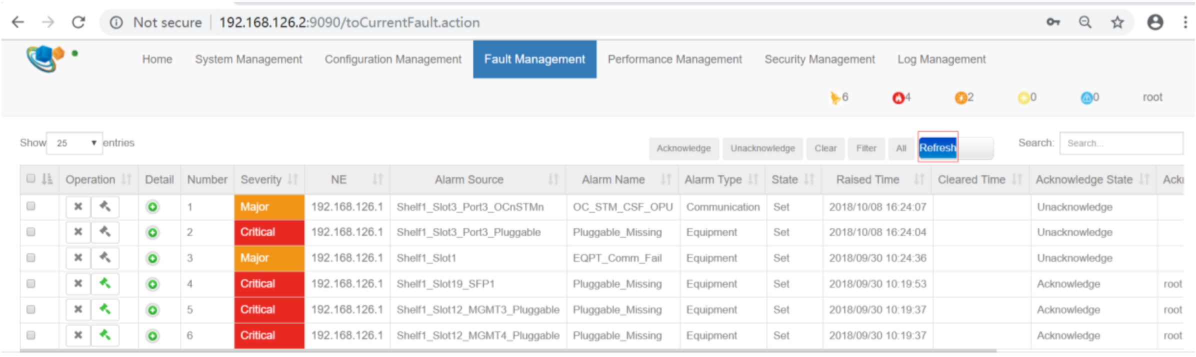
There are three ways to enter the current alarm window:

(1) Click “Fault Management→ Current Alarm” on the navigation bar.

(2) Select and right click NE, and then choose “NE Current Alarm”.

(3) Select and right click the slot, and then choose “Card Current Alarm” to enter the current alarm window of the card, as shown in the figure below.

Move the mouse to the fifth icon on the left side of root (which is on the upper right corner), the number of all uncleared and unconfirmed alarms at each alarm level can be viewed. By clicking the icon, you can enter the alarm interface that displays the corresponding alarm level.



| □ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ | ● | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 |  | Unacknowledge |  |
| □ | ✖ | ● | 2 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 |  | Unacknowledge |  |
| □ | ✖ | ● | 3 | Major | 192.168.126.1 | Shelf1_Slot1 | EQPT_Comm_Fail | Equipment | Set | 2018/09/30 10:24:36 |  | Unacknowledge |  |
| □ | ✖ | ● | 4 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 |  | Acknowledge | root |
| □ | ✖ | ● | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 |  | Acknowledge | root |
| □ | ✖ | ● | 6 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 |  | Acknowledge | root |

Figure 0-10 Current Alarm

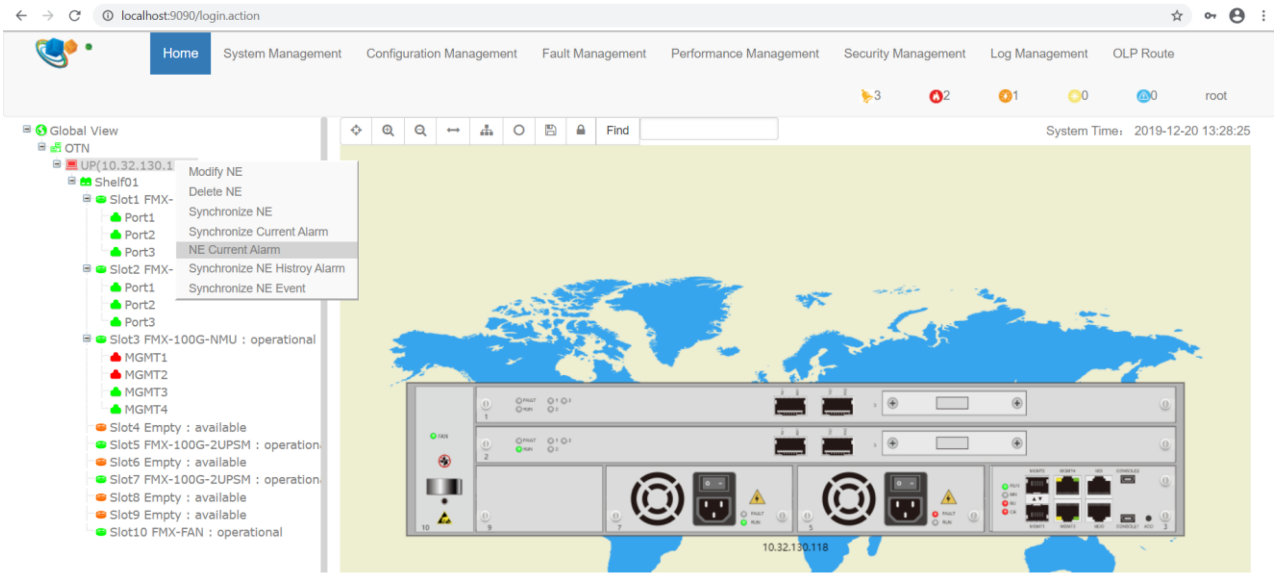


Figure 0-11 NE Current Alarm

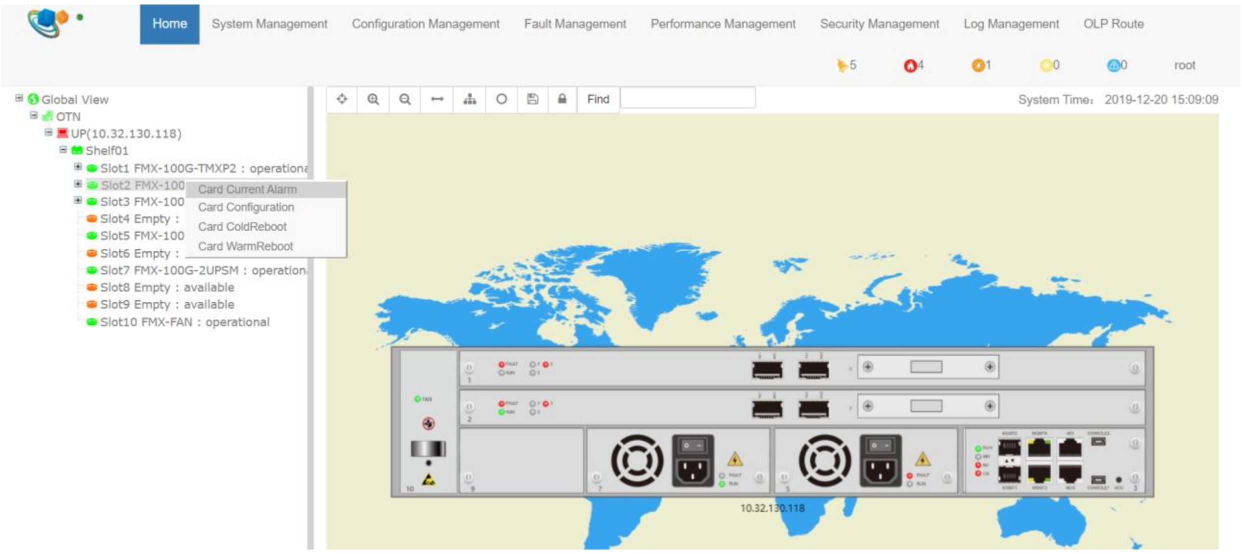
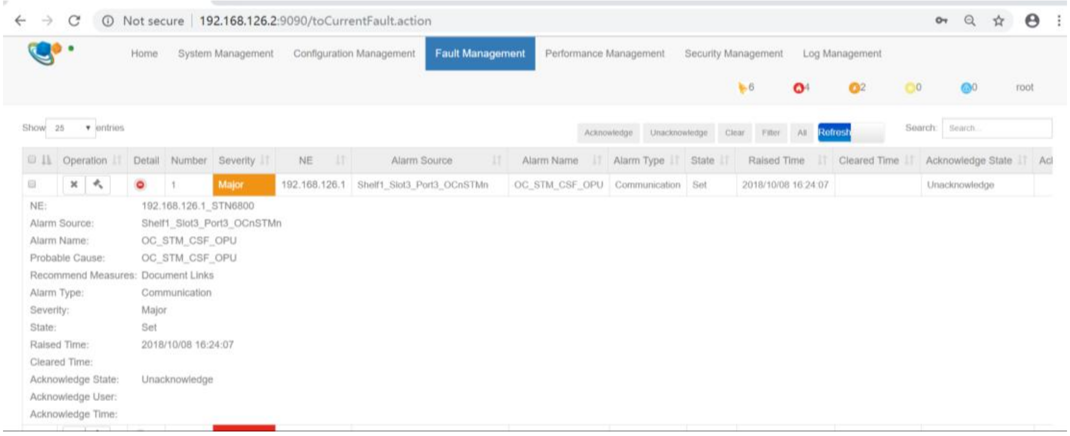


Figure 0-12 Card Current Alarm

When alarm occurs to the NE, the NMS will automatically collect current alarms through Trap. The user can view, clear (by clicking ✖ button), or confirm (by clicking 🔨 button) the alarms. When the user needs to view the alarm details, he can click ⊕ button under "Details", then the window which shows the alarm details will pop up.

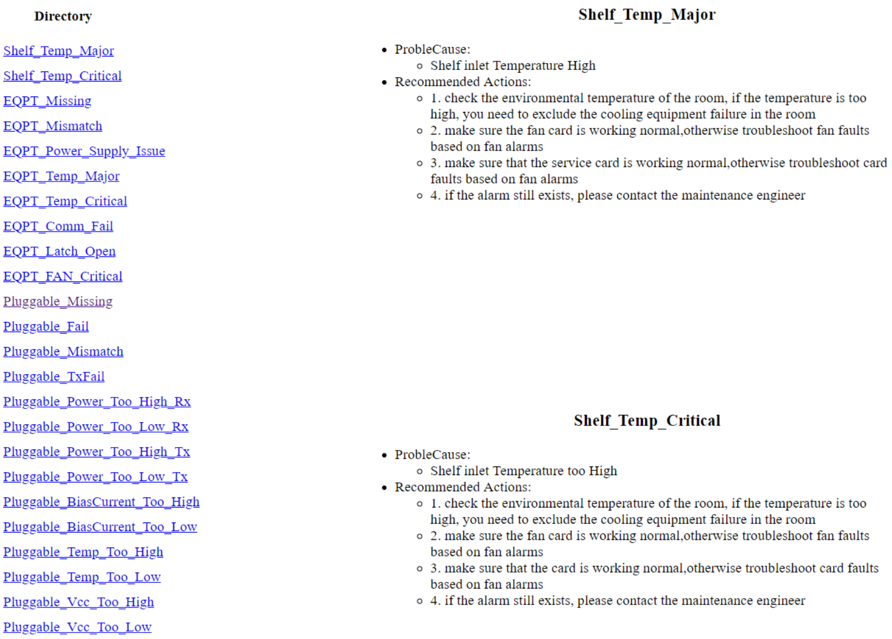


| □ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ac |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ✖ 🔨 | ⊖ | 1 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge | |

NE: 192.168.126.1_STN6800
Alarm Source: Shelf1_Slot3_Port3_OCnSTMn
Alarm Name: OC_STM_CSF_OPU
Probable Cause: OC_STM_CSF_OPU
Recommend Measures: Document Links
Alarm Type: Communication
Severity: Major
State: Set
Raised Time: 2018/10/08 16:24:07
Cleared Time:
Acknowledge State: Unacknowledge
Acknowledge User:
Acknowledge Time:

Figure 0-13 Current Alarm-Alarm Details

Click "Document Link" in NE Information, causes of the alarm and suggested measures can be viewed, as shown in the figure below:



**Directory**

Shelf_Temp_Major
Shelf_Temp_Critical
EQPT_Missing
EQPT_Mismatch
EQPT_Power_Supply_Issue
EQPT_Temp_Major
EQPT_Temp_Critical
EQPT_Comm_Fail
EQPT_Latch_Open
EQPT_FAN_Critical
Pluggable_Missing
Pluggable_Fail
Pluggable_Mismatch
Pluggable_TxFail
Pluggable_Power_Too_High_Rx
Pluggable_Power_Too_Low_Rx
Pluggable_Power_Too_High_Tx
Pluggable_Power_Too_Low_Tx
Pluggable_BiasCurrent_Too_High
Pluggable_BiasCurrent_Too_Low
Pluggable_Temp_Too_High
Pluggable_Temp_Too_Low
Pluggable_Vcc_Too_High
Pluggable_Vcc_Too_Low

**Shelf_Temp_Major**

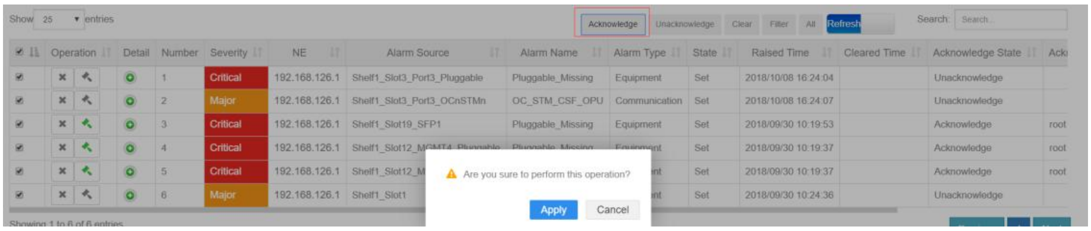
- ProbleCause:
  - Shelf inlet Temperature High
- Recommended Actions:
  - 1. check the environmental temperature of the room, if the temperature is too high, you need to exclude the cooling equipment failure in the room
  - 2. make sure the fan card is working normal,otherwise troubleshoot fan faults based on fan alarms
  - 3. make sure that the service card is working normal,otherwise troubleshoot card faults based on fan alarms
  - 4. if the alarm still exists, please contact the maintenance engineer

**Shelf_Temp_Critical**

- ProbleCause:
  - Shelf inlet Temperature too High
- Recommended Actions:
  - 1. check the environmental temperature of the room, if the temperature is too high, you need to exclude the cooling equipment failure in the room
  - 2. make sure the fan card is working normal,otherwise troubleshoot fan faults based on fan alarms
  - 3. make sure that the card is working normal,otherwise troubleshoot card faults based on fan alarms
  - 4. if the alarm still exists, please contact the maintenance engineer

Figure 0-14 Alarm-Document Link

Tick "Select All" box in the left upper corner, and click the corresponding operation buttons to perform operations such as batch confirmation, batch cancellation, batch removal and so on, as shown in the figure below:



Show 25 entries

| ☑ | Operation | Detail | Number | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ✖ | ⊕ | 1 | Critical | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Set | 2018/10/08 16:24:04 | | Unacknowledge | |
| ☑ | ✖ | ⊕ | 2 | Major | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Set | 2018/10/08 16:24:07 | | Unacknowledge | |
| ☑ | ✖ | ⊕ | 3 | Critical | 192.168.126.1 | Shelf1_Slot19_SFP1 | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:53 | | Acknowledge | root |
| ☑ | ✖ | ⊕ | 4 | Critical | 192.168.126.1 | Shelf1_Slot12_MGMT4_Pluggable | Pluggable_Missing | Equipment | Set | 2018/09/30 10:19:37 | | Acknowledge | root |
| ☑ | ✖ | ⊕ | 5 | Critical | 192.168.126.1 | Shelf1_Slot12_M | | nt | Set | 2018/09/30 10:19:37 | | Acknowledge | root |
| ☑ | ✖ | ⊕ | 6 | Major | 192.168.126.1 | Shelf1_Slot1 | | nt | Set | 2018/09/30 10:24:36 | | Unacknowledge | |

Showing 1 to 6 of 6 entries

Are you sure to perform this operation?

Figure 0-15 Batch Confirmation

The user can manually synchronize alarm. The operation steps are as follows: Return to the Home Page→ Right Click NE name→ Synchronize Current Alarm.

Tips:

(1) The SNMP Trap port monitored by the NMS is 16222.

(2) Configure “Trap Host” of NE as local IP address, and “Trap Port” is 16222.

(3) Unique location of the alarm is realized by NE + Alarm Source + Alarm Name.

## The alarm processing logic is as follows:

(1) Report the alarm processing flow of Trap according to NE.

When alarm is generated, NE will report the alarm and generate trap, and the alarm status is SET.

■ Situation 1

When SET notice is received, the current alarm database does not have the same alarm as SET, and then a new record is added to the current alarm.

■ Situation 2

After receiving SET notice, if there are same alarms with the status of SET in the current alarms of the database (no matter whether the generation time is the same), then the status of the same alarms needs to be set as synchronous removal (If confirmed, move to history alarm.) The received new alarm will add a new record in the current alarm.

When the alarm is removed, NE will report to clear trap, and the alarm status is CLEAR.

■ Situation 3

After receiving CLEAR notice, if there are same alarms with the status of SET in the current alarms of the database, then the status of the same alarms needs to be set as synchronous removal. (If confirmed, then clear the confirmation user and time.)

■ Situation 4

After receiving CLEAR notice, if there is no same alarm with the status of SET in the current alarms of the database, then add a new record in the current alarm. (There is no generation time, but only clear time. The status needs to be set as synchronous removal.)

(1) The processing flow of manual removal of alarms by the user is as follows:

For the current alarm which is not removed, it provides manual removal function. If the alarm still exists in NE (by judging the time stamp), then it cannot be removed. If it is allowed to be removed, set the alarm status as manual removal. (If confirmed, move to history alarm.)

(2) The processing flow of counter-confirmation alarm is as follows when the user manually confirms the alarm:

- Situation 1

It provides alarm confirmation function to the current alarm. After the confirmation, the confirmation user and time need to be recorded. (If removed, move to history alarm.)

- Situation 2

It allows counter-confirmation of the current alarms which have been confirmed. After the counter confirmation, clear the confirmation user and time.

- Situation 3

When the non-removed alarms which have been confirmed are removed, after the confirmation user and time are removed, they need to be confirmed once again before being moved to history alarm.

- Situation 4

It supports batch confirmation and batch removal of alarms. A window to ask whether you are sure to confirm or clear will pop up.

Counter confirmation button:

1) While making batch confirmation of alarms, if the selected alarm has been confirmed before, then the confirmation of this alarm will be ignored.

2)While making batch counter confirmation of alarms, if the selected alarm has not been confirmed before, then the counter confirmation of this alarm will be ignored.

(3) The processing flow of NMS automatic periodic synchronization of alarms:

When starting the NMS, it will synchronize all the online NE alarms. The NMS will trigger the automatic synchronization alarm. During the operation of NMS, automatic synchronization of all online NE alarms will be realized periodically. The processing steps are the same as that of manual alarm.

(4) Processing flow of manual synchronization of current alarm by the user:

When the user manually synchronizes the alarms, he needs to read the current alarms of NMS and NE, and make a comparison. (The time stamp needs to be compared.)

If alarm exists in NMS, but not in NE, the alarm status needs to be set as synchronous removal. (If confirmed, move to history alarm.)

1) If alarm exists in NE, but not in NMS, a new record needs to be added to the current alarm.

2) If alarm exists both in NE and NMS, there is no need to process it.

### 5.3.2.History Alarm

#### Prerequisite

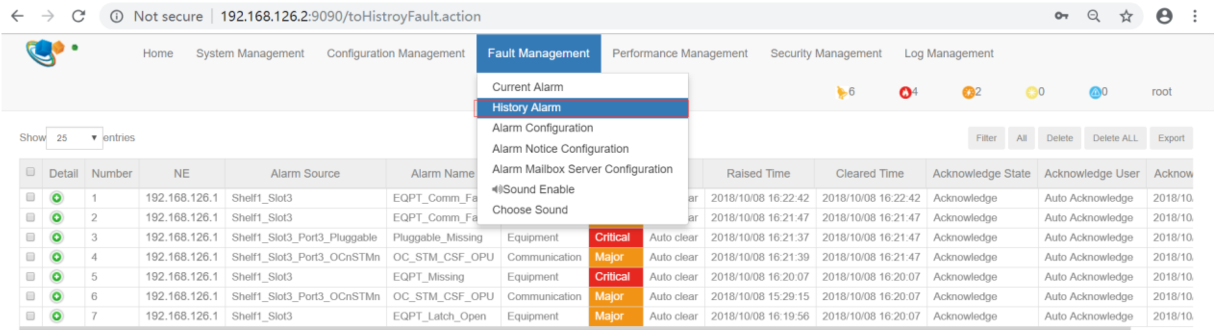
Start the NMS server and successfully login the NMS.

## Related Information

Get history alarm information. The current alarm becomes a history alarm after it is deleted.

## Steps

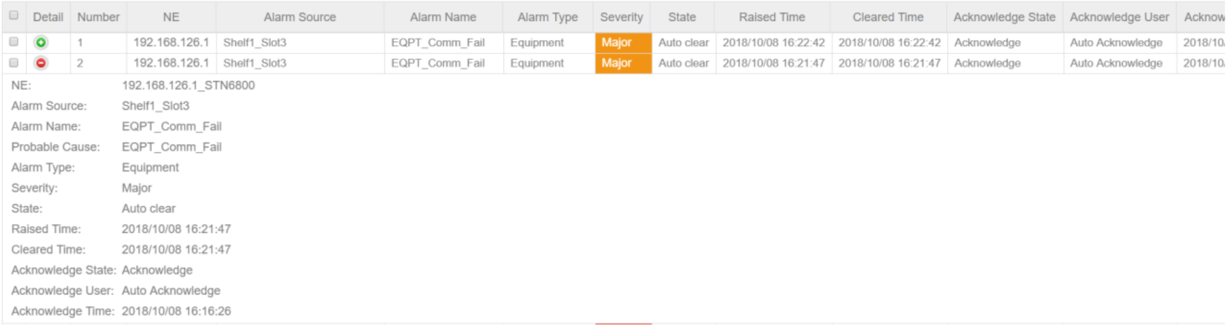
Click “Fault Management→ History Alarm” on the navigation bar to enter the history alarm window.



| □ | Detail | Number | NE | Alarm Source | Alarm Name | | | | Raised Time | Cleared Time | Acknowledge State | Acknowledge User | Acknow |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ⊕ | 1 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fa | | | ar | 2018/10/08 16:22:42 | 2018/10/08 16:22:42 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 2 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fa | | | ar | 2018/10/08 16:21:47 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 3 | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:21:37 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 4 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 16:21:39 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 5 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:20:07 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 6 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 15:29:15 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 7 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Latch_Open | Equipment | Major | Auto clear | 2018/10/08 16:19:56 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |

Figure 0-16 History Alarm

The user can click ⊕ button under “Details” to view detailed information.



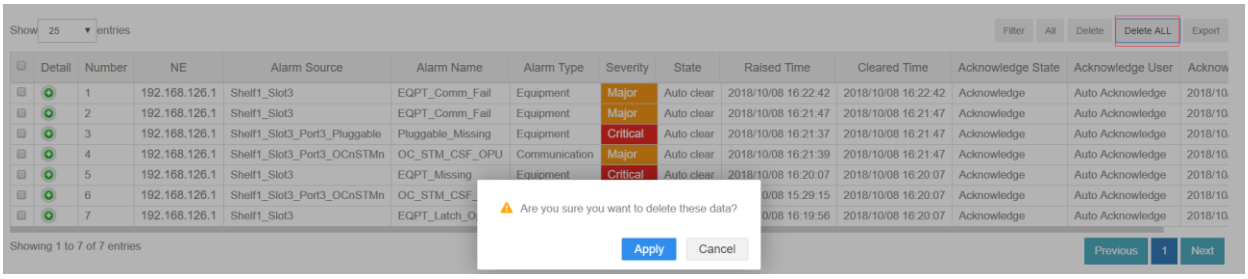
| □ | Detail | Number | NE | Alarm Source | Alarm Name | Alarm Type | Severity | State | Raised Time | Cleared Time | Acknowledge State | Acknowledge User | Acknow |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ⊕ | 1 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:22:42 | 2018/10/08 16:22:42 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊖ | 2 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:21:47 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |

| | |
|---|---|
| NE: | 192.168.126.1_STN6800 |
| Alarm Source: | Shelf1_Slot3 |
| Alarm Name: | EQPT_Comm_Fail |
| Probable Cause: | EQPT_Comm_Fail |
| Alarm Type: | Equipment |
| Severity: | Major |
| State: | Auto clear |
| Raised Time: | 2018/10/08 16:21:47 |
| Cleared Time: | 2018/10/08 16:21:47 |
| Acknowledge State: | Acknowledge |
| Acknowledge User: | Auto Acknowledge |
| Acknowledge Time: | 2018/10/08 16:16:26 |

Figure 0-17 History Alarm Details

Tick the check box on the left side, select the alarms which need to be deleted ( It is allowed to select all), and you can delete the history alarms by clicking “Delete” button, as shown in

the figure below:



| □ | Detail | Number | NE | Alarm Source | Alarm Name | Alarm Type | Severity | State | Raised Time | Cleared Time | Acknowledge State | Acknowledge User | Acknow |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ⊕ | 1 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:22:42 | 2018/10/08 16:22:42 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 2 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:21:47 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 3 | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:21:37 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 4 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 16:21:39 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 5 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:20:07 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 6 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_ | | | | 0/08 15:29:15 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 7 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Latch_O | | | | 0/08 16:19:56 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |

Showing 1 to 7 of 7 entries

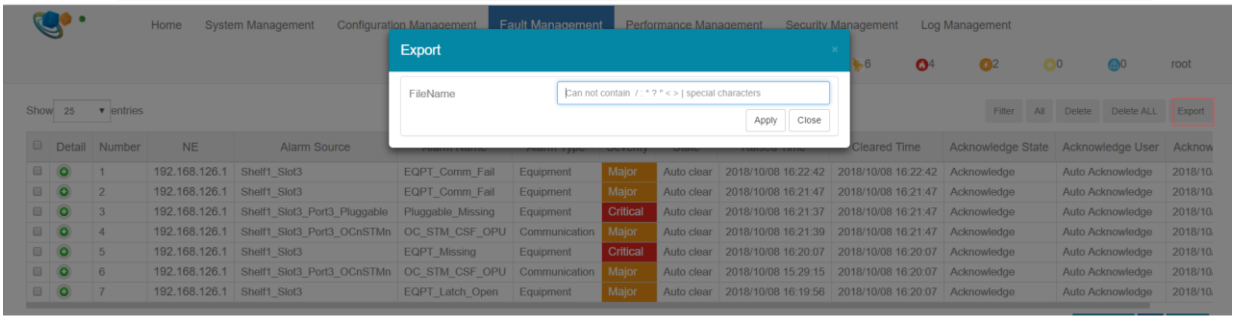
Are you sure you want to delete these data?

Figure 0-18 Delete History Alarm

## 5.4. Alarm Record Maintenance

### 5.4.1. Alarm Export

Tick the history alarm which needs to be exported, and click "Export" button, the history alarm data can be exported. The data will be saved to the report_out folder in the installation root directory, as shown in the figure below:



Export

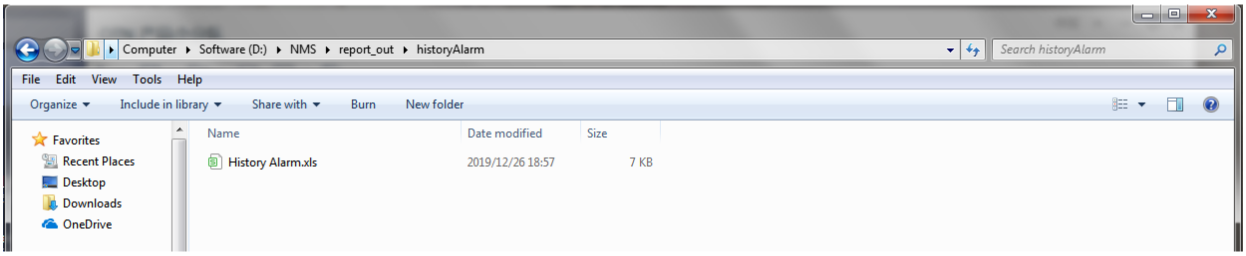
FileName: Can not contain / : * ? " < > | special characters

Apply Close

Show 25 entries

| □ | Detail | Number | NE | Alarm Source | Alarm Name | Alarm Type | Severity | State | Raised Time | Cleared Time | Acknowledge State | Acknowledge User | Acknow |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ⊕ | 1 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:22:42 | 2018/10/08 16:22:42 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 2 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fail | Equipment | Major | Auto clear | 2018/10/08 16:21:47 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 3 | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:21:37 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 4 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 16:21:39 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 5 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:20:07 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 6 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 15:29:15 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ⊕ | 7 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Latch_Open | Equipment | Major | Auto clear | 2018/10/08 16:19:56 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |

Figure 0-19 Export History Alarm



| Name | Date modified | Size |
|---|---|---|
| History Alarm.xls | 2019/12/26 18:57 | 7 KB |

Figure 0-20 History Alarm

## 5.5. Alarm Configuration

The alarm configuration function has many user-defined rules. Many operations and processes of the alarm are carried out around the rules. The setting of alarm rules allows users to add, delete, modify, refresh, activate and suspend various rules.

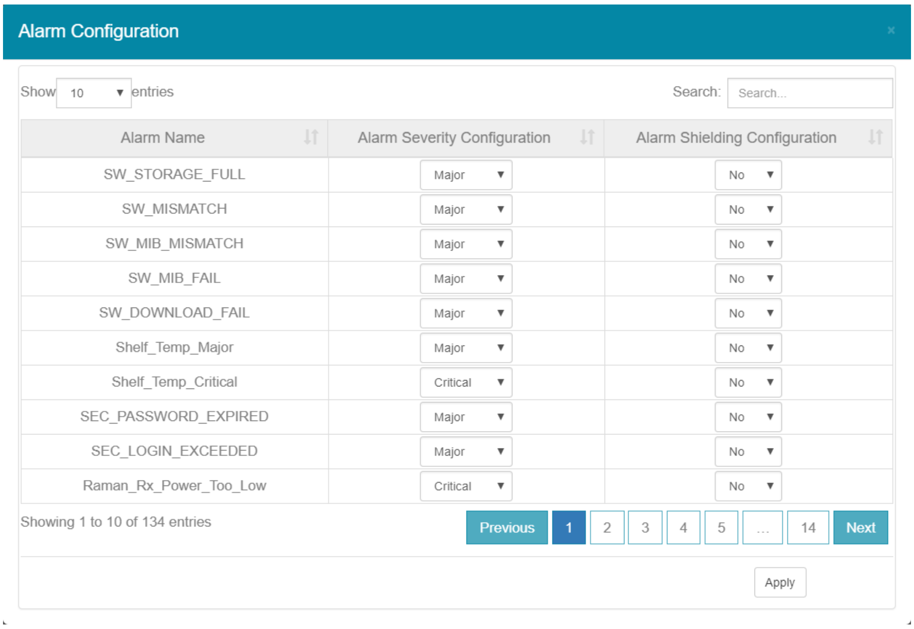
The scope of effect for alarm rules is:

1) Overall effect: Once an alarm rule is set up and activated, it will take effect on all alarms (events and notices) that conform to the rule. It has nothing to do with who makes the rule. The alarms which can be seen by all the users are processed by the rule.

2) User effect: Once an alarm rule is set up and activated, the rule is only effective for the user who makes the rule (e.g. user filtering rule). There is not any effect on other users.

3) Forward effect: Once an alarm rule is set up and activated, the rule is effective to all the current alarms (including alarms which have been reported and will be reported in the future).

4) Backward effect: Once an alarm rule is set up and activated, the rule is only effective to alarms which will be reported in the future, but not effective to alarms which have been reported.



Alarm Configuration

Show 10 entries        Search: Search...

| Alarm Name | Alarm Severity Configuration | Alarm Shielding Configuration |
|---|---|---|
| SW_STORAGE_FULL | Major | No |
| SW_MISMATCH | Major | No |
| SW_MIB_MISMATCH | Major | No |
| SW_MIB_FAIL | Major | No |
| SW_DOWNLOAD_FAIL | Major | No |
| Shelf_Temp_Major | Major | No |
| Shelf_Temp_Critical | Critical | No |
| SEC_PASSWORD_EXPIRED | Major | No |
| SEC_LOGIN_EXCEEDED | Major | No |
| Raman_Rx_Power_Too_Low | Critical | No |

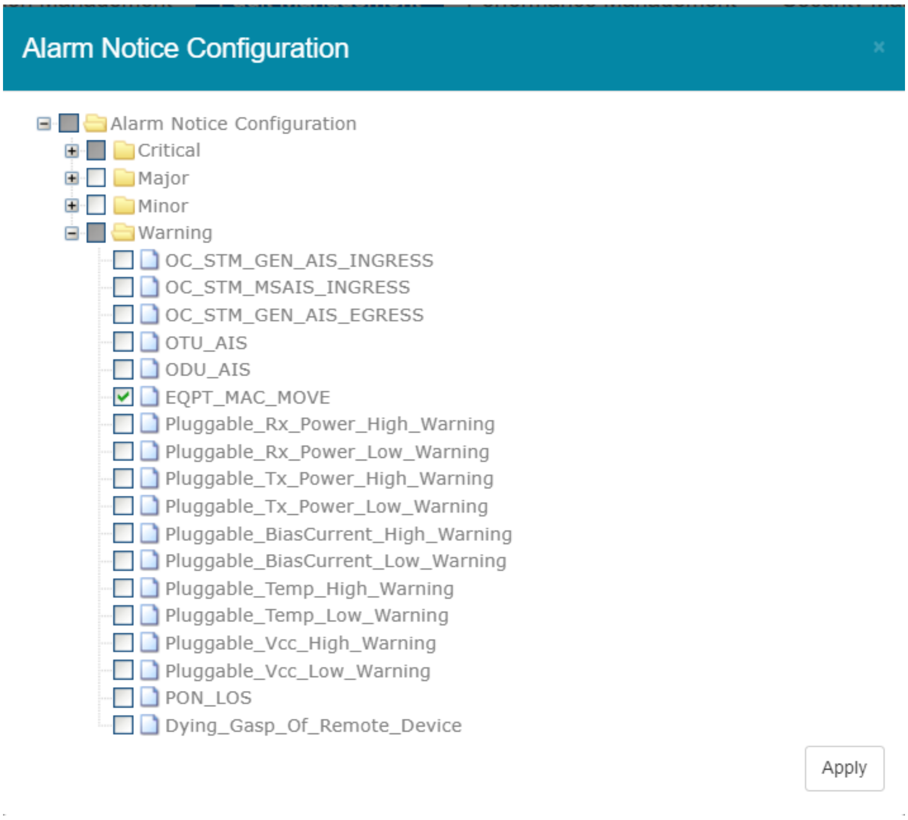
Showing 1 to 10 of 134 entries

Figure 0-21 Alarm Configuration

## 5.6. Alarm Notice

### 5.6.1. Alarm Notice Configuration

Alarm notice configuration is used to configure whether to send the notice of corresponding alarms. The alarm configuration is classified into “emergency”, “main”, “secondary” and “warning” according to the alarm level. By default, it configures the notices of all emergent alarms. The user can make the configuration according to actual needs.



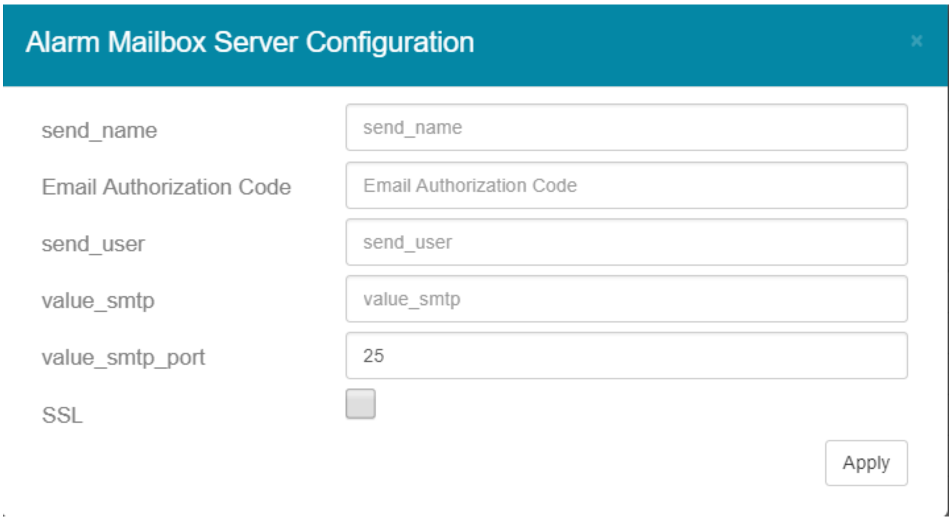
Alarm Notice Configuration

- ⊟ ■ Alarm Notice Configuration
  - ⊞ ■ Critical
  - ⊞ □ Major
  - ⊞ □ Minor
  - ⊟ ■ Warning
    - □ OC_STM_GEN_AIS_INGRESS
    - □ OC_STM_MSAIS_INGRESS
    - □ OC_STM_GEN_AIS_EGRESS
    - □ OTU_AIS
    - □ ODU_AIS
    - ☑ EQPT_MAC_MOVE
    - □ Pluggable_Rx_Power_High_Warning
    - □ Pluggable_Rx_Power_Low_Warning
    - □ Pluggable_Tx_Power_High_Warning
    - □ Pluggable_Tx_Power_Low_Warning
    - □ Pluggable_BiasCurrent_High_Warning
    - □ Pluggable_BiasCurrent_Low_Warning
    - □ Pluggable_Temp_High_Warning
    - □ Pluggable_Temp_Low_Warning
    - □ Pluggable_Vcc_High_Warning
    - □ Pluggable_Vcc_Low_Warning
    - □ PON_LOS
    - □ Dying_Gasp_Of_Remote_Device

Figure 0-22 Alarm Notice Configuration

### 5.6.2.Alarm Mailbox Server Configuration

Alarm mailbox server configuration is used to configure the information about the mailbox which is used to send alarm information, and to set SMTP address and SMTP port information.

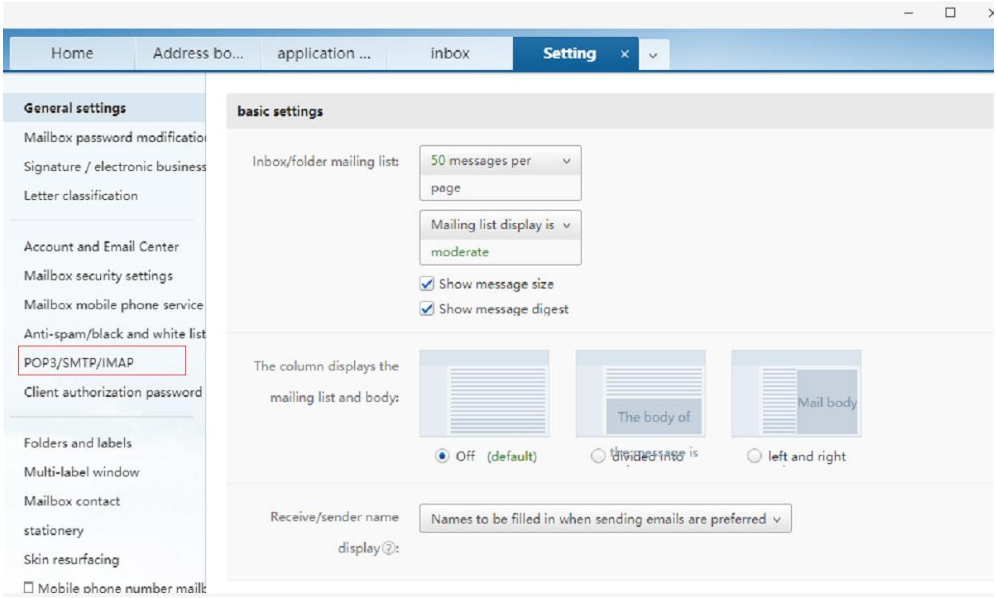


Alarm Mailbox Server Configuration

| | |
|---|---|
| send_name | send_name |
| Email Authorization Code | Email Authorization Code |
| send_user | send_user |
| value_smtp | value_smtp |
| value_smtp_port | 25 |
| SSL | □ |

Figure 0-23 Alarm Mailbox Server Configuration

After the above configuration is completed, you need to login to the corresponding mailbox, such as the 163 mailbox configured in the figure above. After you login to the 163 mailbox, click “settings”, and select POP3/SMTP/IMAP option. After you enter the page, tick the two selection boxes of“POP3/SMTP service” and “IMAP/SMTP service”, as shown in the figure below:



Home
Address bo...
application ...
inbox
Setting
General settings
Mailbox password modificatio
Signature / electronic business
Letter classification
Account and Email Center
Mailbox security settings
Mailbox mobile phone service
Anti-spam/black and white list
POP3/SMTP/IMAP
Client authorization password
Folders and labels
Multi-label window
Mailbox contact
stationery
Skin resurfacing
□ Mobile phone number mailb

basic settings

Inbox/folder mailing list: 50 messages per page

Mailing list display is moderate

☑ Show message size

☑ Show message digest

The column displays the mailing list and body: ● Off (default) ○ the message is divided into ○ left and right

Receive/sender name display: Names to be filled in when sending emails are preferred

Figure 0-24 Mailbox Server Configuration

**A user account can only add one mail address.**

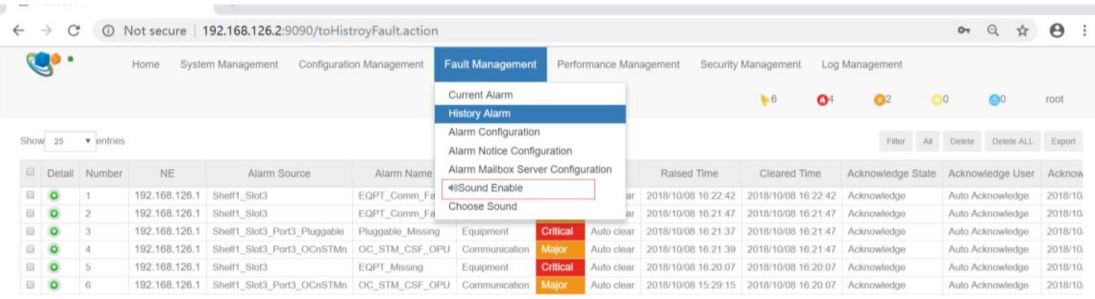
## 5.6.3.Sound Enable

Click "Sound Enable" to enable the alarm sound which is corresponding to the highest level of alarm (which is the highest-level alarm in the current alarm page. Confirmation and removal will not affect the highest-level alarm.)

Every time the page is refreshed or entered, the alarm sound will be reset to disabled, and the user needs to enable it manually.

After the highest-level alarm is confirmed or removed, its alarm sound cannot be automatically switched to the low-level one. It needs to disable the sound manually and then re-enable it.

All the current alarms are moved to the history alarm, and the sound is automatically stopped.



192.168.126.2:9090/toHistroyFault.action

Show 25 entries

| □ | Detail | Number | NE | Alarm Source | Alarm Name | | | | Raised Time | Cleared Time | Acknowledge State | Acknowledge User | Acknow |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | ● | 1 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fa | | | ar | 2018/10/08 16:22:42 | 2018/10/08 16:22:42 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ● | 2 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Comm_Fa | | | ar | 2018/10/08 16:21:47 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ● | 3 | 192.168.126.1 | Shelf1_Slot3_Port3_Pluggable | Pluggable_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:21:37 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ● | 4 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 16:21:39 | 2018/10/08 16:21:47 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ● | 5 | 192.168.126.1 | Shelf1_Slot3 | EQPT_Missing | Equipment | Critical | Auto clear | 2018/10/08 16:20:07 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |
| □ | ● | 6 | 192.168.126.1 | Shelf1_Slot3_Port3_OCnSTMn | OC_STM_CSF_OPU | Communication | Major | Auto clear | 2018/10/08 15:29:15 | 2018/10/08 16:20:07 | Acknowledge | Auto Acknowledge | 2018/10. |

Figure 0-25 Sound Enable

# Chapter 6 Performance Management

## 6.1. Performance Management Introduction

Performance management mainly realizes the display, statistics and synthesis of network element performance and sends alarm information when network element performance is abnormal.

Performance management includes the management of history performance and real-time performance.

- The main function of the history performance is to set data collection of performance tasks and make data analysis.
- The main function of the real-time performance is to make real-time observation of the performance data.

## 6.2. Performance Management Configuration

### 6.2.1. Performance Monitoring Point Management

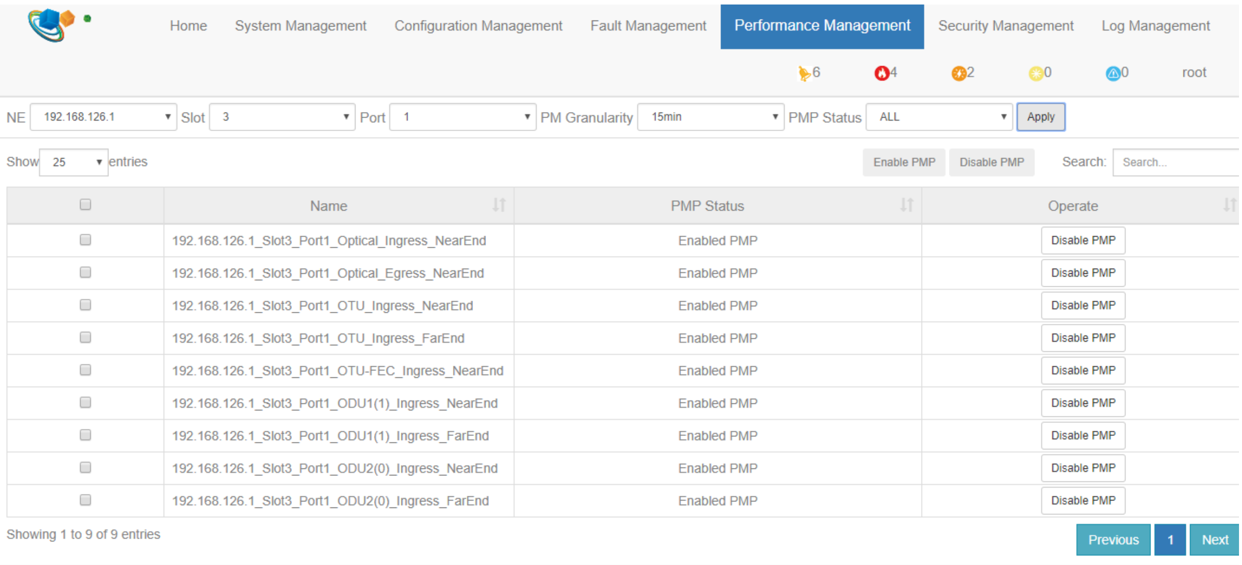
It includes the supported performance management point (PMP) and performance monitoring parameters.

The performance monitoring point (PMP) is determined only by the monitoring cycle and the ID, location and direction of PMP.

- Location of PMP: far-end and near-end (applicable for OTUk and ODUk).
- Near-end PMP: according to the received BIP8.
- Far-end PMP: according to the received BEI.
- Direction of PMP: ingress and egress.

### Steps

Click*"Performance Management"* → *"PMP Management"* on the navigation bar, you can enter the interface to set PMP. NE, channels, ports and time (monitoring time: 15 minutes, 24 hours) of performance monitoring can be set.



NE 192.168.126.1 Slot 3 Port 1 PM Granularity 15min PMP Status ALL

Show 25 entries

Search: Search...

| □ | Name | PMP Status | Operate |
|---|---|---|---|
| □ | 192.168.126.1_Slot3_Port1_Optical_Ingress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_Optical_Egress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_OTU_Ingress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_OTU_Ingress_FarEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_OTU-FEC_Ingress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_ODU1(1)_Ingress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_ODU1(1)_Ingress_FarEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_ODU2(0)_Ingress_NearEnd | Enabled PMP | Disable PMP |
| □ | 192.168.126.1_Slot3_Port1_ODU2(0)_Ingress_FarEnd | Enabled PMP | Disable PMP |

Showing 1 to 9 of 9 entries

Figure 0-1 PMP Management

### 6.2.2.Performance Monitoring Parameters Management

■The monitoring parameters of Optical monitoring point are: maximum optical power, minimum optical power, average optical power and record the time stamp.

■The monitoring parameters of OCh monitoring point are: maximum/minimum/average OSNR, CD, DGD and record the time stamps.

■The monitoring parameters of OTUk FEC monitoring point are: the error rate of maximum error correction, the error rate of average error correction and record the time stamps.

■The monitoring parameters of OTUk monitoring point are: background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds (UAS).

■The monitoring parameters of ODUk monitoring point are: background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds (UAS).

■The monitoring parameters of SDH/SONET monitoring point are: background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds (UAS).

■The monitoring parameters of Ethernet monitoring point are: normal frame number, uni-cast frame number, multicast frame number, broadcast frame number, CRC error frame, alignment error frame number, ultra long frame number, ultra long Jabber frame number (CRC error), ultra short frame number (CRC error), discarded frame number, ultra short frame number (CRC normal), 64-byte frame number, 65-127 byte frame number, 128-255 byte frame number, 256-511 byte frame number, 512-1023 byte frame number, 1024-11518 byte frame number, 1519-maximum byte frame number, ultra long frame number (CRC normal), normal pause frame number and total frame number.

### Steps

Click*"Performance Management"*→ *"Current Performance Statistics"*→ *"Performance Statistics"* on the navigation bar to enter the PMP settings interface.

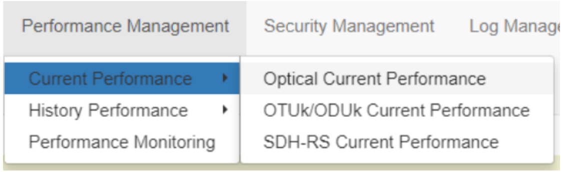


Figure 0-2 Performance Monitoring Parameters

### 6.2.3.Threshold Management

Threshold management includes query and setting of performance threshold. Task management needs to perform threshold alarm processing after polling and evaluating the performance variables that users care about.

After comparing the value with the threshold value which is set by the user, the corresponding alarm processing needs to be carried out for the value beyond the threshold range, and the alarm information needs to be sent to the alarm module.

At present, the parameters that support to set TCA alarm threshold are: background error code block (BBE), bit error second (ES), serious bit error second (SES) and unavailable second (UAS). Therefore, only OTUk/ODUk and SDH support threshold settings.

Different parameters correspond to different threshold values, and the ranges of monitoring threshold values for 15 minutes and 24 hours are different (that is, the monitoring threshold of 24 hours is 96 times that of 15 minutes).

- BBE: The threshold value range of 15 minutes is 1~2159100. The threshold value range of 24 hours is 1~207273600.
- ES: The threshold value range of 15 minutes is 1~900. The threshold value range of 24 hours is 1~86400.
- SES: The threshold value range of 15 minutes is 1~900. The threshold value range of 24 hours is 1~86400.
- UAS: The threshold value range of 15 minutes is 1~900. The threshold value range of 24 hours is 1~86400.

## 6.3. Current Performance Statistics

Current performance statistics are used to collect real-time data for the performance variables that the user is interested in. The values of these performance variables are displayed in forms, and necessary storage operations can be carried out.

### Prerequisite

1. Enable the performance monitoring point of the point.

2. The enable time is 15 minutes or 24 hours.

### Related Information

Obtain real-time current performance statistics data.

### Steps

Click*"Performance Management"*→ *"Current Performance Statistics"* on the navigation bar to enter current performance statistics interface.

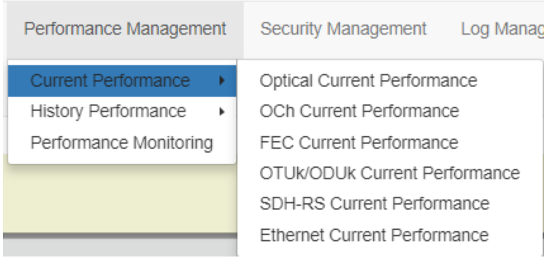
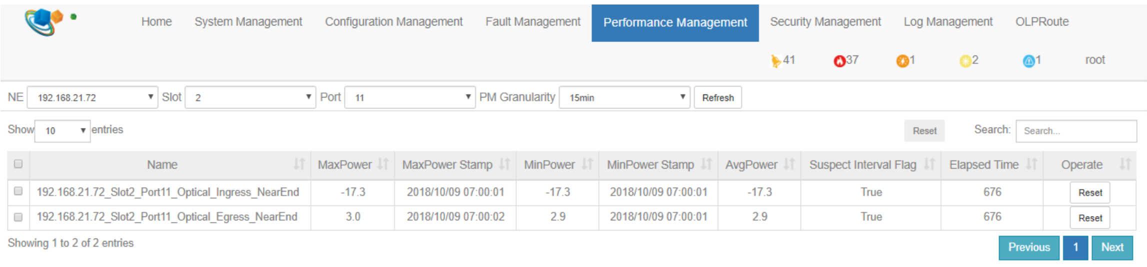


Figure 0-3 Current Performance Statistics



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

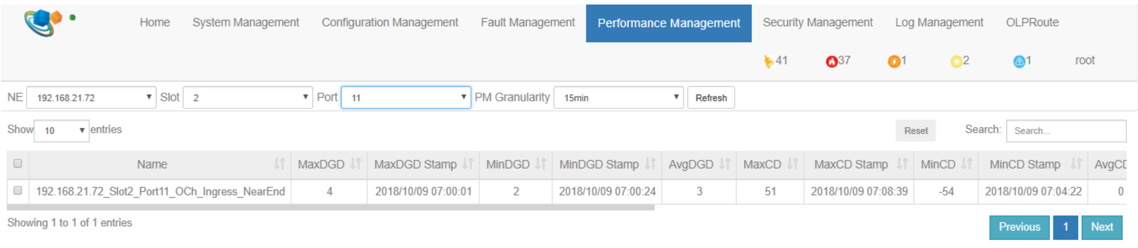
Show 10 entries

Search: Search...

| ☐ | Name | MaxPower | MaxPower Stamp | MinPower | MinPower Stamp | AvgPower | Suspect Interval Flag | Elapsed Time | Operate |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 192.168.21.72_Slot2_Port11_Optical_Ingress_NearEnd | -17.3 | 2018/10/09 07:00:01 | -17.3 | 2018/10/09 07:00:01 | -17.3 | True | 676 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_Optical_Egress_NearEnd | 3.0 | 2018/10/09 07:00:02 | 2.9 | 2018/10/09 07:00:01 | 2.9 | True | 676 | Reset |

Showing 1 to 2 of 2 entries

Figure 0-4 Current Performance Statistics of Optical Power



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

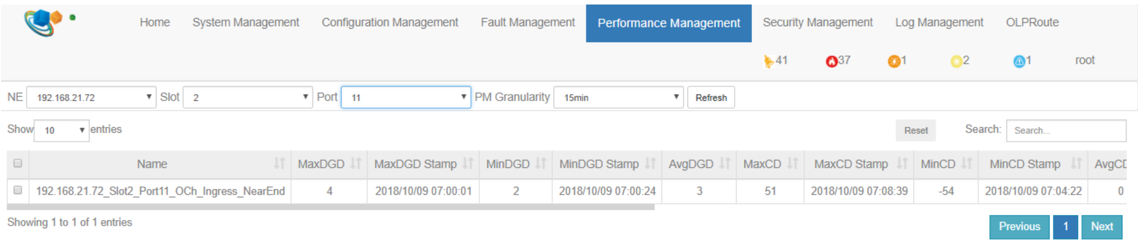
Show 10 entries

Search: Search...

| ☐ | Name | MaxDGD | MaxDGD Stamp | MinDGD | MinDGD Stamp | AvgDGD | MaxCD | MaxCD Stamp | MinCD | MinCD Stamp | AvgCD |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 192.168.21.72_Slot2_Port11_OCh_Ingress_NearEnd | 4 | 2018/10/09 07:00:01 | 2 | 2018/10/09 07:00:24 | 3 | 51 | 2018/10/09 07:08:39 | -54 | 2018/10/09 07:04:22 | 0 |

Showing 1 to 1 of 1 entries

Figure 0-5 OCh Current Performance Statistics



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

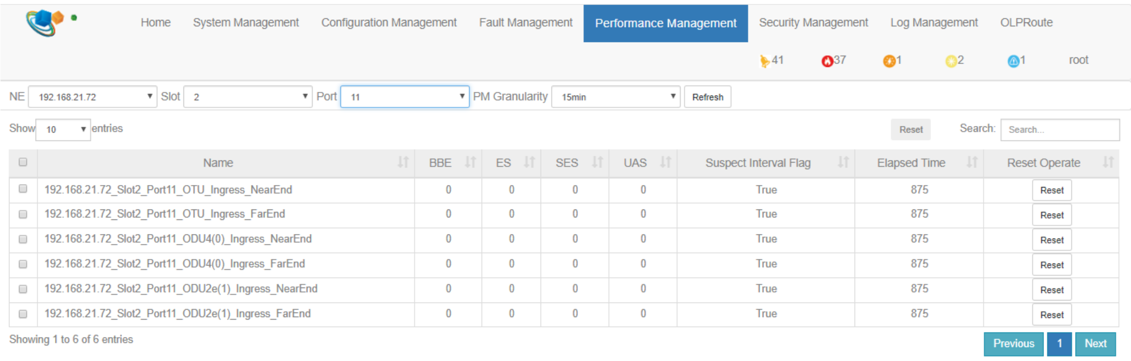
Show 10 entries

Search: Search...

| ☐ | Name | MaxDGD | MaxDGD Stamp | MinDGD | MinDGD Stamp | AvgDGD | MaxCD | MaxCD Stamp | MinCD | MinCD Stamp | AvgCD |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 192.168.21.72_Slot2_Port11_OCh_Ingress_NearEnd | 4 | 2018/10/09 07:00:01 | 2 | 2018/10/09 07:00:24 | 3 | 51 | 2018/10/09 07:08:39 | -54 | 2018/10/09 07:04:22 | 0 |

Showing 1 to 1 of 1 entries

Figure 0-6 FEC Current Performance Statistics



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

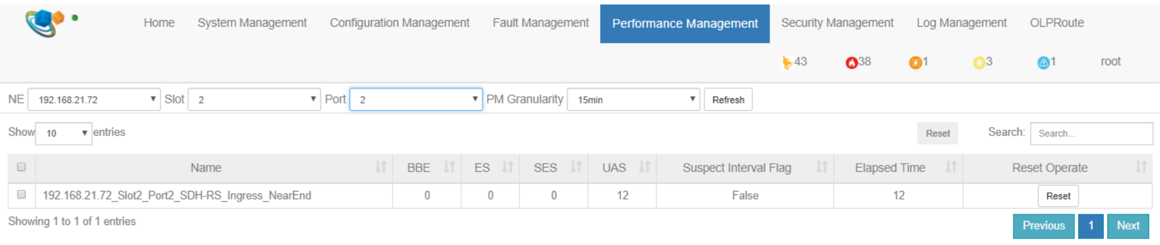
Show 10 entries

Search: Search...

| ☐ | Name | BBE | ES | SES | UAS | Suspect Interval Flag | Elapsed Time | Reset Operate |
|---|---|---|---|---|---|---|---|---|
| ☐ | 192.168.21.72_Slot2_Port11_OTU_Ingress_NearEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_OTU_Ingress_FarEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_ODU4(0)_Ingress_NearEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_ODU4(0)_Ingress_FarEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_ODU2e(1)_Ingress_NearEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |
| ☐ | 192.168.21.72_Slot2_Port11_ODU2e(1)_Ingress_FarEnd | 0 | 0 | 0 | 0 | True | 875 | Reset |

Showing 1 to 6 of 6 entries

Figure 0-7 OTUk/ODUk Current Performance Statistics



NE 192.168.21.72 Slot 2 Port 2 PM Granularity 15min

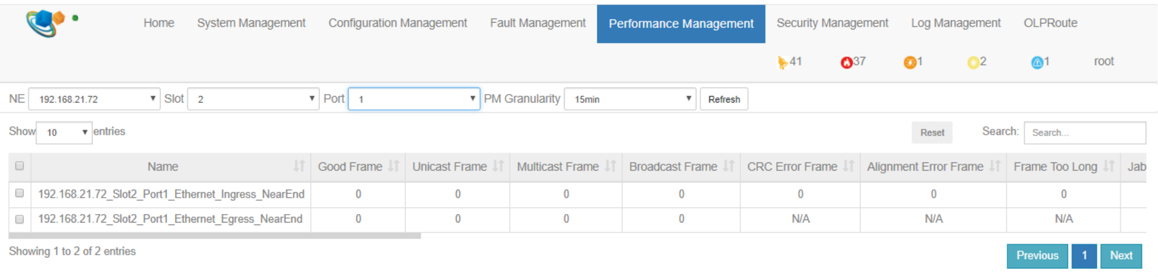
Show 10 entries

Search: Search...

| ☐ | Name | BBE | ES | SES | UAS | Suspect Interval Flag | Elapsed Time | Reset Operate |
|---|---|---|---|---|---|---|---|---|
| ☐ | 192.168.21.72_Slot2_Port2_SDH-RS_Ingress_NearEnd | 0 | 0 | 0 | 12 | False | 12 | Reset |

Showing 1 to 1 of 1 entries

Figure 0-8 Current Performance Statistics of SDH Regenerated Segment



NE 192.168.21.72 Slot 2 Port 1 PM Granularity 15min

Show 10 entries Search: Search...

| □ | Name | Good Frame | Unicast Frame | Multicast Frame | Broadcast Frame | CRC Error Frame | Alignment Error Frame | Frame Too Long | Jab |
|---|---|---|---|---|---|---|---|---|---|
| □ | 192.168.21.72_Slot2_Port1_Ethernet_Ingress_NearEnd | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| □ | 192.168.21.72_Slot2_Port1_Ethernet_Egress_NearEnd | 0 | 0 | 0 | 0 | N/A | N/A | N/A | |

Showing 1 to 2 of 2 entries

Figure 0-3 Ethernet Current Performance Statistics

## 6.4. History Performance Statistics

### Prerequisite

1. The PMP has been opened.

2. FTP server has been configured.

### Related Information

Obtain history performance statistics information. The current performance statistics will become history performance statistics 15 minutes later.

### Steps

Click*"Performance Management"* → *"History Performance Statistics"* on the navigation bar to enter the history performance statistics interface.

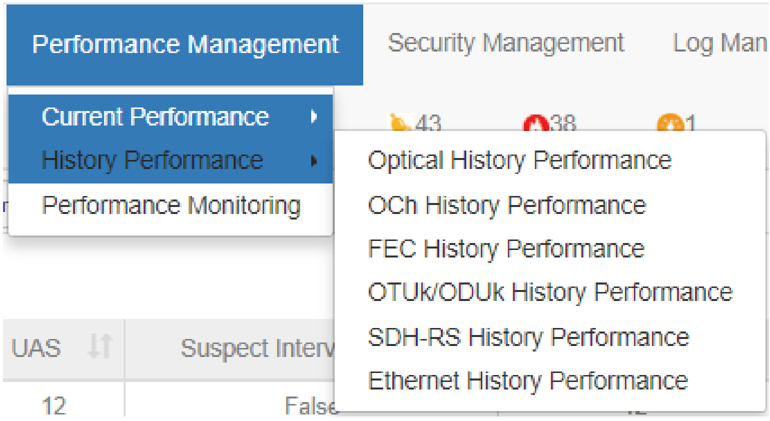
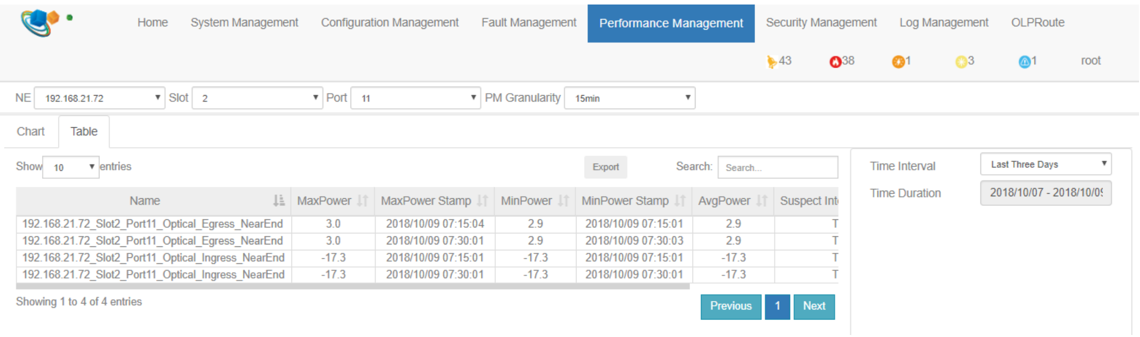


Figure 0-4 History Performance Statistics

The history performance statistics is shown in form and chart.



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

Show 10 entries

Search: Search...

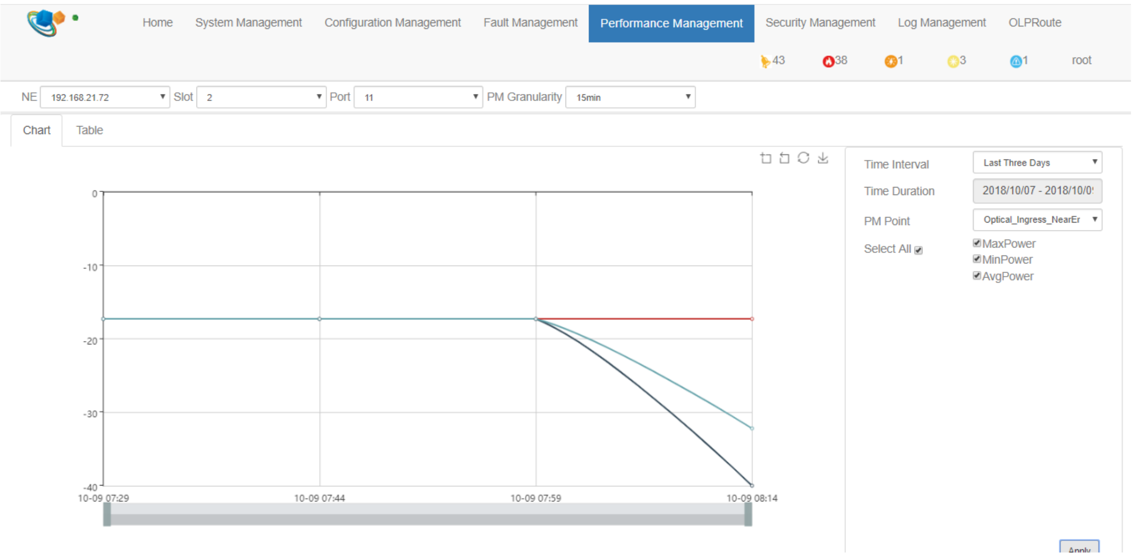
Time Interval Last Three Days

Time Duration 2018/10/07 - 2018/10/0

| Name | MaxPower | MaxPower Stamp | MinPower | MinPower Stamp | AvgPower | Suspect Int |
|---|---|---|---|---|---|---|
| 192.168.21.72_Slot2_Port11_Optical_Egress_NearEnd | 3.0 | 2018/10/09 07:15:04 | 2.9 | 2018/10/09 07:15:01 | 2.9 | T |
| 192.168.21.72_Slot2_Port11_Optical_Egress_NearEnd | 3.0 | 2018/10/09 07:30:01 | 2.9 | 2018/10/09 07:30:03 | 2.9 | T |
| 192.168.21.72_Slot2_Port11_Optical_Ingress_NearEnd | -17.3 | 2018/10/09 07:15:01 | -17.3 | 2018/10/09 07:15:01 | -17.3 | T |
| 192.168.21.72_Slot2_Port11_Optical_Ingress_NearEnd | -17.3 | 2018/10/09 07:30:01 | -17.3 | 2018/10/09 07:30:01 | -17.3 | T |

Showing 1 to 4 of 4 entries

Figure 0-11 History Performance Statistics of Optical Power-Form



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

Time Interval Last Three Days

Time Duration 2018/10/07 - 2018/10/0

PM Point Optical_Ingress_NearEr

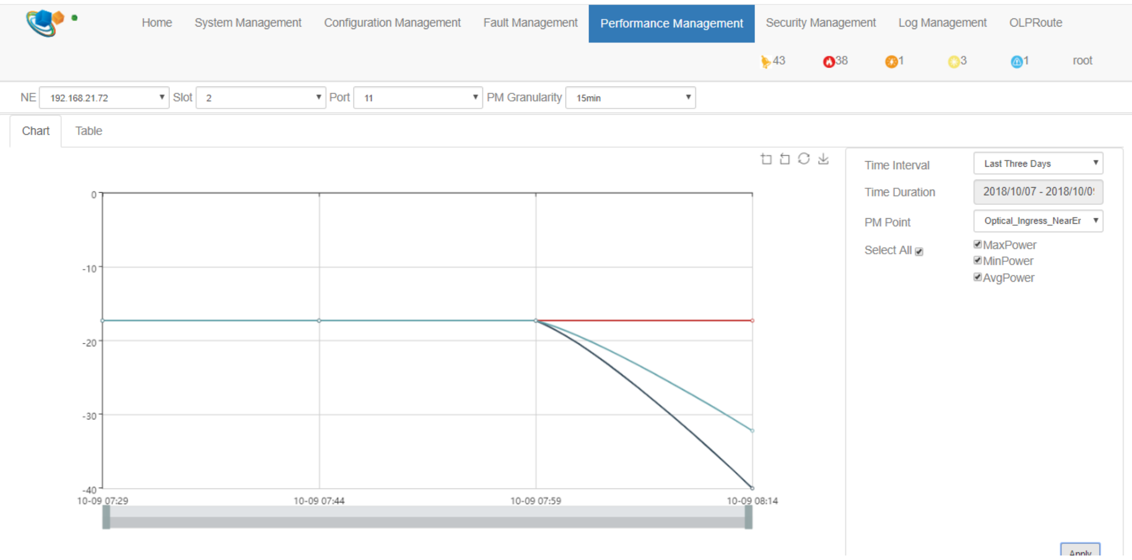
Select All ☑

☑MaxPower

☑MinPower

☑AvgPower

Figure 0-5 History Performance Statistics of Optical Power-Chart



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

Time Interval Last Three Days

Time Duration 2018/10/07 - 2018/10/0

PM Point Optical_Ingress_NearEr

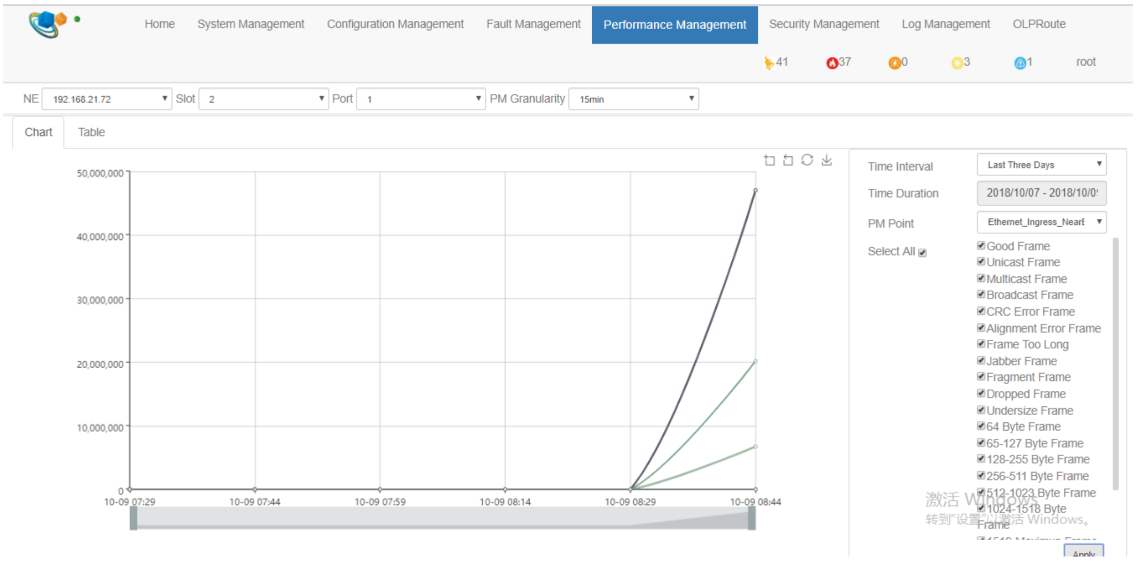
Select All ☑

☑MaxPower

☑MinPower

☑AvgPower

Figure 0-13 Ethernet History Performance Statistics -Form



NE 192.168.21.72 Slot 2 Port 1 PM Granularity 15min

Time Interval: Last Three Days

Time Duration: 2018/10/07 - 2018/10/0

PM Point: Ethernet_Ingress_NearE

Select All ☑

☑Good Frame
☑Unicast Frame
☑Multicast Frame
☑Broadcast Frame
☑CRC Error Frame
☑Alignment Error Frame
☑Frame Too Long
☑Jabber Frame
☑Fragment Frame
☑Dropped Frame
☑Undersize Frame
☑64 Byte Frame
☑65-127 Byte Frame
☑128-255 Byte Frame
☑256-511 Byte Frame
☑512-1023 Byte Frame
☑1024-1518 Byte Frame

Figure 0-6 Ethernet History Performance Statistics -Chart

## 6.5.Performance Statistics Maintenance

### 6.5.1.Export Statistics Data

#### Prerequisite

1. The PMP has been opened.

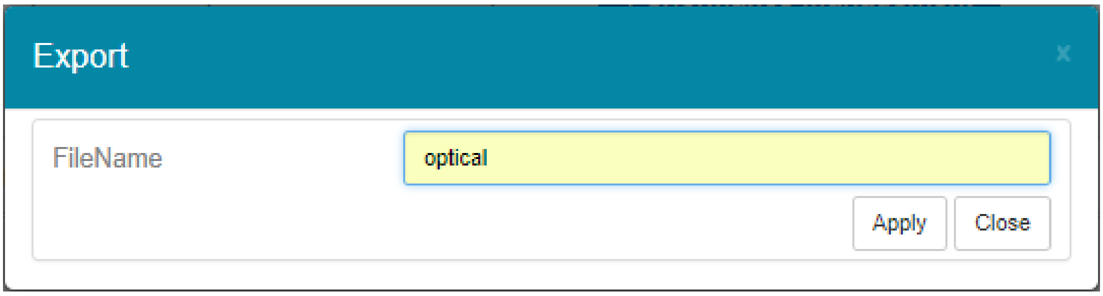
2. FTP server has been configured.

#### Related Information

Export history performance statistics data.

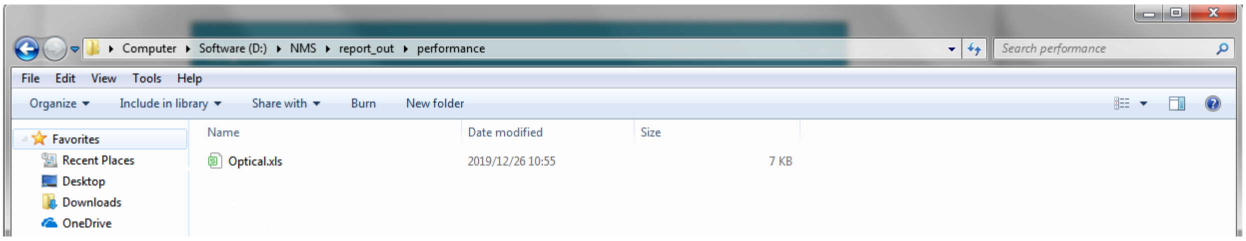
#### Steps

Click*"Performance Management"*→ *"History Performance Statistics"* on the navigation bar to enter history performance statistics interface. The history performance statistics data is exported in forms and pictures. Select*"Form"* and click *"Export"* to export history performance statistics data. The exported file can be viewed in the installation directory of report_out.



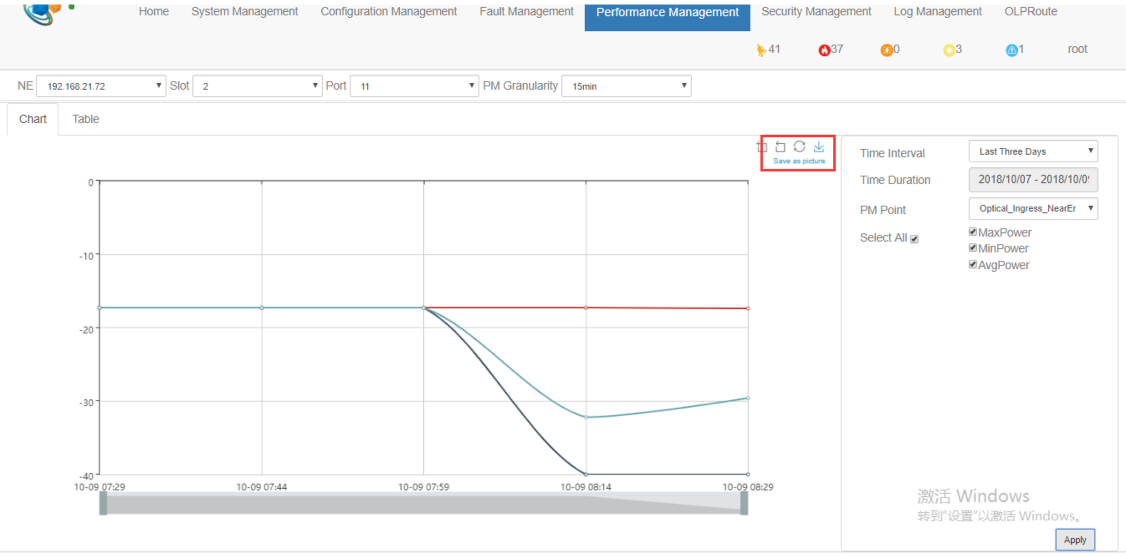
FileName: optical

Figure 0-7 Export History Performance Statistics Data-Form


Computer ▸ Software (D:) ▸ NMS ▸ report_out ▸ performance
Search performance
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ Burn New folder
Favorites
Recent Places
Desktop
Downloads
OneDrive

| Name | Date modified | Size |
|---|---|---|
| Optical.xls | 2019/12/26 10:55 | 7 KB |

Figure 0-8 Exported History Performance Data-Form



NE 192.168.21.72 Slot 2 Port 11 PM Granularity 15min

Time Interval: Last Three Days

Time Duration: 2018/10/07 - 2018/10/0'

PM Point: Optical_Ingress_NearEr

Select All ☑

☑MaxPower
☑MinPower
☑AvgPower

Figure 0-9 Export History Performance Statistics Data-Picture

The exported pictures will be automatically saved in download folder.

# Chapter 7 Log Management

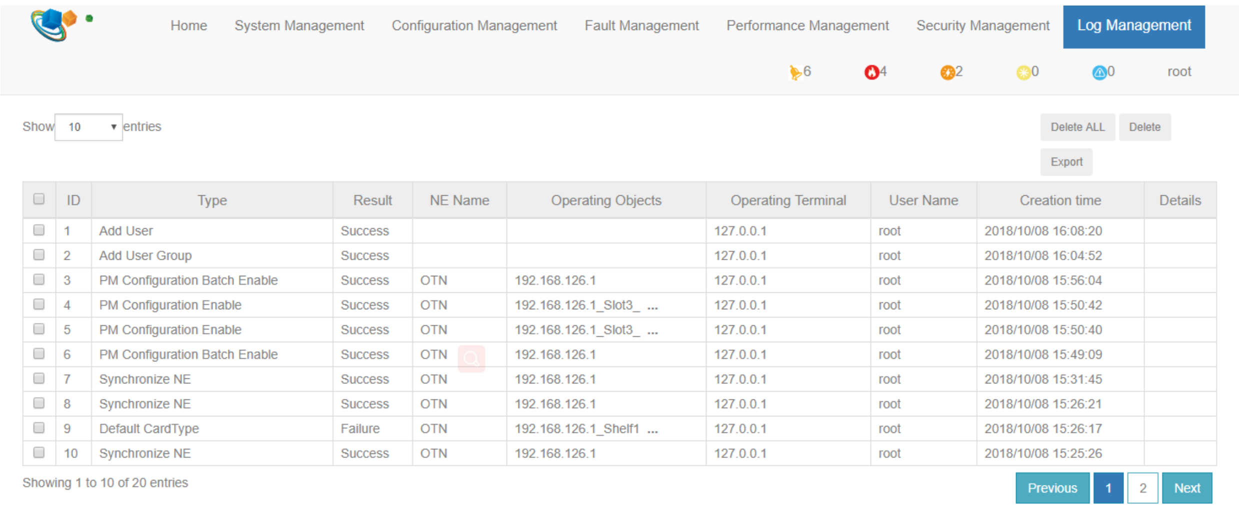
## 7.1. Log Management Introduction

There are three types of logs:

- The operation log records the user's operation information, including log ID, operation level, user name, operation name, host address, command function, detailed information, operation result, failure reason, access mode, operation object, operation start time, operation end time and associated log information.
- The security log records the user's login status, including log ID, user name, host address, log name, operation time, access mode and detailed information.
- The system log records the completion of the timed task of the server, including log ID, level, source, log name, detailed information, host address, operation start time, operation end time and associated log information.

## 7.2 . Log Query

Click "Log Management" in the home page to enter the interface, as shown in the figure below:



| □ | ID | Type | Result | NE Name | Operating Objects | Operating Terminal | User Name | Creation time | Details |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Add User | Success | | | 127.0.0.1 | root | 2018/10/08 16:08:20 | |
| □ | 2 | Add User Group | Success | | | 127.0.0.1 | root | 2018/10/08 16:04:52 | |
| □ | 3 | PM Configuration Batch Enable | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:56:04 | |
| □ | 4 | PM Configuration Enable | Success | OTN | 192.168.126.1_Slot3_ ... | 127.0.0.1 | root | 2018/10/08 15:50:42 | |
| □ | 5 | PM Configuration Enable | Success | OTN | 192.168.126.1_Slot3_ ... | 127.0.0.1 | root | 2018/10/08 15:50:40 | |
| □ | 6 | PM Configuration Batch Enable | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:49:09 | |
| □ | 7 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:31:45 | |
| □ | 8 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:26:21 | |
| □ | 9 | Default CardType | Failure | OTN | 192.168.126.1_Shelf1 ... | 127.0.0.1 | root | 2018/10/08 15:26:17 | |
| □ | 10 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:25:26 | |

Showing 1 to 10 of 20 entries

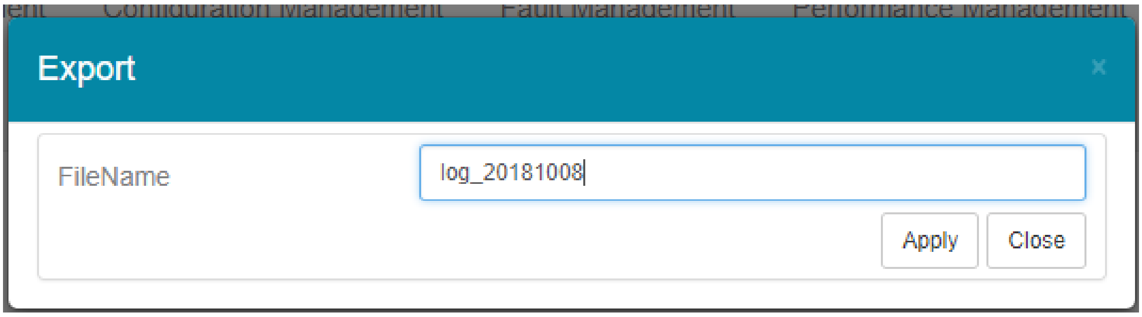
Figure 0-1 Log Management

A piece of log information will generate every time when the user add, modify and delete the data. That is to say, except for query operation, every operation the user performed will lead in the generation of log information.

## 7.3. Log Maintenance

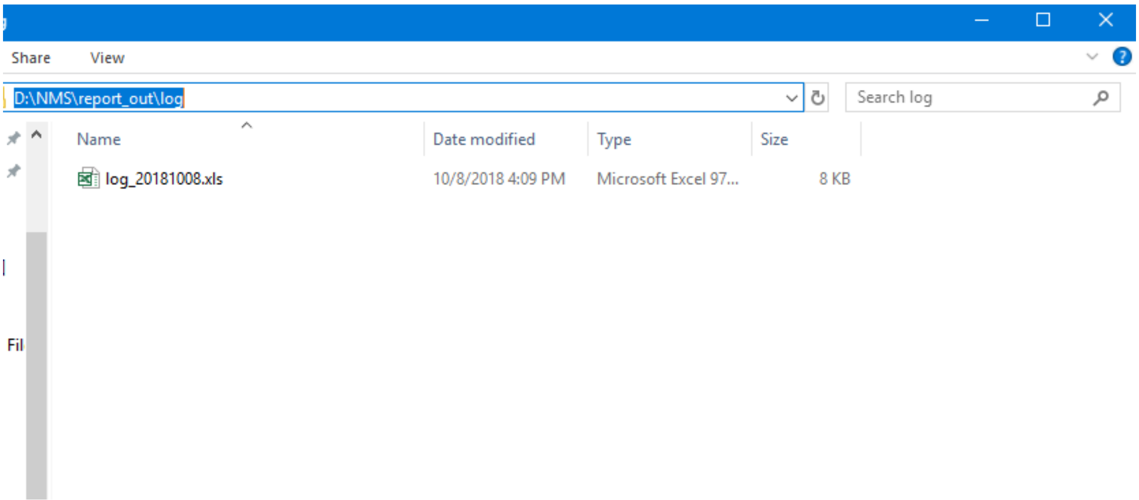
### 7.3.1. Export Log

Select the check box in the upper left corner, and click "Export" button, the selected logs can be exported. The exported logs will be saved to the report_out folder in the installation root directory, as shown in the figure below:



FileName: log_20181008

Figure 0-2 Export Log



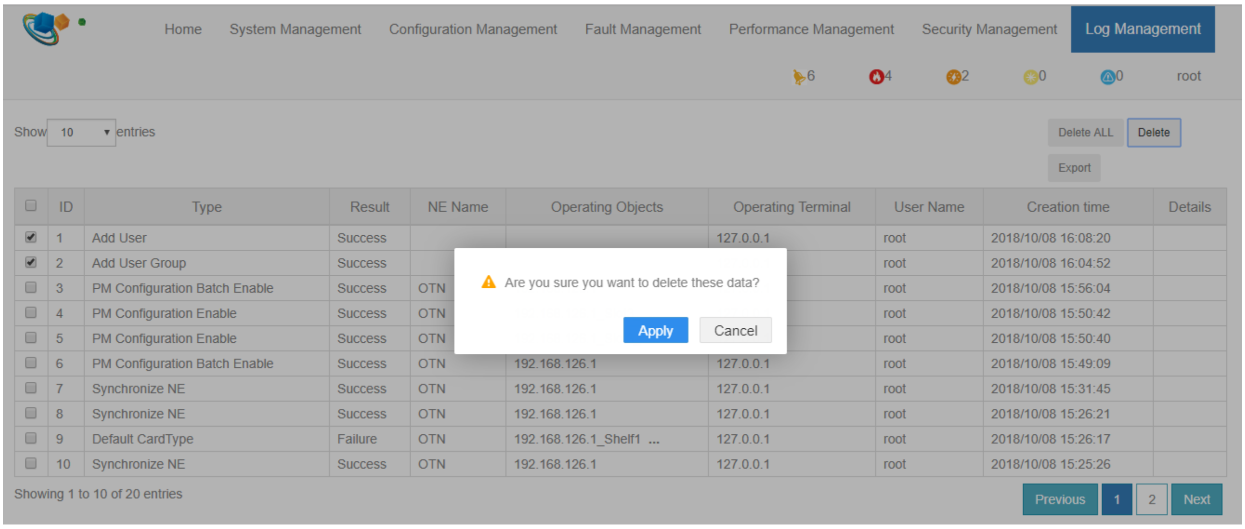
D:\NMS\report_out\log

| Name | Date modified | Type | Size |
|---|---|---|---|
| log_20181008.xls | 10/8/2018 4:09 PM | Microsoft Excel 97... | 8 KB |

Figure 0-3 Exported Logs

### 7.3.2. Delete Log

Select the data which needs to be deleted in the table (The deletion of log will also generate a piece of log information.), and click “Delete” button, a prompt message will appear to ask whether you are sure to delete the data, as shown in the figure below:



Are you sure you want to delete these data?

| □ | ID | Type | Result | NE Name | Operating Objects | Operating Terminal | User Name | Creation time | Details |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | Add User | Success | | | 127.0.0.1 | root | 2018/10/08 16:08:20 | |
| ☑ | 2 | Add User Group | Success | | | | root | 2018/10/08 16:04:52 | |
| □ | 3 | PM Configuration Batch Enable | Success | OTN | | | root | 2018/10/08 15:56:04 | |
| □ | 4 | PM Configuration Enable | Success | OTN | | | root | 2018/10/08 15:50:42 | |
| □ | 5 | PM Configuration Enable | Success | OTN | | | root | 2018/10/08 15:50:40 | |
| □ | 6 | PM Configuration Batch Enable | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:49:09 | |
| □ | 7 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:31:45 | |
| □ | 8 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:26:21 | |
| □ | 9 | Default CardType | Failure | OTN | 192.168.126.1_Shelf1 ... | 127.0.0.1 | root | 2018/10/08 15:26:17 | |
| □ | 10 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:25:26 | |

Showing 1 to 10 of 20 entries

Figure 0-4 Log Management-Delete Log

# Chapter 8 Security Management

## 8.1. Security Management Introduction

Security management is mainly used to ensure the user's legitimate use of the system. It is divided into two parts:

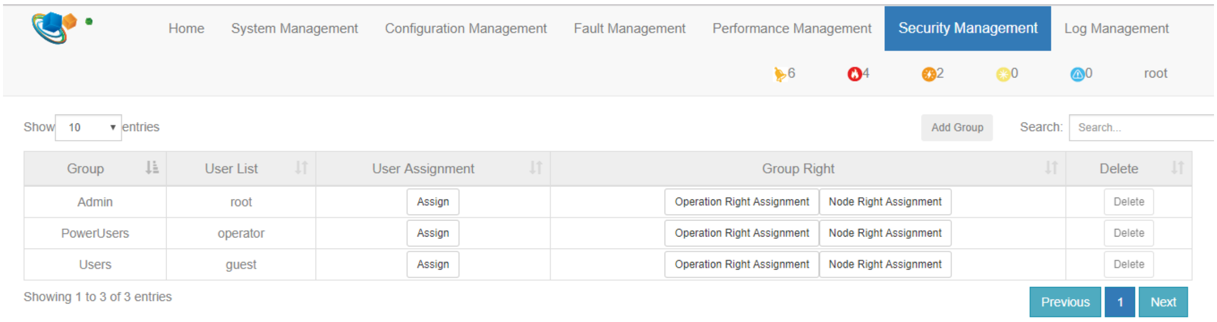
- User group management which can add user group and perform corresponding delete and modify operations.
- User management which can check login user, modify login password and delete login user.

The security management realizes the management of the user and the user group etc. It provides security control for the operator's security management operation. Through the login authentication, the illegal user can be prevented from entering the system, and the security control is provided to the operator's operation through operation authentication method.

## 8.2. User Group Management

### 8.2.1. Add User Group

Click "Security Management → User Group Management in the home page to enter the interface, as shown in the figure below:



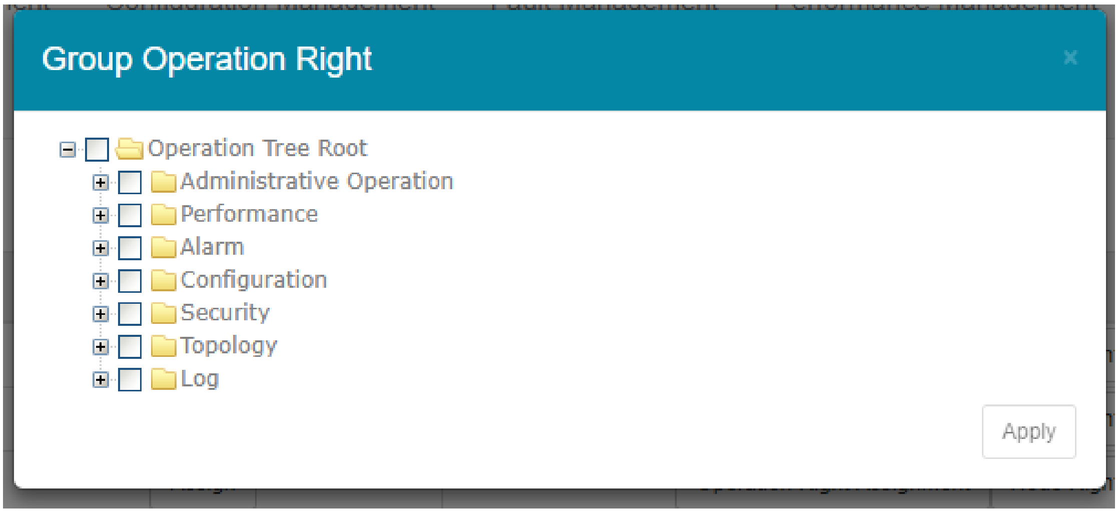
Show 10 entries

| Group | User List | User Assignment | Group Right | Delete |
|---|---|---|---|---|
| Admin | root | Assign | Operation Right Assignment<br>Node Right Assignment | Delete |
| PowerUsers | operator | Assign | Operation Right Assignment<br>Node Right Assignment | Delete |
| Users | guest | Assign | Operation Right Assignment<br>Node Right Assignment | Delete |

Showing 1 to 3 of 3 entries

Figure 0-1 User Group Management

Groups can be added by clicking "Add Group" button, and corresponding permissions can be assigned for the groups, as shown in the figure below:



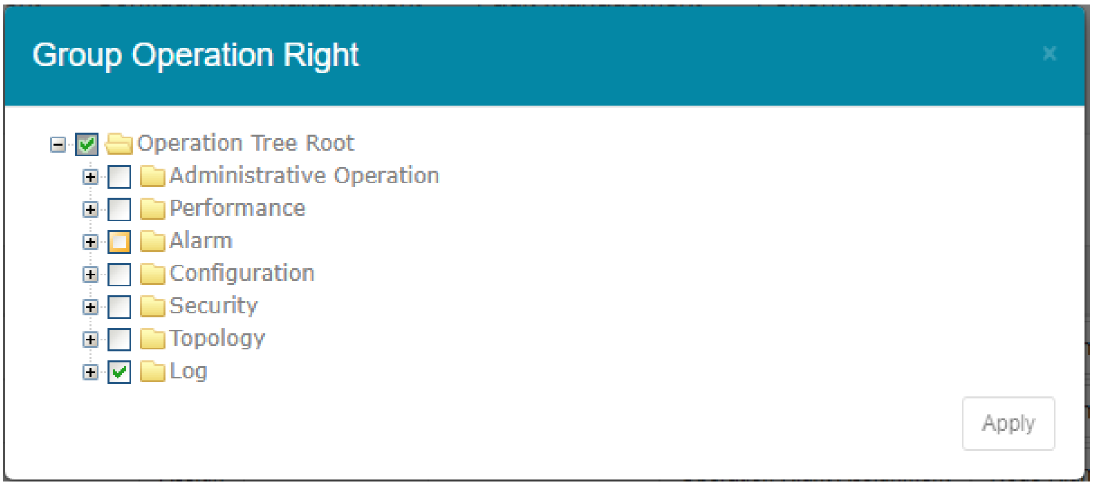
Group Operation Right

- □ Operation Tree Root
  - □ Administrative Operation
  - □ Performance
  - □ Alarm
  - □ Configuration
  - □ Security
  - □ Topology
  - □ Log

Figure 0-2 User Group Management-Add Group

### 8.2.2.Modify User Group

The user group right can be modified by clicking "Modify" button in the table of the user group management page, as shown in the figure below:



Group Operation Right

- ☑ Operation Tree Root
  - □ Administrative Operation
  - □ Performance
  - □ Alarm
  - □ Configuration
  - □ Security
  - □ Topology
  - ☑ Log

Figure 0-3 User Group Management-Modify Group Right

The user can be moved to a group or be removed from a group by clicking "Assign" button in the table of the user group management page. The user permissions will change after the removal, as shown in the figure below:

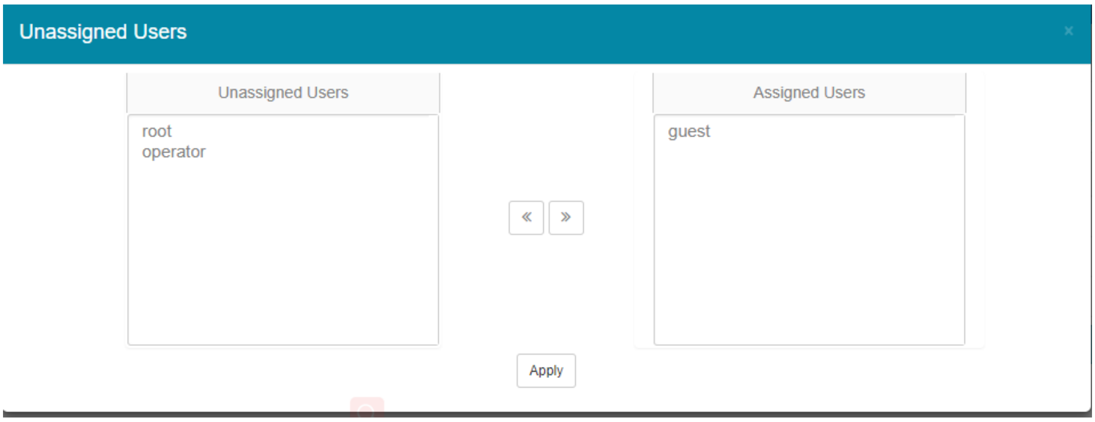
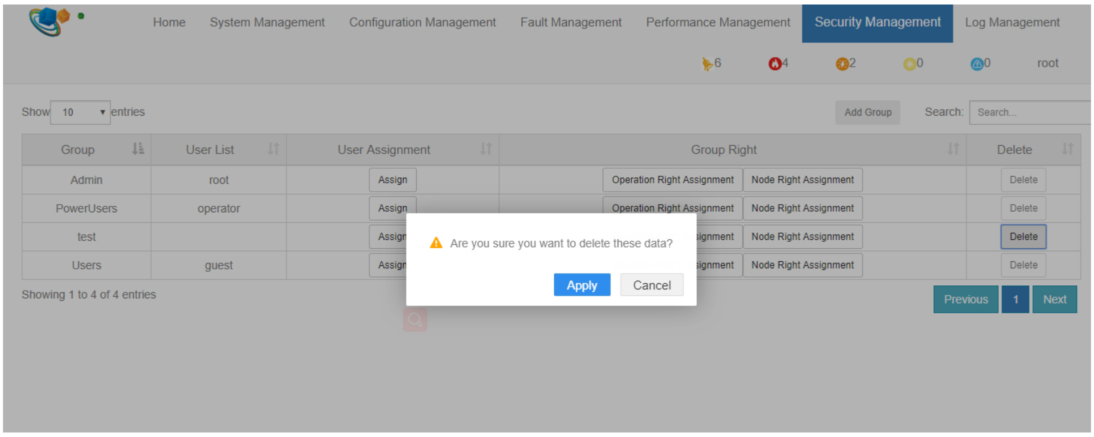


Figure 0-4 User Group Management-Unassigned Users

### 8.2.3.Delete User Group

The corresponding data can be deleted by clicking “Delete” button in the table of the user group management interface. A window will pop up to ask whether you are sure to perform the deletion operation, as shown in the figure below:



| Group | User List | User Assignment | Group Right | | Delete |
|---|---|---|---|---|---|
| Admin | root | Assign | Operation Right Assignment | Node Right Assignment | Delete |
| PowerUsers | operator | Assign | Operation Right Assignment | Node Right Assignment | Delete |
| test | | Assign | ignment | Node Right Assignment | Delete |
| Users | guest | Assign | ignment | Node Right Assignment | Delete |

Showing 1 to 4 of 4 entries

Are you sure you want to delete these data?

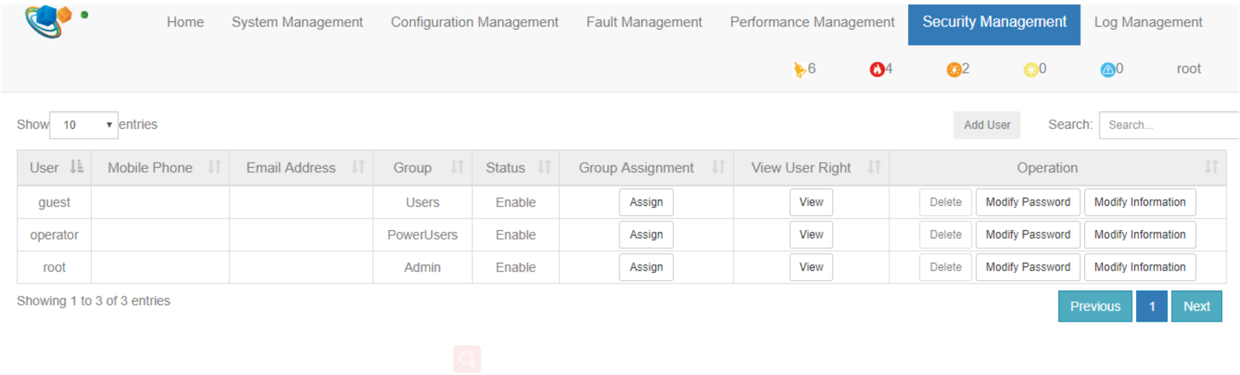
Figure 0-5 User Group Management-Delete Group

Admin, PowerUsers and Users are default groups. They cannot be deleted.

## 8.3.User Management

### 8.3.1.Add User

Click *“Security Management”*→ *”User Management”* in the home page to enter the interface, as shown in the figure below:



| User | Mobile Phone | Email Address | Group | Status | Group Assignment | View User Right | Operation | | |
|---|---|---|---|---|---|---|---|---|---|
| guest | | | Users | Enable | Assign | View | Delete | Modify Password | Modify Information |
| operator | | | PowerUsers | Enable | Assign | View | Delete | Modify Password | Modify Information |
| root | | | Admin | Enable | Assign | View | Delete | Modify Password | Modify Information |

Showing 1 to 3 of 3 entries

Figure 0-6 User Management

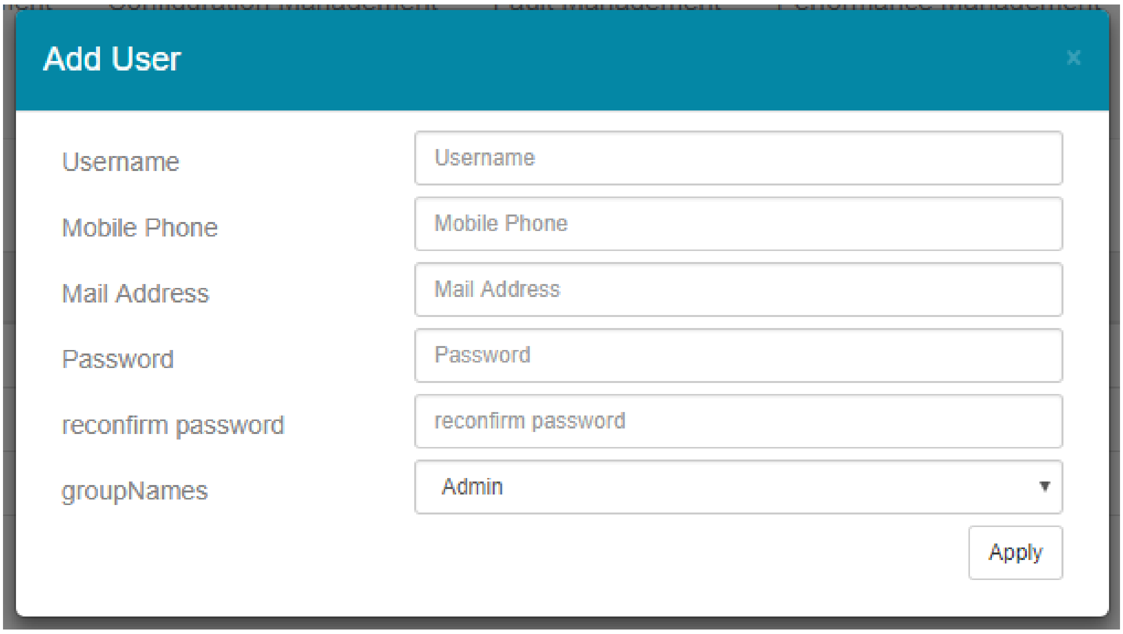
Tips:

(1) Root user has all the operation permissions.

(2) Operator does not have the permission for security management.

(3) Guest only has the permission for performance.

The user can add new user by clicking *"Add User"* button, as shown in the figure below:



Add User

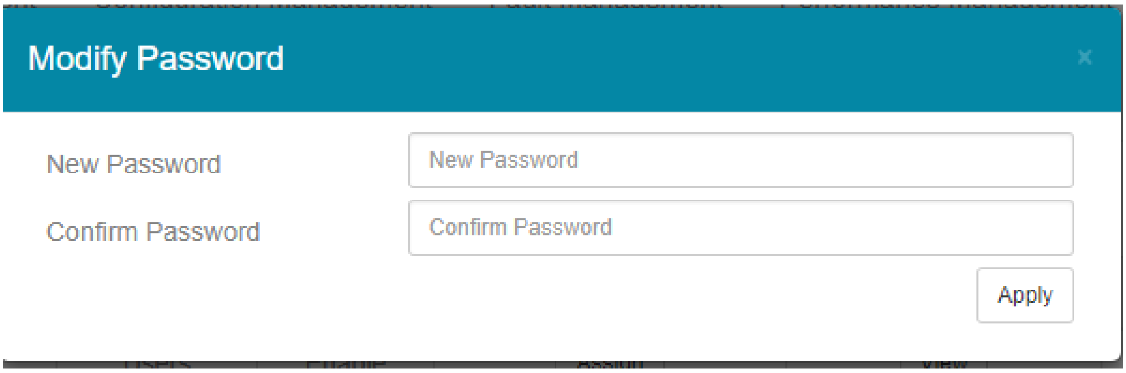
| | |
|---|---|
| Username | Username |
| Mobile Phone | Mobile Phone |
| Mail Address | Mail Address |
| Password | Password |
| reconfirm password | reconfirm password |
| groupNames | Admin |

Figure 0-7 User Management-Add User

### 8.3.2.Modify User

The password can be modified by clicking *"Modify"* button in the table of the user management interface, as shown in the figure below:

(User password is not needed if the administrator modifies the password)

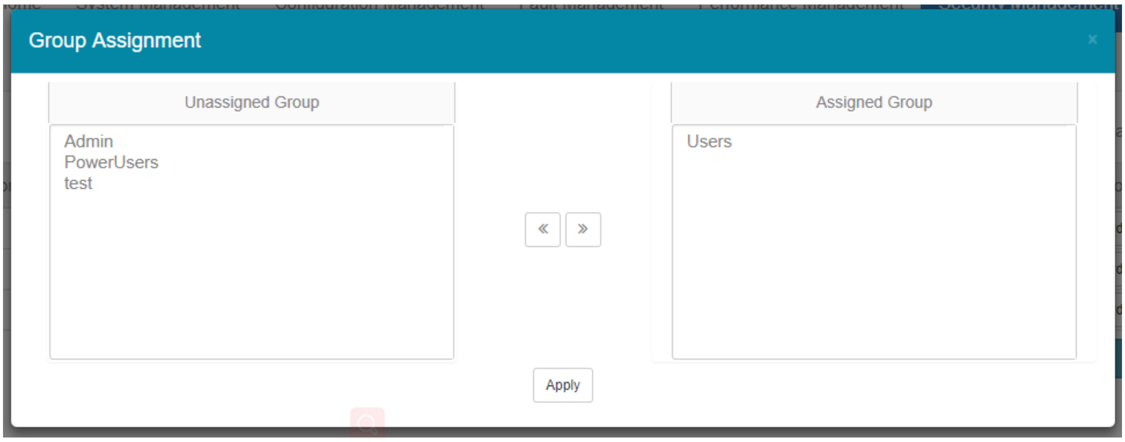


Modify Password

| | |
|---|---|
| New Password | New Password |
| Confirm Password | Confirm Password |

Figure 0-8 User Management-Modify Password

If you want to move the user to a certain group or remove the user from a group, you can click *"Assign"* button in the table of the user management interface. The user has the permissions of the group that he belongs to and can perform the corresponding operations, as shown in the figure below:

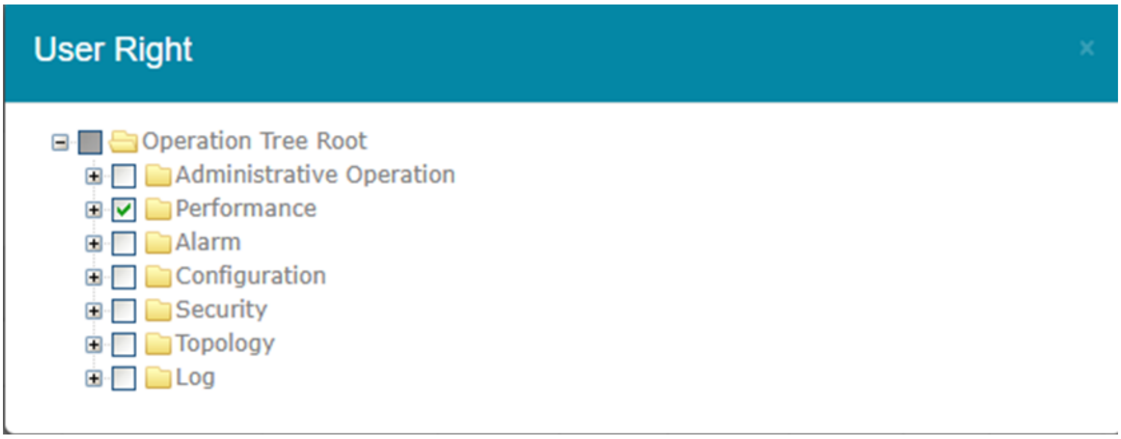


Group Assignment

| Unassigned Group | Assigned Group |
|---|---|
| Admin<br>PowerUsers<br>test | Users |

Figure 0-9 User Management-Group Assignment

The user right can be viewed by clicking *"View"* button in the table of the user management interface. The user should have the rights to perform corresponding operations, as shown in the figure below:



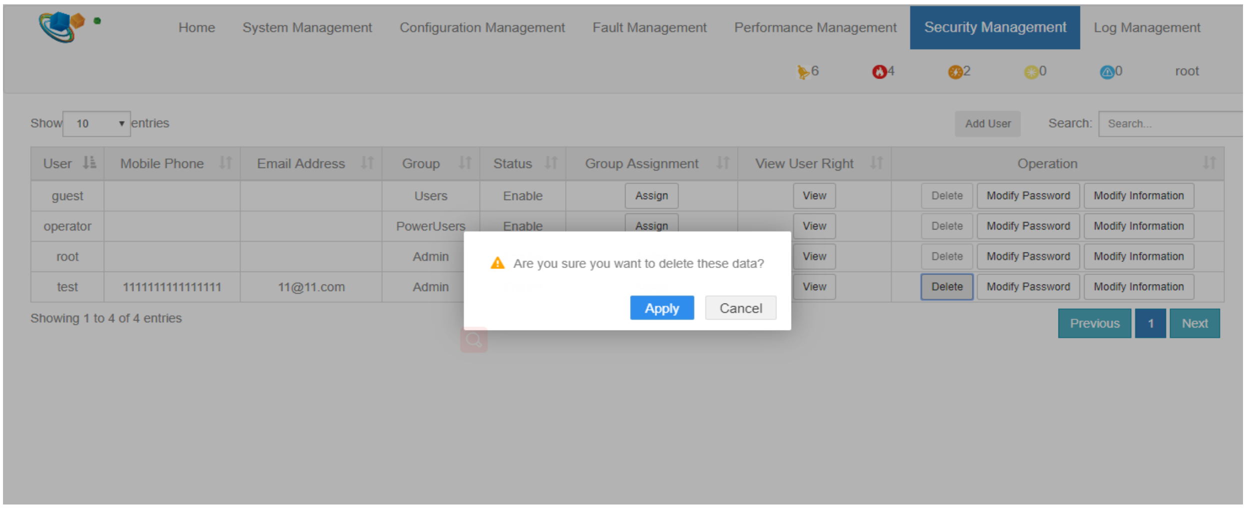
User Right

- □ Operation Tree Root
  - □ Administrative Operation
  - ☑ Performance
  - □ Alarm
  - □ Configuration
  - □ Security
  - □ Topology
  - □ Log

Figure 0-10 User Management-User Right

### 8.3.3.Delete User

The corresponding data can be deleted by clicking *"Delete"* button in the table of the user management interface. A window will pop up to ask whether you are sure to delete the data, as shown in the figure below:



| User | Mobile Phone | Email Address | Group | Status | Group Assignment | View User Right | Operation | | |
|---|---|---|---|---|---|---|---|---|---|
| guest | | | Users | Enable | Assign | View | Delete | Modify Password | Modify Information |
| operator | | | PowerUsers | Enable | Assign | View | Delete | Modify Password | Modify Information |
| root | | | Admin | | | View | Delete | Modify Password | Modify Information |
| test | 1111111111111111 | 11@11.com | Admin | | | View | Delete | Modify Password | Modify Information |

Showing 1 to 4 of 4 entries

Are you sure you want to delete these data?

Figure 0-11 User Management-Delete User

# Chapter 9 Routine Maintenance

## 9.1. Maintenance Requirements

### 9.1.1.Duties of Maintenance Personnel

■Do daily and periodical maintenance according to the requirements of maintenance regulations and make corresponding records.

■When there is a sudden accident, please follow the requirements of the maintenance regulations and report it to the competent department or the supervisor immediately. If necessary, please request the other departments immediately to configure to eliminate the faults in the shortest time. Meanwhile, record the major failure process and related data and archive them regularly.

■Do not change the NMS configuration data at will. Do not change the machine disk or software at will. Whenever operations such as change of disk and software or change of configuration data are performed, please make a record for maintenance and use in the future.

### 9.1.2.Requirements for the Maintenance Personnel

In addition to doing the routine maintenance work carefully, finding out the hidden troubles in time and eliminating the hidden troubles and faults, the maintenance personnel should also analyze, quickly locate and solve the problems that have occurred. Therefore, there are high requirements for the maintenance personnel's professional skills, operation standards and psychological qualities.

■Familiar with NMS operations

■Familiar with the networking of the system

■Familiar with all kinds of alarms and performances of SDH system and correctly understand the meaning

■Usually, the NMS system can send alarm before the user. If the user's complaints precedes the NMS system, it should be timely reflected to relevant units or departments after fault handling, so as to improve network management function and improve network monitoring capability.

■The processing principle: When each station receives the alarm or other abnormal situation, the station should contact and confirm it with the Bureau. The fault point should be judged and located by using the NMS system or the monitoring terminal, and the failures should be dealt with timely.

⚠**It is strictly prohibited to displace the disk at will, operate at will and break the fiber at will. Do not do other operations that have nothing to do with the troubleshooting!**

■When major circuit interruption occurs, departments at all levels should immediately organize rush repairs.

## 9.2.Routine Maintenance Items

Routine maintenance is the maintenance items that must be carried out every day. Through routine maintenance, we can grasp the operation of the NMS system in time, find problems and solve problems in time, so as to maintain and remove hidden dangers in time. As a result, we can make the NMS system run reliably. In daily routine maintenance, we need to record the problems and failures in detail, and provide reliable basis for analyzing the problems.

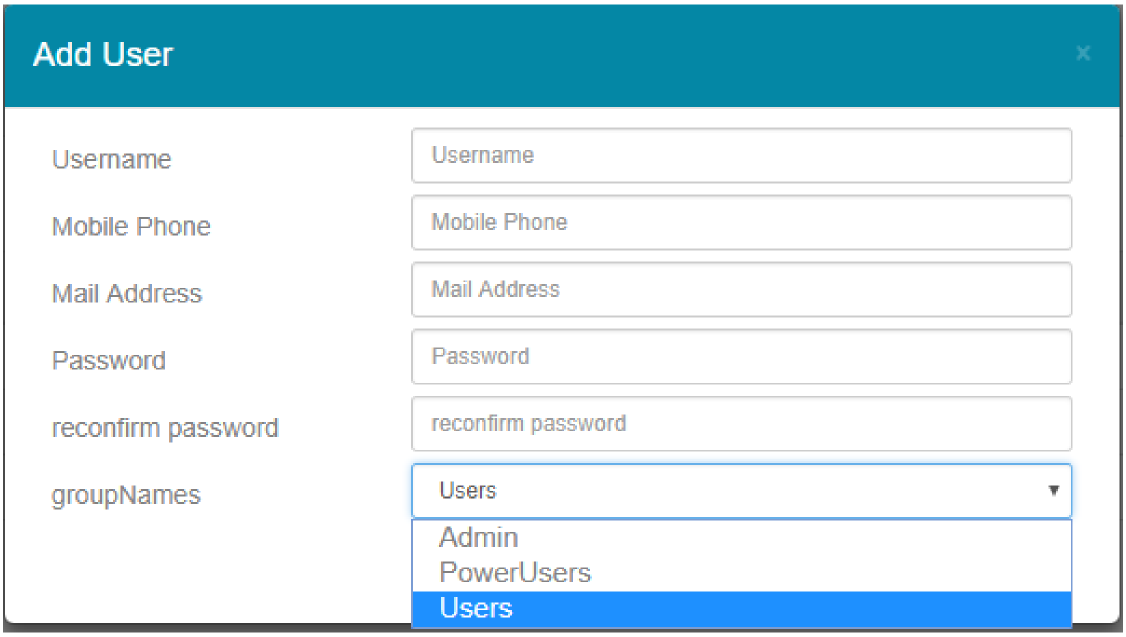
Table 0-1 Daily Routine Maintenance Items

| Maintenance Items | Requirements |
|---|---|
| Login the NMS System with Low Level User Identity | It should be able to log in normally. The operation permissions are not changed. |
| Ping NE | Ensure that there is communication between NE and NMS. |
| Check Board State | Check the state of every board, and ensure that every board is in its position. Check the state of non-single board and ensure that the check state is successful. |
| Check Alarm | Ensure that it can normally obtain or view the current or history alarm of every board. The ineffective alarm should be shielded in time. |
| Check Performance | Ensure that the performance data of every board can be obtained or viewed. |
| Check Information Record | Open “Log Management” window in the NMS Status bar, the log information of the system can be seen. |
| Instant Data Backup | Data backup should be carried out in time before change the configuration, so as to avoid loss of important data caused by misoperation. |

### 9.2.1. Login the NMS System with Low Level User Identity

Because advanced users have all the permissions, if they login the NMS system, once misoperation is performed, it will cause serious consequences. Therefore, unless necessary, it is recommended not to log in as an advanced user. A low level user (Users) should be created to login the NMS system to perform daily operation.

Login the browser, firstly login with the advanced user identity, then select*“Security Management”* → *“User Management”* ,  and then select*“Add User”*button, the dialogue box of “Add User” pops up, as shown in the figure below: enter the user name, the mail address, the user password and the user level (that is group name), and click*“Add”*.


Add User

Username: Username

Mobile Phone: Mobile Phone

Mail Address: Mail Address

Password: Password

reconfirm password: reconfirm password

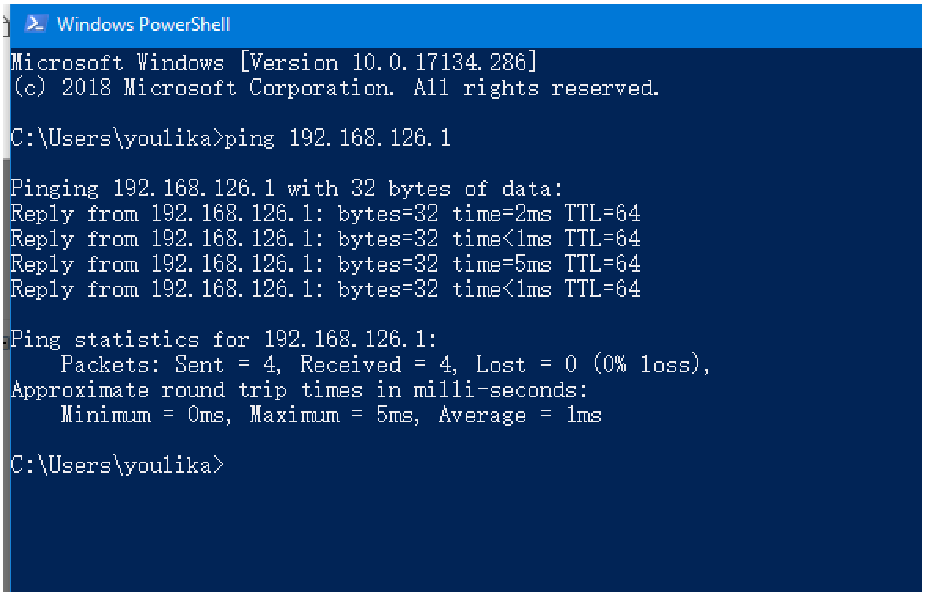
groupNames: Users

Figure 0-1 Add User—Assign Permissions

Then log off the login interface, and log in again with the identity of the newly added user. In daily operation, it is recommended that users log in with this user identity.

### 9.2.2. Ping NE

In NMS server, click*"CMD"*→ *"Command Prompt"*, then you can ping the IP address of NE. If the text below is shown, it indicates that NE is successfully ping, that is, there is communication between NMS and NE. In the same way, Ping the remaining NE to ensure that there is communication between NMS and all devices.

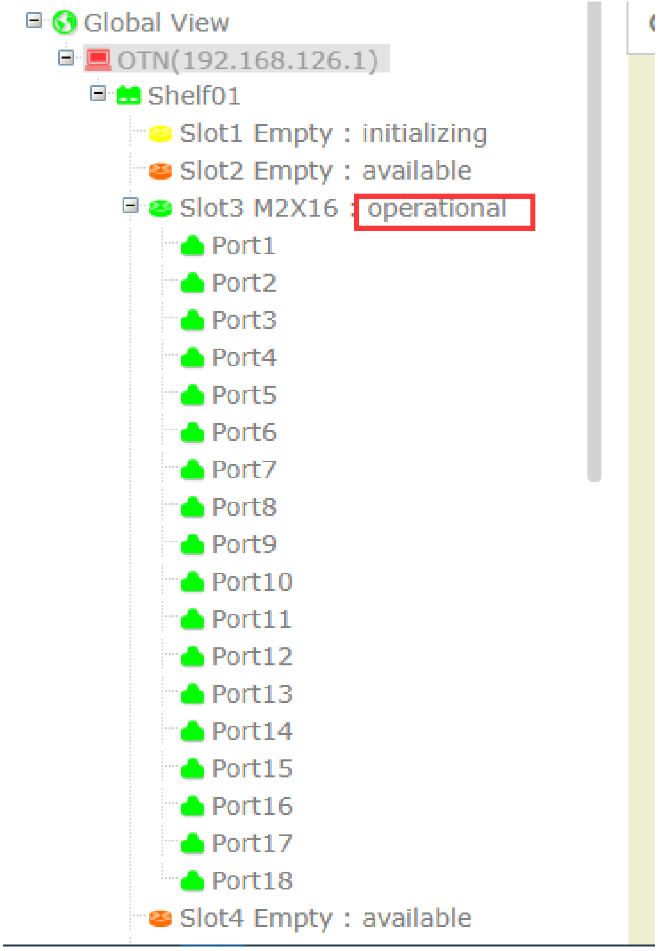


```
Microsoft Windows [Version 10.0.17134.286]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\youlika>ping 192.168.126.1

Pinging 192.168.126.1 with 32 bytes of data:
Reply from 192.168.126.1: bytes=32 time=2ms TTL=64
Reply from 192.168.126.1: bytes=32 time<1ms TTL=64
Reply from 192.168.126.1: bytes=32 time=5ms TTL=64
Reply from 192.168.126.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.126.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\Users\youlika>
```

Figure 0-2 Ping NE

### 9.2.3.Check Board State

The state of every board needs to be checked every day. Alarm that single disk is not in position is not allowed. In the "global view" of the browser, right click NE and select "synchronize NE" to view the board state and ensure that all the online disks are in the position and the state is normal.



Global View
OTN(192.168.126.1)
Shelf01
Slot1 Empty : initializing
Slot2 Empty : available
Slot3 M2X16 : operational
Port1
Port2
Port3
Port4
Port5
Port6
Port7
Port8
Port9
Port10
Port11
Port12
Port13
Port14
Port15
Port16
Port17
Port18
Slot4 Empty : available

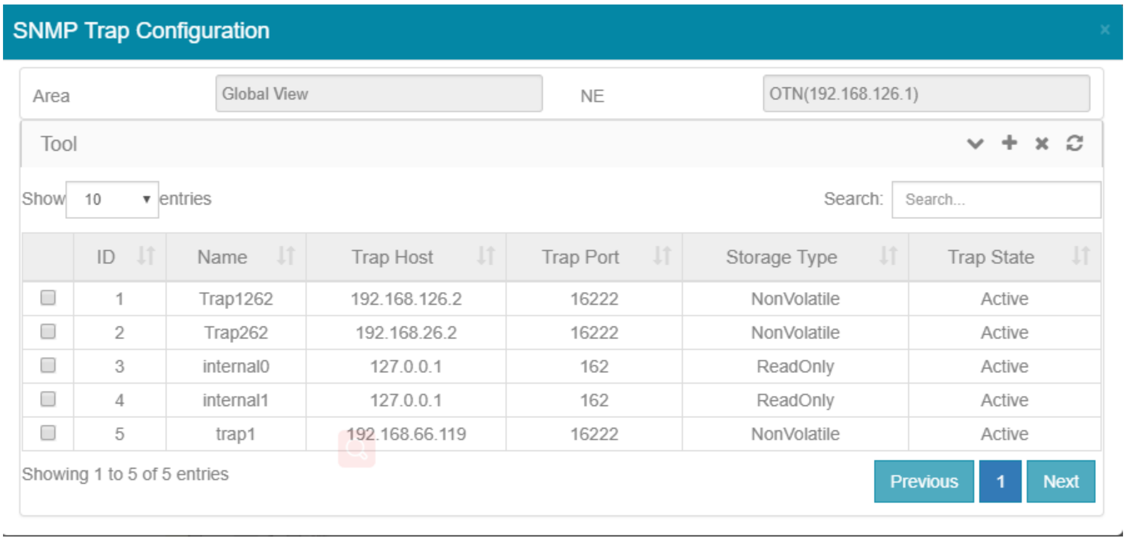
Figure 0-3 NE Single Board State

### 9.2.4.Check Alarm

FMX NMS provides a perfect alarm management function. In the routine maintenance, the network management personnel should check the alarm information of all network elements every day, so as to find out the hidden troubles in time and prevent them in the bud.

### Report Alarms

Select*"System Management"*→ *"SNMP Trap Configuration"* to check whether there is trap address which is in the same network segment with the NMS server. If it is not configured, please add the trap address in time, so as to avoid that the alarm of NE cannot be reported in time. Click "+"button to add trap address. The default trap port number is 16222.



SNNMP Trap Configuration

Area: Global View  NE: OTN(192.168.126.1)

Tool

Show 10 entries  Search: Search...

| | ID | Name | Trap Host | Trap Port | Storage Type | Trap State |
|---|---|---|---|---|---|---|
| □ | 1 | Trap1262 | 192.168.126.2 | 16222 | NonVolatile | Active |
| □ | 2 | Trap262 | 192.168.26.2 | 16222 | NonVolatile | Active |
| □ | 3 | internal0 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 4 | internal1 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 5 | trap1 | 192.168.66.119 | 16222 | NonVolatile | Active |

Showing 1 to 5 of 5 entries

Figure 0-4 Trap Report Alarm

## Set Alarm Sound

The NMS computer is configured with sound card and hi-fi. When alarm occurs, the hi-fi will send out alarm to remind the maintenance personnel to deal with the alarm. This function is very convenient for maintenance.

Select*"Alarm Management"* → *"Enable Sound"*, as shown in the figure below:

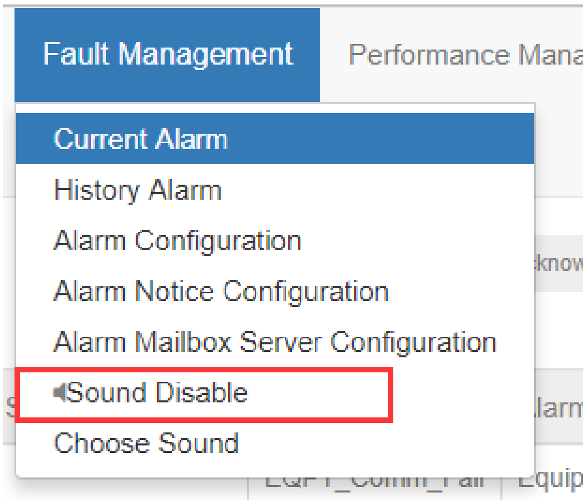


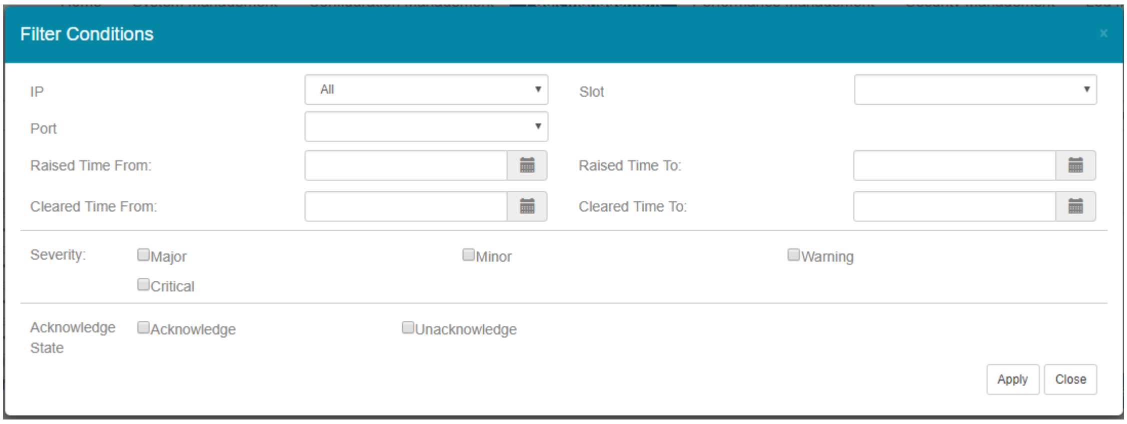
Figure 0-5 Enable Alarm Sound

## Browse Alarm Events

In routine maintenance, the user should read the alarms every day. Once he finds a new alarm, he should record it immediately and make analysis.

Browsing alarm events includes browsing current alarms and browsing history alarms. Current alarms are the unfinished and unconfirmed alarms. History alarms are the finished and confirmed alarms.

In the window to set the filtering rules of current alarms, “alarm level” and “confirmation state” can be selected. Meanwhile, the alarms can be filtered according to the start time and end time.



IP: All

Slot:

Port:

Raised Time From:

Raised Time To:

Cleared Time From:

Cleared Time To:

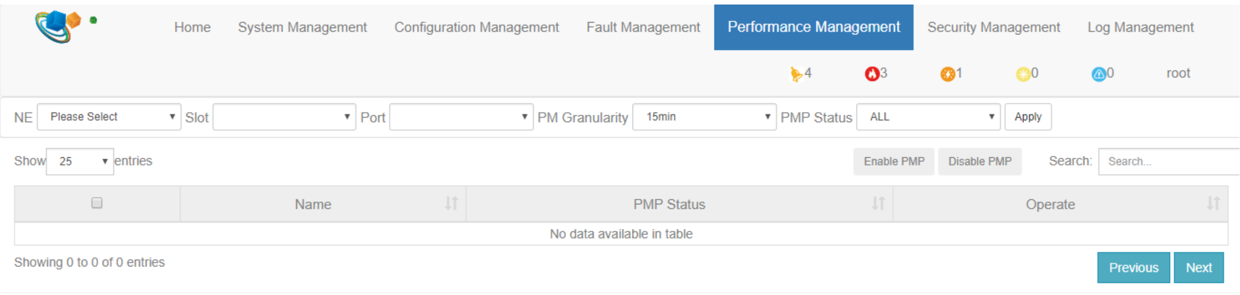
Severity: □Major □Minor □Warning □Critical

Acknowledge State: □Acknowledge □Unacknowledge

Figure 0-6 Filter Current Alarms

## 9.2.5.Check Performance

If you want to check the performance, you need to configure performance statistics first. Then you can check the current performance. In the performance statistics, performance events such as background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds (UAS) are very important. They need to be checked very carefully. When the system is in normal operation, these performance events should be 0 or very few (Performance values such as optical power cannot be 0). If a large number of performance data is found, it indicates that the transmission signal quality of the system has deteriorated and there are potential failures. At this time, you should not take lightly. The hidden dangers must be identified, so as to avoid major accidents such as business interruption.



NE: Please Select Slot: Port: PM Granularity: 15min PMP Status: ALL

Show 25 entries

Search: Search...

| □ | Name | PMP Status | Operate |
|---|---|---|---|
| No data available in table | | | |

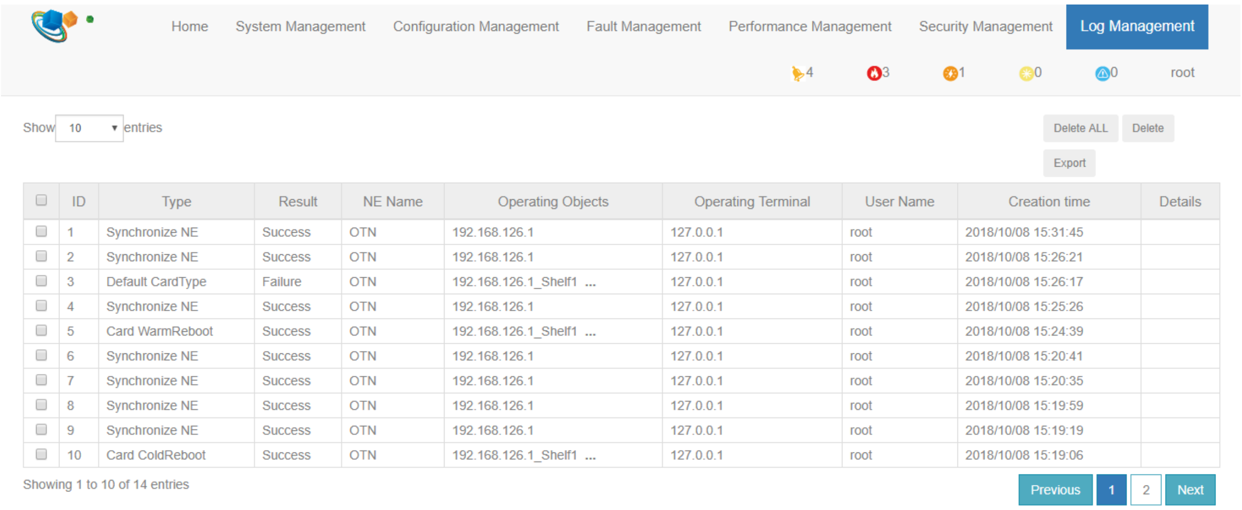
Showing 0 to 0 of 0 entries

Figure 0-7 View Current Performance Statistics

## 9.2.6.Query Message Record

Operations in the NMS system by all the users who login to the NMS system and some cases of the NMS system (e.g. the system startup and exit, the user’s login and logout, illegal login, change of the continuous relationship between NMS and NE etc.) will be recorded by the NMS system. Users need to check them regularly, so as to ensure the safety of the NMS system.

Select*“Log Management”* to check the log state.



| □ | ID | Type | Result | NE Name | Operating Objects | Operating Terminal | User Name | Creation time | Details |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:31:45 | |
| □ | 2 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:26:21 | |
| □ | 3 | Default CardType | Failure | OTN | 192.168.126.1_Shelf1 ... | 127.0.0.1 | root | 2018/10/08 15:26:17 | |
| □ | 4 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:25:26 | |
| □ | 5 | Card WarmReboot | Success | OTN | 192.168.126.1_Shelf1 ... | 127.0.0.1 | root | 2018/10/08 15:24:39 | |
| □ | 6 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:20:41 | |
| □ | 7 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:20:35 | |
| □ | 8 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:19:59 | |
| □ | 9 | Synchronize NE | Success | OTN | 192.168.126.1 | 127.0.0.1 | root | 2018/10/08 15:19:19 | |
| □ | 10 | Card ColdReboot | Success | OTN | 192.168.126.1_Shelf1 ... | 127.0.0.1 | root | 2018/10/08 15:19:06 | |

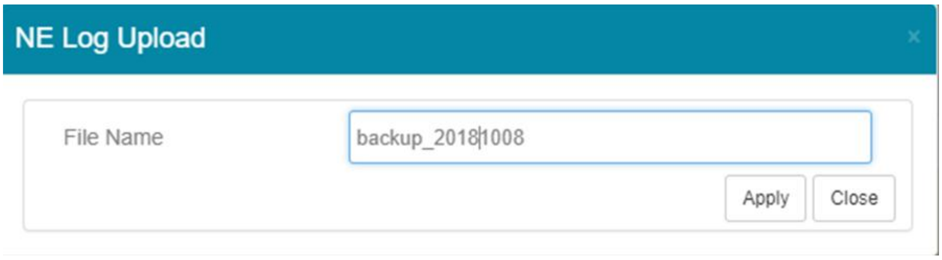
Showing 1 to 10 of 14 entries

Figure 0-8 Log Query

### 9.2.7.Instant Data Backup

In routine maintenance, data backup should be done before modifying the configuration, so as to avoid loss of important data caused by misoperation. If the configuration is not modified, then data backup is not necessary.

Select*"System Management"*→ *"Upload NE Configuration"* to upload all the configurations of NE to the NMS server.



File Name: backup_20181008

Figure 0-9 Upload NE Configuration

## 9.3.Monthly Routine Maintenance

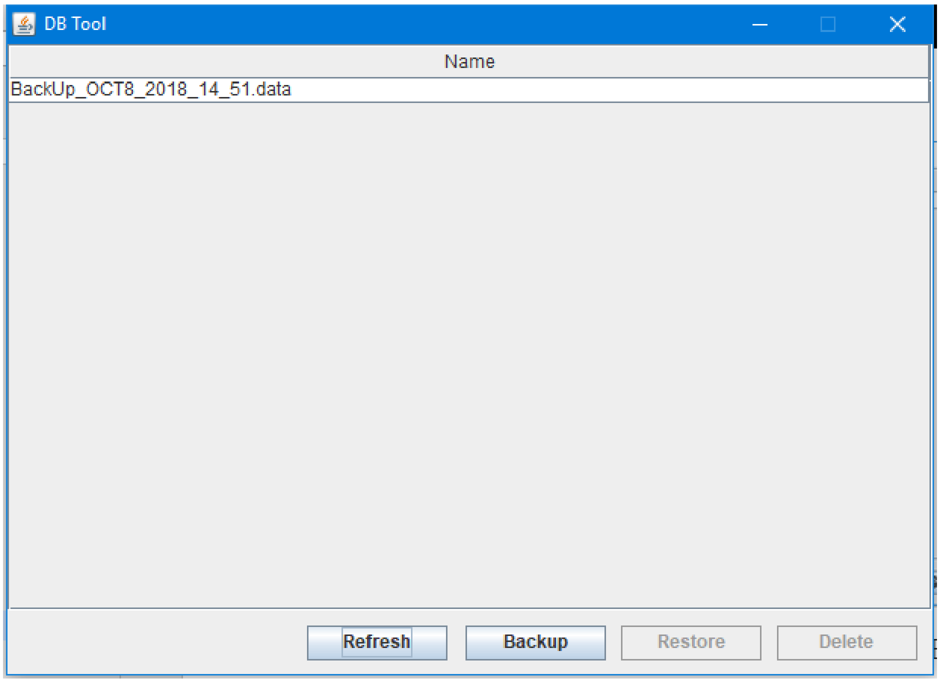
Table 0-2 Items of Monthly Routine Maintenance

| Maintenance Items | Requirements |
|---|---|
| Data Backup | Make data backup to avoid loss of important data caused by misoperation. |
| Performance Acquisition | Check whether the NE performance acquisition is correctly set. |
| Check Hardware Work State | Modem is with factory configuration. It must be special device for special use. It cannot be used for other purpose. It needs to check whether other work state is normal.<br>Check whether the work state of mouse, keyboard, printer and display is normal. |
| History Alarm & Performance Backup | The history alarm and performance data needs to be backed up and archived. |
| Check the Connection of the Database | Close FMX NMS interface and then log back to FMX NMS to check whether the connection of the database is normal. |

### 9.3.1.Data Backup

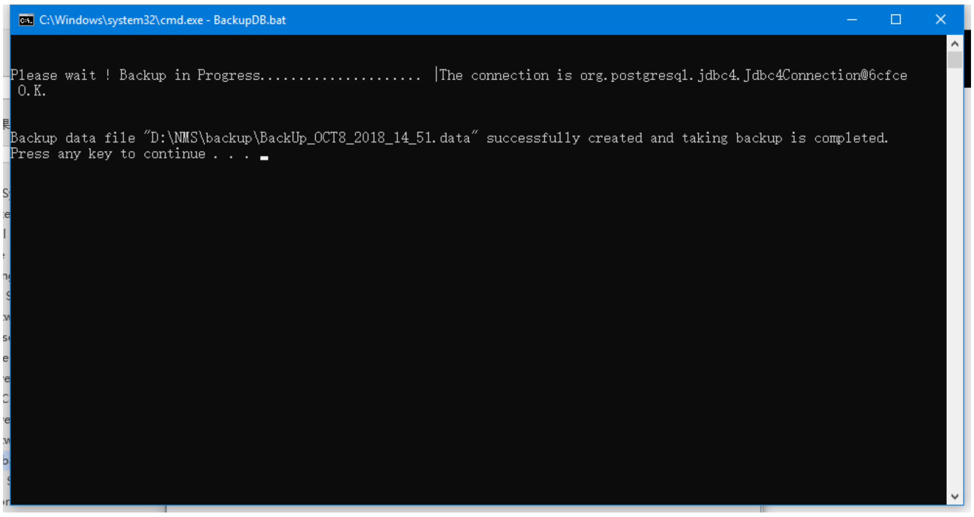
#### NMS Data Backup

Data backup needs to be performed in routine maintenance, so as to avoid loss of important data caused by misoperation. The prerequisite is to shut down the NMS server first, and click to open "DB Tool", then backup all the NMS configurations to the NMS server.



| Name |
|---|
| BackUp_OCT8_2018_14_51.data |

Figure 0-10 DB Tool

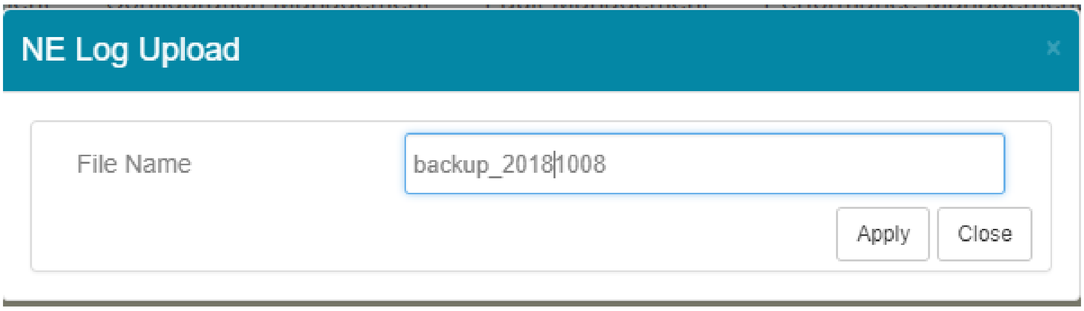


```
Please wait ! Backup in Progress.................... |The connection is org.postgresql.jdbc4.Jdbc4Connection@6cfce
 O.K.

Backup data file "D:\NMS\backup\BackUp_OCT8_2018_14_51.data" successfully created and taking backup is completed.
Press any key to continue . . .
```

Figure 0-11 NMS Data Backup

#### NE Data Backup

Select *"System Management"* → *"Upload NE Configuration"* to upload all the NE configurations to the NMS server.


NE Log Upload

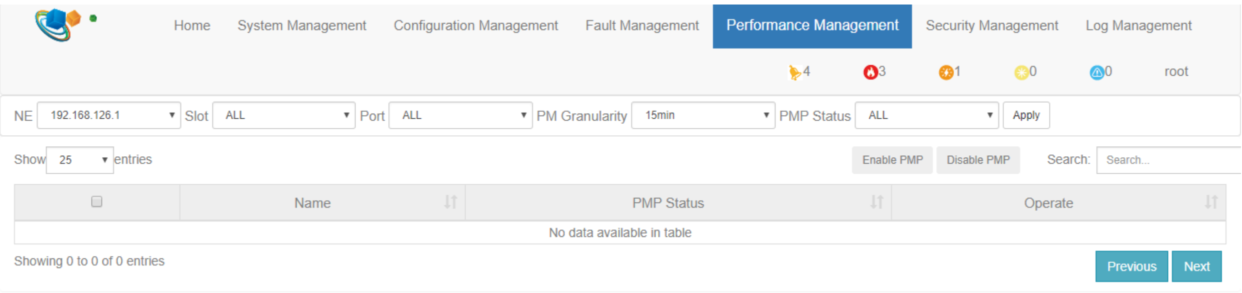
File Name: backup_20181008

Figure 0-12 Upload NE Configuration

### 9.3.2.Performance Acquisition

The NMS System will only collect the history performance of network elements which set the performance monitoring point and the monitoring time. Other network elements will not be reported. Therefore, it needs to regularly check whether the performance monitoring point and the monitoring time of the network elements are correctly set.

Select*"Performance Management"*→ *"Performance Monitoring Point"* , the performance monitoring point window pops up, as shown in the figure below:



NE 192.168.126.1 Slot ALL Port ALL PM Granularity 15min PMP Status ALL

| □ | Name | PMP Status | Operate |
|---|---|---|---|
| No data available in table | | | |

Showing 0 to 0 of 0 entries

Figure 0-13 Performance Monitoring Point

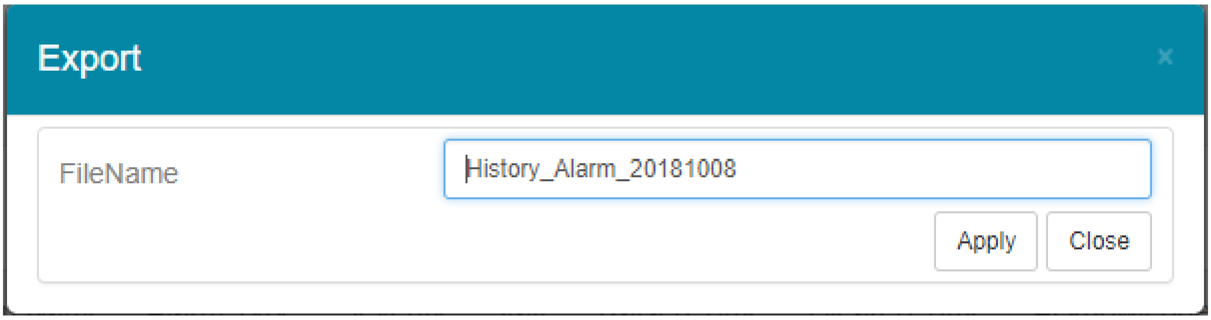
Check whether all the ports which need to collect performance data enable the performance monitoring point.

### 9.3.3.Check Hardware Work State

- Modem is with factory configuration. It must be special device for special use. It cannot be used for other purpose. It needs to check whether other work state is normal.
- Check whether the work state of mouse, keyboard, printer and display is normal.

### 9.3.4.History Alarm & Performance Backup

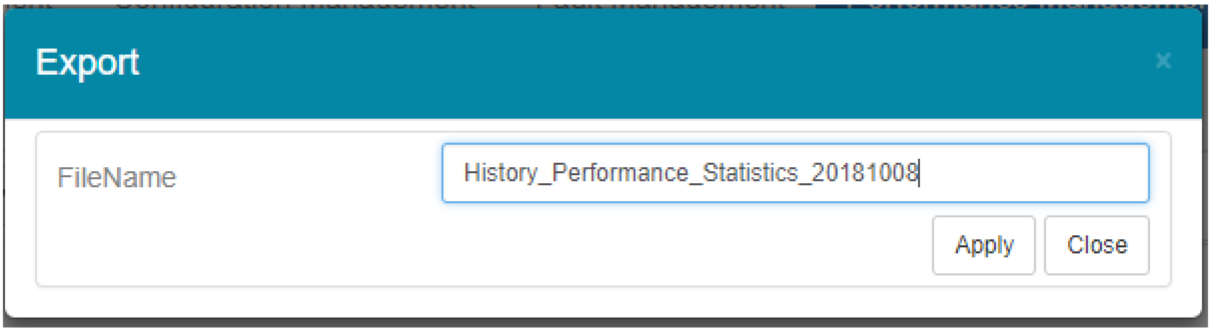
Select*"Alarm Management"*→ *"History Alarm"*and select the history alarms which need to be exported, and then click*"Export"*button, the history alarm data can be exported to the NMS server installation directory (D:\NMS\report_out\history_ Alarm).


Export

FileName: History_Alarm_20181008

Figure 0-14 Export History Alarm Data

Select*"Performance Management"* → *"History Performance Statistics"* → *"OTUk/ODUk History Performance Statistics"*and click *"Export"*button to export the history performance statistics data to the NMS server installation directory (D:\NMS\report_out\performance).


Export

FileName: History_Performance_Statistics_20181008

Figure 0-15 Export History Performance Statistics Data

### 9.3.5.Check Connection of Database

Close FMX NMS interface and then log back to NMS system to check whether the connection of the database is normal.

⚠ **No illegal shutdown of the NMS system!**

## 9.4.Quarterly Routine Maintenance

Table 0-3 Quarterly Routine Maintenance Items

| Maintenance Items | Requirements |
|---|---|
| Proofread NMS Time | Check the NMS clock and proofread it with the standard time. |
| Regularly change the login user name | Login with a new user name and make detailed record of the user name and password. |
| Check Remote Login | The device providers can login to the local host from the far end by dial-up. |
| Check NMS Function | Check whether NE and boards can be clicked. If there is equipped with the sound card, check whether the sound of alarms can be normally got. |

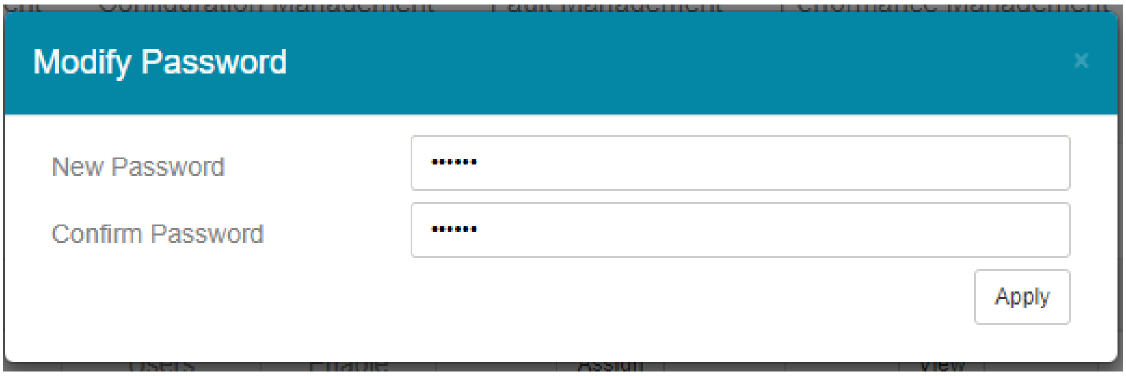
### 9.4.1.Proofread NMS Time

Check the NMS clock and proofread it with the standard time. The purpose of this operation is to make the time of the NMS computer consistent with the actual time, otherwise it will lead to start time and end time errors of the alarms and performances displayed in the NMS, and will further cause misjudgment.

### 9.4.2.Regularly Change Login User Name

In order to improve the security of the system, the NMS login name and password need to be periodically changed.

Select*"Security Management"*to add user and change password. After it changes to the new password, click*"OK"*, it will automatically exit the NMS system. The user needs to use the new user name or password to log in.


Modify Password

New Password ••••••

Confirm Password ••••••

Figure 0-16 Change User Password

### 9.4.3.Check Remote Login

Remote login plays an important role in quickly locating the fault. Therefore, it needs to check the remote maintenance function regularly. Meanwhile, every maintenance personnel in the machine room should be familiar with the operation of remote maintenance. As long as the NMS computer is with remote maintenance function, it needs to be checked regularly.

Please contact our technician to make functional test at the far end. If the maintenance personnel of the machine room are familiar with this operation, the remote maintenance function can be checked by another computer. That's no problem if remote login to NE is available.

### 9.4.4.Check NMS Function

The following items need to be checked:

(1) Whether alarms and performances can be got;

(2) Whether the new alarm can be automatically refreshed;

(3) Whether the NE and board can be clicked;

(4) If it is equipped with the sound card, whether all the alarm sounds can be obtained;

(5) Whether the board state is normal.

All these maintenance items are also daily routine maintenance items. For detailed check methods, please refer to the first three sections of this chapter.

# Chapter 10 Common Problems

This chapter introduces some problems and their solutions while using FMX NMS system. It mainly includes:

- The server program cannot start.
- The account cannot log in.
- NE cannot be added.
- NE time synchronization problem.
- NMS configuration cannot be uploaded.
- NE cannot automatically report alarm.

## 10.1.Server Program Cannot Start

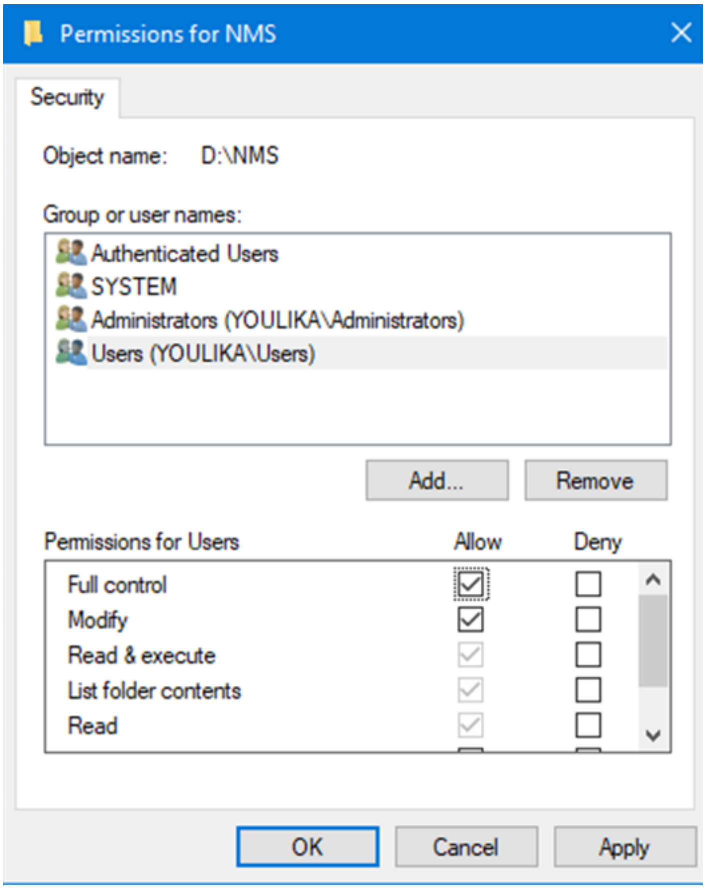
There are two possible reasons:

1. The program is not installed properly, or there is an error in the installation process.

2. The disk installed by NMS is with low permissions, so that the server program cannot start normally.

The solution to possible reason 1: Re-download the installation package and re-install it.

The solution to possible reason 2: Right click the NMS root folder, then click*"Properties"* → *"Safety"* → *"Users",* and click *"Edit"* to add all the permissions.



Object name: D:\NMS

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (YOULIKA\Administrators)
- Users (YOULIKA\Users)

| Permissions for Users | Allow | Deny |
|---|---|---|
| Full control | ☑ | □ |
| Modify | ☑ | □ |
| Read & execute | ✓ | □ |
| List folder contents | ✓ | □ |
| Read | ✓ | □ |

Figure 0-1 Modify User Right

## 10.2.Account Cannot Log In

Possible Reason: There are space, Chinese or special characters in the directory installed by NMS.

Solution: Shut down NMS server, move NMS folder to the correct root directory or re-select the directory for installation.

## 10.3.NE Cannot Be Added

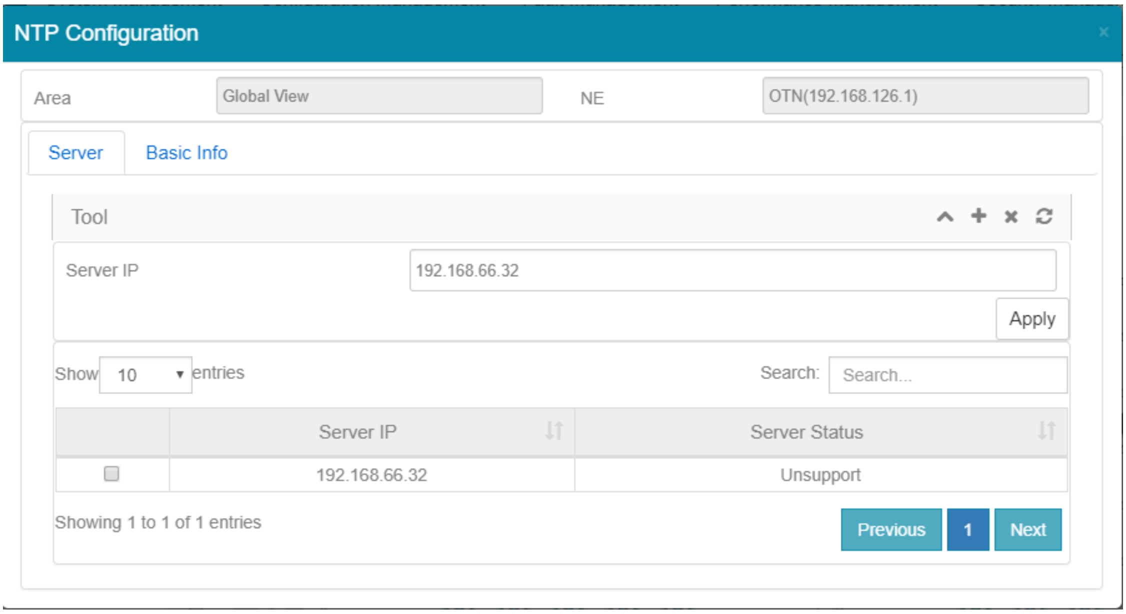
Possible Reason: Whether normal communication can be made between NE and NMS.

Solution: Enter through CMD, and ping NE IP to check whether it can communicate.

## 10.4.NE Time Is Not Synchronized

Possible Reason: NTP time server is not configured.

Solution: Select *"System Management"* → *"NTP Configuration"* to configure server IP address.



NTP Configuration

Area: Global View

NE: OTN(192.168.126.1)

Server | Basic Info

Tool

Server IP: 192.168.66.32

Apply

Show 10 entries

Search: Search...

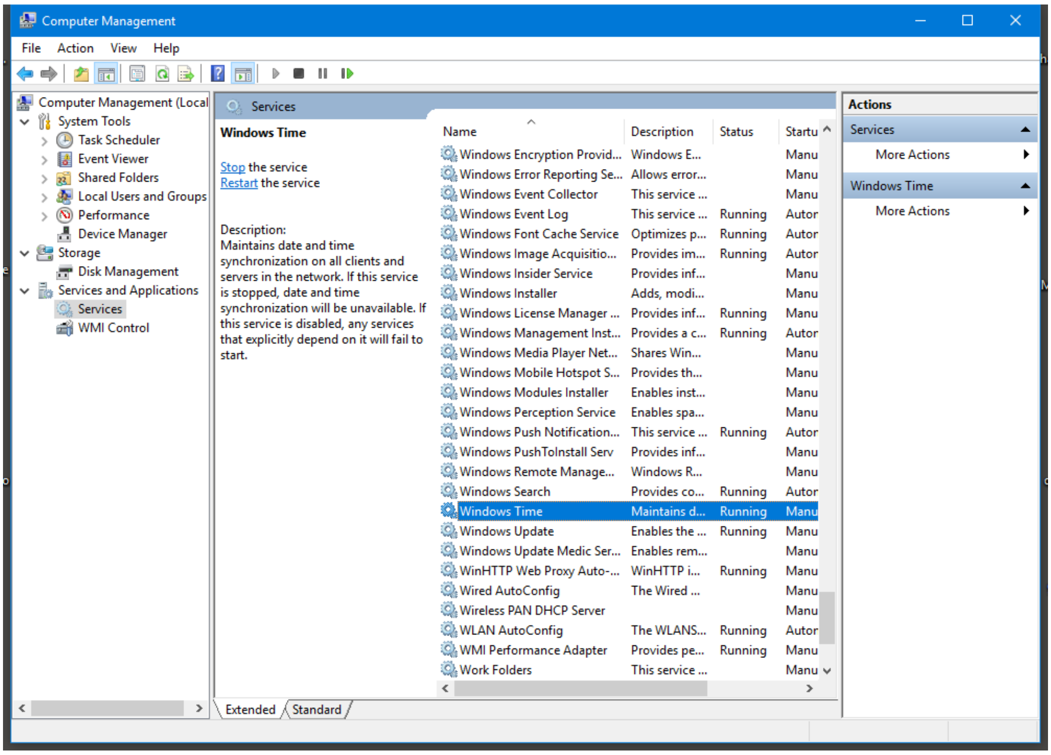
| | Server IP | Server Status |
|---|---|---|
| □ | 192.168.66.32 | Unsupport |

Showing 1 to 1 of 1 entries

Previous 1 Next

Figure 0-2 NTP Configuration

The configuration mode of the NMS server and the NTP server is as follows: right click*"Computer"* → *"Management"*→ *"Services and Applications"*→ *"Services"*→ *"Windows Time"*.



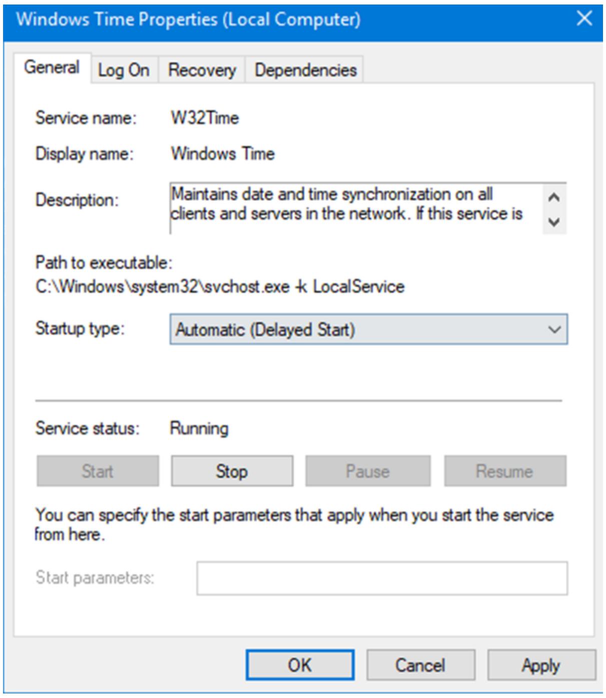
**Windows Time**

Stop the service
Restart the service

Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

| Name | Description | Status | Startu |
|---|---|---|---|
| Windows Encryption Provid... | Windows E... | | Manu |
| Windows Error Reporting Se... | Allows error... | | Manu |
| Windows Event Collector | This service ... | | Manu |
| Windows Event Log | This service ... | Running | Autor |
| Windows Font Cache Service | Optimizes p... | Running | Autor |
| Windows Image Acquisitio... | Provides im... | Running | Autor |
| Windows Insider Service | Provides inf... | | Manu |
| Windows Installer | Adds, modi... | | Manu |
| Windows License Manager ... | Provides inf... | Running | Manu |
| Windows Management Inst... | Provides a c... | Running | Autor |
| Windows Media Player Net... | Shares Win... | | Manu |
| Windows Mobile Hotspot S... | Provides th... | | Manu |
| Windows Modules Installer | Enables inst... | | Manu |
| Windows Perception Service | Enables spa... | | Manu |
| Windows Push Notification... | This service ... | Running | Autor |
| Windows PushToInstall Serv | Provides inf... | | Manu |
| Windows Remote Manage... | Windows R... | | Manu |
| Windows Search | Provides co... | Running | Autor |
| Windows Time | Maintains d... | Running | Manu |
| Windows Update | Enables the ... | Running | Manu |
| Windows Update Medic Ser... | Enables rem... | | Manu |
| WinHTTP Web Proxy Auto-... | WinHTTP i... | Running | Manu |
| Wired AutoConfig | The Wired ... | | Manu |
| Wireless PAN DHCP Server | | | Manu |
| WLAN AutoConfig | The WLANS... | Running | Autor |
| WMI Performance Adapter | Provides pe... | Running | Manu |
| Work Folders | This service ... | | Manu |

Figure 0-3 Start NTP Server



Service name: W32Time

Display name: Windows Time

Description: Maintains date and time synchronization on all clients and servers in the network. If this service is

Path to executable:
C:\Windows\system32\svchost.exe -k LocalService

Startup type: Automatic (Delayed Start)

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 0-4 NTP Server Start Type Configuration

## 10.5.Network Management Configuration Cannot Be Uploaded

Possible Reason: The NMS server has not been shut down.

Solution: The NMS server needs to be normally shut down before exporting the network management configurations.

## 10.6.NE Cannot Automatically Report Alarms

There are two possible reasons:

1. The NMS SNMP Trap address is not correctly configured.

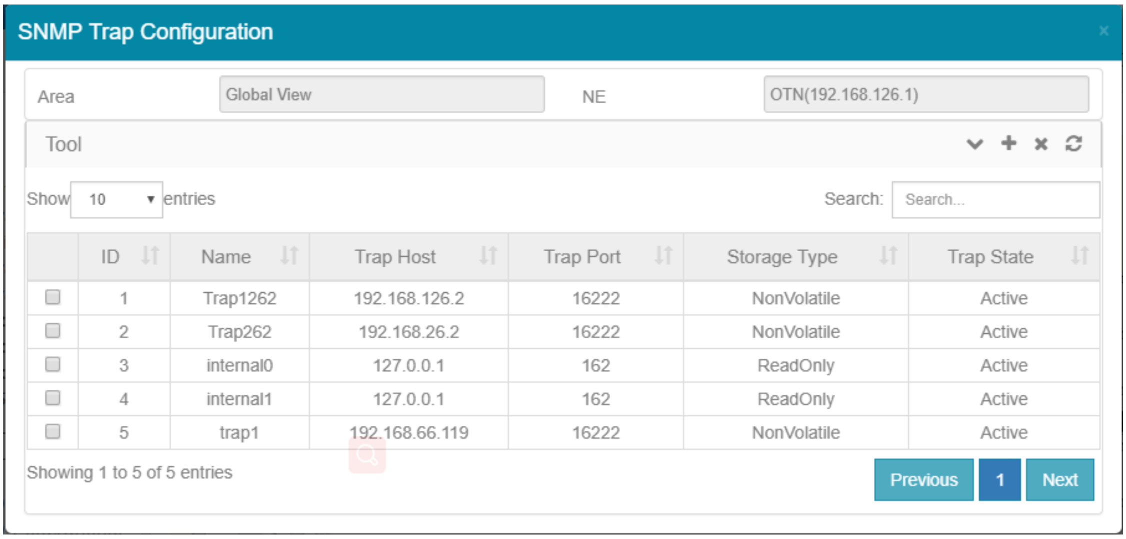
2. There is a firewall blocking on the computer that installs NMS server.

The solution to possible reason 1:

Enter SNMP Trap configuration interface to view Trap information configured for the current NE. Check whether the configured address is the same as the IP address of the NE communication.

The solution to possible reason 2:

Shut down firewall or set the firewall rule to allow opening ports.



SNMP Trap Configuration

Area: Global View NE: OTN(192.168.126.1)

Tool

Show 10 entries Search: Search...

| | ID | Name | Trap Host | Trap Port | Storage Type | Trap State |
|---|---|---|---|---|---|---|
| □ | 1 | Trap1262 | 192.168.126.2 | 16222 | NonVolatile | Active |
| □ | 2 | Trap262 | 192.168.26.2 | 16222 | NonVolatile | Active |
| □ | 3 | internal0 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 4 | internal1 | 127.0.0.1 | 162 | ReadOnly | Active |
| □ | 5 | trap1 | 192.168.66.119 | 16222 | NonVolatile | Active |

Showing 1 to 5 of 5 entries

Figure 0-5 NTP Server Startup Type Configuration

# Abbreviation

**This table introduces some Acronym definition. It mainly includes:**

| Item | Definition |
|---|---|
| AIS | Alarm Indication Signal |
| BDI | Backward Defect Indication |
| BEI | Backward Error Indication |
| BER | Bit Error Ratio |
| BIAE | Backward Incoming Alignment Error |
| DCM | Dispersion Compensation Module |
| DCN | Data Communication Network |
| DWDM | Dense Wavelength Division Multiplexing |
| EDFA | Erbium-Doped Fiber Amplifier |
| EMS | Element Management System |
| FEC | Forward Error Correction |
| GCC | General Communication Channel |
| GE | Gigabit Ethernet |
| GFP | Generic Framing Procedure |
| IP | Internet Protocol |
| NE | Network Element |
| OCh | Optical Channel |
| OSC | Optical Supervisory Channel |
| OSNR | Optical Signal-to-Noise Ratio |
| OTN | Optical Transport Network |
| PM | Path Monitoring |
| SDH | Synchronous Digital Hierarchy |
| TCM | Tandem Connection Monitoring |
| TTI | Trail Trace Identifier |
| WDM | Wavelength Division Multiplexing |