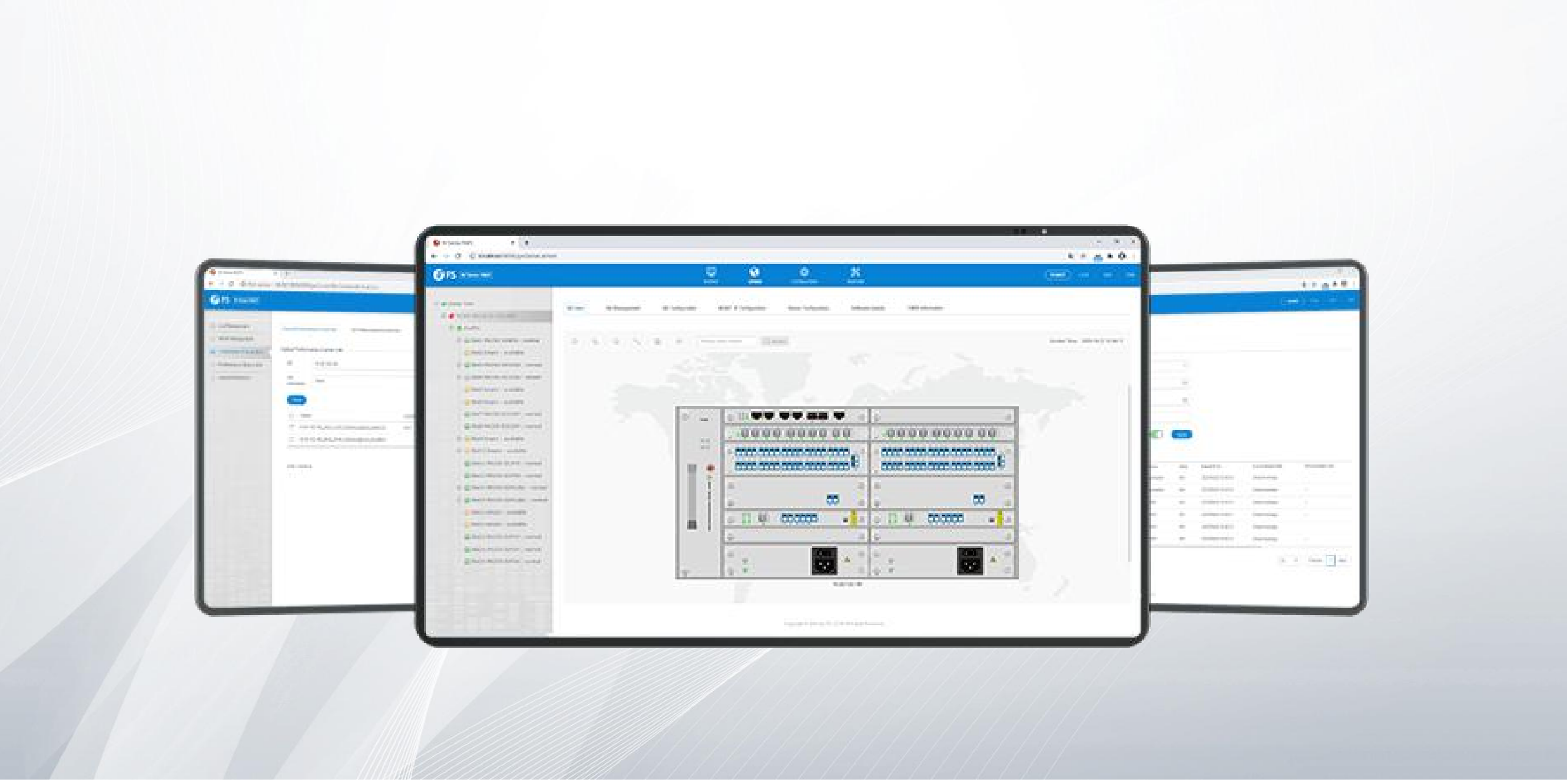
M Series NMS

Network Management User Manual



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
M Series NMS	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.

1. NMS System Overview

1.1. NMS System Introduction

M Series 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

M Series 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.

M Series 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 M Series system includes all kinds of IP devices in backbone layer, convergence layer and access layer. At present, the management of soft switch, integrated access server, digital subscriber loop, Ethernet switch, router and ADSL device has been implemented.

M Series system covers four layers of TMN management:

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

M Series system adopts friendly and full graphical interface, which is simple and easy to operate.

M Series 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 1-1 Hardware and Operating System Requirements

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

The M Series 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.

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

1.4. Networking Mode

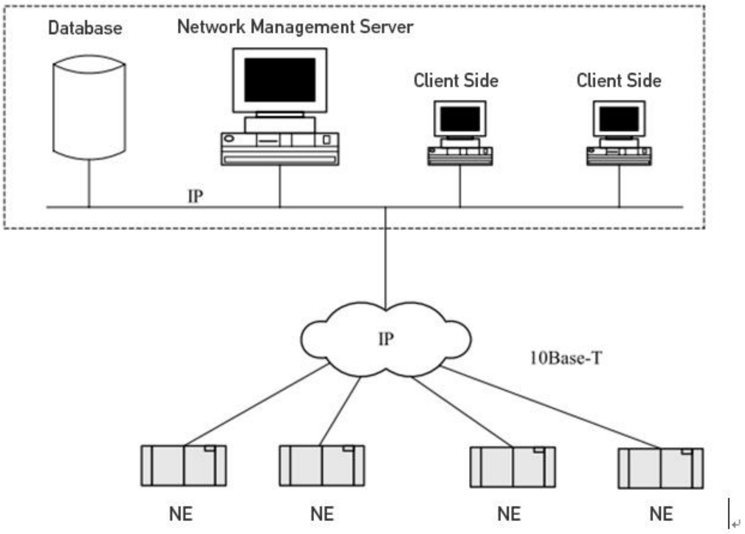


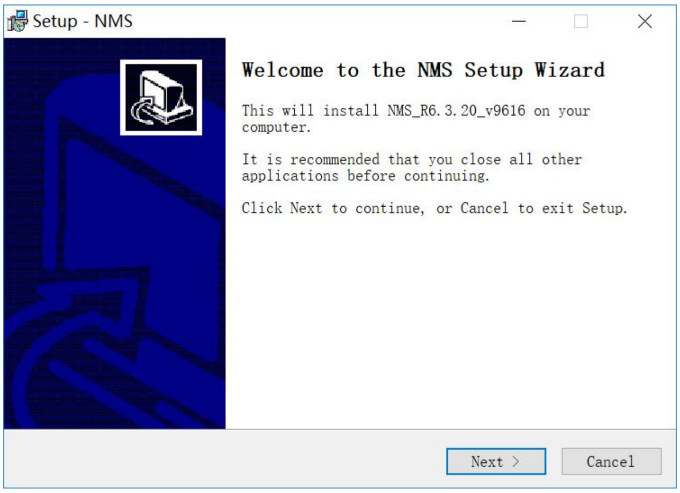
Figure 1-1 Network Diagram

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

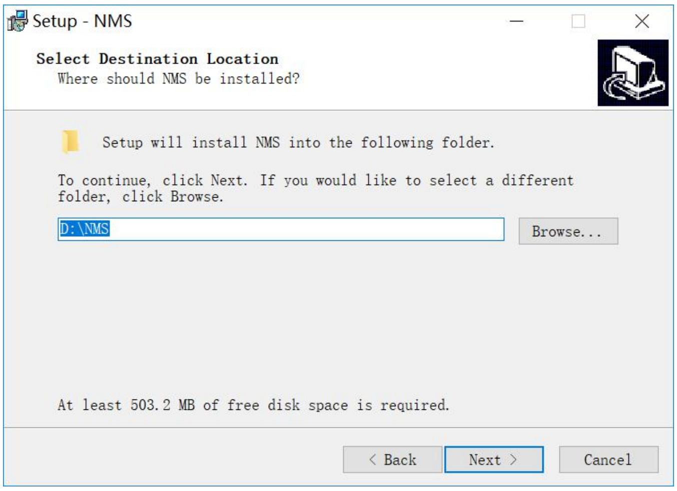
This will install NMS_R6.3.20_v9616 on your computer.

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

Click Next to continue, or Cancel to exit Setup.

Figure 2-1 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.

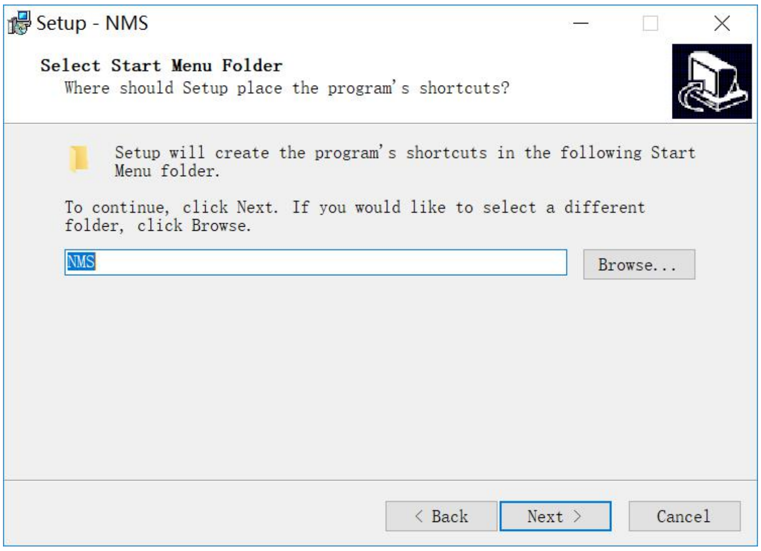
To continue, click Next. If you would like to select a different folder, click Browse.

D:\NMS

At least 503.2 MB of free disk space is required.

Figure 2-2 Software Installation-Destination Location

3. After selecting the installation path, click*"Next".*



Setup - NMS

Select Start Menu Folder

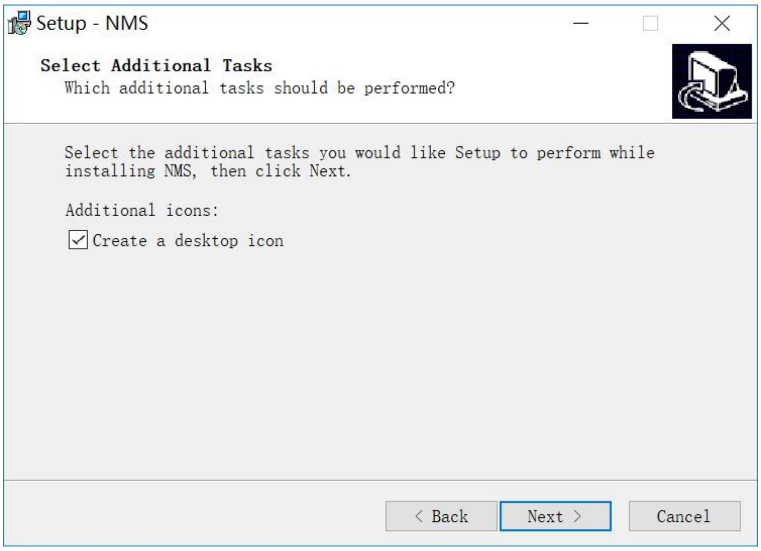
Where should Setup place the program's shortcuts?

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 2-3 Software Installation-Select Start Menu Folder



Setup - NMS

Select Additional Tasks

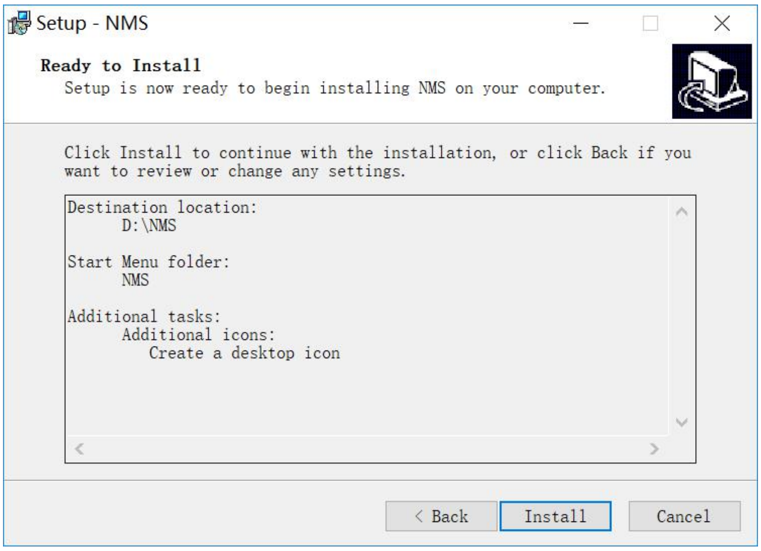
Which additional tasks should be performed?

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

Additional icons:

☑ Create a desktop icon

Figure 2-4 Software Installation-Create A Desktop Icon



Setup - NMS

Ready to Install

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

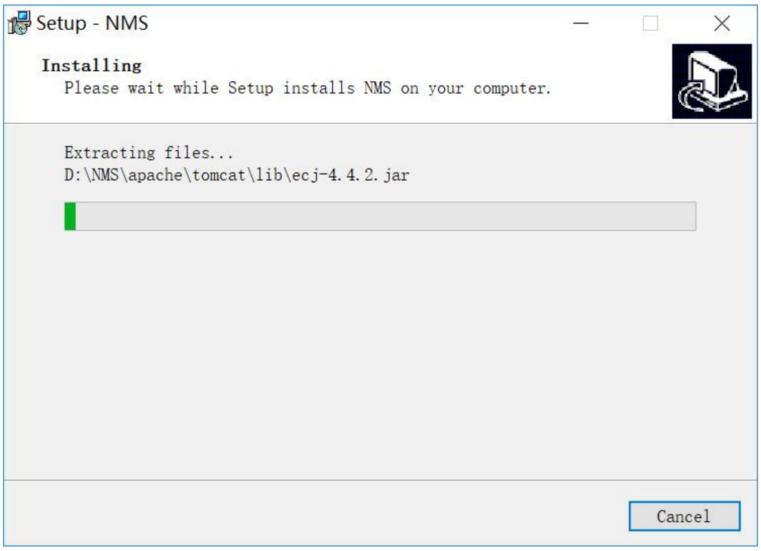
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      D:\NMS

Start Menu folder:
      NMS

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

Figure 2-5 Software Installation-Ready to Install

Click*"Install"*to install the software.

4. Start the installation.



Setup - NMS

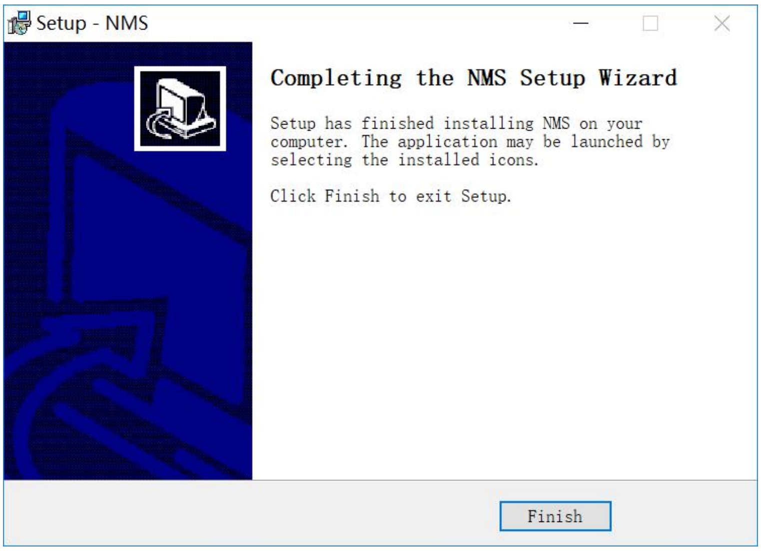
Installing

Please wait while Setup installs NMS on your computer.

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

Figure 2-6 Software Installation-Installing

5. The installation is successfully completed.



Setup - NMS

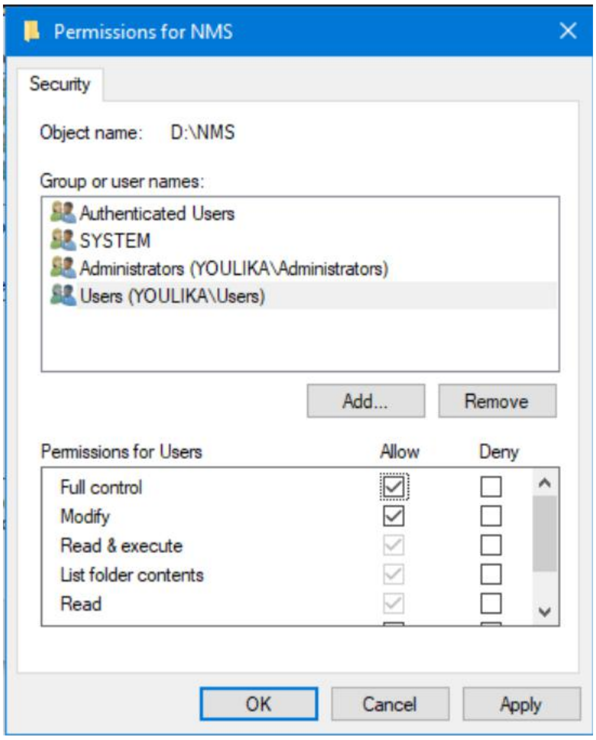
Completing the NMS Setup Wizard

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

Click Finish to exit Setup.

Figure 2-7 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:



Object name: D:\NMS

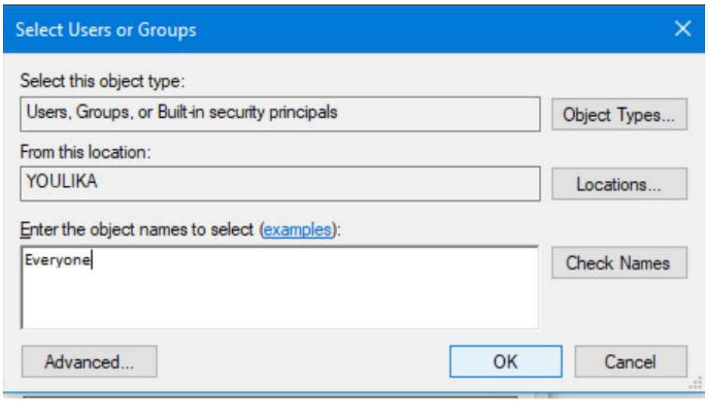
Group or user names:

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

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

Figure 2-8 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 this object type: Users, Groups, or Built-in security principals

From this location: YOULIKA

Enter the object names to select (examples): Everyone

Figure 2-9 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 M Series 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 M Series network management software.

2.2. Key License Validation

Steps

The key license validation is needed when you use the software for the first time. The license key is included in the CD. (If you can't find the license key, please contact FS sales manager for help.)

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:

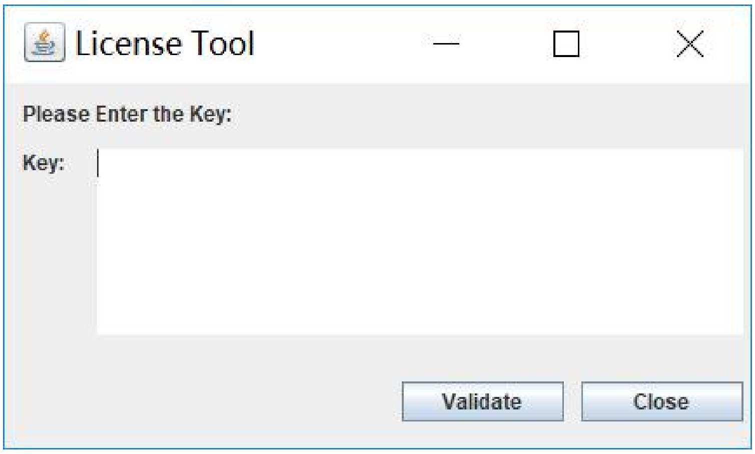


Figure 2-10 Key License Validation Interface

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.

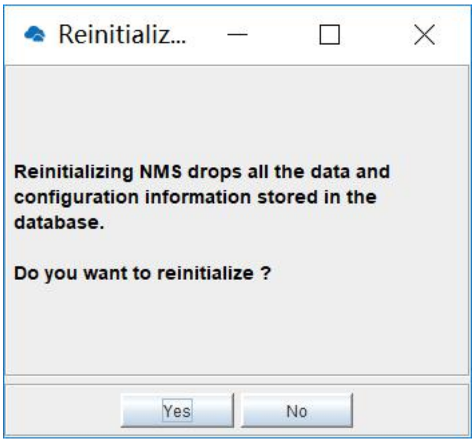
Related Information

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.

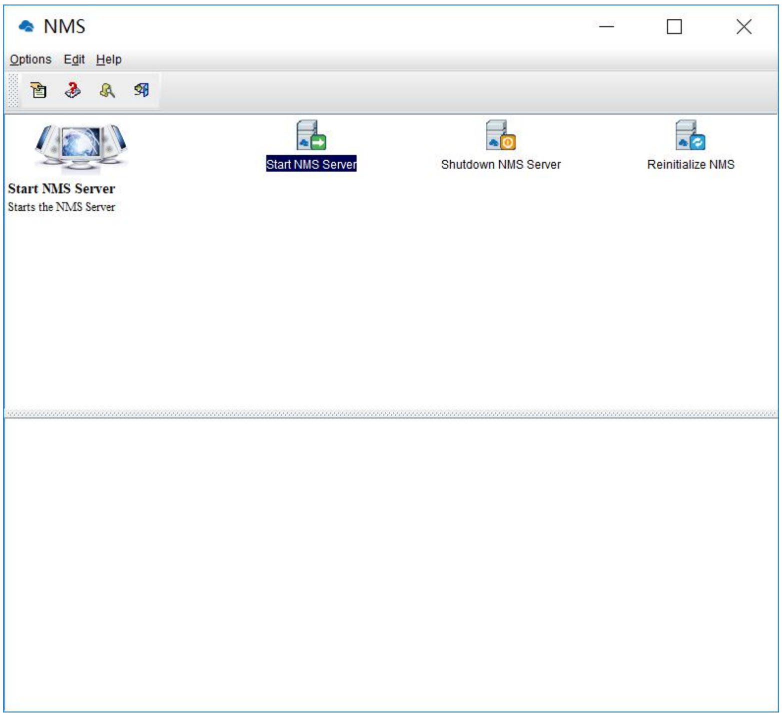
Do you want to reinitialize ?

Figure 2-11 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:

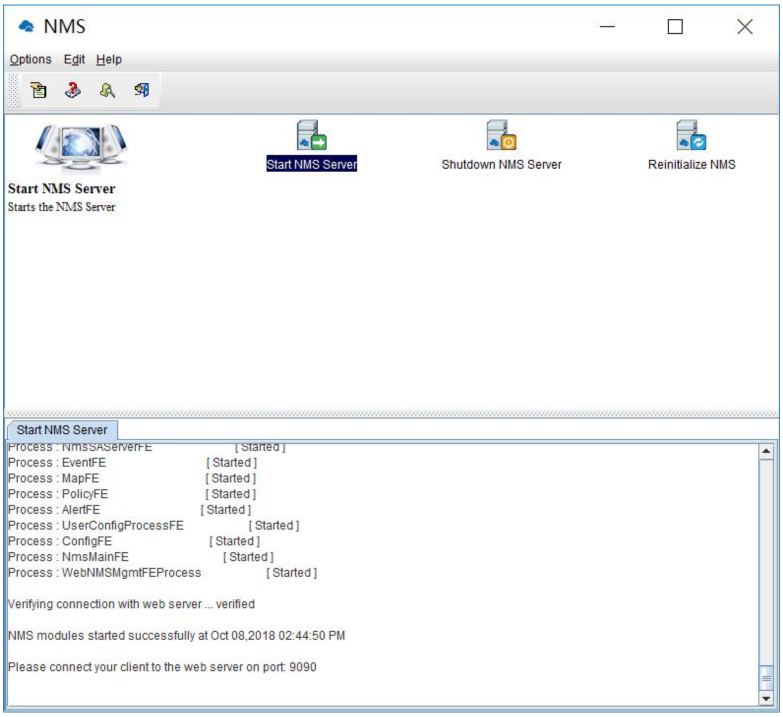


Start NMS Server

Starts the NMS Server

Figure 2-12 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
```

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:

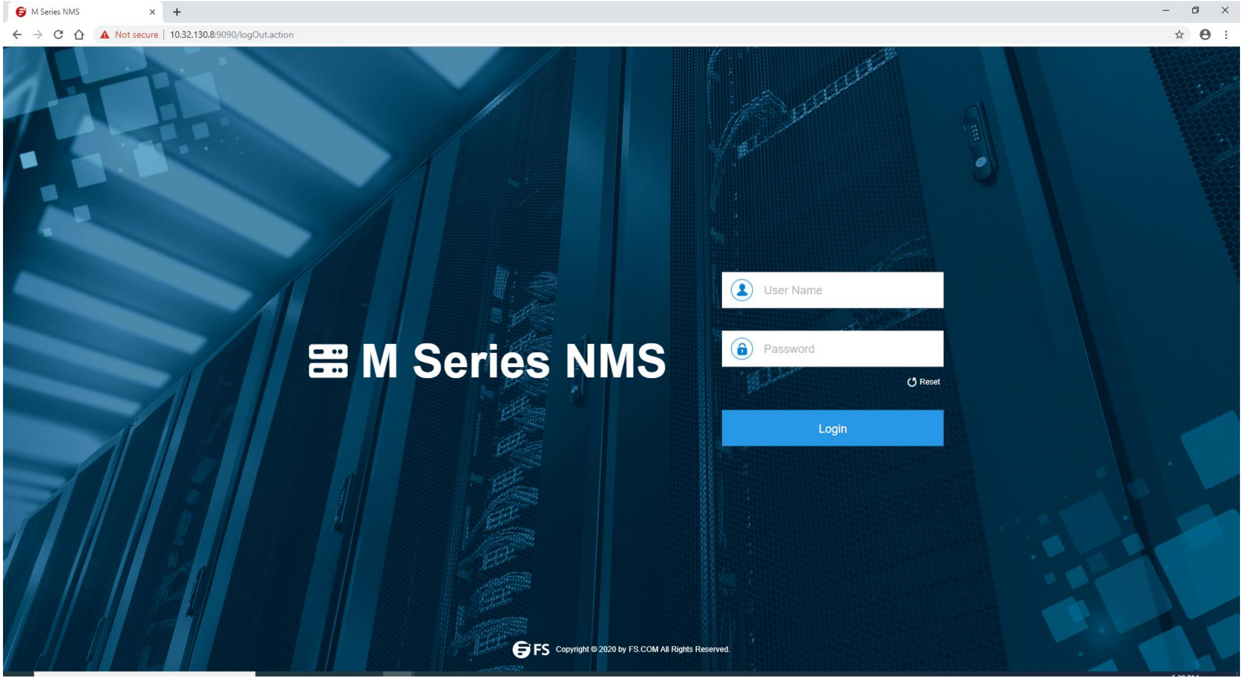
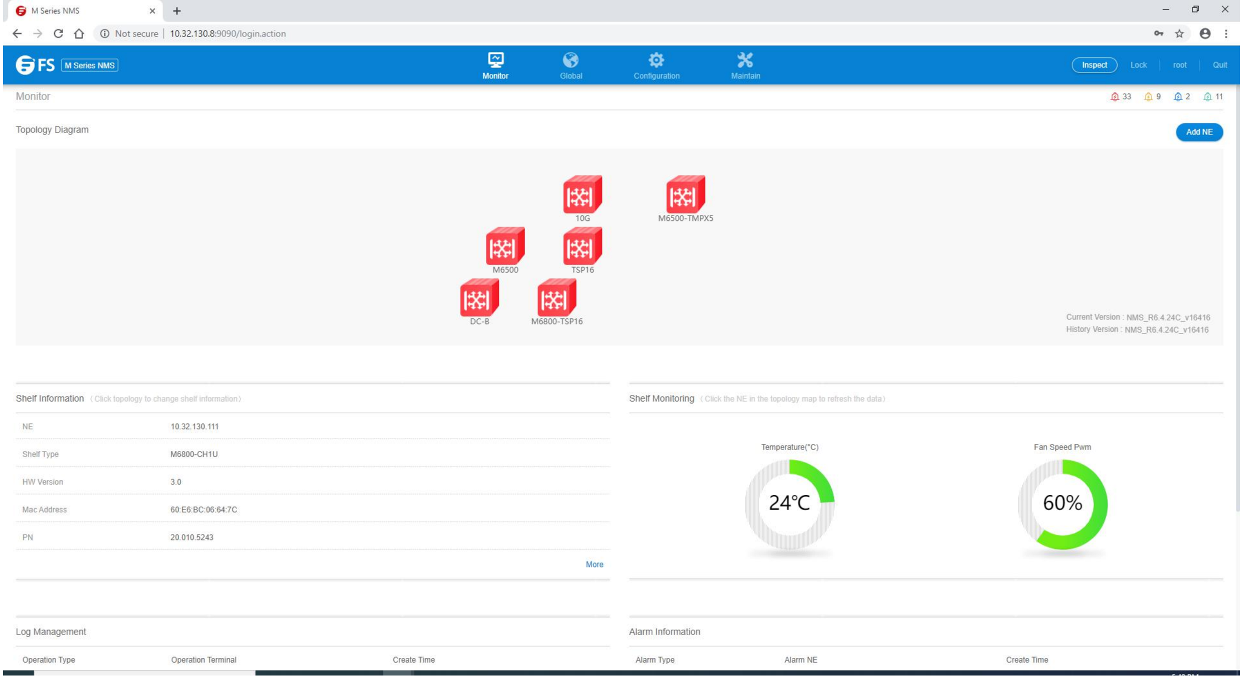

M Series NMS
Not secure | 10.32.130.8:9090/logOut.action
M Series NMS
User Name
Password
Reset
Login
FS Copyright © 2020 by FS.COM All Rights Reserved.

Figure 2-13 Login NMS - Login Interface

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



Current Version : NMS_R6.4.24C_v16416
History Version : NMS_R6.4.24C_v16416

Shelf Information (Click topology to change shelf information)

NE	10.32.130.111
Shelf Type	M6800-CH1U
HW Version	3.0
Mac Address	60:E6:BC:06:64:7C
PN	20.010.5243

Figure 2-14 Login NMS - Home

2.6. Stop Server End Program

Prerequisite

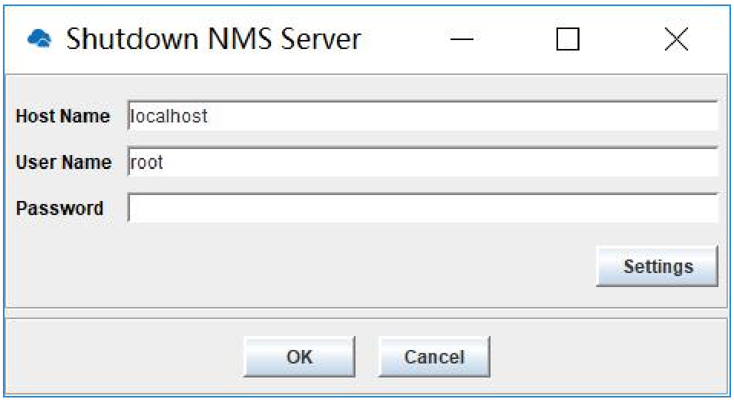
The NMS server has been successfully started.

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 2-15 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:

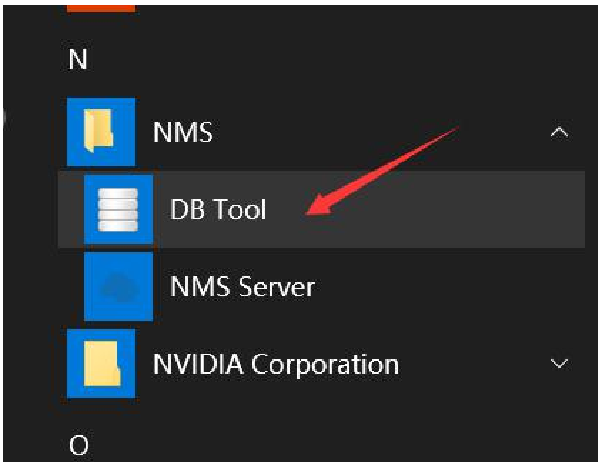


Figure 2-16 DB Tool Path

Steps

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

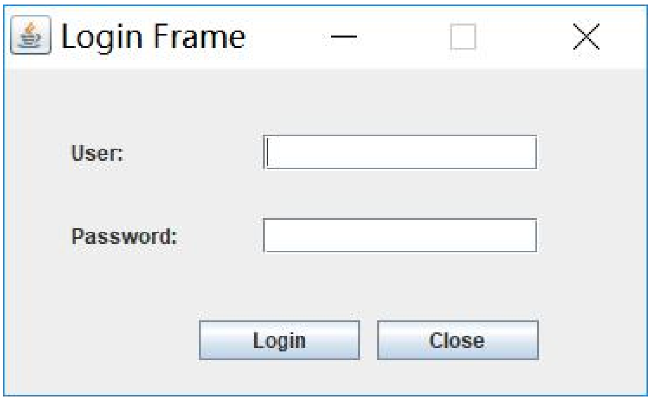


Figure 2-17 DB Tool Login Frame

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

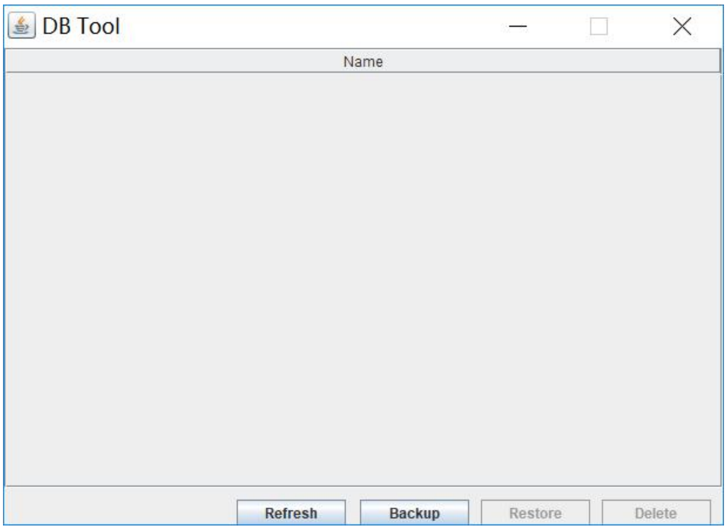
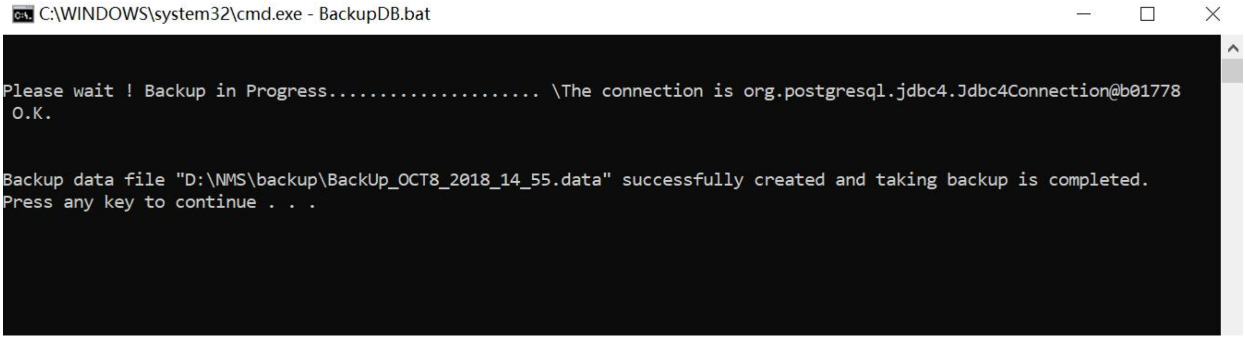


Figure 2-18 DB Tool Interface

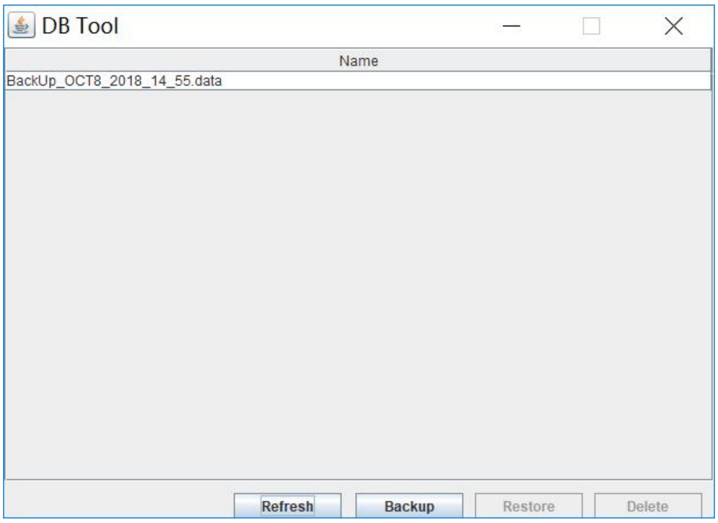
The database backup can be realized by clicking*"Backup"* button. After the backup is successful, you can view the backup data by clicking *"Refresh"*button, as shown in the figure below:



C:\WINDOWS\system32\cmd.exe - BackupDB.bat

```
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 2-19 Successful Database Backup



DB Tool

Name
BackUp_OCT8_2018_14_55.data

Figure 2-20 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

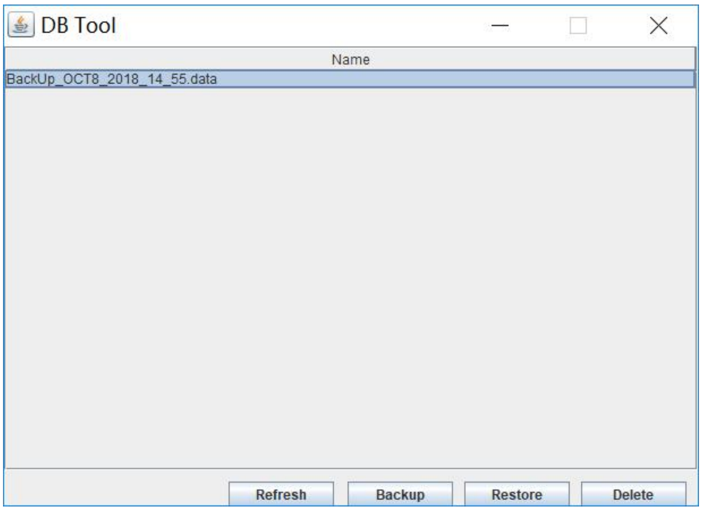
The NMS server has been shut down.

Related Information

Shutdown NMS server

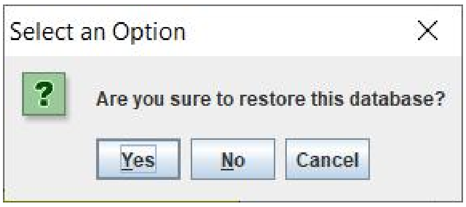
Steps

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:



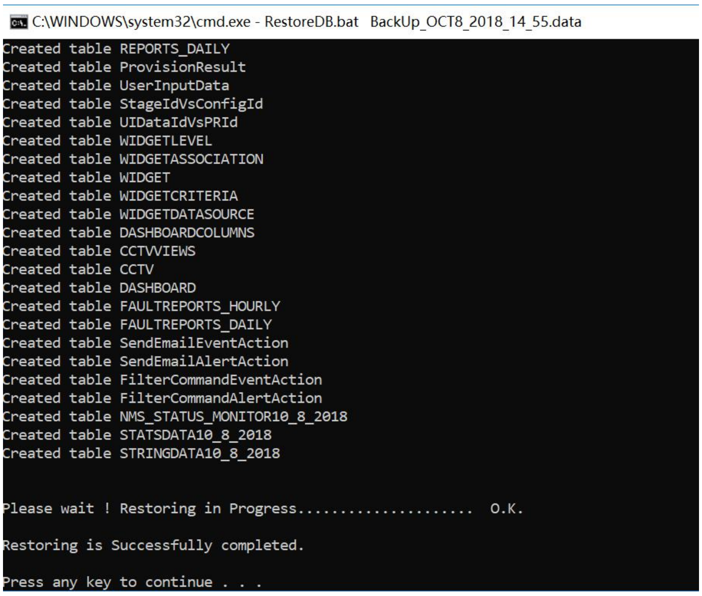
BackUp_OCT8_2018_14_55.data

Figure 2-21 View Restored Data



Are you sure to restore this database?

Figure 2-22 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 2-23 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.

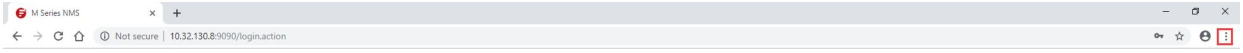


Figure 2-24 Chrome Settings

2. Open the menu and select “Settings”.

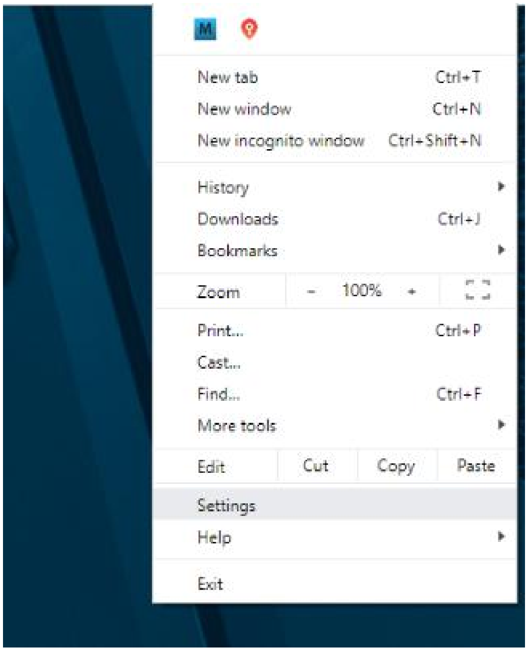
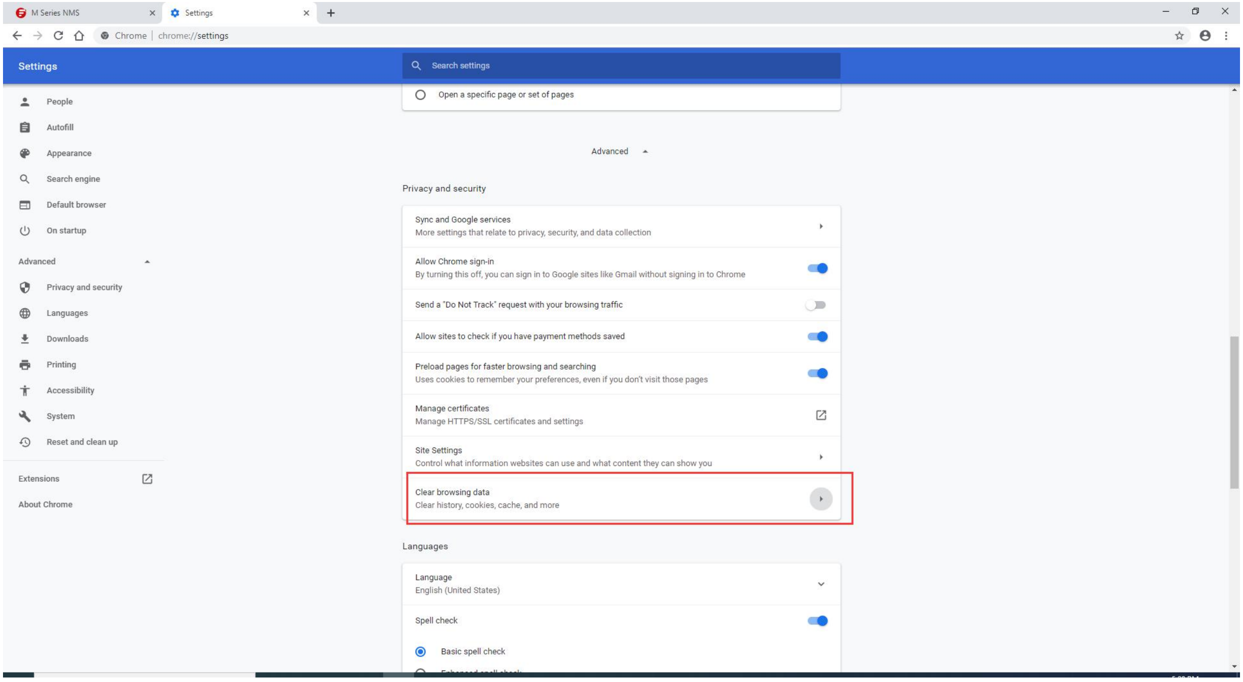


Figure 2-25 Menu Options

3. Enter the settings page, select the last option *“”Clear browsing data”* to clear the browser cache.



○ Open a specific page or set of pages

Advanced

Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

Site Settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

Languages

Language
English (United States)

Spell check

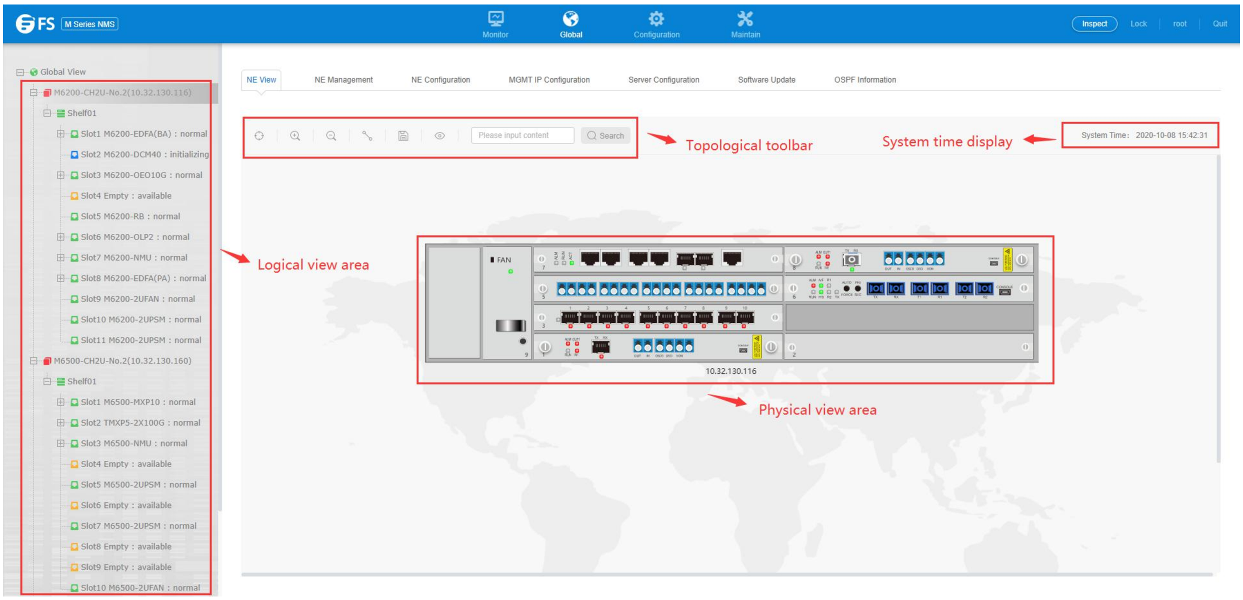
● Basic spell check

Figure 2-26 Clear Cache

3. Interface Operation of NMS System

3.1. Interface Operation

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



Global View
M6200-CH2U-No.2(10.32.130.116)
Shelf01
Slot1 M6200-EDFA(BA) : normal
Slot2 M6200-DCM40 : initializing
Slot3 M6200-OEO10G : normal
Slot4 Empty : available
Slot5 M6200-RB : normal
Slot6 M6200-OLP2 : normal
Slot7 M6200-NMU : normal
Slot8 M6200-EDFA(PA) : normal
Slot9 M6200-2UFAN : normal
Slot10 M6200-2UPSM : normal
Slot11 M6200-2UPSM : normal
M6500-CH2U-No.2(10.32.130.160)
Shelf01
Slot1 M6500-MXP10 : normal
Slot2 TMXP5-2X100G : normal
Slot3 M6500-NMU : normal
Slot4 Empty : available
Slot5 M6500-2UPSM : normal
Slot6 Empty : available
Slot7 M6500-2UPSM : normal
Slot8 Empty : available
Slot9 Empty : available
Slot10 M6500-2UFAN : normal

System Time: 2020-10-08 15:42:31

Topological toolbar

System time display

Logical view area

Physical view area

Figure 3-1 Logon Main Interface of NMS System

3.2. Interface Operation

3.1.1. Screen Lock

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

Click "*Lock*" in the upper right corner of the top menu bar to lock the network management interface.

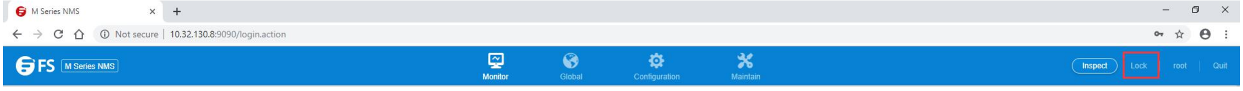


Figure 3-2 Root User Menu-Screen Lock

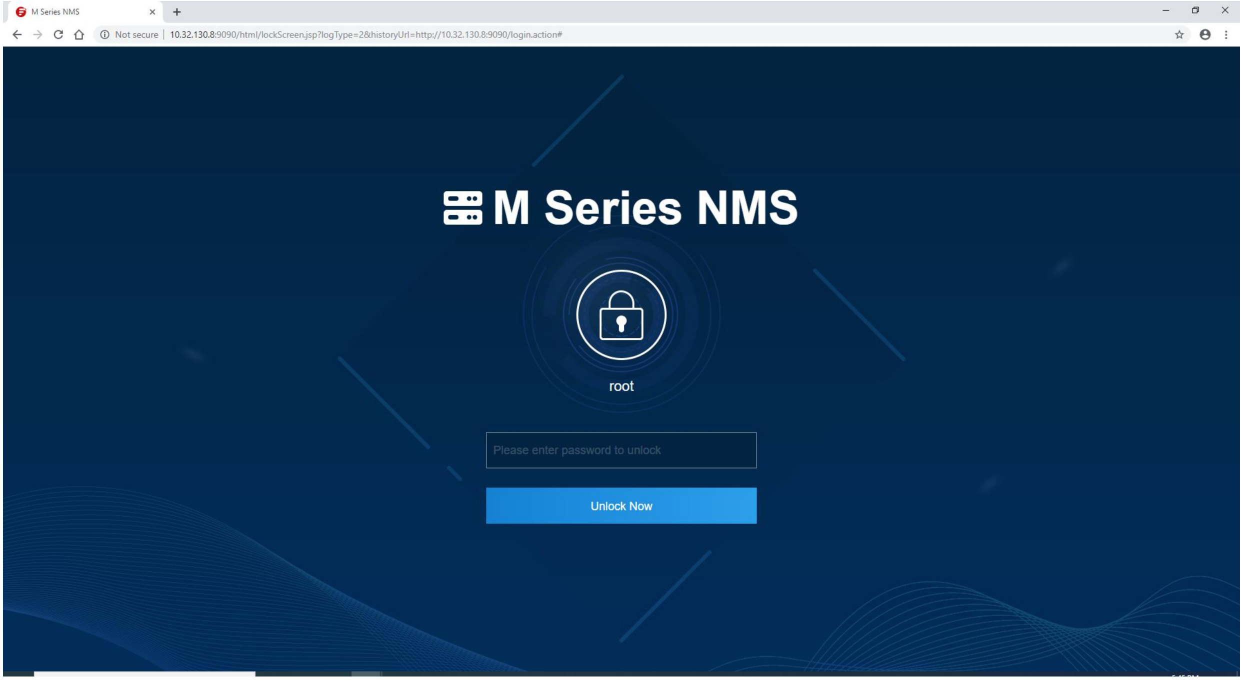
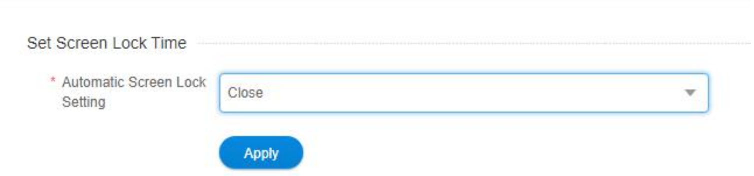

M Series NMS
Not secure | 10.32.130.8:9090/html/lockScreen.jsp?logType=2&historyUrl=http://10.32.130.8:9090/login.action#
M Series NMS
root
Please enter password to unlock
Unlock Now

Figure 3-3 Screen Lock Interface

Set automatic screen lock time:

Click the "*Configure*" button in the top menu, select "*Set Lock Screen Time*", the following interface will pop up. (The lock screen function is off by default)

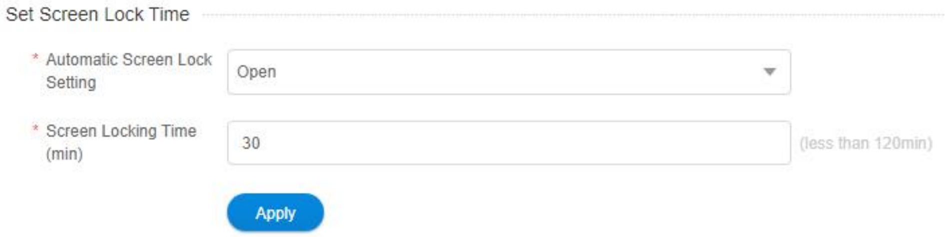


Set Screen Lock Time

* Automatic Screen Lock Setting: Close

Figure 3-4 Turn on setting the screen lock time

Select the drop-down menu to enable the lock screen and enter the lock time.



Set Screen Lock Time

* Automatic Screen Lock Setting: Open

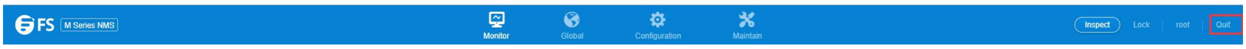
* Screen Locking Time (min): 30 (less than 120min)

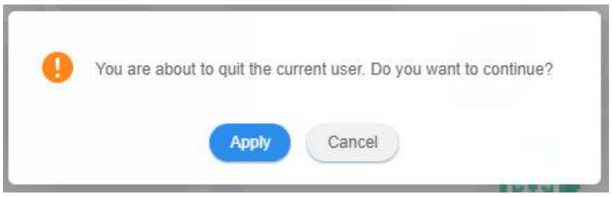
Figure 3-5 Turn on the lock screen to set the lock time

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 "*Quit*" in the upper right corner of the top menu bar, you can exit the login and the following interface will pop up.



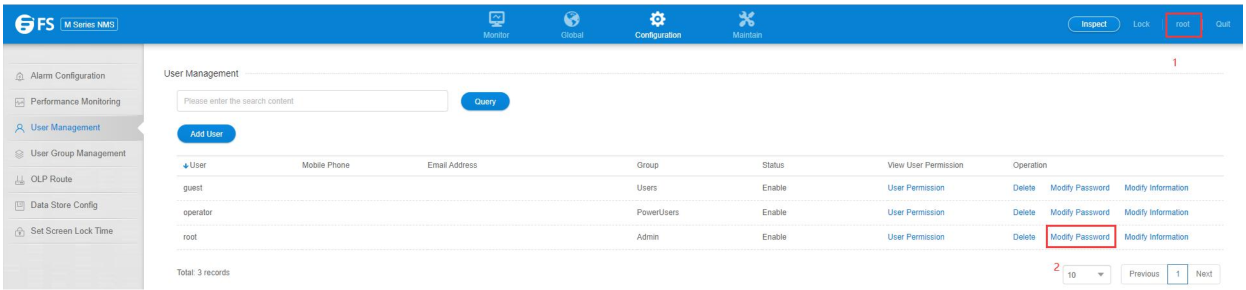


You are about to quit the current user. Do you want to continue?

Figure 3-6 Root User Menu-Exit

3.1.3.Change Password

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



User Management

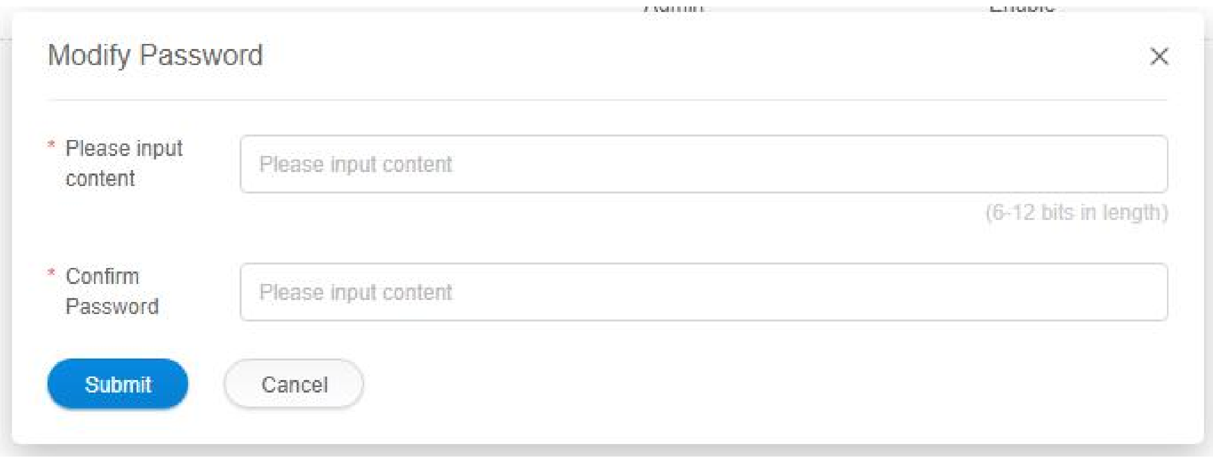
Please enter the search content

User	Mobile Phone	Email Address	Group	Status	View User Permission	Operation		
guest			Users	Enable	User Permission	Delete	Modify Password	Modify Information
operator			PowerUsers	Enable	User Permission	Delete	Modify Password	Modify Information
root			Admin	Enable	User Permission	Delete	Modify Password	Modify Information

Total: 3 records

10

Figure 3-7 Root User Menu-Change Password



Modify Password

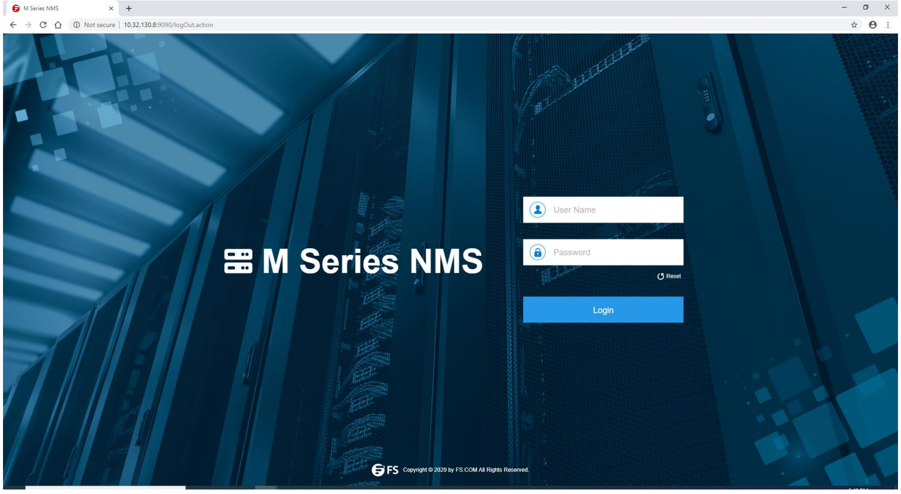
* Please input content: Please input content

(6-12 bits in length)

* Confirm Password: Please input content

Figure 3-8 Change Password

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



M Series NMS
Not secure | 10.32.130.8:9090/logOut.action
M Series NMS
User Name
Password
Reset
Login
FS Copyright © 2020 by FS.COM All Rights Reserved.

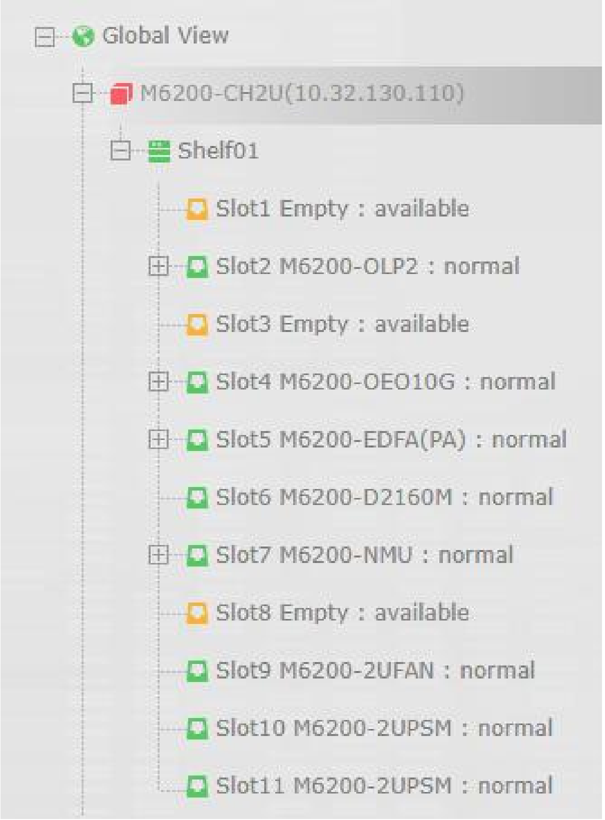
Figure 3-9 Login with New Password

4. System Management

4.1. NE(Network Element) Management

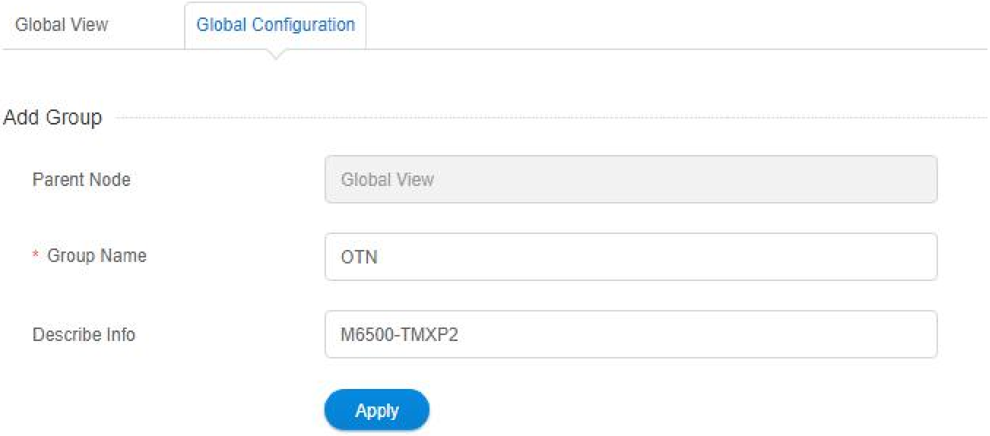
4.1.1. Add Group

Click *"Global View"* --> *"Global Configuration"* to add user groups. There is no limit to the number of groups (users can create multi-level group menus to differentiate between devices in different rooms).



Global View
- M6200-CH2U(10.32.130.110)
  - Shelf01
    - Slot1 Empty : available
    - Slot2 M6200-OLP2 : normal
    - Slot3 Empty : available
    - Slot4 M6200-OEO10G : normal
    - Slot5 M6200-EDFA(PA) : normal
    - Slot6 M6200-D2160M : normal
    - Slot7 M6200-NMU : normal
    - Slot8 Empty : available
    - Slot9 M6200-2UFAN : normal
    - Slot10 M6200-2UPSM : normal
    - Slot11 M6200-2UPSM : normal

Figure 4-1 NE Management-Global View



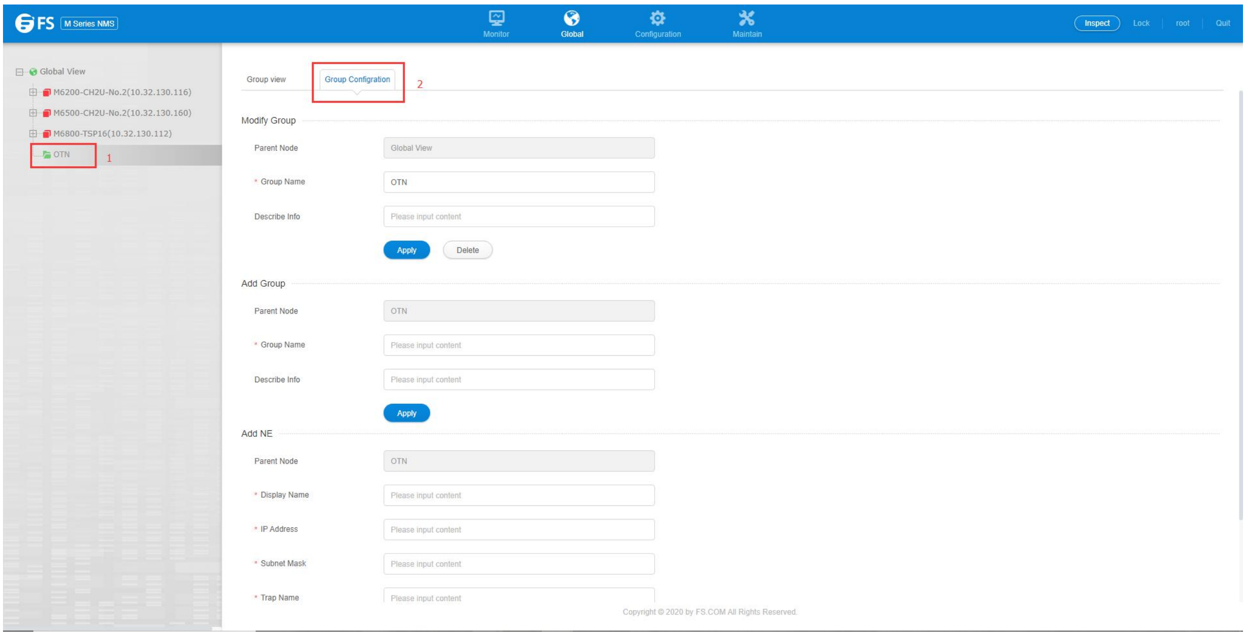
Add Group

Parent Node	Global View
* Group Name	OTN
Describe Info	M6500-TMXP2

Figure 4-2 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.


FS M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Global View
M6200-CH2U-No.2(10.32.130.116)
M6500-CH2U-No.2(10.32.130.160)
M6800-TSP16(10.32.130.112)
OTN
1
Group view
Group Configration
2
Apply
Delete
Apply
Copyright © 2020 by FS.COM All Rights Reserved

Modify Group

Parent Node: Global View

* Group Name: OTN

Describe Info: Please input content

Add Group

Parent Node: OTN

* Group Name: Please input content

Describe Info: Please input content

Add NE

Parent Node: OTN

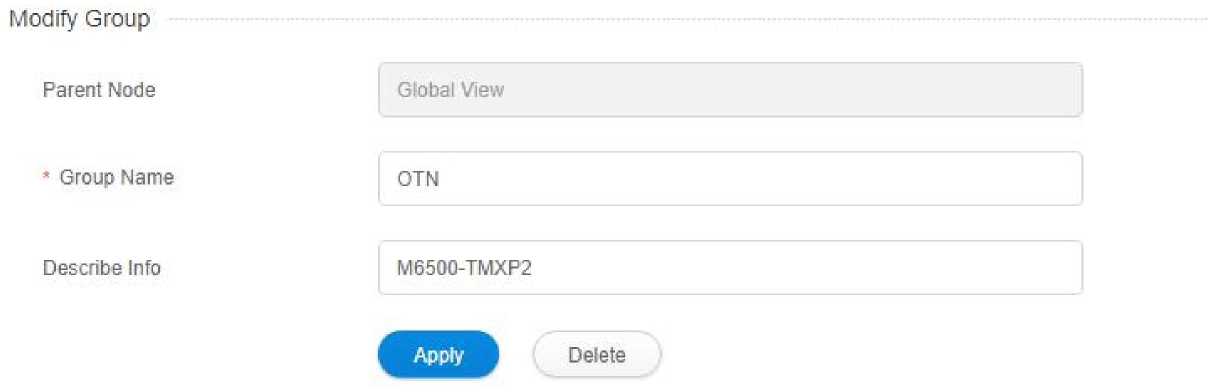
* Display Name: Please input content

* IP Address: Please input content

* Subnet Mask: Please input content

* Trap Name: Please input content

Figure 4-3 NE Management-Group Node



Modify Group

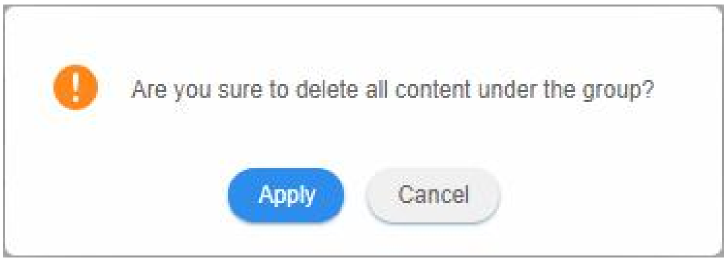
Parent Node: Global View

* Group Name: OTN

Describe Info: M6500-TMXP2

Figure 4-4 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 4-5 NE Management-Delete Group

4.1.2. Add NE

Prerequisite

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

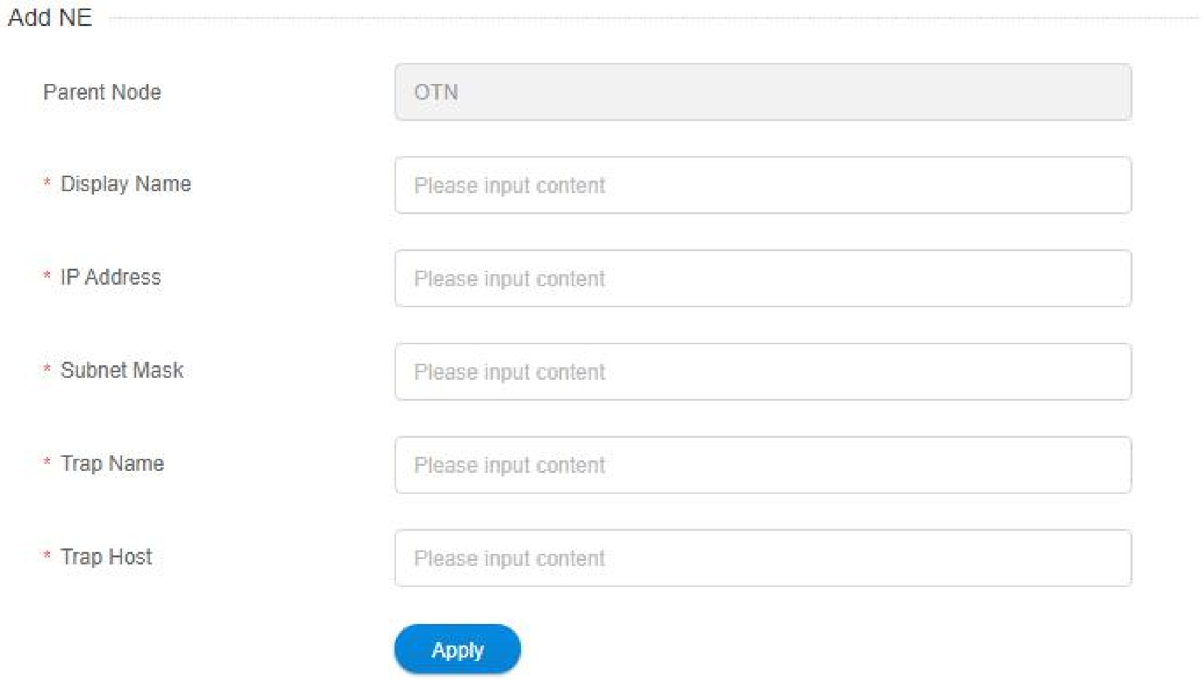
2. The NE has been physically connected with the NMS server.

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

Steps

1.Open the browser to enter the web page of Network Management, log in to Network Management, and in *"Global View"* -> *"Global Configuration"*, the Add Device interface will pop up.

2.Enter the network element name, IP address, subnet mask, Trap name and select the Trap host, click *"Apply"* to complete the creation (display name is to display the name of the network element, Trap name is to set the name of the Trap host), as shown in the figure.



Add NE

Parent Node: OTN

* Display Name: Please input content

* IP Address: Please input content

* Subnet Mask: Please input content

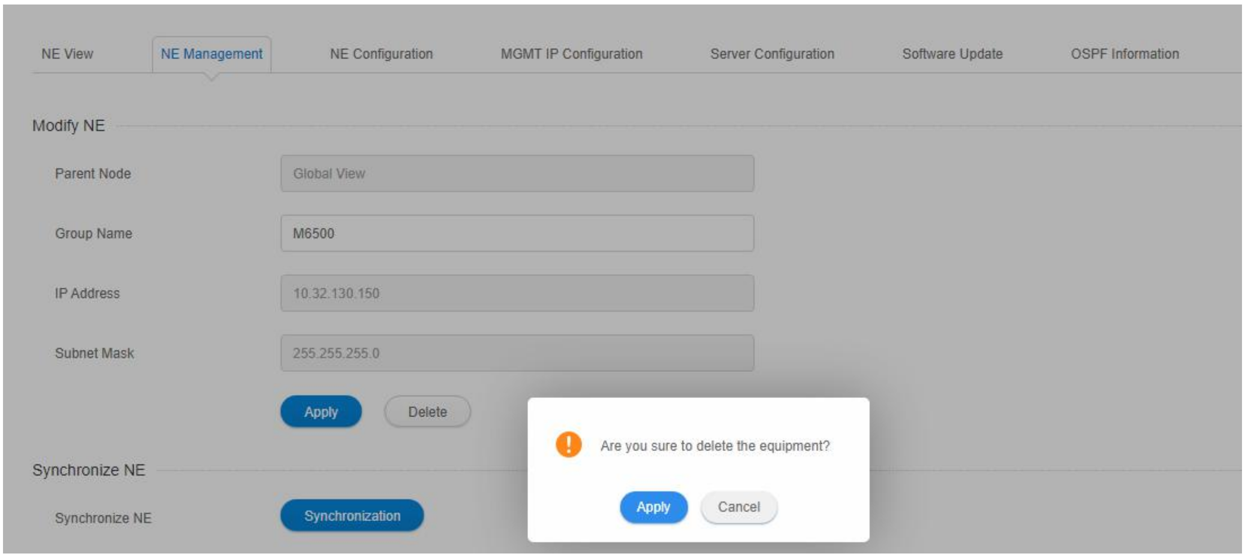
* Trap Name: Please input content

* Trap Host: Please input content

Figure 4-6 NE Management-Add Equipment

3. (Optional) If you want to modify the attributes of an already created element, click on the element you want to modify, select *"NE Management"* on the right navigation bar, and then modify the attributes of the modified element.

4. (Optional) To delete an already created element, select *"Delete"* in the Modify Element field, and click the Apply button in the pop-up box.



Parent Node: Global View

Group Name: M6500

IP Address: 10.32.130.150

Subnet Mask: 255.255.255.0

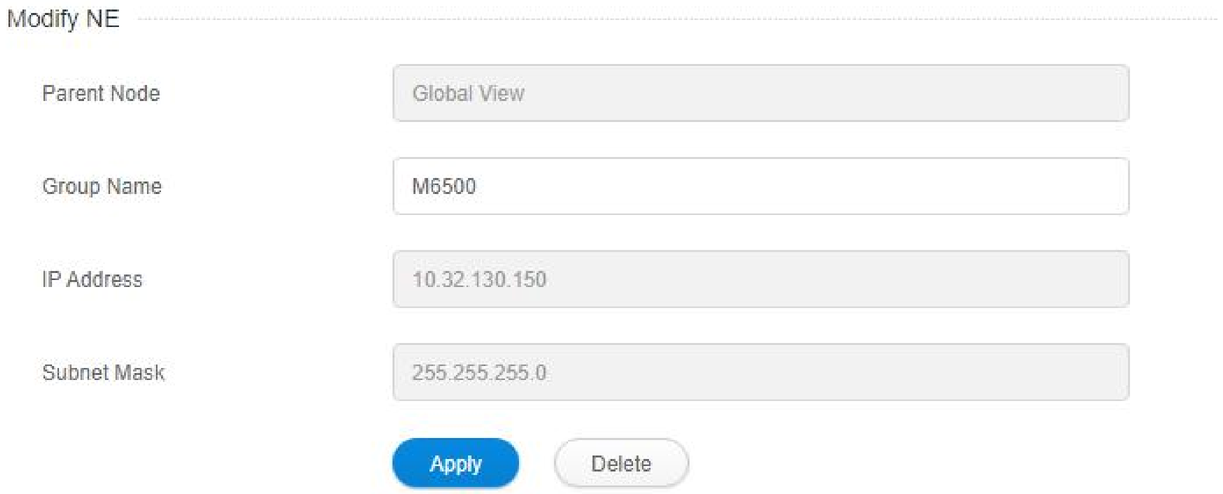
Synchronize NE

Are you sure to delete the equipment?

Figure 4-7 NE Management-NE Nodes

4.1.3. Modify NE

Click the element and select *"NE Management"* to modify the element's description name.



Parent Node: Global View

Group Name: M6500

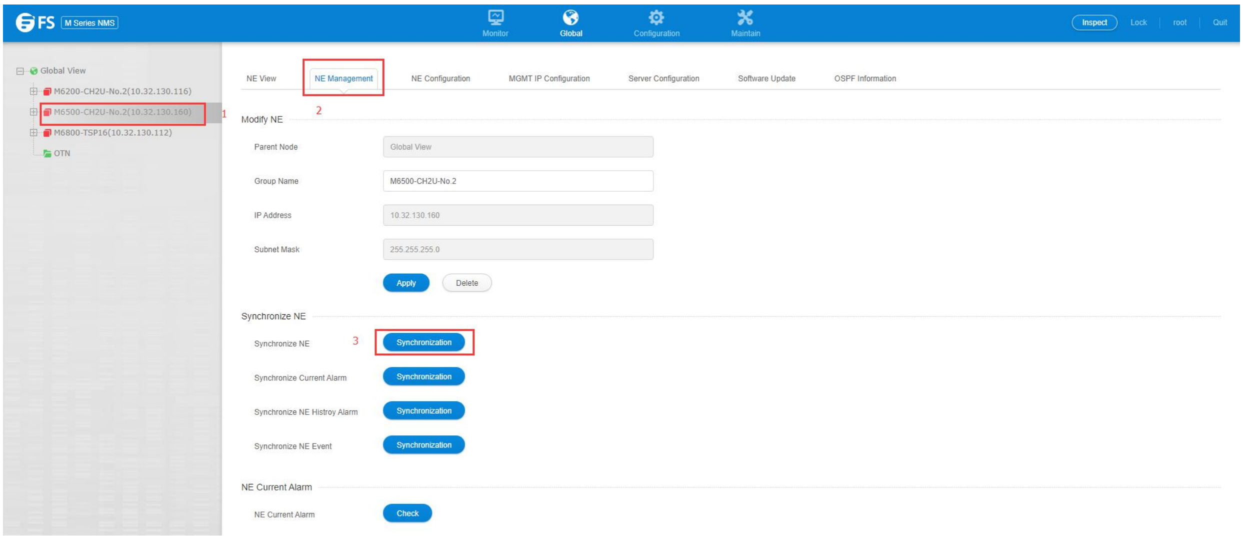
IP Address: 10.32.130.150

Subnet Mask: 255.255.255.0

Figure 4-8 NE Management-Modify NE

4.1.4. Synchronize NE

Click the Element node, select *"NE Management"*, and in the Synchronization Element, click the *"Synchronize NE"* synchronization button to synchronize the status of all network element boards.



Parent Node: Global View

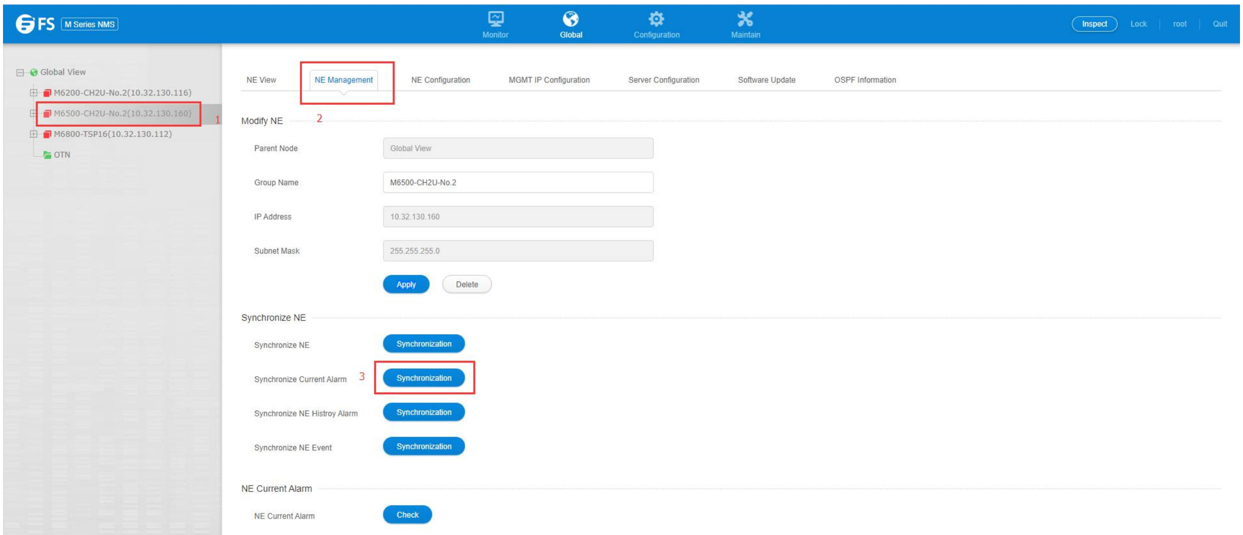
Group Name: M6500-CH2U-No.2

IP Address: 10.32.130.160

Subnet Mask: 255.255.255.0

Figure 4-9 NE Management-Synchronize NE

Click the element node, select *"NE Management"*, and then click the *"Synchronize Current Alarm"* button to synchronize the current alarms of the element.



Parent Node: Global View

Group Name: M6500-CH2U-No.2

IP Address: 10.32.130.160

Subnet Mask: 255.255.255.0

Figure 4-10 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.

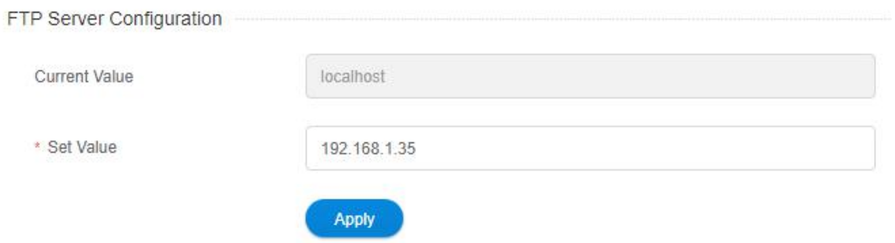
2. There is IP which can be connected with the external network.

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 Nethub, click *"Server Configuration"*-->*"FTP Server Configuration"* on the navigation bar to enter the FTP configuration interface.



FTP Server Configuration

Current Value: localhost

* Set Value: 192.168.1.35

Figure 4-11 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.

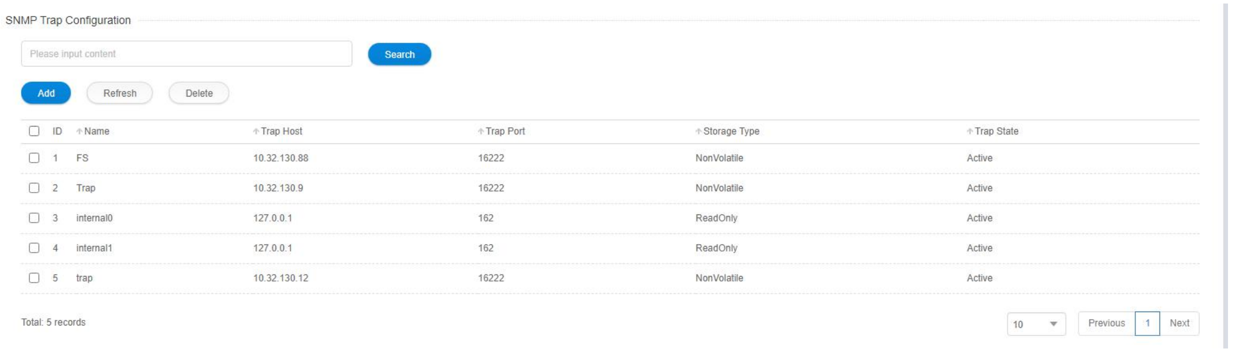
Related Information

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 network element in the left menu, click *"Server Configuration"*-->*"SNMP Trap Configuration"* in the navigation bar.



□	ID	Name	Trap Host	Trap Port	Storage Type	Trap State
□	1	FS	10.32.130.88	16222	NonVolatile	Active
□	2	Trap	10.32.130.9	16222	NonVolatile	Active
□	3	internal0	127.0.0.1	162	ReadOnly	Active
□	4	internal1	127.0.0.1	162	ReadOnly	Active
□	5	trap	10.32.130.12	16222	NonVolatile	Active

Total: 5 records

Figure 4-12 SNMP Configuration

When the user needs to add a new IP address, click the "Add" button to bring up the Add page.

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.

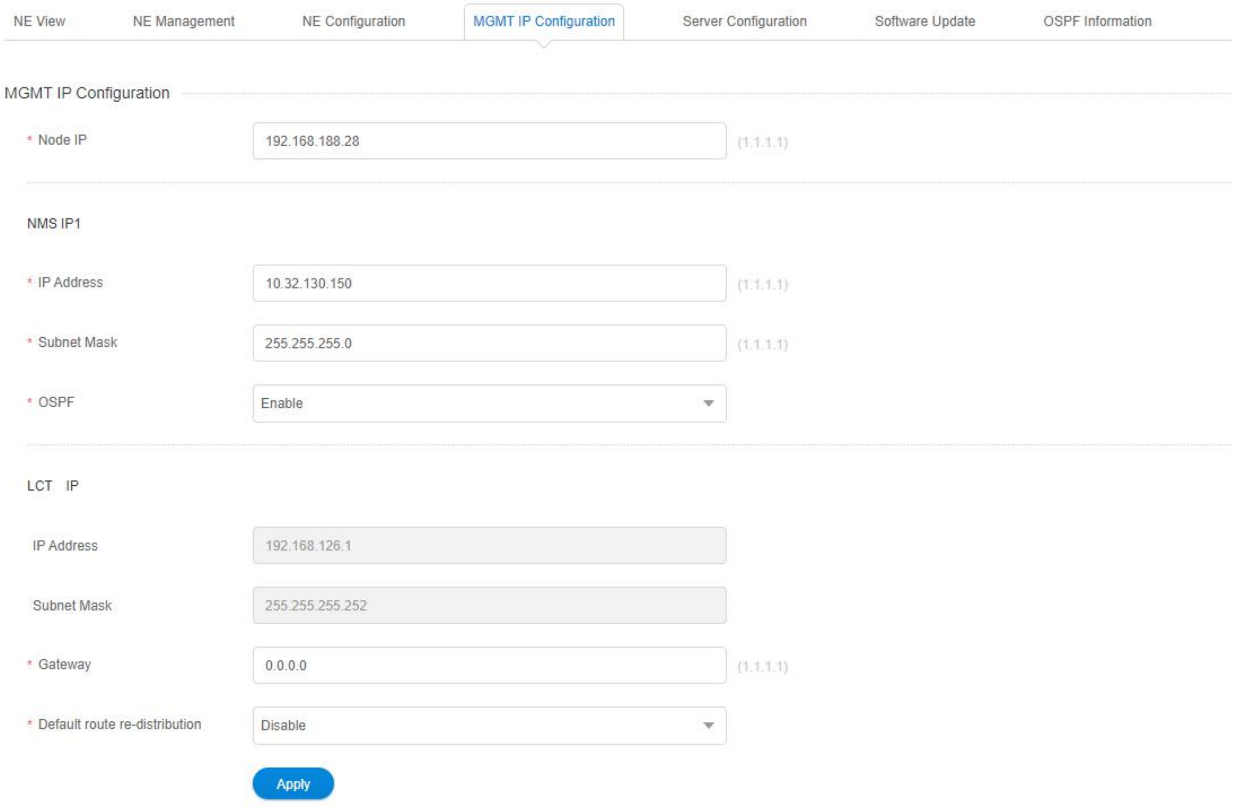
3. The physical configuration has been completed.

Related Information

Configure IP address of the Ethernet port.

Steps

Select the network element in the left menu and click *"MGMT IP Configuration"* in the navigation bar.



MGMT IP Configuration

* Node IP: 192.168.188.28 (1.1.1.1)

NMS IP1

* IP Address: 10.32.130.150 (1.1.1.1)

* Subnet Mask: 255.255.255.0 (1.1.1.1)

* OSPF: Enable

LCT IP

IP Address: 192.168.126.1

Subnet Mask: 255.255.255.252

* Gateway: 0.0.0.0 (1.1.1.1)

* Default route re-distribution: Disable

Figure 4-13 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

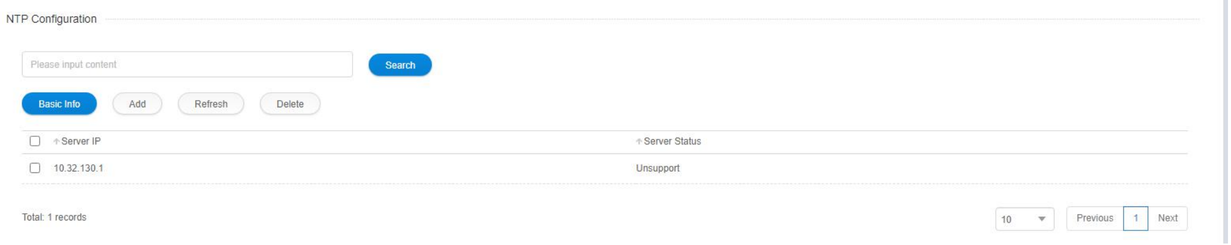
Related Information

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

Steps

Select the network element in the left menu, click the navigation bar *"Server Configuration"* --> *"NTP Configuration"* button to enter the configuration interface.

NTP is divided into "server" and "basic information", the server side can display the current configuration of the NTP server information, the user can click the "Add" button in the toolbar to add a new NTP server.



□ Server IP	Server Status
□ 10.32.130.1	Unsupport

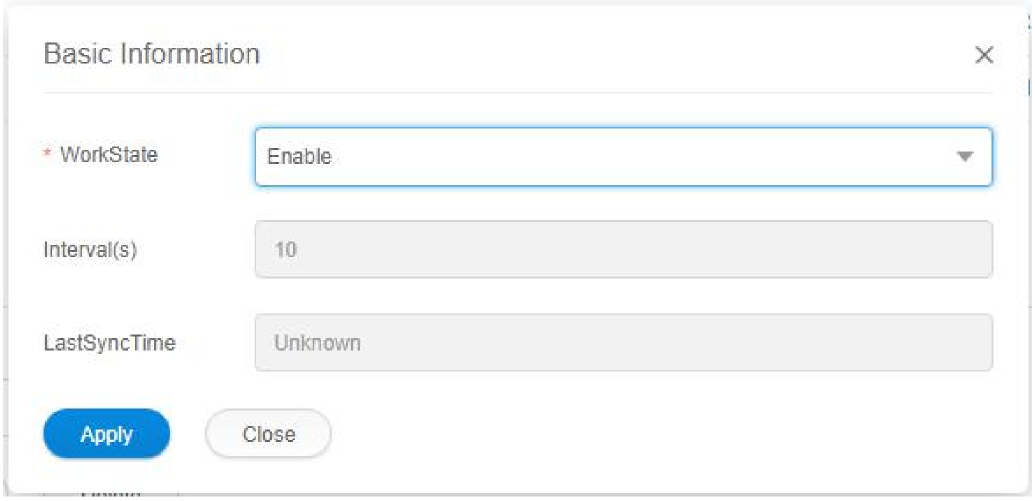
Total: 1 records

Figure 4-14 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.

In the *"Basic Information"* user can choose whether to start the NTP service, the interval time is fixed 10, in seconds.



* WorkState: Enable

Interval(s): 10

LastSyncTime: Unknown

Figure 4-15 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.

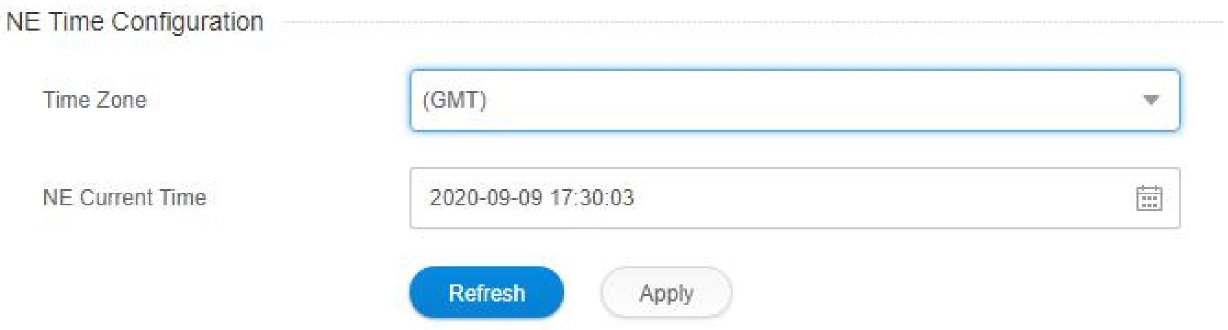
3. Physical configuration has been completed.

Related Information

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

Steps

Select the network element in the left menu, click *"NE Configuration"* --> *"NE Time Configuration"* in the navigation bar.



NE Time Configuration

Time Zone: (GMT)

NE Current Time: 2020-09-09 17:30:03

Figure 4-16 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

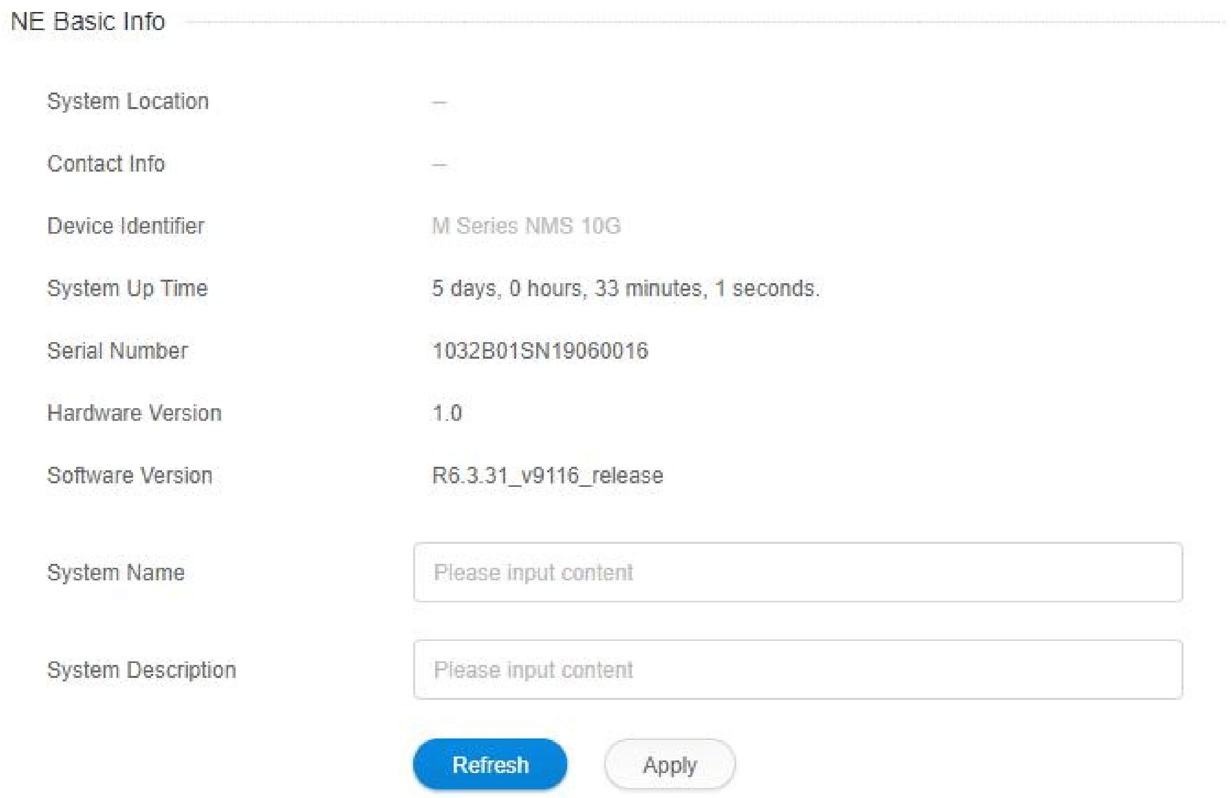
Run the NMS server, login NMS and NE is successfully added.

Related Information

Show NE basic information

Steps

Select Element in the left menu, click *"NE Configuration"*-->*"NE Basic Info"* in the navigation bar. Users can modify the system name and system description.



NE Basic Info

System Location	–
Contact Info	–
Device Identifier	M Series NMS 10G
System Up Time	5 days, 0 hours, 33 minutes, 1 seconds.
Serial Number	1032B01SN19060016
Hardware Version	1.0
Software Version	R6.3.31_v9116_release
System Name	Please input content
System Description	Please input content

Figure 4-17 NE Basic Information

4.6.2. Configuration Data Saving

Prerequisite

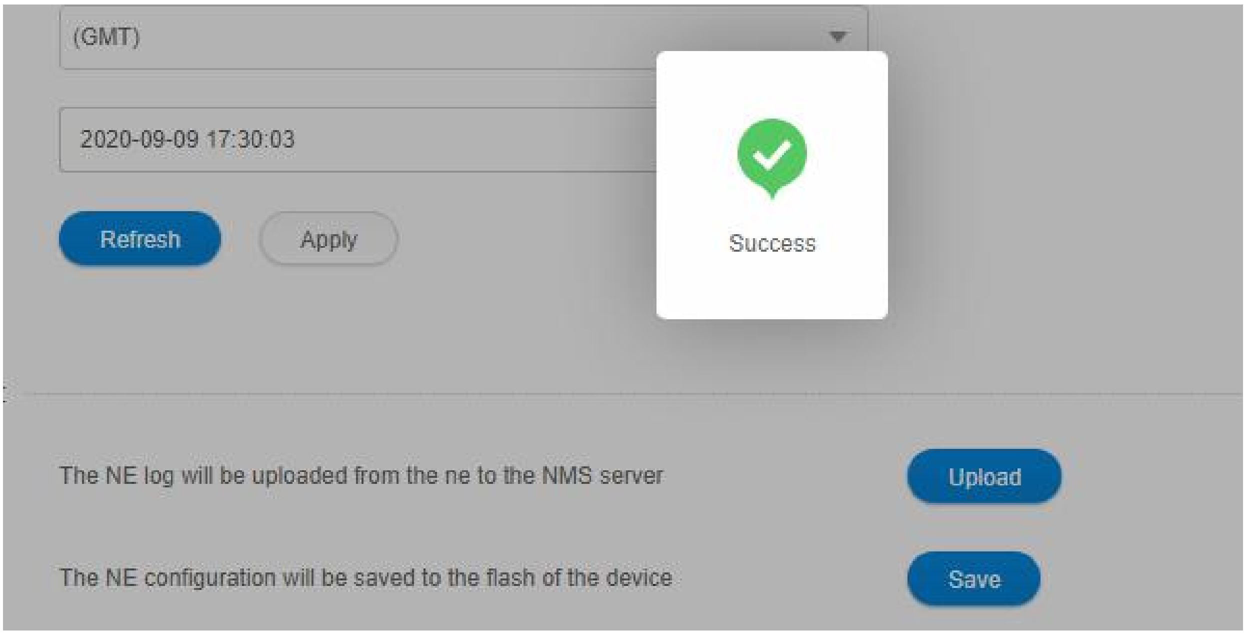
The NMS server has been opened and NMS has been logged in.

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 network element in the left menu, click the navigation bar *"NE Configuration"* --> *"Configuration Data Save"*, click the *"Save"* button and prompt whether the message is successful or not.



(GMT)

2020-09-09 17:30:03

The NE log will be uploaded from the ne to the NMS server

The NE configuration will be saved to the flash of the device

Figure 4-18 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

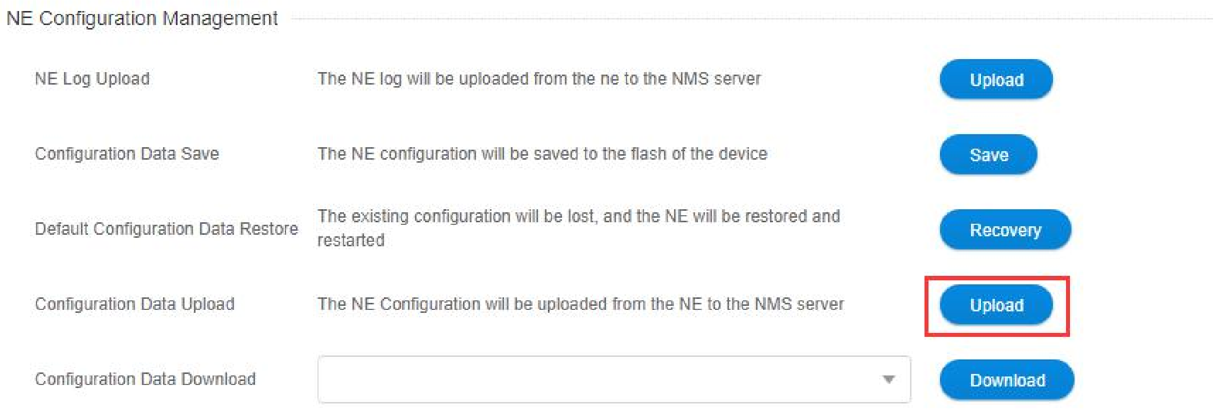
Upload the current NE configuration to the NMS system.

Steps

1, select the network element in the left menu, click the navigation bar *"NE Configuration"* --> *"Configuration Data Upload"*.

2、Click *"Upload"*, enter the file name (32-bit combination of numbers, letters, underscores and underscores "_"), and then you will be prompted for success or failure.

3, the configuration file will be saved in the following directory: server installation root directory NMS --> TFTP --> config.



NE Configuration Management

NE Log Upload	The NE log will be uploaded from the ne to the NMS server	Upload
Configuration Data Save	The NE configuration will be saved to the flash of the device	Save
Default Configuration Data Restore	The existing configuration will be lost, and the NE will be restored and restarted	Recovery
Configuration Data Upload	The NE Configuration will be uploaded from the NE to the NMS server	Upload
Configuration Data Download		Download

Figure 4-19 Configuration Data Upload

4.6.4. Configuration Data Download

Prerequisite

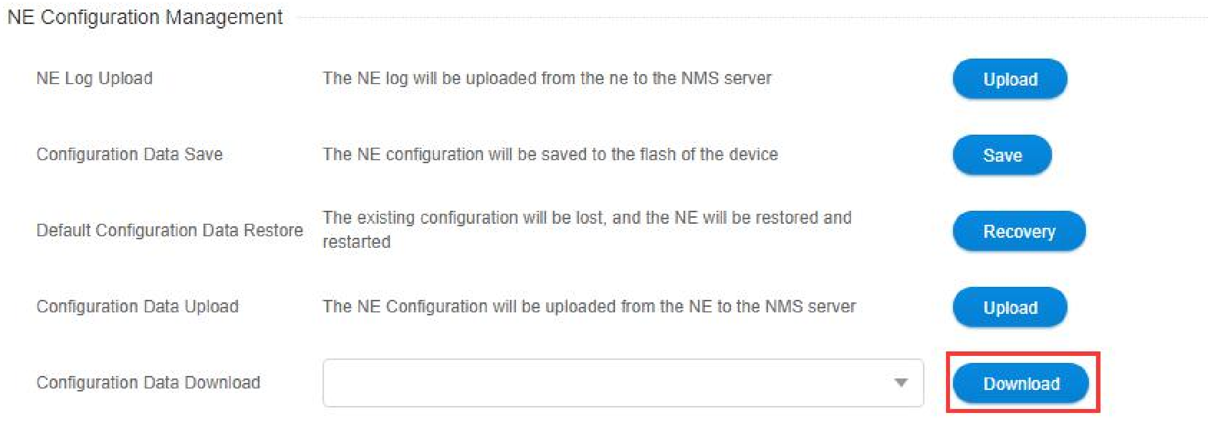
1. Run the NMS server and login NMS.
2. FTP has been successfully configured.

Related Information

Download the current NE configuration to the NMS system.

Steps

Select the network element in the left menu, click *"NE Configuration"* , Select the file you want to download to the network element in the *"Configuration Data Download"* column, if there is no file, the operation cannot be executed. The configuration file should be placed in the NMS-->TFTP-->config folder of the server installation root directory.



NE Configuration Management

NE Log Upload	The NE log will be uploaded from the ne to the NMS server	Upload
Configuration Data Save	The NE configuration will be saved to the flash of the device	Save
Default Configuration Data Restore	The existing configuration will be lost, and the NE will be restored and restarted	Recovery
Configuration Data Upload	The NE Configuration will be uploaded from the NE to the NMS server	Upload
Configuration Data Download		Download

Figure 4-20 Configuration Data Download

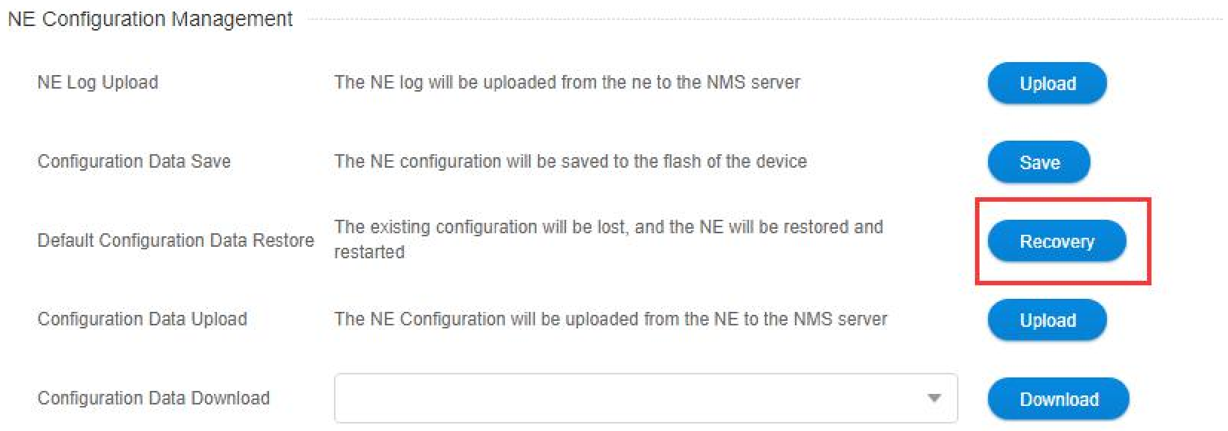
4.6.5. Restore the Default Configuration

Related Information

Restore NE configuration to default configuration.

Steps

Select the network element in the left menu, click *"NE Configuration"* --> *"Default Configuration Data Restore"*., click the "Recovery" button to restore the default configuration.



NE Configuration Management

NE Log Upload	The NE log will be uploaded from the ne to the NMS server	Upload
Configuration Data Save	The NE configuration will be saved to the flash of the device	Save
Default Configuration Data Restore	The existing configuration will be lost, and the NE will be restored and restarted	Recovery
Configuration Data Upload	The NE Configuration will be uploaded from the NE to the NMS server	Upload
Configuration Data Download		Download

Figure 4-21 Default Configuration Data Restore

4.6.6. NE Log Upload

Prerequisite

1. Run the NMS server and login the NMS.

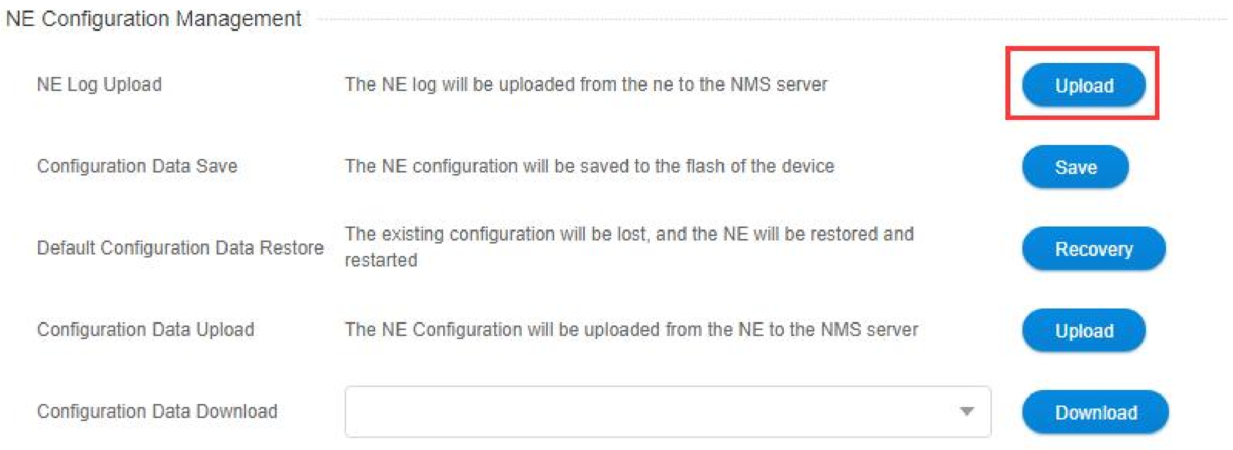
2. FTP has been successfully configured.

Related Information

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

Steps

Select "Element" in the left menu, click *NE Configuration"* --> *"NE Log Upload"*, and enter the file name of the uploaded log (32-bit numbers, letters, underscores and underscores are supported). " consisting of a combination of characters), clicking submit prompts a success or failure message. The configuration file will be saved to the browser's default download location.



NE Configuration Management

NE Log Upload	The NE log will be uploaded from the ne to the NMS server	Upload
Configuration Data Save	The NE configuration will be saved to the flash of the device	Save
Default Configuration Data Restore	The existing configuration will be lost, and the NE will be restored and restarted	Recovery
Configuration Data Upload	The NE Configuration will be uploaded from the NE to the NMS server	Upload
Configuration Data Download		Download

Figure 4-22 NE Log Upload

4.6.7. NE Software Upgrade

Prerequisite

1. Run the NMS server and login NMS.

2. FTP has been successfully configured.

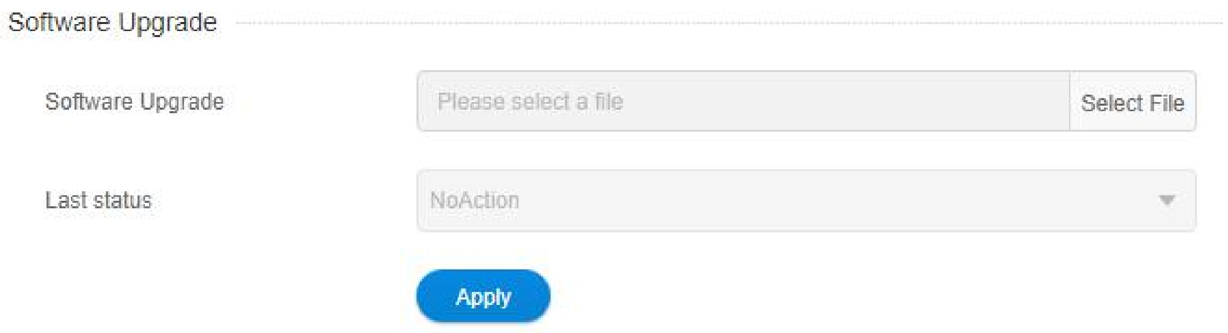
3. The software upgrade file and the MD5 validating file have been successfully imported to the following directory: Server Installation Root NMS→ TFTP → software. The user can modify the upgrade file name and the MD5 validating file name locally. The names of the two files must be consistent (except 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 Netmatics in the left menu, click *"Software Update"* on the navigation bar --> *"Software Upgrade"*, the software upgrade interface will pop up, the user can select the file to be upgraded and click *"Apply"*.



Software Upgrade

Software Upgrade: Please select a file | Select File

Last status: NoAction

Apply

Figure 4-23 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

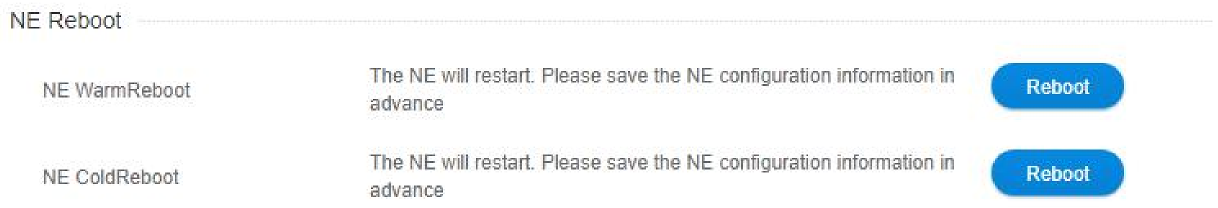
Remote reboot of NE can be realized by the NMS system.

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

Steps

If you select "Element" in the left menu, click *"Software Update"* --> *"NE WarmReboot"* in the navigation bar, a message box will pop up to remind you whether you want to restart, click the "Restart" button to restart.

Select the network element in the left menu, click the *"Software Update"* in the navigation bar --> *"NE ColdReboot"*, the prompt box will pop up whether you want to reboot, click the "Restart" button to restart.



NE Reboot

NE WarmReboot — The NE will restart. Please save the NE configuration information in advance — Reboot

NE ColdReboot — The NE will restart. Please save the NE configuration information in advance — Reboot

Figure 4-24 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 network element in the left menu, click the navigation bar *"software update"* --> *"SC Bsp Upgrade"*, the master card BSP upgrade interface pops up, the user selects the file that can be upgraded, click *"Apply"* to execute the operation.

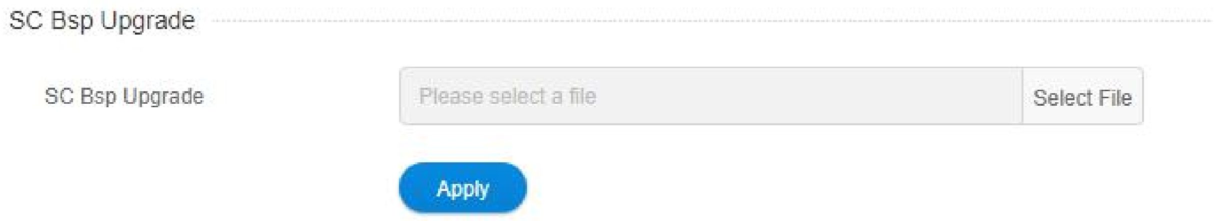


Figure 4-25 BSP Upgrade of NMU Module

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 network element in the left menu, click *"Software Upgrade"* --> "*"LC Bsp Upgrade"*", the interface of Line Card BSP upgrade will pop up, users can select the upgrade file, click *"Apply"* to execute the operation.

The line card BSP upgrade will display all the online line cards in the upgrade interface, you can select multiple line cards to upgrade, or you can select a single line card to upgrade.

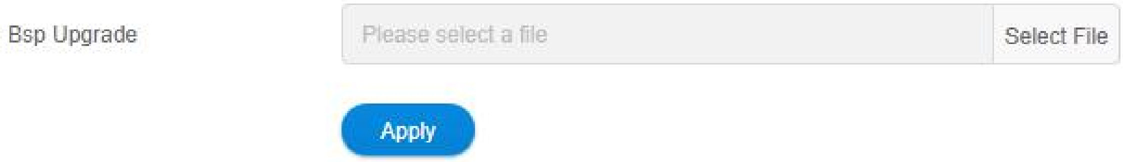


Figure 4-26 BSP Upgrade of LC Module

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

4.6.11.One Touch Inspection

Prerequisite

The network management server is turned on and logged into network management.

Related Information

Aggregate some of the information from all network element devices on the network management into a report.

Steps

Select the network element in the left menu, click *"inspect"* in the top navigation bar, the network management will collect the information and statistics of all network elements, including basic information of network elements, IP configuration, frame and card information, optical module information and alarm information.

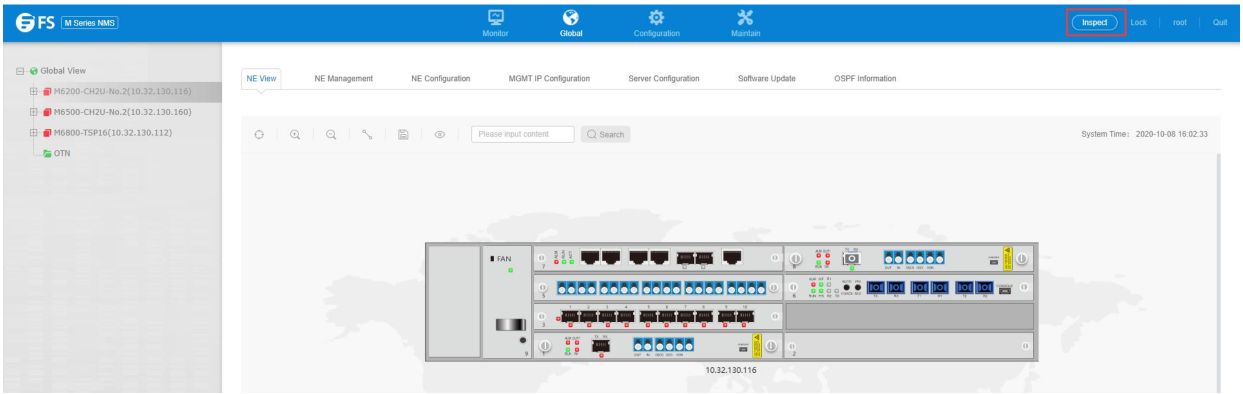
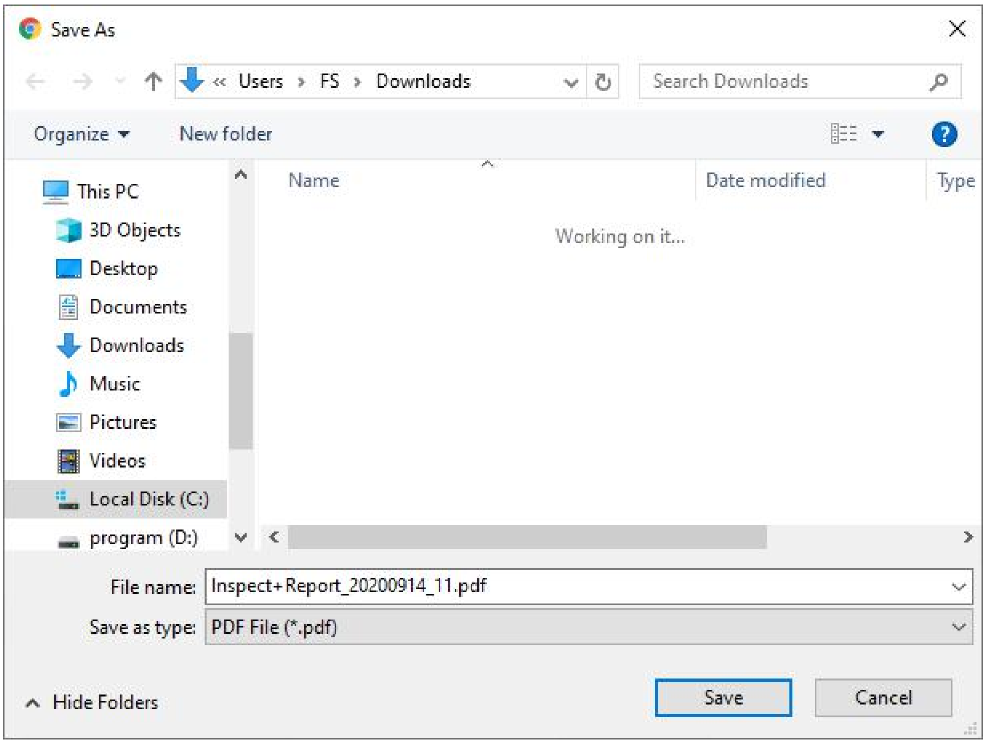


Figure 4-27 One Touch Inspection



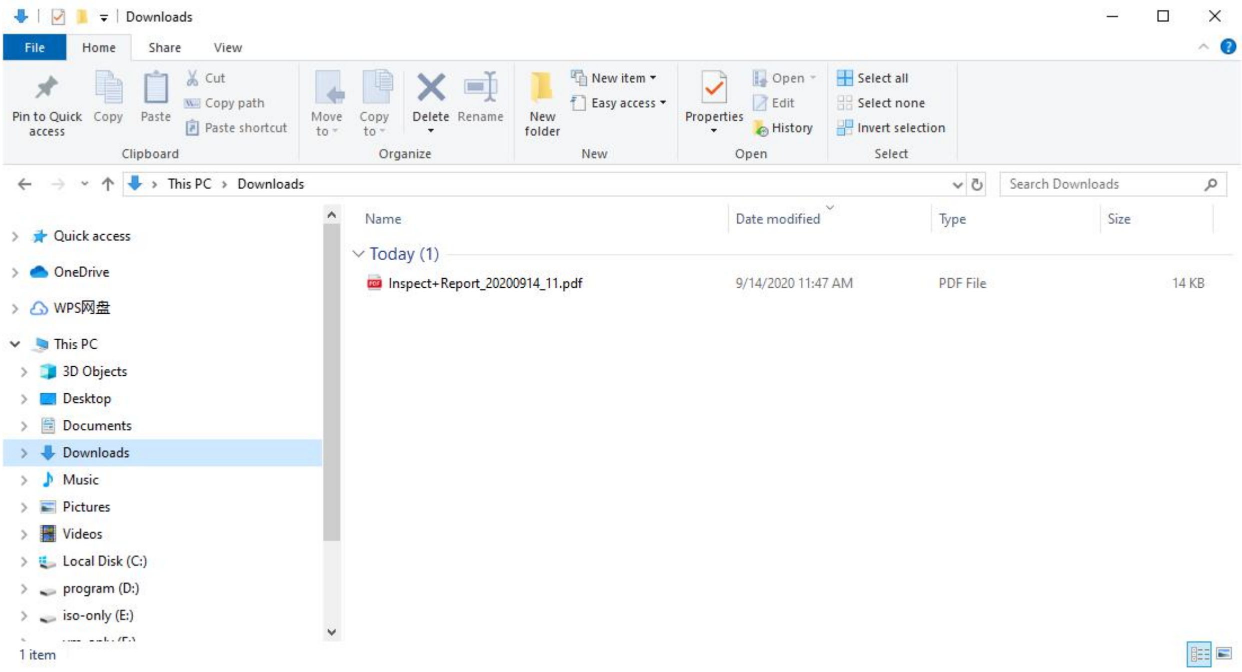
Working on it...

File name: Inspect+Report_20200914_11.pdf

Save as type: PDF File (*.pdf)

Figure 4-28 One-click inspection report generation

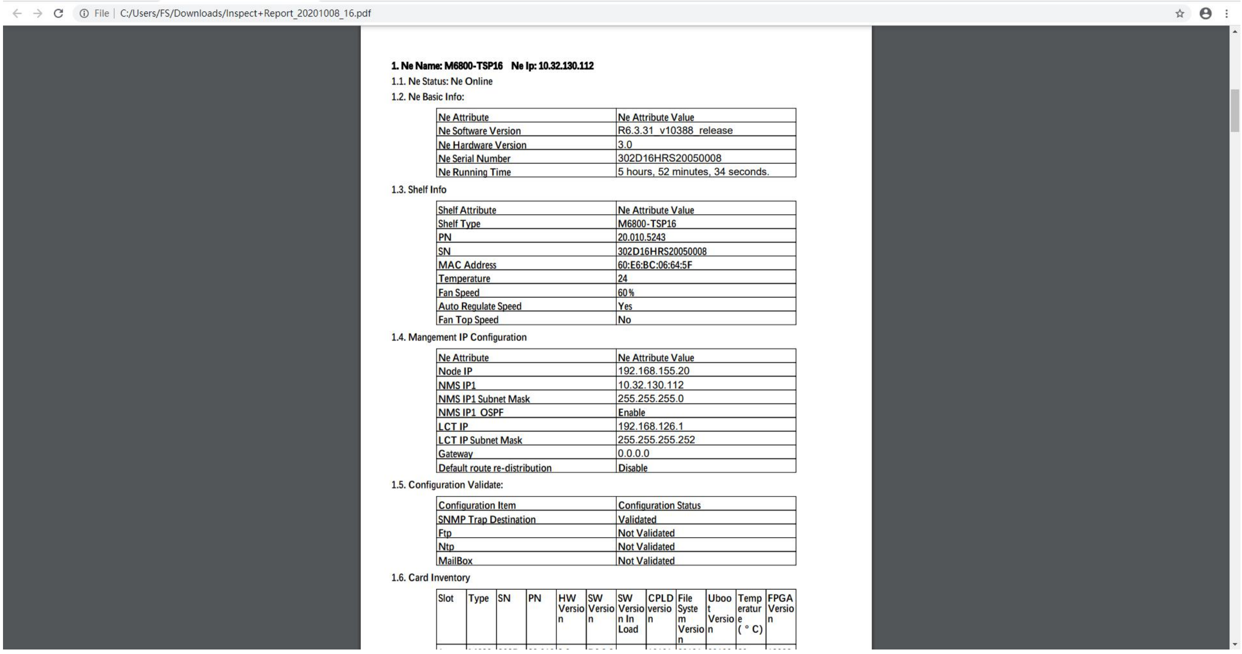
Inspection Report Generator Directory: Custom Directory --> Inspection Reports. As shown in the figure below.



Name	Date modified	Type	Size
Today (1)			
Inspect+Report_20200914_11.pdf	9/14/2020 11:47 AM	PDF File	14 KB

Figure 4-29 Directory of inspection reports

The contents of the inspection report are as follows (in terms of network elements): 1) network element online status; 2) network element basic information; 3) frame information; 4) management IP configuration; 5) configuration checksum; 6) card information; 7) optical module parameters; 8) current alarm list; 9) OLP optical power parameters; 10) OA optical power parameters.



File | C:/Users/FS/Downloads/Inspect+Report_20201008_16.pdf

1. Ne Name: M6800-TSP16 Ne Ip: 10.32.130.112

1.1. Ne Status: Ne Online

1.2. Ne Basic Info:

Ne Attribute	Ne Attribute Value
Ne Software Version	R6.3.31_v10388_release
Ne Hardware Version	3.0
Ne Serial Number	302D16HRS20050008
Ne Running Time	5 hours, 52 minutes, 34 seconds.

1.3. Shelf Info

Shelf Attribute	Ne Attribute Value
Shelf Type	M6800-TSP16
PN	20.010.5243
SN	302D16HRS20050008
MAC Address	60:E6:BC:06:64:5F
Temperature	24
Fan Speed	60%
Auto Regulate Speed	Yes
Fan Top Speed	No

1.4. Mangement IP Configuration

Ne Attribute	Ne Attribute Value
Node IP	192.168.155.20
NMS IP1	10.32.130.112
NMS IP1 Subnet Mask	255.255.255.0
NMS IP1_OSPF	Enable
LCT IP	192.168.126.1
LCT IP Subnet Mask	255.255.255.252
Gateway	0.0.0.0
Default route re-distribution	Disable

1.5. Configuration Validate:

Configuration Item	Configuration Status
SNMP Trap Destination	Validated
Ftp	Not Validated
Ntp	Not Validated
MailBox	Not Validated

1.6. Card Inventory

Slot	Type	SN	PN	HW Version	SW Version	SW Version In Load	CPLD version	File System Version	Uboot Version	Temperature (° C)	FPGA Version

Figure 4-30 Content format of inspection reports

4.6.12. Data storage capacity configuration

Prerequisite

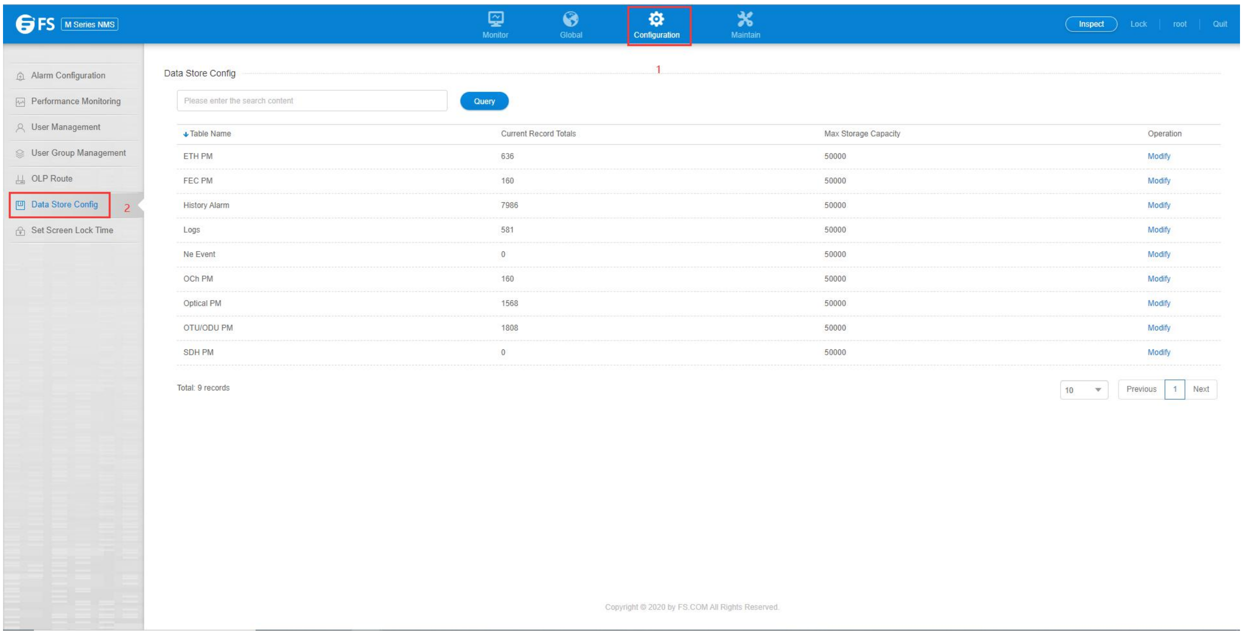
The network management server is turned on and logged into network management.

Related Information

Displays performance statistics, historical alarms, logging, number of network element event data and can configure data storage capacity

Steps

Click *"Configuration"* on the top navigation bar --> *"Data Store Config"*, you can view the current performance statistics, historical alarms, logs and the total number of element events, and can set the capacity limit.



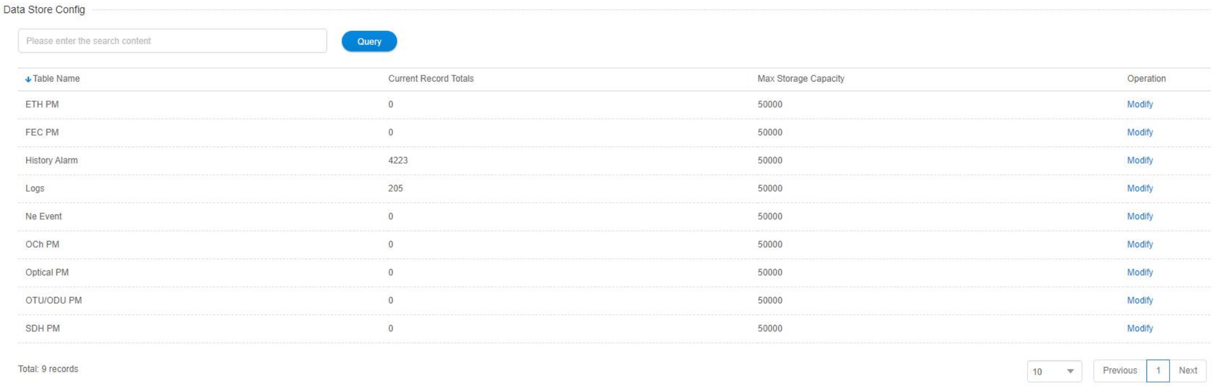
Data Store Config

Please enter the search content   Query

Table Name	Current Record Totals	Max Storage Capacity	Operation
ETH PM	636	50000	Modify
FEC PM	160	50000	Modify
History Alarm	7986	50000	Modify
Logs	581	50000	Modify
Ne Event	0	50000	Modify
OCh PM	160	50000	Modify
Optical PM	1568	50000	Modify
OTU/ODU PM	1808	50000	Modify
SDH PM	0	50000	Modify

Total: 9 records   10   Previous 1 Next

Figure 4-31 Data storage capacity configuration



Data Store Config

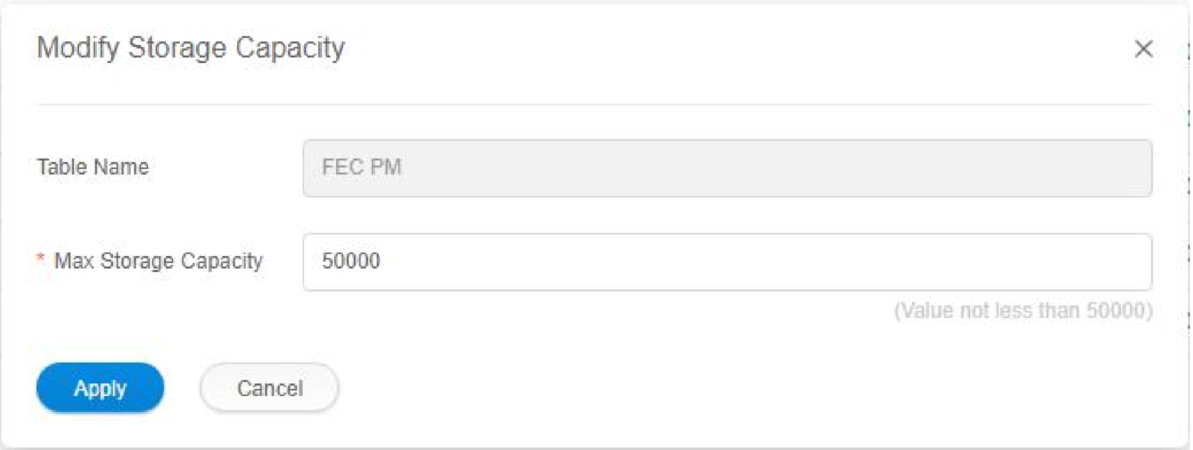
Please enter the search content   Query

Table Name	Current Record Totals	Max Storage Capacity	Operation
ETH PM	0	50000	Modify
FEC PM	0	50000	Modify
History Alarm	4223	50000	Modify
Logs	205	50000	Modify
Ne Event	0	50000	Modify
OCh PM	0	50000	Modify
Optical PM	0	50000	Modify
OTU/ODU PM	0	50000	Modify
SDH PM	0	50000	Modify

Total: 9 records   10   Previous 1 Next

Figure 4-34 Data storage capacity configuration interface

At present, the data storage capacity is limited to: 50,000 < set number < 100,000, when the data storage capacity exceeds the set value, the network administrator will automatically delete the old data of 20% of the capacity limit. For example, if the upper limit is set to 50,000, when the number of stored data exceeds 50,000, 24 hours later, the latest 40,000 data will be kept and the old 10,000 data will be deleted.



Modify Storage Capacity

Table Name: FEC PM

* Max Storage Capacity: 50000

(Value not less than 50000)

Figure 4-35 Data storage capacity limit setting

5. Alarm Management

5.1. Alarm Management Introduction

The alarm management function is a functional group that manages the faults occurring in various network devices managed by the network management system during the operation of the system. The managed faults are commonly known as alarms.

The network management alarm management function of the managed fault contains two types and four levels: equipment alarms and communication alarms of two types; emergency, major, minor, warning four levels.

5.2. Alarm Management Main Interface

After logging in to Network Management, left click *"Maintain"* in the navigation bar - *"Alarm Management"*, the content includes: alarm management (current alarm, historical alarm, network element events). Left click *"Configuration"* - *"Alarm Configuration"*, the content includes: alarm configuration, alarm notification configuration (sound on, alarm sound customization, alarm notification configuration), alarm email server configuration.

Alarm statistics are displayed in the upper right corner of the network management monitoring interface.

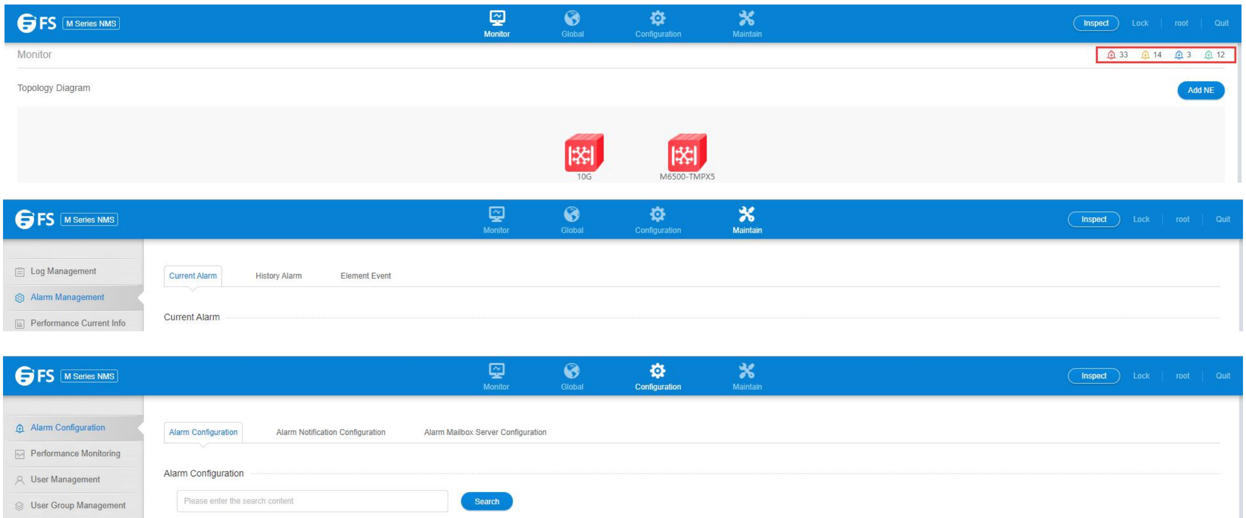
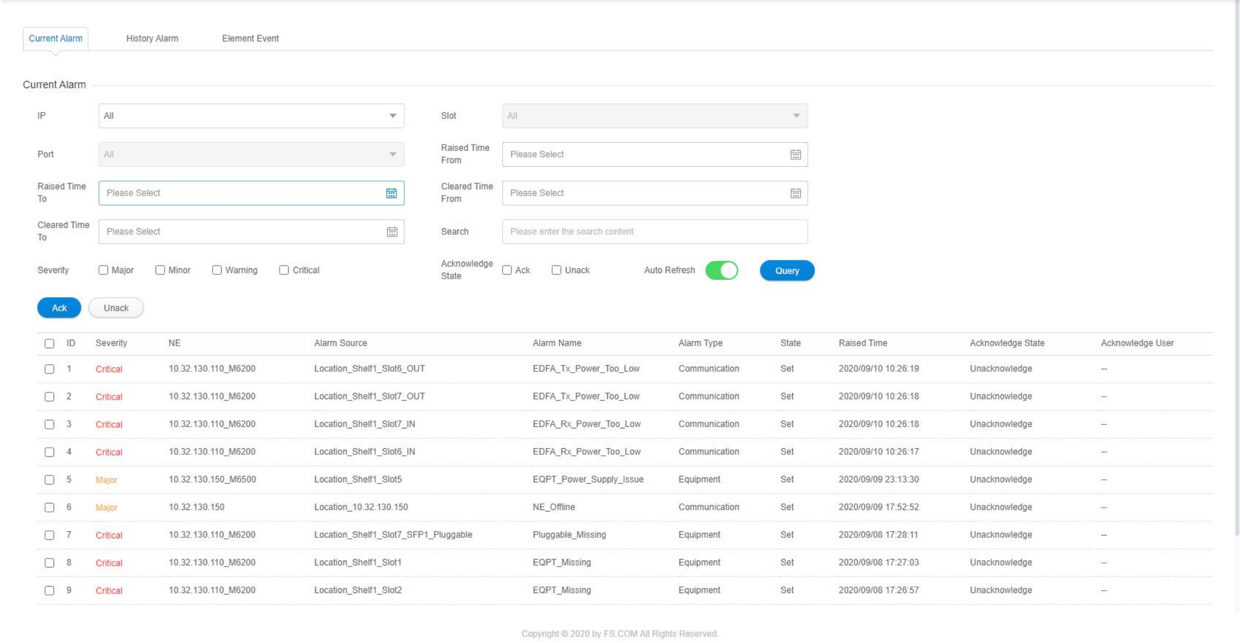


Figure 5-1 Alarm management

5.2.1. Current alarm

Click *"Maintenance"* in the top navigation bar -> *"Alarm Management"* in the left navigation bar -> *"Current Alarm"* in the sub-menu to enter the current alarm page. As shown in the figure.



Current Alarm | History Alarm | Element Event

Current Alarm

IP: All

Slot: All

Port: All

Raised Time From: Please Select

Raised Time To: Please Select

Cleared Time From: Please Select

Cleared Time To: Please Select

Search: Please enter the search content

Severity: □ Major □ Minor □ Warning □ Critical

Acknowledge State: □ Ack □ Unack

Auto Refresh ● Query

Ack Unack

□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
□	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:19	Unacknowledge	--
□	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
□	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
□	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
□	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
□	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
□	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
□	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
□	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--

Copyright © 2020 by FS.COM All Rights Reserved.

Figure 5-2 Current alarm

The area at the bottom right of the table allows you to filter the number of alerts displayed on the current page, and the number of alerts per page can be adjusted to 10, 20, 50 and 100.

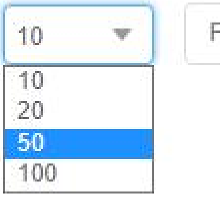
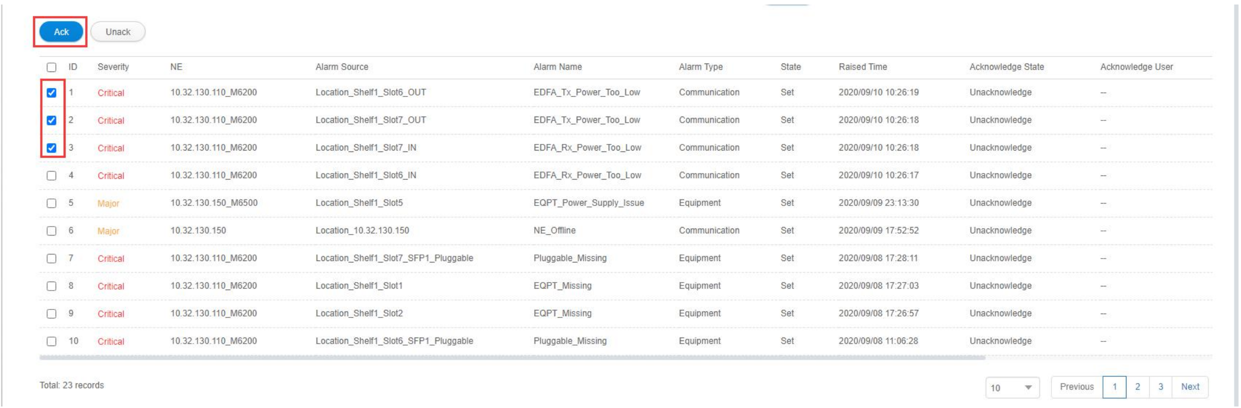


Figure 5-3 Displays the current number of alarms

The middle right area under the navigation bar is *"Ack", "Unack"*， button, which functions as.

The "*Ack"* button is used to confirm the selected alert. By selecting the check box to the left of the selected alert, and clicking the "*Ack"* button, all the selected alerts will be in the status of confirmation. The confirmation status of the alert is *"Acknowledge"*, The *"Ack"* button in the operation bar changes to *"Unack"*. The specific operation is as follows: Select the alarm to be confirmed → Click *"Ack"* button → Click *"Apply"* → Alarm confirmation.

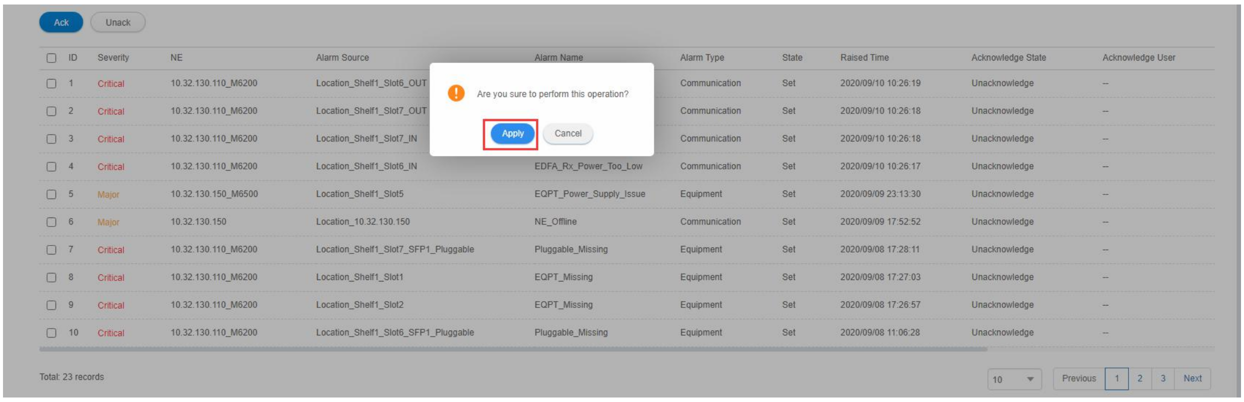
⚠ As the current page will be refreshed once every ten seconds, if the selected alarm is not confirmed in time, the selected state will become unchecked after refreshing.



□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
☑	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:19	Unacknowledge	--
☑	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
☑	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
□	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
□	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
□	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
□	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
□	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
□	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
□	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

Total: 23 records

Figure 5-4 Select to confirm current alerts

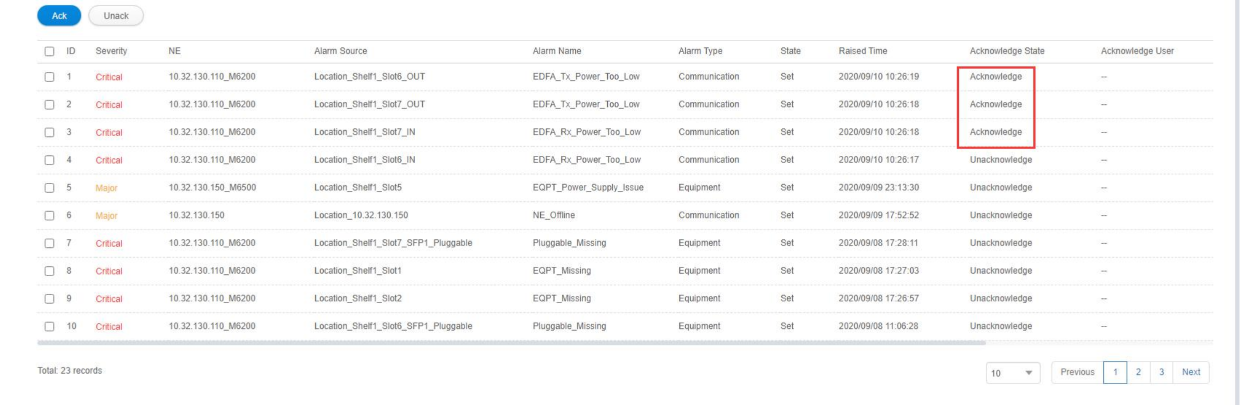


Are you sure to perform this operation?

□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
□	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT		Communication	Set	2020/09/10 10:26:19	Unacknowledge	--
□	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT		Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
□	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN		Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
□	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
□	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
□	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
□	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
□	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
□	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
□	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

Total: 23 records

Figure 5-5 Perform confirmation of current alerts

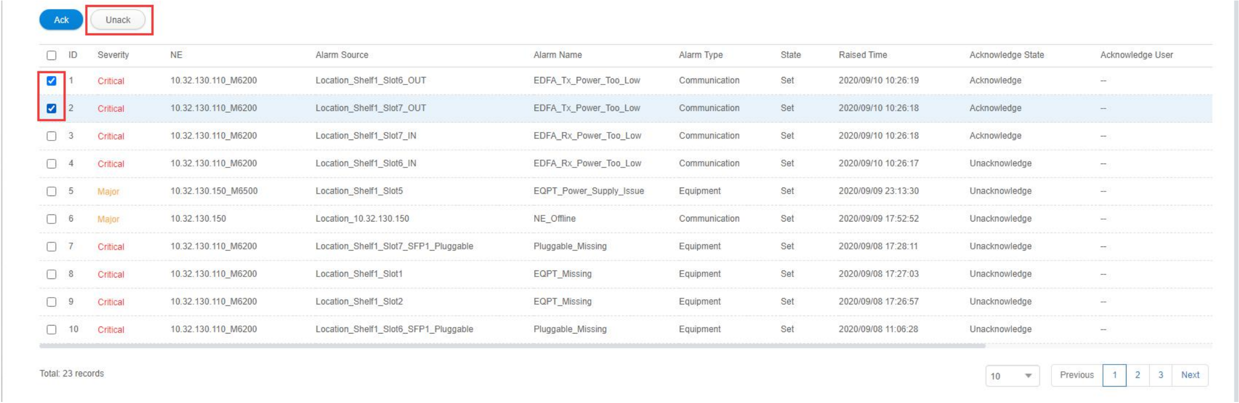


□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
□	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:19	Acknowledge	--
□	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Acknowledge	--
□	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Acknowledge	--
□	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
□	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
□	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
□	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
□	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
□	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
□	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

Total: 23 records

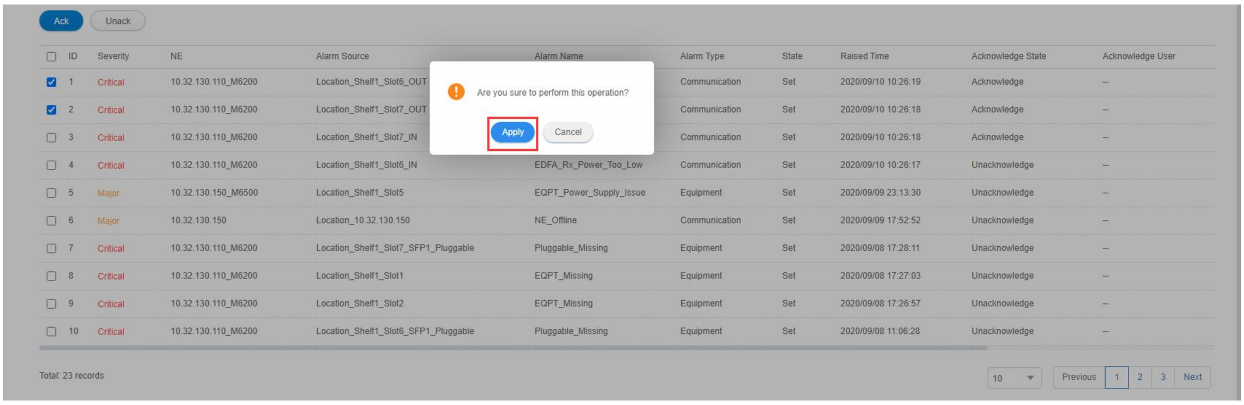
Figure 5-6 Complete current alarm confirmation

⚠ As the current page will be refreshed once every ten seconds, if the selected alarm is not confirmed in time, the selected state will become unchecked after refreshing.



☐	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
☑	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:19	Acknowledge	--
☑	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Acknowledge	--
☐	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Acknowledge	--
☐	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
☐	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
☐	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
☐	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
☐	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
☐	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
☐	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

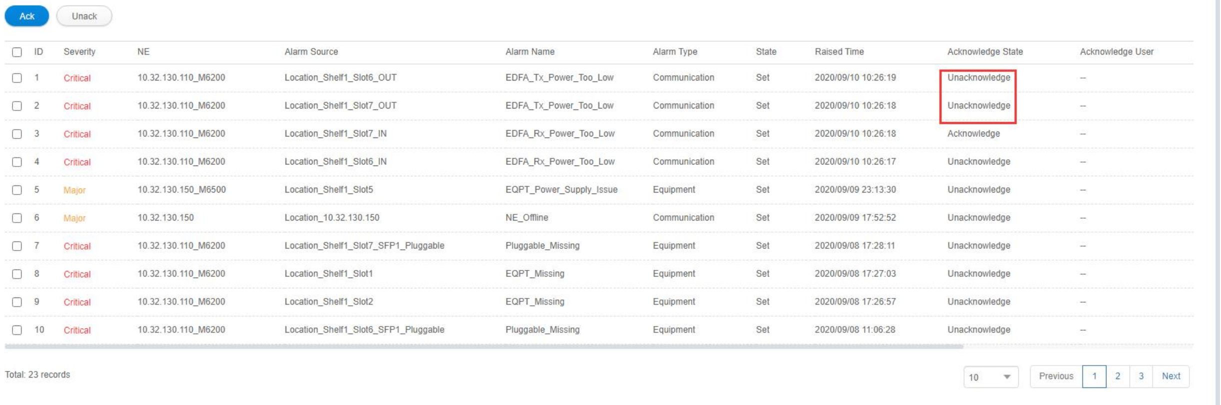
Figure 5-7 Cancel confirmation of current alerts



Are you sure to perform this operation?

☐	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
☑	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT		Communication	Set	2020/09/10 10:26:19	Acknowledge	--
☑	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT		Communication	Set	2020/09/10 10:26:18	Acknowledge	--
☐	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN		Communication	Set	2020/09/10 10:26:18	Acknowledge	--
☐	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
☐	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
☐	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
☐	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
☐	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
☐	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
☐	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

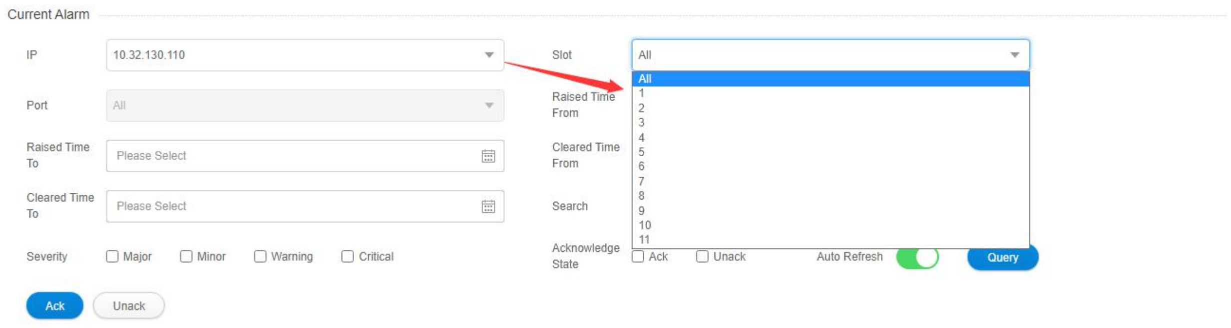
Figure 5-8 Cancel confirmation



☐	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
☐	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:19	Unacknowledge	--
☐	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Unacknowledge	--
☐	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:18	Acknowledge	--
☐	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low	Communication	Set	2020/09/10 10:26:17	Unacknowledge	--
☐	5	Major	10.32.130.150_M6500	Location_Shelf1_Slot5	EQPT_Power_Supply_Issue	Equipment	Set	2020/09/09 23:13:30	Unacknowledge	--
☐	6	Major	10.32.130.150	Location_10.32.130.150	NE_Offline	Communication	Set	2020/09/09 17:52:52	Unacknowledge	--
☐	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
☐	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot1	EQPT_Missing	Equipment	Set	2020/09/08 17:27:03	Unacknowledge	--
☐	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot2	EQPT_Missing	Equipment	Set	2020/09/08 17:26:57	Unacknowledge	--
☐	10	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--

Figure 5-9 Complete current alarm cancellation confirmation

- The *"Query"* button can use known conditions to view and operate the specified alarm, the filtering conditions include: the IP element, the specified IP slot, the specified port under the specified slot, the alarm creation time (i.e., the alarm generation time period), the alarm clear start and stop. The time; the level of the alert; the acknowledgement status of the alert. A single filter can be used alone, or several filters can be combined to filter out the desired alarms. For example, the following figure shows.



Current Alarm

IP: 10.32.130.110

Port: All

Raised Time To: Please Select

Cleared Time To: Please Select

Slot: All

Raised Time From

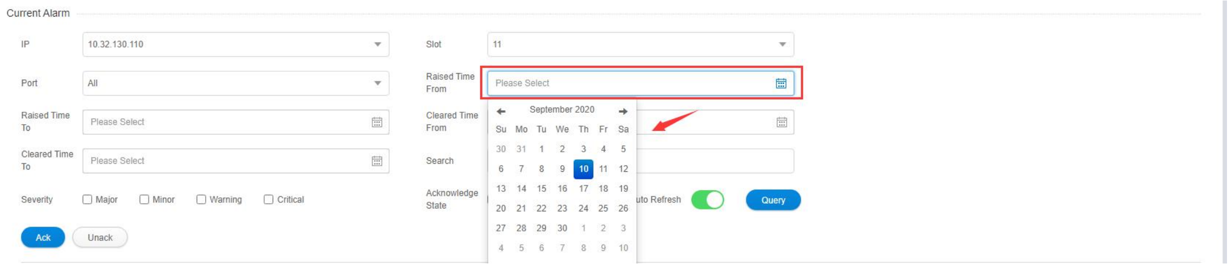
Cleared Time From

Search

Acknowledge State: □ Ack □ Unack

Severity: □ Major □ Minor □ Warning □ Critical

Figure 5-10 IP Filtering Current Alerts



Current Alarm

IP: 10.32.130.110

Port: All

Raised Time To: Please Select

Cleared Time To: Please Select

Slot: 11

Raised Time From: Please Select

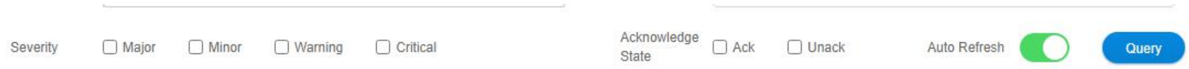
Cleared Time From

Search

Acknowledge State

Severity: □ Major □ Minor □ Warning □ Critical

Figure 5-11 Slotted port filtering current alarms



Severity □ Major □ Minor □ Warning □ Critical

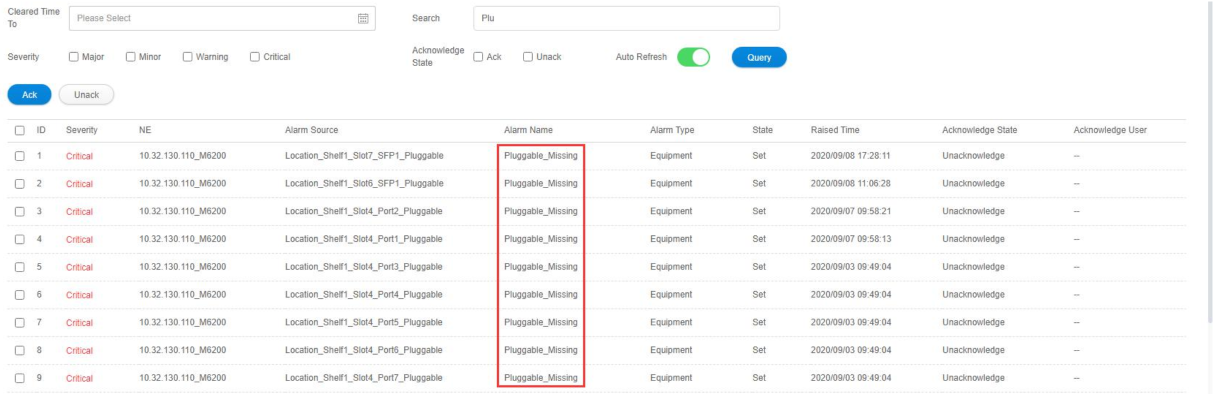
Acknowledge State □ Ack □ Unack

Figure 5-12 Alert level and acknowledgement status filtering of current alerts

⚠ Filter IP, Slot, Port, The way to filter IP, Slot, Port is IP → Slot → Port, or IP → Slot, or IP. select Slot or Port individually is not selectable.

- The "Auto Refresh" button is a left/right moving button (when clicked, it switches from refresh to close or from close to refresh), and the current page is refreshed every 10 seconds when it is in the refresh state, and it is not refreshed when it is in the close state.

The top area of the table is a search function that automatically retrieves all alerts containing the specified content by typing it in, as shown in the following figure.



Cleared Time To: Please Select

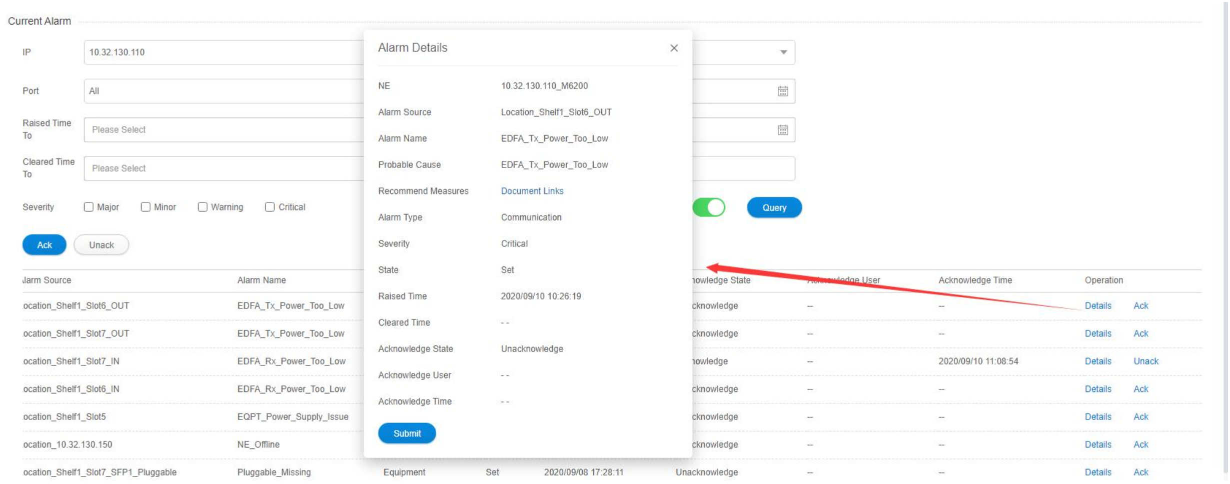
Search: Plu

Severity: □ Major □ Minor □ Warning □ Critical

Acknowledge State: □ Ack □ Unack

□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Acknowledge State	Acknowledge User
□	1	Critical	10.32.130.110_M6200	Location_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--
□	2	Critical	10.32.130.110_M6200	Location_Shelf1_Slot6_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 11:06:28	Unacknowledge	--
□	3	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port2_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/07 09:58:21	Unacknowledge	--
□	4	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/07 09:58:13	Unacknowledge	--
□	5	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port3_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/03 09:49:04	Unacknowledge	--
□	6	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port4_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/03 09:49:04	Unacknowledge	--
□	7	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port5_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/03 09:49:04	Unacknowledge	--
□	8	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port6_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/03 09:49:04	Unacknowledge	--
□	9	Critical	10.32.130.110_M6200	Location_Shelf1_Slot4_Port7_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/03 09:49:04	Unacknowledge	--

Figure 5-13 Search current alerts



Current Alarm

IP: 10.32.130.110

Port: All

Raised Time To: Please Select

Cleared Time To: Please Select

Severity: □ Major □ Minor □ Warning □ Critical

Alarm Details

NE: 10.32.130.110_M6200

Alarm Source: Location_Shelf1_Slot6_OUT

Alarm Name: EDFA_Tx_Power_Too_Low

Probable Cause: EDFA_Tx_Power_Too_Low

Recommend Measures: Document Links

Alarm Type: Communication

Severity: Critical

State: Set

Raised Time: 2020/09/10 10:26:19

Cleared Time: - -

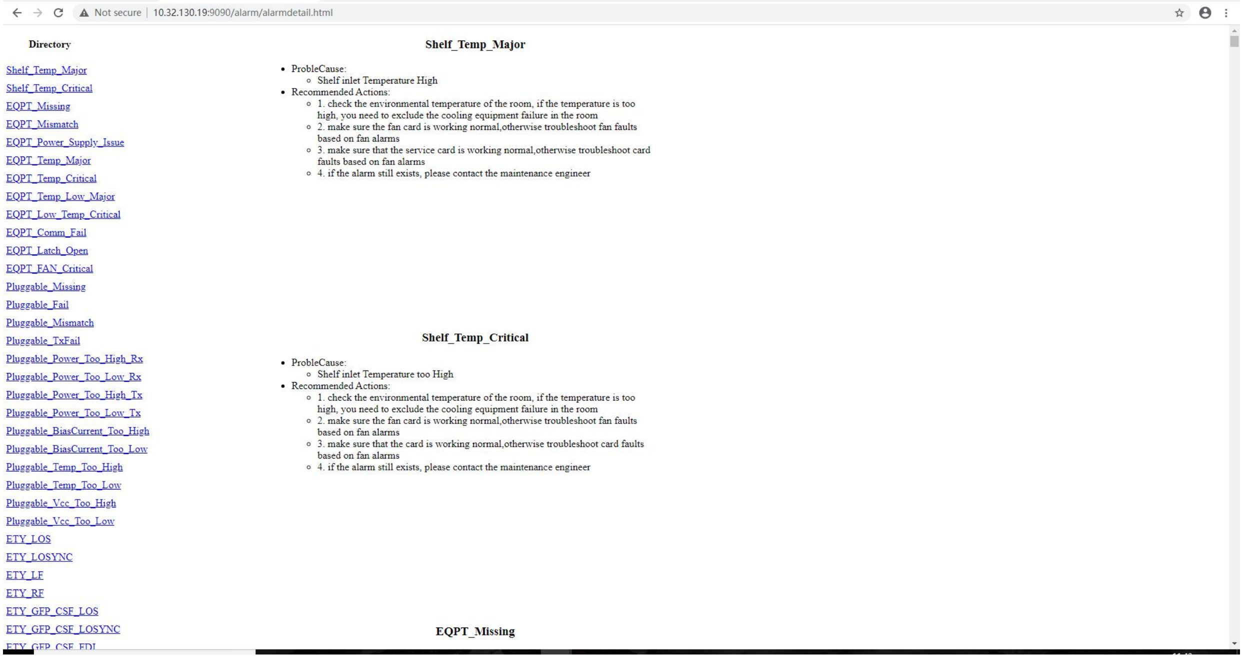
Acknowledge State: Unacknowledge

Acknowledge User: - -

Acknowledge Time: - -

larm Source	Alarm Name				nowledge State	Acknowledge User	Acknowledge Time	Operation
ocation_Shelf1_Slot6_OUT	EDFA_Tx_Power_Too_Low				cknowledge	--	--	Details Ack
ocation_Shelf1_Slot7_OUT	EDFA_Tx_Power_Too_Low				cknowledge	--	--	Details Ack
ocation_Shelf1_Slot7_IN	EDFA_Rx_Power_Too_Low				nowledge	--	2020/09/10 11:08:54	Details Unack
ocation_Shelf1_Slot6_IN	EDFA_Rx_Power_Too_Low				cknowledge	--	--	Details Ack
ocation_Shelf1_Slot5	EQPT_Power_Supply_Issue				cknowledge	--	--	Details Ack
ocation_10.32.130.150	NE_Offline				cknowledge	--	--	Details Ack
ocation_Shelf1_Slot7_SFP1_Pluggable	Pluggable_Missing	Equipment	Set	2020/09/08 17:28:11	Unacknowledge	--	--	Details Ack

Figure 5-14 Details of the warning



Not secure | 10.32.130.19:9090/alarm/alarmdetail.html

Directory

Shelf_Temp_Major
Shelf_Temp_Critical
EQPT_Missing
EQPT_Mismatch
EQPT_Power_Supply_Issue
EQPT_Temp_Major
EQPT_Temp_Critical
EQPT_Temp_Low_Major
EQPT_Low_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
ETY_LOS
ETY_LOSYNC
ETY_LF
ETY_RF
ETY_GFP_CSF_LOS
ETY_GFP_CSF_LOSYNC
ETY_GFP_CSF_FDI

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

EQPT_Missing

http://localhost:9090/alarm/alarmdetail.html

Figure 5-15 Link to warning document

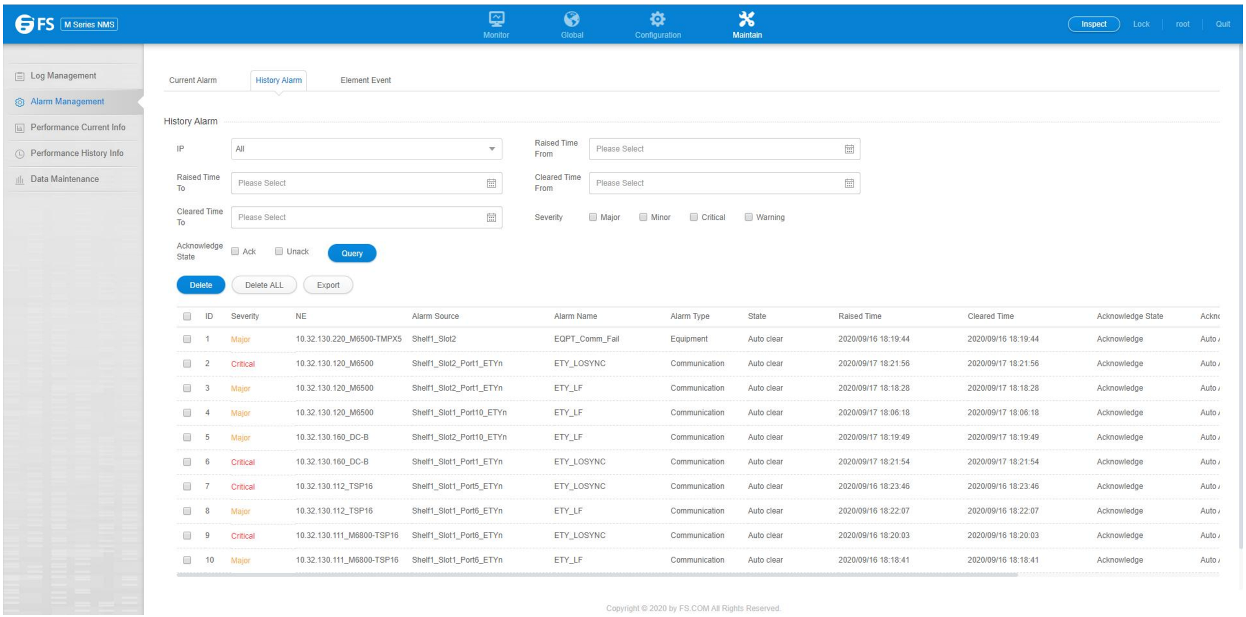
The bottom middle area is the alarm display part of the current alarm, the table header from left to right: check box, serial number, alarm level, network element, alarm source, alarm name, alarm type, status, generate time, clear time, acknowledge status, acknowledge person, acknowledge time, action, details.

- The check boxes are used to check or uncheck specific alarms, or you can use the first check box to select all alarms for the current page.
- The serial number is the target number of the alarm and is incremented starting from 1.
- There are four warning levels, identified by different colors: emergency level (red), primary level (orange), secondary level (blue) and warning level (blue-green).
- A network element is the IP address of the network device generating the alarm.
- The alarm source is information about the specific slot or port of the network element that generated the alarm.

- Alarm name, alarm type, status, generation time, confirmation status, confirmation person, confirmation time content is relatively simple, do not repeat here.
- Details, when clicked, this alert will open a popup window to display the details of the alert. The details include: network element, alarm source, alarm name, alarm reason, recommended action, alarm type, alarm level, status, generation time, clear time, confirmation status, acknowledgement person, and acknowledgement time. The network element, alarm source, alarm name, alarm type, status, generation time, clearing time, confirmation status, confirming person, confirmation time and the contents of the table header are the same, the cause of the alarm refers to the cause of the current alarm, and the recommended measures are links. page, you can see the possible causes of alarms and recommended actions to help engineers troubleshoot problems.
- Confirmation has the same function as "Confirm" and "Cancel" buttons respectively, but the icon buttons in the operation bar are only available for alarms on the line.

5.2.2. Historical alarm

Click *"Maintenance"* in the top navigation bar -> *"Alarm Management"* in the left navigation bar -> *"History Alarm"* in the sub-menu to enter the historical alarm page. As shown in the figure.



History Alarm

IP: All

Raised Time From: Please Select

Raised Time To: Please Select

Cleared Time From: Please Select

Cleared Time To: Please Select

Severity: □ Major □ Minor □ Critical □ Warning

Acknowledge State: □ Ack □ Unack

□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Cleared Time	Acknowledge State	Ackn
□	1	Major	10.32.130.220_M6500-TMPX5	Shelf1_Slot2	EQPT_Comm_Fail	Equipment	Auto clear	2020/09/16 18:19:44	2020/09/16 18:19:44	Acknowledge	Auto
□	2	Critical	10.32.130.120_M6500	Shelf1_Slot2_Port1_ETYn	ETY_LOSYNC	Communication	Auto clear	2020/09/17 18:21:56	2020/09/17 18:21:56	Acknowledge	Auto
□	3	Major	10.32.130.120_M6500	Shelf1_Slot2_Port1_ETYn	ETY_LF	Communication	Auto clear	2020/09/17 18:18:28	2020/09/17 18:18:28	Acknowledge	Auto
□	4	Major	10.32.130.120_M6500	Shelf1_Slot1_Port10_ETYn	ETY_LF	Communication	Auto clear	2020/09/17 18:06:18	2020/09/17 18:06:18	Acknowledge	Auto
□	5	Major	10.32.130.160_DC-B	Shelf1_Slot2_Port10_ETYn	ETY_LF	Communication	Auto clear	2020/09/17 18:19:49	2020/09/17 18:19:49	Acknowledge	Auto
□	6	Critical	10.32.130.160_DC-B	Shelf1_Slot1_Port1_ETYn	ETY_LOSYNC	Communication	Auto clear	2020/09/17 18:21:54	2020/09/17 18:21:54	Acknowledge	Auto
□	7	Critical	10.32.130.112_TSP16	Shelf1_Slot1_Port5_ETYn	ETY_LOSYNC	Communication	Auto clear	2020/09/16 18:23:46	2020/09/16 18:23:46	Acknowledge	Auto
□	8	Major	10.32.130.112_TSP16	Shelf1_Slot1_Port6_ETYn	ETY_LF	Communication	Auto clear	2020/09/16 18:22:07	2020/09/16 18:22:07	Acknowledge	Auto
□	9	Critical	10.32.130.111_M6800-TSP16	Shelf1_Slot1_Port6_ETYn	ETY_LOSYNC	Communication	Auto clear	2020/09/16 18:20:03	2020/09/16 18:20:03	Acknowledge	Auto
□	10	Major	10.32.130.111_M6800-TSP16	Shelf1_Slot1_Port6_ETYn	ETY_LF	Communication	Auto clear	2020/09/16 18:18:41	2020/09/16 18:18:41	Acknowledge	Auto

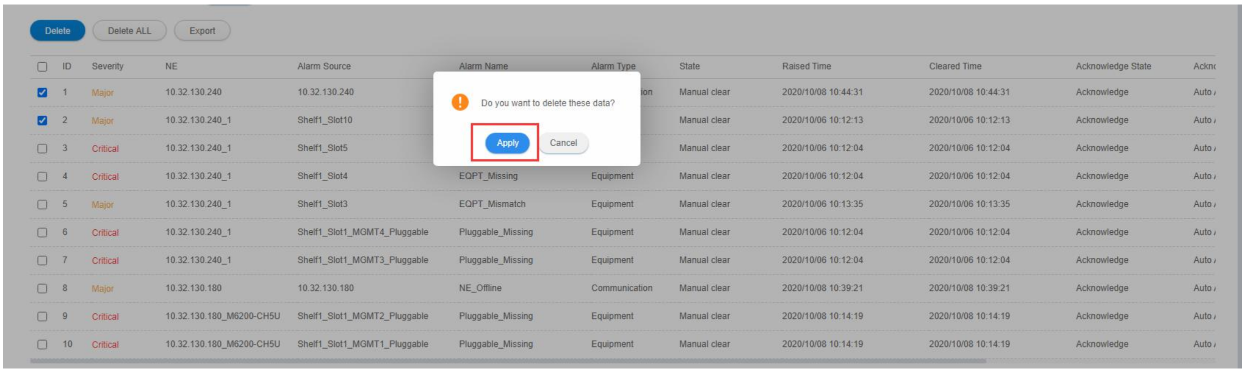
Copyright © 2020 by FS.COM All Rights Reserved.

Figure 5-16 History alarm

The right area under the table can filter the number of alarms displayed on the current page, and the number of alarms per page can be adjusted to 10, 20, 50 and 100.

The area below the navigation bar is for "Search", "Delete", "Delete All" and "Export" buttons.

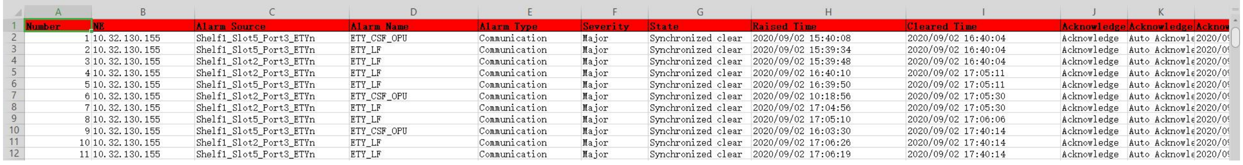
- The *"Query"* button has the same function as the current alarm.
- The *"Delete"* button functions to delete the selected historical alarms, as shown in the following figure.



□	ID	Severity	NE	Alarm Source	Alarm Name	Alarm Type	State	Raised Time	Cleared Time	Acknowledge State	Ackn
☑	1	Major	10.32.130.240	10.32.130.240		ion	Manual clear	2020/10/08 10:44:31	2020/10/08 10:44:31	Acknowledge	Auto
☑	2	Major	10.32.130.240_1	Shelf1_Slot10			Manual clear	2020/10/06 10:12:13	2020/10/06 10:12:13	Acknowledge	Auto
□	3	Critical	10.32.130.240_1	Shelf1_Slot5			Manual clear	2020/10/06 10:12:04	2020/10/06 10:12:04	Acknowledge	Auto
□	4	Critical	10.32.130.240_1	Shelf1_Slot4	EQPT_Missing	Equipment	Manual clear	2020/10/06 10:12:04	2020/10/06 10:12:04	Acknowledge	Auto
□	5	Major	10.32.130.240_1	Shelf1_Slot3	EQPT_Mismatch	Equipment	Manual clear	2020/10/06 10:13:35	2020/10/06 10:13:35	Acknowledge	Auto
□	6	Critical	10.32.130.240_1	Shelf1_Slot1_MGMT4_Pluggable	Pluggable_Missing	Equipment	Manual clear	2020/10/06 10:12:04	2020/10/06 10:12:04	Acknowledge	Auto
□	7	Critical	10.32.130.240_1	Shelf1_Slot1_MGMT3_Pluggable	Pluggable_Missing	Equipment	Manual clear	2020/10/06 10:12:04	2020/10/06 10:12:04	Acknowledge	Auto
□	8	Major	10.32.130.180	10.32.130.180	NE_Offline	Communication	Manual clear	2020/10/08 10:39:21	2020/10/08 10:39:21	Acknowledge	Auto
□	9	Critical	10.32.130.180_M6200-CH5U	Shelf1_Slot1_MGMT2_Pluggable	Pluggable_Missing	Equipment	Manual clear	2020/10/08 10:14:19	2020/10/08 10:14:19	Acknowledge	Auto
□	10	Critical	10.32.130.180_M6200-CH5U	Shelf1_Slot1_MGMT1_Pluggable	Pluggable_Missing	Equipment	Manual clear	2020/10/08 10:14:19	2020/10/08 10:14:19	Acknowledge	Auto

Figure 5-17 Delete historical alerts

- The *"Delete All"* button deletes all history alarms.
- The *"Export"* button is used to export all alarms to a local file: click Export to download the file to a local file with the default name "HistoryAlarm.xlsx".



	A	B	C	D	E	F	G	H	I	J	K	
1	Number	NE	Alarm Source	Alarm Name	Alarm Type	Severity	State	Raised Time	Cleared Time	Acknowledge	Acknowledge	Acknow
2	1	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_CSF_OPU	Communication	Major	Synchronized clear	2020/09/02 15:40:08	2020/09/02 16:40:04	Acknowledge	Auto Acknowle	2020/0
3	2	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 15:39:34	2020/09/02 16:40:04	Acknowledge	Auto Acknowle	2020/0
4	3	10.32.130.155	Shelf1_Slot2_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 15:39:48	2020/09/02 16:40:04	Acknowledge	Auto Acknowle	2020/0
5	4	10.32.130.155	Shelf1_Slot2_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 16:40:10	2020/09/02 17:05:11	Acknowledge	Auto Acknowle	2020/0
6	5	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 16:39:50	2020/09/02 17:05:11	Acknowledge	Auto Acknowle	2020/0
7	6	10.32.130.155	Shelf1_Slot2_Port3_ETYn	ETY_CSF_OPU	Communication	Major	Synchronized clear	2020/09/02 10:18:56	2020/09/02 17:05:30	Acknowledge	Auto Acknowle	2020/0
8	7	10.32.130.155	Shelf1_Slot2_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 17:04:56	2020/09/02 17:05:30	Acknowledge	Auto Acknowle	2020/0
9	8	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 17:05:10	2020/09/02 17:06:06	Acknowledge	Auto Acknowle	2020/0
10	9	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_CSF_OPU	Communication	Major	Synchronized clear	2020/09/02 16:03:30	2020/09/02 17:40:14	Acknowledge	Auto Acknowle	2020/0
11	10	10.32.130.155	Shelf1_Slot2_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 17:06:26	2020/09/02 17:40:14	Acknowledge	Auto Acknowle	2020/0
12	11	10.32.130.155	Shelf1_Slot5_Port3_ETYn	ETY_LF	Communication	Major	Synchronized clear	2020/09/02 17:06:19	2020/09/02 17:40:14	Acknowledge	Auto Acknowle	2020/0

Figure 5-18 Exporting Historical Alerts

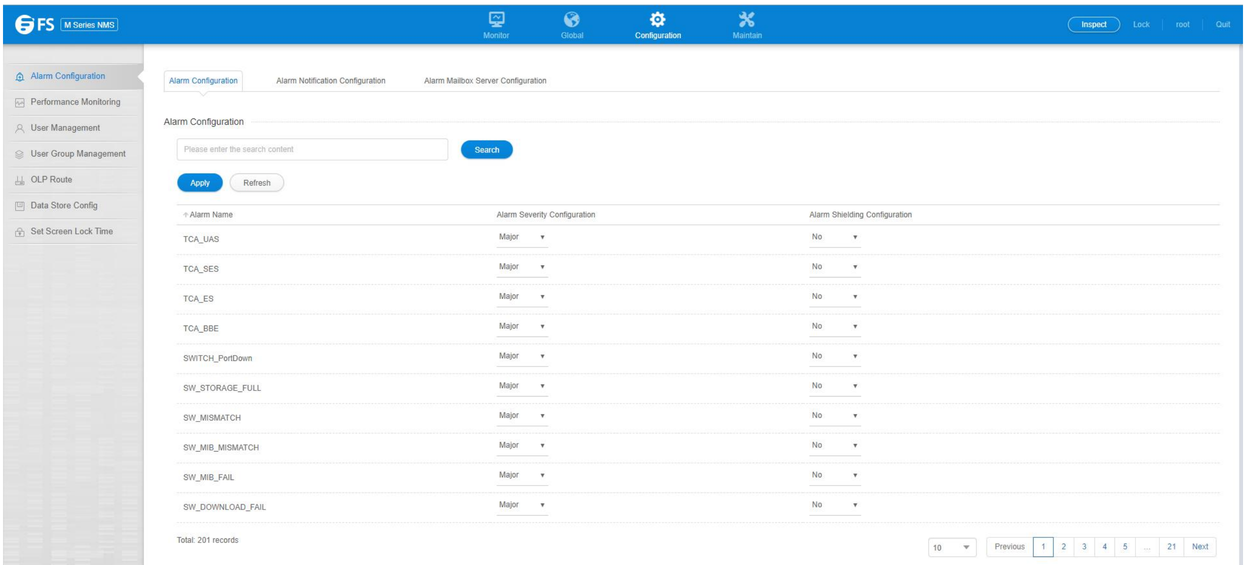
The area below the navigation bar is the alarm display part of the historical alarm, the table header from left to right: Serial Number, NE, Alarm Source, Alarm Name, Alarm Type, Severity, status, Raised Time, Cleared Time, Acknowledge State,Acknowledge User, Acknowledge Time.. (The function is the same as the current alarm, so I won't repeat it)

⚠ There are three alarm clearing states (auto clear, manual clear, and synchronous clear); the acknowledgement state is "acknowledgement" only; there are two types of acknowledgement (auto acknowledgement, acknowledgement by current logged in user, such as root).

5.3. Alarm Configuration

5.3.1. Alarm Configuration

Click *"Configuration"* in the top navigation bar -> *"Alarm Configuration"* in the left navigation bar -> *"Alarm Configuration"* in the sub-menu to enter the alarm configuration page. As shown in the figure.



Alarm Configuration

Alarm Name	Alarm Severity Configuration	Alarm Shielding Configuration
TCA_UAS	Major	No
TCA_SES	Major	No
TCA_ES	Major	No
TCA_BBE	Major	No
SWITCH_PortDown	Major	No
SW_STORAGE_FULL	Major	No
SW_MISMATCH	Major	No
SW_MIB_MISMATCH	Major	No
SW_MIB_FAIL	Major	No
SW_DOWNLOAD_FAIL	Major	No

Total: 201 records

Figure 5-19 Alarm Configuration

The number of alerts displayed on the current page can be filtered in the right-hand area under the Alert Configuration table.

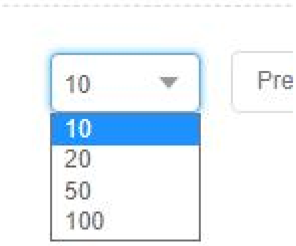
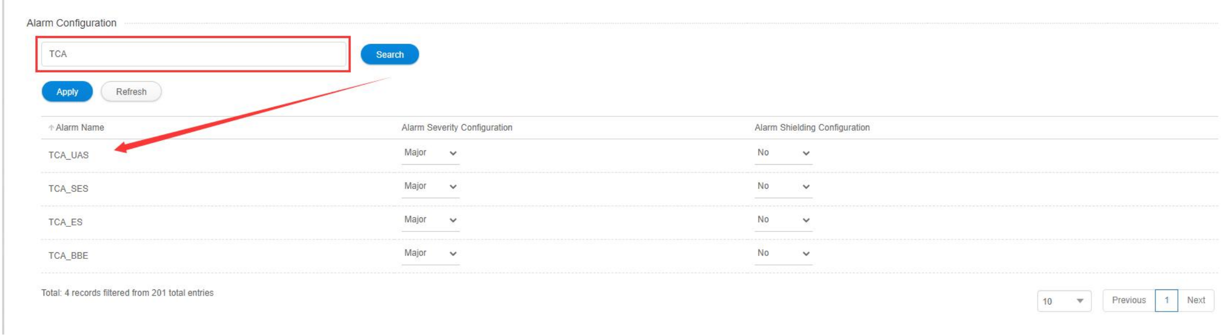


Figure 5-20 Number of alarm configuration displays

The left side of the table is the search function. By typing in the specified content and clicking on the search element, you can get all the alarms containing that content, as shown in the following figure.



Alarm Configuration

Alarm Name	Alarm Severity Configuration	Alarm Shielding Configuration
TCA_UAS	Major	No
TCA_SES	Major	No
TCA_ES	Major	No
TCA_BBE	Major	No

Total: 4 records filtered from 201 total entries

Figure 5-21 Alert Configuration Search

The header of the alarm configuration table data is: alarm name, alarm level configuration, alarm mask configuration.

- Alert name: All alerts on the net meta are under the alert name.
- Alarm level configuration: can set the specified alarm level for the specified alarm, there are emergency, major, minor, warning four kinds of levels can be selected (there is no setting before the default level for the alarm level).

- Alarm shield configuration: the specified alarm can be shielded, after shielding, when the network element produces this alarm will not be displayed on the network management (the default configuration for all alarms are not shielded).

5.3.2. Alarm notification configuration

Click *"Configuration"* in the top navigation bar -> *"Alarm Configuration"* in the left navigation bar -> *"Alarm Notification Configuration"* in the sub-menu, in the Alarm Notification Configuration module. As shown in the figure.

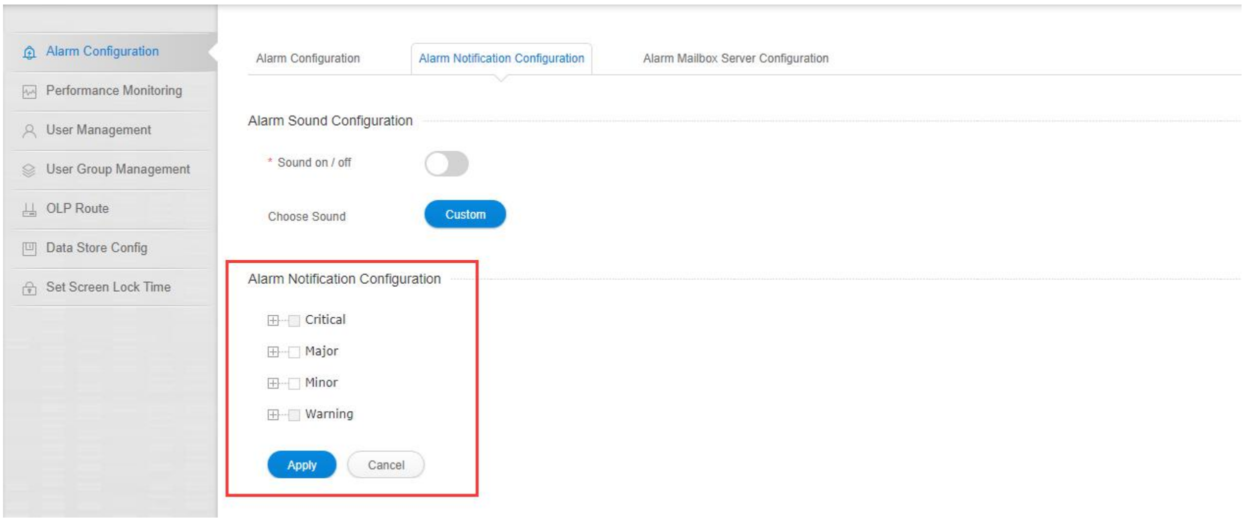


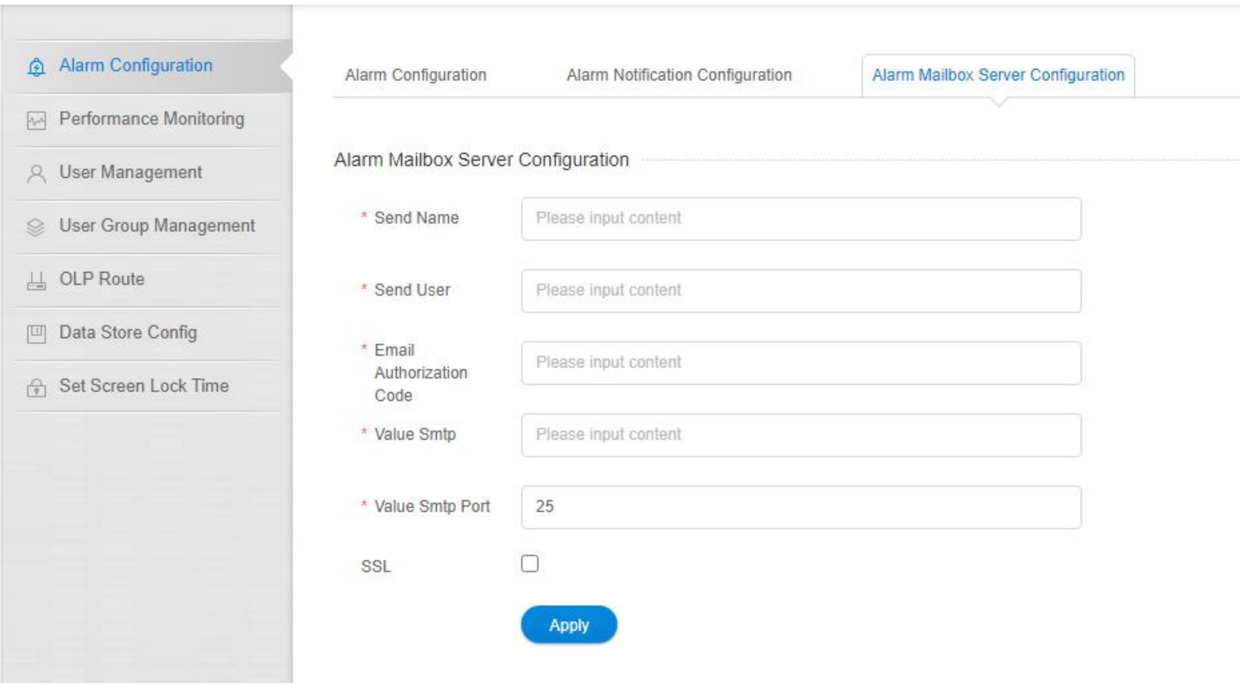
Figure 5-22 Alarm notification configuration

⚠ The alert notification configuration is the alert configuration for alert email notifications, and by default, only urgent alerts are checked (i.e. emails will only receive urgent alert notification messages).

Expand the emergency level alarm tree, all the emergency level alarms are selected by default, you can check or uncheck the specified alarm or all the alarms, only the selected alarm generation and elimination information will be received in the mail system after the application.

5.3.3. Alarm notification configuration

Click *"Configuration"* in the top navigation bar -> *"Alarm Configuration"* in the left navigation bar -> *"Alarm mail server configuration"* in the sub-menu to enter the page of alarm mail server configuration. As shown in the figure.



Alarm Mailbox Server Configuration

* Send Name: Please input content

* Send User: Please input content

* Email Authorization Code: Please input content

* Value Smtp: Please input content

* Value Smtp Port: 25

SSL □

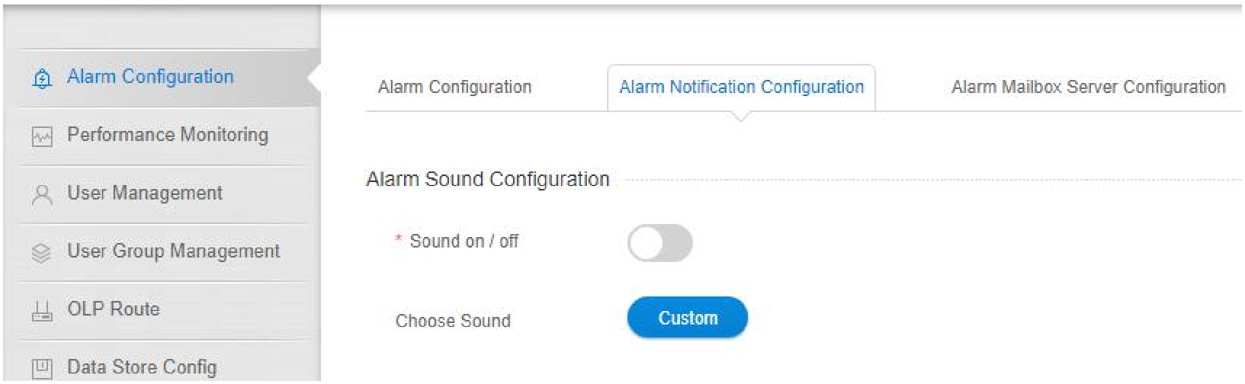
Figure 5-23 Alert Mail Server Configuration

The function of alarm mailbox server configuration is: configure a mailbox as server mailbox, and then change information in navigation bar→Configuration→User management→(Assign user column) and fill in an email address to receive alarm notification. In this way, the alarm generated by the network element (after the configuration in the previous section) will be sent to the mailbox server through the mailbox server to receive the alarm email.

⚠ Different types of mailboxes have different STMP addresses and port numbers, so please check the server mailbox type and SMTP information before setting the server mailbox.

5.3.4. Turn on the alarm sounds

Click *"Configuration"* in the top navigation bar -> *"Alarm Configuration"* in the left navigation bar -> *"Alarm Notification Configuration"* in the sub-menu, in the alarm sound configuration module. As shown in the figure.



Alarm Sound Configuration

* Sound on / off

Choose Sound

Figure 5-24 Alarm sound configuration

Turning on the sound function means that when there is an alarm on the network management, when this function is turned on, the network management server will continue to sound an alarm, indicating that there is an alarm on the network management. At present, the network management only has the function to turn on and off.

⚠ There are four kinds of alarm sound, corresponding to emergency alarm, major alarm, minor alarm and warning alarm, but after the network management open sound only the sound of the highest level alarm; When the alarm level changes alarm sound type also changes (for example, the current alarm level for emergency and major, the prompt for the highest level of emergency alarm sound, if the emergency level alarm disappears, it will be converted to major level alarm sound).

5.3.5. Customize alarm sounds

Alarm sound customization means that customers can set different alarm tones for different types of alarms according to their own needs.

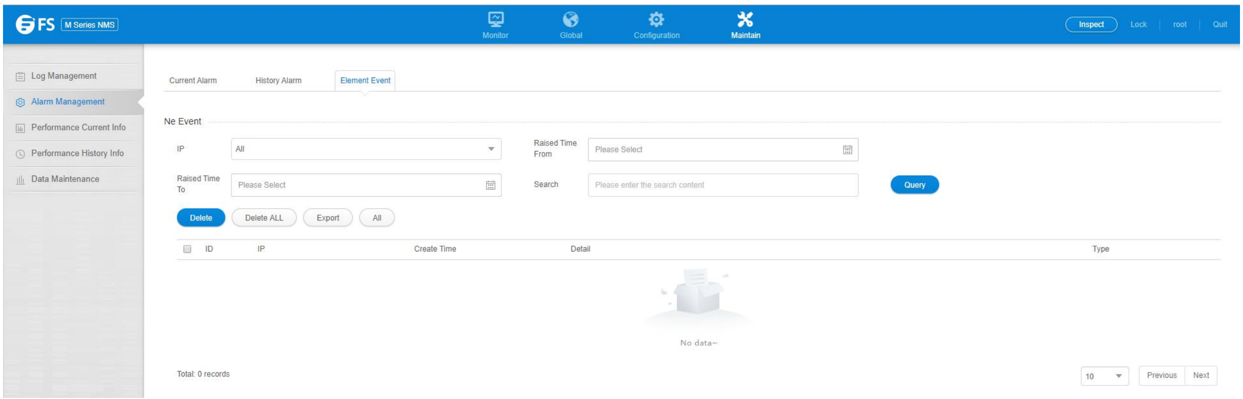
5.4. Element Event

5.4.1. Introduction to Net Element Events

The network element event function is a function that manages the SNC protection inversions that occur in various network devices managed by the network management system during system operation. The managed inversion functions are collectively called events.

5.4.2. Element Event

Click *"Maintenance"* in the top navigation bar -> *"Alarm Management"* in the left navigation bar -> *"Element Events"* in the sub-menu to enter the current element event interface. As shown in the figure.



Ne Event

IP: All

Raised Time From: Please Select

Raised Time To: Please Select

Search: Please enter the search content

☐	ID	IP	Create Time	Detail	Type

No data~

Total: 0 records

10

Figure 5-25 Element Event

The top left area under the navigation bar filters the number of events displayed on the current page, and the number displayed per page can be adjusted to: 10, 20, 50 and 100 (as shown below).

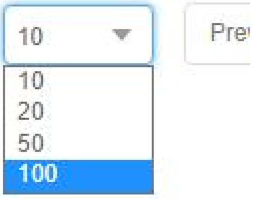
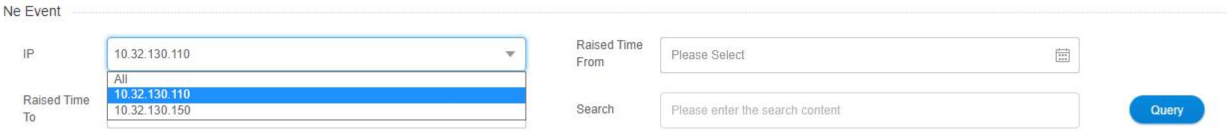


Figure 5-26 Show number of current events

The area under the navigation bar is for "Search", "Delete", "Export", "Delete All" buttons, whose functions are.

- The "Query" button function can be used to view and operate on a specified event using known conditions, including: network element IP, event creation start and end time (i.e., event generation time period); a single filtering condition can be used alone, or several filtering conditions can be used in combination, thus Filter out the required events. For example, the figure below shows.


Ne Event

IP: 10.32.130.110

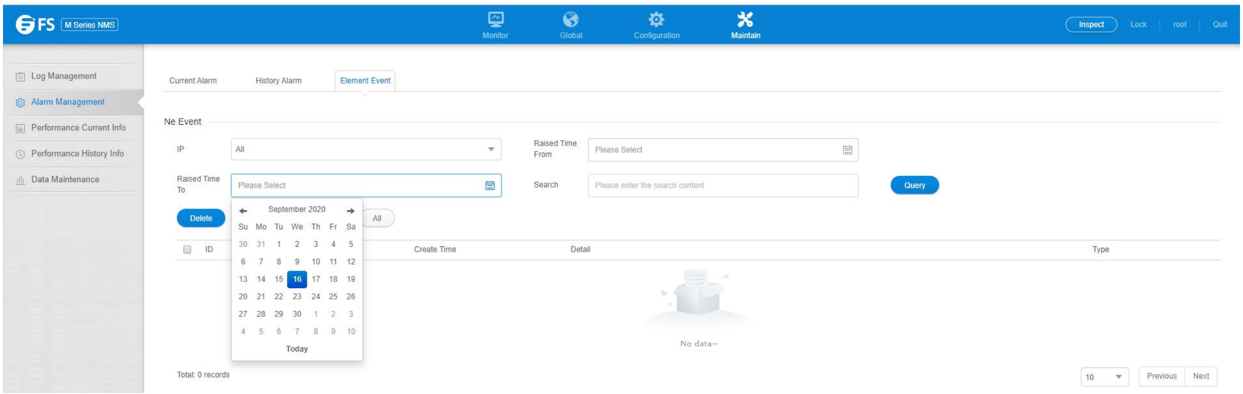
All
10.32.130.110
10.32.130.150

Raised Time From: Please Select

Raised Time To

Search: Please enter the search content

Figure 5-27 IP Query Network Element Event



Ne Event

IP: All

Raised Time From: Please Select

Raised Time To: Please Select

Search: Please enter the search content

September 2020

Su	Mo	Tu	We	Th	Fr	Sa
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

□	ID	Create Time	Detail	Type

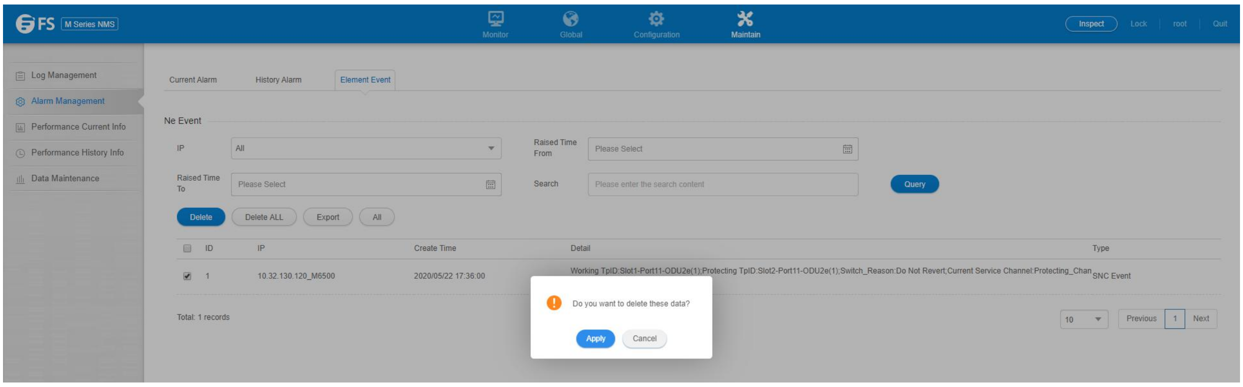
No data~

Total: 0 records

10

Figure 5-28 Create Time Query Net Element Events

- The *"Delete"* button function is to delete the selected element event as shown in the following figure.



Ne Event

IP: All

Raised Time From: Please Select

Raised Time To: Please Select

Search: Please enter the search content

□	ID	IP	Create Time	Detail	Type
☑	1	10.32.130.120_M6500	2020/05/22 17:36:00	Working TplD:Slot1-Port11-ODU2e(1);Protecting TplD:Slot2-Port11-ODU2e(1);Switch_Reason:Do Not Revert;Current Service Channel:Protecting_Chan	SNC Event

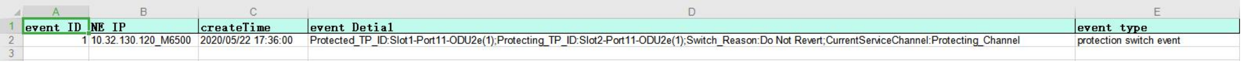
Do you want to delete these data?

Total: 1 records

10 1

Figure 5-29 Deleting a Net Element Event

- The *"Export"* button is used to export all element events: click Export to download the file to a local file with the default name "NEevents.xlsx".

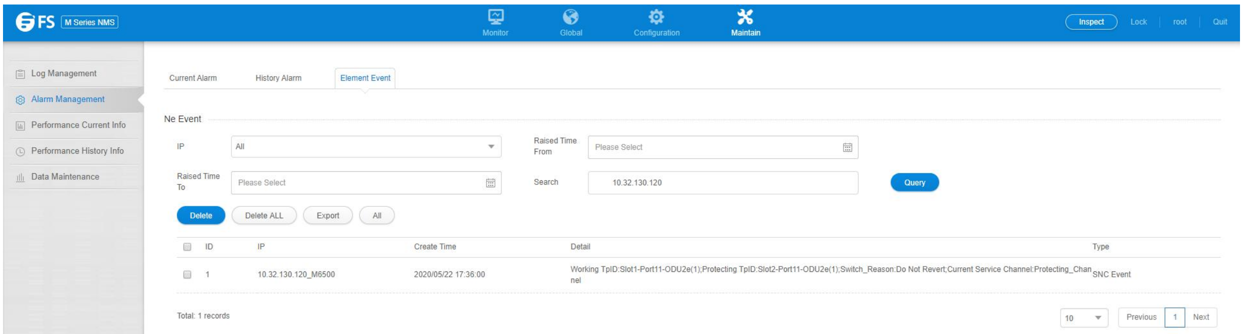


	A	B	C	D	E
1	event ID	NE IP	createTime	event Detial	event type
2	1	10.32.130.120_M6500	2020/05/22 17:36:00	Protected_TP_ID:Slot1-Port11-ODU2e(1);Protecting_TP_ID:Slot2-Port11-ODU2e(1);Switch_Reason:Do Not Revert;CurrentServiceChannel:Protecting_Channel	protection switch event
3					

Figure 5-30 Exporting Net Elements Events

- The "Delete All" button is used to delete all the element events.

The upper right area under the navigation bar is the search function: you can get all the events that contain the content by entering the specified content, as shown in the following figure.



Ne Event

IP: All

Raised Time From: Please Select

Raised Time To: Please Select

Search: 10.32.130.120

☐	ID	IP	Create Time	Detail	Type
☐	1	10.32.130.120_M6500	2020/05/22 17:36:00	Working TpID:Slot1-Port11-ODU2e(1);Protecting TpID:Slot2-Port11-ODU2e(1);Switch_Reason:Do Not Revert;Current Service Channel:Protecting_Channel	SNC Event

Total: 1 records

10 · 1

Figure 5-31 Searching for a net meta event

In the middle of the lower part of the table is the element event display section, with the following headers from left to right: check box, ID, IP, generation time, details, and element event type.

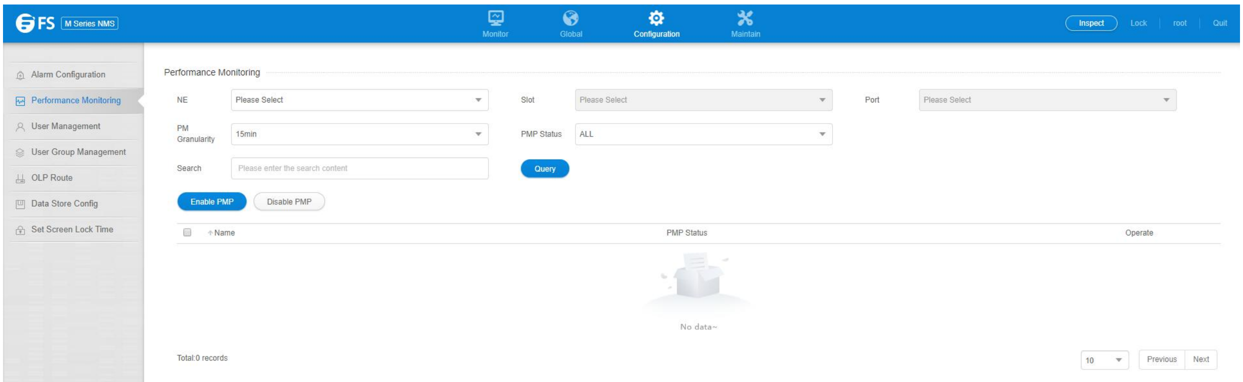
- The checkbox is used to check or uncheck the specified event, or you can use the first checkbox to select the current page event in full.
- ID is the event's numeric target number, increasing sequentially from 1.
- IP is the IP of the network device that generated the event.
- The details are Show Working TP ID, Protect TP ID, Reverse Cause, and Current Service Channel.
- The generation time and the network element time type are not described here.

6. Performance Management

The first step in performance management is to go to the performance monitoring point management interface and open the performance monitoring point that you want to monitor.

6.1. Performance Management Introduction

6.1.1. filter box



Performance Monitoring

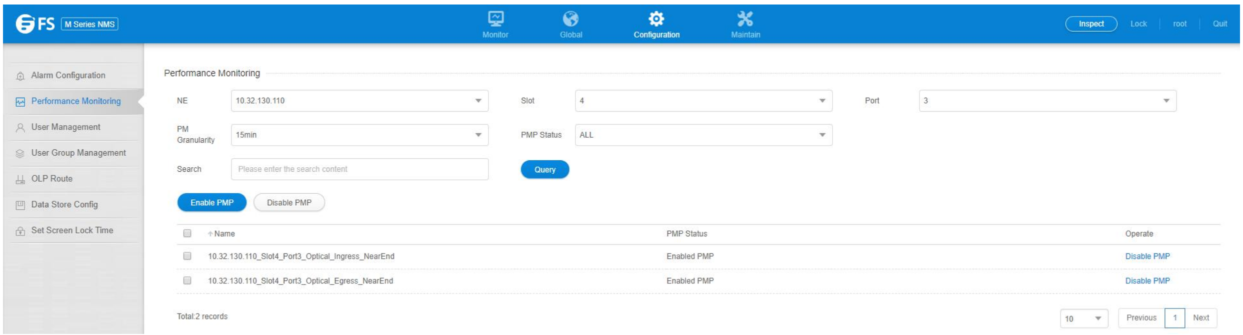
NE: Please Select
Slot: Please Select
Port: Please Select
PM Granularity: 15min
PMP Status: ALL
Search: Please enter the search content

□	Name	PMP Status	Operate

Total:0 records
10

Figure 6-1 Performance monitoring point management interface

You can check the monitoring status of the corresponding monitoring point by the above filtering box, the filtering conditions include network element, channel, port, PM monitoring period, performance monitoring status (there are three kinds of monitoring status: off, on and all, you can view the off, on or all monitoring status separately), after selecting all the filtering conditions, click Query to display the corresponding information, as shown in the figure.



Performance Monitoring

NE: 10.32.130.110
Slot: 4
Port: 3
PM Granularity: 15min
PMP Status: ALL
Search: Please enter the search content

□	Name	PMP Status	Operate
□	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Enabled PMP	Disable PMP
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Enabled PMP	Disable PMP

Total:2 records
10

Figure 6-2 Monitor the display of management information

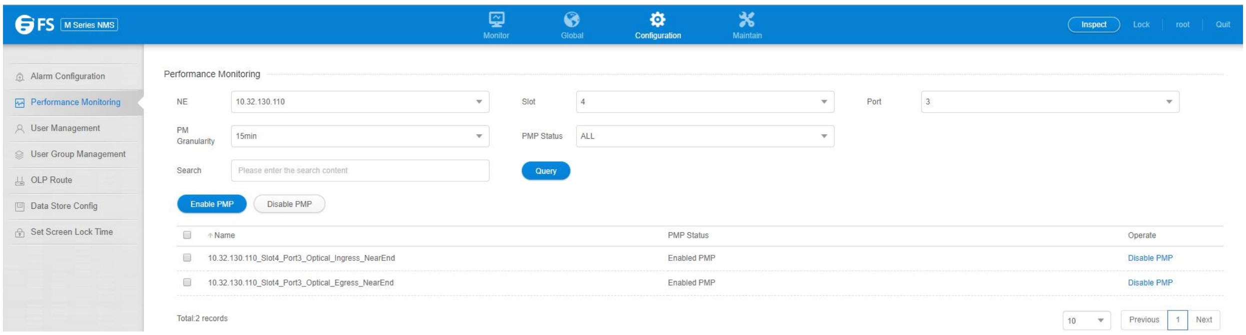
6.1.2. Introduction of performance monitoring points

- The performance monitoring point is determined and unique by monitoring point id, monitoring point location, monitoring point direction and monitoring period.
- Location of performance monitoring point: remote end and near-end (for OTUk and ODUk).
- Near-end monitor point (near-end): based on the received BIP8.
- Far-end monitor point (far-end): according to the received BEI.
- Direction of performance monitoring points: ingress and egress.

- Monitoring period: 15 minutes, 24 hours.

6.1.3. Turn on the performance monitoring point

When the current 15-minute performance monitoring point is opened, all the performance monitoring parameters under the performance monitoring point are opened at the same time, so only after the performance monitoring point is opened can the current performance statistics be viewed. As the performance monitoring operation will affect the performance of a network element, it supports up to 500 performance monitoring points (including 15 minutes and 24 hours) for a single network element, more than 500 points will show failed operation.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

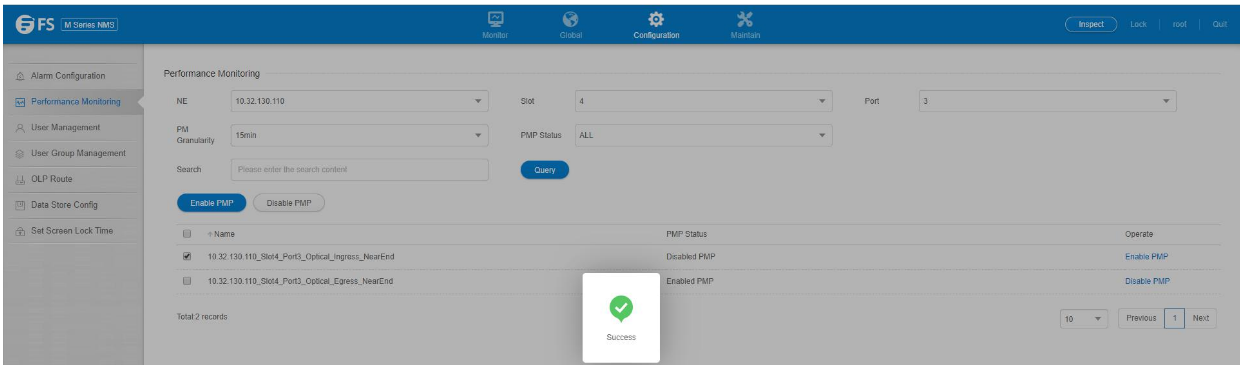
PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content

□	Name	PMP Status	Operate
□	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Enabled PMP	Disable PMP
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Enabled PMP	Disable PMP

Total 2 records | 10

Figure 6-3 Opening of monitoring points



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content

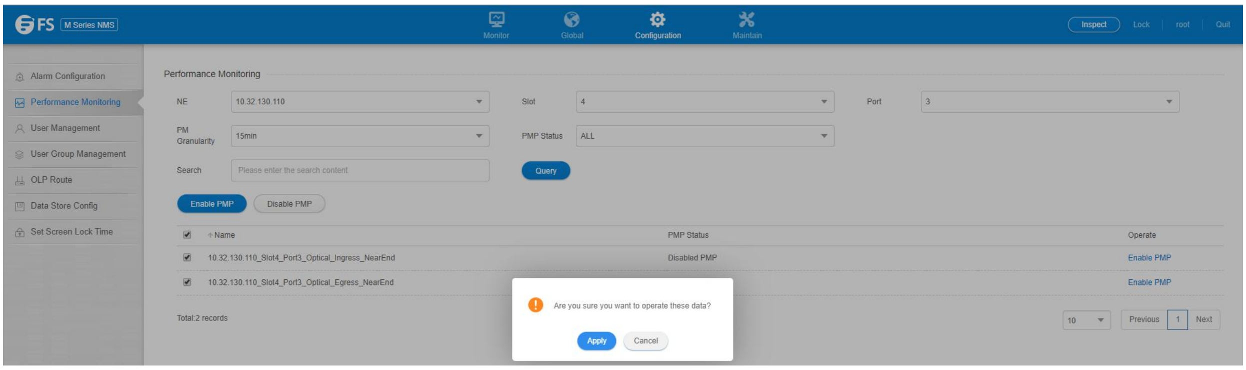
□	Name	PMP Status	Operate
☑	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Enabled PMP	Disable PMP

Total 2 records | 10

Success

Figure 6-4 Single monitoring point open

To batch open multiple data, you can select them by using the checkboxes in front of you, then click the button on top of the table (Open Performance Monitor) to open the selected Performance Monitor, as shown in the figure.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content

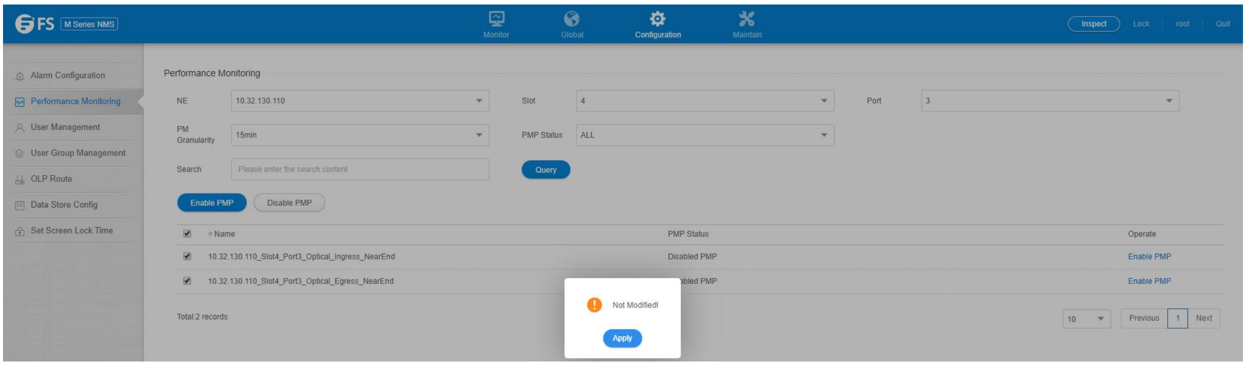
☑	Name	PMP Status	Operate
☑	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
☑	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd		Enable PMP

Total 2 records | 10

Are you sure you want to operate these data?

Figure 6-5 Batch monitoring points open

Select multiple performance monitors that are already open, then select Open Performance Monitor and click Confirm to show no changes as shown.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content | Query

Enable PMP | Disable PMP

☑	Name	PMP Status	Operate
☑	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
☑	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Disabled PMP	Enable PMP

Total:2 records

Not Modified!

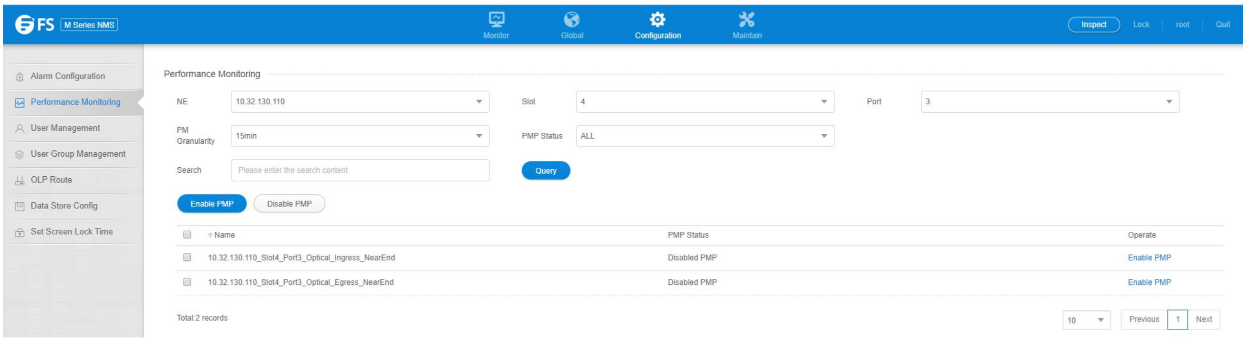
Apply

10 | Previous | 1 | Next

Figure 6-6 No modifications to monitor point status

6.1.4. Turn off performance monitoring points

When the current 15-minute performance monitoring point is closed, 24-hour performance monitoring is automatically closed by default, and all the performance monitoring parameters under this performance monitoring point are closed at the same time, so when the performance monitoring point is closed, you can't see the current performance statistics, as shown in the figure.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content | Query

Enable PMP | Disable PMP

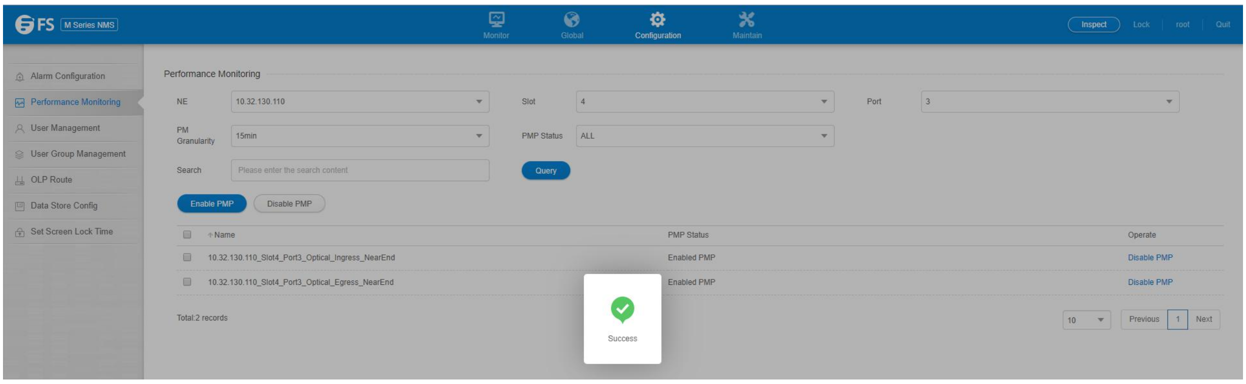
□	Name	PMP Status	Operate
□	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Disabled PMP	Enable PMP

Total:2 records

10 | Previous | 1 | Next

Figure 6-7 Closure of monitoring points

Each monitor point is modified in state via the buttons behind it, and can be de-activated individually, as shown in the figure.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content | Query

Enable PMP | Disable PMP

□	Name	PMP Status	Operate
□	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Enabled PMP	Disable PMP
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	Enabled PMP	Disable PMP

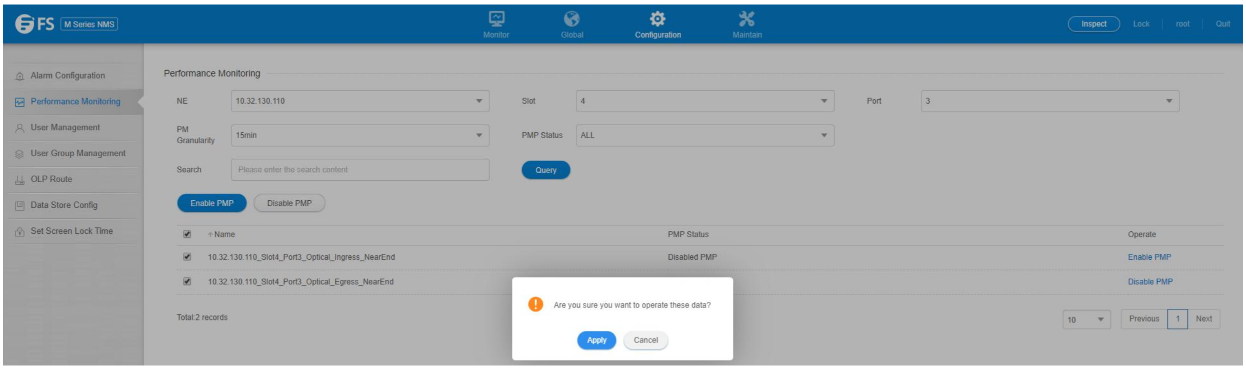
Total:2 records

Success

10 | Previous | 1 | Next

Figure 6-8 Single monitoring point off

To close the batch operation for multiple data, you can click the button (Close Performance Monitor) on the top of the table to close the selected Performance Monitor, as shown in the figure.



Performance Monitoring

NE: 10.32.130.110 Slot: 4 Port: 3

PM Granularity: 15min PMP Status: ALL

Search: Please enter the search content

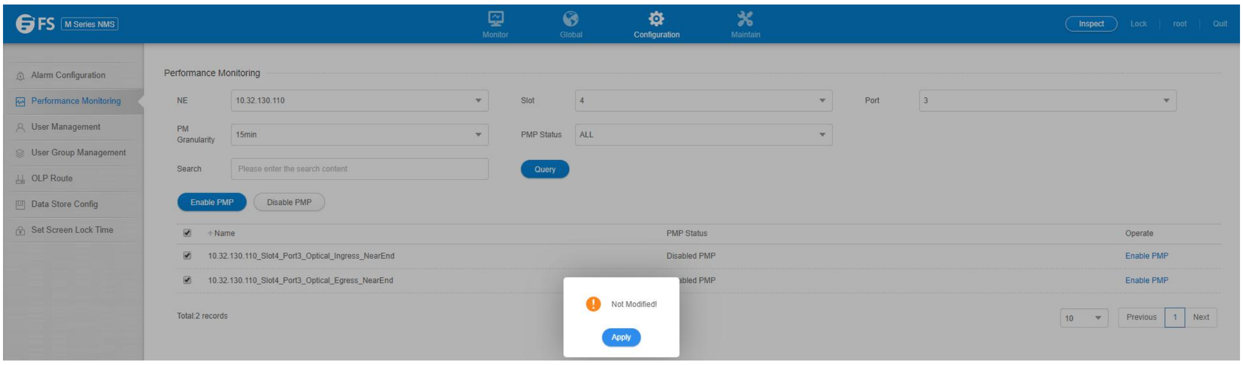
☑	Name	PMP Status	Operate
☑	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
☑	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd		Disable PMP

Total:2 records 10

Are you sure you want to operate these data?

Figure 6-9 Batch monitoring point closure

Select multiple performance monitors that have been turned off, then select Turn off performance monitoring and click OK to show no changes as shown.



Performance Monitoring

NE: 10.32.130.110 Slot: 4 Port: 3

PM Granularity: 15min PMP Status: ALL

Search: Please enter the search content

☑	Name	PMP Status	Operate
☑	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	Disabled PMP	Enable PMP
☑	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	abled PMP	Enable PMP

Total:2 records 10

Not Modified!

Figure 6-10 No modifications to monitor point status

6.1.5. Notes on monitoring performance

- Note 1, the monitoring point turns off when it is turned on in several situations.

(1) Manually close the monitoring points individually or in batch.

(2) When the board mode is switched, all 15 minutes, 24 hours monitoring points under the port are automatically shut down.

(3) When the port switching mode is switched, all the 15 minutes and 24 hours performance monitoring points under the port will be automatically shut down, only the optical power monitoring point will not be shut down.

(4) When the 15-minute performance monitoring point is turned off, the corresponding 24-hour performance monitoring point will be turned off automatically.

- Note 2, when the user closes the performance monitoring point.

(1) Current performance data can no longer be obtained.

(2) Already saved historical performance data can be queried by network administrators and users.

(3) When a user issues a shutdown command, the monitoring data that has been counted for that period of time (without reaching the full monitoring cycle of 15 minutes or 24 hours) will not be saved to the historical performance data.

(4) When the port mode is switched or when the port mode is set to empty, all performance monitoring points below it will be automatically deleted (previously stored historical performance data is still retained).

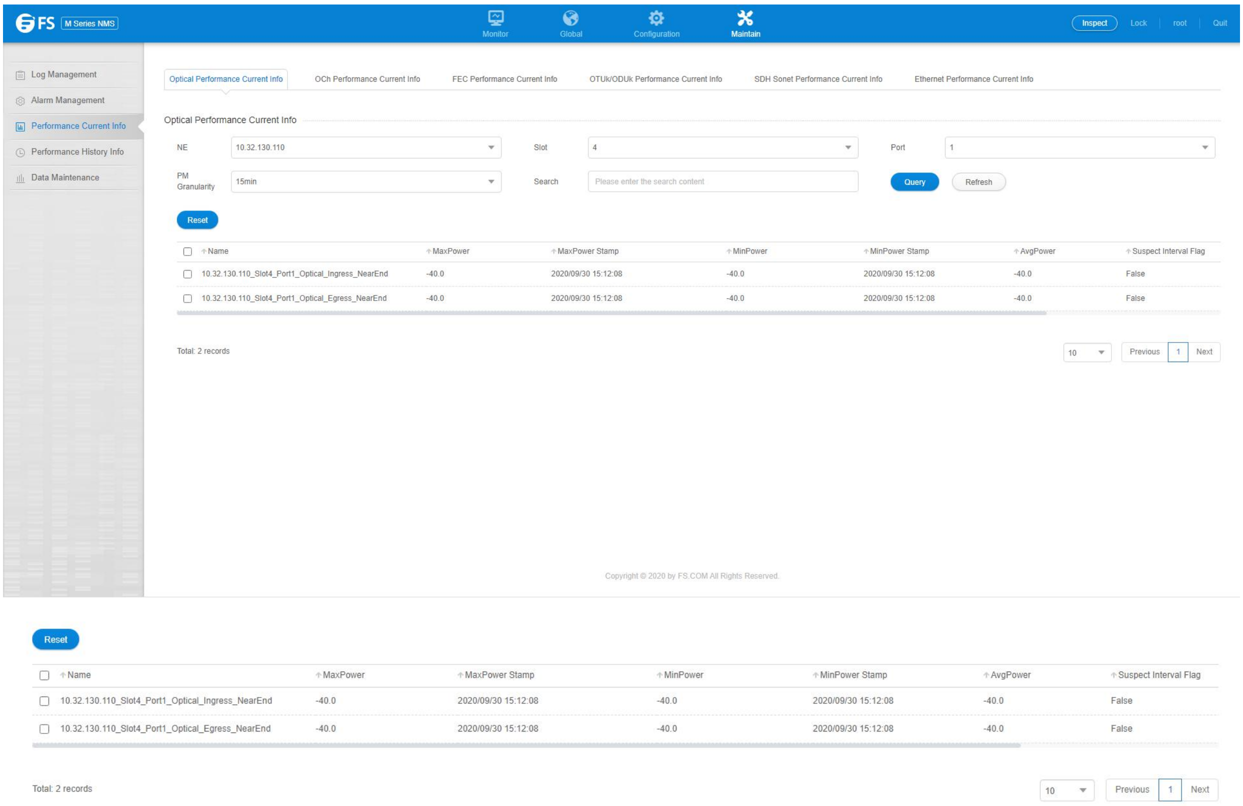
(5) When the TP corresponding to a port or monitoring point, such as OCh, OTUk, ODUk, Ethernet, SDH/SONET, is administratively down, all the performance monitoring points below it will be automatically closed (the previously stored historical performance data is still preserved).

6.2. Current Performance Statistics

6.2.1. Optical Power Monitoring

6.2.1.1. Introduction of optical power monitoring parameters

Monitoring parameters for monitoring points of optical power: including maximum optical power, maximum optical power timestamp, minimum optical power, minimum optical power timestamp, average optical power, suspicious interval flag, runtime and zero operation. The performance parameters at the optical power will be turned on and off simultaneously.


FS M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Log Management
Alarm Management
Performance Current Info
Performance History Info
Data Maintenance
Optical Performance Current Info
OCh Performance Current Info
FEC Performance Current Info
OTUk/ODUk Performance Current Info
SDH Sonet Performance Current Info
Ethernet Performance Current Info
Query
Refresh
Reset
Previous
1
Next
Copyright © 2020 by FS.COM All Rights Reserved.

Optical Performance Current Info

NE: 10.32.130.110
Slot: 4
Port: 1
PM Granularity: 15min
Search: Please enter the search content

□	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□	10.32.130.110_Slot4_Port1_Optical_Ingress_NearEnd	-40.0	2020/09/30 15:12:08	-40.0	2020/09/30 15:12:08	-40.0	False
□	10.32.130.110_Slot4_Port1_Optical_Egress_NearEnd	-40.0	2020/09/30 15:12:08	-40.0	2020/09/30 15:12:08	-40.0	False

Total: 2 records

10

□	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□	10.32.130.110_Slot4_Port1_Optical_Ingress_NearEnd	-40.0	2020/09/30 15:12:08	-40.0	2020/09/30 15:12:08	-40.0	False
□	10.32.130.110_Slot4_Port1_Optical_Egress_NearEnd	-40.0	2020/09/30 15:12:08	-40.0	2020/09/30 15:12:08	-40.0	False

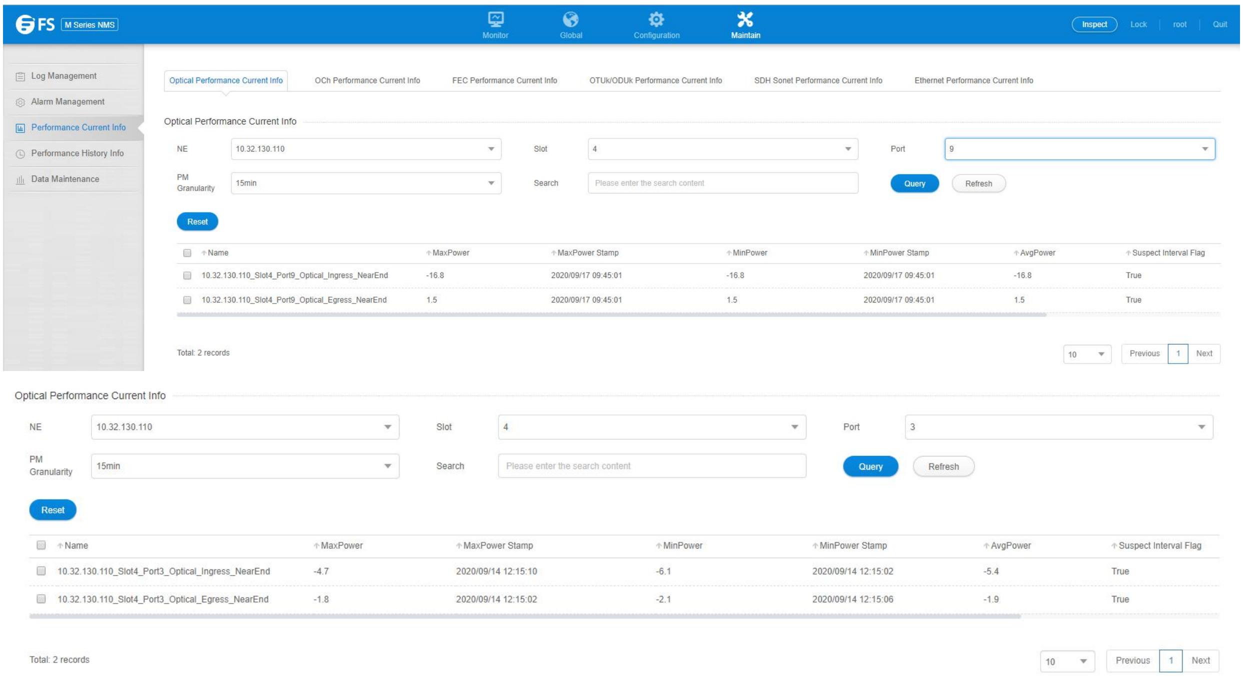
Total: 2 records

10

Figure 6-11 Monitoring parameter display

6.2.1.2. View Optical Power Monitoring Information

Select the corresponding network element, channel, port and monitoring period by the filter box at the top of the menu, the optical power data of a channel and a port of a network element will be displayed directly at the bottom. The monitoring port is inserted into the optical module, the maximum optical power and minimum optical power and the corresponding generation time will display the current reading data. 15 minutes after the monitoring port is opened, the suspicious interval marker should be untrustworthy, the running time will start counting from 0, after 900 seconds, the suspicious interval marker will become trustworthy, the running time will start counting again from 0, the previous 15 minutes data will automatically enter the history data. Medium.



Optical Performance Current Info

NE: 10.32.130.110 Slot: 4 Port: 9

PM Granularity: 15min Search: Please enter the search content

□ Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□ 10.32.130.110_Slot4_Port9_Optical_Ingress_NearEnd	-16.8	2020/09/17 09:45:01	-16.8	2020/09/17 09:45:01	-16.8	True
□ 10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/17 09:45:01	1.5	2020/09/17 09:45:01	1.5	True

Total: 2 records 10 1

Optical Performance Current Info

NE: 10.32.130.110 Slot: 4 Port: 3

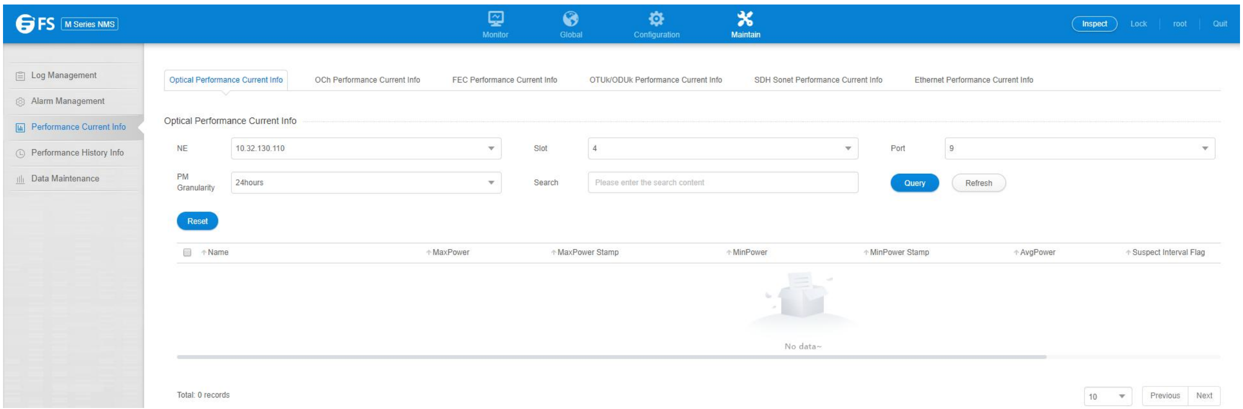
PM Granularity: 15min Search: Please enter the search content

□ Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□ 10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	-4.7	2020/09/14 12:15:10	-6.1	2020/09/14 12:15:02	-5.4	True
□ 10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	-1.8	2020/09/14 12:15:02	-2.1	2020/09/14 12:15:06	-1.9	True

Total: 2 records 10 1

Figure 6-12 Minute monitoring point data display

When the 24-hour monitoring port is first opened, the suspicious interval marker should be untrustworthy and the run time should start counting from 0. After waiting for 86400 seconds, the suspicious interval marker will become trustworthy and the run time will start counting again from 0. The 24-hour data from the previous entry is automatically entered into the historical data.



Optical Performance Current Info

NE: 10.32.130.110 Slot: 4 Port: 9

PM Granularity: 24hours Search: Please enter the search content

□ Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag

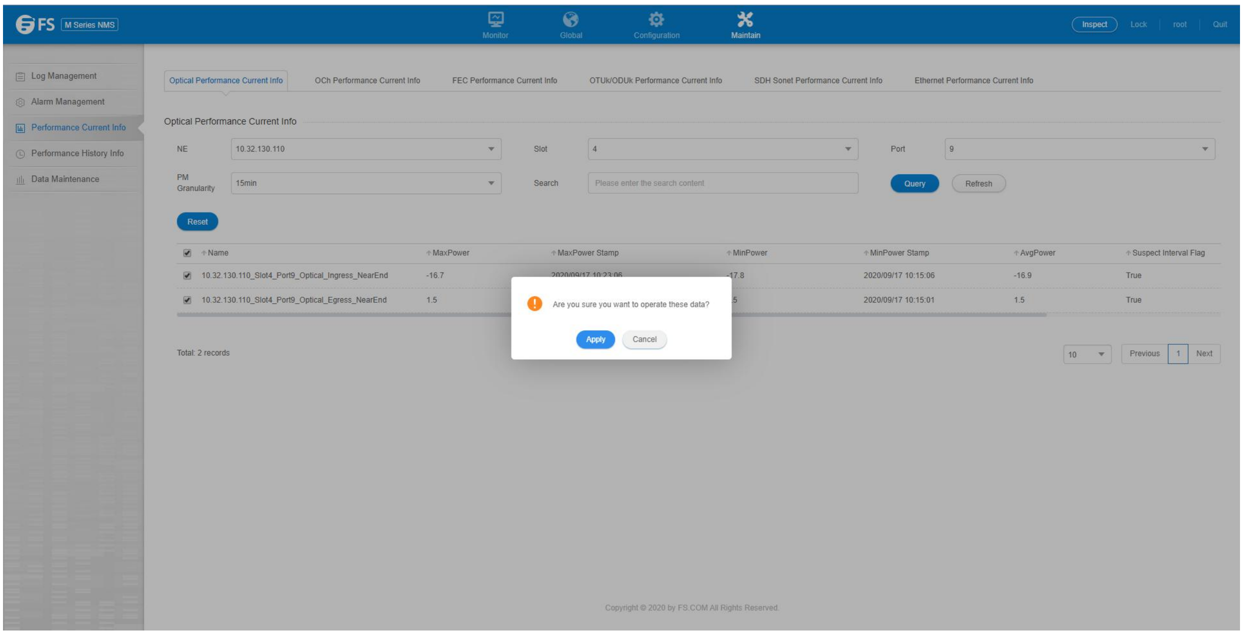
No data~

Total: 0 records 10

Figure 6-13 24-hour monitoring point data display

6.2.1.3. Zeroing of optical power monitoring data

When the current optical power monitoring point wants to zero out and start monitoring again, the 15 minutes and 24 hours operations are the same. Take 15 minutes as an example, you can click the zero operation at the end of each monitoring for single zero, or select the top box for batch zero, as shown in the figure.


FS M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Log Management
Alarm Management
Performance Current Info
Performance History Info
Data Maintenance
Optical Performance Current Info
OCh Performance Current Info
FEC Performance Current Info
OTUk/ODUk Performance Current Info
SDH Sonet Performance Current Info
Ethernet Performance Current Info
Query
Refresh
Reset
Previous
1
Next
Copyright © 2020 by FS.COM All Rights Reserved.

Optical Performance Current Info

NE: 10.32.130.110 | Slot: 4 | Port: 9

PM Granularity: 15min | Search: Please enter the search content

☑	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
☑	10.32.130.110_Slot4_Port9_Optical_Ingress_NearEnd	-16.7	2020/09/17 10:23:06	-17.8	2020/09/17 10:15:06	-16.9	True
☑	10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	[illegible]	[illegible]	2020/09/17 10:15:01	1.5	True

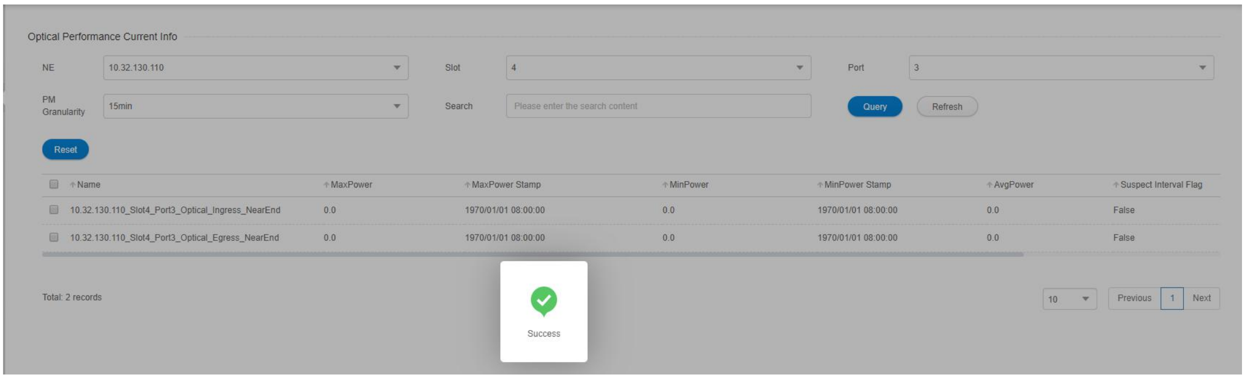
Total: 2 records | 10

Are you sure you want to operate these data?

Apply | Cancel

Figure 6-14 Optical power batch zeroing

Then click the Apply button, as shown in the figure, the display operation is successful, then you need to click the Refresh button to refresh the whole page, this time the suspicious interval marker will change from the original credible to untrustworthy, the running time will start from 0 to count again, the maximum optical power timestamp and minimum optical power timestamp will be updated to read the optical power of the latest time point, the maximum optical power and minimum optical power is also updated to the latest time point to read the value.



Optical Performance Current Info

NE: 10.32.130.110 | Slot: 4 | Port: 3

PM Granularity: 15min | Search: Please enter the search content

□	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□	10.32.130.110_Slot4_Port3_Optical_Ingress_NearEnd	0.0	1970/01/01 08:00:00	0.0	1970/01/01 08:00:00	0.0	False
□	10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	0.0	1970/01/01 08:00:00	0.0	1970/01/01 08:00:00	0.0	False

Total: 2 records | 10

Success

Figure 6-15 Zeroing operation successful

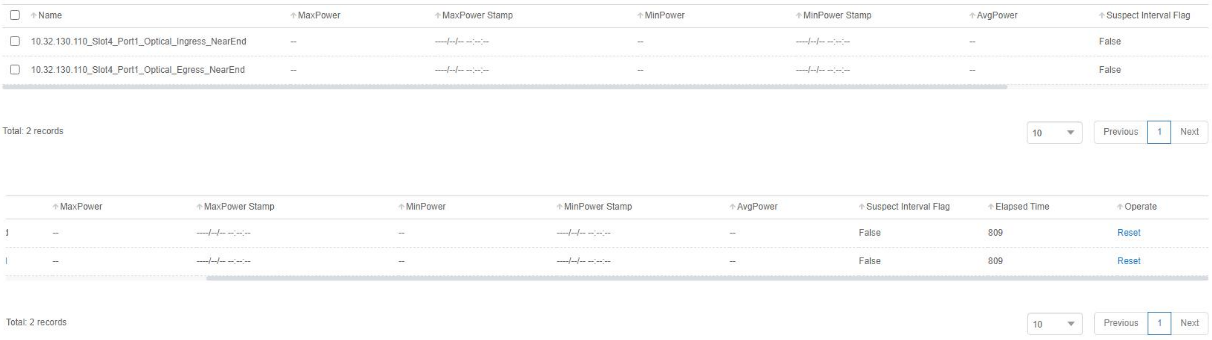
6.2.1.4. Optical power monitoring data display "--"

For ports:

(1) When no module is inserted into the port, that is, when the optical module is not in place but the port is enabled.

(2) When there is a module but mismatch on the port and the port is enabled.

At this time, the maximum and minimum optical power will be displayed "-", the maximum and minimum optical power time-stamp is displayed "- - - / - - / - - : - - : - -", the suspicious interval is marked as untrustworthy, the runtime display is normal, or counting from 0. As shown.



□	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□	10.32.130.110_Slot4_Port1_Optical_Ingress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False
□	10.32.130.110_Slot4_Port1_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False

Total: 2 records

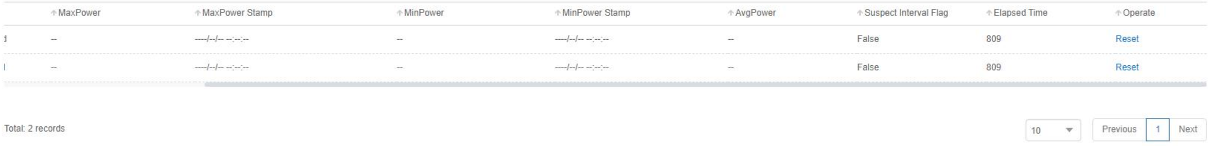
	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Elapsed Time	Operate
d	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset
l	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset

Total: 2 records

Figure 6-16 Module out of place display

For the board:

When the board is not in place or pre-configured empty channel and the board port is enable, the maximum and minimum optical power will display "--", the maximum and minimum optical power time-stamp will display "- - - - / - - / - - : - - - : - -", the suspect interval. Marked as untrustworthy, the run time is always 0 and does not change, as shown in the figure.

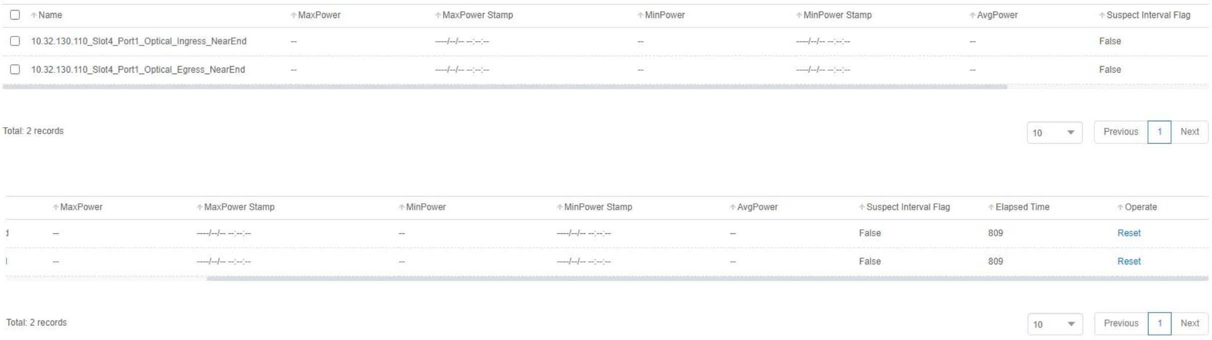


	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Elapsed Time	Operate
d	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset
l	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset

Total: 2 records

Figure 6-17 Monitor data display

When board mismatch and board port enable, the maximum and minimum optical power will display "--", the maximum and minimum optical power time-stamp will display "- - - / - - / - - : - - : - -", and the suspect interval is marked as untrustworthy. The runtime is normally counted from 0 as shown in the figure.



□	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag
□	10.32.130.110_Slot4_Port1_Optical_Ingress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False
□	10.32.130.110_Slot4_Port1_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False

Total: 2 records

	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Elapsed Time	Operate
d	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset
l	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	809	Reset

Total: 2 records

Figure 6-18 Monitoring data display during Mismatch

6.3. Historical performance statistics

6.3.1. Optical power historical performance statistics

6.3.1.1. Introduction of optical power history monitoring parameters

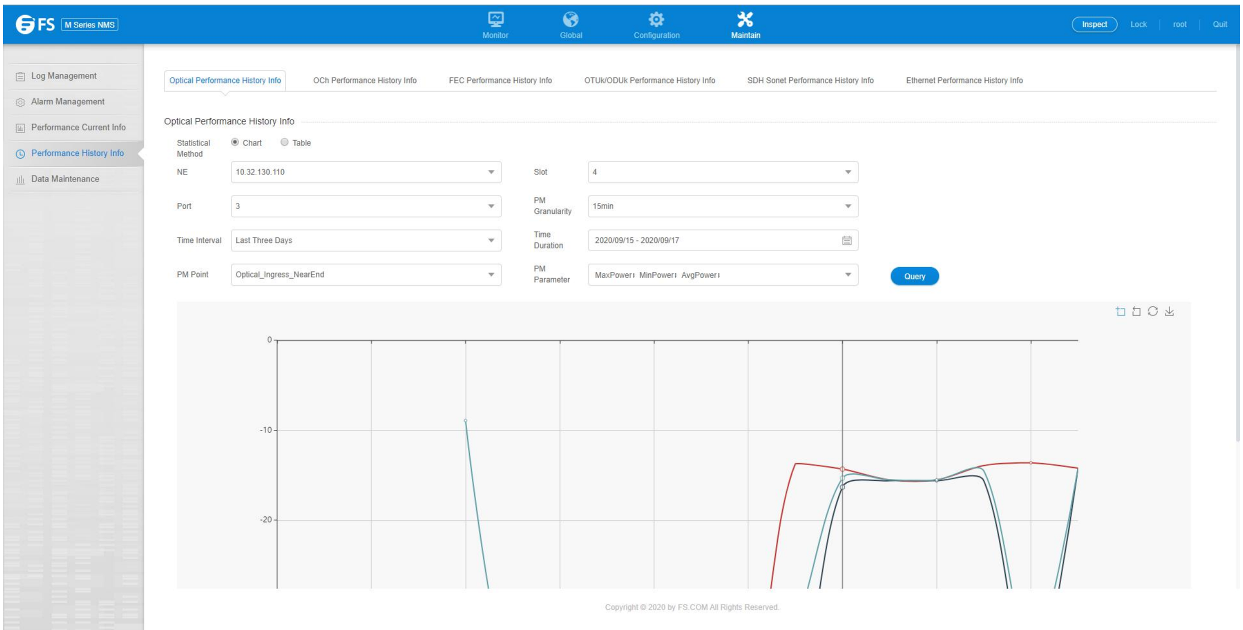
Monitoring parameters for historical monitoring points of optical power, including.

Time interval: It is a shortcut to choose the time, you can choose one day, three days, one week.

Duration: you can select a specific day or a period of time according to your needs.

Performance monitoring point: inlet - near end, outlet - near end.

Performance monitoring parameters: maximum optical power, minimum optical power, average optical power.


FS M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Log Management
Alarm Management
Performance Current Info
Performance History Info
Data Maintenance
Optical Performance History Info
OCh Performance History Info
FEC Performance History Info
OTUk/ODUk Performance History Info
SDH Sonet Performance History Info
Ethernet Performance History Info
Query
0
-10
-20
Copyright © 2020 by FS.COM All Rights Reserved.

Optical Performance History Info

Statistical Method: ● Chart ○ Table

NE: 10.32.130.110

Slot: 4

Port: 3

PM Granularity: 15min

Time Interval: Last Three Days

Time Duration: 2020/09/15 - 2020/09/17

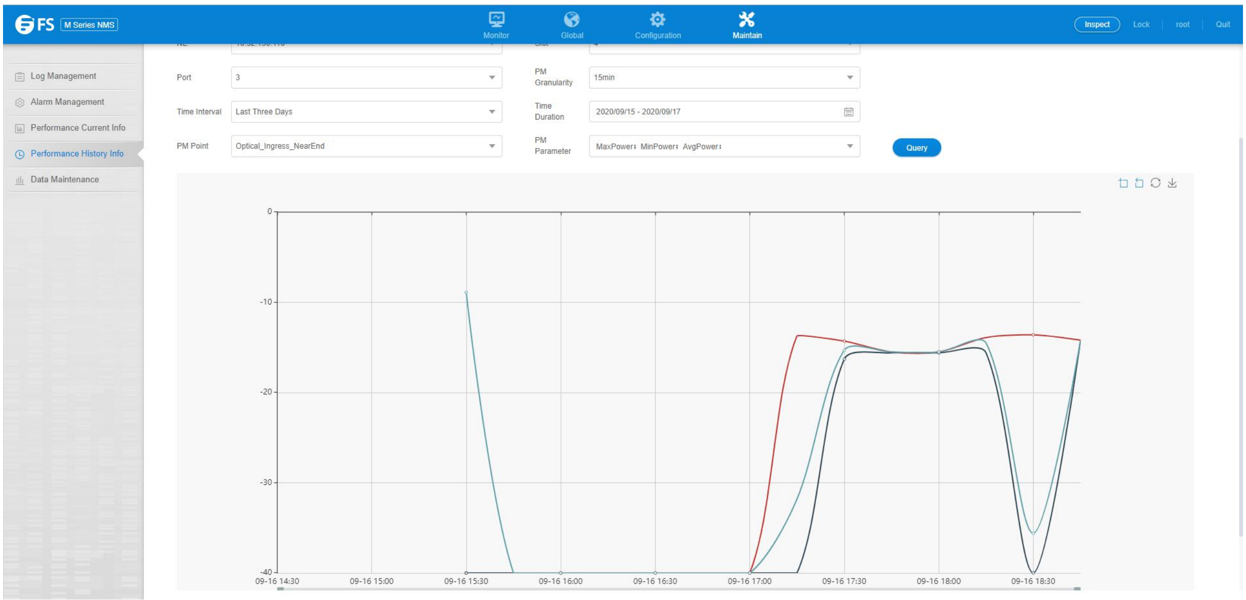
PM Point: Optical_Ingress_NearEnd

PM Parameter: MaxPower; MinPower; AvgPower;

Figure 6-19 Optical power history performance parameter display

6.3.1.2. View optical power history monitoring information

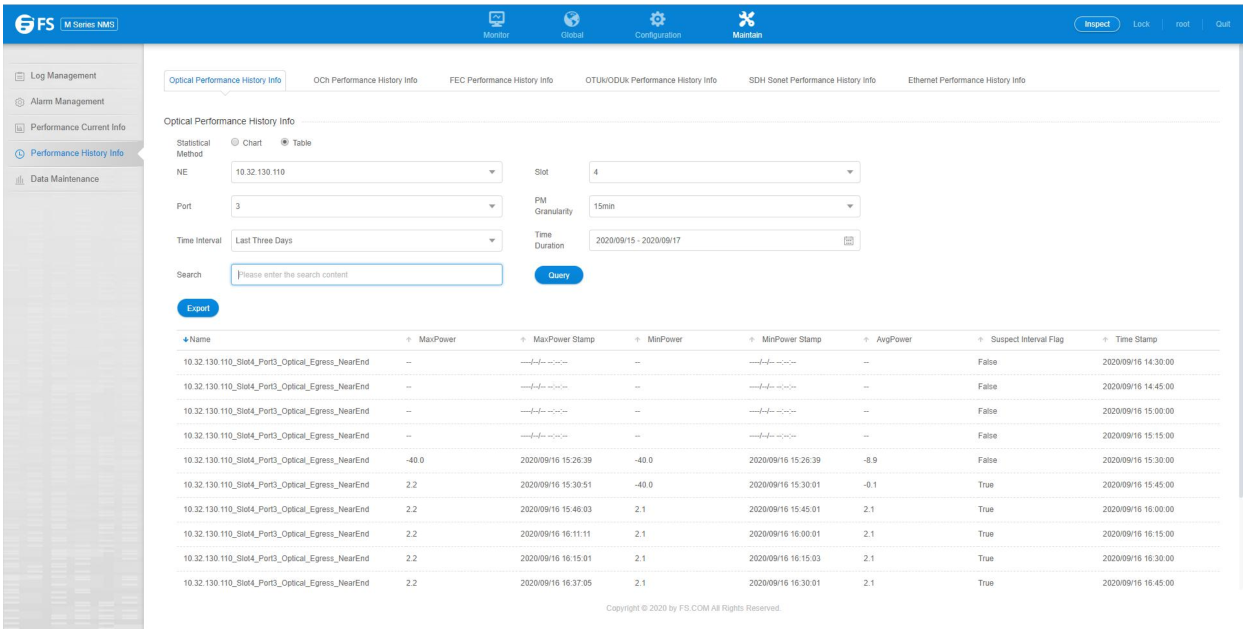
The operation and display of 15 minutes and 24 hours optical power are in the same format, the following is an example of 15 minutes optical power history monitoring point. You can select the corresponding network element, channel, port, monitoring period from the filter box at the top of the menu, and then select the time interval, performance monitoring point and the parameters you want to monitor. The maximum optical power, minimum optical power and average optical power are shown in the graph, the vertical axis represents the optical power value, the horizontal axis represents the time point, the data of 15 minutes are automatically transferred from the current statistics to the historical statistics.



Port: 3
PM Granularity: 15min
Time Interval: Last Three Days
Time Duration: 2020/09/15 - 2020/09/17
PM Point: Optical_Ingress_NearEnd
PM Parameter: MaxPower; MinPower; AvgPower;
Query

Figure 6-20 15-minute chart data display

The historical performance statistics of optical power can also be presented in the form of a table, click on the table, the interface shown in the figure.


FS
M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Log Management
Alarm Management
Performance Current Info
Performance History Info
Data Maintenance
Optical Performance History Info
OCh Performance History Info
FEC Performance History Info
OTUk/ODUk Performance History Info
SDH Sonet Performance History Info
Ethernet Performance History Info

Optical Performance History Info

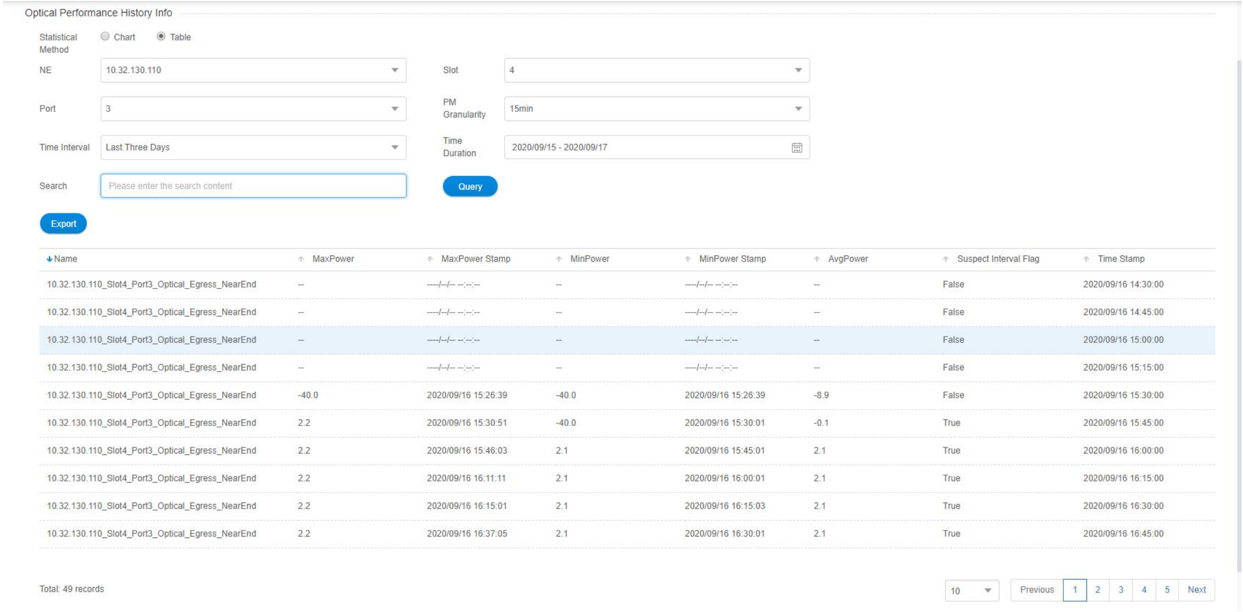
Statistical Method: ○ Chart ● Table
NE: 10.32.130.110
Slot: 4
Port: 3
PM Granularity: 15min
Time Interval: Last Three Days
Time Duration: 2020/09/15 - 2020/09/17
Search: Please enter the search content
Query
Export

Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Time Stamp
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 14:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 14:45:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:00:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:15:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	-40.0	2020/09/16 15:26:39	-40.0	2020/09/16 15:26:39	-8.9	False	2020/09/16 15:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 15:30:51	-40.0	2020/09/16 15:30:01	-0.1	True	2020/09/16 15:45:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 15:46:03	2.1	2020/09/16 15:45:01	2.1	True	2020/09/16 16:00:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:11:11	2.1	2020/09/16 16:00:01	2.1	True	2020/09/16 16:15:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:15:01	2.1	2020/09/16 16:15:03	2.1	True	2020/09/16 16:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:37:05	2.1	2020/09/16 16:30:01	2.1	True	2020/09/16 16:45:00

Copyright © 2020 by FS.COM All Rights Reserved.

Figure 6-21 15-minute table screen display

Select the time interval and duration, click Query, and a history of all optical power currently recorded by this port will appear, as shown in the screen.



Optical Performance History Info

Statistical Method ○ Chart ● Table

NE: 10.32.130.110

Slot: 4

Port: 3

PM Granularity: 15min

Time Interval: Last Three Days

Time Duration: 2020/09/15 - 2020/09/17

Search: Please enter the search content

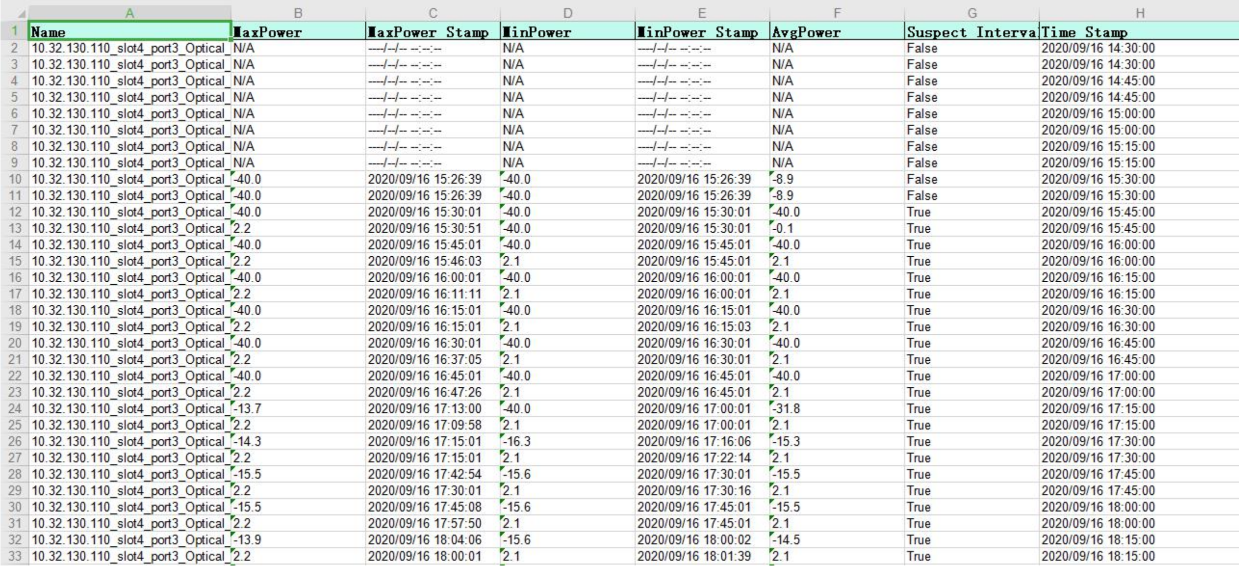
Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Time Stamp
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 14:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 14:45:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:00:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:15:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	-40.0	2020/09/16 15:26:39	-40.0	2020/09/16 15:26:39	-8.9	False	2020/09/16 15:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 15:30:51	-40.0	2020/09/16 15:30:01	-0.1	True	2020/09/16 15:45:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 15:46:03	2.1	2020/09/16 15:45:01	2.1	True	2020/09/16 16:00:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:11:11	2.1	2020/09/16 16:00:01	2.1	True	2020/09/16 16:15:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:15:01	2.1	2020/09/16 16:15:03	2.1	True	2020/09/16 16:30:00
10.32.130.110_Slot4_Port3_Optical_Egress_NearEnd	2.2	2020/09/16 16:37:05	2.1	2020/09/16 16:30:01	2.1	True	2020/09/16 16:45:00

Total: 49 records

Figure 6-22 15-minute table history data display

6.3.1.3. Exporting optical power history monitoring information

If you want to save the history data, you can click the export button above to download the file to a local file with the default name "HistoryOpticalPm.xls", as shown in the figure below.



	A	B	C	D	E	F	G	H
1	Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interva	Time Stamp
2	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 14:30:00
3	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 14:30:00
4	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 14:45:00
5	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 14:45:00
6	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 15:00:00
7	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 15:00:00
8	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 15:15:00
9	10.32.130.110_slot4_port3_Optical_	N/A	----/--/-- --:--:--	N/A	----/--/-- --:--:--	N/A	False	2020/09/16 15:15:00
10	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 15:26:39	-40.0	2020/09/16 15:26:39	-8.9	False	2020/09/16 15:30:00
11	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 15:26:39	-40.0	2020/09/16 15:26:39	-8.9	False	2020/09/16 15:30:00
12	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 15:30:01	-40.0	2020/09/16 15:30:01	-40.0	True	2020/09/16 15:45:00
13	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 15:30:51	-40.0	2020/09/16 15:30:01	-0.1	True	2020/09/16 15:45:00
14	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 15:45:01	-40.0	2020/09/16 15:45:01	-40.0	True	2020/09/16 16:00:00
15	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 15:46:03	2.1	2020/09/16 15:45:01	2.1	True	2020/09/16 16:00:00
16	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 16:00:01	-40.0	2020/09/16 16:00:01	-40.0	True	2020/09/16 16:15:00
17	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 16:11:11	2.1	2020/09/16 16:00:01	2.1	True	2020/09/16 16:15:00
18	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 16:15:01	-40.0	2020/09/16 16:15:01	-40.0	True	2020/09/16 16:30:00
19	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 16:15:01	2.1	2020/09/16 16:15:03	2.1	True	2020/09/16 16:30:00
20	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 16:30:01	-40.0	2020/09/16 16:30:01	-40.0	True	2020/09/16 16:45:00
21	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 16:37:05	2.1	2020/09/16 16:30:01	2.1	True	2020/09/16 16:45:00
22	10.32.130.110_slot4_port3_Optical_	-40.0	2020/09/16 16:45:01	-40.0	2020/09/16 16:45:01	-40.0	True	2020/09/16 17:00:00
23	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 16:47:26	2.1	2020/09/16 16:45:01	2.1	True	2020/09/16 17:00:00
24	10.32.130.110_slot4_port3_Optical_	-13.7	2020/09/16 17:13:00	-40.0	2020/09/16 17:00:01	-31.8	True	2020/09/16 17:15:00
25	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 17:09:58	2.1	2020/09/16 17:00:01	2.1	True	2020/09/16 17:15:00
26	10.32.130.110_slot4_port3_Optical_	-14.3	2020/09/16 17:15:01	-16.3	2020/09/16 17:16:06	-15.3	True	2020/09/16 17:30:00
27	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 17:15:01	2.1	2020/09/16 17:22:14	2.1	True	2020/09/16 17:30:00
28	10.32.130.110_slot4_port3_Optical_	-15.5	2020/09/16 17:42:54	-15.6	2020/09/16 17:30:01	-15.5	True	2020/09/16 17:45:00
29	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 17:30:01	2.1	2020/09/16 17:30:16	2.1	True	2020/09/16 17:45:00
30	10.32.130.110_slot4_port3_Optical_	-15.5	2020/09/16 17:45:08	-15.6	2020/09/16 17:45:01	-15.5	True	2020/09/16 18:00:00
31	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 17:57:50	2.1	2020/09/16 17:45:01	2.1	True	2020/09/16 18:00:00
32	10.32.130.110_slot4_port3_Optical_	-13.9	2020/09/16 18:04:06	-15.6	2020/09/16 18:00:02	-14.5	True	2020/09/16 18:15:00
33	10.32.130.110_slot4_port3_Optical_	2.2	2020/09/16 18:00:01	2.1	2020/09/16 18:01:39	2.1	True	2020/09/16 18:15:00

Figure 6-23 Exporting Historical Data

7. Log Management

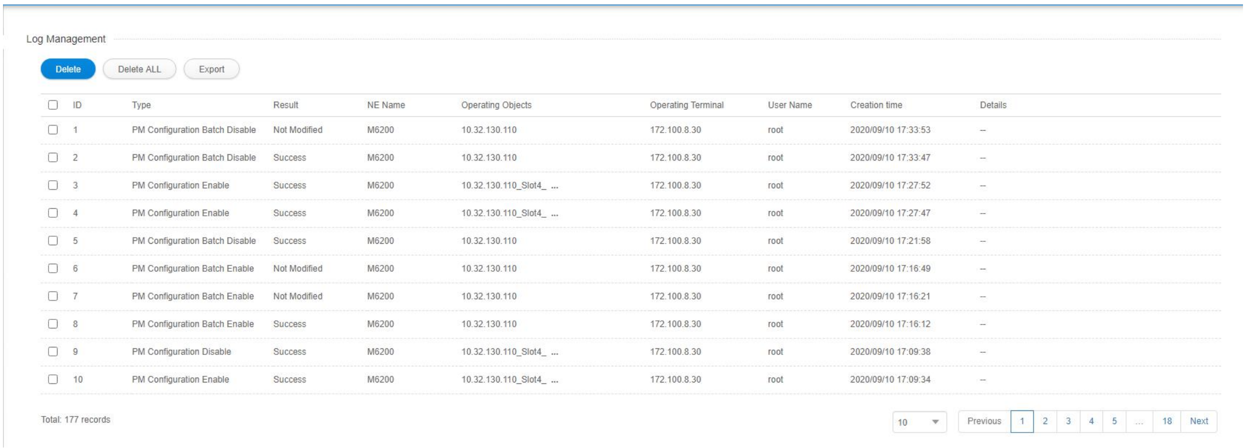
7.1. Log Management Introduction

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 "Maintenance" on the top navigation bar -> "Log Management" to enter the page, as shown in the figure below.



□	ID	Type	Result	NE Name	Operating Objects	Operating Terminal	User Name	Creation time	Details
□	1	PM Configuration Batch Disable	Not Modified	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:53	--
□	2	PM Configuration Batch Disable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:47	--
□	3	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:52	--
□	4	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:47	--
□	5	PM Configuration Batch Disable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:21:58	--
□	6	PM Configuration Batch Enable	Not Modified	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:16:49	--
□	7	PM Configuration Batch Enable	Not Modified	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:16:21	--
□	8	PM Configuration Batch Enable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:16:12	--
□	9	PM Configuration Disable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:09:38	--
□	10	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:09:34	--

Total: 177 records

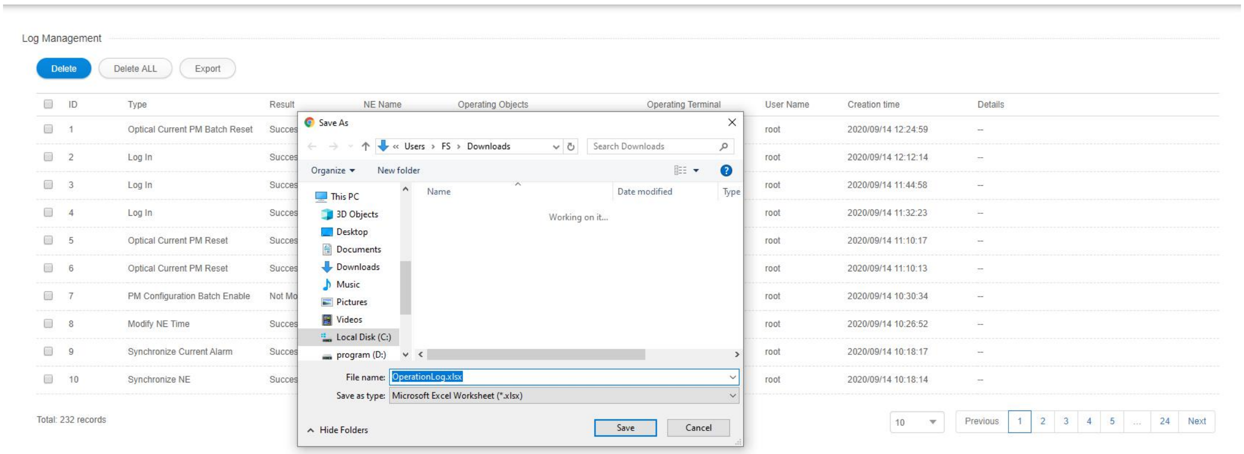
Figure 7-1 Log Management

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

Check the check box in the upper left corner, click the *"Export"* button to export the selected logs, and click Save As to put the exported logs in a custom directory.



Log Management

□	ID	Type	Result	NE Name	Operating Objects	Operating Terminal	User Name	Creation time	Details
□	1	Optical Current PM Batch Reset	Succes				root	2020/09/14 12:24:59	--
□	2	Log In	Succes				root	2020/09/14 12:12:14	--
□	3	Log In	Succes				root	2020/09/14 11:44:58	--
□	4	Log In	Succes				root	2020/09/14 11:32:23	--
□	5	Optical Current PM Reset	Succes				root	2020/09/14 11:10:17	--
□	6	Optical Current PM Reset	Succes				root	2020/09/14 11:10:13	--
□	7	PM Configuration Batch Enable	Not Mo				root	2020/09/14 10:30:34	--
□	8	Modify NE Time	Succes				root	2020/09/14 10:26:52	--
□	9	Synchronize Current Alarm	Succes				root	2020/09/14 10:18:17	--
□	10	Synchronize NE	Succes				root	2020/09/14 10:18:14	--

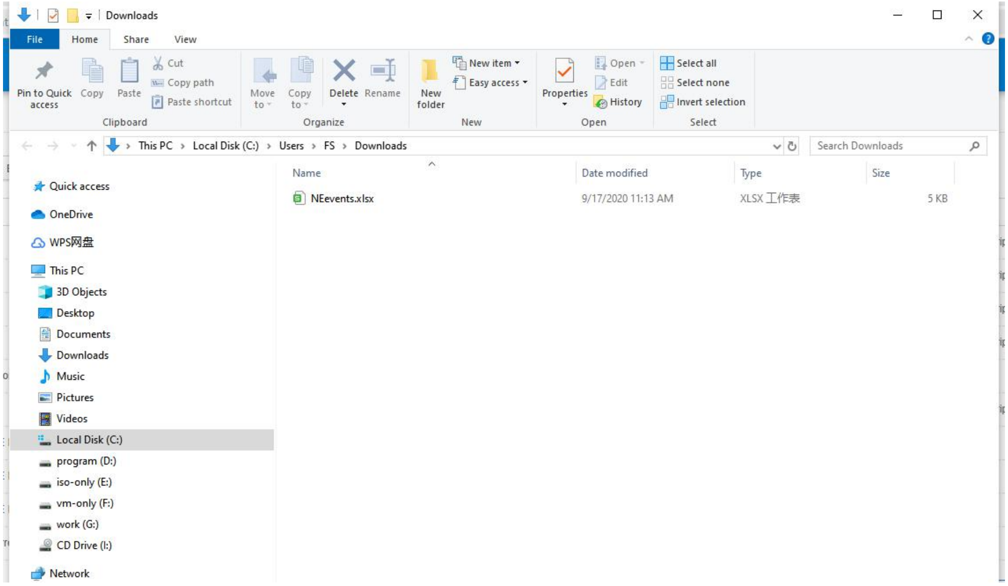
Total: 232 records

Save As

File name: OperationLog.xlsx

Save as type: Microsoft Excel Worksheet (*.xlsx)

Figure 7-2 Export Log

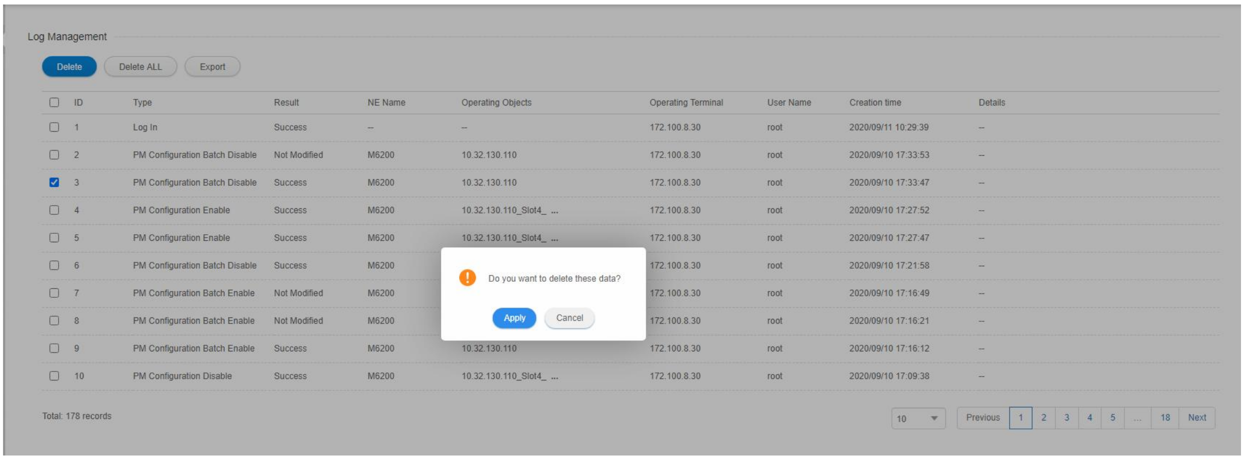


Name	Date modified	Type	Size
NEevents.xlsx	9/17/2020 11:13 AM	XLSX 工作表	5 KB

Figure 7-1 Exported Logs

7.3.2. Delete Log

Select the form in the data you want to delete (the deletion log itself will also generate a "deletion log" of the log record), click the *"Delete"* button will prompt the user to confirm the deletion operation again. The following figure.



Log Management

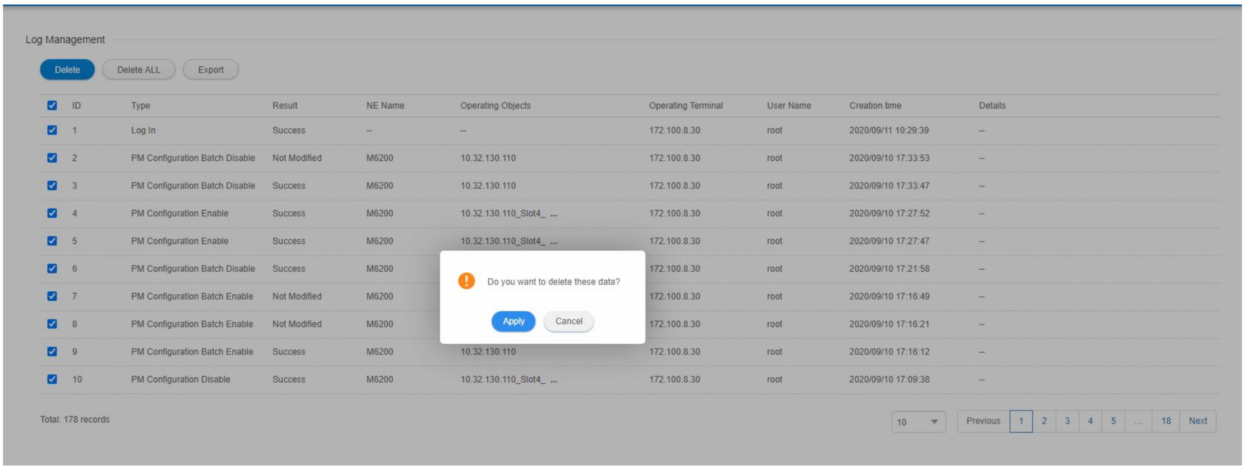
□	ID	Type	Result	NE Name	Operating Objects	Operating Terminal	User Name	Creation time	Details
□	1	Log In	Success	--	--	172.100.8.30	root	2020/09/11 10:29:39	--
□	2	PM Configuration Batch Disable	Not Modified	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:53	--
☑	3	PM Configuration Batch Disable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:47	--
□	4	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:52	--
□	5	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:47	--
□	6	PM Configuration Batch Disable	Success	M6200		172.100.8.30	root	2020/09/10 17:21:58	--
□	7	PM Configuration Batch Enable	Not Modified	M6200		172.100.8.30	root	2020/09/10 17:16:49	--
□	8	PM Configuration Batch Enable	Not Modified	M6200		172.100.8.30	root	2020/09/10 17:16:21	--
□	9	PM Configuration Batch Enable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:16:12	--
□	10	PM Configuration Disable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:09:38	--

Total: 178 records

Do you want to delete these data?

Figure 7-2 Log Management-Delete Log

Click the *"Delete All"* button, the user will be prompted to confirm to change the deletion operation here. The following figure.



Log Management

☑	ID	Type	Result	NE Name	Operating Objects	Operating Terminal	User Name	Creation time	Details
☑	1	Log In	Success	--	--	172.100.8.30	root	2020/09/11 10:29:39	--
☑	2	PM Configuration Batch Disable	Not Modified	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:53	--
☑	3	PM Configuration Batch Disable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:33:47	--
☑	4	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:52	--
☑	5	PM Configuration Enable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:27:47	--
☑	6	PM Configuration Batch Disable	Success	M6200		172.100.8.30	root	2020/09/10 17:21:58	--
☑	7	PM Configuration Batch Enable	Not Modified	M6200		172.100.8.30	root	2020/09/10 17:16:49	--
☑	8	PM Configuration Batch Enable	Not Modified	M6200		172.100.8.30	root	2020/09/10 17:16:21	--
☑	9	PM Configuration Batch Enable	Success	M6200	10.32.130.110	172.100.8.30	root	2020/09/10 17:16:12	--
☑	10	PM Configuration Disable	Success	M6200	10.32.130.110_Slot4_ ...	172.100.8.30	root	2020/09/10 17:09:38	--

Total: 178 records

Do you want to delete these data?

Figure 7-5 Log management - delete all logs

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:

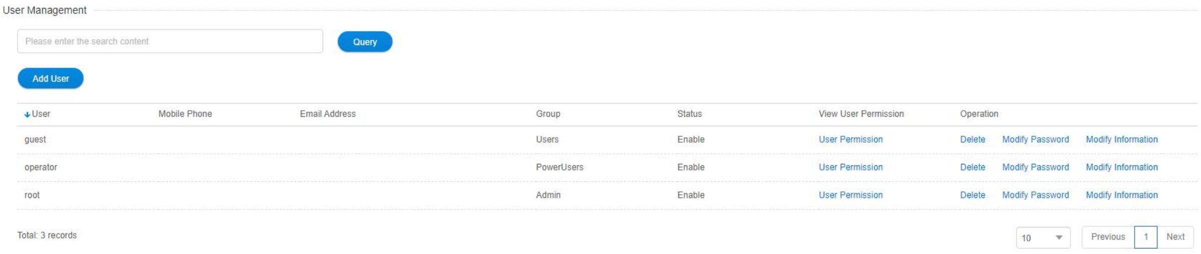
- User group management which can add user group and perform corresponding delete and modify operations.
- User management which can check login user, modify login password and delete login user.

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 *"Configuration"* on the top navigation bar --> *"User Group Management"* to enter the page, as shown in the figure.

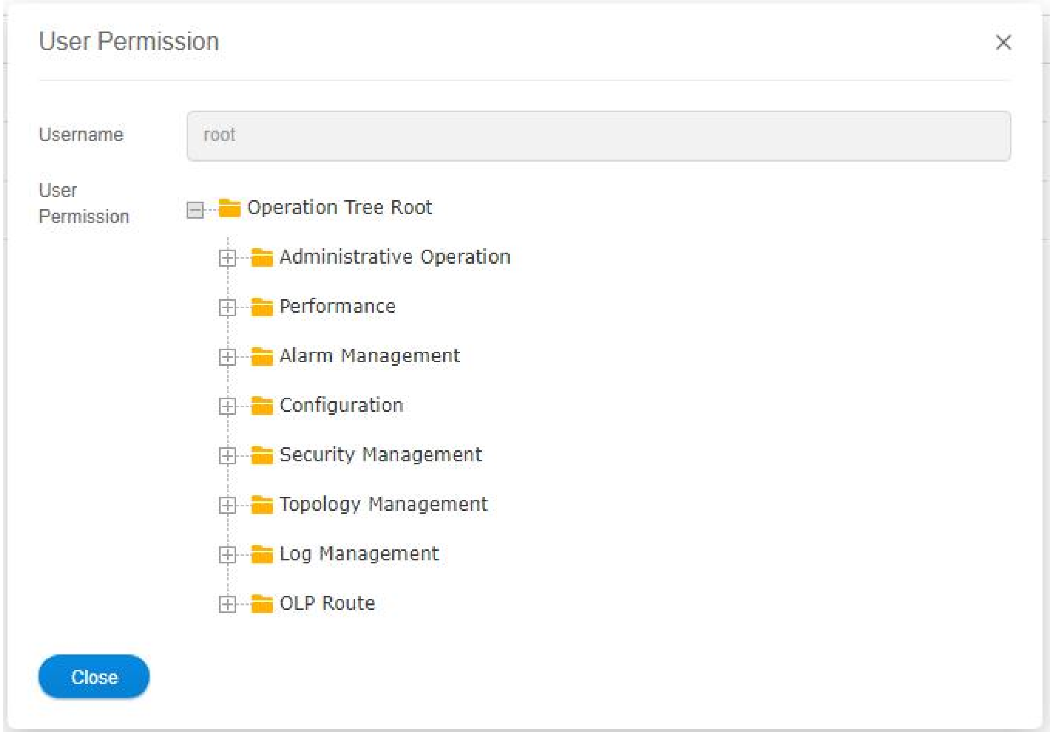


User	Mobile Phone	Email Address	Group	Status	View User Permission	Operation
guest			Users	Enable	User Permission	Delete Modify Password Modify Information
operator			PowerUsers	Enable	User Permission	Delete Modify Password Modify Information
root			Admin	Enable	User Permission	Delete Modify Password Modify Information

Total: 3 records

Figure 8-1 User Group Management

The *"Add Group"* button allows you to add a group and assign corresponding permissions to the group, as shown in the figure.



User Permission ×

Username: root

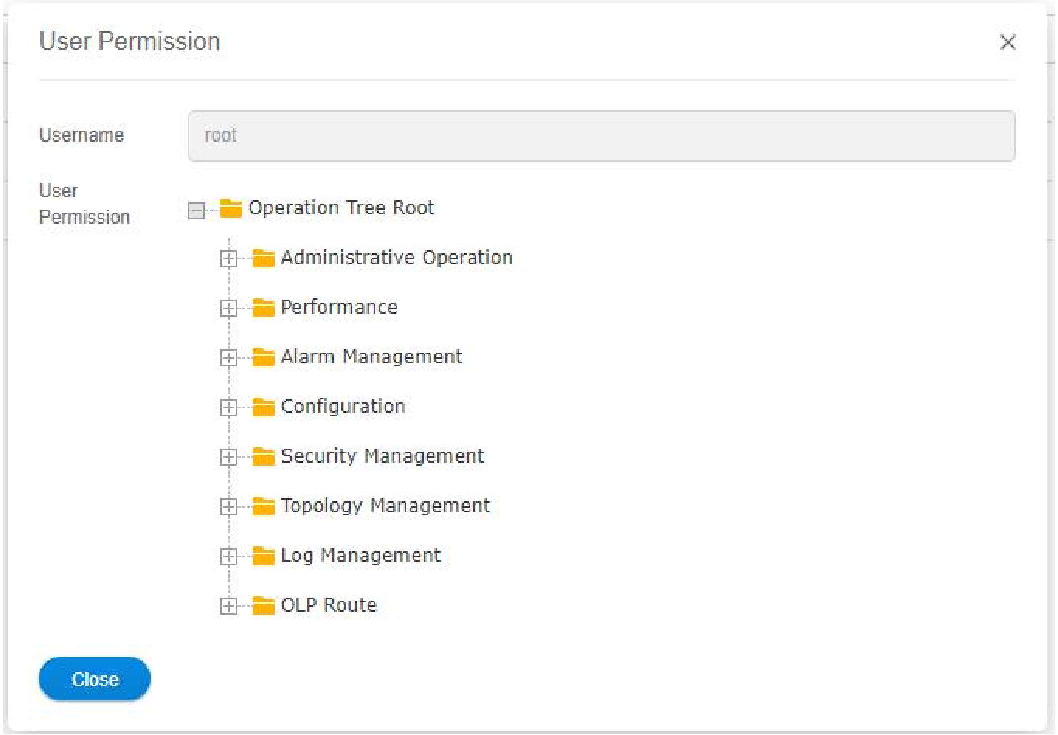
User Permission:

- Operation Tree Root
  - Administrative Operation
  - Performance
  - Alarm Management
  - Configuration
  - Security Management
  - Topology Management
  - Log Management
  - OLP Route

Figure 8-2 User Group Management-Add Group

8.2.2. Modify User Group

Select the *"Group Permissions"* column in the table in the user group management page --> *"Operation Permission Assignment"* button to modify the operation permissions of this user group, as shown in the figure.



User Permission ×

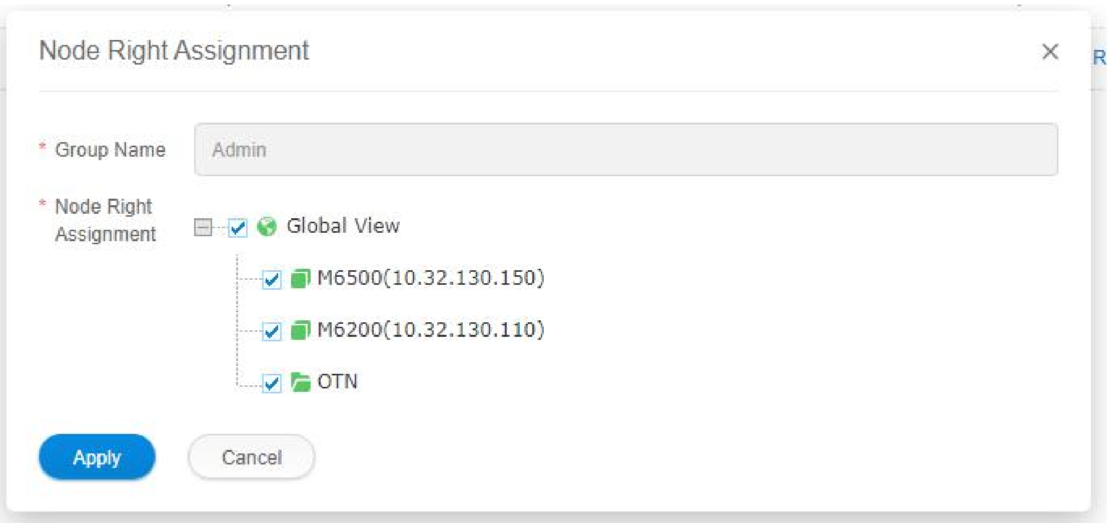
Username: root

User Permission:

- Operation Tree Root
  - Administrative Operation
  - Performance
  - Alarm Management
  - Configuration
  - Security Management
  - Topology Management
  - Log Management
  - OLP Route

Figure 8-3 User Group Management-Modify Group Right

Select the *"Group Permissions"* column in the user group management page table --> *"Node Permission Assignment"* button to assign different node devices to the user, as shown in the figure.



* Group Name: Admin

* Node Right Assignment:

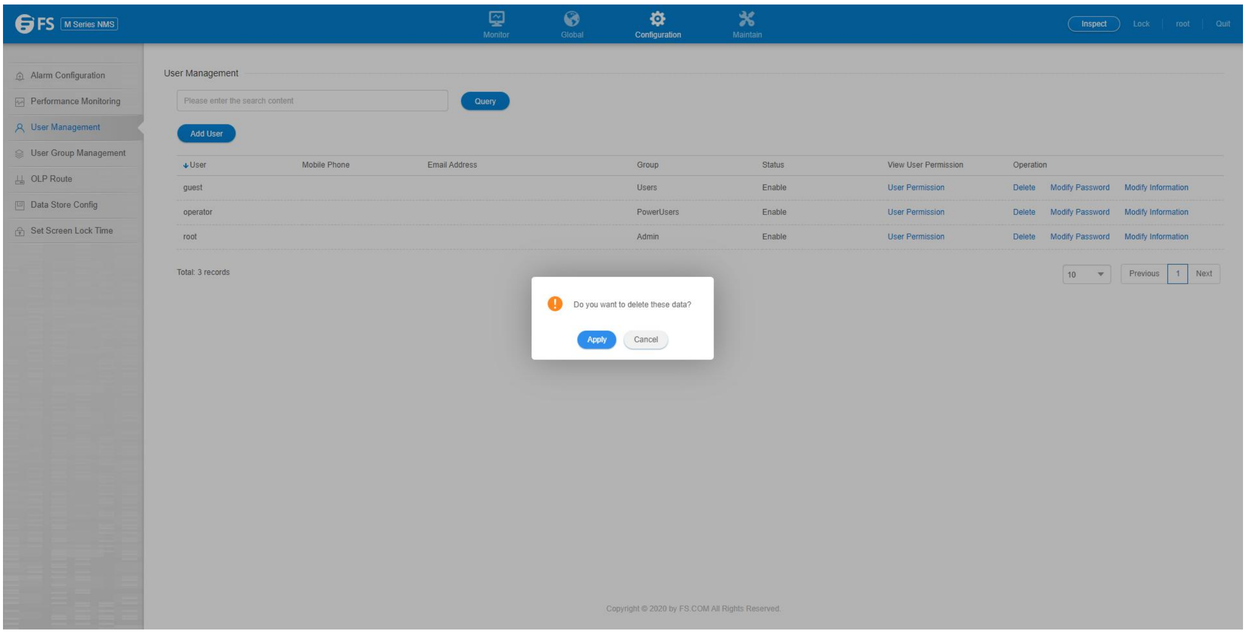
- ☑ Global View
  - ☑ M6500(10.32.130.150)
  - ☑ M6200(10.32.130.110)
  - ☑ OTN

Figure 8-1 User Group Management-Unassigned Users

Note: If the user group does not have *"device management"* privilege, it will have no privilege to assign node privilege to the user group. There are three types of permission settings, a tick means operable, a x means visible and inoperable, a null means invisible. The default user cannot be modified.

8.2.3. Delete User Group

The *"Delete"* button on the user group management screen can delete the corresponding data, and you will be prompted again if you want to confirm the deletion, as shown in the figure below.



User Management

Please enter the search content

User	Mobile Phone	Email Address	Group	Status	View User Permission	Operation
guest			Users	Enable	User Permission	Delete Modify Password Modify Information
operator			PowerUsers	Enable	User Permission	Delete Modify Password Modify Information
root			Admin	Enable	User Permission	Delete Modify Password Modify Information

Total: 3 records

10

Do you want to delete these data?

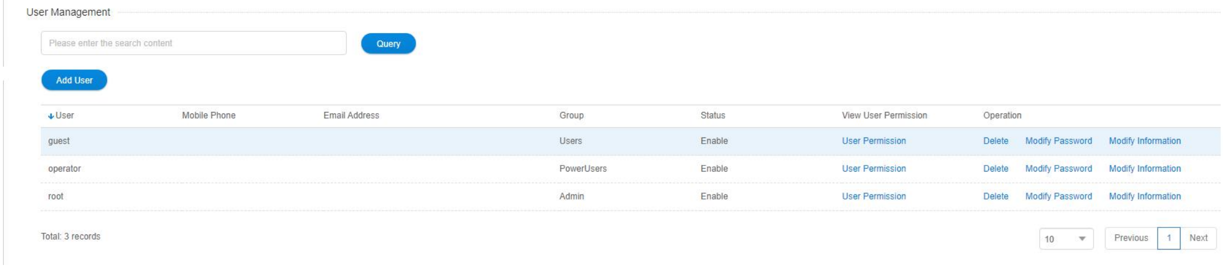
Figure 8-2 User Group Management-Delete Group

Admin, Power-users and Users are default groups. They cannot be deleted.

8.3. User Management

8.3.1. Add User

Click *"Configuration"* on the top navigation bar --> *"User Management"* to enter the page, as shown in the figure.



User Management

Please enter the search content

User	Mobile Phone	Email Address	Group	Status	View User Permission	Operation
guest			Users	Enable	User Permission	Delete Modify Password Modify Information
operator			PowerUsers	Enable	User Permission	Delete Modify Password Modify Information
root			Admin	Enable	User Permission	Delete Modify Password Modify Information

Total: 3 records

Figure 8-3 User Management

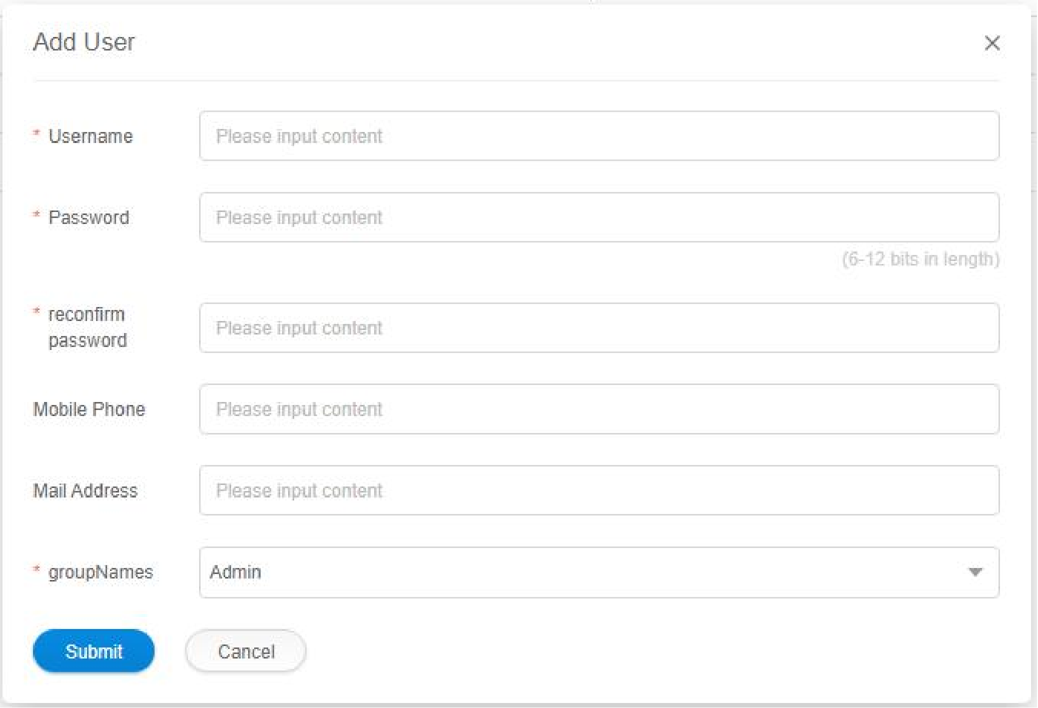
Tips:

(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:



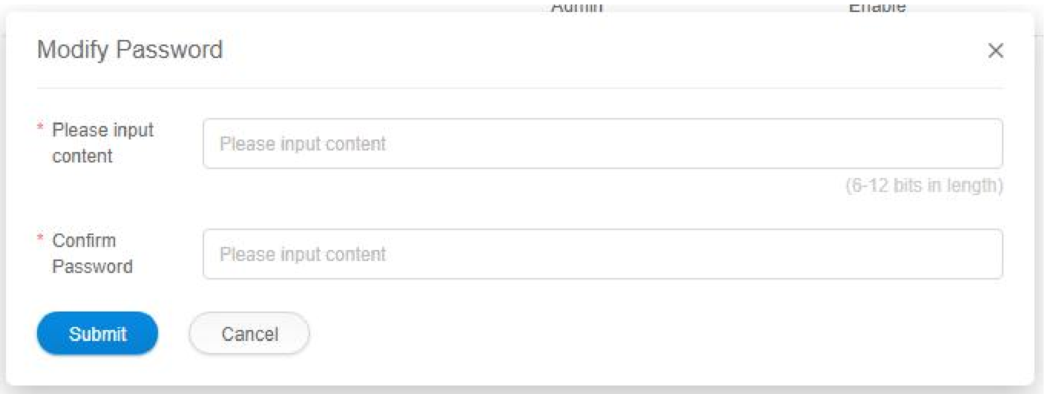
Add User

* Username	Please input content
* Password	Please input content (6-12 bits in length)
* reconfirm password	Please input content
Mobile Phone	Please input content
Mail Address	Please input content
* groupNames	Admin

Figure 8-4 User Management-Add User

8.3.2. Modify User

You can change the password by clicking the *"Modify Password"* button in the table in the user management interface, as shown below.



Modify Password

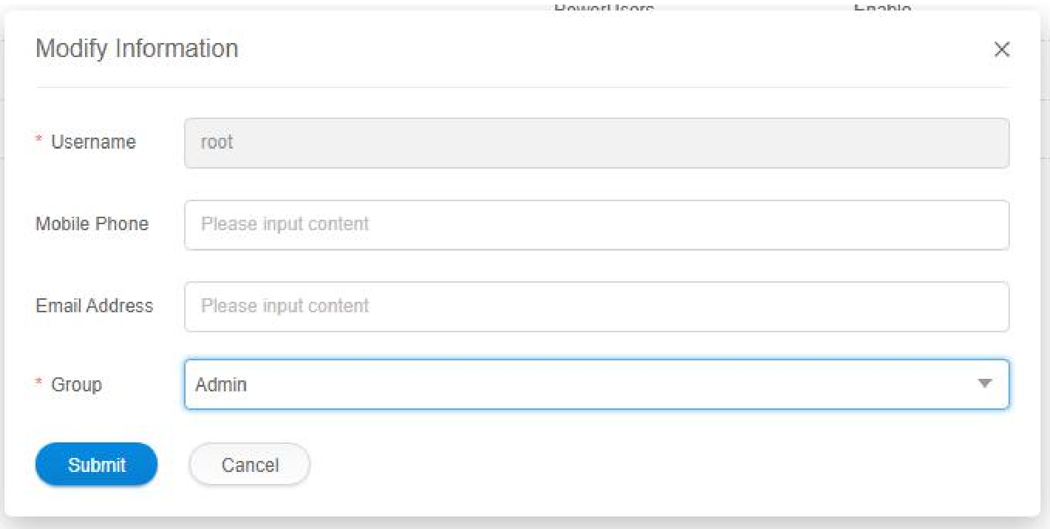
* Please input content: Please input content

(6-12 bits in length)

* Confirm Password: Please input content

Figure 8-5 User Management-Modify Password

The *"Modify Information"* button in the table in the user management interface can move the user to a group or remove the user from a group, the user has the privileges of the group to which he/she belongs, and can perform the corresponding operation privileges. As shown in the figure below.



Modify Information

* Username: root

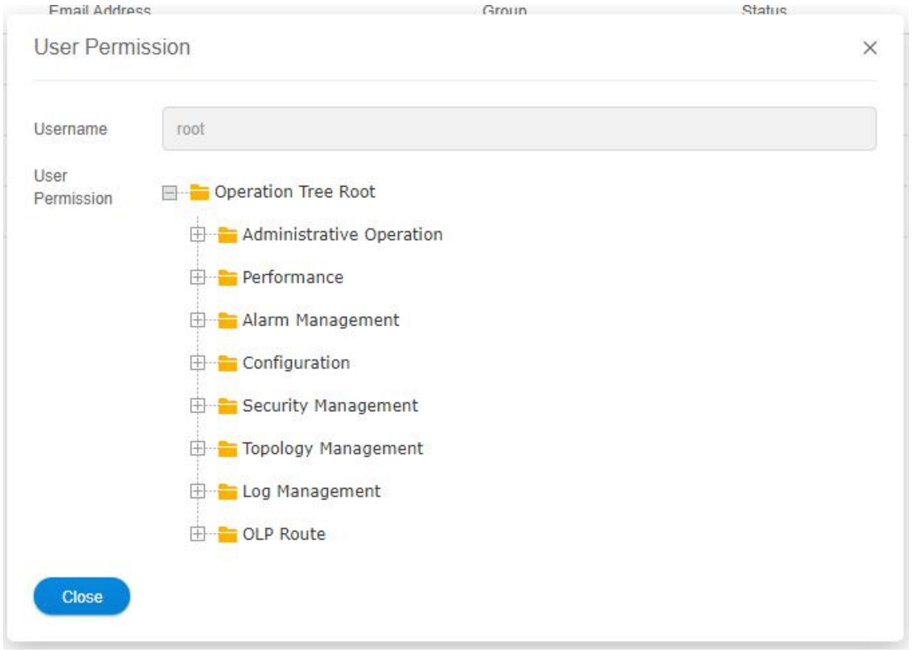
Mobile Phone: Please input content

Email Address: Please input content

* Group: Admin

Figure 8-6 User Management-Group Assignment

The *"User Permission"* button in the table in the user management interface can view the user's permissions, and the user needs corresponding operating privileges to perform corresponding operations. As shown in the figure.



Username: root

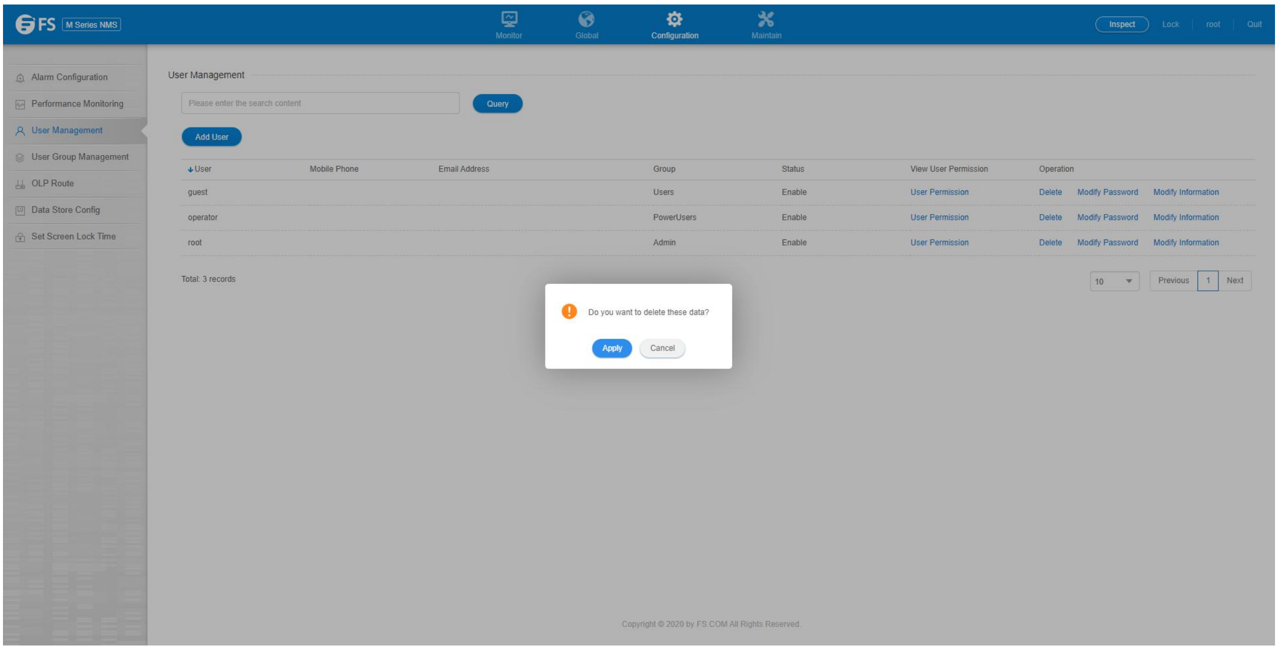
User Permission:

- Operation Tree Root
  - Administrative Operation
  - Performance
  - Alarm Management
  - Configuration
  - Security Management
  - Topology Management
  - Log Management
  - OLP Route

Figure 8-7 User Management-User Right

8.3.3. Delete User

The *"Delete"* button on the table in the user management interface can delete the corresponding data, and the deletion operation will confirm if the data is to be deleted or not, as shown below.



User Management

User	Mobile Phone	Email Address	Group	Status	View User Permission	Operation
guest			Users	Enable	User Permission	Delete Modify Password Modify Information
operator			PowerUsers	Enable	User Permission	Delete Modify Password Modify Information
root			Admin	Enable	User Permission	Delete Modify Password Modify Information

Total: 3 records

Do you want to delete these data?

Figure 8-8 User Management-Delete User

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 9-1 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.

Log in as an advanced user, then select *"Configuration"*--->*"User Management"* and select *"Add User"* button to pop up the *"Add User"* dialog box, as shown in the figure below: Enter user name, email address, password and user level (i.e. group name) and click *"Add"*.

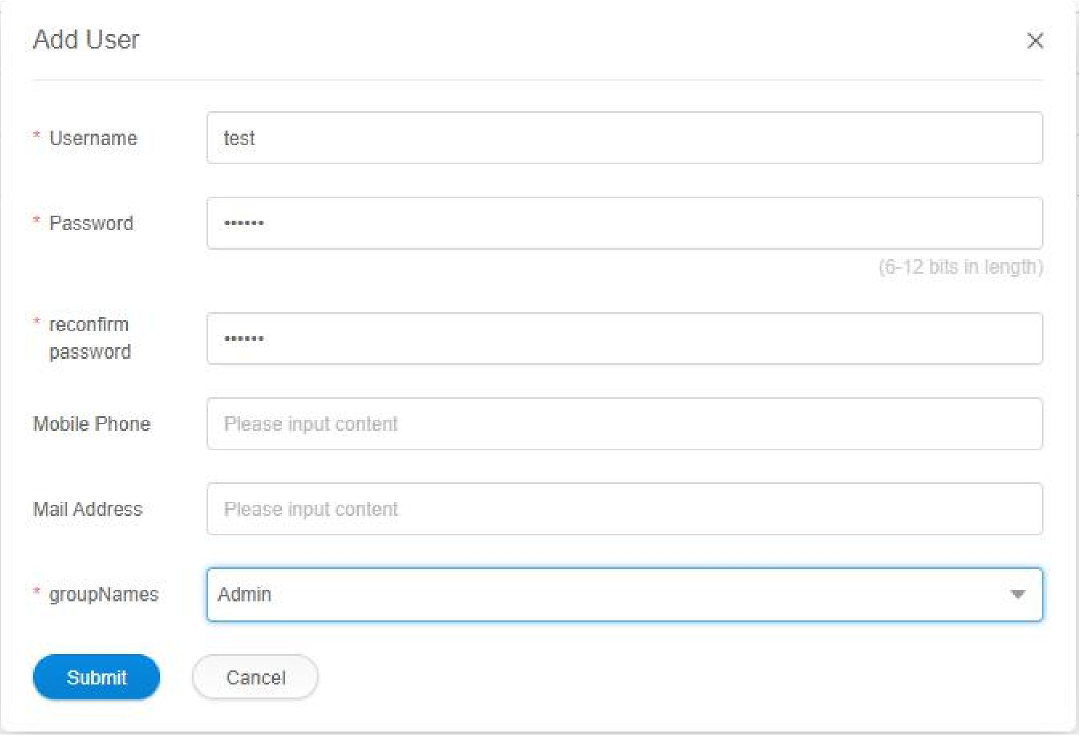
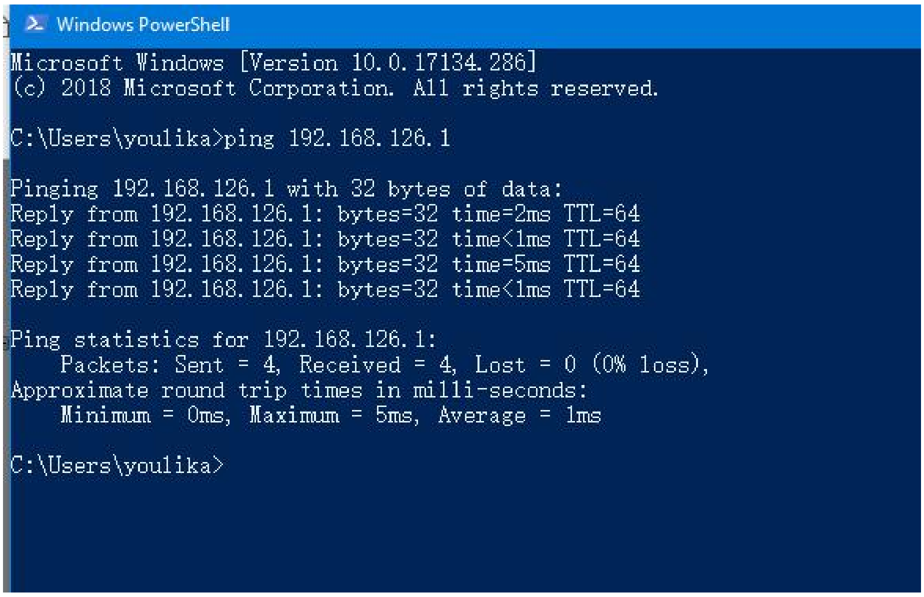


Figure 9-1 Add User—Assign Permissions

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.

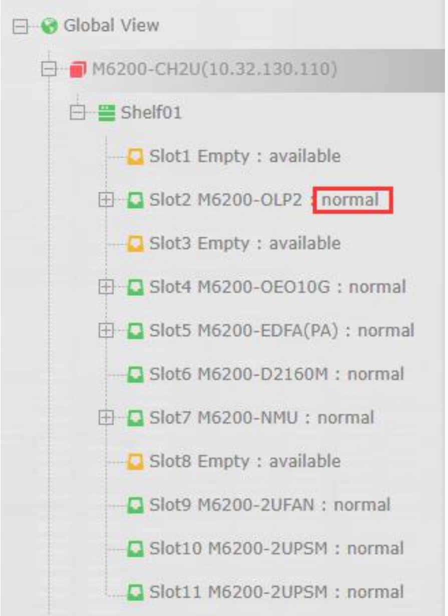


```
Microsoft Windows [Version 10.0.17134.286]
(c) 2018 Microsoft Corporation. All rights reserved.

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 9-1 Ping NE

9.2.3. Check Board State

Check the status of every single board every day, there should be no alarm that the single board is not in place. In the "Global View" of the browser, select the frame of the device you want to view, you can see the status of the single board.



Global View
M6200-CH2U(10.32.130.110)
Shelf01
Slot1 Empty : available
Slot2 M6200-OLP2 : normal
Slot3 Empty : available
Slot4 M6200-OEO10G : normal
Slot5 M6200-EDFA(PA) : normal
Slot6 M6200-D2160M : normal
Slot7 M6200-NMU : normal
Slot8 Empty : available
Slot9 M6200-2UFAN : normal
Slot10 M6200-2UPSM : normal
Slot11 M6200-2UPSM : normal

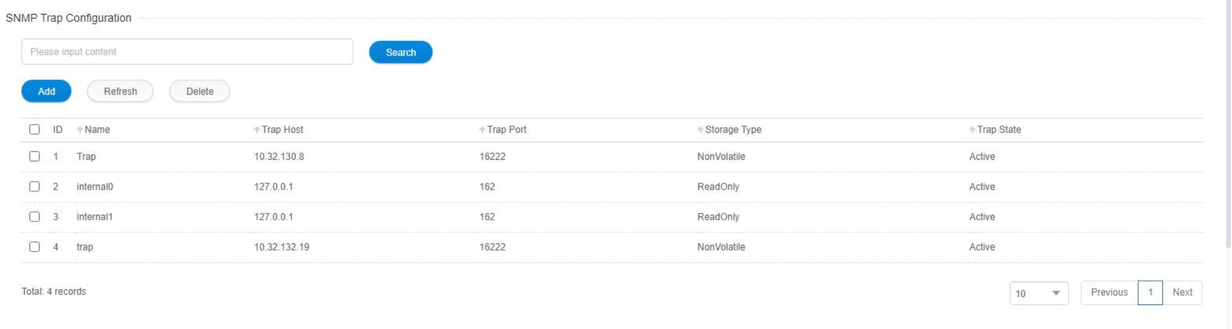
Figure 9-2 NE Single Board State

9.2.4. Check Alarm

M Series 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

Click the current network element and select *"Server Configuration"*-->*"SNMP Trap Configuration"* to check if there is a trap address on the same network segment as the managed server. If no configuration, please add the trap address in time to avoid the network element alarm cannot be reported in time. Click the "Add" button to add the trap address, the default trap port is 16222.



SNMP Trap Configuration

☐	ID	Name	Trap Host	Trap Port	Storage Type	Trap State
☐	1	Trap	10.32.130.8	16222	NonVolatile	Active
☐	2	internal0	127.0.0.1	162	ReadOnly	Active
☐	3	internal1	127.0.0.1	162	ReadOnly	Active
☐	4	trap	10.32.132.19	16222	NonVolatile	Active

Total: 4 records

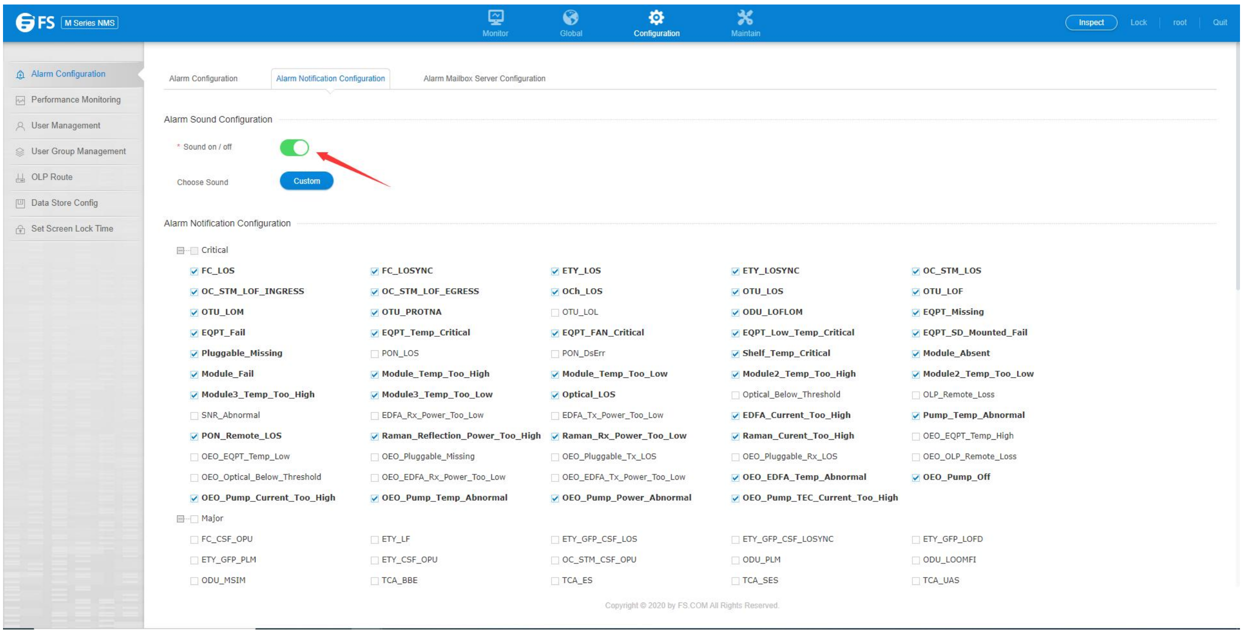
Figure 9-3 Trap Report Alarm

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:

Select *"Alarm Management"*-->*"Alarm Configuration Notification"*-->*"Sound on"*, as shown below.



Alarm Sound Configuration

* Sound on / off ●

Choose Sound: Custom

Alarm Notification Configuration

□ Critical

☑ FC_LOS	☑ FC_LOSYNC	☑ ETY_LOS	☑ ETY_LOSYNC	☑ OC_STM_LOS
☑ OC_STM_LOF_INGRESS	☑ OC_STM_LOF_EGRESS	☑ OCh_LOS	☑ OTU_LOS	☑ OTU_LOF
☑ OTU_LOM	☑ OTU_PROTNA	□ OTU_LOL	☑ ODU_LOFLOM	☑ EQPT_Missing
☑ EQPT_Fail	☑ EQPT_Temp_Critical	☑ EQPT_FAN_Critical	☑ EQPT_Low_Temp_Critical	☑ EQPT_SD_Mounted_Fail
☑ Pluggable_Missing	□ PON_LOS	□ PON_DsErr	☑ Shelf_Temp_Critical	☑ Module_Absent
☑ Module_Fail	☑ Module_Temp_Too_High	☑ Module_Temp_Too_Low	☑ Module2_Temp_Too_High	☑ Module2_Temp_Too_Low
☑ Module3_Temp_Too_High	☑ Module3_Temp_Too_Low	☑ Optical_LOS	□ Optical_Below_Threshold	□ OLP_Remote_Loss
□ SNR_Abnormal	□ EDFA_Rx_Power_Too_Low	□ EDFA_Tx_Power_Too_Low	☑ EDFA_Current_Too_High	☑ Pump_Temp_Abnormal
☑ PON_Remote_LOS	☑ Raman_Reflection_Power_Too_High	☑ Raman_Rx_Power_Too_Low	☑ Raman_Curent_Too_High	□ OEO_EQPT_Temp_High
□ OEO_EQPT_Temp_Low	□ OEO_Pluggable_Missing	□ OEO_Pluggable_Tx_LOS	□ OEO_Pluggable_Rx_LOS	□ OEO_OLP_Remote_Loss
□ OEO_Optical_Below_Threshold	□ OEO_EDFA_Rx_Power_Too_Low	□ OEO_EDFA_Tx_Power_Too_Low	☑ OEO_EDFA_Temp_Abnormal	☑ OEO_Pump_Off
☑ OEO_Pump_Current_Too_High	☑ OEO_Pump_Temp_Abnormal	☑ OEO_Pump_Power_Abnormal	☑ OEO_Pump_TEC_Current_Too_High	

□ Major

□ FC_CSF_OPU	□ ETY_LF	□ ETY_GFP_CSF_LOS	□ ETY_GFP_CSF_LOSYNC	□ ETY_GFP_LOFD
□ ETY_GFP_PLM	□ ETY_CSF_OPU	□ OC_STM_CSF_OPU	□ ODU_PLM	□ ODU_LOOMFI
□ ODU_MSIM	□ TCA_BBE	□ TCA_ES	□ TCA_SES	□ TCA_UAS

Copyright © 2020 by FS.COM All Rights Reserved.

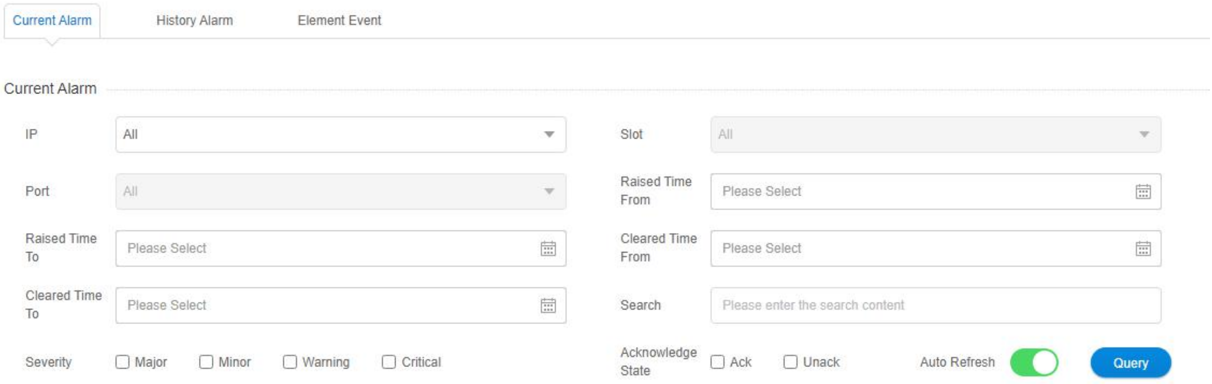
Figure 9-4 Enable Alarm Sound

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.



Current Alarm

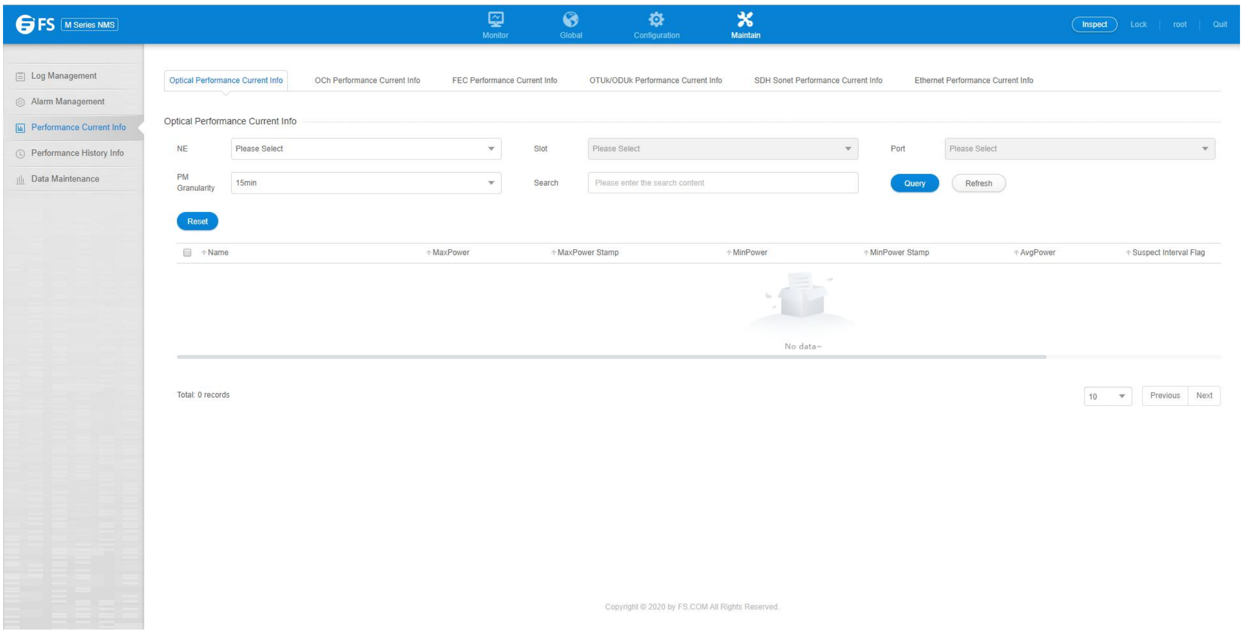
IP	All	Slot	All
Port	All	Raised Time From	Please Select
Raised Time To	Please Select	Cleared Time From	Please Select
Cleared Time To	Please Select	Search	Please enter the search content
Severity	□ Major □ Minor □ Warning □ Critical	Acknowledge State	□ Ack □ Unack

Auto Refresh ● Query

Figure 9-5 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.



Optical Performance Current Info

NE: Please Select
Slot: Please Select
Port: Please Select
PM Granularity: 15min
Search: Please enter the search content

Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag

No data~

Total: 0 records

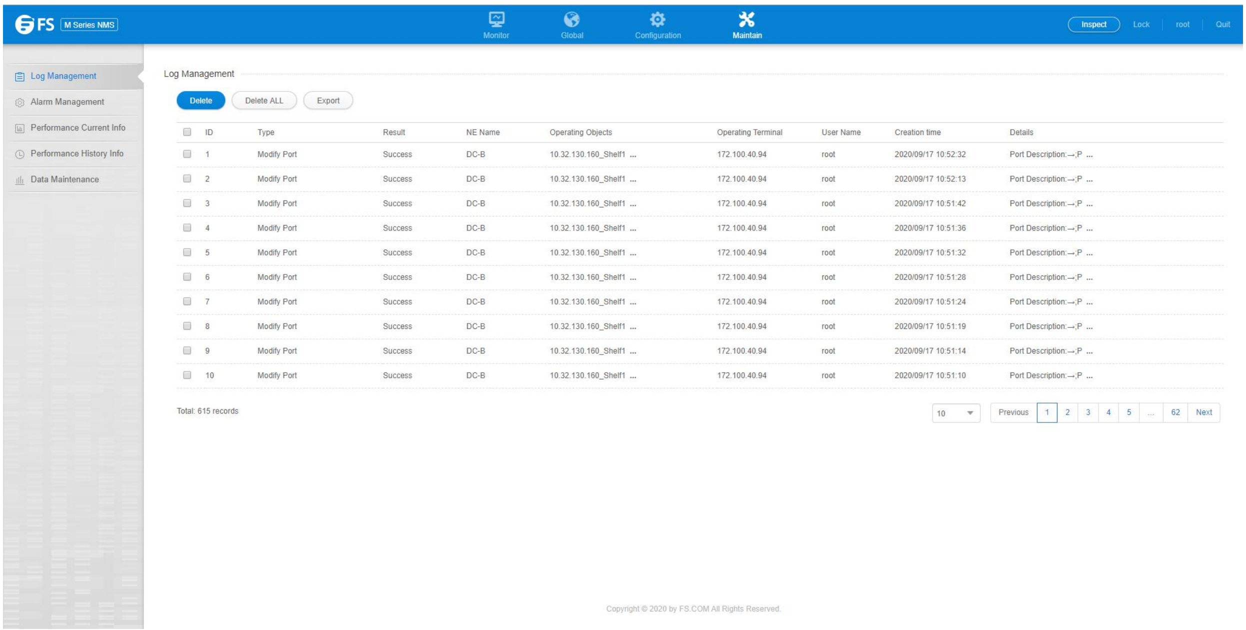
Copyright © 2020 by FS.COM All Rights Reserved.

Figure 9-6 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.



Log Management

□	ID	Type	Result	NE Name	Operating Objects	Operating Terminal	User Name	Creation time	Details
□	1	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:52:32	Port Description:→;P ...
□	2	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:52:13	Port Description:→;P ...
□	3	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:42	Port Description:→;P ...
□	4	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:36	Port Description:→;P ...
□	5	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:32	Port Description:→;P ...
□	6	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:28	Port Description:→;P ...
□	7	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:24	Port Description:→;P ...
□	8	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:19	Port Description:→;P ...
□	9	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:14	Port Description:→;P ...
□	10	Modify Port	Success	DC-B	10.32.130.160_Shelf1 ...	172.100.40.94	root	2020/09/17 10:51:10	Port Description:→;P ...

Total: 615 records

Copyright © 2020 by FS.COM All Rights Reserved.

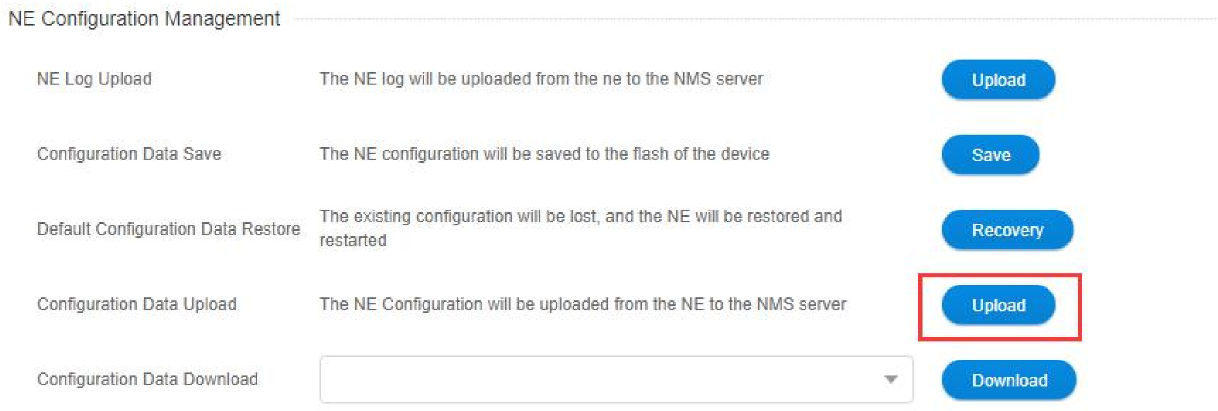
Figure 9-7 Log Query

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.

Select *"NE Configuration"*-->*"NE Configuration Management"* to upload all the configuration of the element to the network management server.



NE Configuration Management

NE Log Upload	The NE log will be uploaded from the ne to the NMS server	Upload
Configuration Data Save	The NE configuration will be saved to the flash of the device	Save
Default Configuration Data Restore	The existing configuration will be lost, and the NE will be restored and restarted	Recovery
Configuration Data Upload	The NE Configuration will be uploaded from the NE to the NMS server	Upload
Configuration Data Download		Download

Figure 9-8 Upload NE Configuration

9.2.8. Use One-Click Inspection

Use the one-click inspection function to export the information of all network elements on the network management to PDF files, so that it is easy to view the basic information, optical power, alarms and other related information of all network element devices, and it is convenient to check the abnormal status devices. (Refer to Section 4.6.11)

9.3. Monthly Routine Maintenance

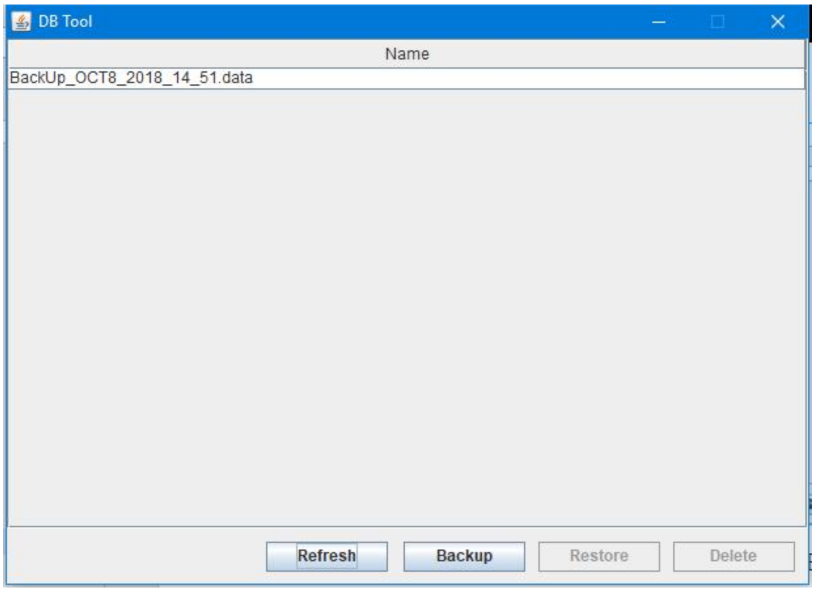
Table 9-2 Items of Monthly Routine Maintenance

Maintenance Items	Requirements
Data Backup	Make data backup to avoid loss of important data caused by mis-operation.
Performance Acquisition	Check whether the NE performance acquisition is correctly set.
History Alarm & Performance Backup	The history alarm and performance data needs to be backed up and archived.
Check the Connection of the Database	Close M Series interface and then log back to M Series to check whether the connection of the database is normal.

9.3.1. Data Backup

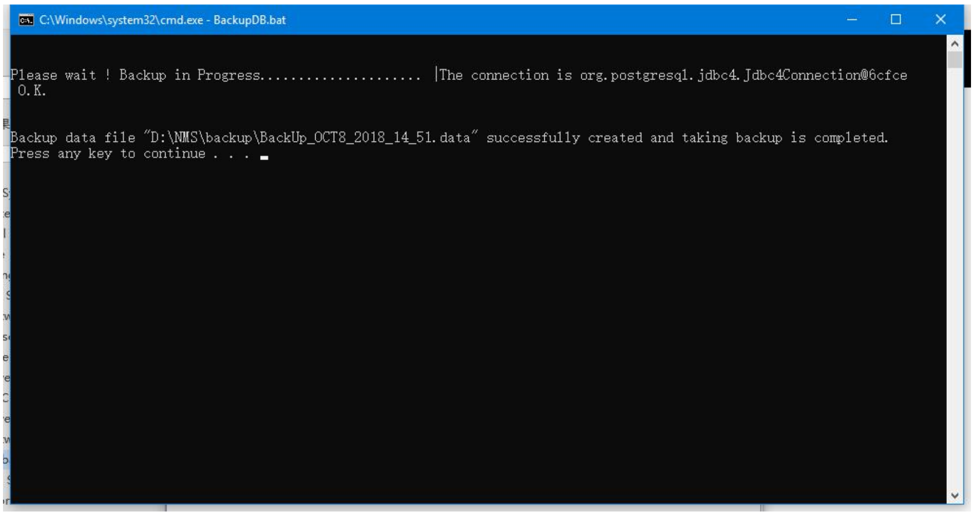
NMS Data Backup

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.



BackUp_OCT8_2018_14_51.data

Figure 9-9 DB Tool

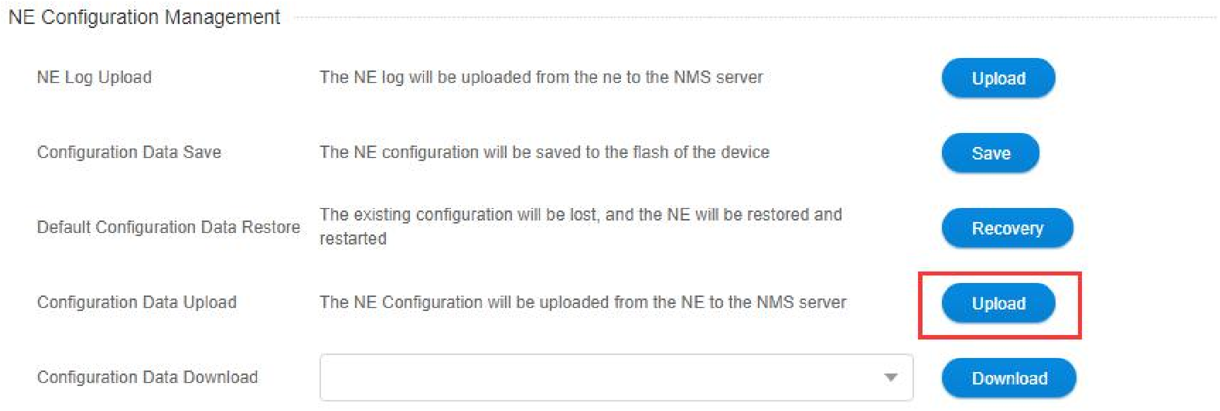


```
Please wait ! Backup in Progress.................... |The connection is org.postgresql.jdbc4.Jdbc4Connection@6cfce
 O.K.

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 9-10 NMS Data Backup

NE Data Backup

Select *"NE Configuration"*-->*"NE Configuration Management"* to upload all the configuration of the element to the network management server.


NE Configuration Management

NE Log Upload — The NE log will be uploaded from the ne to the NMS server

Configuration Data Save — The NE configuration will be saved to the flash of the device

Default Configuration Data Restore — The existing configuration will be lost, and the NE will be restored and restarted

Configuration Data Upload — The NE Configuration will be uploaded from the NE to the NMS server

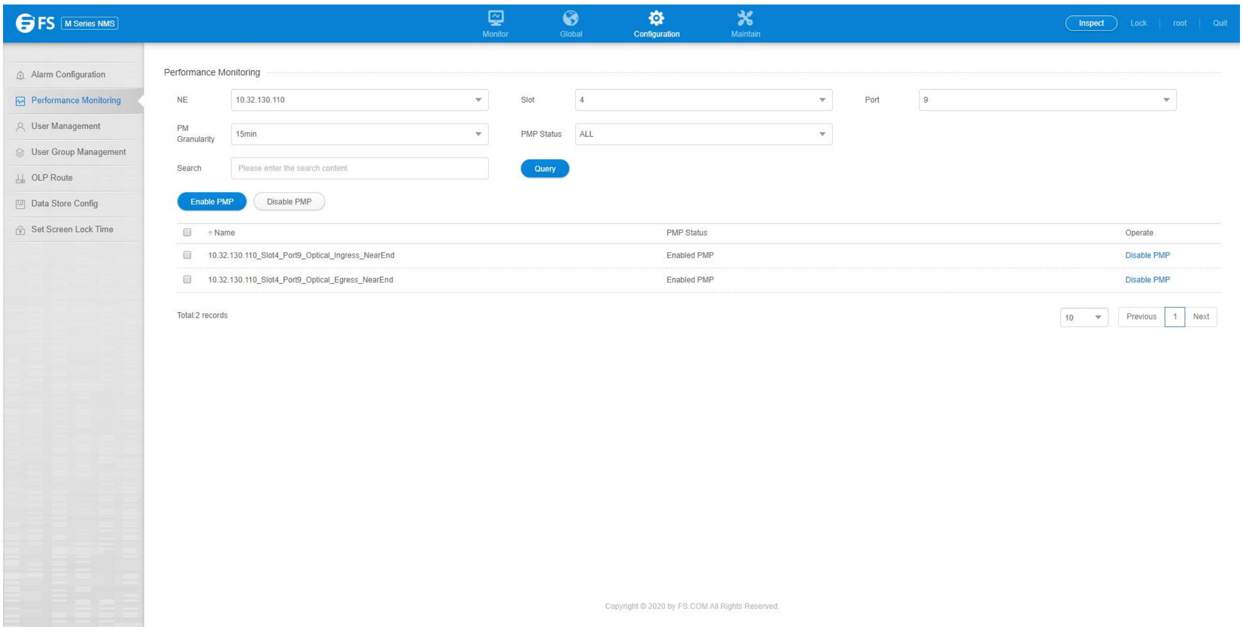
Configuration Data Download

Figure 9-11 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 *"Configuration"*--->*"Performance Monitoring"*, then the Performance Monitoring Point page will pop up as shown in the figure below.



Performance Monitoring

NE: 10.32.130.110 | Slot: 4 | Port: 9

PM Granularity: 15min | PMP Status: ALL

Search: Please enter the search content | Query

Enable PMP | Disable PMP

☐	Name	PMP Status	Operate
☐	10.32.130.110_Slot4_Port9_Optical_Ingress_NearEnd	Enabled PMP	Disable PMP
☐	10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	Enabled PMP	Disable PMP

Total:2 records

Copyright © 2020 by FS.COM All Rights Reserved.

Figure 9-12 Performance Monitoring Point

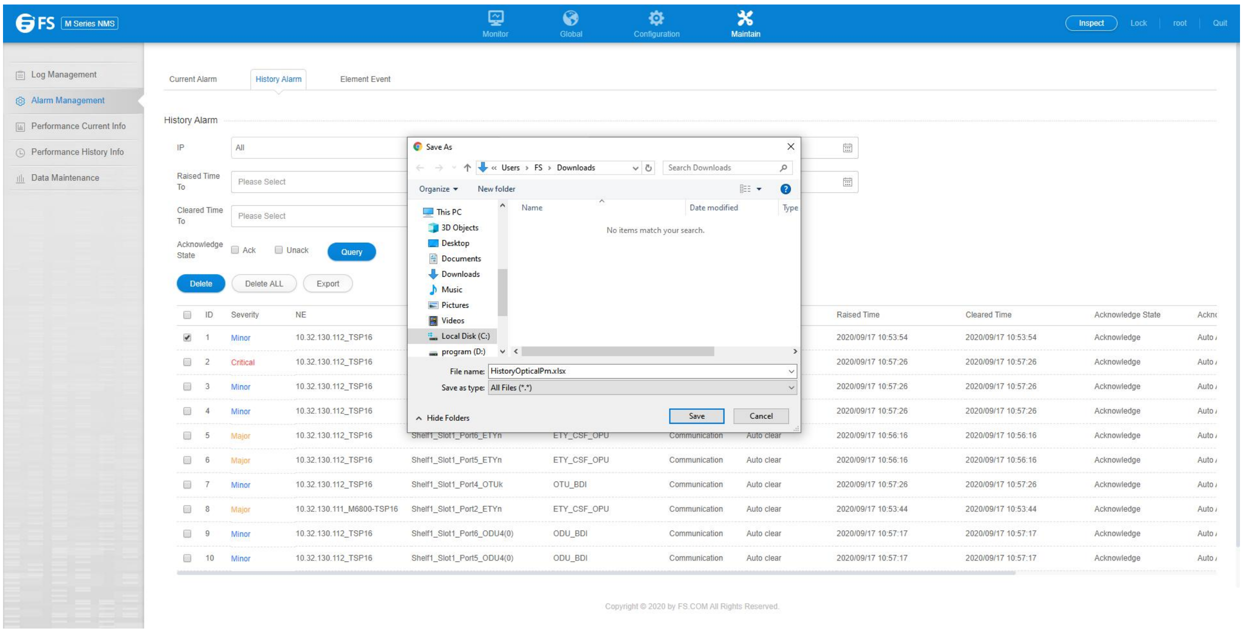
Check whether all the ports which need to collect performance data enable the performance monitoring point.

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).



History Alarm

IP: All

Raised Time To: Please Select

Cleared Time To: Please Select

Acknowledge State: ☐ Ack ☐ Unack | Query

Delete | Delete ALL | Export

No items match your search.

File name: HistoryOpticalPm.xlsx

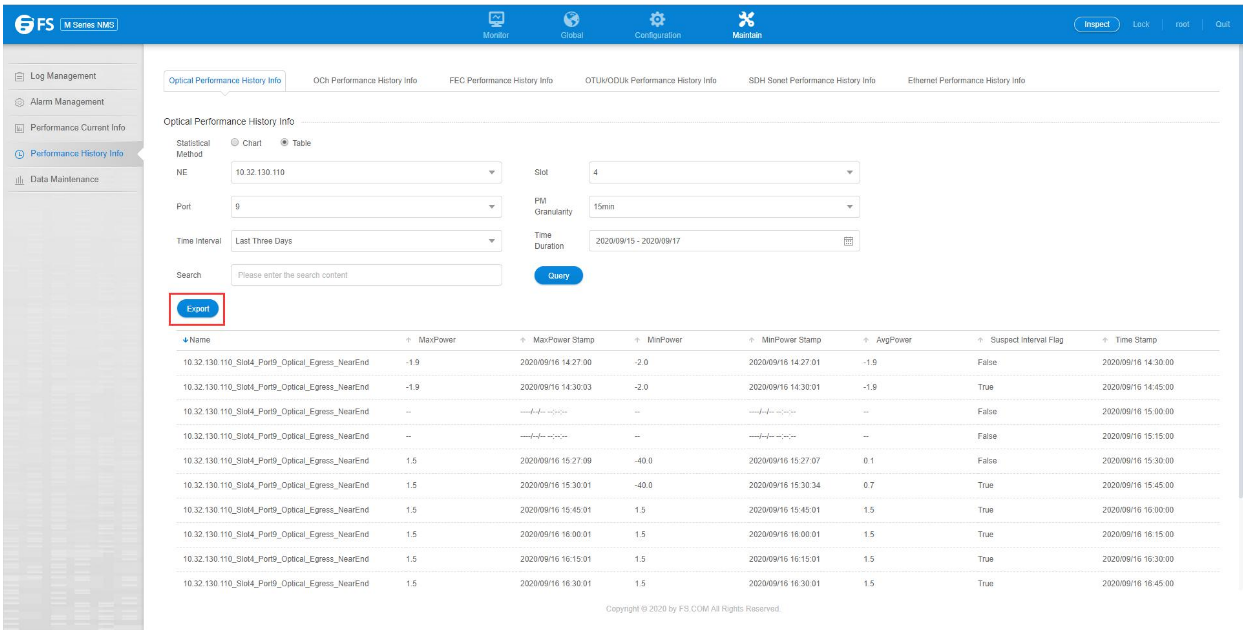
Save as type: All Files (*.*)

☐	ID	Severity	NE					Raised Time	Cleared Time	Acknowledge State	Ackn
☑	1	Minor	10.32.130.112_TSP16					2020/09/17 10:53:54	2020/09/17 10:53:54	Acknowledge	Auto
☐	2	Critical	10.32.130.112_TSP16					2020/09/17 10:57:26	2020/09/17 10:57:26	Acknowledge	Auto
☐	3	Minor	10.32.130.112_TSP16					2020/09/17 10:57:26	2020/09/17 10:57:26	Acknowledge	Auto
☐	4	Minor	10.32.130.112_TSP16					2020/09/17 10:57:26	2020/09/17 10:57:26	Acknowledge	Auto
☐	5	Major	10.32.130.112_TSP16	Shelf1_Slot1_Port6_ETYn	ETY_CSF_OPU	Communication	Auto clear	2020/09/17 10:56:16	2020/09/17 10:56:16	Acknowledge	Auto
☐	6	Major	10.32.130.112_TSP16	Shelf1_Slot1_Port5_ETYn	ETY_CSF_OPU	Communication	Auto clear	2020/09/17 10:56:16	2020/09/17 10:56:16	Acknowledge	Auto
☐	7	Minor	10.32.130.112_TSP16	Shelf1_Slot1_Port4_OTUk	OTU_BDI	Communication	Auto clear	2020/09/17 10:57:26	2020/09/17 10:57:26	Acknowledge	Auto
☐	8	Major	10.32.130.111_M6800-TSP16	Shelf1_Slot1_Port2_ETYn	ETY_CSF_OPU	Communication	Auto clear	2020/09/17 10:53:44	2020/09/17 10:53:44	Acknowledge	Auto
☐	9	Minor	10.32.130.112_TSP16	Shelf1_Slot1_Port6_ODU4(0)	ODU_BDI	Communication	Auto clear	2020/09/17 10:57:17	2020/09/17 10:57:17	Acknowledge	Auto
☐	10	Minor	10.32.130.112_TSP16	Shelf1_Slot1_Port5_ODU4(0)	ODU_BDI	Communication	Auto clear	2020/09/17 10:57:17	2020/09/17 10:57:17	Acknowledge	Auto

Copyright © 2020 by FS.COM All Rights Reserved.

Figure 9-13 Export History Alarm Data

Select *"Maintain"*-->*"Performance History Info"*, click the *"Export"* button to export the historical performance statistics to the custom directory of the network management server.


FS M Series NMS
Monitor
Global
Configuration
Maintain
Inspect
Lock
root
Quit
Log Management
Alarm Management
Performance Current Info
Performance History Info
Data Maintenance
Optical Performance History Info
OCh Performance History Info
FEC Performance History Info
OTUk/ODUk Performance History Info
SDH Sonet Performance History Info
Ethernet Performance History Info
Query
Export

Optical Performance History Info

Statistical Method: ○ Chart ● Table

NE: 10.32.130.110

Slot: 4

Port: 9

PM Granularity: 15min

Time Interval: Last Three Days

Time Duration: 2020/09/15 - 2020/09/17

Search: Please enter the search content

Name	MaxPower	MaxPower Stamp	MinPower	MinPower Stamp	AvgPower	Suspect Interval Flag	Time Stamp
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	-1.9	2020/09/16 14:27:00	-2.0	2020/09/16 14:27:01	-1.9	False	2020/09/16 14:30:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	-1.9	2020/09/16 14:30:03	-2.0	2020/09/16 14:30:01	-1.9	True	2020/09/16 14:45:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:00:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	--	----/--/-- --:--:--	--	----/--/-- --:--:--	--	False	2020/09/16 15:15:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 15:27:09	-40.0	2020/09/16 15:27:07	0.1	False	2020/09/16 15:30:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 15:30:01	-40.0	2020/09/16 15:30:34	0.7	True	2020/09/16 15:45:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 15:45:01	1.5	2020/09/16 15:45:01	1.5	True	2020/09/16 16:00:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 16:00:01	1.5	2020/09/16 16:00:01	1.5	True	2020/09/16 16:15:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 16:15:01	1.5	2020/09/16 16:15:01	1.5	True	2020/09/16 16:30:00
10.32.130.110_Slot4_Port9_Optical_Egress_NearEnd	1.5	2020/09/16 16:30:01	1.5	2020/09/16 16:30:01	1.5	True	2020/09/16 16:45:00

Copyright © 2020 by FS.COM All Rights Reserved.

Figure 9-14 Export History Performance Statistics Data

9.3.5. Check Connection of Database

Close M Series 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 9-3 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.

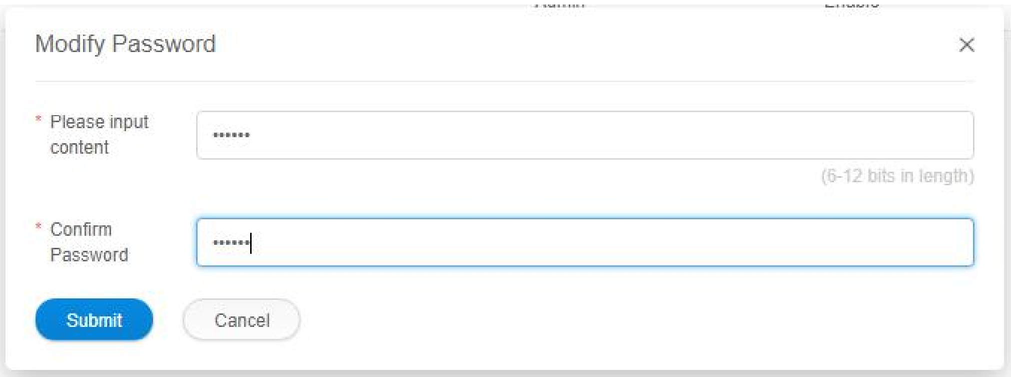
9.4.1. Proofread NMS Time

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 "*User Management*" menu, change the login user password, change the new password, click *"Submit "*, the network management system will automatically exit, the user uses a new user name or password to log in.



Modify Password

* Please input content: ••••••

(6-12 bits in length)

* Confirm Password: ••••••

Figure 9-15 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

Whether the alarm and performance can be obtained; whether the new alarm can be refreshed automatically; whether the network element and board can be clicked; if the sound card is installed, whether each alarm sound can be obtained normally; whether the state of the single board is normal. These maintenance items are also routine maintenance items, please refer to the first three sections of this chapter; Routine Maintenance Items for more details.

10. Common Problems

This chapter introduces some problems and their solutions while using M Series 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

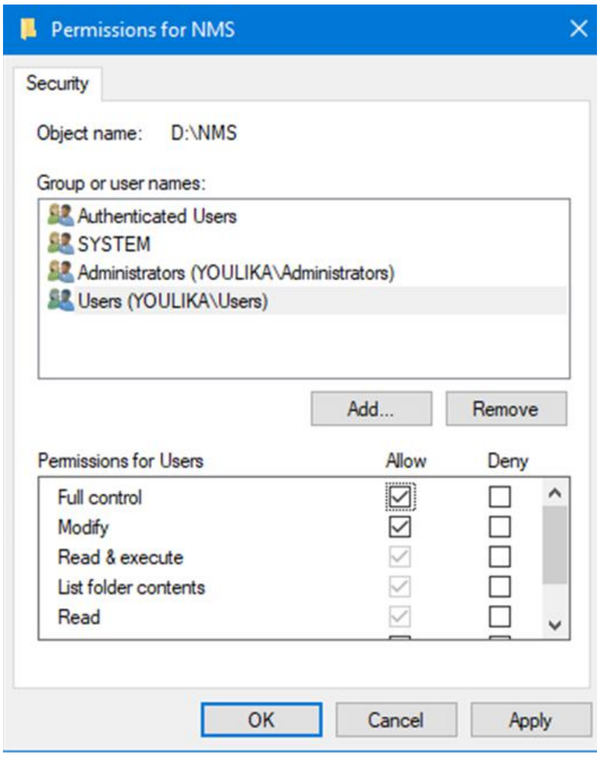
There are two possible reasons:

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 10-1 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 *"Server Configuration"* → *"NTP Configuration"* to configure server IP address.

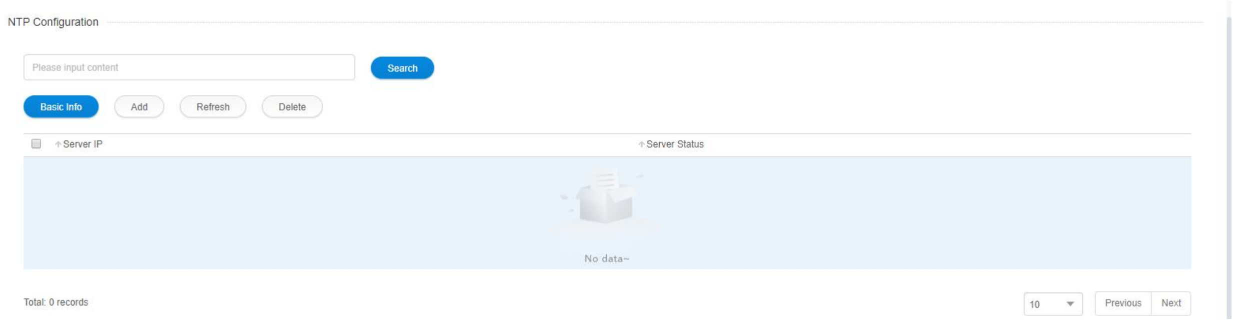
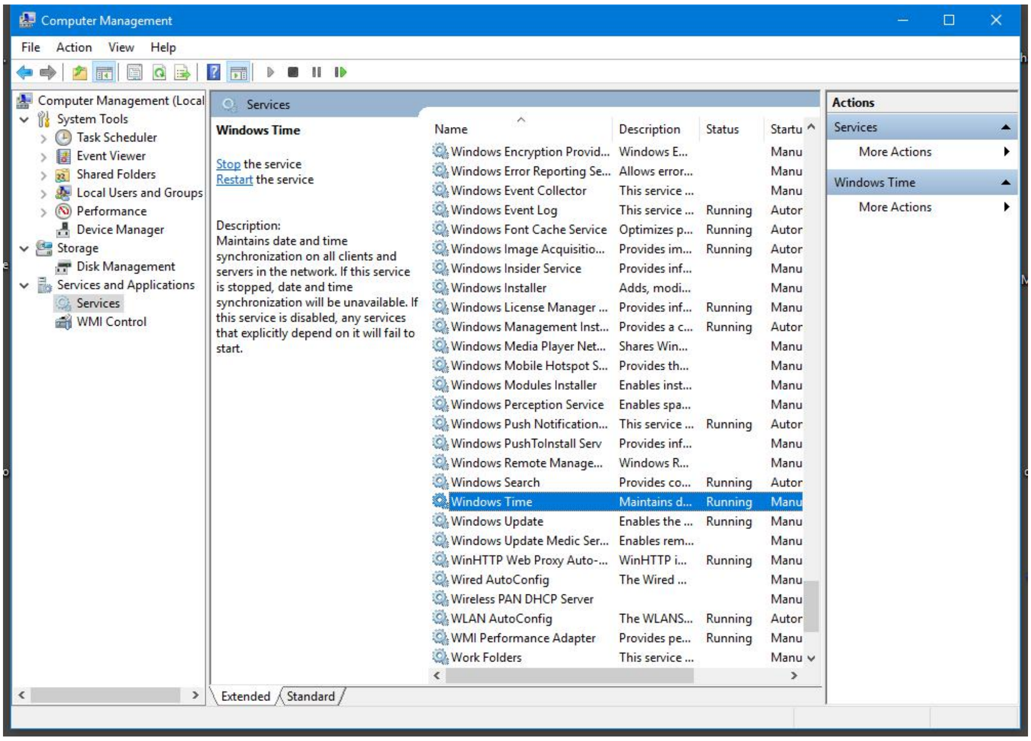


Figure 10-2 NTP Configuration

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



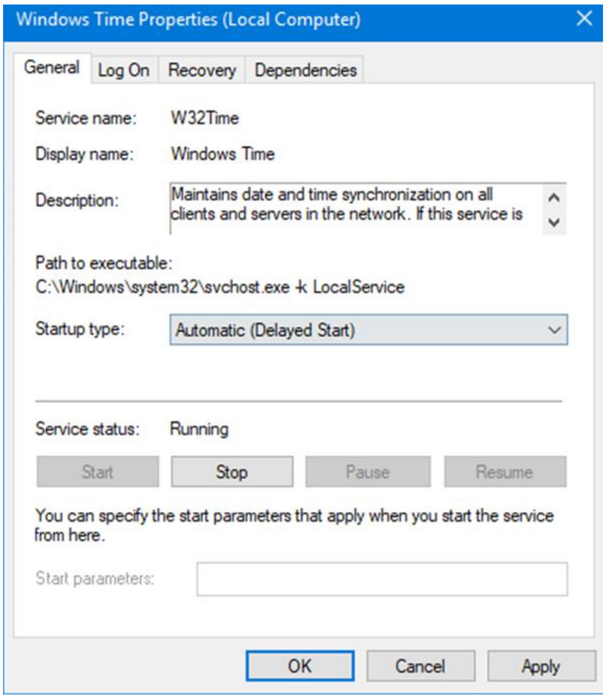
Windows Time

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 10-3 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 10-4 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.

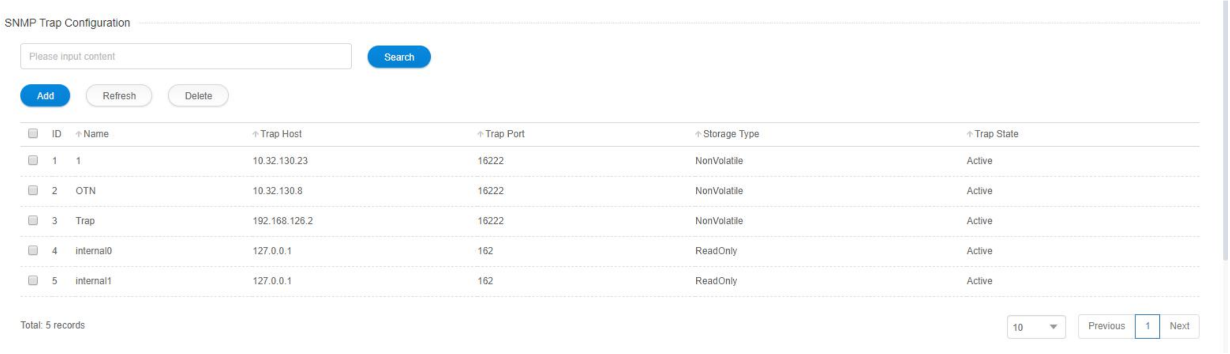
2. There is a firewall blocking on the computer that installs NMS server.

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

Please input content

☐	ID	Name	Trap Host	Trap Port	Storage Type	Trap State
☐	1	1	10.32.130.23	16222	NonVolatile	Active
☐	2	OTN	10.32.130.8	16222	NonVolatile	Active
☐	3	Trap	192.168.126.2	16222	NonVolatile	Active
☐	4	internal0	127.0.0.1	162	ReadOnly	Active
☐	5	internal1	127.0.0.1	162	ReadOnly	Active

Total: 5 records

Figure 10-5 NTP Server Startup Type Configuration

10.7. Network elements cannot report performance statistics

Possible causes.

1. The performance monitoring point of the specified port is not open or was open before, and it is closed due to misoperation.

2. The number of open performance monitoring points exceeds the limit.

3. FTP address is not configured correctly.

Possible cause: the performance monitoring points on the specified ports are open, if they are closed, you need to open them again.

Possible cause: the maximum number of performance monitoring points of a device is 500, you need to close some ports to open the specified ports.

Possible cause 3 solution: Configure the correct FTP address (i.e. the IP address to communicate with the device).

10.8. After changing the IP address of the server PC, the running server cannot login or shuts down automatically.

Possible Reason: When the NMS software is running on the back end of the network management server, modifying the IP address of the server will cause the NMS application on the back end of the network management server to fail to take effect on the newly modified IP address or cause the NMS application on the back end of the network management server to shut down automatically, as the network management client browser cannot log in (display user name and password error) to the network management server.

Solution: After changing the IP address of the managed server, you need to manually close the NMS application on the managed server, and then you need to manually restart the NMS application to make the newly modified IP address take effect on the NMS application.

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