Core Network OMC Operation Manual

Contents

1 About this manual

This manual is the 5G core network management manual, mainly describing the system's software and hardware environment, system functions, operation guides, common problems and solutions. The manual can provide guidance for network management in terms of maintenance, status monitoring, element configuration, abnormal alarms, statistical reports, and other related operations.

Abbreviations

abbreviation	English explanation
OMC	Operations & Maintenance Centre
NFV	Network Function Virtualization
VNF	Virtualized Network Function
PNF	Physical Network Function
GUI	Graphic User Interface
IMS	IP Multi-media Subsystem
CS	Circuit Switched
DRA	Diameter Routing Agent
VoLTE	Voice over LTE
TCE	Trace Collection Entity
EPC	Evolved Packet Core
NB-IOT	Narrow Band Internet of Things
SMSC	Short Message Service Center
MMSC	Multimedia Messaging Service Center
IP-SM-GW	IP-Short Message-Gateway
ISMG	Internet Short Message Gateway
SCP	Service Control Point
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
AMF	Access and Mobility Management Function
SMF	Session Management Function
UPF	User Plane Function
UDM	Unified Data Management
AUSF	Authentication Server Function
PCF	Policy Control Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
IWF	Interworking Function
NSSMF	Network Slice Subnet Management Function
5GMC	5G Message Center

1.1 Hardware Environment

5GC and network management support physical machine, local virtualization or cloud deployment, the following is a basic function of the 5GC core network (support

multiple base stations) hardware specifications recommended:

NF	Memory(G)	Hard disk(G)	Vcpu	Remark
AMF	4	100	4	
SMF	4	100	4	
AUSF	4	100	4	
UDM	4	100	4	
UPF	8	100	8	
PCF	4	100	4	
NSSF	4	100	4	
NRF	4	100	4	
OMC	8	100	4	

The Dell PowerEdge R640 server is recommended and the specifications are as follows：

Configuration	Specification	Quantity
CPU	24 cores x Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz	>=20
Memory	2666MT/s RDIMMs	64G
Hard disk	10K RPM SAS 12Gbps 512n 2.5-inch hot swappable hard disk	2TB*2
Network card	Intel Ethernet I350 QP 1Gb network sub card	1
Video interface	Front: Video, 1 x USB2.0 interface, USB3.0 available, dedicated iDRAC Direct USB Rear: Video, serial port, 2 x USB3.0, dedicated waiting network port	1

1.2 Software Environment

The system runs on VMWare ESXi + Linux VMs.

1.3 Software Installation

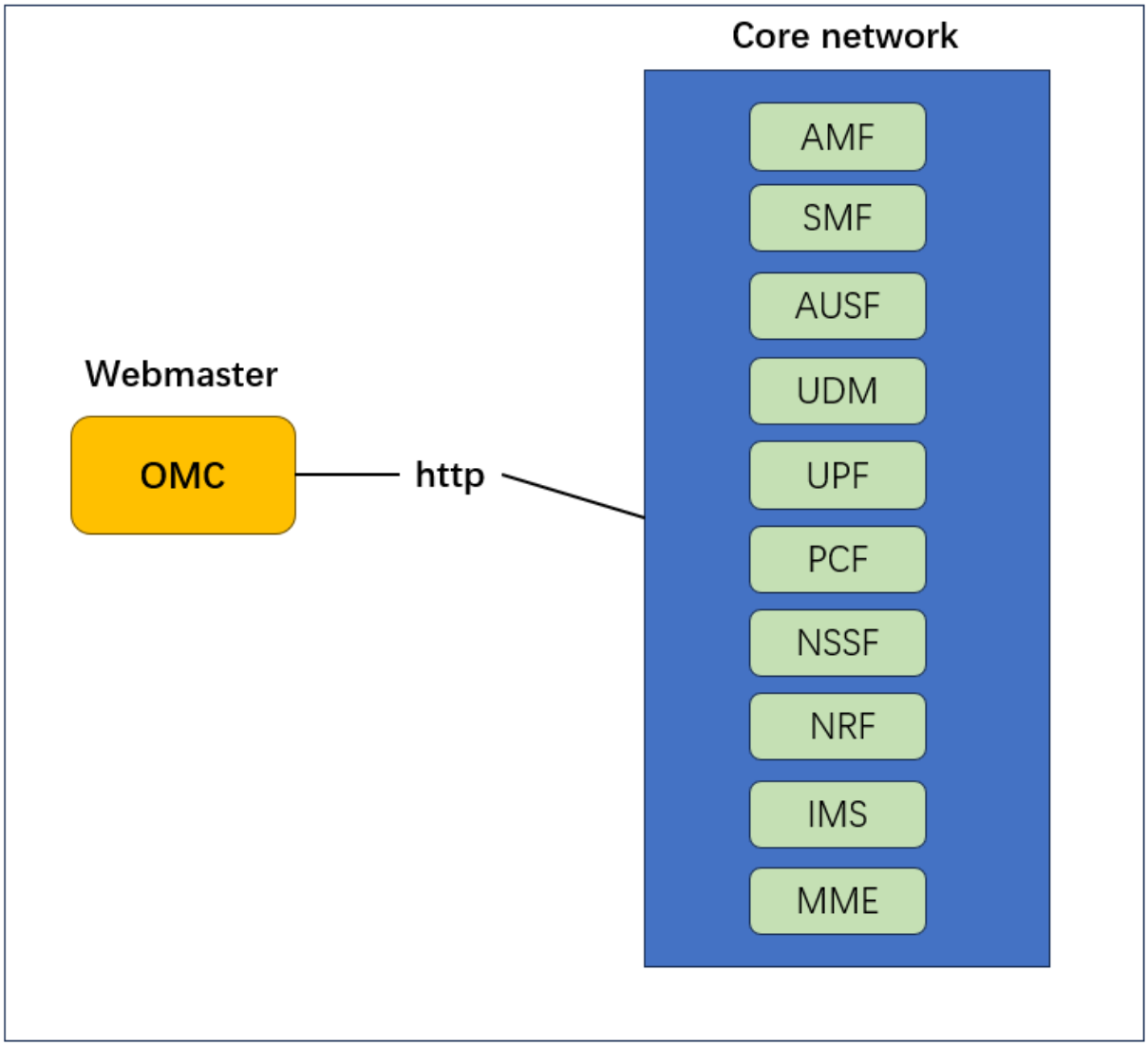
The software is shipped with the hardware and has been installed and tested before the delivery, or you can check the installation guide from OMC User Manual

1.4 Software Uninstallation

You can check the uninstallation guide from OMC User Manual

2 System functions

2.1 Overall architecture of the system core network



The information exchange between network management and 5GC network elements is mainly achieved through the HTTP protocol.

2.2 Function Introduction

1. OMC network management function

Management and maintenance, status monitoring, network element configuration, abnormal alarms, statistical reports, etc.

2. AMF functions

Complete mobility management, NAS MM signalling processing, NAS SM signalling routing, security context management, etc.

3. AUSF functions

Complete the authentication function for user access.

4. UDM functions

Manage and store subscription data and authentication data.

5. SMF functions

Complete session management, UE IP address allocation and management, UPF selection and control, etc

6. UPF functions

Complete the processing of different user planes.

7. PCF functions

Support the development of a unified policy framework and provide policy rules.

8. NRF functions

Support service discovery function, receive NF discovery requests from NF instances, and provide the information of the discovered NF instance to another NF instance for policy rules.

9. NSSF functions

Support network slicing selection function.

10. IMS functions

Support multimedia functional requirements.

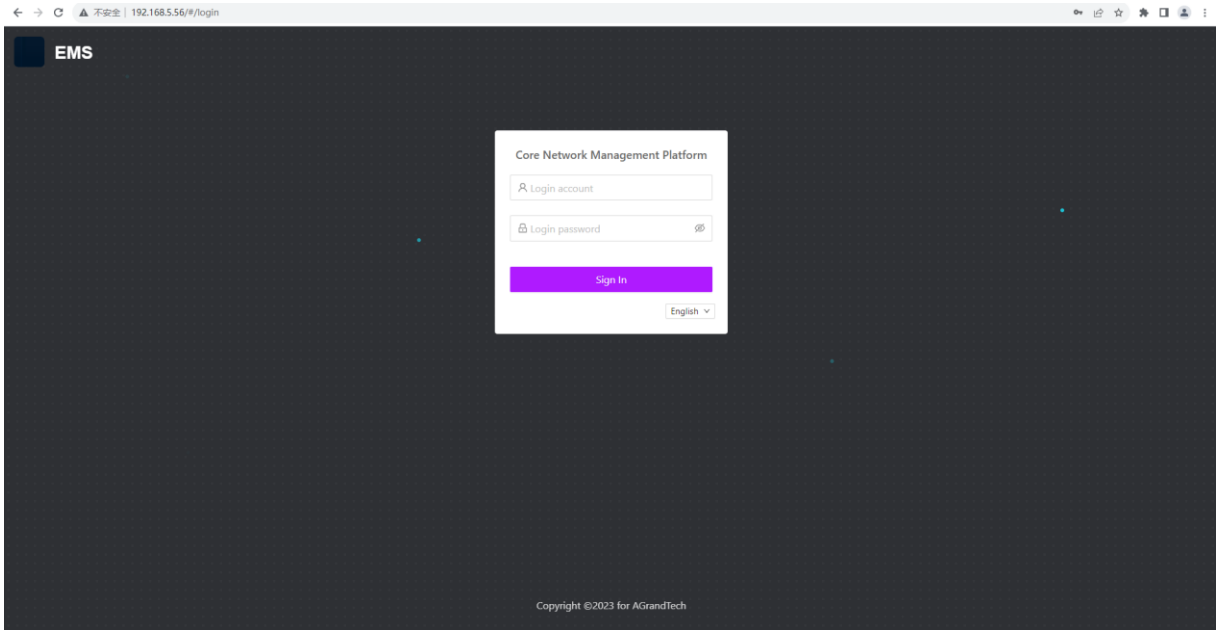
11. MME functions

It is the network element of the EPC core network control plane, responsible for the signalling processing part.

3 Operation Guide

3.1 Login to OMC

In the browser address bar, enter “http://<OMC Network Management IP>”to access the web management interface. The login interface is shown in the following figure

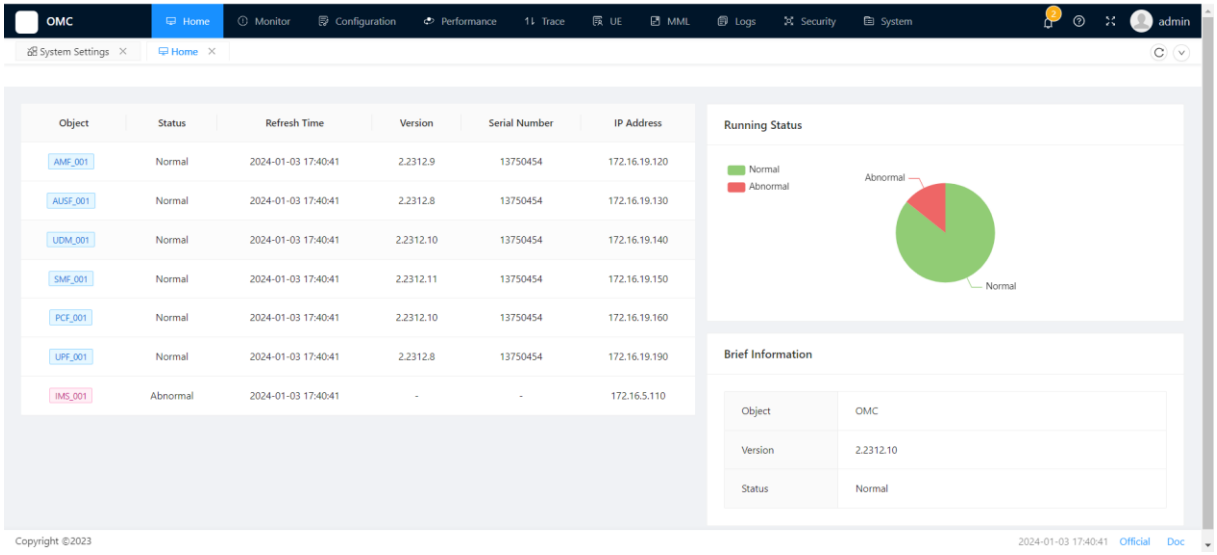


●Recommend using Google, Firefox browsers or Microsoft Edge

3.2 System Status：

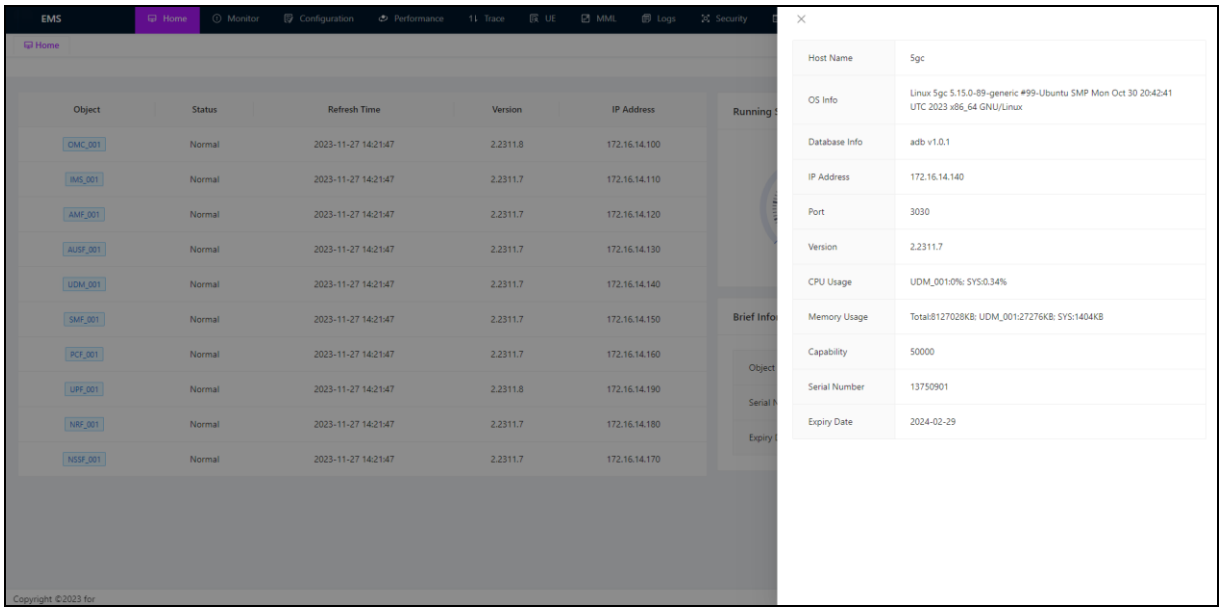
3.2.1 Network Element Status:

●After logging into the interface, the system status of all network elements will be automatically displayed, including element name and ID, running status, update time, version, license serial number and IP address:



●After clicking on the network element in the home page, the detailed information of the network element can be viewed on the right side of the window, such as CPU and memory usage and validity period, operating system, database, IP, port, user capacity etc.

The network element status display will refresh every 10 seconds:



3.3 Monitor

If there is a fault in the system or network element, OMC will immediately detect and report an alarm, generate corresponding level alarms based on the severity of the fault, and use different colours (customizable) and sounds to remind. After the fault is

eliminated, the corresponding alarm will also be automatically cleared in the historical alarm.

Alarm management enables O&M personnel to monitor and manage alarms or events reported by the system or NE. Alarm management provides various monitoring and handling rules and notifies O&M personnel of faults. In this way, network faults can be efficiently monitored, quickly located, and handled, ensuring proper service running.

The alarm severity indicates the severity, importance, and urgency of a fault. It helps O&M personnel quickly identify the importance of an alarm, take corresponding handling policies, and change the severity of an alarm as required.

Alarm severity

Alarm Severity	Default Color	Description	Handling Policy
Critical	Critical	Services are affected. Corrective measures must be taken immediately.	The fault must be rectified immediately. Otherwise, services may be interrupted or the system may break down.
Major	Major	Services are affected. If the fault is not rectified in a timely manner, serious consequences may occur.	Major alarms need to be handled in time. Otherwise, important services will be affected.
Minor	Minor	The impact on services is minor. Corrective measures are required to prevent serious faults.	You need to find out the cause of the alarm and rectify the fault.
Warning	Warning	Potential or imminent fault that affects services is detected, but services are not affected.	Warning alarms are handled based on network and NE running status.

Alarm status:

Status Name	Status	Description

Alarm Status	Confirm and Not Confirm	The initial alarm status is **Not Confirm**. A user who views a not confirm alarm and plans to handle it can confirm the alarm. When an alarm is confirmed, its status changes to Confirm. An confirmed alarm can be set to not confirm when the alarm is not handled temporarily but requires attention or other users will handle it. When an alarm is not confirmed, its status is restored to **Not Confirm**. Users can also configure auto confirm rules to automatically confirm alarms.
Clear Status	Cleared and Uncleared	The initial clearance status is **Uncleared**. When a fault that causes an alarm is rectified, a clearance notification is automatically reported to Alarm Management and the clearance status changes to **Cleared**. For some alarms, clearance notifications cannot be automatically reported. You need to manually clear these alarms after corresponding faults are rectified. The background color of cleared alarms is green.

Event Alarm Types

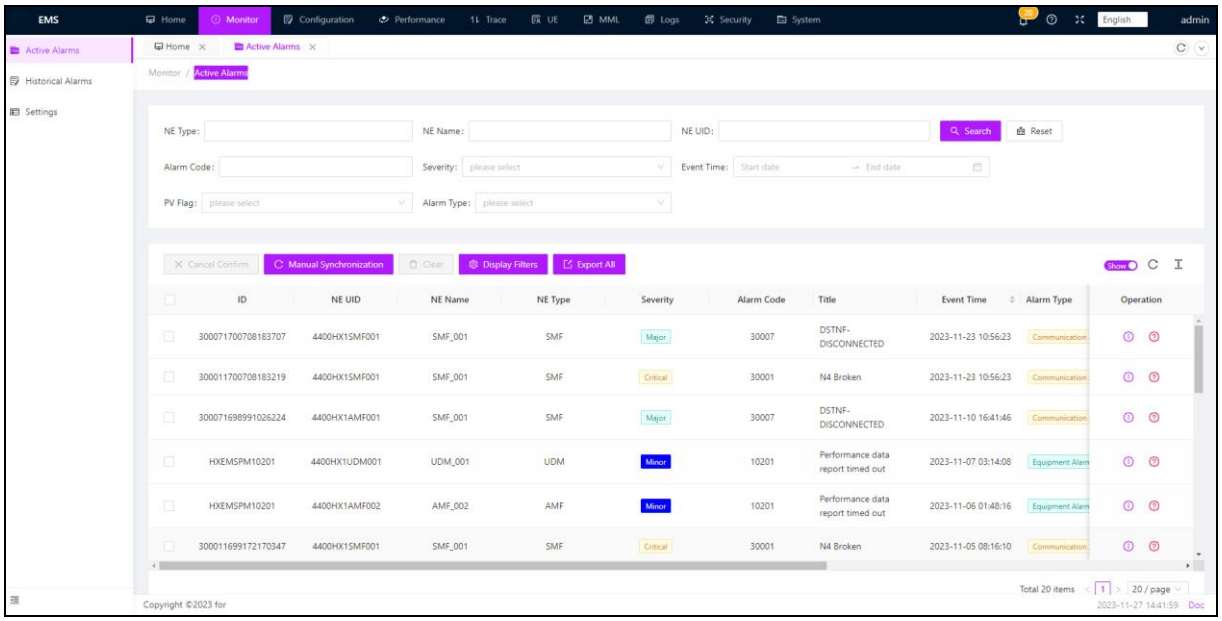
Name	Description
Communication Alarm	A fault on the communication system, such as a network cable disconnection or network equipment fault.
Equipment Alarm	A fault on the equipment
Processing Failure Alarm	An error or exception that occurs during processing, for example, the database is abnormal or the NE exits abnormally.
Environmental Alarm	A fault on the environment of the equipment room, such as a power supply fault or overheated CPU.
Quality of Service Alarm	It usually refers to the alarm of abnormal conditions that occur when the quality of service in the core network is monitored and managed.

3.3.1 Active Alarms

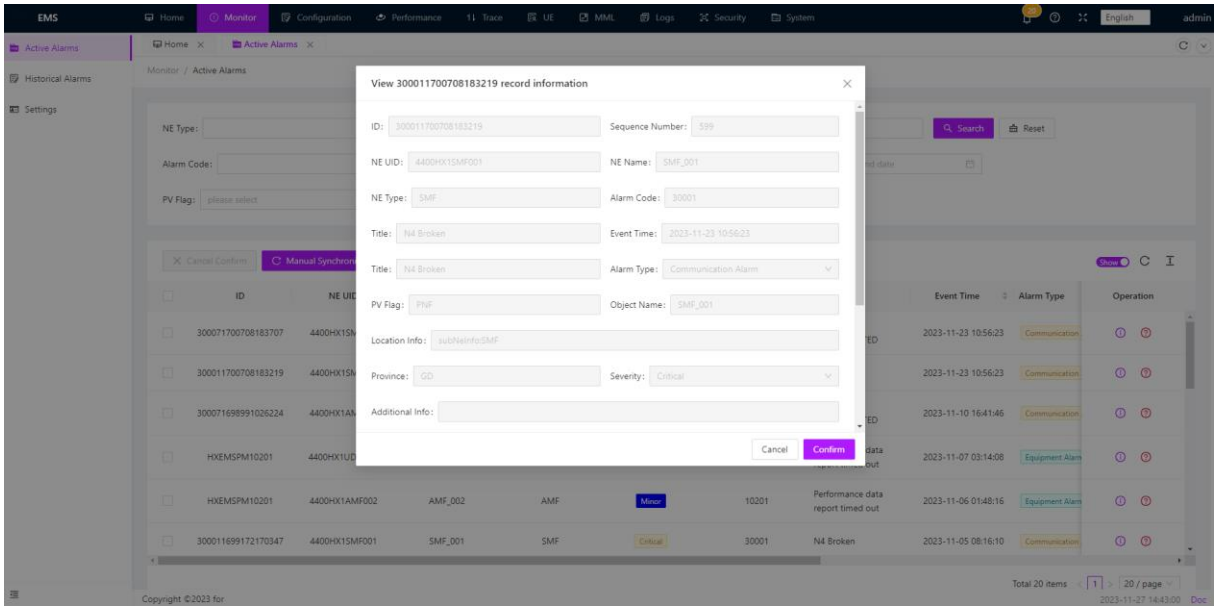
Active alarms include **Uncleared** and **Not Confirm** alarms, **Confirm** and **Uncleared** alarms, **Not Confirm** and **Cleared** alarms. When monitoring current alarms, you can identify faults in time, operate accordingly, and notify O&M personnel of these faults.

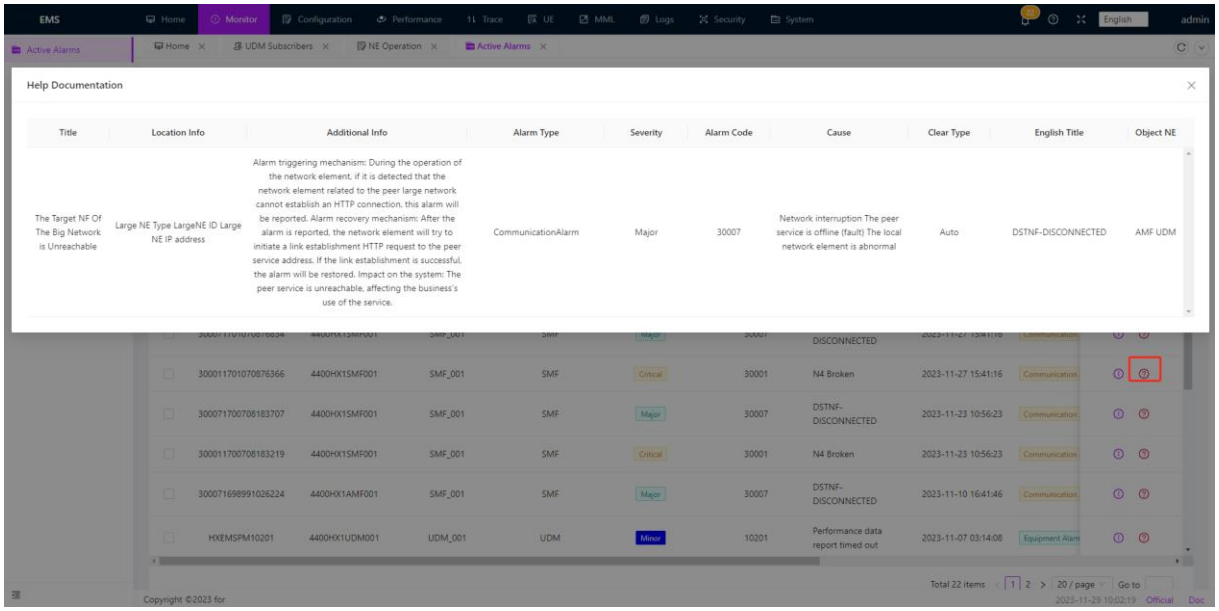
The operator can perform alarm search, filtering, automatic confirmation, export functions, and view detailed alarm information.

Current active alarm list：



Synchronously display the current number of active alarms in the upper right corner of the window; On the right side of each alarm, there is a detailed alarm information and relevant help documents for alarms.

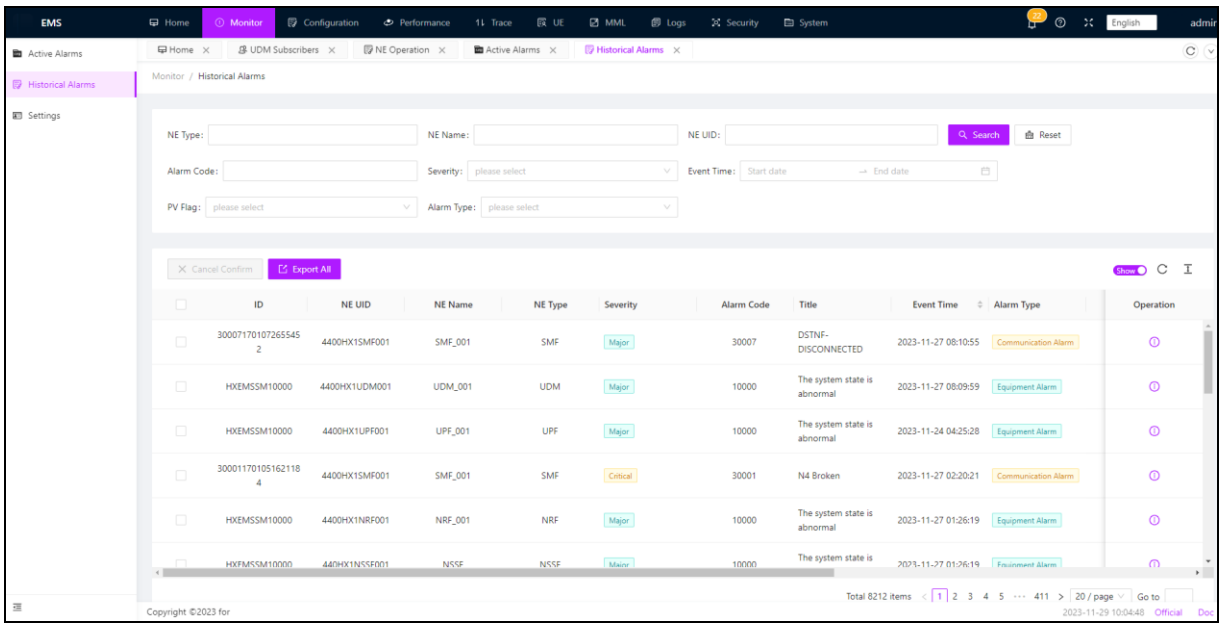


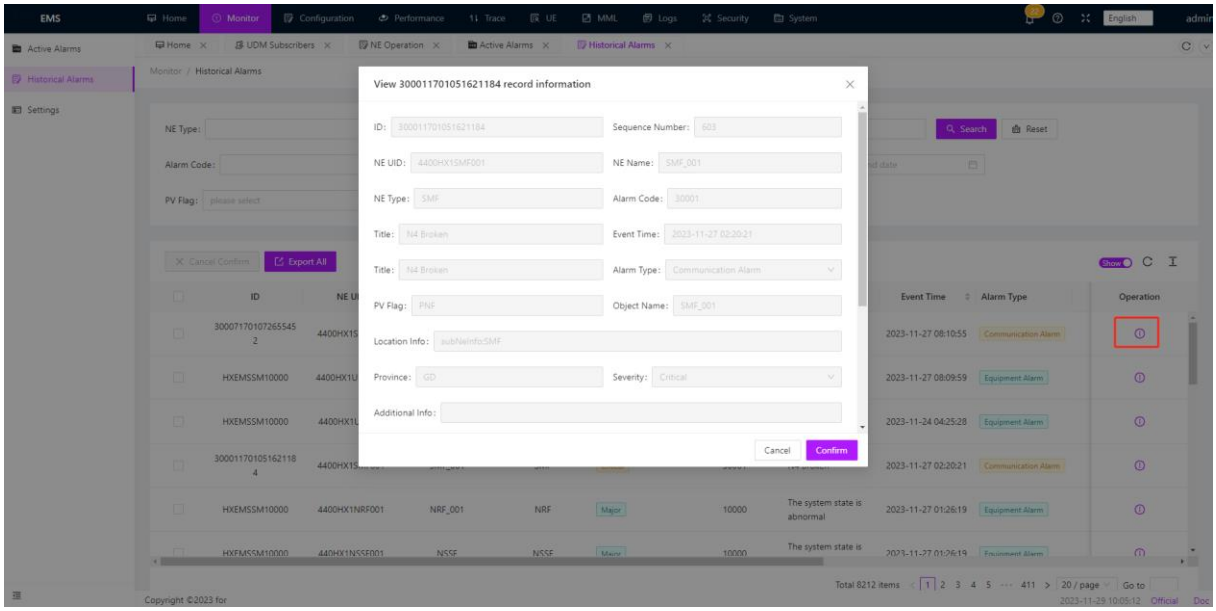


3.3.2 Historical Alarms

Confirm and Cleared alarms are historical alarms, Not Confirm and Cleared alarms are historical alarms also. You can analyze historical alarms to optimize system performance.

If you have set the current alarm lifecycle, the Confirm and Cleared alarms are displayed on the **Current Alarms** page for a period of time. After the lifecycle ends, the Confirm and Cleared alarms are moved to the historical alarm list.





3.3.3 Settings

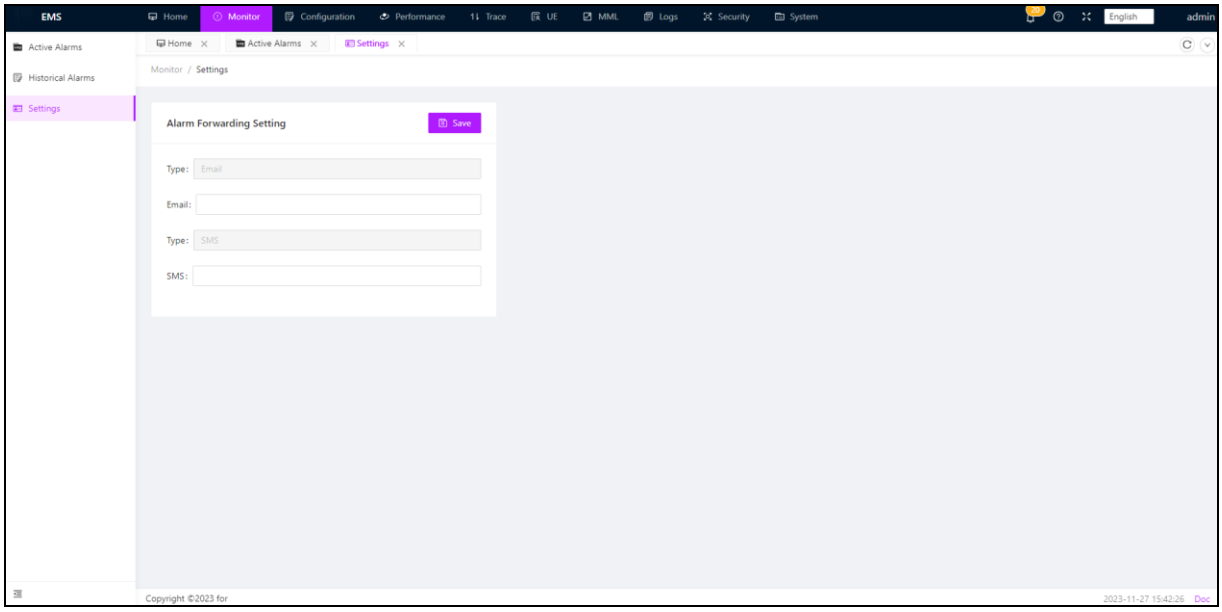
Alarm Forwarding is a technology and mechanism used to monitor and manage the core network. Core network equipment and systems need to maintain normal operation at all times to provide stable and efficient services. However, due to various reasons, such as equipment failure, network congestion, configuration errors, etc., the core network may experience abnormal conditions or failures.

The purpose of alarm forwarding on the core network is to discover and handle faults or exceptions on the core network in a timely manner to ensure network reliability and service continuity. When a device or system in the core network is faulty or abnormal, the device or system generates an alarm. Through the monitoring and detection of the alarm system, the alarm information can be automatically forwarded to the network operator or the technical personnel with network maintenance responsibilities, so that they can take measures to rectify the fault in time

Alarm forwarding on the core network is a key technology. By forwarding alarm information on the core network in a timely manner, the fault detection and handling efficiency can be improved to ensure the stable operation and service quality of the core network. It is essential for the normal operation of network operators and the good experience of users.

The operator can configure the alarm forwarding interface settings to redirect to the

target email before setting an alarm, which can be multiple target email addresses at the same time. As shown in the figure, fill in the email address for the alarm forwarding email.



3.4 Configuration

This document describes common configuration operations and how to view NE configuration information. This includes NE management, Parameter management, Backup management, Software management and License management.

3.4.1 NE Management

Network Element Management (NEM) is a key part of the core network management system. It's responsible for monitoring and controlling various network elements like AMF, SMF, UDM, PCF, AUSF, UPF, IMS, MME, NRF, NSSF, etc. Through NEM, operators can ensure the continuous and reliable operation of the network. NEM covers the entire lifecycle of network elements, including configuration, monitoring, maintenance, and optimization.

- Adding, deleting, and modifying network elements: The management system provides an intuitive user interface for operators to add new elements to expand the network or remove old elements when necessary. Users can use a graphical interface to architect the network through drag-and-drop components or use automation scripts for batch operations.

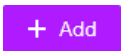
- Stopping, starting, and restarting operations: The OSS provides control to stop, start, and restart network devices. These operations are usually used for routine maintenance or applying new configurations. The management system includes security protocols and processes to ensure smooth operations and avoid unnecessary network interruptions.
- Importing and exporting network element configurations: Network administrators can export critical configuration files for backup and quickly recover in case of data loss or failure. Similarly, new configuration files can be imported into network elements for quick updates and deployment of new network settings. Import and export operations usually support standardized formats like XML or JSON for cross-platform configuration management.
- Modifying network element details: From internal identifiers, resource identifiers to vendor and location information, the management system makes it easy to modify and update these details. Changing the orientation, IP, ports, etc. can be done directly through the UI or through API for automation. It can also involve parameter adjustments to optimize network performance and capacity.

Administrators also need to pay attention to changes in information like network element names, physical addresses, and network identifiers to ensure the network map remains up to date. They can also set logical classifications like service provinces for network elements to achieve more detailed network management.

Additionally, with the development of Network Function Virtualization (NFV), the management system can differentiate between Physical Network Functions (PNF) and Virtual Network Functions (VNF) and manage them separately. This provides additional flexibility for network operations as VNFs can be rapidly deployed and scaled to adapt to changing traffic demands.

In summary, Network Element Management is an essential part of 5G core network management, ensuring that network infrastructure operates according to predetermined performance and efficiency standards.

The operation part is as follows:

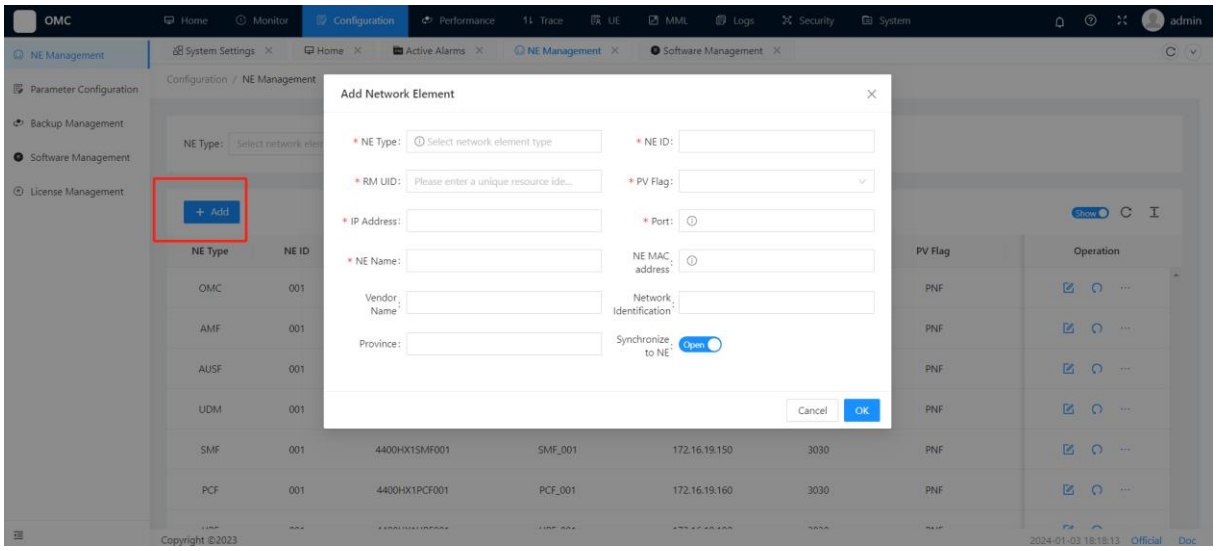
Click on 

to add the NE. The following parameters need to be consistent with the network element configuration:

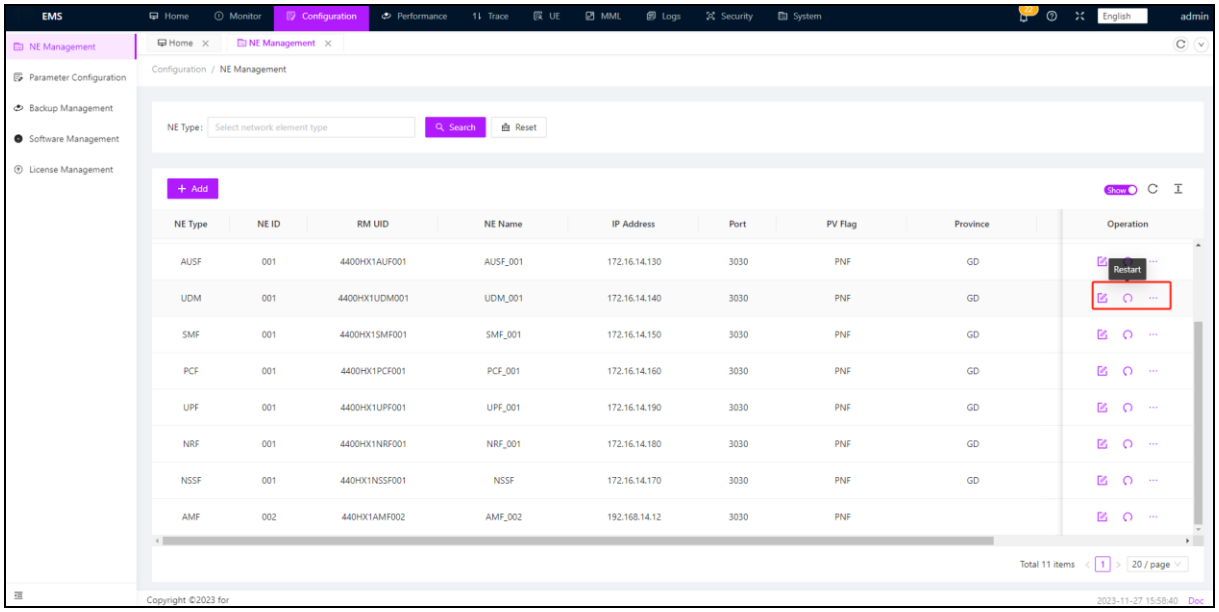
- NE Type

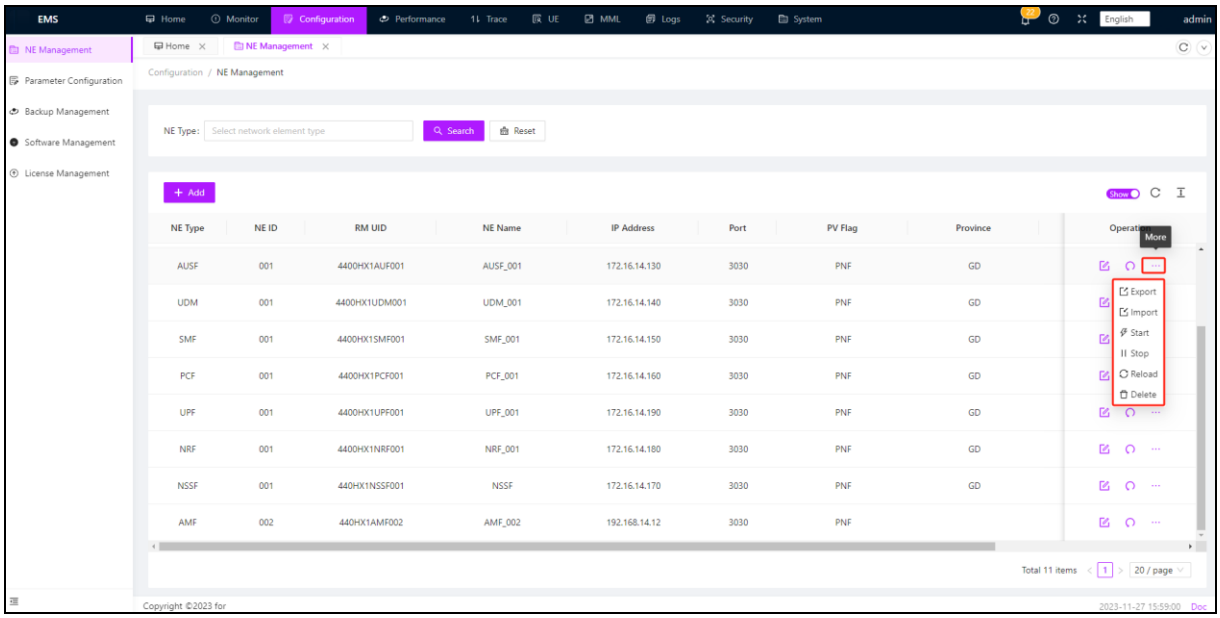
- NE ID
- RM UID
- PV Flag
- Port（Generally set to 3030）
- IP Address
- NE Name

The above is a required field when adding a new network element



The right side of each network element is configured with functions for restarting, starting, stopping, reloading, deleting, as well as importing and exporting network element configurations.

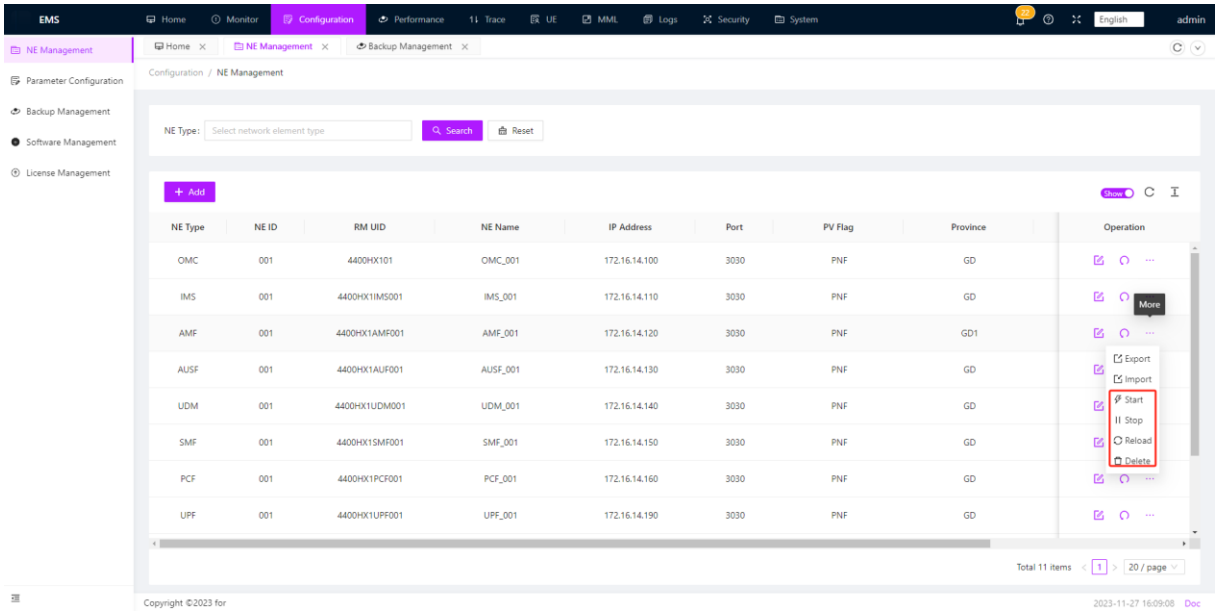




Export: After exporting the network element configuration, it can be queried in the backup management.

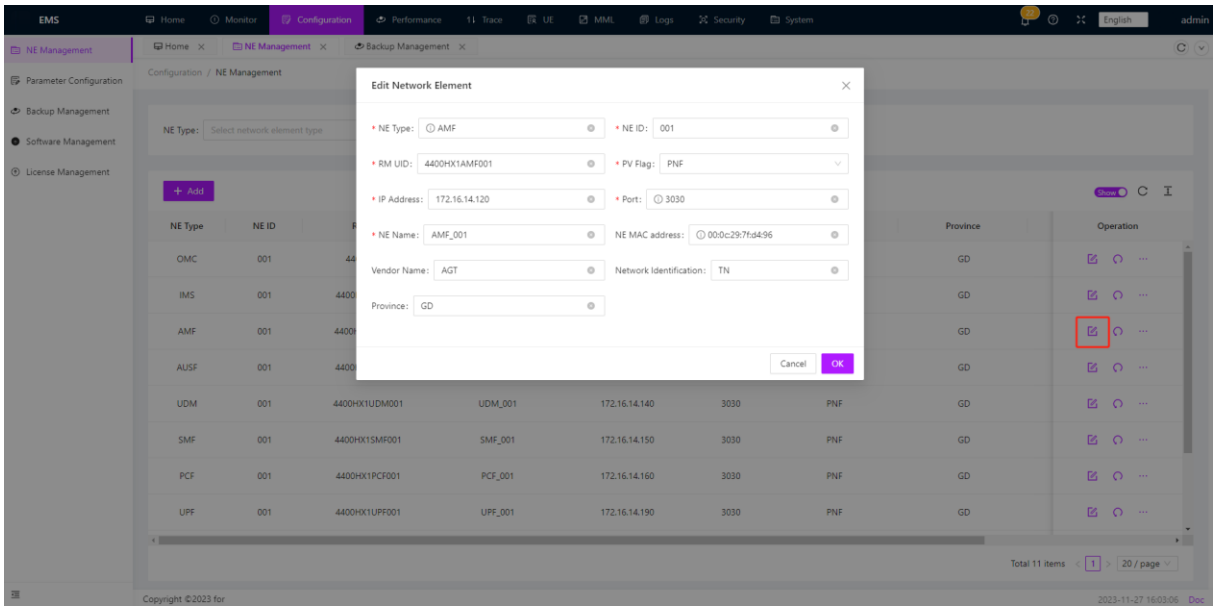
Import: Click "Import" to import the configuration of the network element. Select Server File to import the previous backup files on the server. Select Local File to import the local files.

The operator can click "Start" in "More" to start running the network element, click "Stop" to stop running the network element, click "Reload" to reset the network element parameters, and click "Delete" to delete the network element.



On the right side of the network element, you can click the modify icon to modify

the network element



3.4.2 Parameter Configuration.

Parameter configuration is a key link in optimizing 5G core network performance and services.

1. Function overview: Parameter configuration allows network administrators to finely adjust the operating parameters of each network element in the core network. it involves

to all aspects of the network, from data transmission rates to signal processing strategies, from security protocols to access control lists

(ACLs). The flexibility and atomicity of parameter configuration are key indicators to measure the maturity of the 5G network management operating system.

2. Add, delete, and modify network element parameters: In network operations, it is sometimes necessary to introduce new parameters to support new technologies.

or service policy; sometimes it is necessary to delete old parameters to optimize network performance or comply with new specifications; sometimes it is necessary to modify

Modify existing parameters to adapt to changes in network quality or customer needs. These operations are performed in the network management system of the 5G core network

This can be done manually via a graphical user interface (GUI) or automatically via a command line interface (CLI) or API.

Animation. Parameter changes are often triggered by real-time monitoring of network status, which requires a high degree of real-time performance in the network management system.

and sensitivity.

3. The configuration takes effect quickly: In traditional network systems, parameter changes often require restarting the network element before the configuration can take effect.

effect. This is no longer necessary in a 5G environment. Modern network management systems can implement hot changes, allowing parameter configuration changes to

Can take effect immediately without restarting. This immediate function is essential to maintain the highest timeliness of the network.

is important and ensures that service will not be interrupted due to configuration changes.

4. Parameter configuration challenges and automation: In the highly complex 5G core network, manual parameter adjustment may no longer be possible.

Reality therefore relies more on intelligent tools and automated strategies. Predefined strategies and machine learning models can be based on

Realize automatic tuning based on real-time data flow and network performance indicators. Automated parameter configuration not only improves efficiency, but also

20

It improves accuracy and reduces network failures that may be caused by configuration errors. At the same time, the automation strategy must include relevant

Appropriate security mechanisms to prevent misconfiguration and network attacks.

5. Parameter audit and compliance: In order to ensure that the network complies with prescribed policies and standards, parameter configuration is an important method.

The focus is on auditing and compliance checks. Network management systems usually include audit logs and compliance reporting functions to ensure that all configuration

Configuration changes are logged and can be traced. These records are critical when troubleshooting network issues or performing security audits.

Parameter configuration This function corresponds to the configuration parameters of each network element. This function determines the operation quality and performance of the 5G core network.

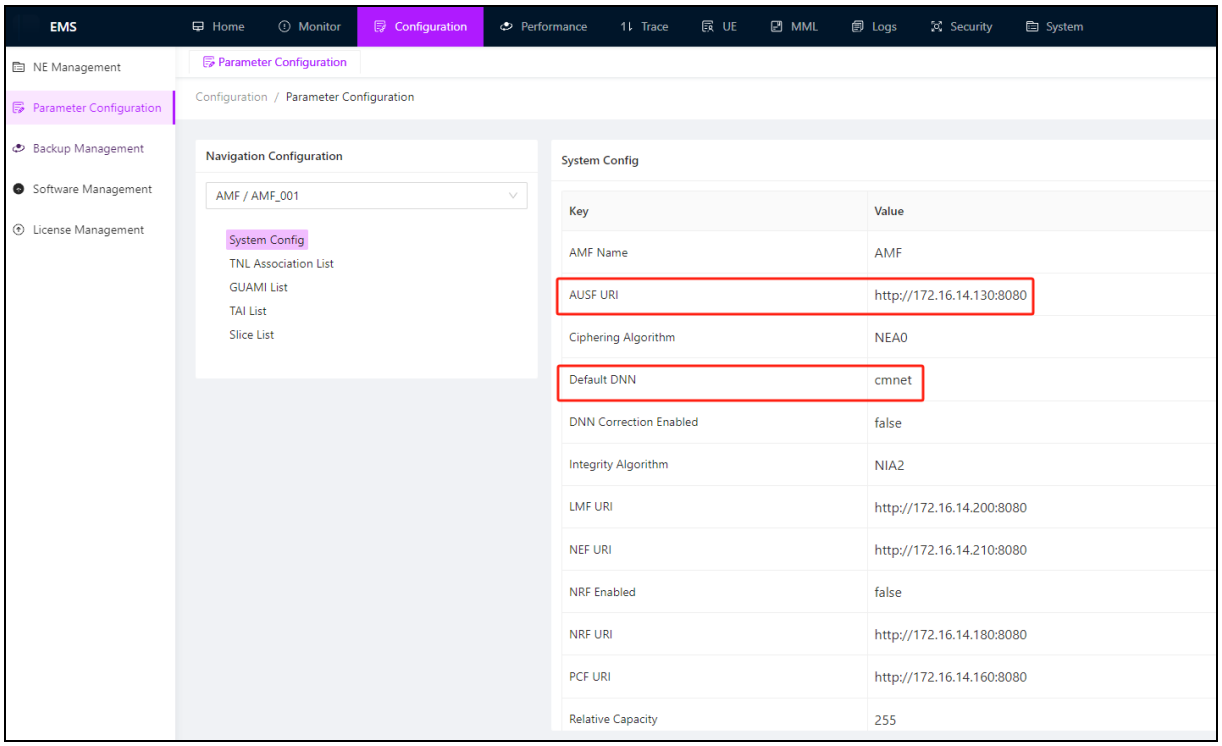
Efficiency is the key to network health and functionality.

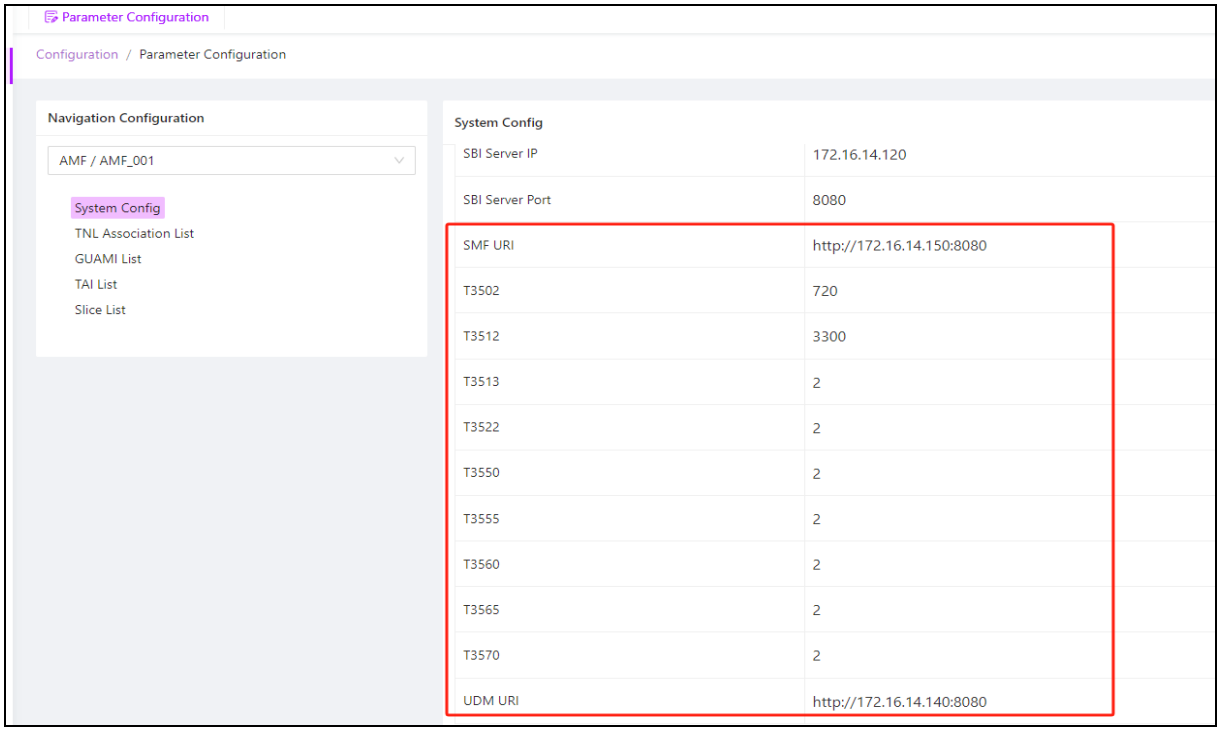
The following is an example of common network element configuration modifications. When modifications are required, place the mouse on the modification where the modification mark appears.

On the value, click to modify it, or a modification mark will appear on the right side of some places, click to modify it. Select the corresponding network element to obtain configuration information or modify it.

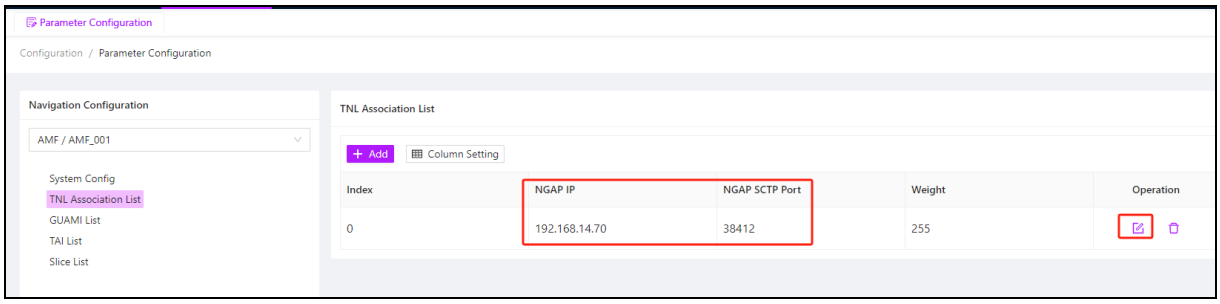
3.4.2.1 AMF

1、System Config: in the System Config of the AMF, the AUSF URI, UDM URI and SMF URI are mainly changed for connecting to the AUSF and UDM and SMF, the Default DNN is changed for connecting to the DNN, and some timers, such as 3512, are modified.

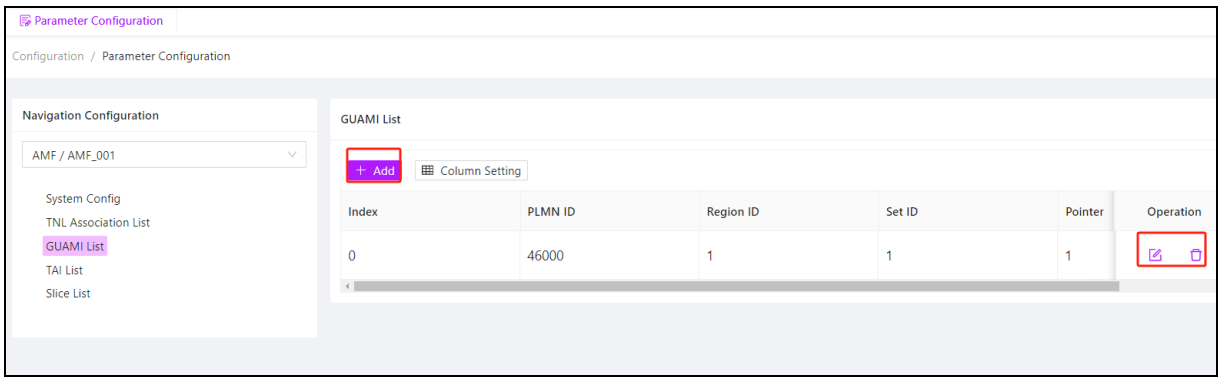




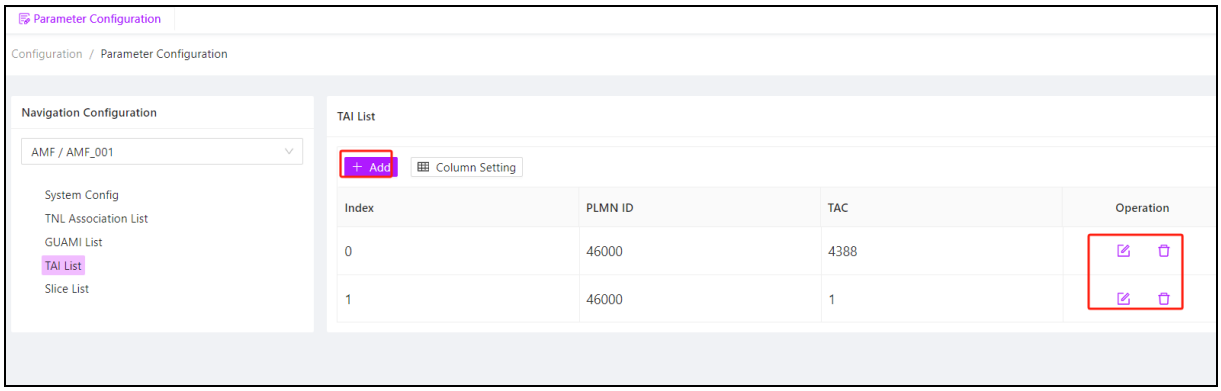
2、TNL Association List: in the TNL Association List, you can modify the N2 IP and NGAP SCTP Port, which are used to interconnect with gNB.



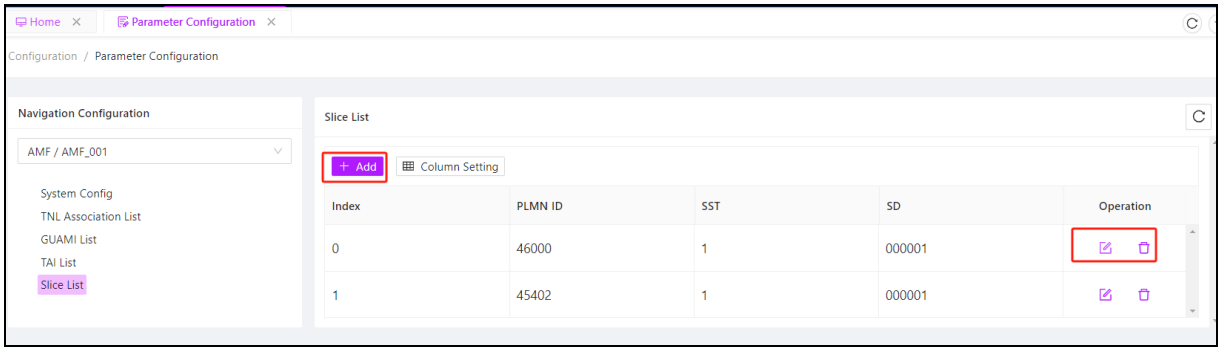
3、**GUAMI List:** GUAMI List can be modified, added, and deleted. When a user device attempts to access or manage mobility, the network determines the required AMF based on the AMF ID in the GUAMI list and routes the relevant control signaling to the corresponding AMF.



4、**TAI List**: In the TAI List, you can modify, add, and delete TAC corresponding to PLMN, PLMN and TAC correspond to base stations. If the AMF is incorrectly filled, the connection between the AMF and the base station may be interrupted.

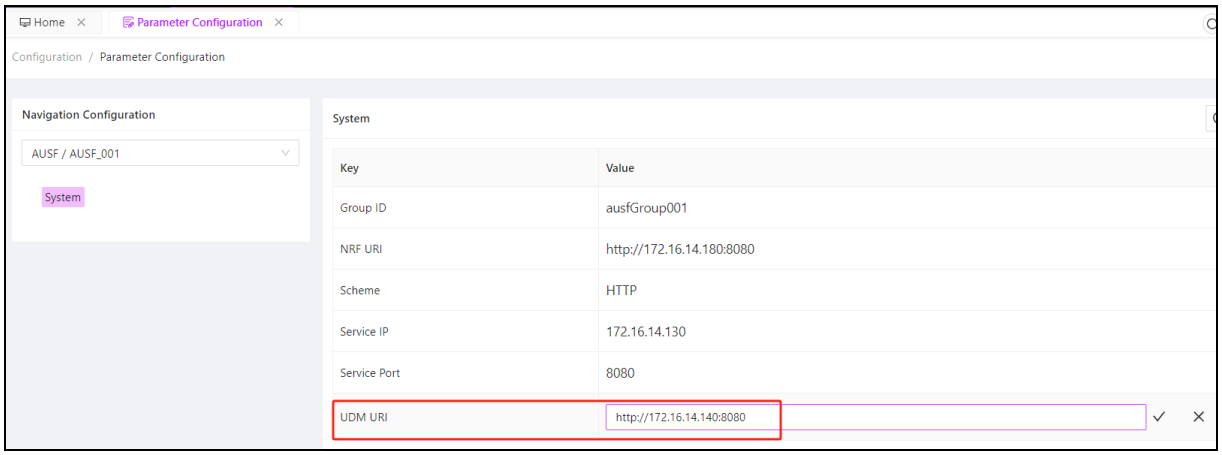


5、Slice List: In the Slice List, you can modify the slice information corresponding to the PLMN, which is the slice that the AMF allows to access



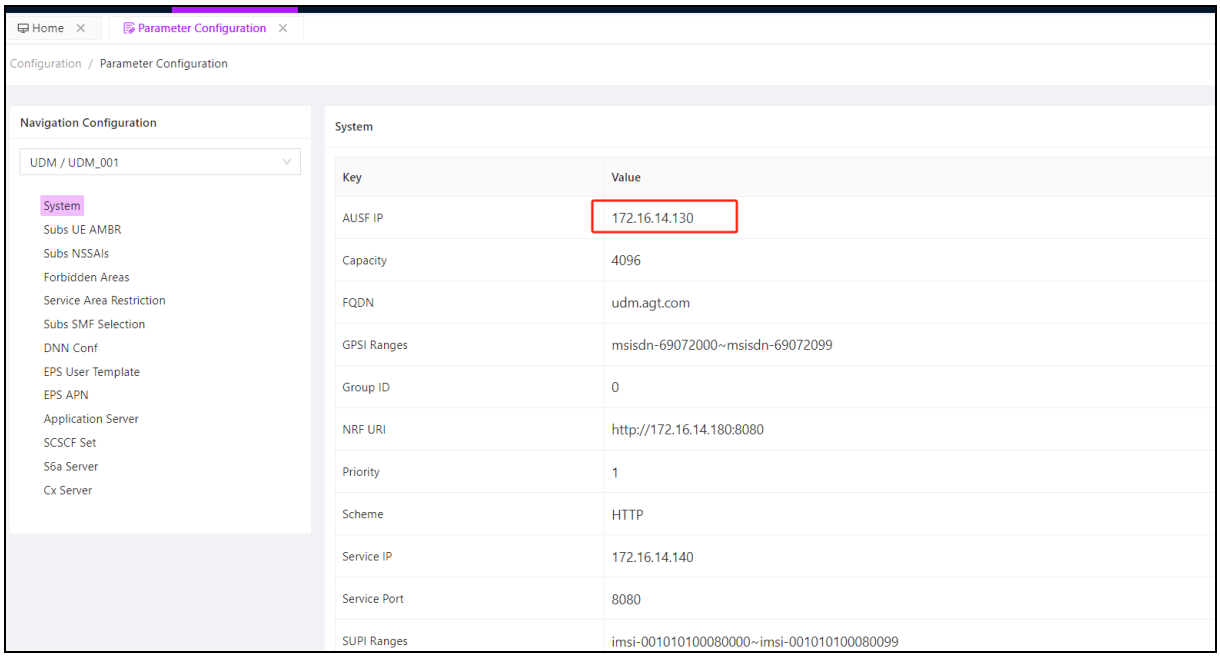
3.4.2.2 AUSF

1、System:In the AUSF configuration file, change the UDM URI and configure the UDM IP address for interconnection with the AUSF:

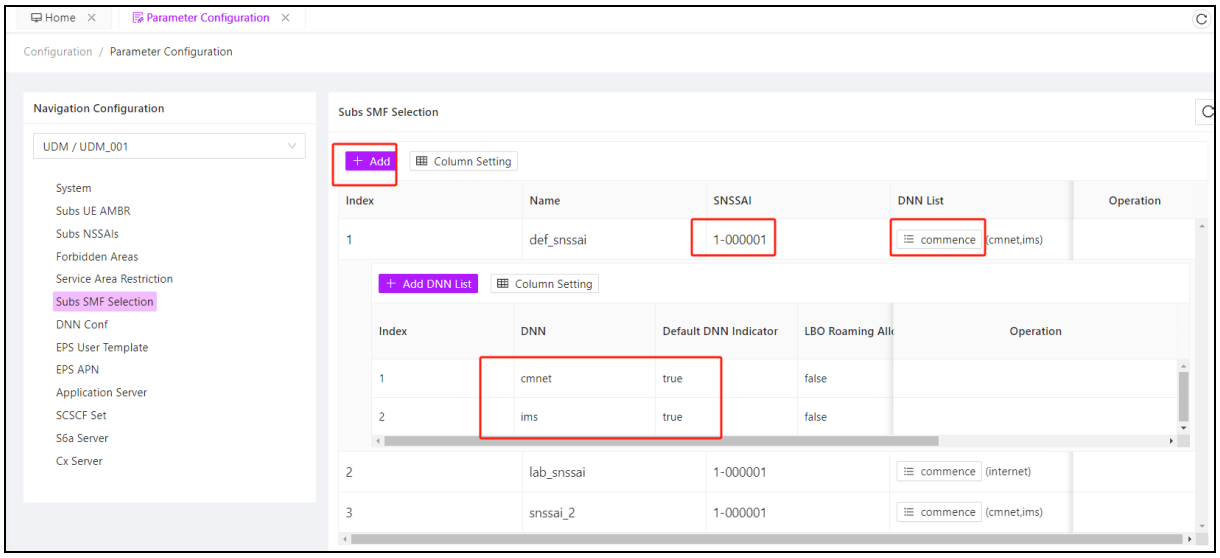


3.4.2.3 UDM

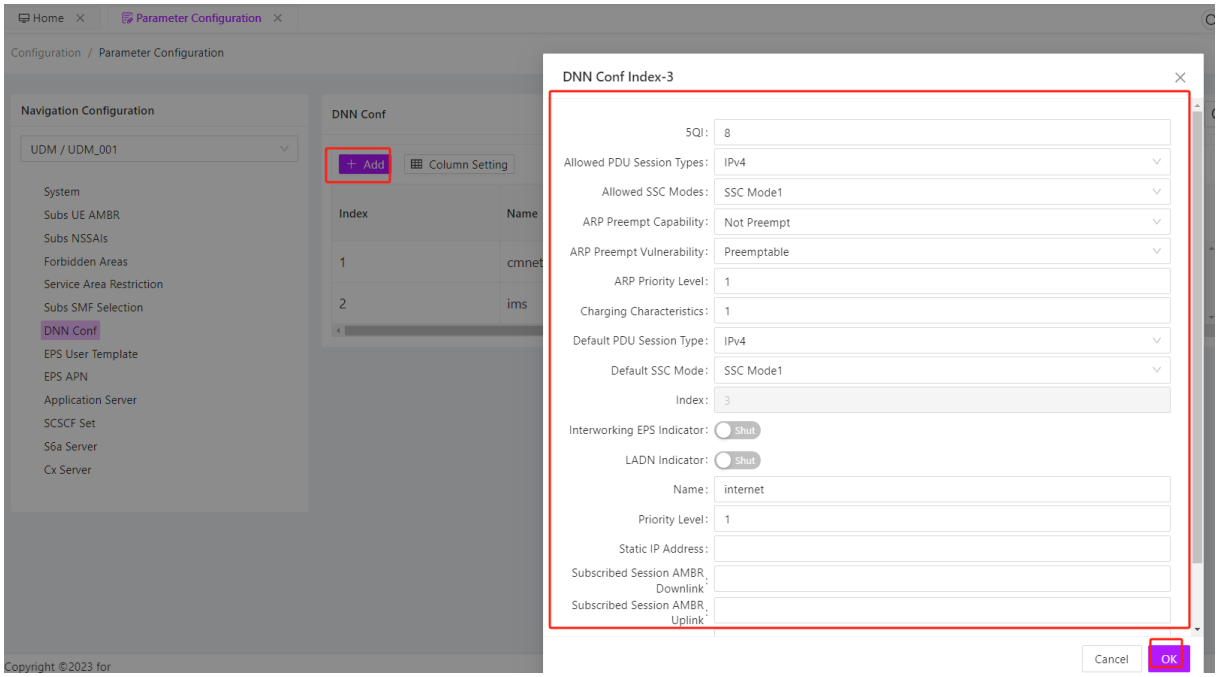
1、System: the operator mainly modifies the AUSF IP here



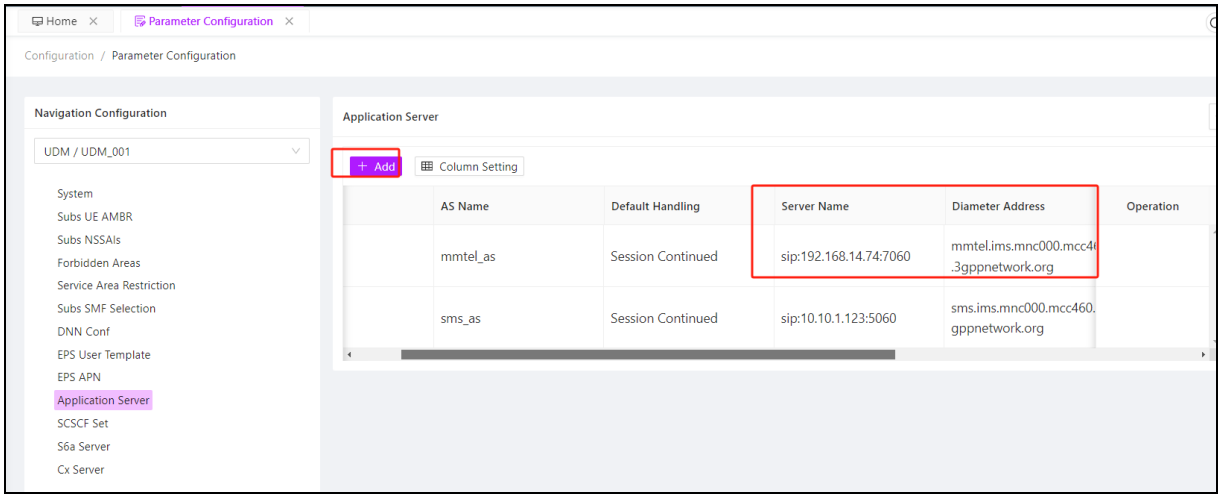
2、Subs SMF Selection: the operator here mainly refers to the DNN corresponding to the slice information in session management



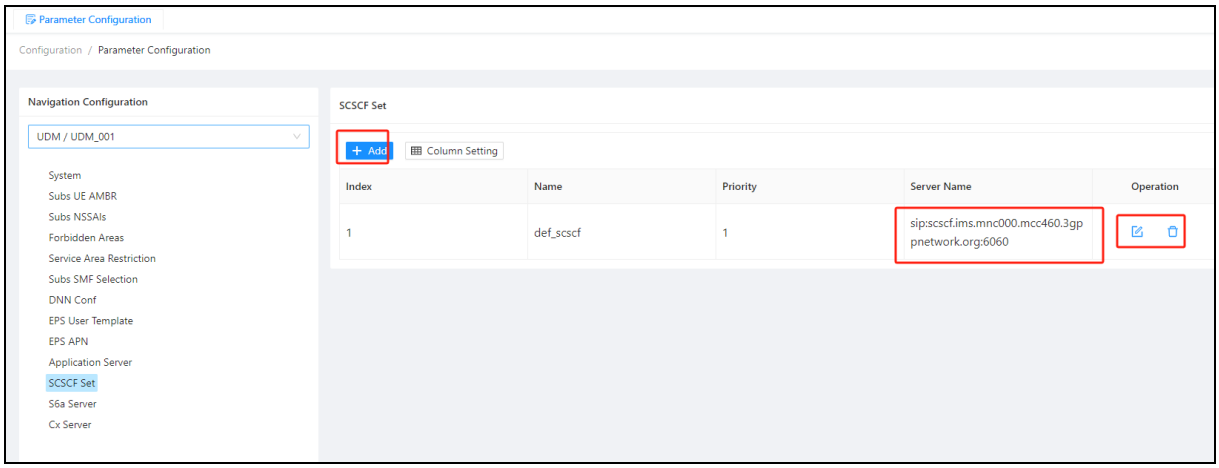
3、DNN Conf: Operators need to add, delete, and modify DNNs connected to UE. They can add different DNNs as required and modify the parameter settings for different DNNs, such as the Default SSC Mode and Subscribed Session AMBR Uplink, and so on.



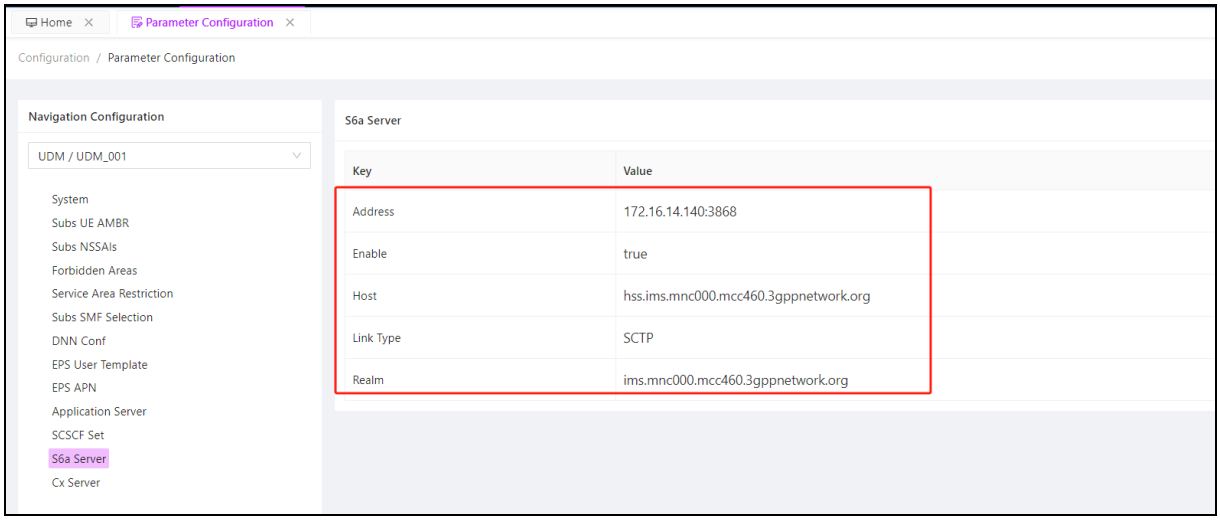
4、Application Server: the operator's main focus here is to add or modify MMTEL_AS corresponding to IMS data, modify the IP address of sip in Server Name and Diameter Address.



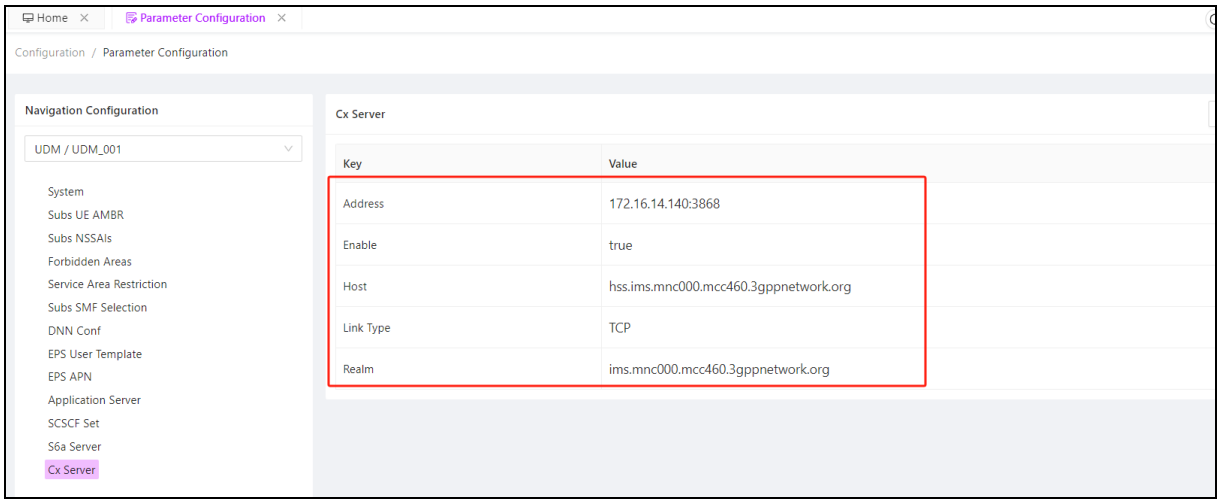
5、SCSCF Set： the operator's main task here is to modify the SIP data of SCSCF corresponding to IMS.



6、S6a Server: the operator mainly switches on the interface with s6a and modifies host

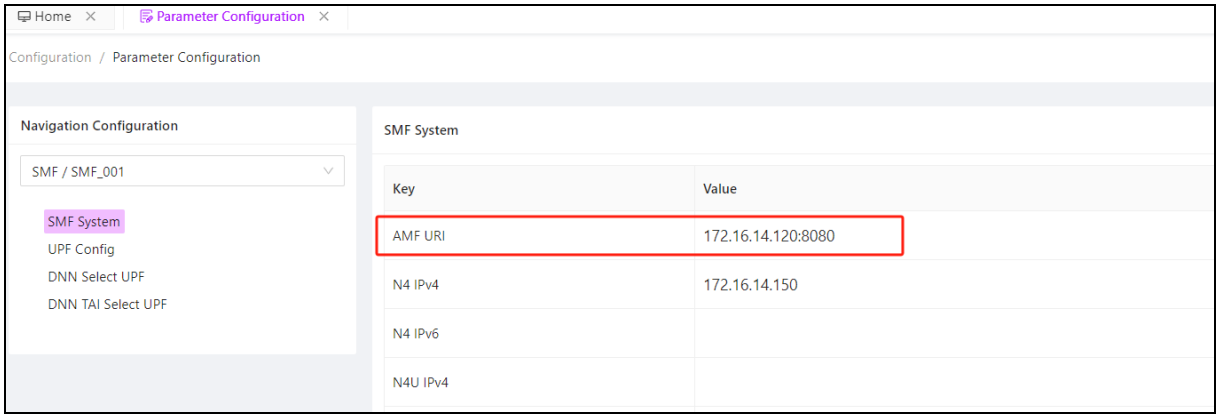


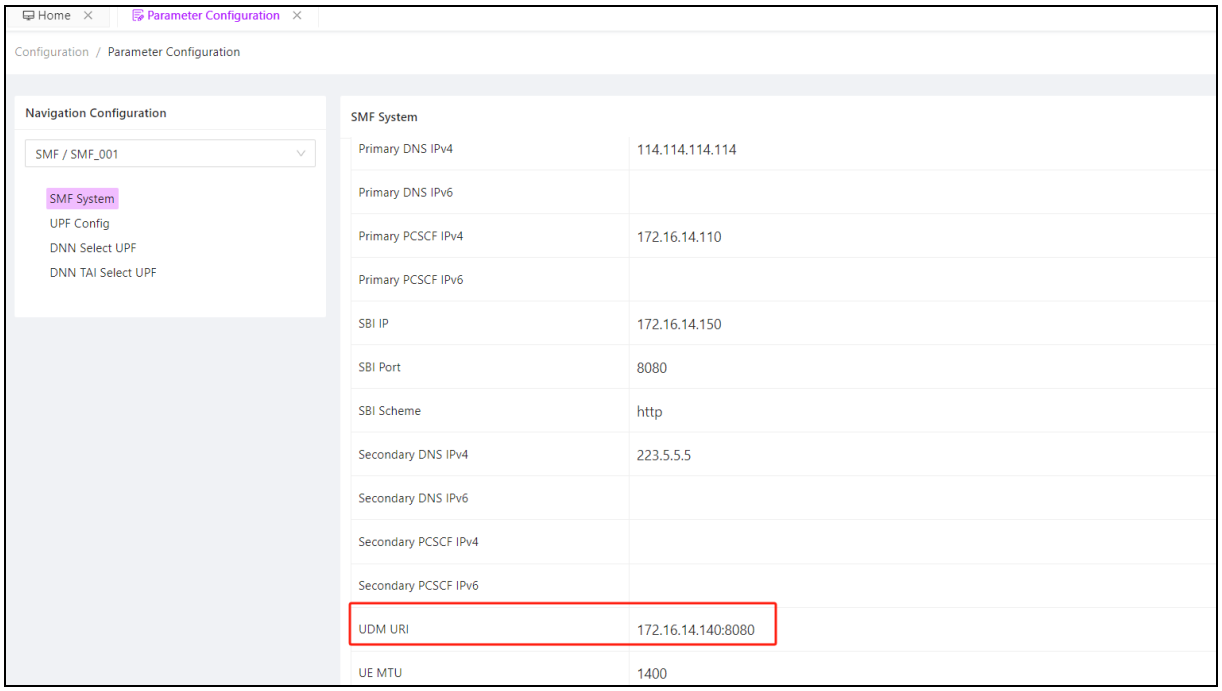
7、Cx Server: the operator mainly switches on the Cx port corresponding to the IMS and changes the corresponding host



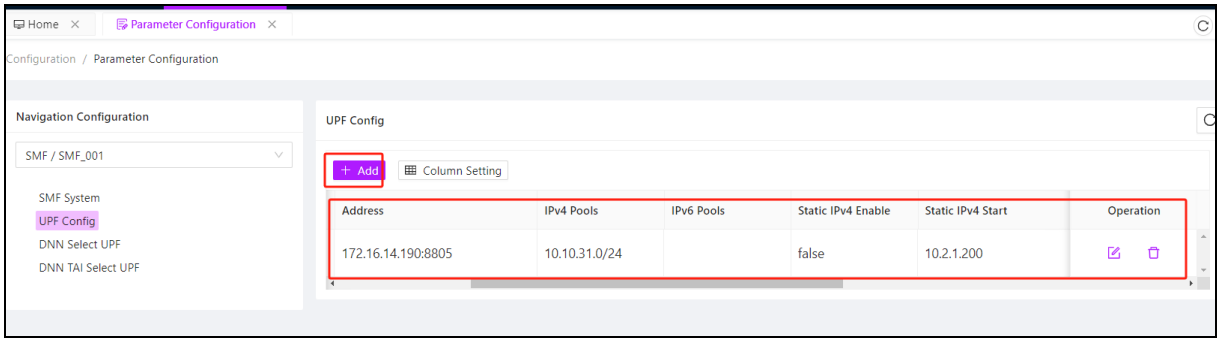
3.4.3.4 SMF

1、SMF System: the operator's main task here is to modify AMF URI and UDM URI



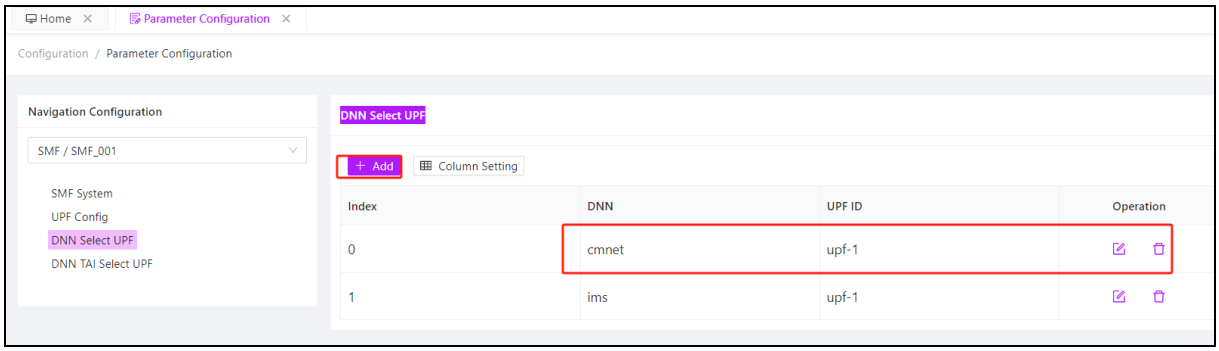


2、UPF Config: the operator can configure the UPF IP corresponding to the SMF in UPF config, set the IP address pool assigned to the UE, and set the static IP address.



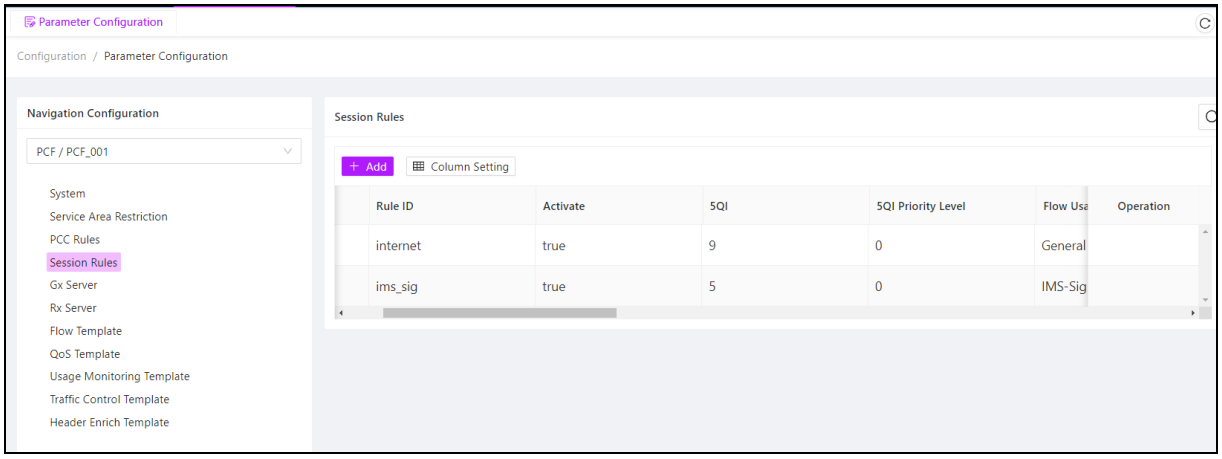
3、DNN Select UPF: the operator can configure different DNN to correspond to different

UPF.

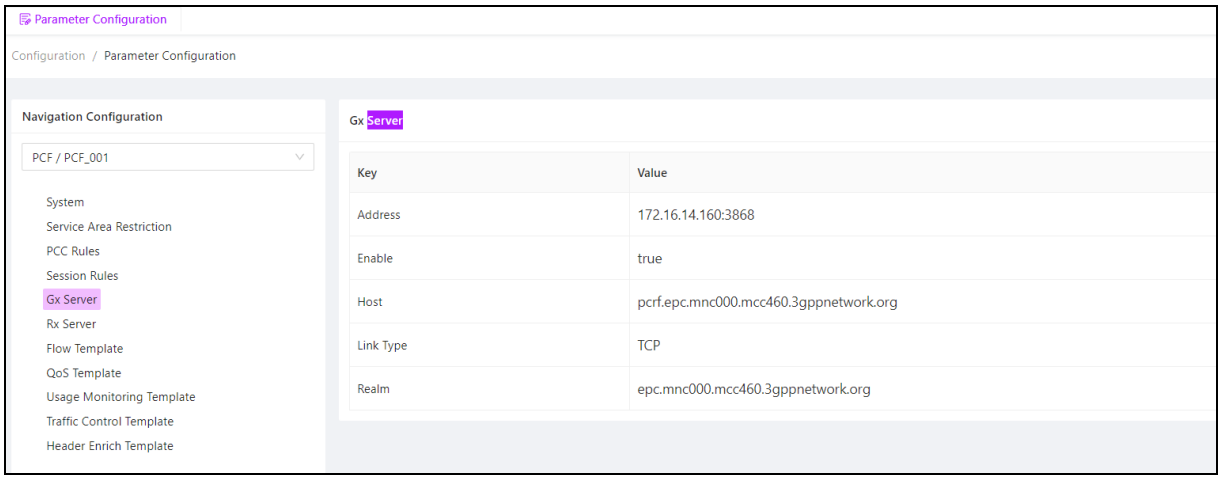


3.4.4.5 PCF

1、Session Rules: Operators can configure different session rules and modify 5QI and AMBR Downlink parameters of corresponding rules

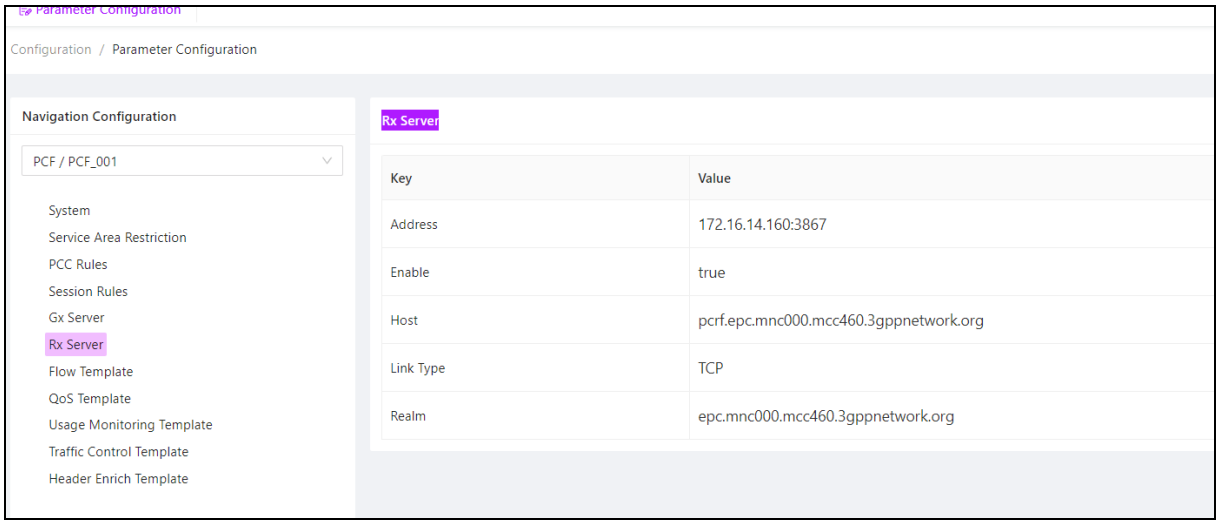


2、Gx Server: The operator can configure Gx Server parameters including Gx switch, host, etc



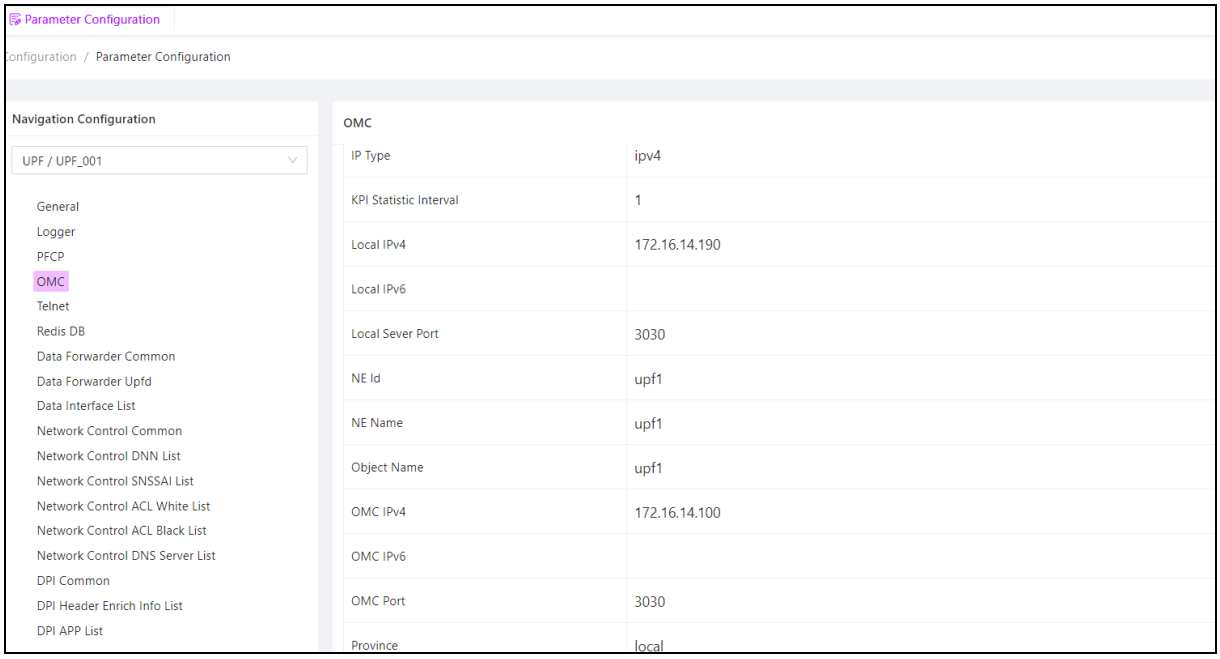
3、Rx Server: The operator can configure Rx Server parameters including Rx switch, host,

etc

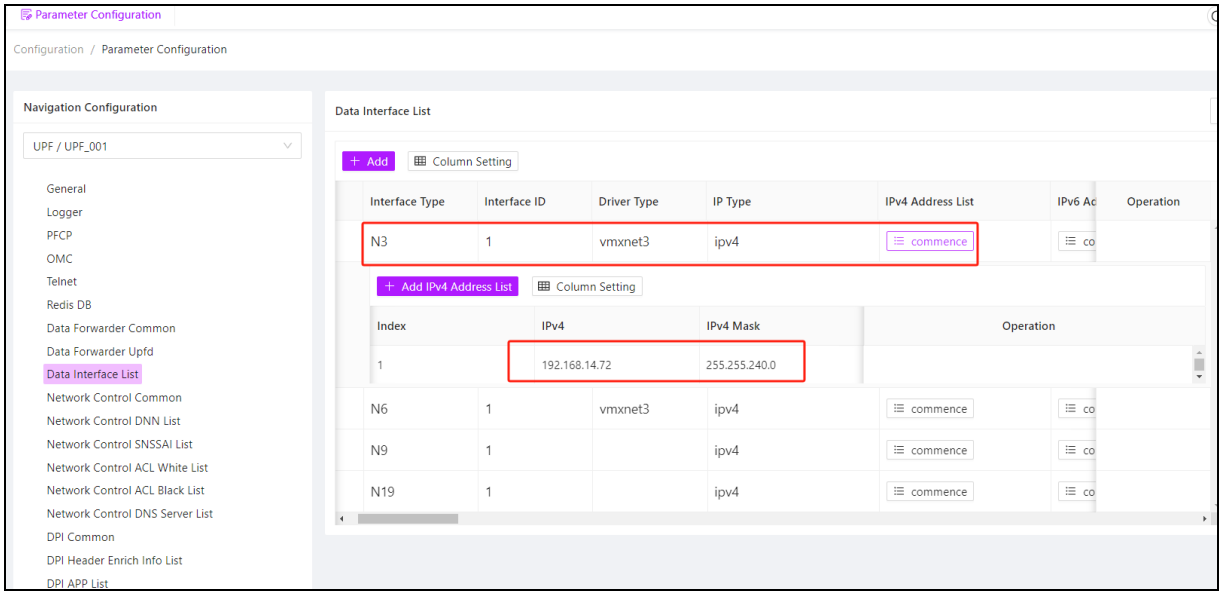


3.4.4.6 UPF

1、OMC: The operator can set OMC-related parameters, such as the IP address and port of the OMC

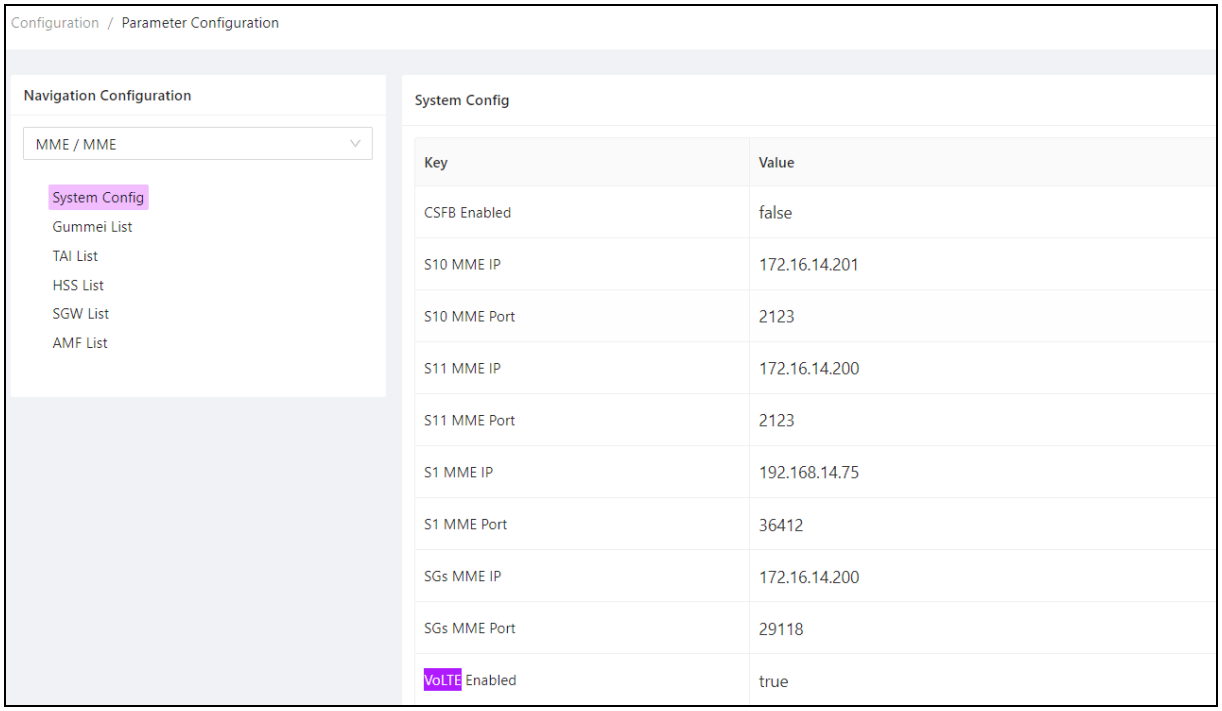


2、Data Interface List： the operator can configure the parameters of N3/N6/N9/N19, including IP, Driver Type, MAC Address, Interface PCI, Gateway IPv4, etc.

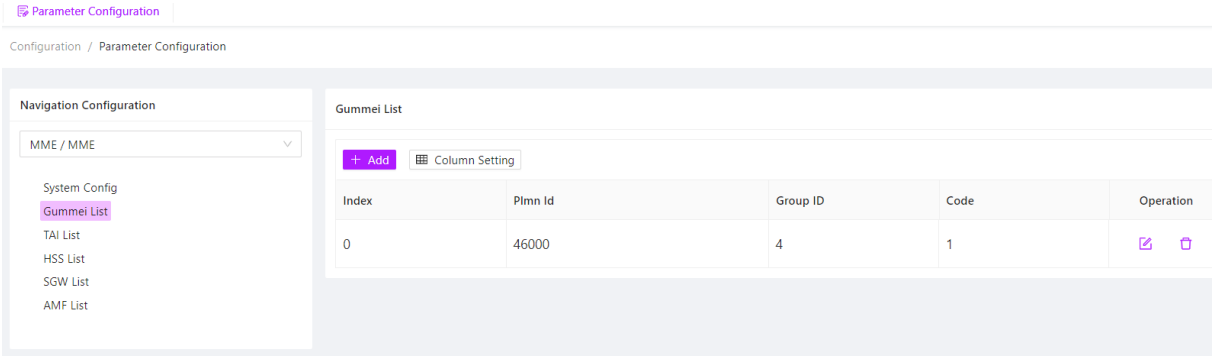


3.4.4.7 MME

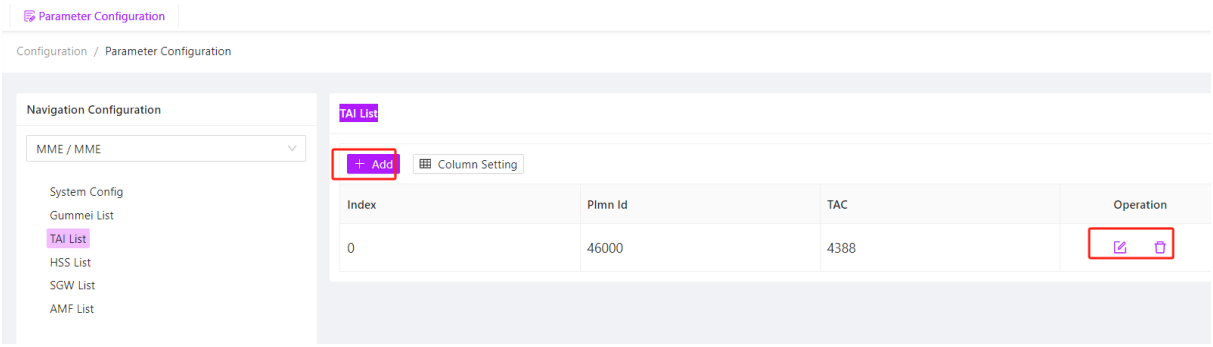
1、System Config: The operator mainly configures the IP and ports of S10, S11, S1, SGs, and VoLTE switches can be configured



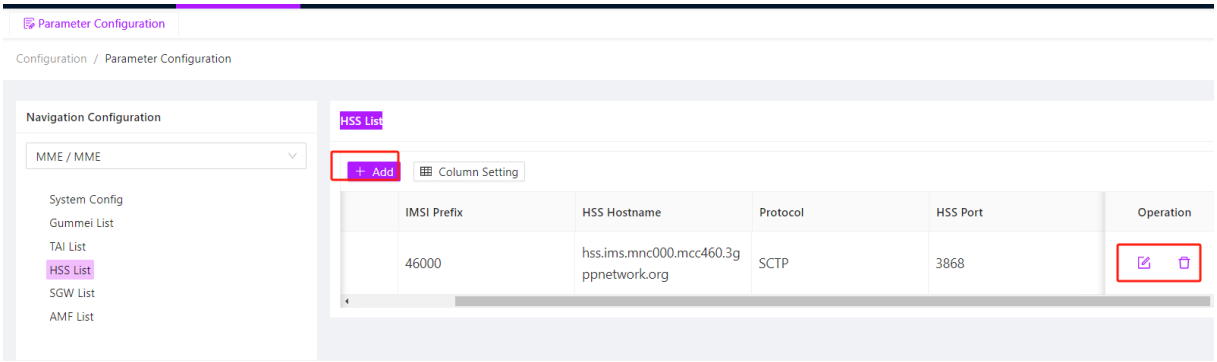
2、Gummei List: The operator mainly configures the parameters of GUMMEI List, including PLMN and Group ID.



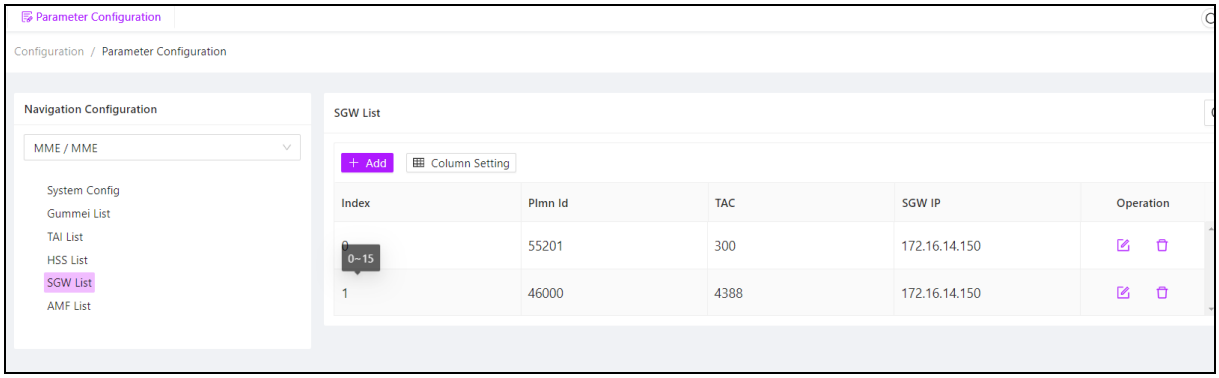
3、TAI List: The operator mainly configures the TAC corresponding to the PLMN that can access the core network



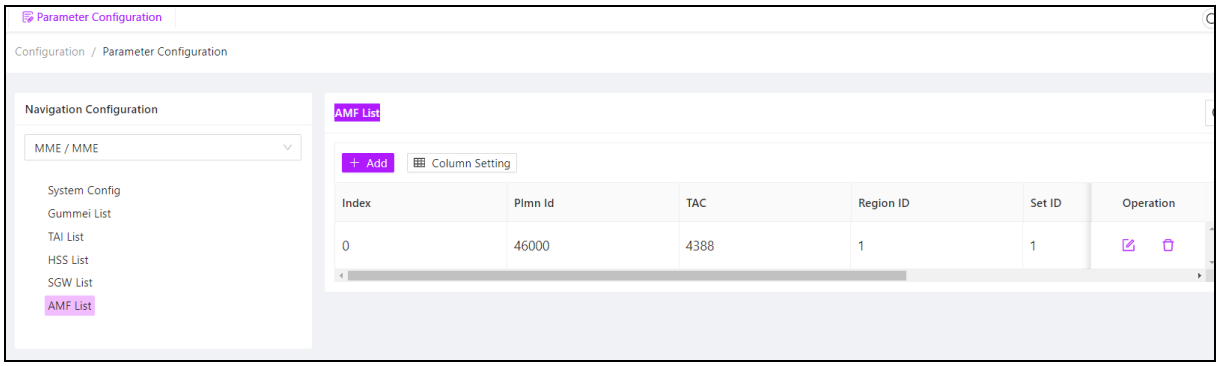
4、HSS List: The main configuration of the operator here is the HSS Hostname interconnecting with the MME



5、SGW List: The operator mainly configures the IP, TAC and plmn of the SGW that interconnects with the MME.



6、AMF List: The main configuration of the operator here is the information of the AMF interoperable with the MME, including the AMF, PLMN, TAC, etc.



3.4.3 Backup Management

Backup management is a core component of any IT infrastructure management, and it is especially important in core networks because it ensures that services can be quickly restored in the event of data loss, failure, or other catastrophic events. The following backup management is described in detail:

1. The importance of backup strategy

An effective backup strategy requires comprehensive consideration of the value of data, recovery time objectives (RTO), data recovery point objective (RPO) and business continuity requirements. Strategy development, but also need to weigh the frequency and cost of backup. For example, more frequent backups can reduce data loss, but at the same time will also increase the cost of storage and resources.

2. Full versus incremental backups

A full backup means copying all selected data sets, which consumes more time and storage resources, but is simpler to restore. Although it consumes more time and storage resources, it is easier to restore. An incremental backup copies only the data that has

changed since the last backup. This saves storage space and backup time, but the recovery process can be more complex and time-consuming because it requires all previous incremental backups to work together.

3. Automatic Backup

Modern 5G network management systems can automate backup tasks to minimize human error and ensure regular backups. This may include daily or weekly scheduling of tasks, as well as backups triggered based on specific events or conditions, such as before a major before a major update. The configuration backup is now set to occur daily at 0:30am for all network elements.

4. Fault Tolerance

A good backup management system should be fault-tolerant to ensure that even if part of the backup process fails, the system can recover and complete the backup as much as possible. System can also recover and complete the backup task as far as possible. It can verify the accuracy of the backup file through checksums or other integrity checks. file accuracy.

5. Backup Storage

The storage of backup data is equally important. Backups should be stored in a safe and reliable location, and preferably geographically separated from the production environment location, in order to protect the data from physical disasters. Often, local, network, or cloud storage solutions are often used, sometimes even in combination to provide additional security.

6. Recovery Processes

A well-prepared backup strategy also needs to be able to guide an efficient data recovery process. This means that in the event of a failure, you must be able to quickly locate the proper backup quickly locate the appropriate backup set and follow a predetermined procedure to get the system back up and running. In addition, regular recovery In addition, regular recovery drills are valuable to validate the effectiveness of backups and ensure that the team is familiar with the recovery process.

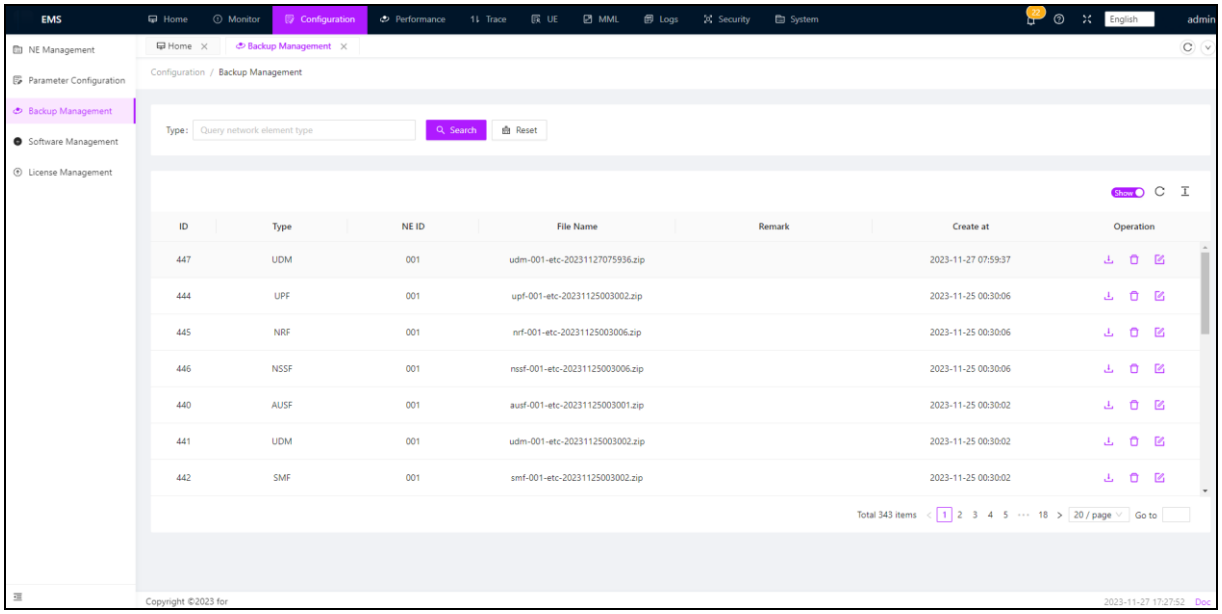
Backup management ensures the reliability of 5G network services and the security of data, and is a key strategy for delivering continuous business services.

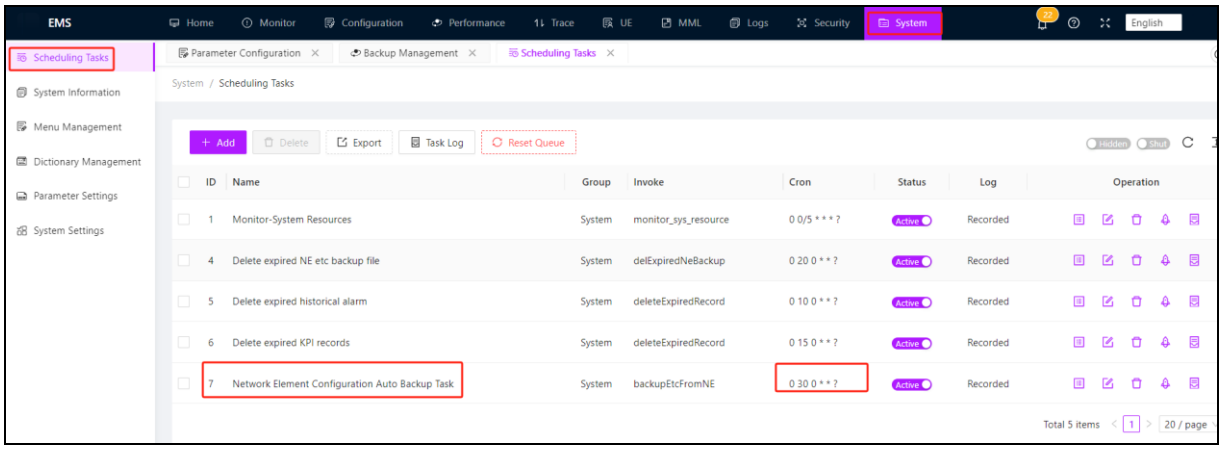
Strategies.

Currently, backup management for network elements typically consists of automatic system backups and manual backups.

Manual Backup: Manual backup is mainly the backup file obtained after the export operation of the network element in the network element management. The exported configuration file will be displayed in the backup management.

Auto Backup: In Auto Backup, the system realizes automatic backup and scheduling management for network element backup. You can configure the backup task under the scheduling task configured by the system. configure the backup task under the scheduling task configured by the system. Currently, the configuration file of each network element is backed up once a day at 00:30.





3.4.4 Software Management

Software management is the process of managing and upgrading the software of each network element in the network, and ensuring that the stability and functionality of the network is upgraded and functionality upgrades are carried out smoothly. Network element upgrades are very important in a network to bring new features and performance improvements, as well as to It also fixes known problems and vulnerabilities.

Software Version Management: Manages the software version of each network element. This includes logging and managing the current software version running on each network element, as well as the status of new versions. This includes recording and managing the current software version running on each network element, as well as the release and upgrade schedule for new versions.

Software Upgrade Plan: Create a reasonable upgrade plan based on the software updates and upgrades provided. You can start by uploading the network elements that need to be upload the network elements that need to be upgraded to the server, and then upgrade them as needed.

Rollback and downgrade management: When problems or unexpected situations occur during the software upgrade process, you need to set up a rollback and downgrade strategy to ensure that the corresponding network elements can be upgraded. strategies to ensure that the corresponding network elements can be rolled back.

Software upgrade process:

Upload software: Upload the new version of network element software to the software library of the core network management system.

Distribute software: Select the upgrade operation for the target network element in the management system, which is usually started by clicking a "Delivery" button.

Activate software: After the software is released, to complete the upgrade process, you often need to activate the software. This is accomplished by clicking "Activate", a step that usually triggers a reboot of the network element to use the new software version.

Software rollback process:

If the upgraded software has problems or does not meet your needs, you can roll back to the previous version of the software through the following steps:

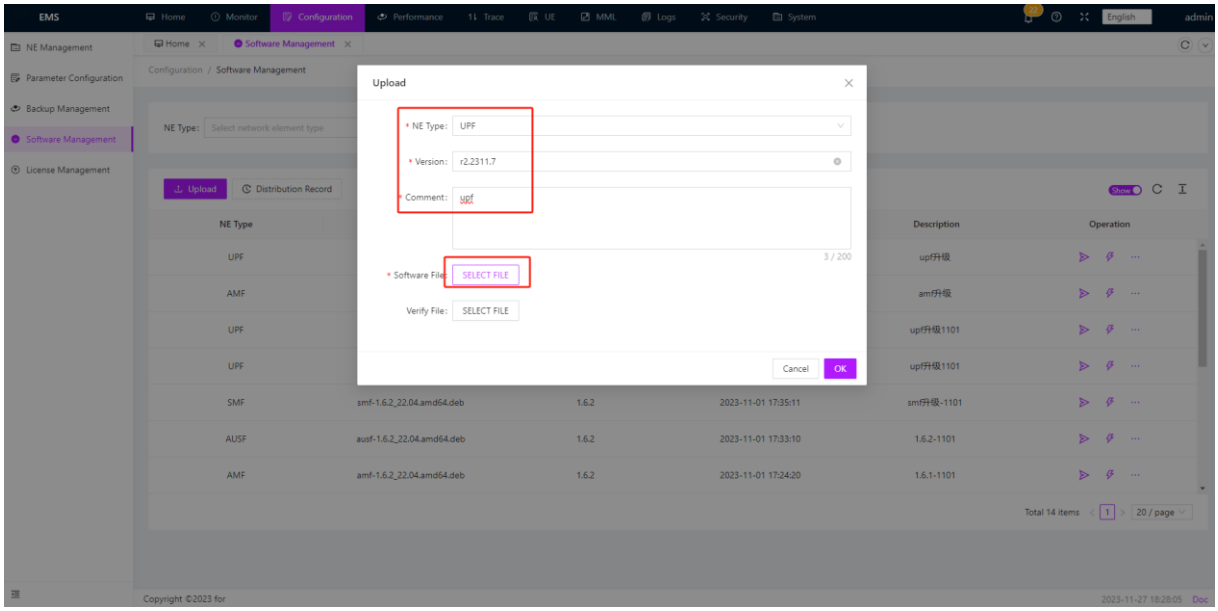
Click rollback: Select the network element that needs to roll back the software and perform the rollback operation. Network operation and maintenance personnel can operate through the "Back" button on the management system interface.

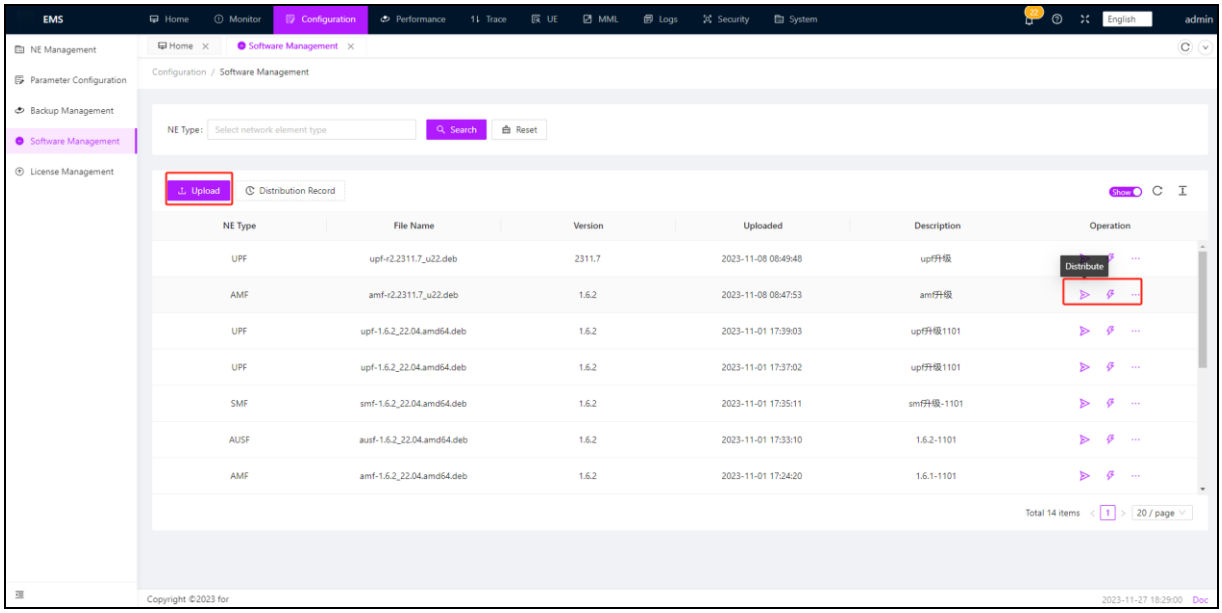
During this entire process, administrators can monitor and record each software upgrade or rollback operation through the management system.

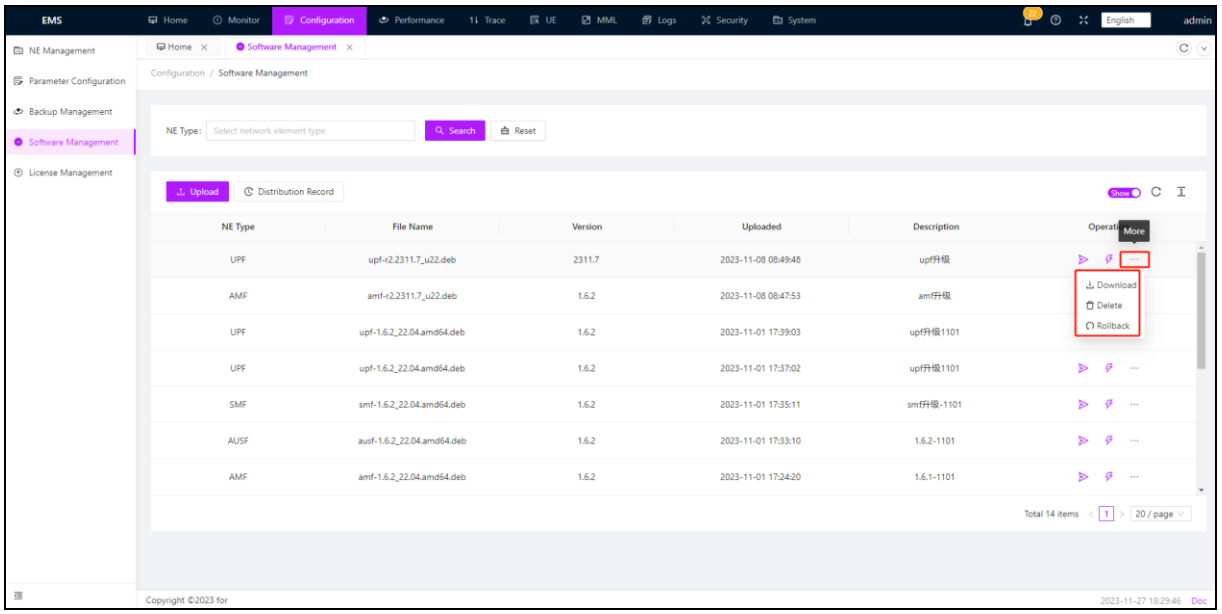
Distribution records: Operation records of software upgrades or rollbacks are usually recorded by the system for audit and review when necessary. Administrators can view all executed operation records in the "Distribution Records" section, including detailed information such as time, operator, and results.

This software management process is an important part of core network operation and maintenance to ensure that network element software is running in the latest version and in the best condition. Through the software management interface, the operation and maintenance team can easily upgrade and maintain the network element software to ensure the stability and security of the network.

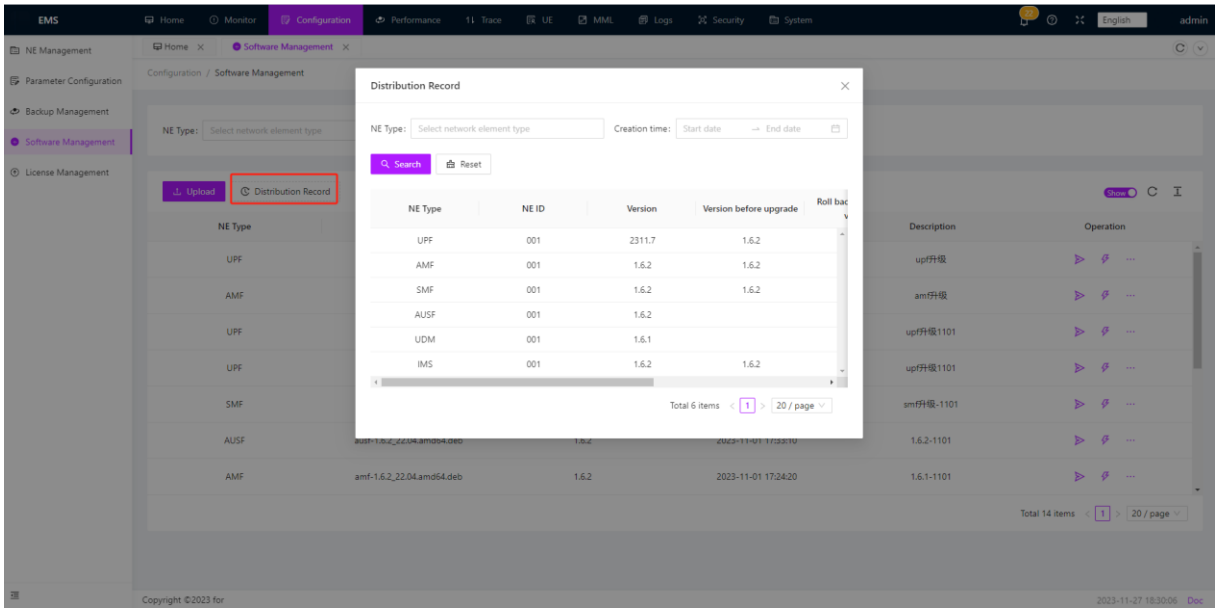
Operation: Upload->Distribute->Activate/Rollback







Can view the distribution records of each network element



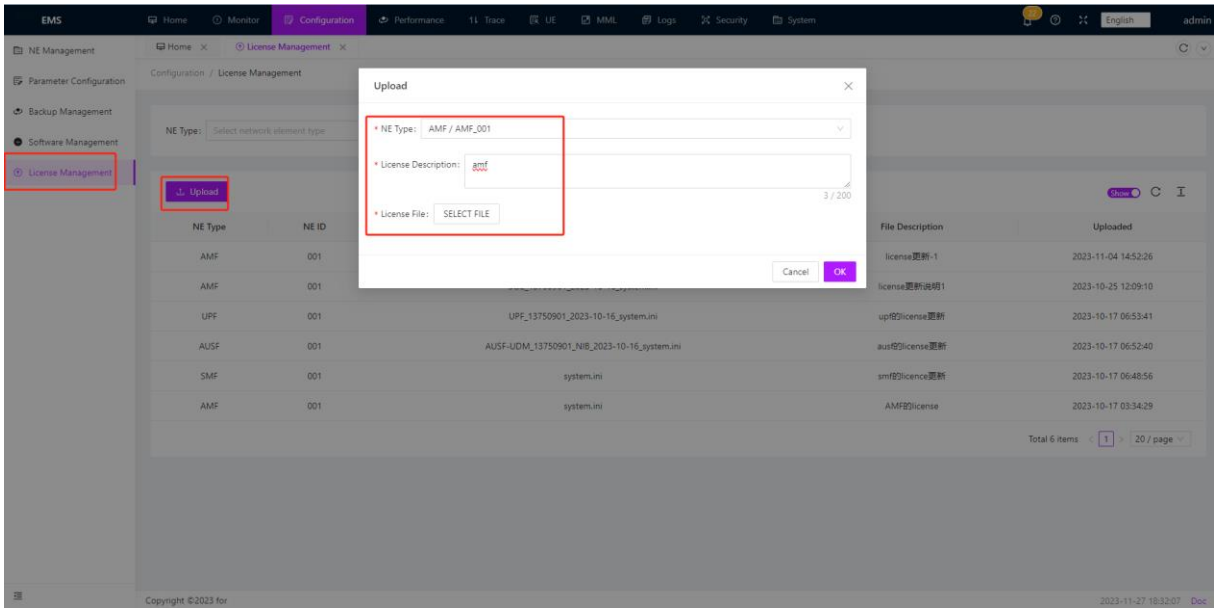
3.4.5 License Management

License management is used to manage and update licenses of NE to ensure compliance and resource management efficiency of network operators. A License of an NE is a certificate of network function authorization, which determines the functions and service capabilities of the NE.

License management records and manages the license information of each NE, including the license type, validity period and authorization functions. This is very important to accurately grasp the license status of each network element and reasonably plan and manage network resources.

Effective License management ensures compliance and validity of network devices and functions, properly manages network resources, and improves network stability and performance. This is very important for providing high-quality 5G services and optimizing the efficiency of network resource utilization.

Operation: Click Upload, enter NE Type and License Description, click SELECT FILE, select the updated license file to upload, and click OK to complete the update.



3.5 Performance

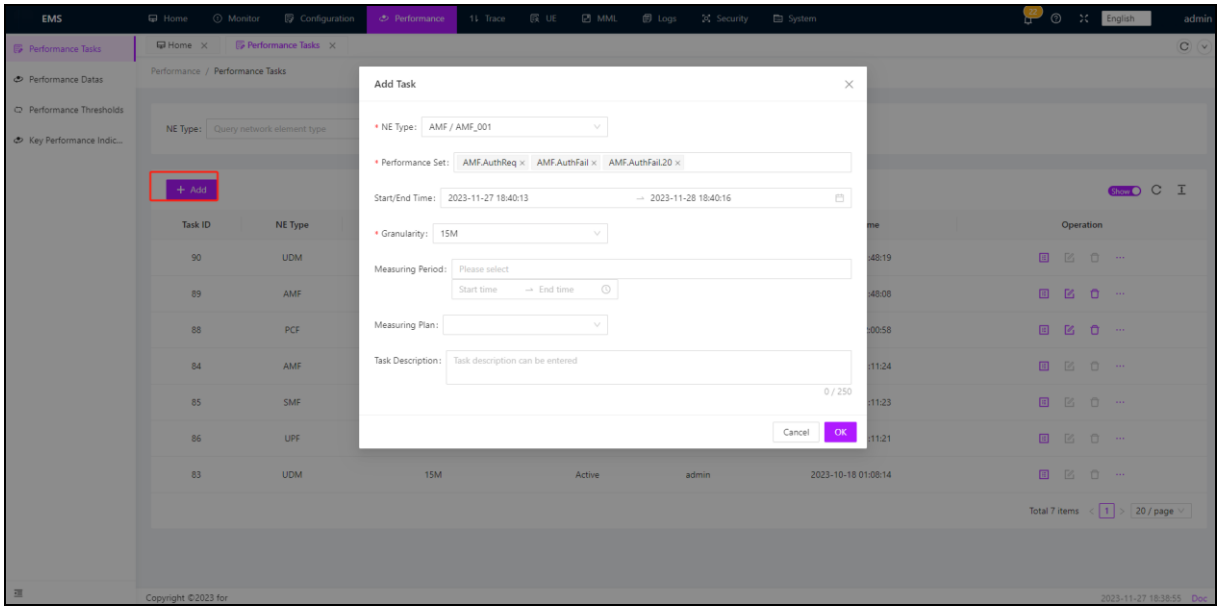
Performance management refers to the management and monitoring of the performance of the core network to ensure the efficient operation and reliability of the network. Core network performance management collects and analyses performance data on a regular basis to ensure standardization of network geology and timely detection of problems and their root causes. It mainly includes four aspects: performance tasks, performance data, performance thresholds, and key performance indicators.

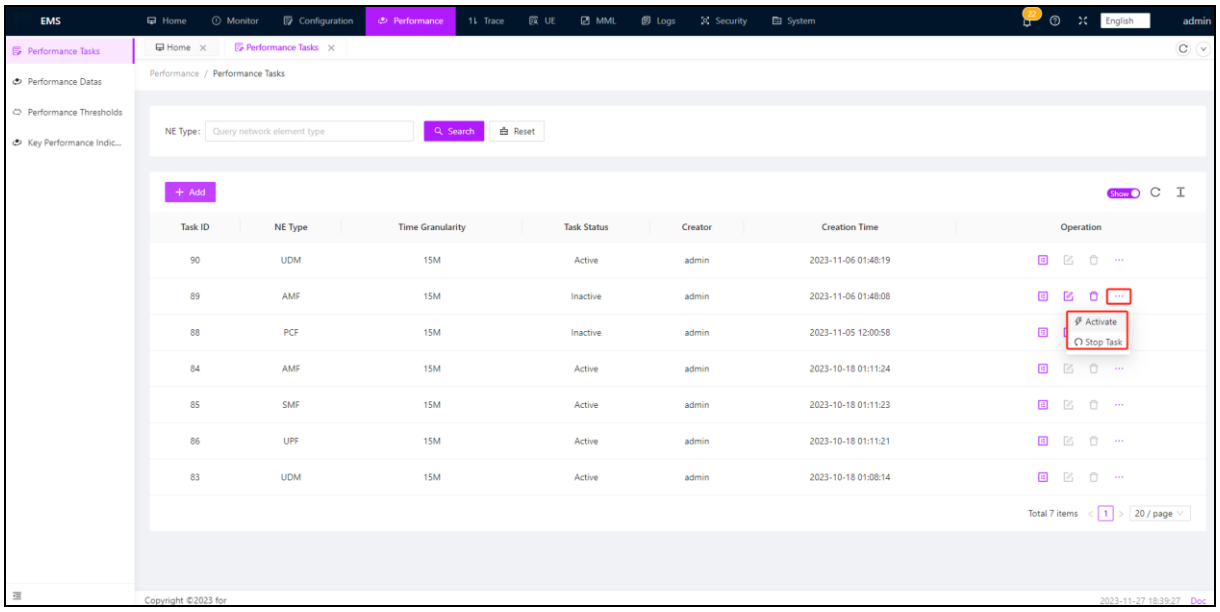
3.5.1 Performance Tasks

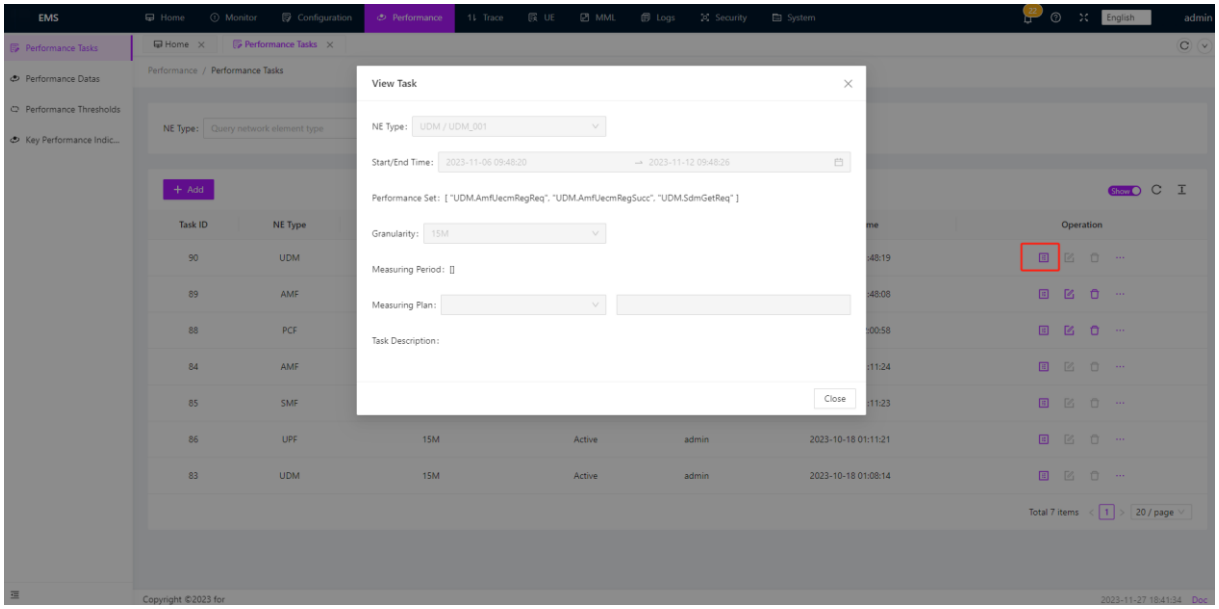
Performance Tasks: This function is to ensure the geological reliability of the network by monitoring the performance indicators of each core network element, performing performance evaluation and analysis. You can create different performance tasks for different NE. You can set the start and end time of the task. The granularity of the counter statistics can be divided into four types: 15 minutes, 30 minutes, 1 hour, and 24 hours

If creating an AMF task, configure the corresponding measurement tasks based on network element AMF, measurement parameters, measurement granularity, measurement period, etc. After creating the task, click “activate” on the right side. If the

task is interrupted, you can click “stop task”. After creating a task, the details on the right side of each task can be viewed to provide specific information about the task being created.



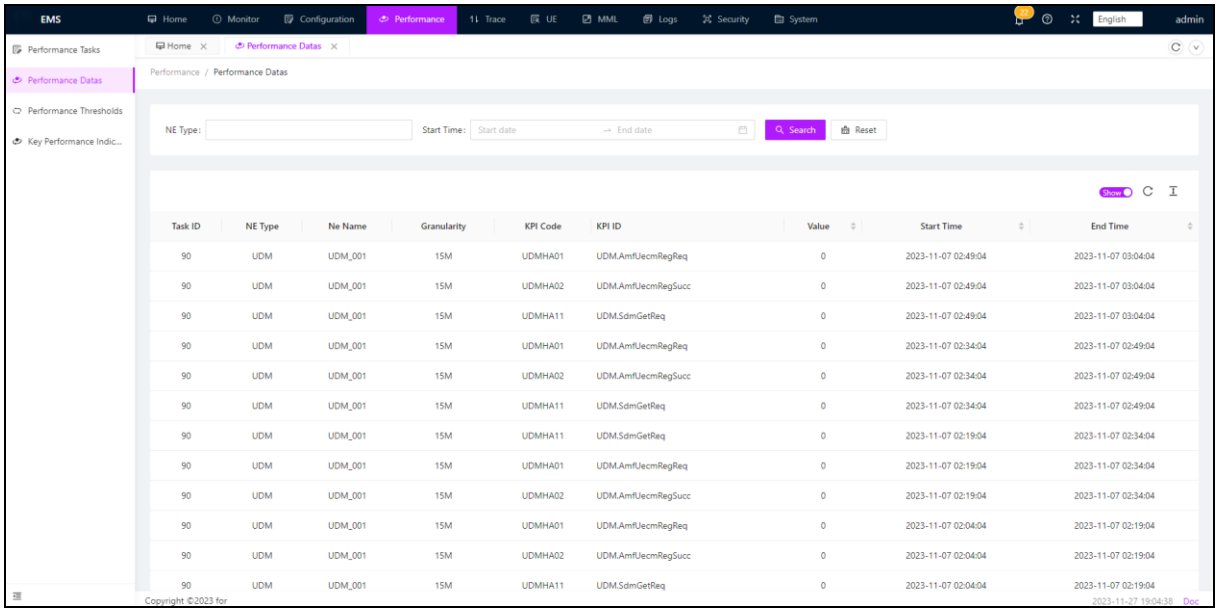




3.5.2 Performance Data

Performance data refers to collecting and recording performance indicators of core NE in different time periods, and then analyzing and displaying the data. Performance data shows the metrics measured in the performance tasks created in the performance tasks

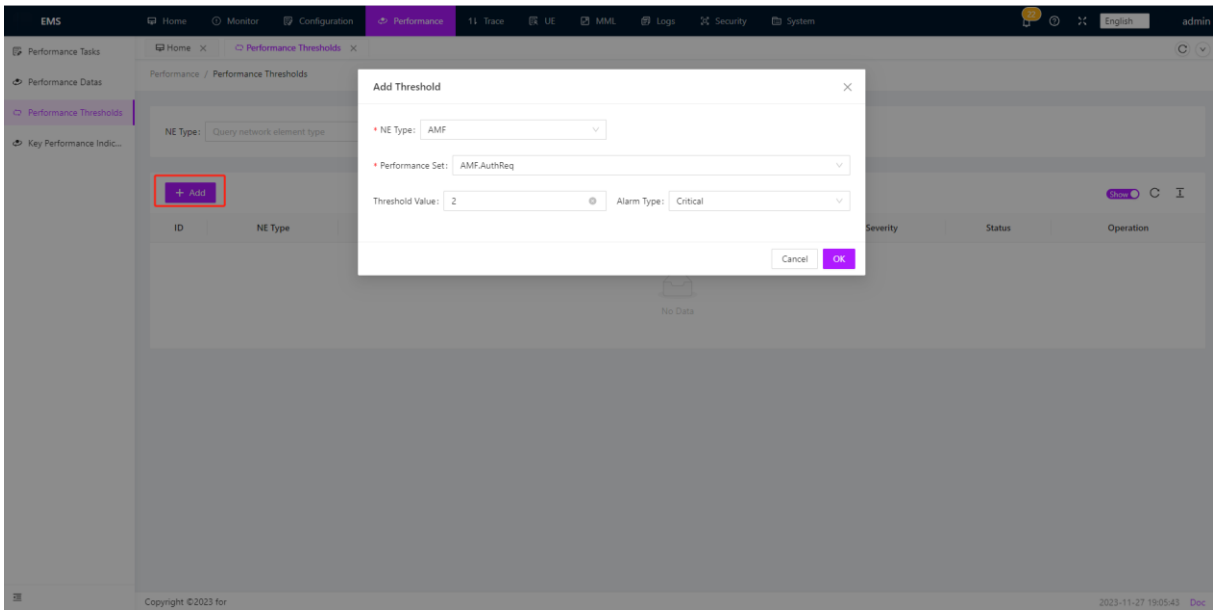
Network element measurement tasks can be formulated based on measurement tasks, and corresponding statistical indicator item values can be viewed based on network element type and task ID:



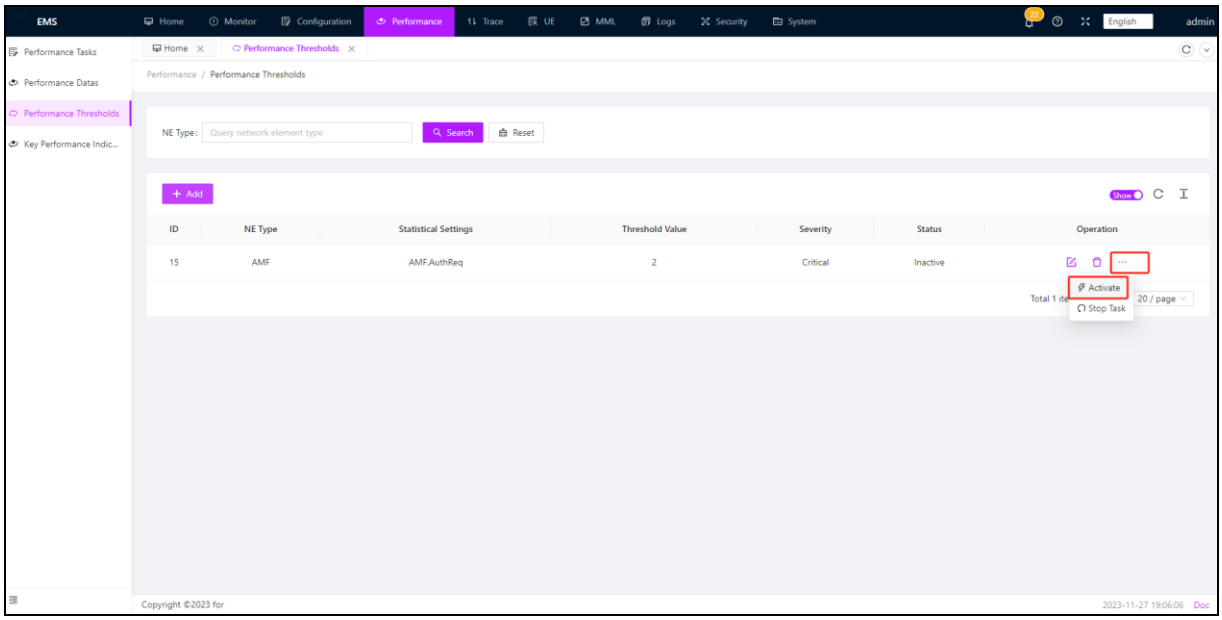
3.5.3 Performance Thresholds

Performance threshold: The performance threshold refers to a normal range and a warning range for performance data to detect anomalies in a timely manner. The performance threshold must be set based on the current network load, topology, requirements, and device performance.

OMC monitors performance measurement items defined by performance thresholds and generates business quality alerts to alert business anomalies when performance measurement data exceeds the threshold. The generated alarms will be displayed in the active alarms and historical alarms in the monitor

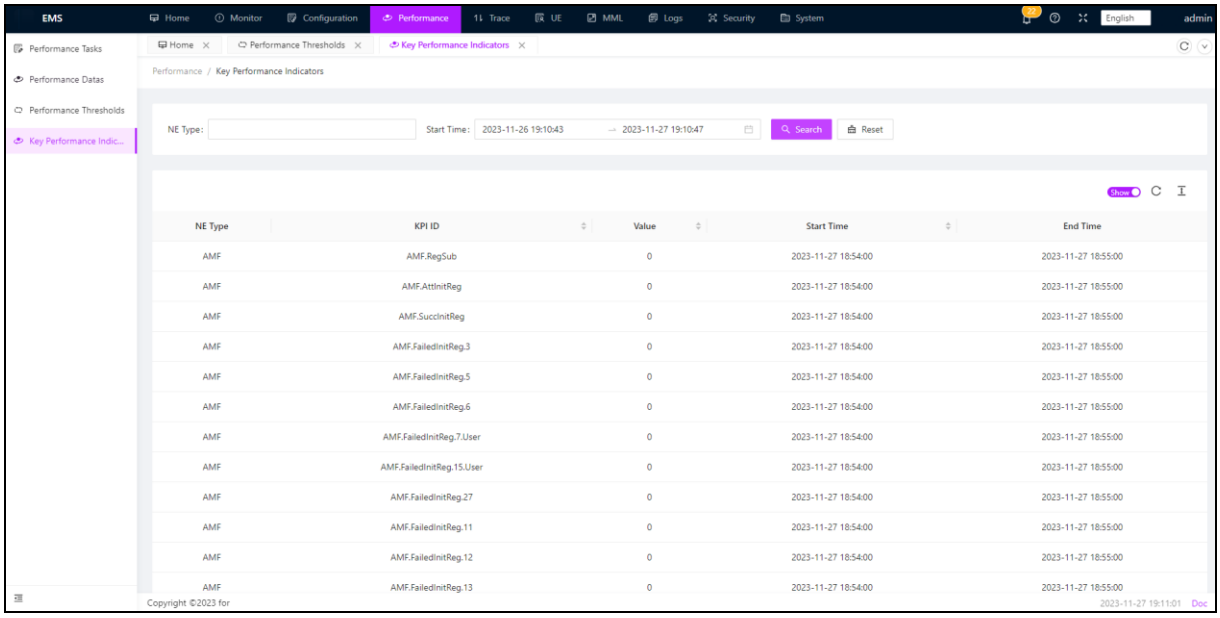


Activate after successfully adding tasks



3.5.4 Key Performance Indicators

Key performance indicators: Key performance indicators of core NE, which directly affect network stability and user experience. By monitoring important performance indicators, you can find performance problems in time and take appropriate measures to ensure efficient network operation and user satisfaction.



3.6 Trace

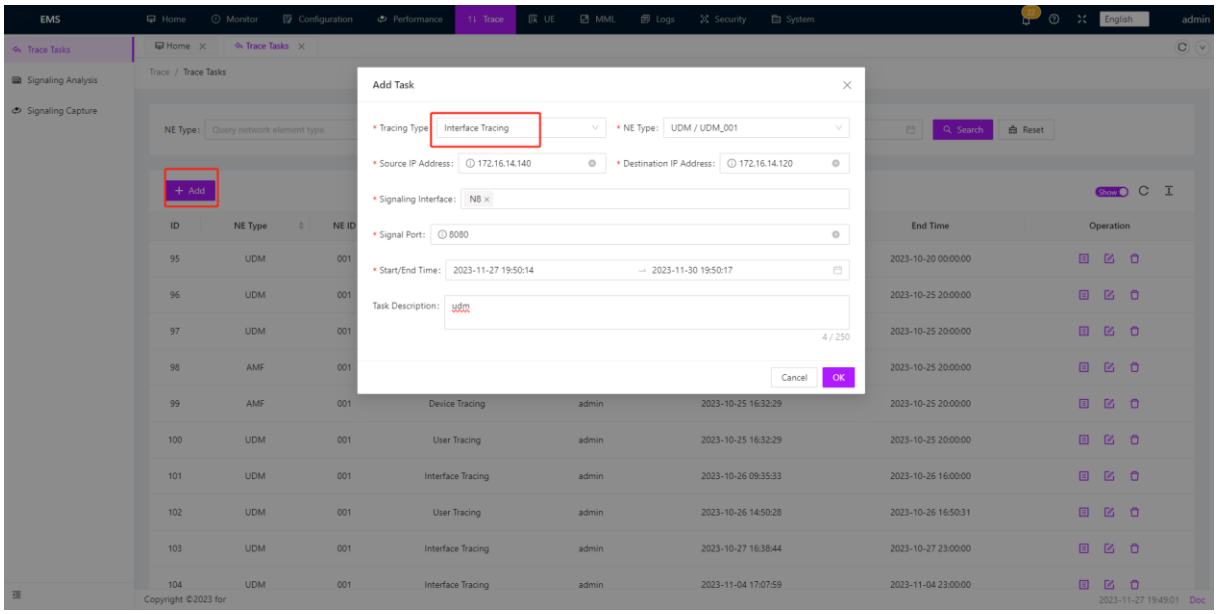
Trace management refers to the management method of monitoring and analysing

key business processes and signalling in the core network. It realizes real-time monitoring and troubleshooting of core network by establishing tracking task, analysing signalling and capturing signalling. In trace management, currently trace tasks related to user data management (UDM) can only be established, including interface trace, device trace, and user trace.

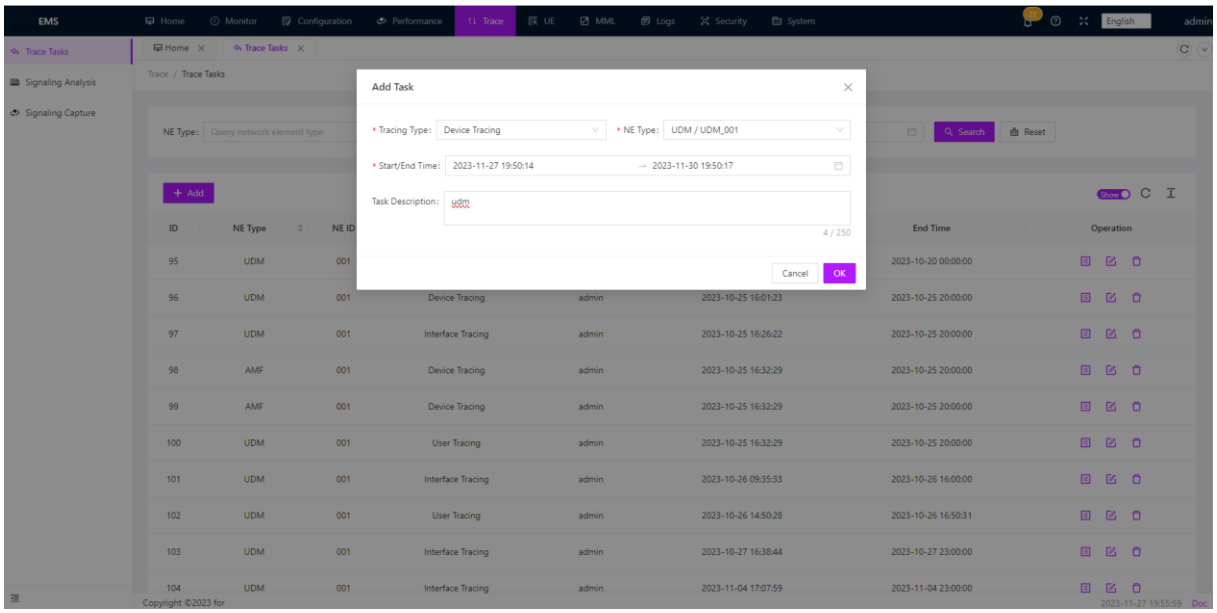
3.6.1 Trace Tasks

The trace task is the basis of the core network trace management and is used to monitor and analyze specific core network business processes. In trace management related to user data management (UDM), trace tasks can be classified into interface trace, device trace, and user trace.

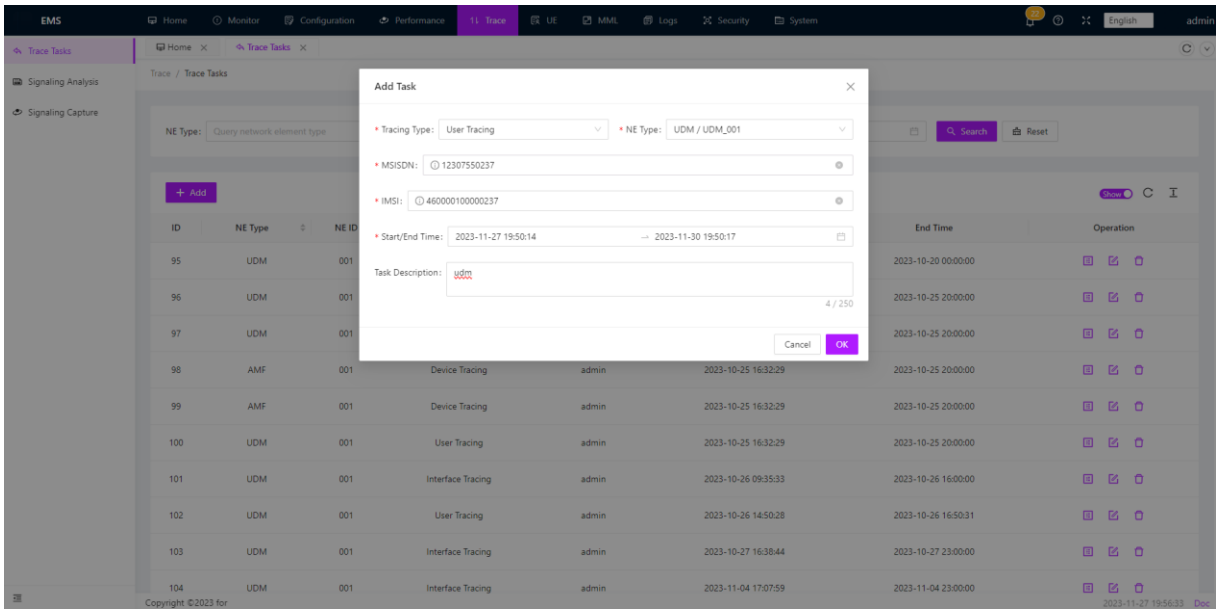
Interface Tracing：



Device Tracing:



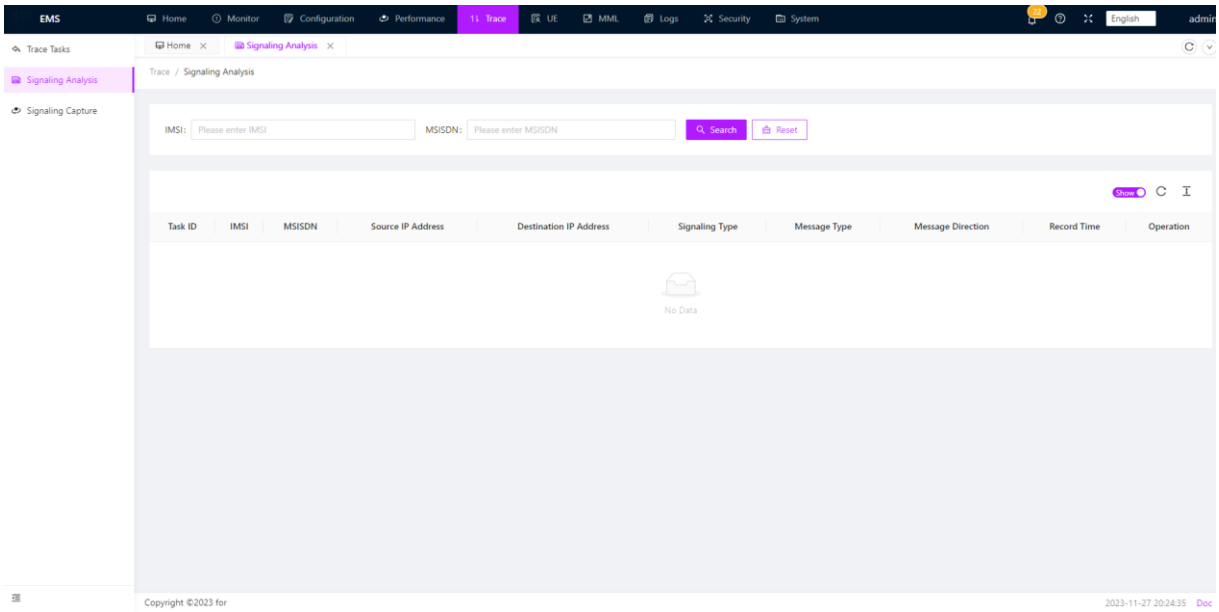
User Tracing:



3.6.2 Signaling Analysis

Signaling analysis is to monitor and analyze signaling data transmitted by the core network in real time, and extract valuable information and indicators from it. By in-depth analysis of signaling data, you can discover network performance problems, faults, and anomalies in a timely manner, and provide references for fault diagnosis and performance optimization. (Remember to set the gtpUri as omc ip at

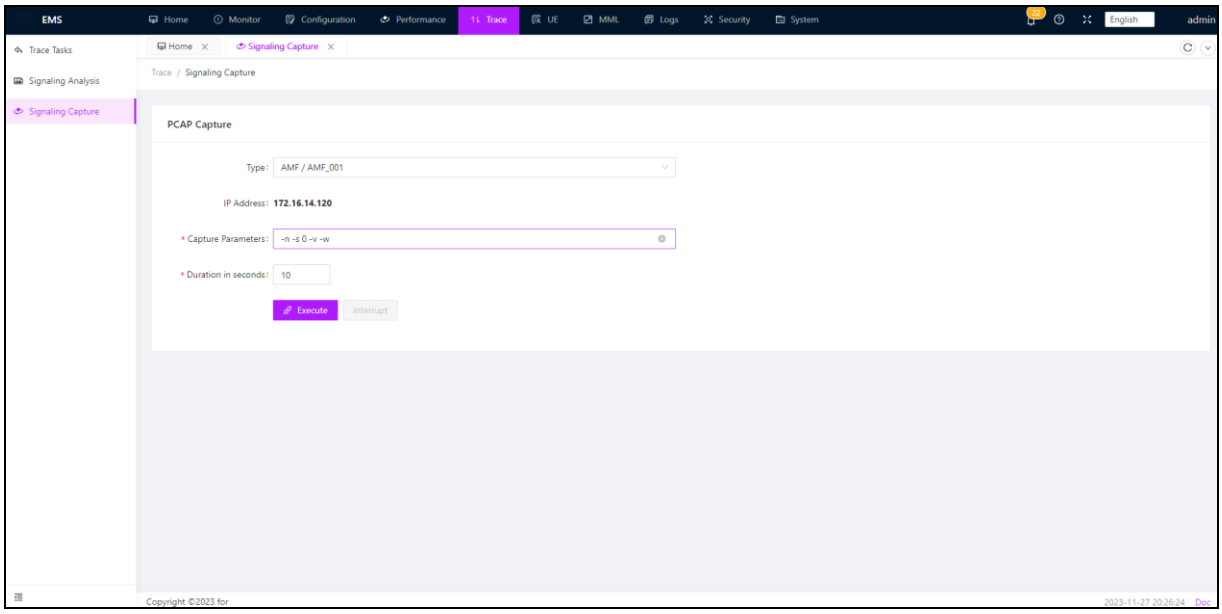
/usr/local/omc/etc/restconf.yaml and enable trace in udm at /usr/local/etc/udm/udmcfg.yaml)



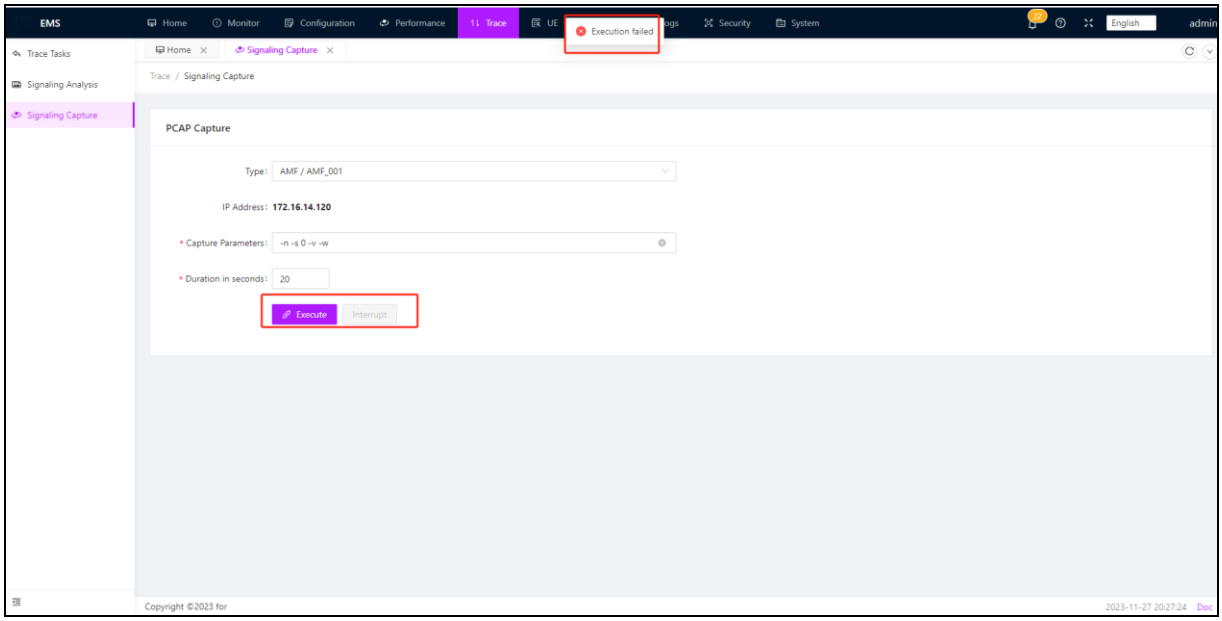
3.6.3 Signaling Capture

Signaling capture: Signaling capture refers to capturing and recording specific signaling traffic in the core network for subsequent analysis and debugging. Through signaling capture, the operator can conduct detailed inspection and analysis of the relevant signaling when there is a problem, help locate the cause of the fault, and formulate targeted solutions. At present, signaling capture of each NE can be realized.

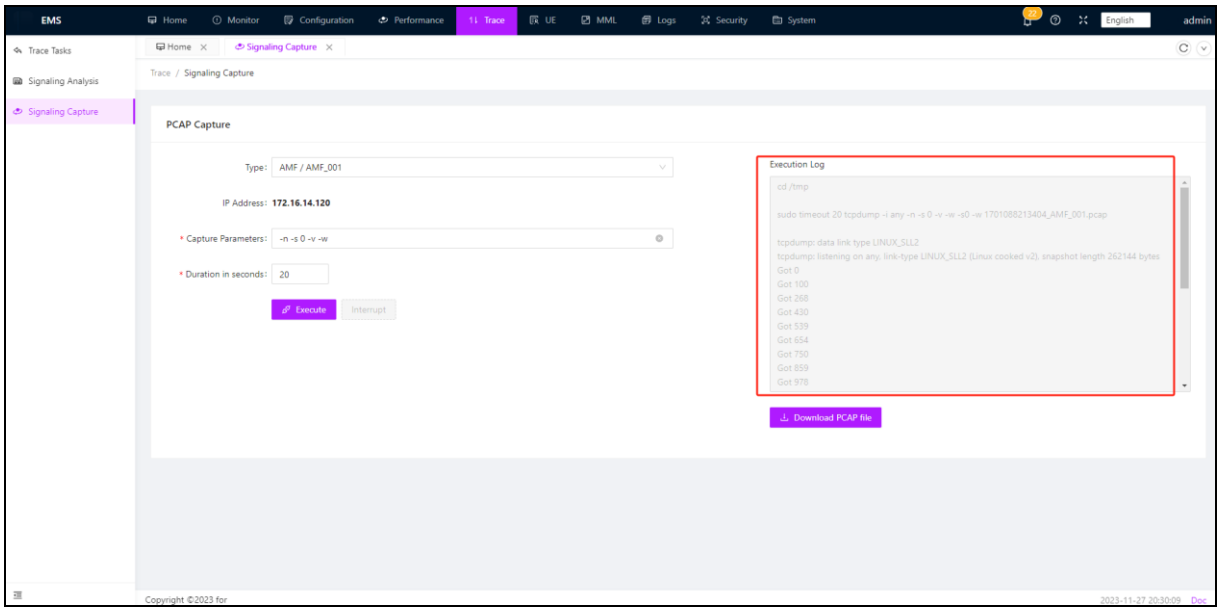
On the signaling capture screen, select the NE for which the signaling is to be captured, enter arrest parameters and arrest time, and click Execute. After the capture is complete, you can download the packet on the right.



Clicking "interrupt" during the execution process can stop capturing packets midway, and if you click “execute”, you can re-execute the packet capture task.



After the packet capture is completed, you can view the packet capture result on the right side, the name of the packet capture, and the number of captured packets.



After completing the execution, click the "Download PCAP File" button in the bottom right corner to download the file.

3.7 UE

Core network terminal management refers to the management and control of terminal devices in the core network to ensure the security and smooth operation of the network. The core network terminal management includes the UDM authentication and UDM subscribers in the User data management (UDM), and the management of IMS online users, UE online information, and NODEB information.

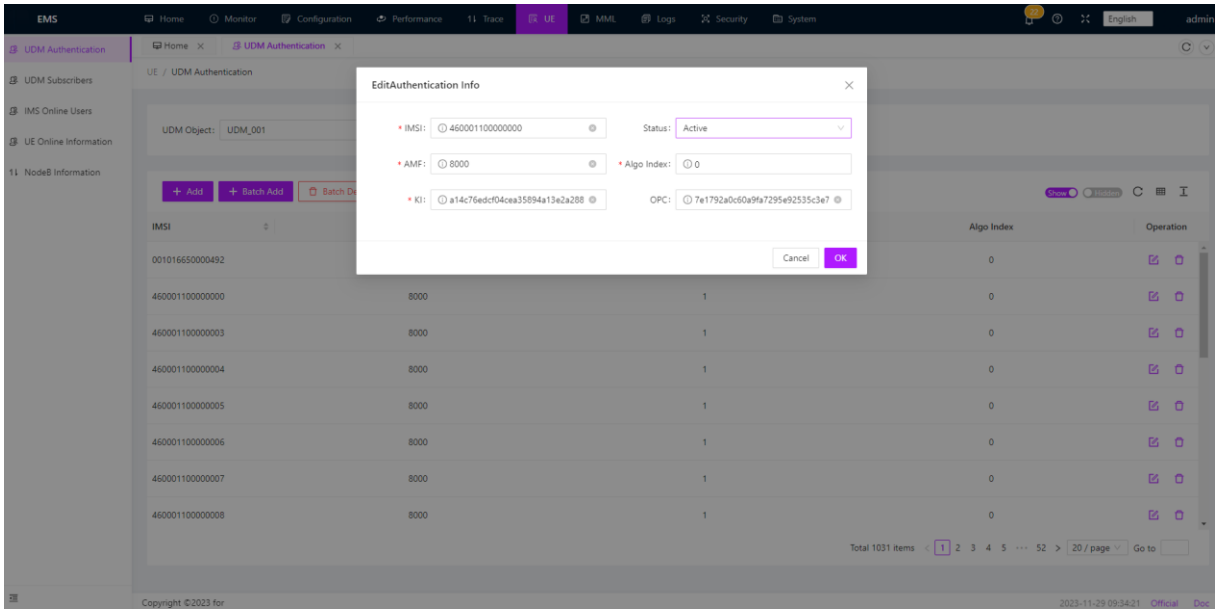
Through effective core network terminal management, operators can ensure the security and reliability of terminal equipment, improve the stability and performance of the network, and provide users with high-quality services and good user experience. At the same time, terminal management can also help operators optimize the utilization of network resources, improve network operational efficiency and cost control.

3.7.1 UDM Authentication

The UDM authentication data is the authentication information of terminal devices stored in the User Data management (UDM). The data includes the KI information and OPC information of terminals, and is used for secure authentication and authentication between terminals and the core network. The core network terminal management can

add, modify, and delete authentication data individually or in batches to ensure the accuracy and timeliness of authentication information.

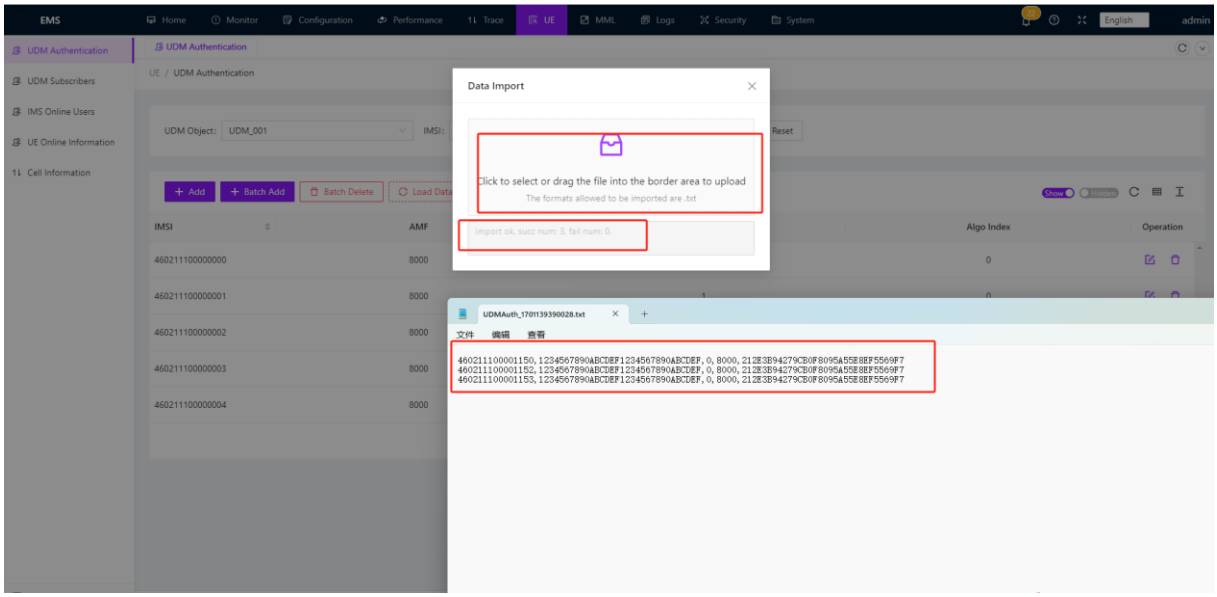
Click , you can view and modify IMSI's ki, OPC, and other parameters



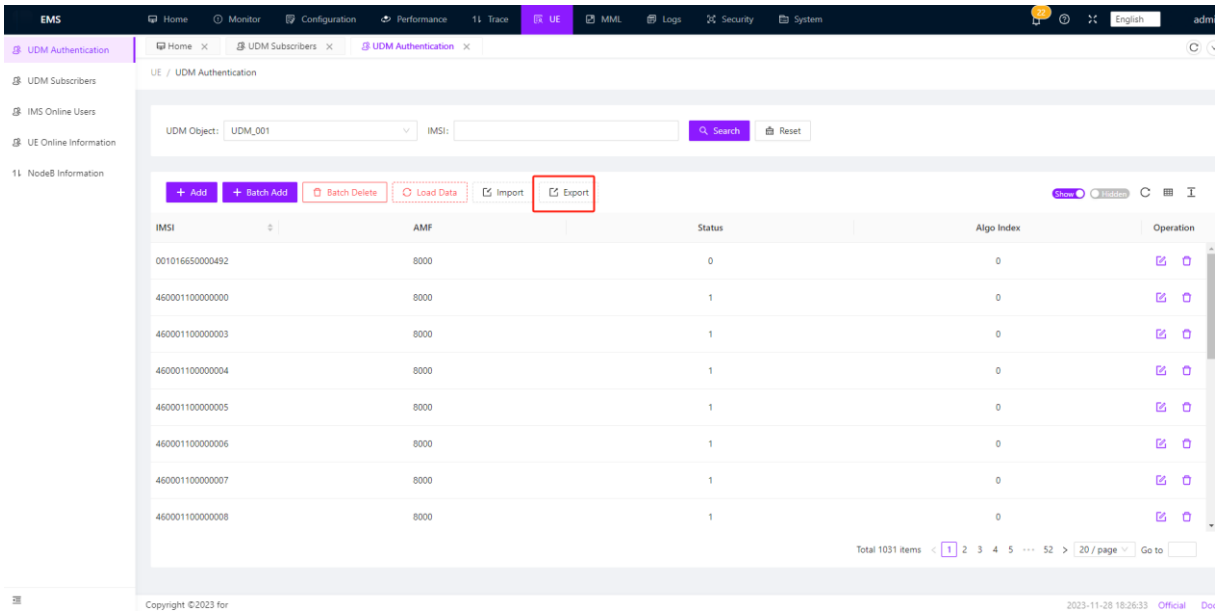
UDM authentication users can be added individually, added in batches, deleted individually, and deleted in batches. Items marked with * are mandatory. After filling them, click OK to proceed.

The operator can import or export individual or batch data using a txt file.

Import: Click "Import", click on the window that pops up, then select the file you want to import. Once confirmed, a prompt will appear below indicating whether the import was successful.



Export: Click the“Export”, the system will export the file and automatically download it.

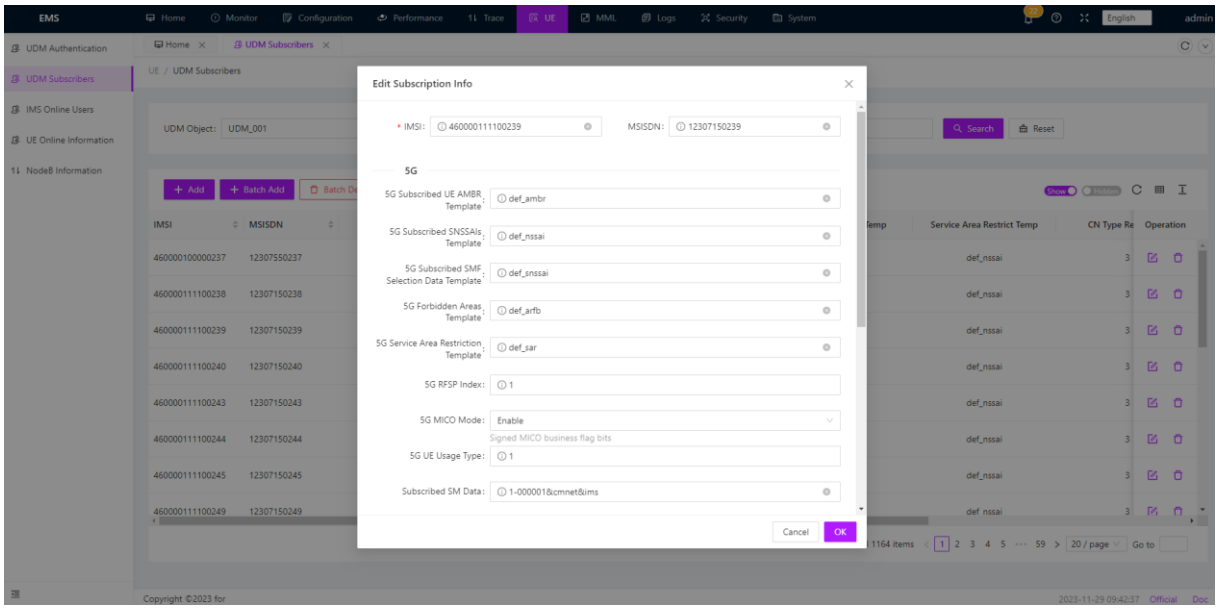


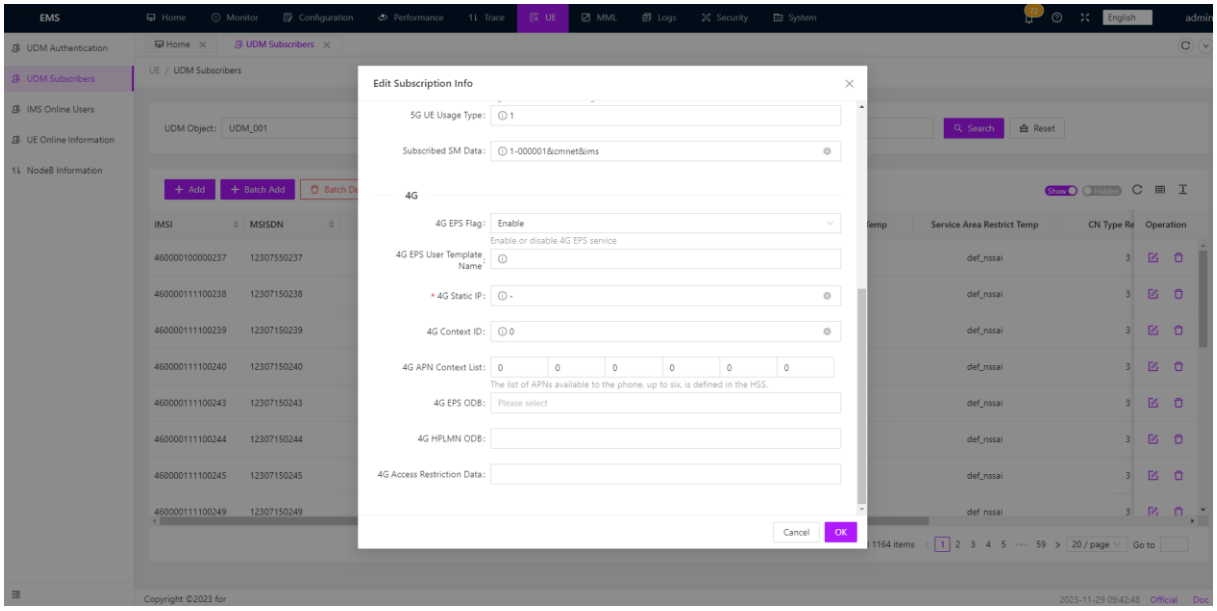
3.7.2 UDM Subscribers

UDM subscriber is the user information of the terminal device stored in UDM. These data include the user's IMSI, MSISDN, SM-DATA, 4G static IP, 4G context list, etc., and are used for user identification and service management of the core network. Core network terminal management can add, modify and delete subscriber data individually or in batches to ensure the integrity and updateability of user information.

Click the modify button on the right to view more detailed user data and make

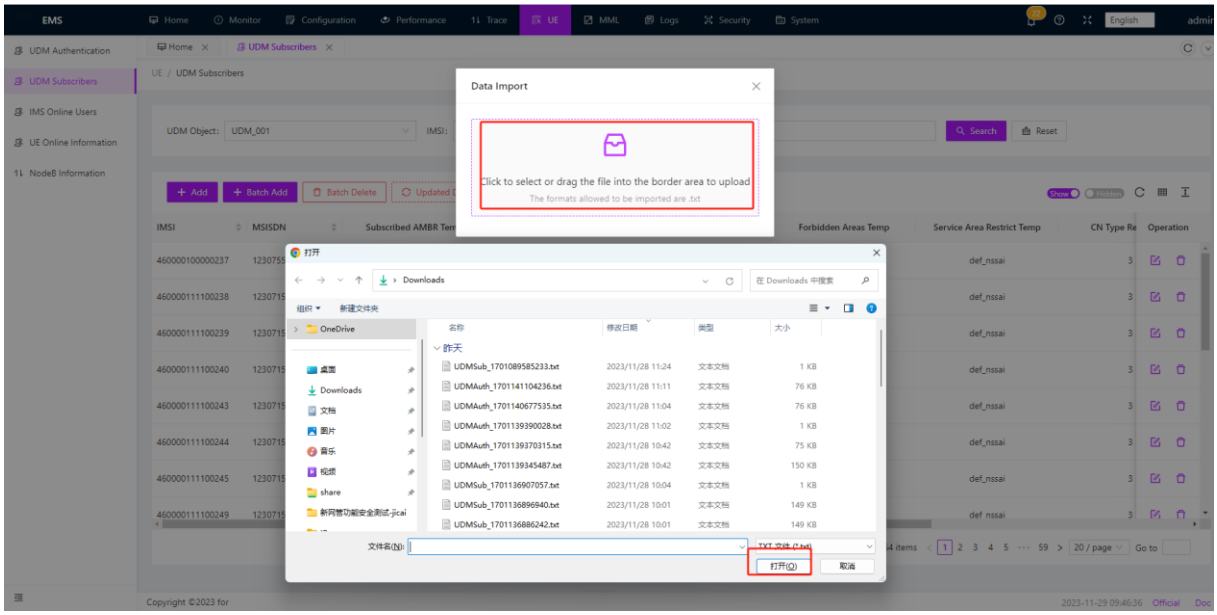
modifications, such as modifying static IP data. Here you can view UDM contract user data, including imsi, msisdn, sm-date, Eps flag and other data

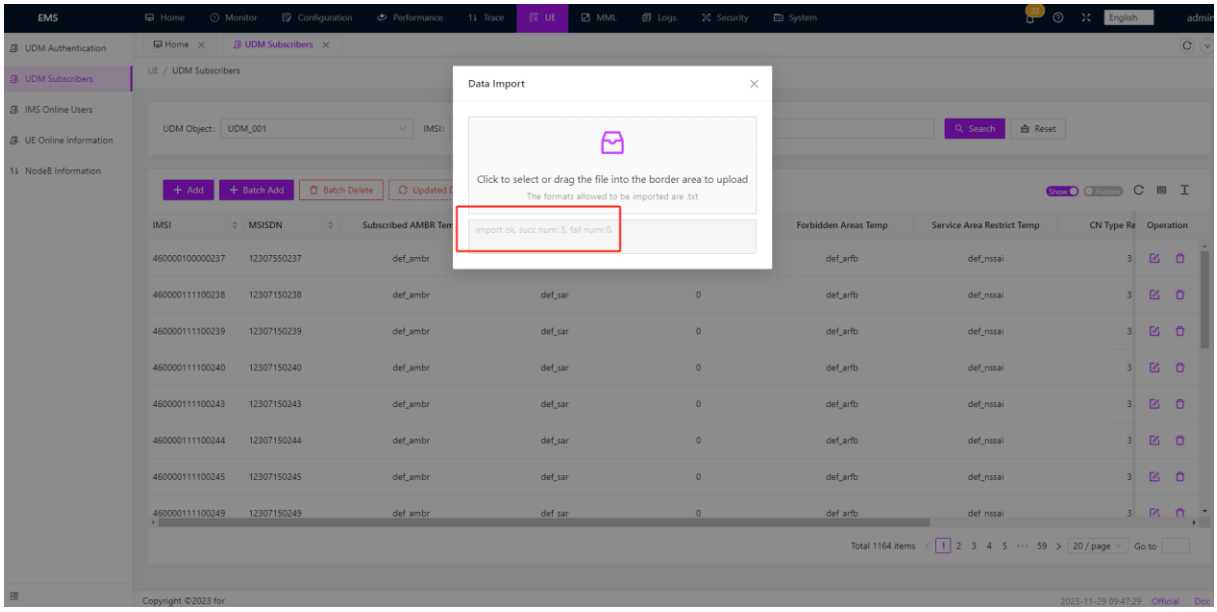




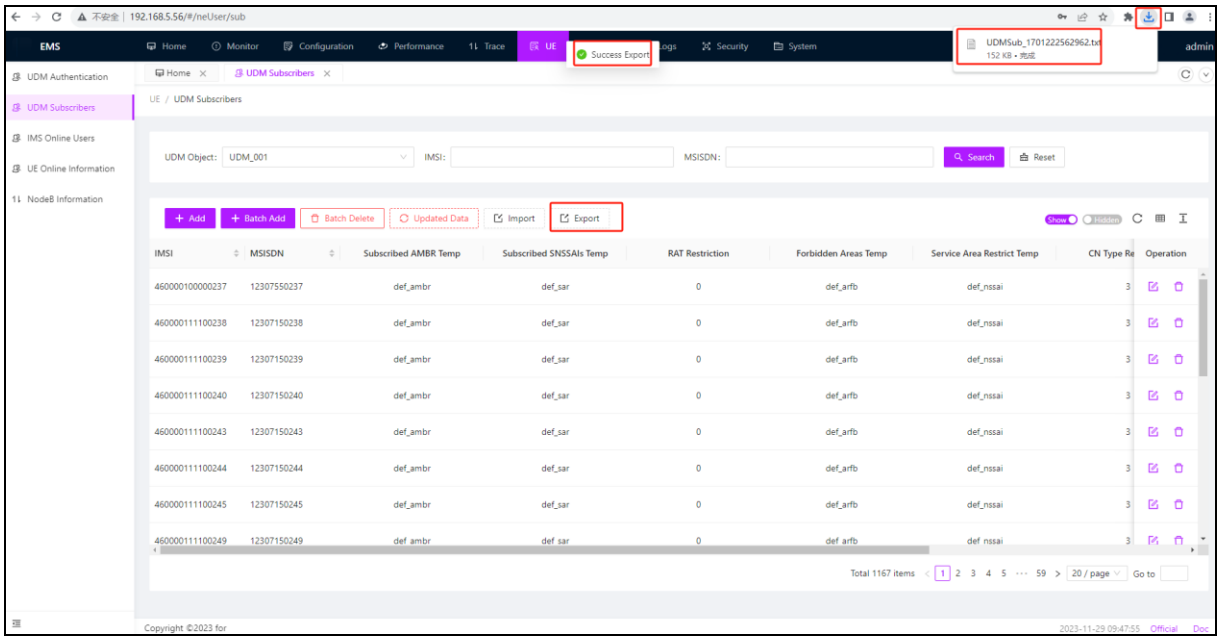
Can import and export UDM Subscribers data:

Import: Click “Import”, click on the window that pops up, then select the file you want to import. Once confirmed, a prompt will appear below indicating whether the import was successful.



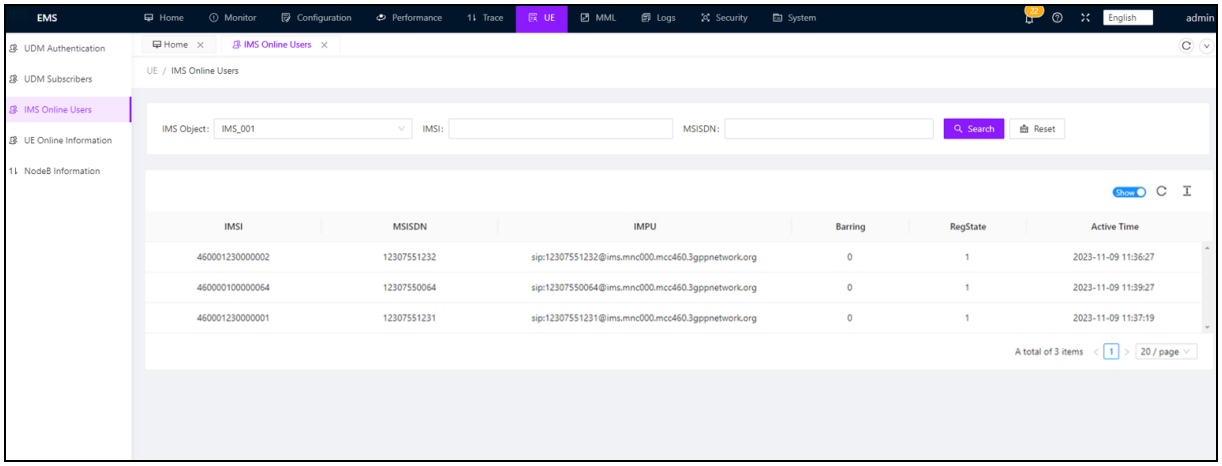


Export: Click the“Export”, the system will export the file and automatically download it.



3.7.3 IMS Online Users

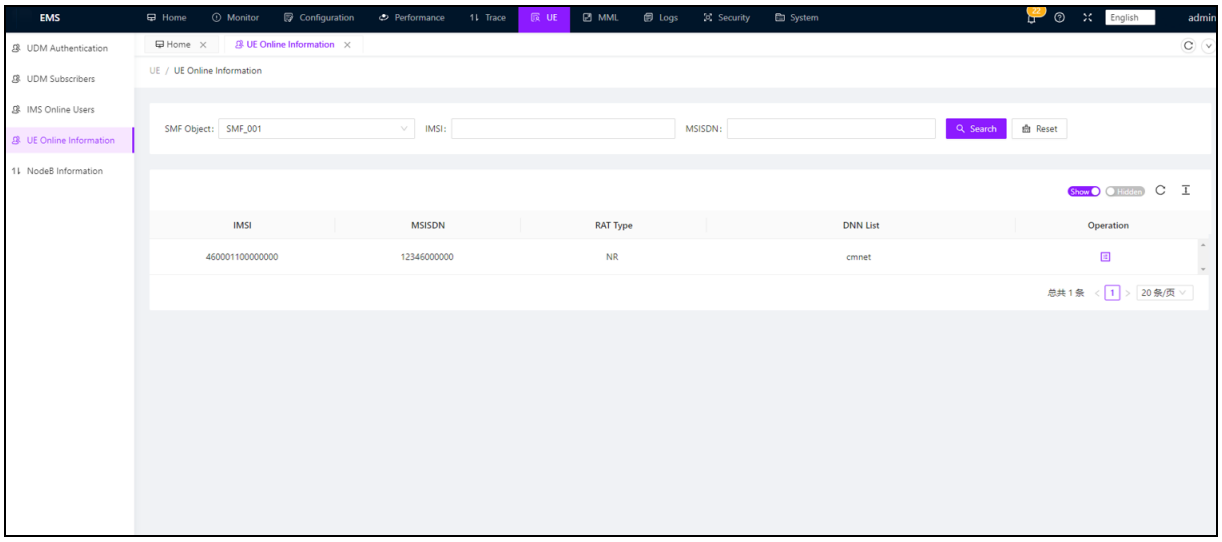
An IMS online user refers to an online user on the core network of the IP-based multimedia subsystem (IMS). Core network terminal management monitors and manages IMS online users, including the number of online users, user IMSI, MSISDN, registration loading, and activation time, to ensure proper allocation of network resources and optimize performance.



3.7.4 UE Online Information

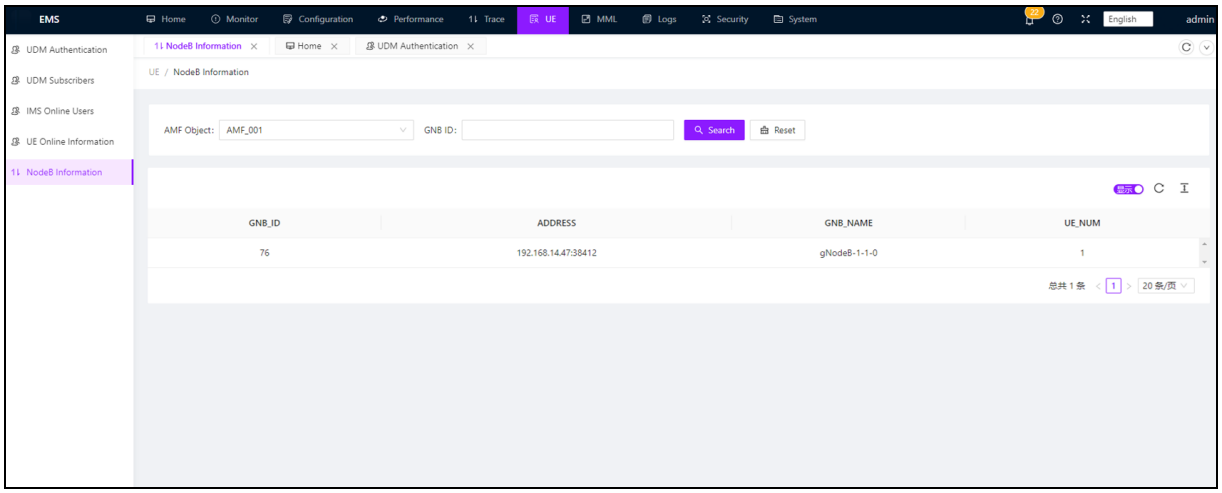
UE online information refers to the online status and connection status of terminal devices in the core network. Core network terminal management can monitor the

online status of terminals in real time. Users registered in SMF can view UE information such as IMSI, MSISDN, RAT Type, and DNN List



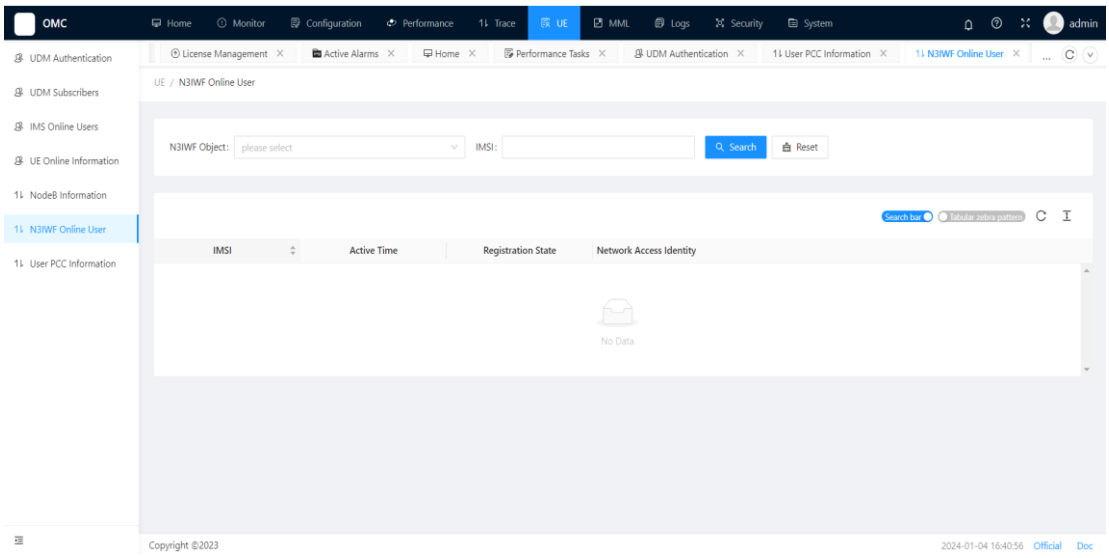
3.7.5 NodeB Information

NodeB information: Base station information refers to the relevant information of base station equipment in the core network, including the IP, ID, name of the 4G and 5G base station and the number of UE of the access base station. OMC can manage the information of base stations connected to AMF, so that operators can better understand the number and information of base stations connected to AMF.



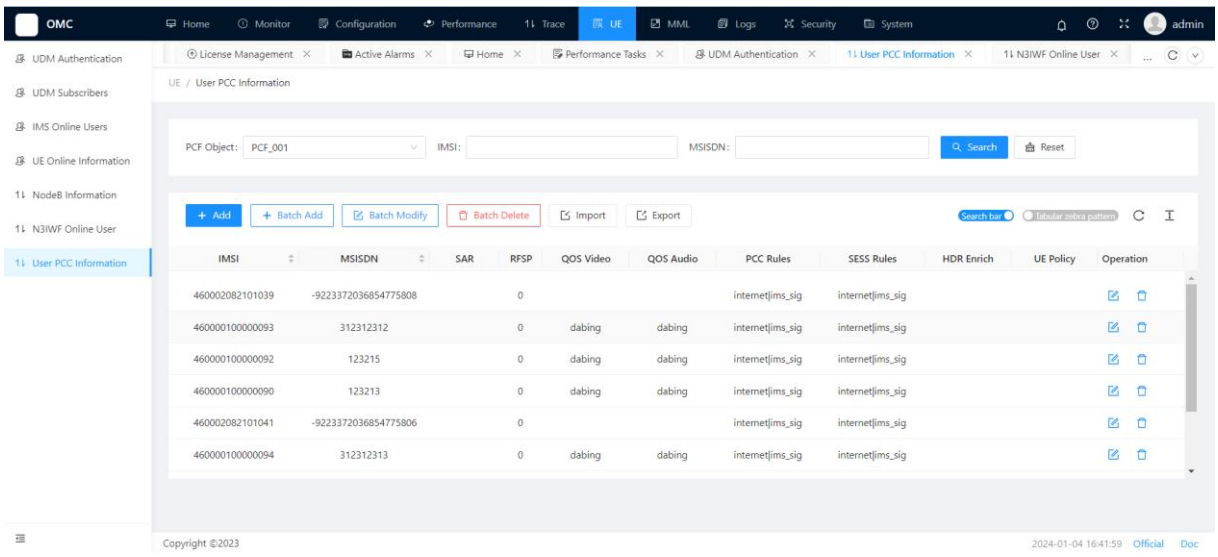
3.7.6 N3IWF Online User

N3IWF online users can monitor N3IWF online users in real time and view the IMSI, Active Time, Registration State and Network Access Identity used online.



3.7.7 User PCC Information

User policy control information can set different PCC Rules and SESS Rules for different users.



3.8 MML

MML (Man-Machine Language) management refers to the method of managing and configuring various parts of the core network by using specific command languages. MML management covers NE operation, UDM operation, and OMC operation.

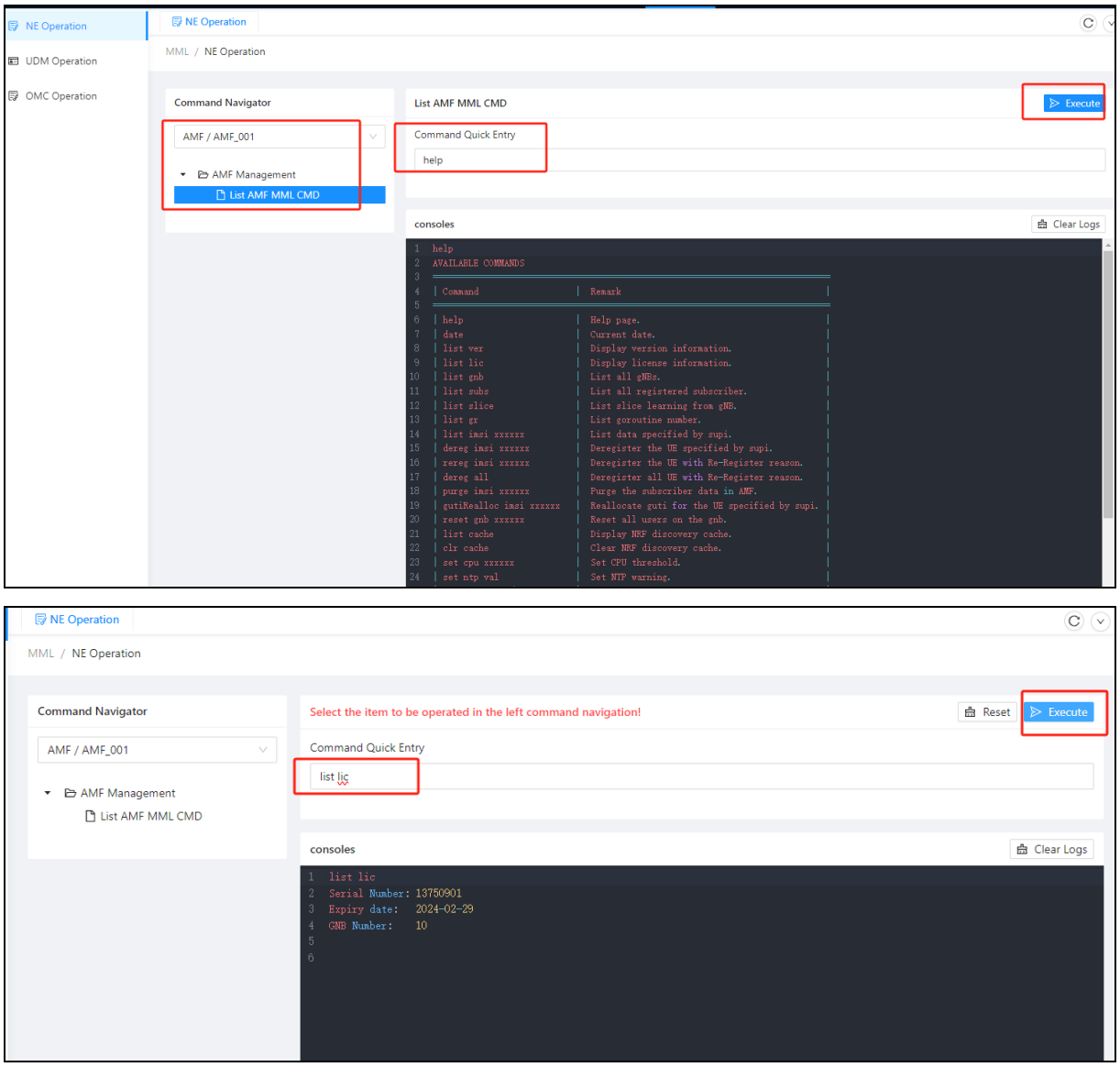
Through MML management, operators can manage and configure the core network to ensure the stable operation and high performance of the network. MML commands

are flexible and scalable, and can be customized and configured according to specific network needs and operator requirements. At the same time, MML management also requires operators to have the appropriate technology and knowledge to ensure the accuracy and safety of management operations.

3.8.1 NE Operation

NE manage and configure core network elements through MML commands. Network element operations can query and configure the data information of each network element, such as querying the license information and version information of the network element, querying the access base station information in AMF, adding and deleting user data in batches in UDM, etc. Through MML commands, operators can flexibly and accurately configure network elements of the entire core network to meet network performance requirements.

Operation steps: Select the network element that needs to be operated in the network element operation interface, click "List XXX MML CMD" below, and then click "Execute" on the right side. A console will pop up below, and the console will display operation commands and command explanations of the network element. Click "Clear Logs" to clear the console. If you need to enter a command, enter the command in the box below "Command Quick Entry", such as entering "list lic", and then click "Execute", the corresponding result will appear in the console.



3.8.2 UDM Operation

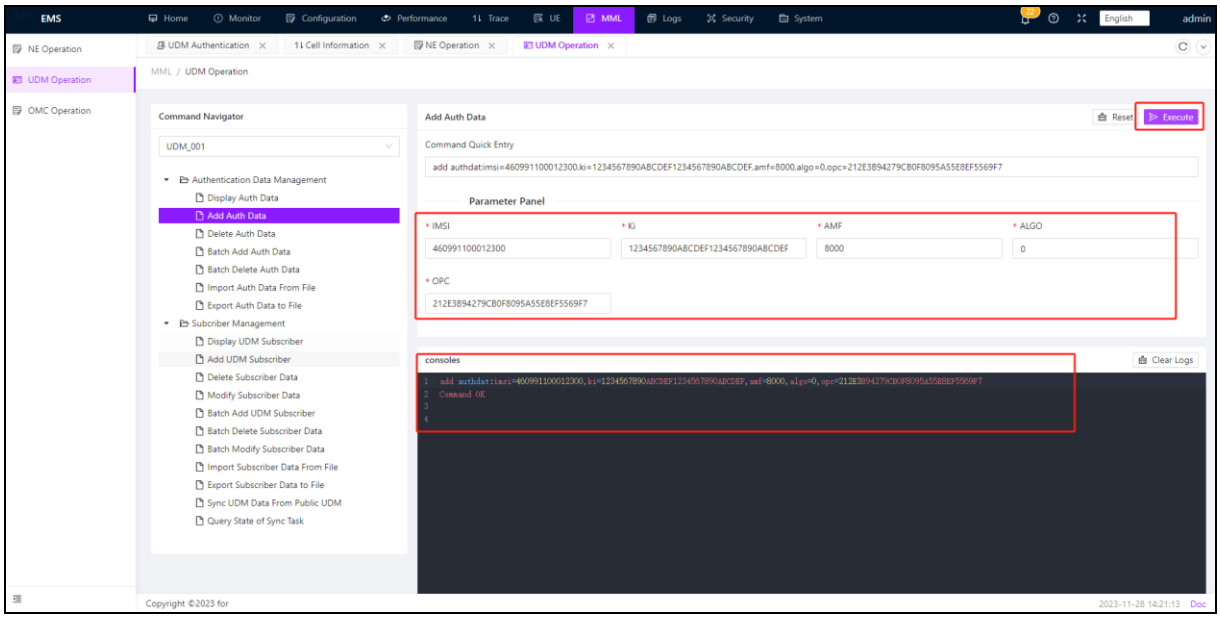
The UDM operation are mainly configured for user data management (UDM). This section describes how to configure UDM authentication information, including the identity and key information of the terminal device, to ensure the correct security authentication. At the same time, UDM operation also include the configuration of UDM subscribers, including user identity information, subscription information, and service configuration.

You can operate on UDM subscribers' data and authentication data, including adding, deleting, batch adding, batch deleting user data, and authentication data. The functions of each command are as follows: click on the command with a red * mark as a

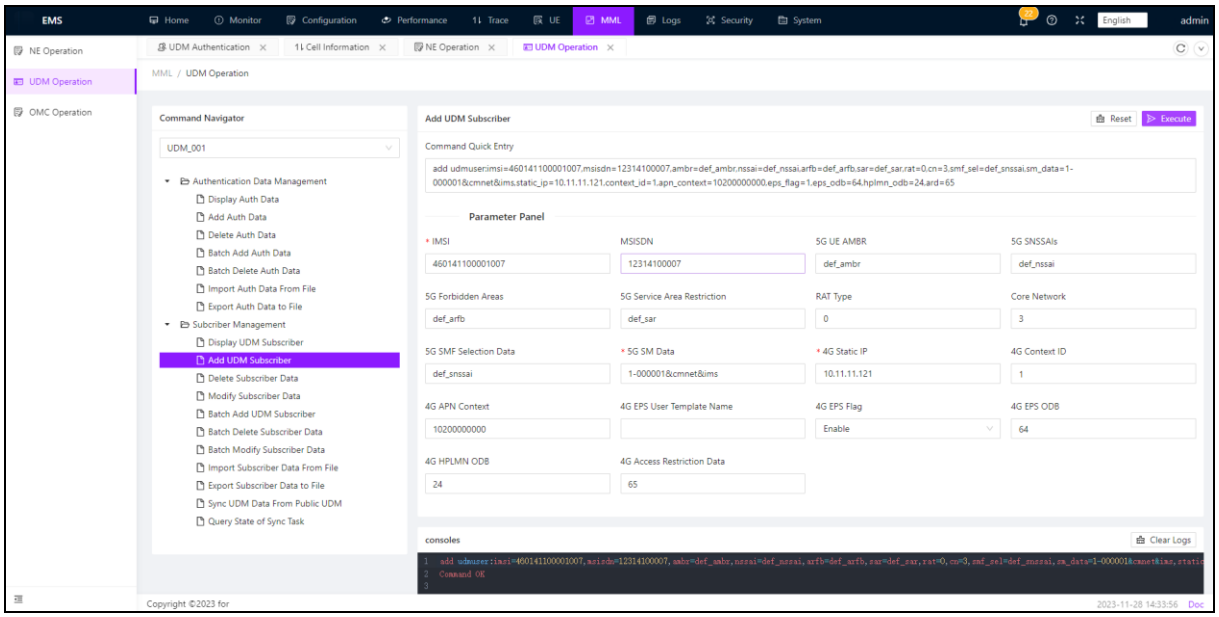
required field, and then click "Execute" in the upper right corner. The result is displayed in the black window below.

MML Commd
Export Subscriber Data to File
Display UDM Subscriber
Add UDM Subscriber
Delete Subscriber Data
Modify Subscriber Data
Batch Add UDM Subscriber
Batch Delete Subscriber Data
Batch Modify Subscriber Data
Import Subscriber Data From File
Upload Subscriber Data
Sync UDM Data From Public UDM
Query State of Sync Task
Display Auth Data
Add Auth Data
Delete Auth Data
Batch Add Auth Data
Batch Delete Auth Data
Import Auth Data From File
Export Auth Data to File

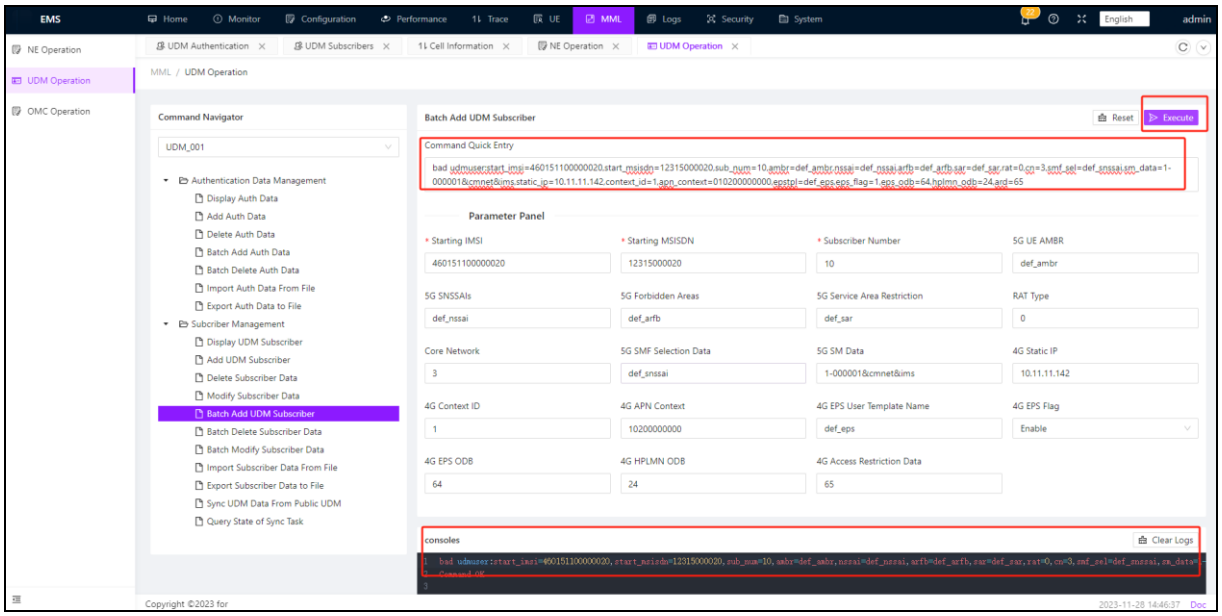
Add UDM Auth data as follows:



Add UDM Subscriber data as follows:



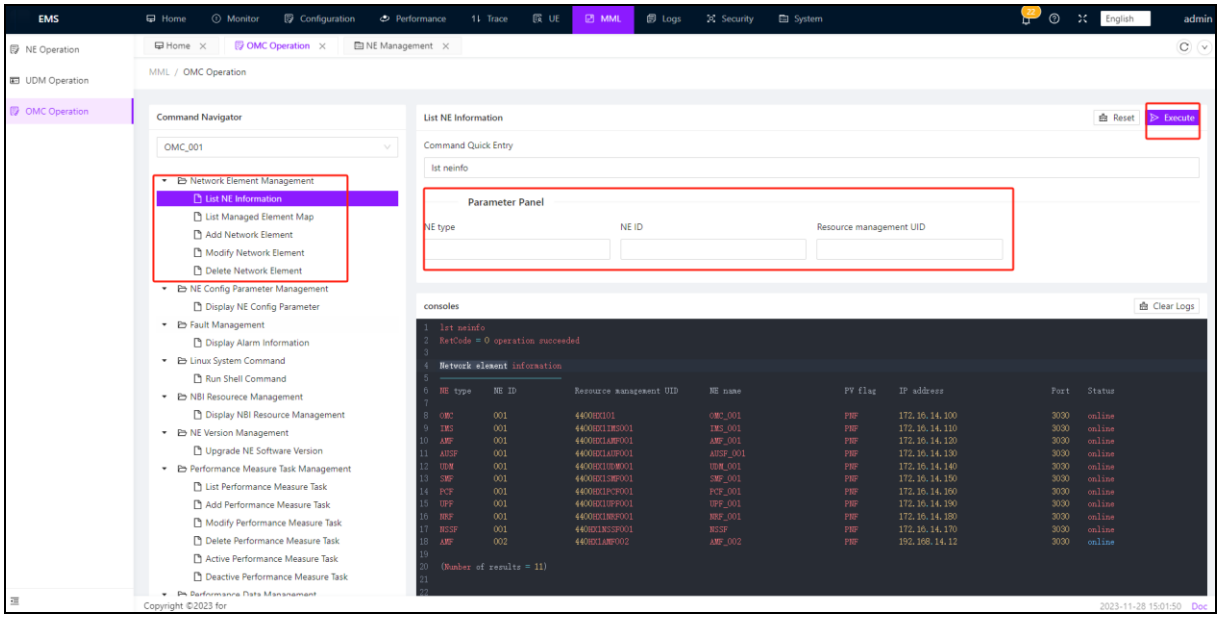
The operator can also enter the MML command in the box below “Command Quick Entry” and click execute:



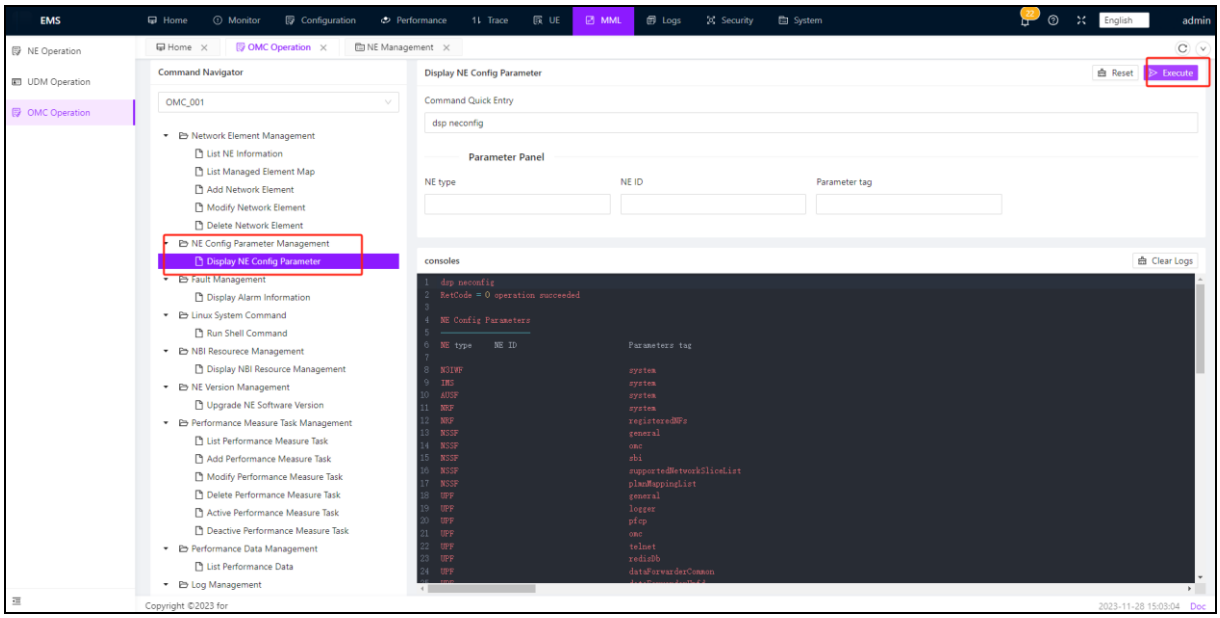
3.8.3 OMC Operation

OMC operates and manages the management parts of the core network. This includes the management of NEs, such as adding, deleting, and modifying NE information. Manage NE configuration parameters, for example, query NE configuration parameters. Perform fault management operations, such as querying alarms of NEs such as AMF. Performance management operations, such as the collection and analysis of performance data; Perform system management operations, such as querying the system information of NEs such as AMF.

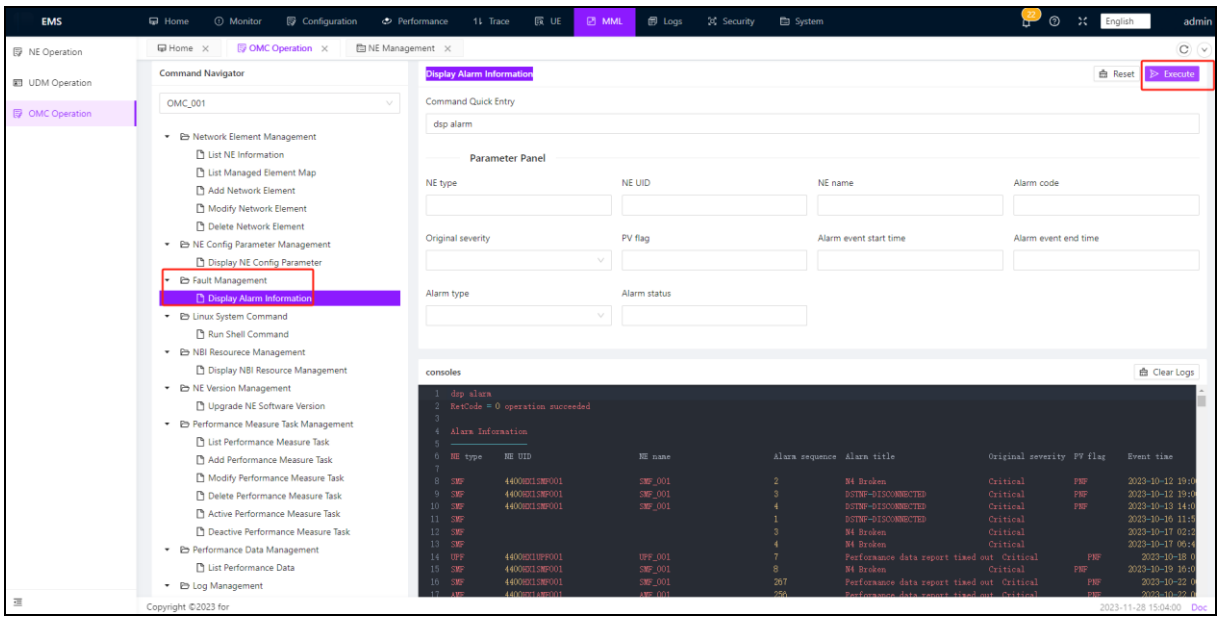
NE Management:



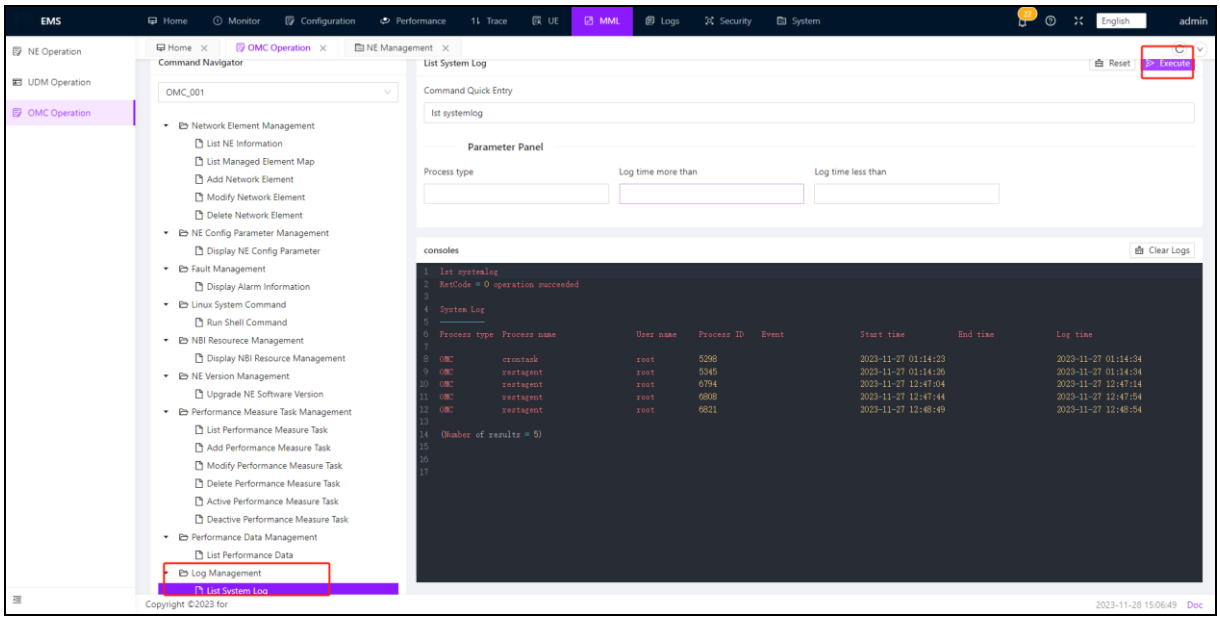
NE Config Parameter Management:



Fault Management:



Log Management:



3.9 Logs

Core network Logs management is a critical part of network uptime maintenance, allowing managers to track the status of various parts of the core network, record potential problems, and perform troubleshooting and performance analysis. Logs management covers operation logs, MML logs, security logs, alarm logs, and alarm forwarding logs.

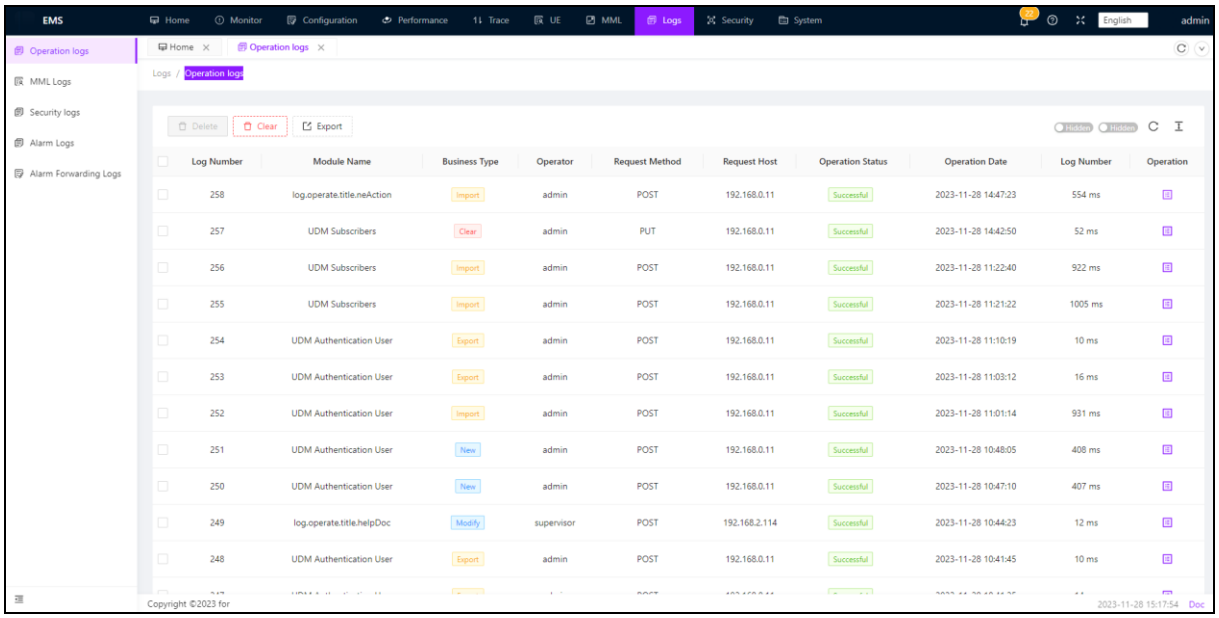
Logs management is an important support for efficient and accurate operation and maintenance, and plays a very important role in ensuring the stable operation of the core network, protecting network security and optimizing network performance. In practice, Logs management generally needs to be combined with the corresponding log analysis tools, through the comprehensive analysis of a variety of logs, in order to play the maximum value.

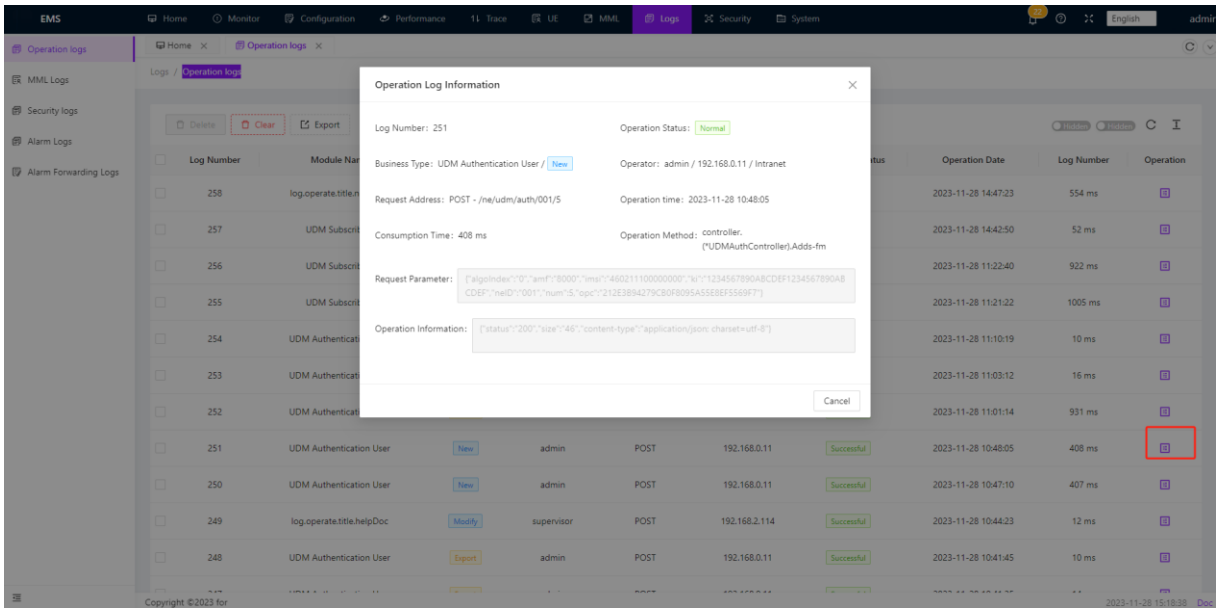
3.9.1 Operation logs

Operation logs record detailed information about operations performed by O&M personnel on network devices or systems, such as data change, system configuration, and account management. These logs can be used for analyzing system health, troubleshooting, and auditing.

The operator can view the operation records related to network management, and

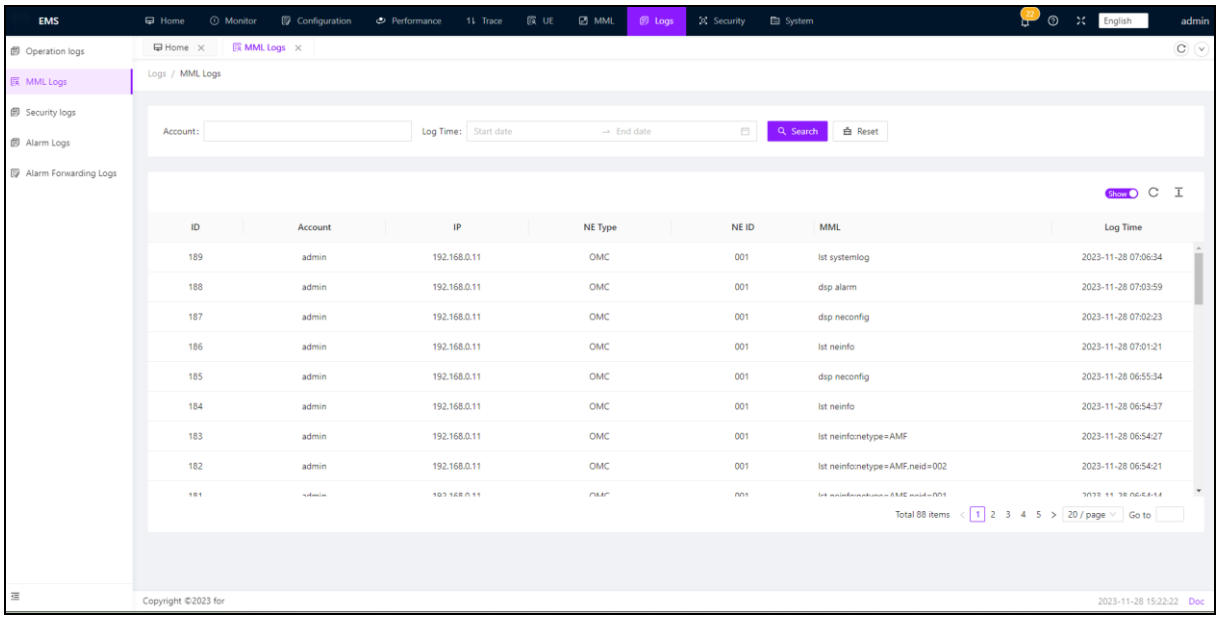
specific operation information can be seen in the details on the right side.





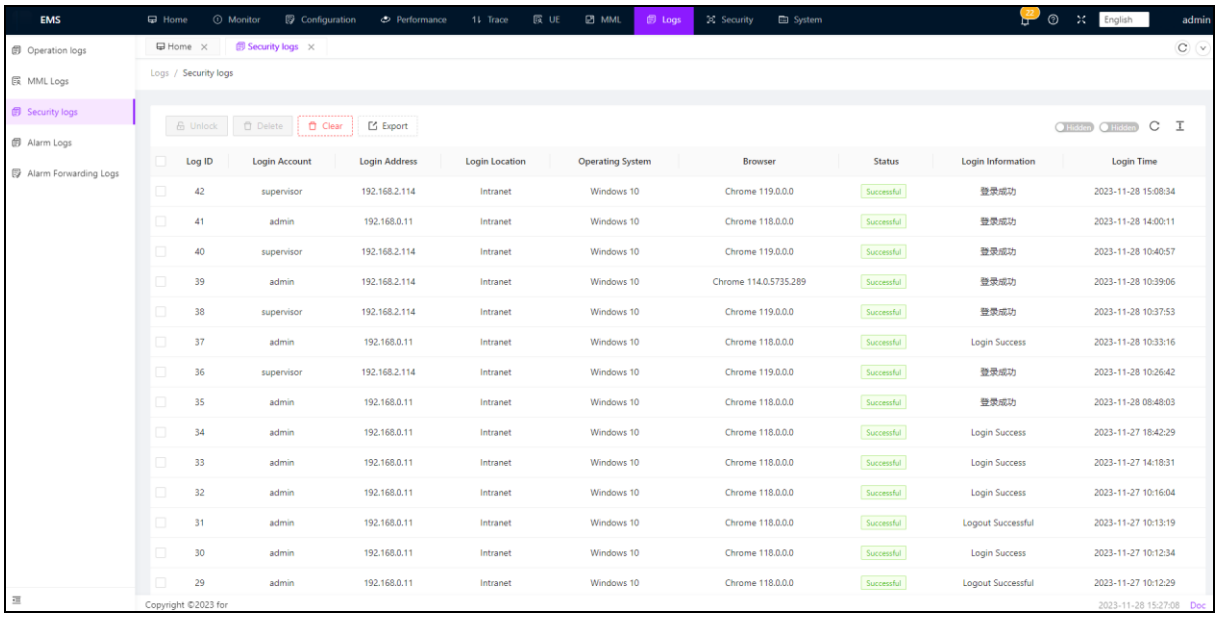
3.9.2 MML Logs

MML logs record operations performed using MML commands. This includes any parameter configuration, status query, etc., which is very helpful for auditing configuration changes of the core network, identifying configuration errors, fault tracing, etc.



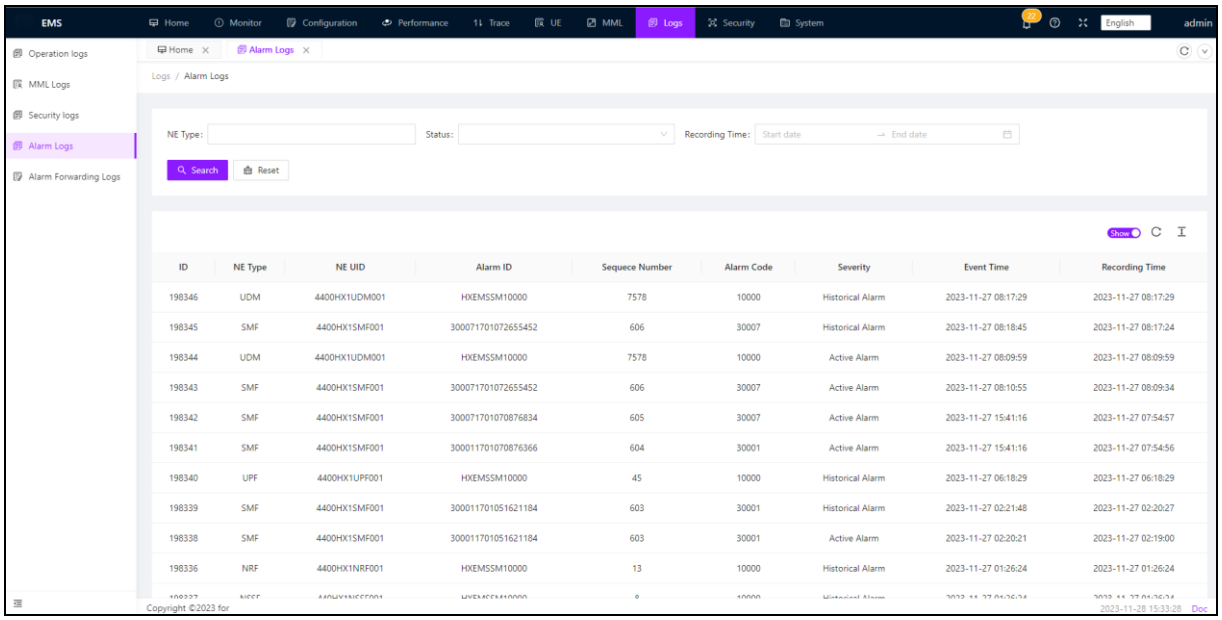
3.9.3 Security logs

Security logs record user login information, including login account, IP address, operating system, login time, and status. It is used to monitor and ensure the security of the core network, as well as to analyze and find security problems when they occur.



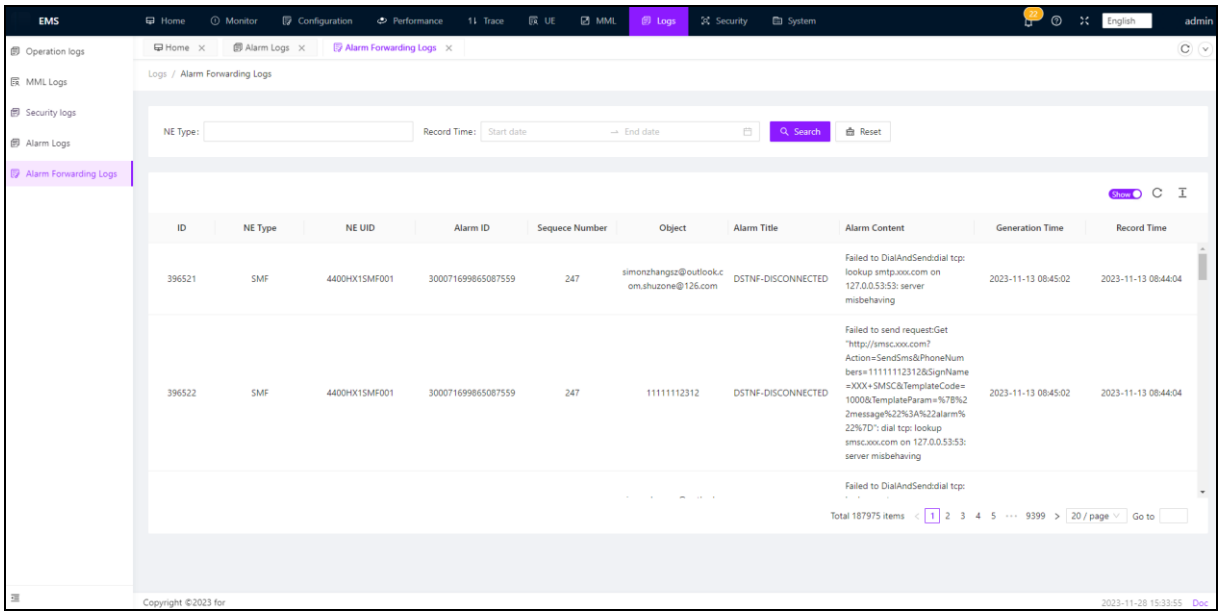
3.9.4 Alarm Logs

Alarm logs record all information about system faults, exceptions, or important events, including activation alarms and historical alarms, so that O&M personnel can quickly locate and rectify existing problems.



3.9.5 Alarm Forwarding Logs

The alarm forwarding log records all the alarm events that are forwarded. It is useful for the administrator to track and handle alarms and check whether alarms are correctly routed to the target processing system.



3.10 Security

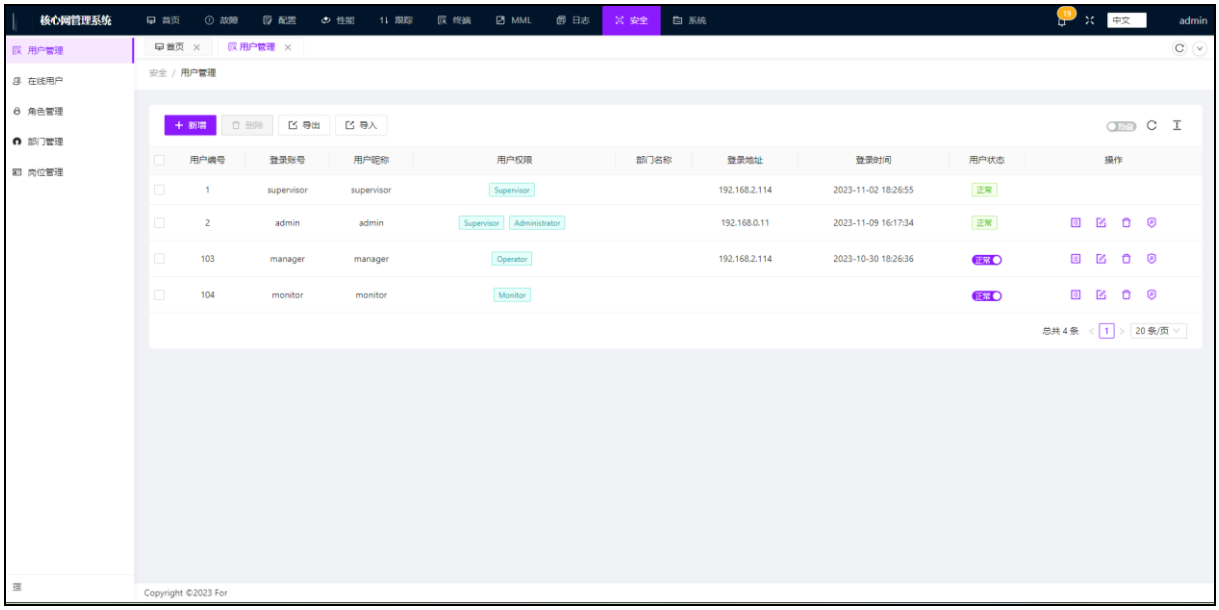
Core network security management refers to the management and permission control of users on the core network to ensure network security and protect the system

from unauthorized access or malicious attacks. Core network security management includes user management, online user management, role management, department management and position management.

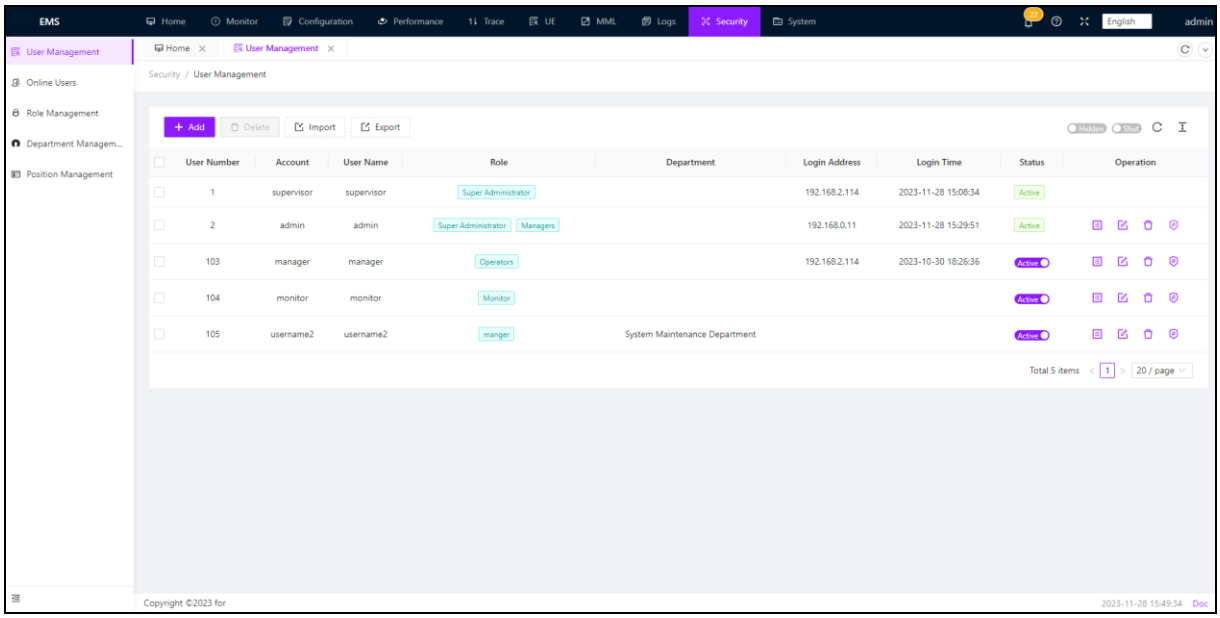
3.10.1 User Management

User management is to manage and control the login users in the core network. Administrators can add, modify, and delete login users, and set user information and permissions. By default, the core network provides default users such as supervisor, admin, manager, and monitor. Each user has different rights. For example, supervisor is the super administrator, admin has the rights of the administrator and super administrator, manager has the rights of the operation and maintenance personnel, and monitor has the rights of the monitoring personnel. User management ensures that only authorized users can access and operate the core network.

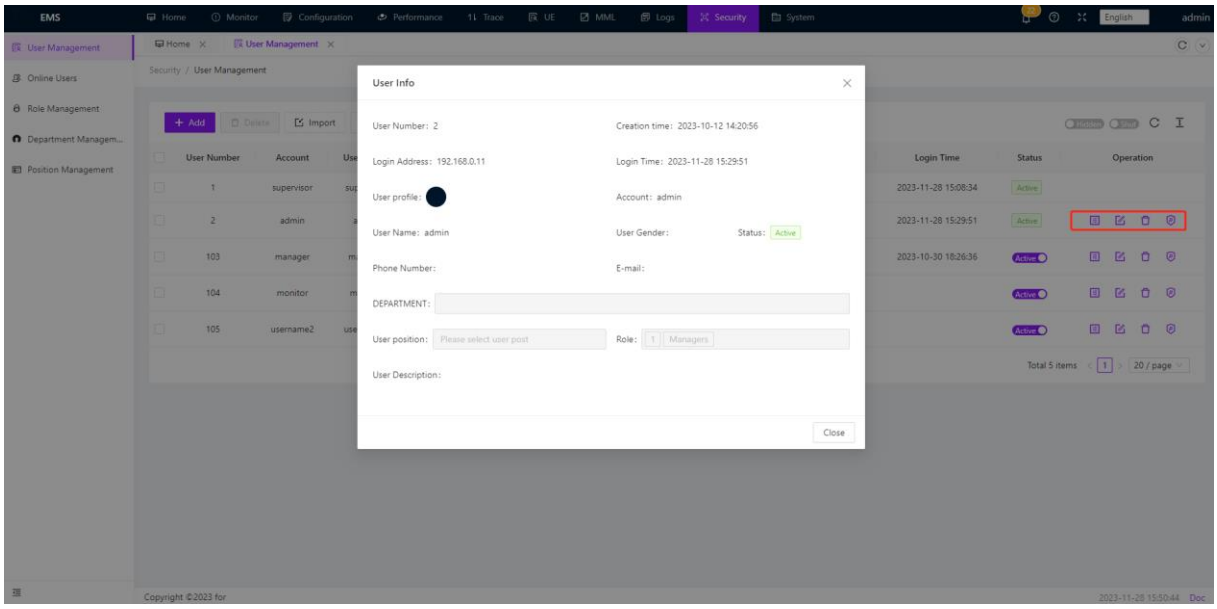
The operator can view user related information and operate to add, delete, and modify user information (“admin” and “supervisor” are super management users). Note that only high-privileged users can delete low-privileged users.

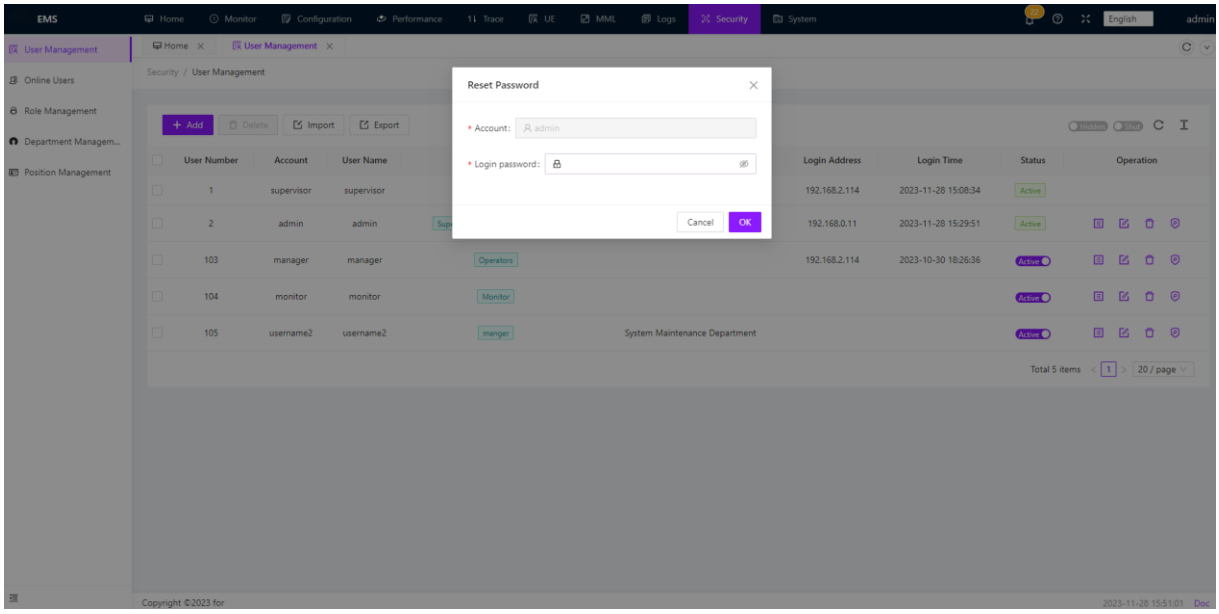


Click “Add” to add a logged-in user. Different user positions can be set according to needs, and different user permissions can be added. For specific permissions, please refer to Role Management：



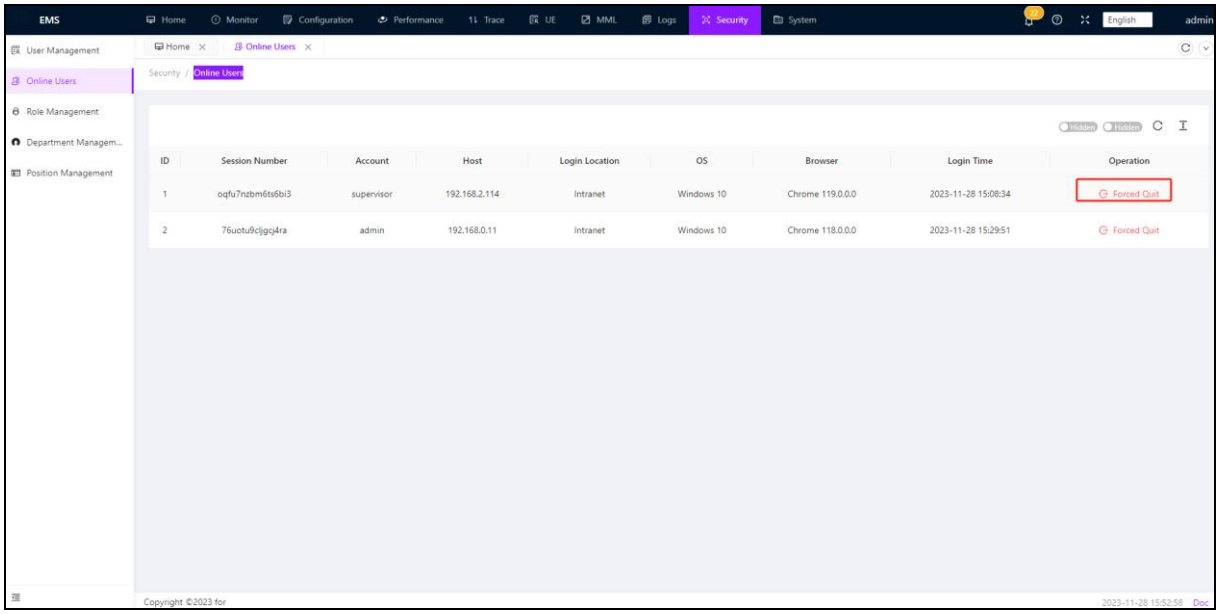
Users can be imported and exported, and import templates can be downloaded to add user data. On the right side, specific detailed information of the user can be viewed, and the user password can be modified:





3.10.2 Online Users

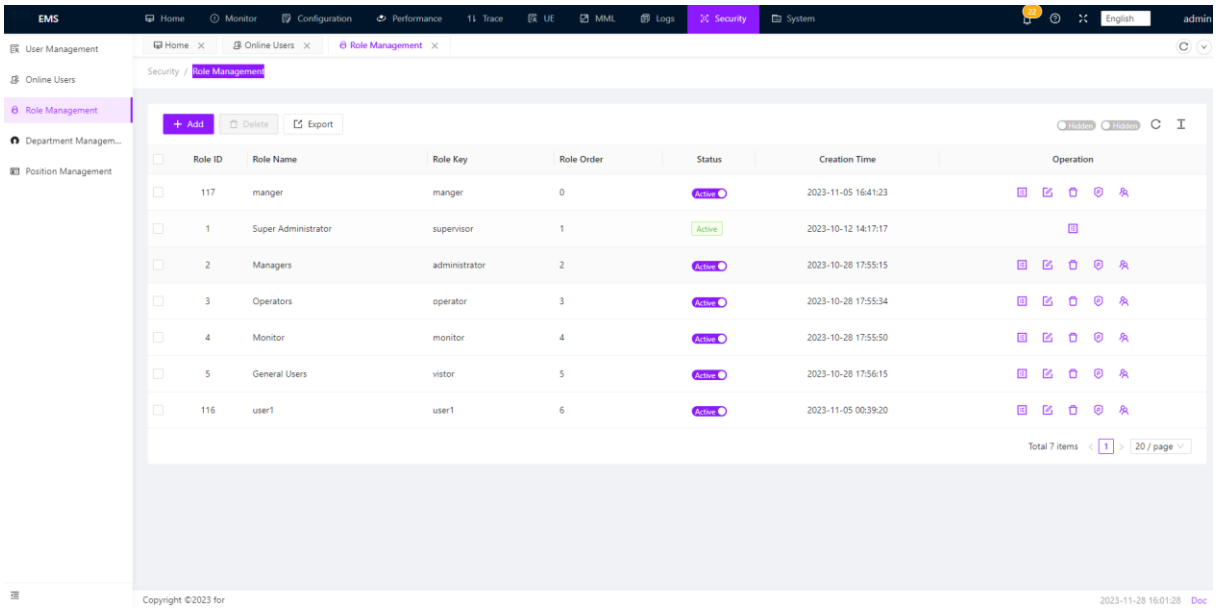
Online user management is used to monitor and manage users currently logged in to the core network. The administrator can view information about online users, such as the account name, host IP address, operating system, and login time. Online user management also provides strong logout operations. Administrators can terminate the login sessions of specified users to ensure the security of the core network.



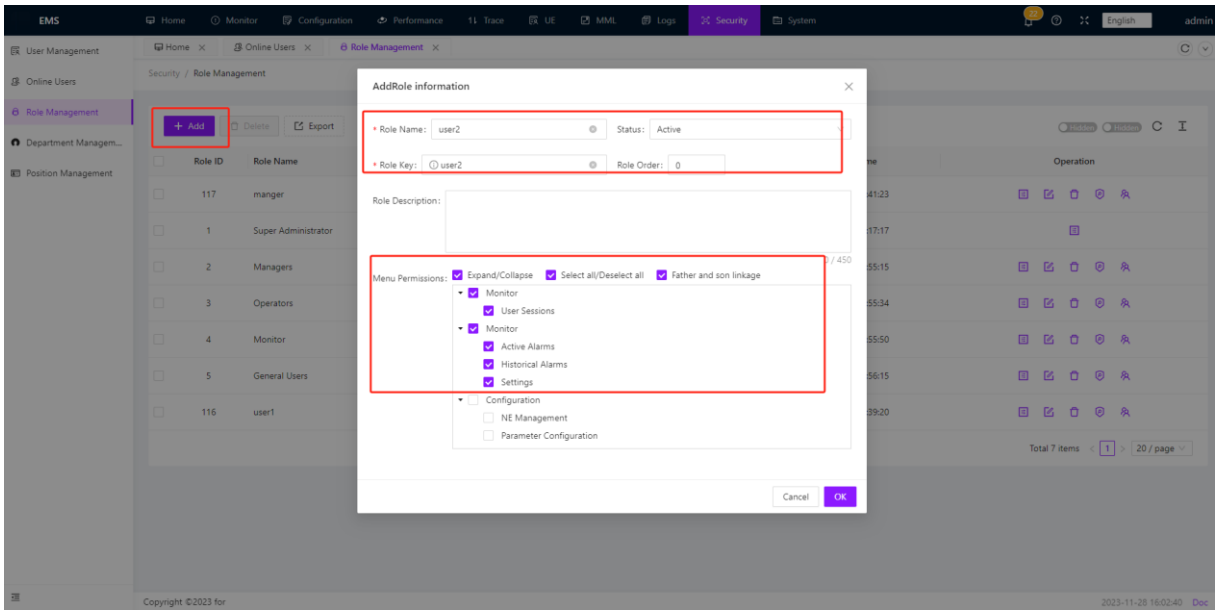
3.10.3 Role Management

Role management: Role management assigns specific roles and rights to different users. The administrator can create different role names and assign permissions to each role. Roles can be customized to meet the rights requirements of different users. Through role management, you can effectively control the access rights of users and achieve fine control of permissions.

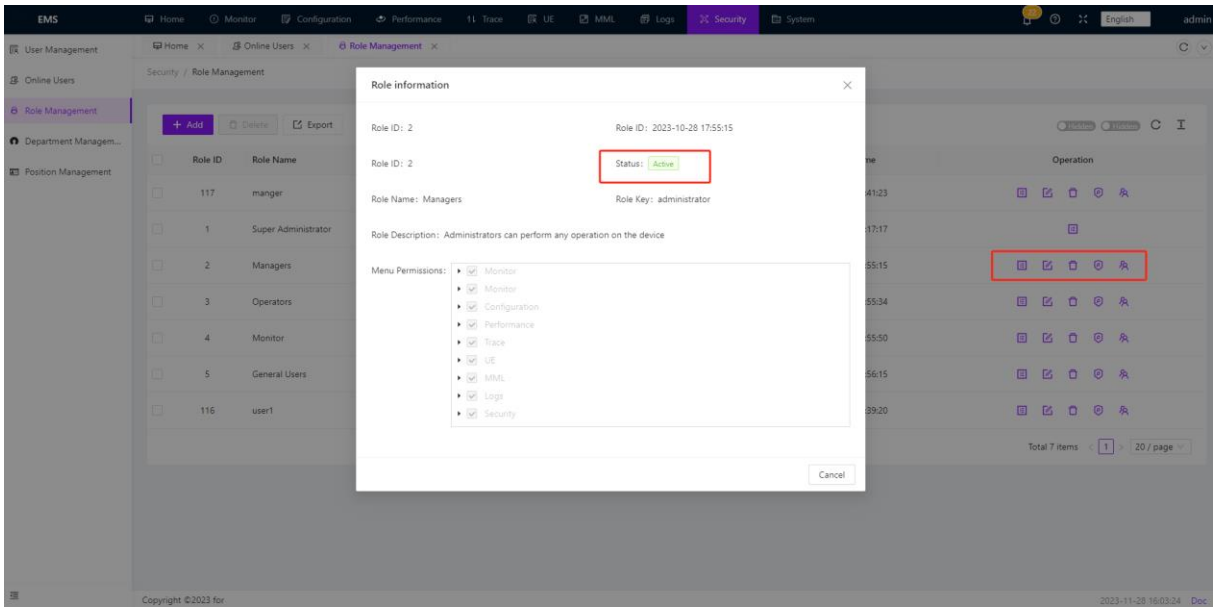
The operator can view role related information and perform operations such as adding, deleting, and modifying. The operator can also add role permission sets:



Add role information and assign different menu permissions to different roles as needed:



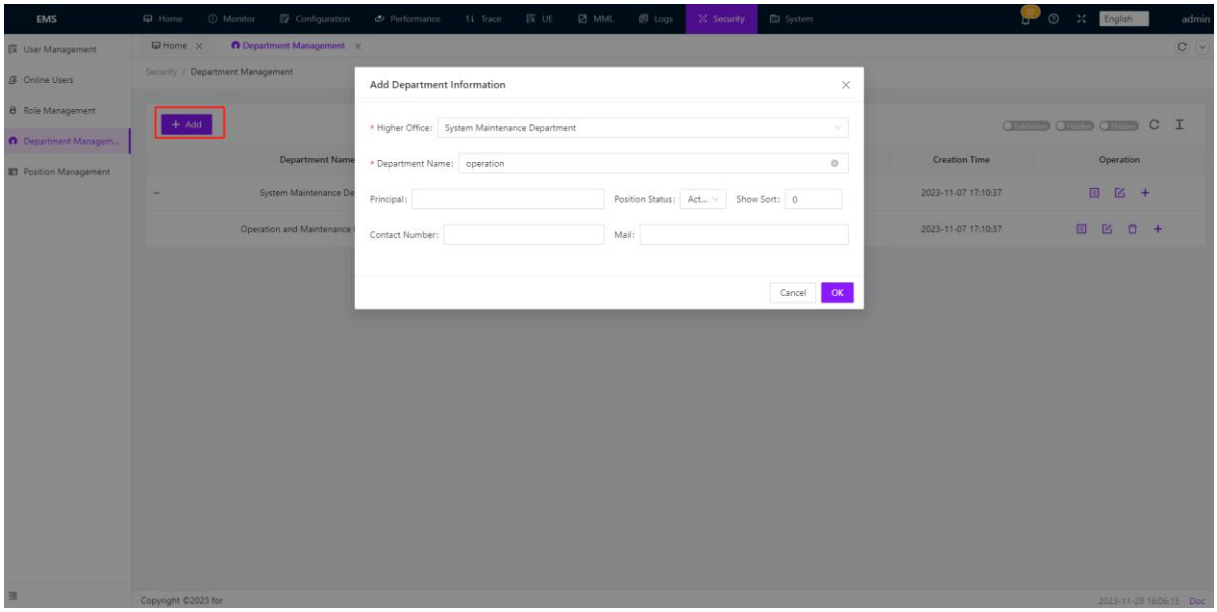
On the right side of the character name, the operator can view the specific menu permissions for each role and perform modification and deletion operations:

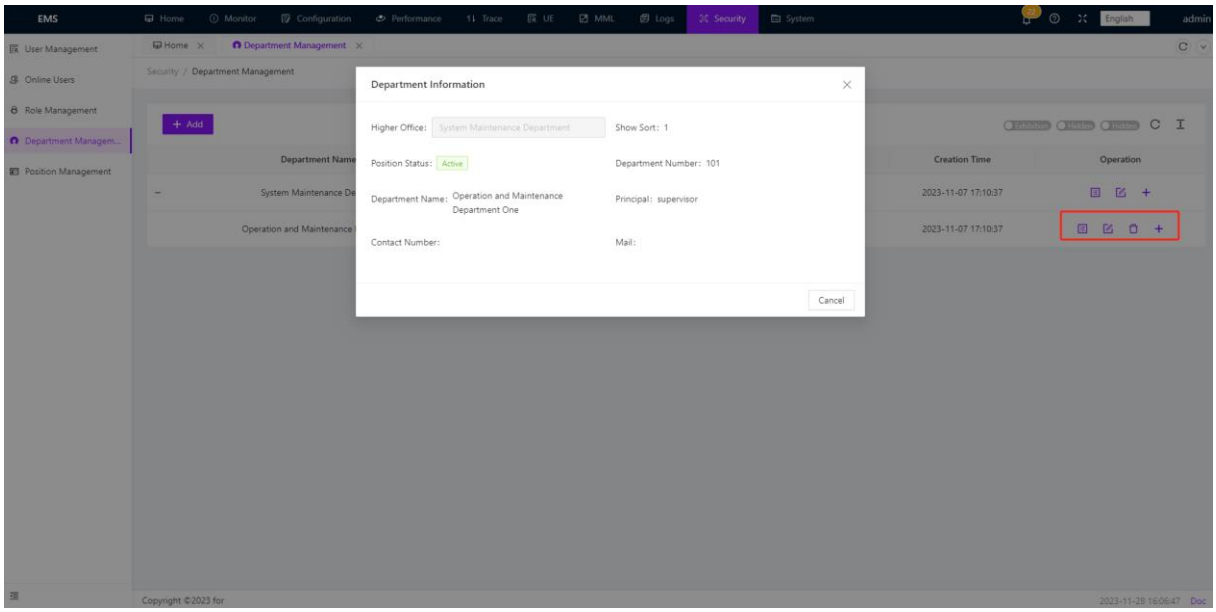


3.10.4 Department Management

Department management is used to organize and classify users in the core network. Administrators can create and manage different departments and assign users to different departments. With department management, you can easily divide and manage the rights of different departments and users, making permission control more flexible and orderly.

The operator can see the department categories, create different departments as needed, and assign different departments to different users:

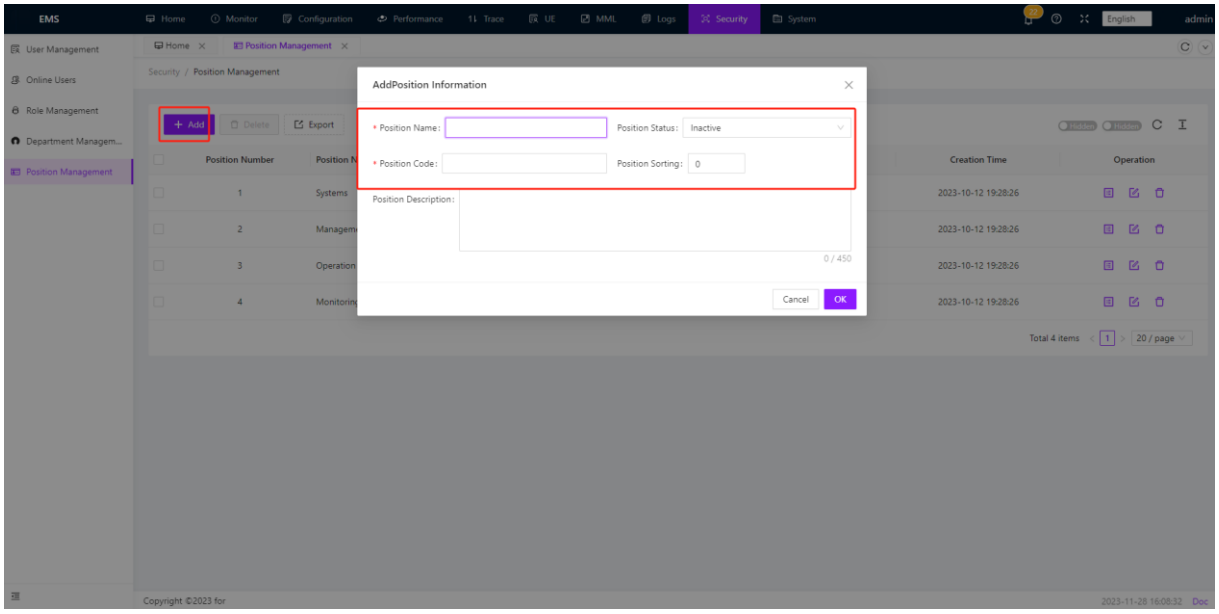




3.10.5 Position Management

Position management is to manage the duties or positions of the core network users. Administrators can create and manage different jobs and assign users to corresponding jobs. Post management can help realize the division of responsibilities and authority of users, so as to better manage the security and operation of the core network.

The operator can see different position names and search, add, delete, and modify positions:



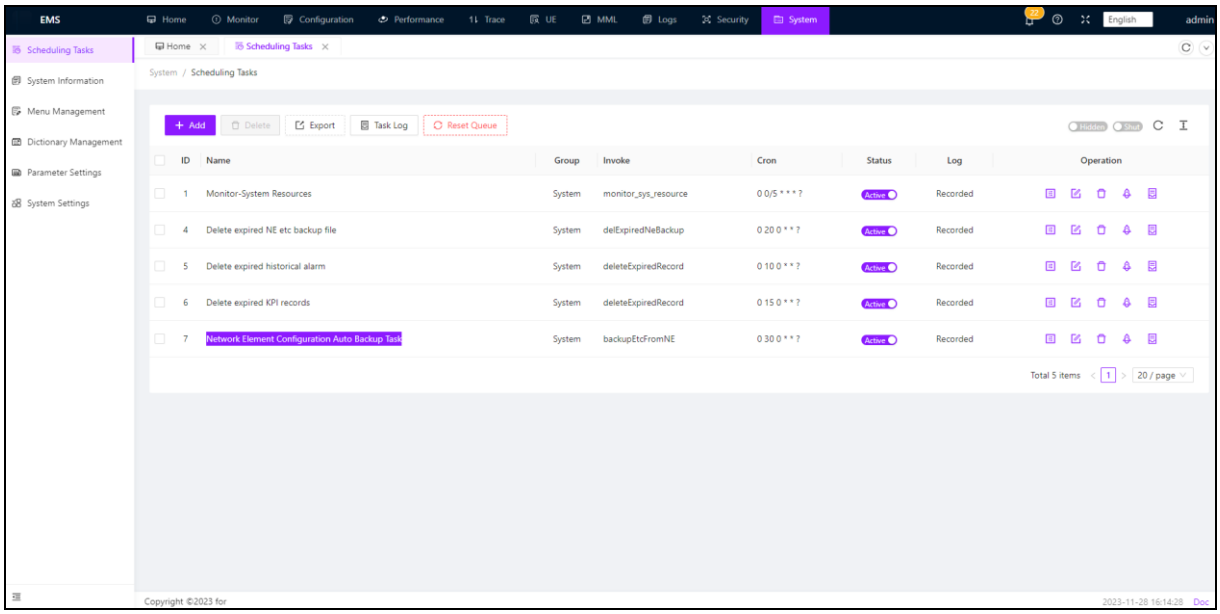
3.11 System

Core network system management refers to the management and maintenance of the functions and configurations of the core network system. It mainly includes scheduling tasks, system information, menu management, dictionary management, parameter setting, system setting, and so on.

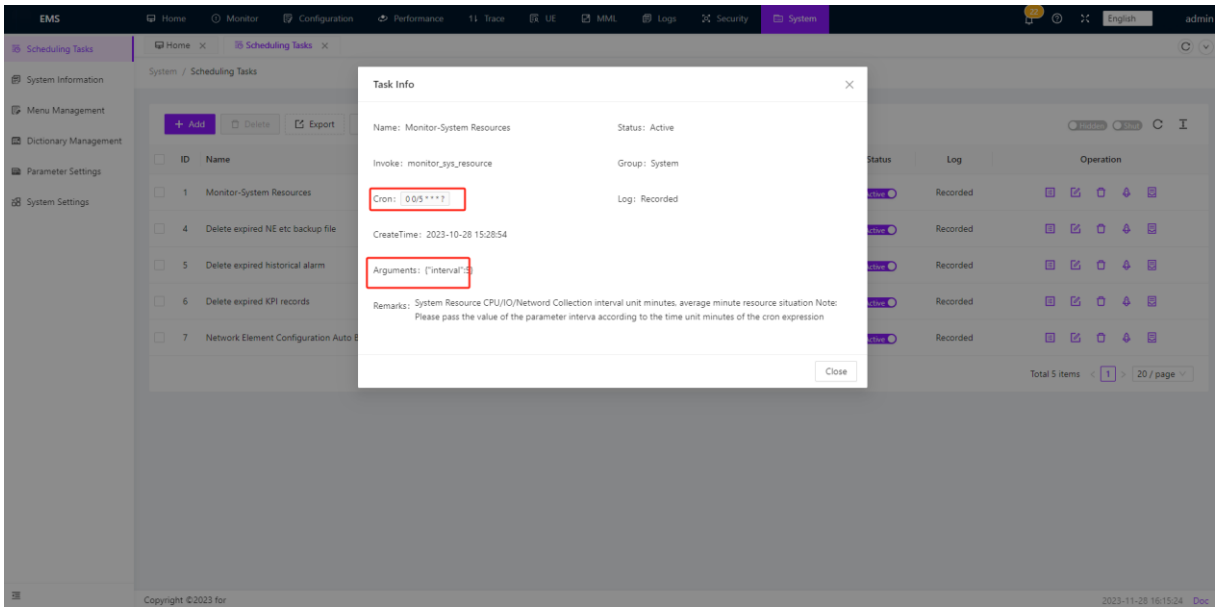
With core network system management, administrators can flexibly configure and manage core network systems to meet service requirements and improve system availability and security. Administrators can customize configurations based on actual conditions to ensure stable running and efficient maintenance of the system.

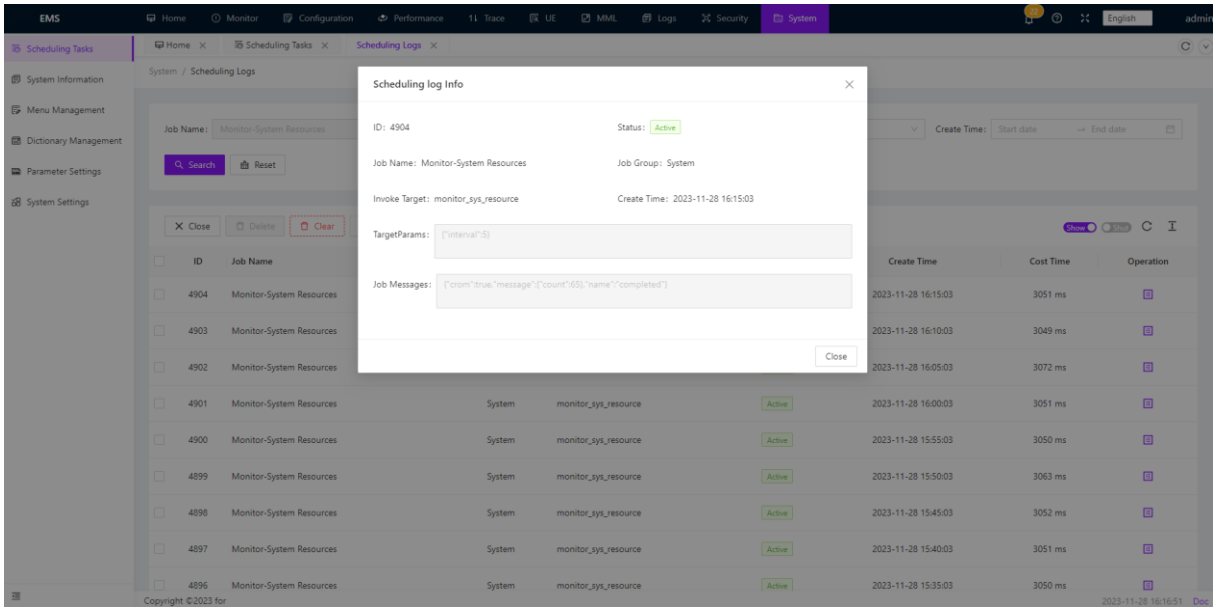
3.11.1 Scheduling Tasks

Scheduling tasks are used to schedule and manage scheduled tasks in the core network system. The initial configuration includes monitoring-system resources, deleting expired NE backup files, deleting expired historical alarm records, deleting expired KPI records, and Network Element Configuration Auto Backup Task. Administrators can set and manage the scheduling time, interval, and execution mode of these tasks to ensure the punctual execution and stability of periodic tasks.

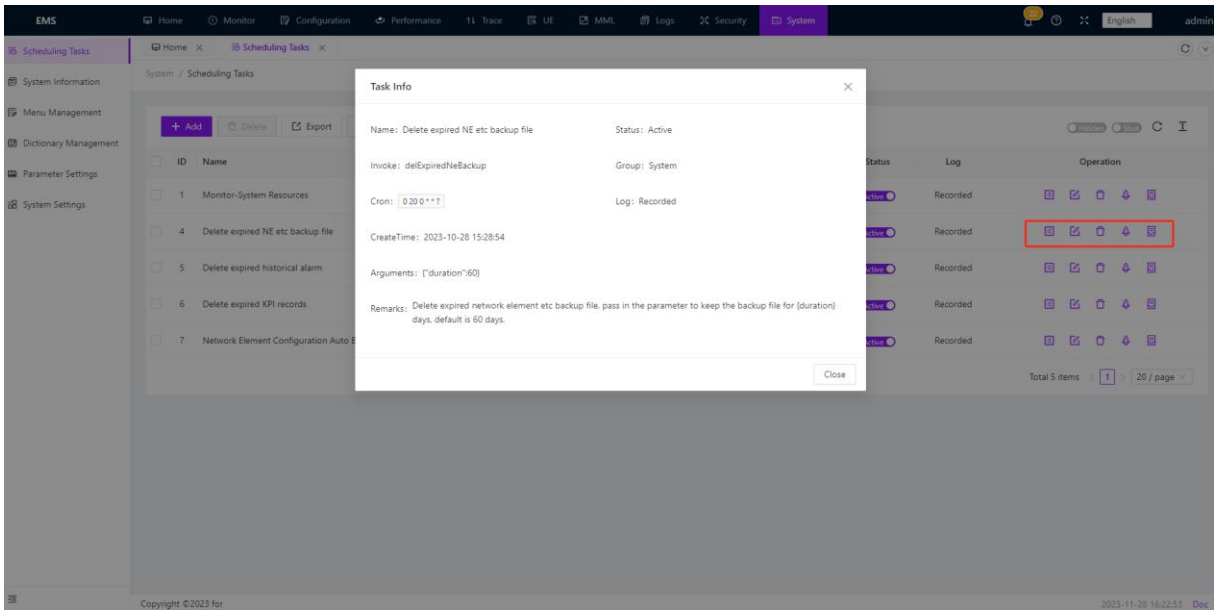


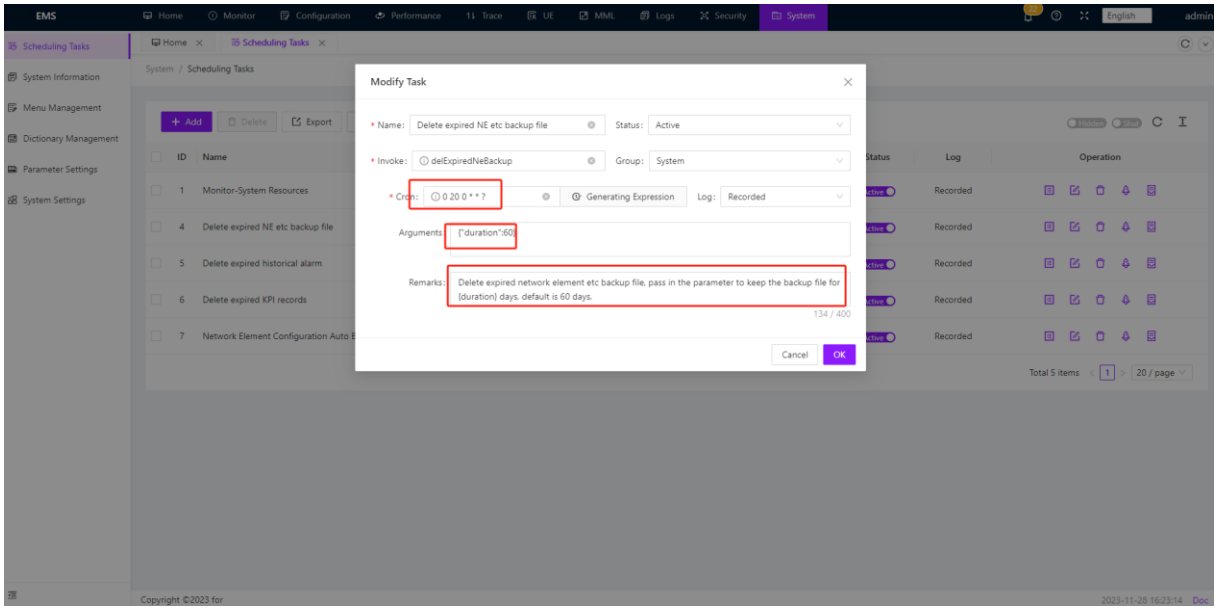
Monitoring - System Resources: This item is for collecting CPU/IO/Word resources, which can be used to view and modify the average interval 5-minute resource status of the system. After clicking on the log on the right side of the task, you can view the specific refresh time of the system resources each time, also you can modify them.

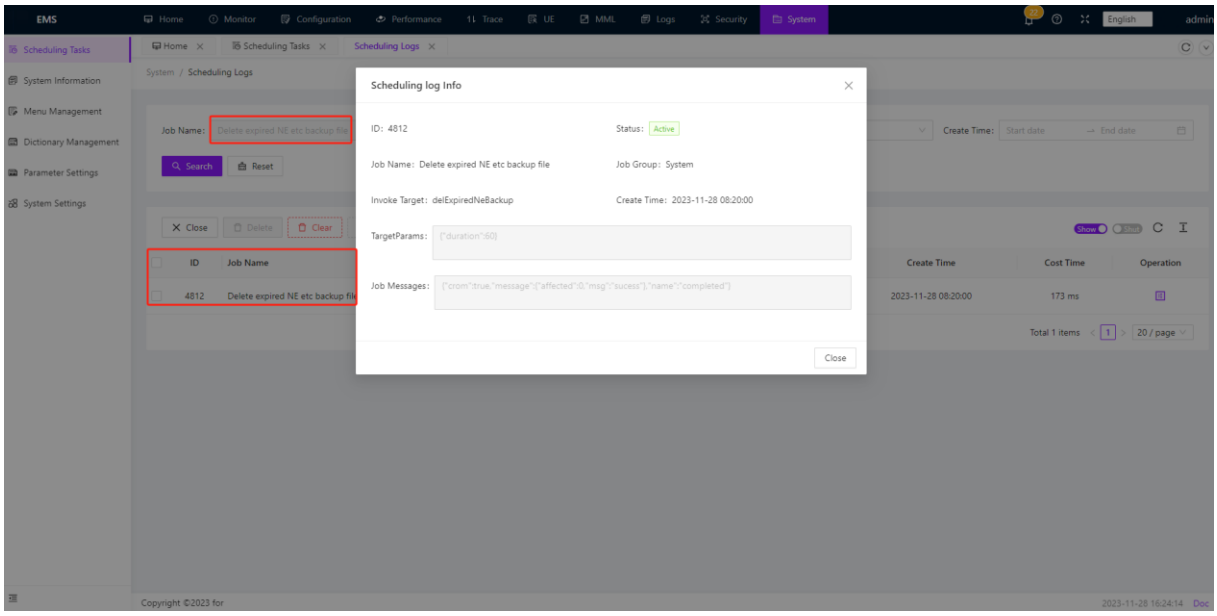




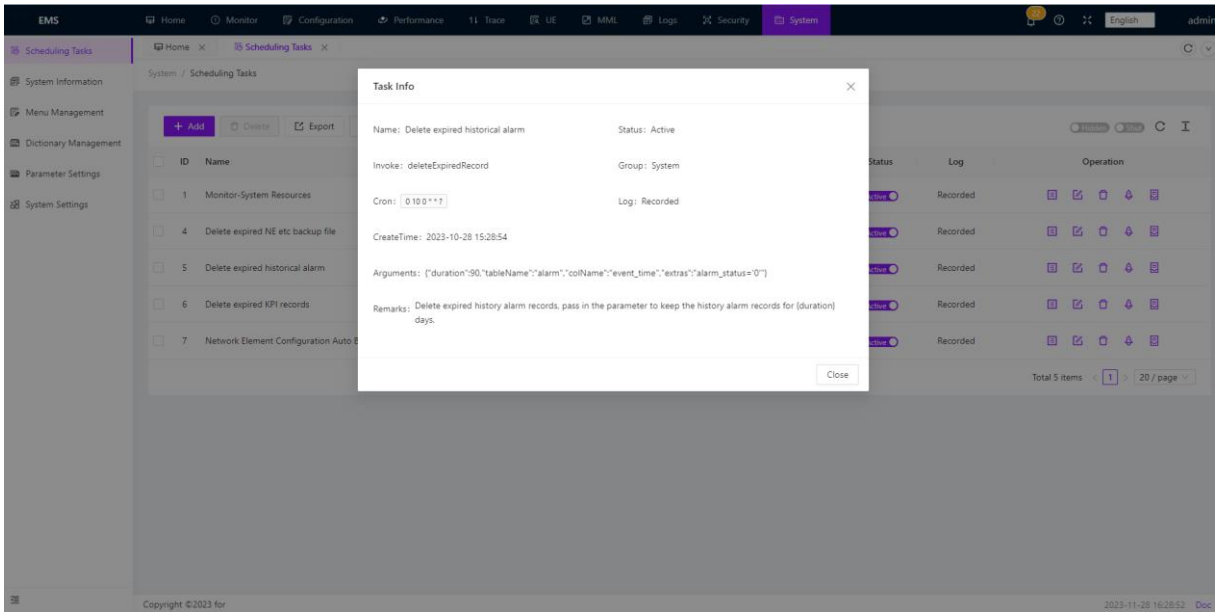
Delete expired network element backup files: This option allows you to view and modify the time of the expired network element ETC backup files. After reaching the time, record and delete them. The parameter passed in indicates that the backup files will be retained for 60 days, with a deletion time of 0:20. Click on the log on the right to view the history of deleting expired network element backup files before

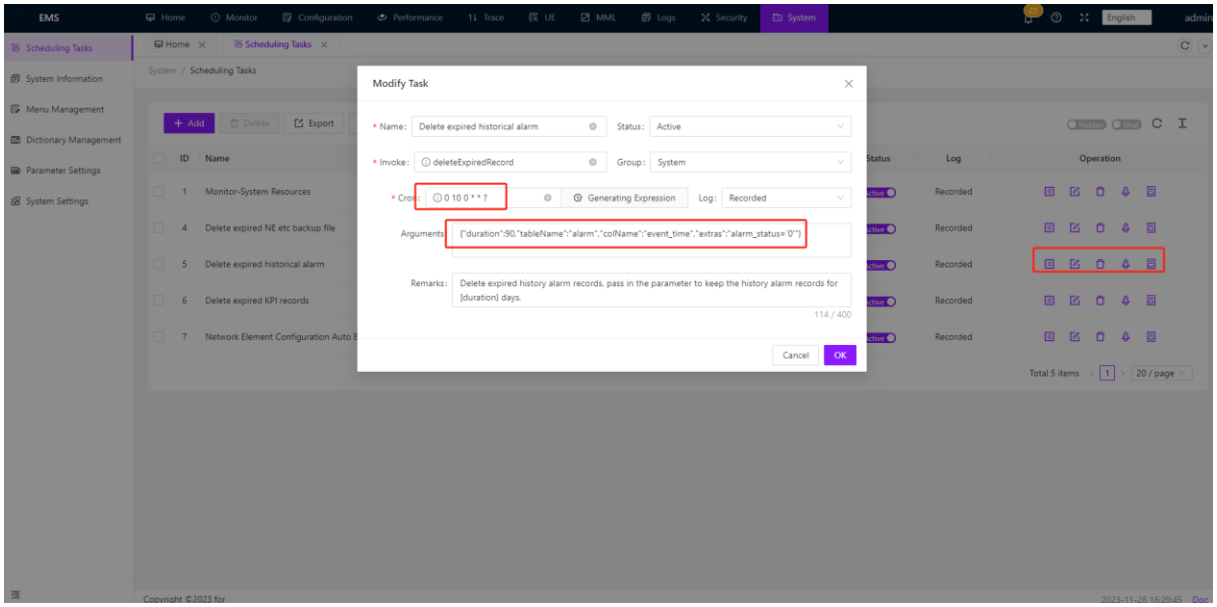




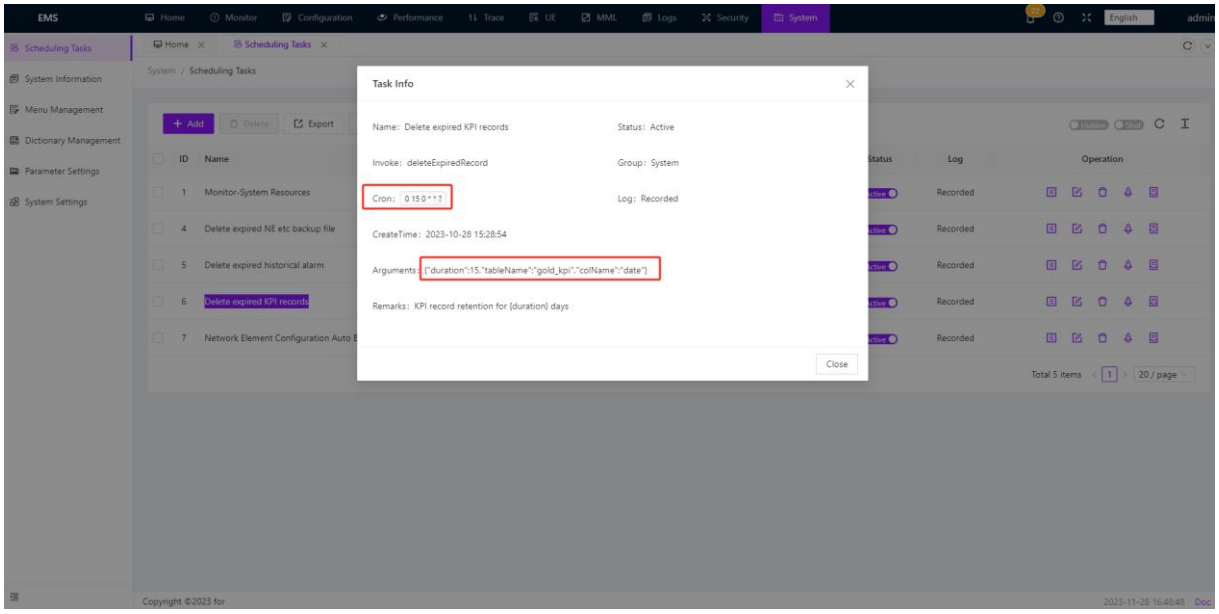


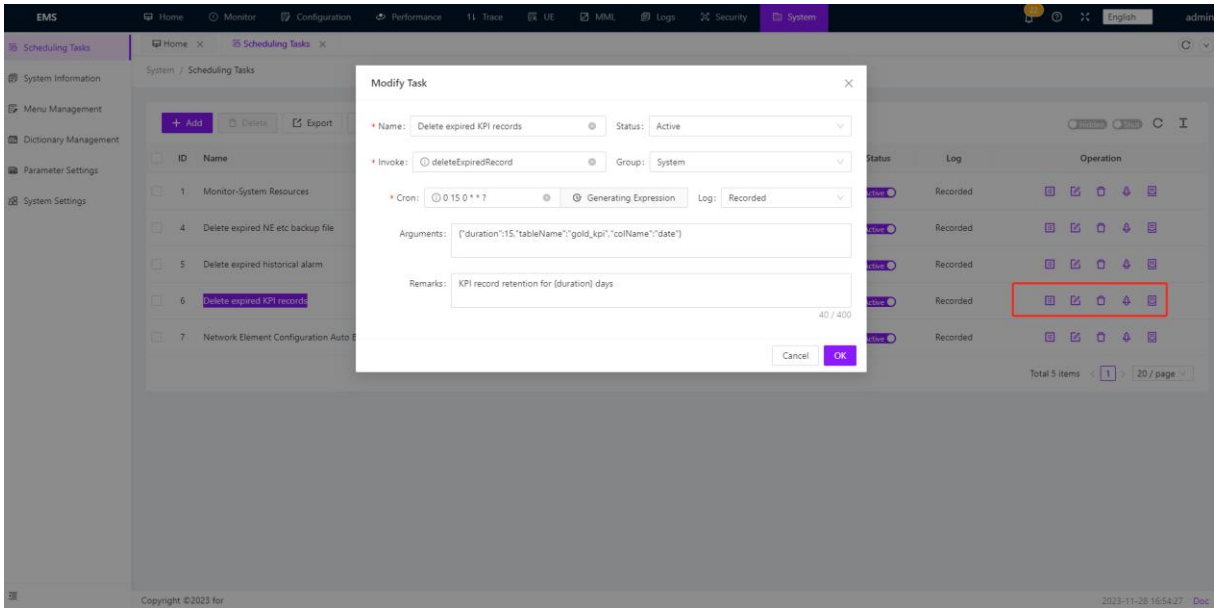
Delete expired historical alarm: This option allows you to view and modify the time of the expired historical alarm records. Once the time is reached, the records will be deleted. The parameter duration: 90 is passed in to retain the historical alarm records for 90 days, with a deletion time of 0:10. Click on the log on the right to view the history of deleting expired alarm records before.

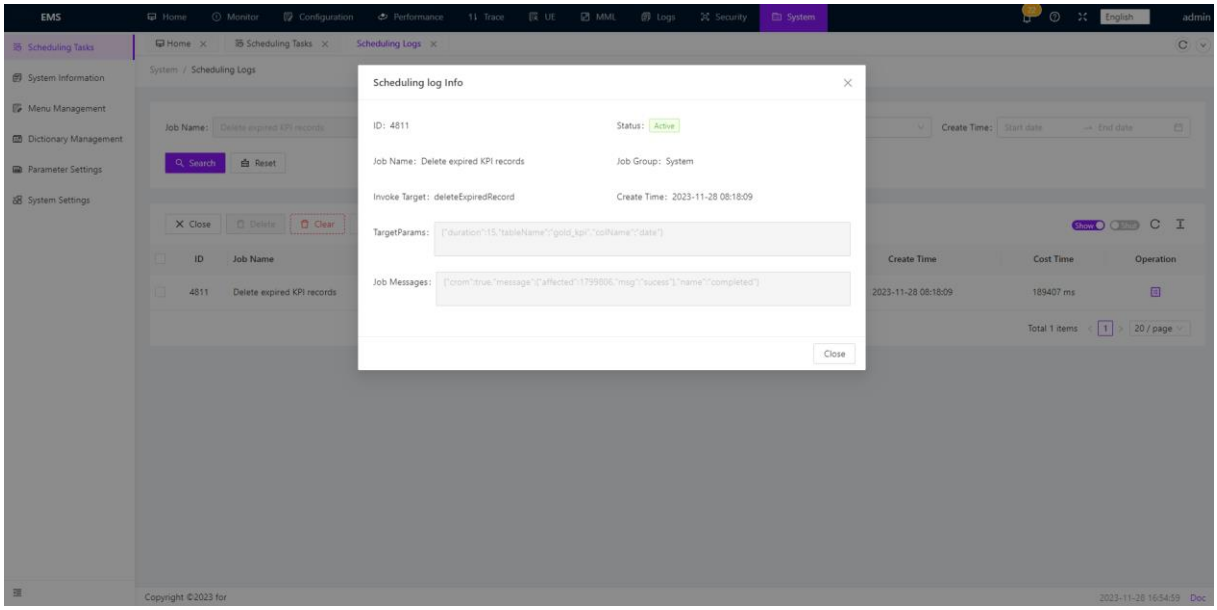




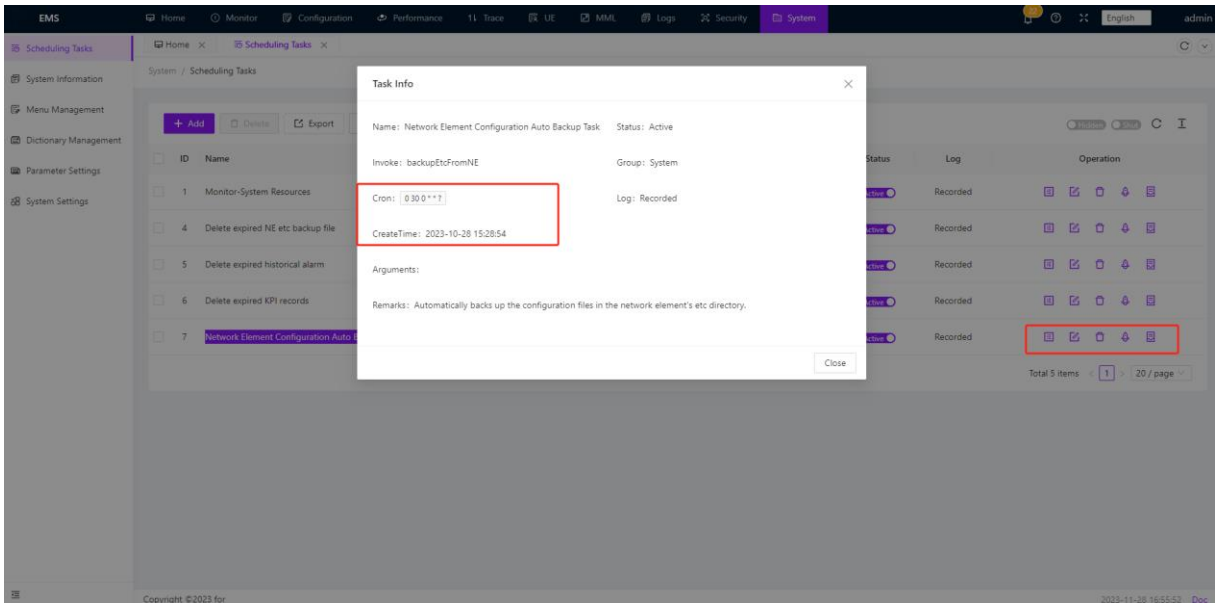
Delete expired KPI records: This option allows you to view and modify the time of the expired gold indicator record. Once the time is reached, the record will be deleted. Duration: 15 indicates that the gold indicator record will be retained for 15 days, and the deletion time is 0:15 after 39 days. Click on the log on the right to view the history of deleting gold indicator records before.

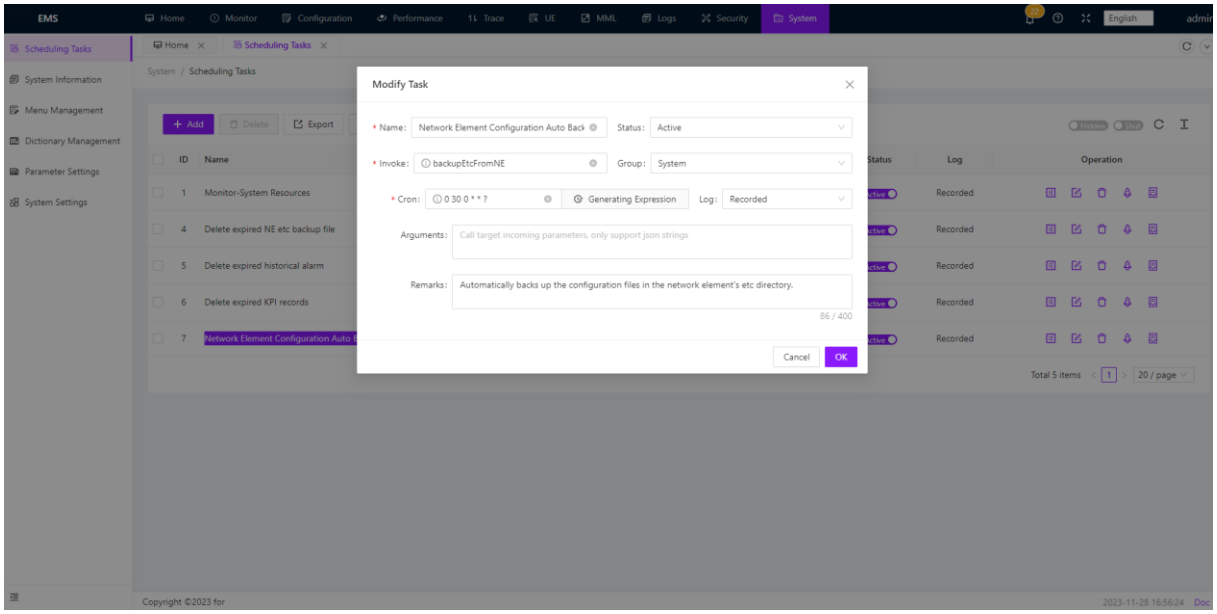

EMS
Home
Monitor
Configuration
Performance
Trace
UE
MML
Logs
Security
System
Scheduling Tasks
System Information
Menu Management
Dictionary Management
Parameter Settings
System Settings
System / Scheduling Tasks
Add
Delete
Export
ID
Name
Status
Log
Operation
1 Monitor-System Resources
4 Delete expired NE etc backup file
5 Delete expired historical alarm
6 Delete expired KPI records
7 Network Element Configuration Auto B
Recorded
Total 5 items
20 / page
Task Info
Name: Delete expired KPI records
Status: Active
Invoke: deleteExpiredRecord
Group: System
Cron: 0 15 0 * * ?
Log: Recorded
CreateTime: 2023-10-28 15:28:54
Arguments: {"duration":15,"tableName":"gold_kpi","colName":"date"}
Remarks: KPI record retention for {duration} days
Close
Copyright ©2023 for

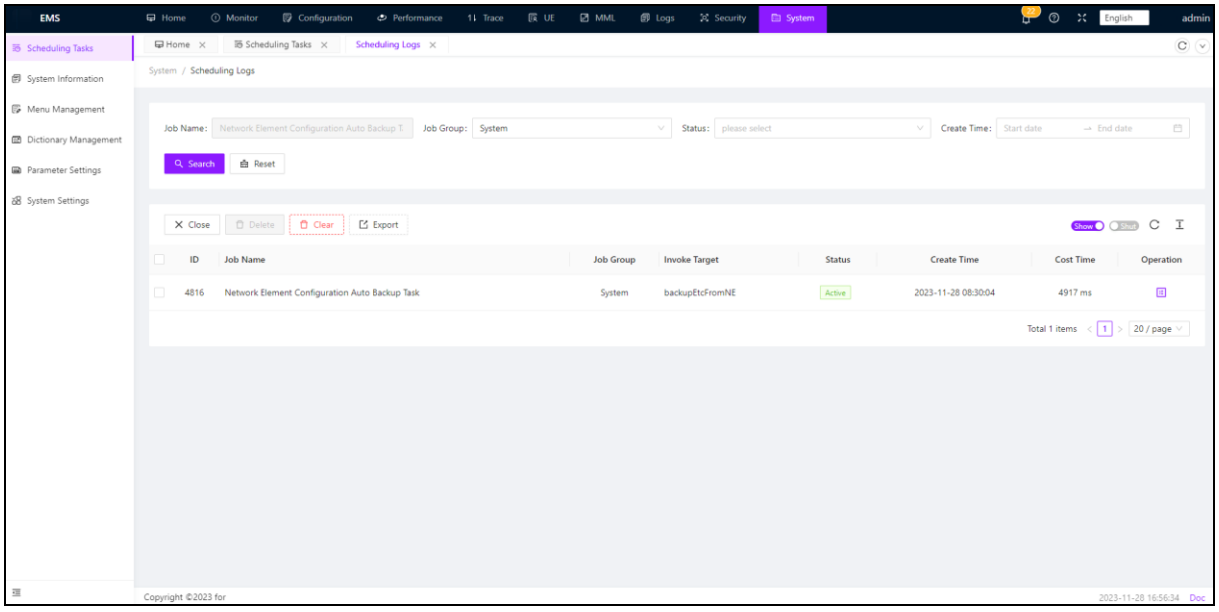

EMS
Home
Monitor
Configuration
Performance
Trace
UE
MML
Logs
Security
System
Scheduling Tasks
System Information
Menu Management
Dictionary Management
Parameter Settings
System Settings
System / Scheduling Tasks
Add
Delete
Export
ID
Name
Status
Log
Operation
1 Monitor-System Resources
4 Delete expired NE etc backup file
5 Delete expired historical alarm
6 Delete expired KPI records
7 Network Element Configuration Auto B
Recorded
Total 5 items
20 / page
Modify Task
* Name: Delete expired KPI records
Status: Active
* Invoke: deleteExpiredRecord
Group: System
* Cron: 0 15 0 * * ?
Generating Expression
Log: Recorded
Arguments: {"duration":15,"tableName":"gold_kpi","colName":"date"}
Remarks: KPI record retention for {duration} days
40 / 400
Cancel
OK
Copyright ©2023 for



Network element configuration automatic backup task: The automatic backup time of the network element can be viewed and modified. In the Cron expression in the figure, "0 30 0 * *?" indicates that the backup is performed at 0:30 every day. Backup history can be viewed in the scheduling log.

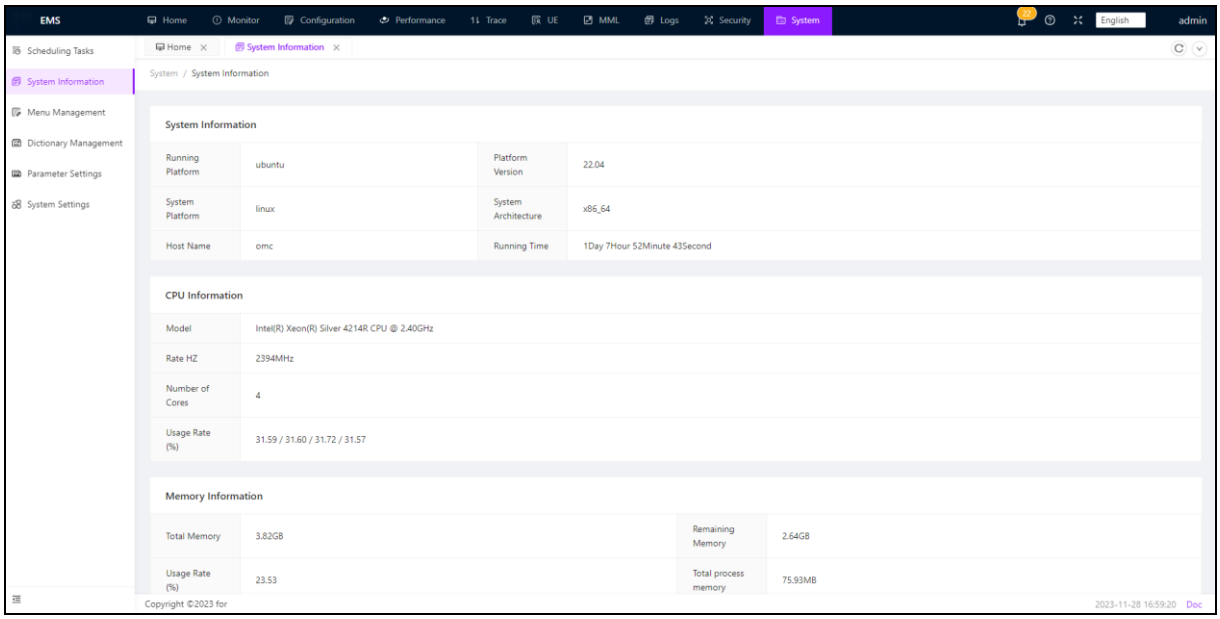


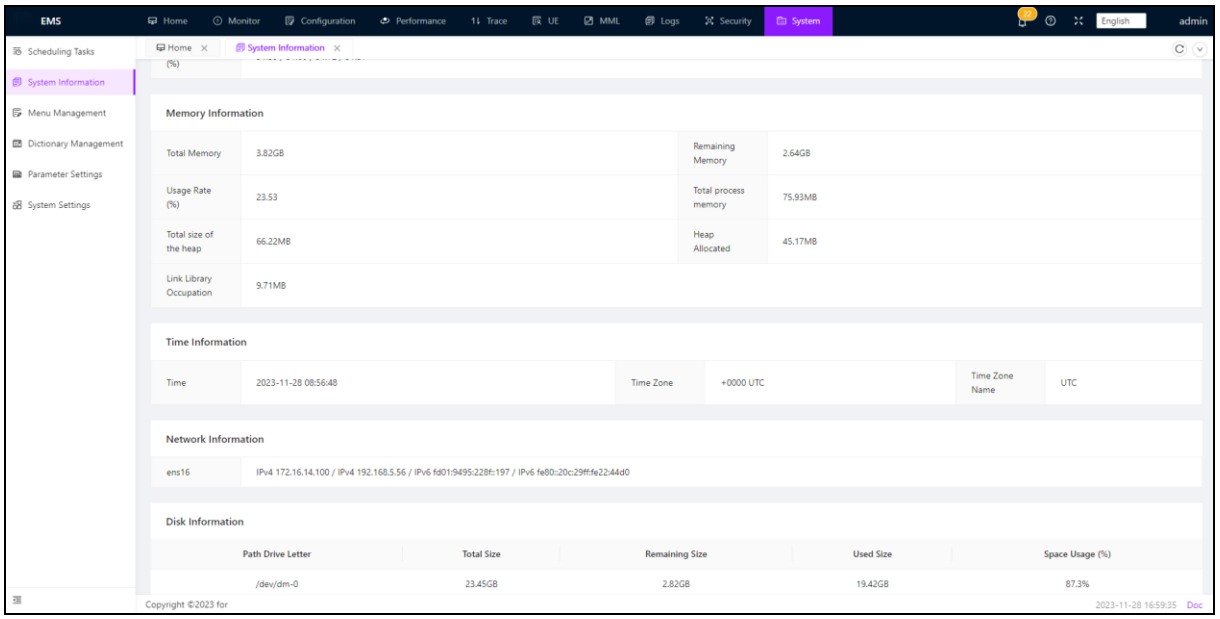




3.11.2 System Information

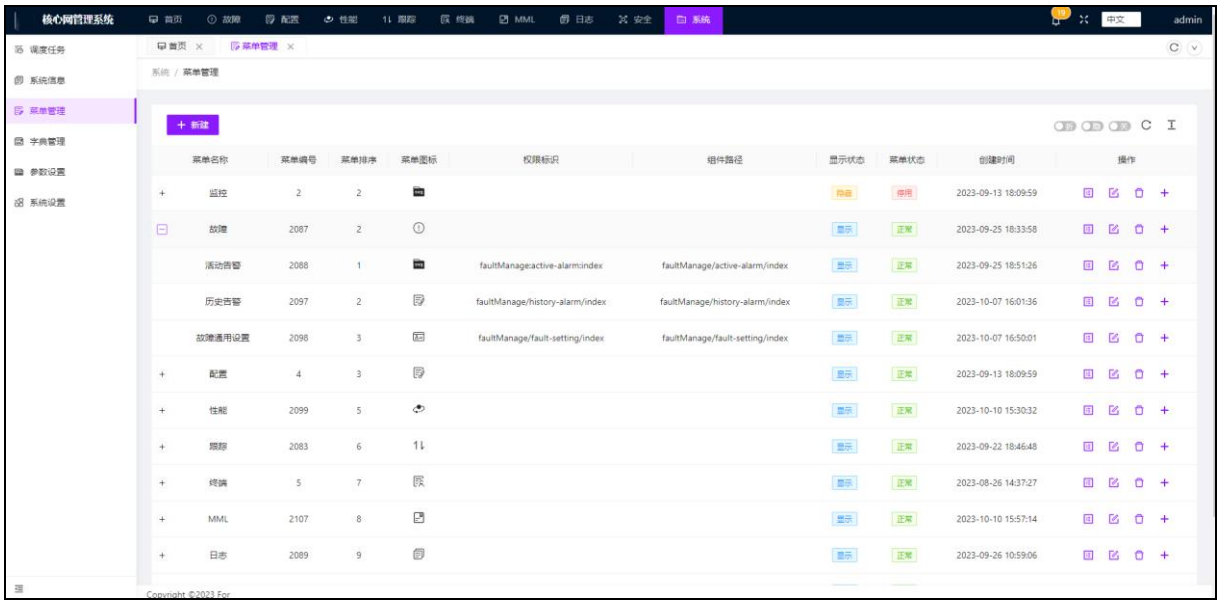
System information provides the basic information and status monitoring of the core network system. Including system information, CPU information, memory information, time information, network information, disk information and so on. The information helps administrators learn about the running status and resource utilization of the core network system in real time, and then analyze system performance and troubleshoot faults.





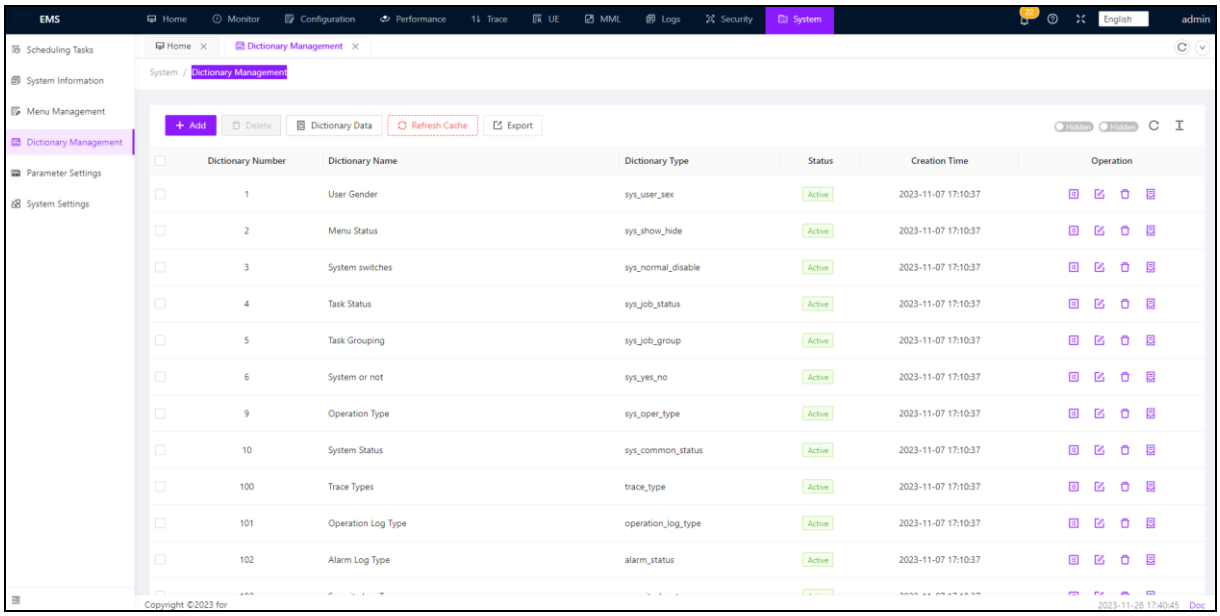
3.11.3 Menu Management

Menu management is used to manage and configure the menus of the management system. The administrator can add, delete, or modify menus as required, so that users can access required function modules based on permissions. Through the menu management, you can flexibly configure and adjust the menu navigation of the management system to improve the user's convenience and work efficiency.



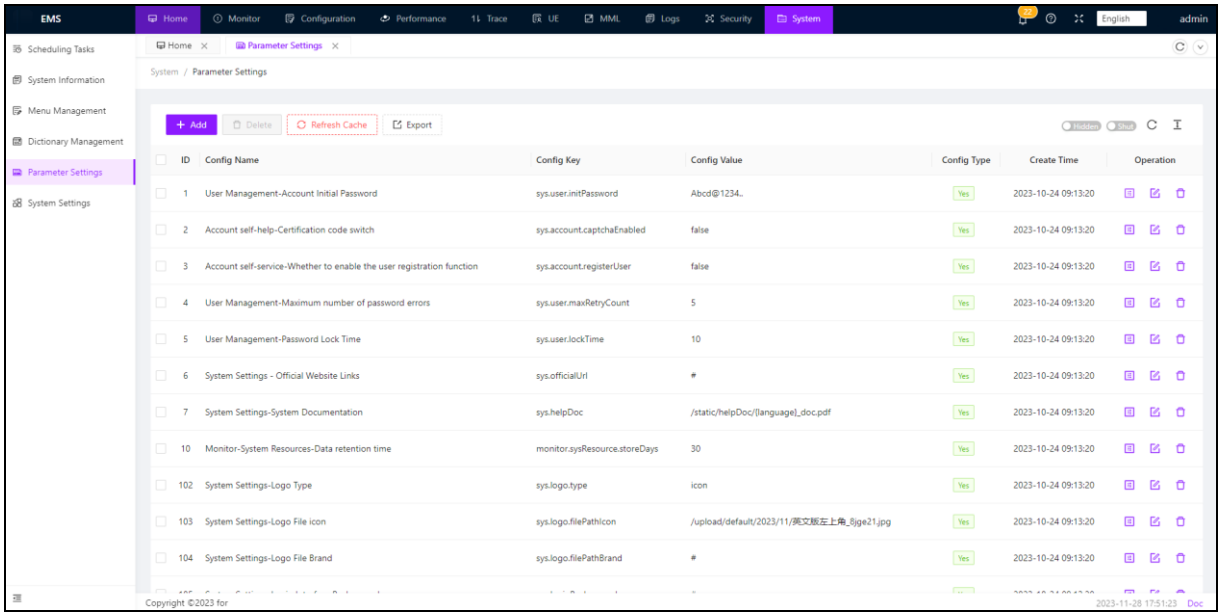
3.11.4 Dictionary Management

Dictionary management is used to manage dictionary data in the core network system. Administrators can add, modify, and delete dictionary data to ensure the accuracy and consistency of data in the core network system. Dictionary management can also help to realize the classification and standardization of data to improve the efficiency of data management system.



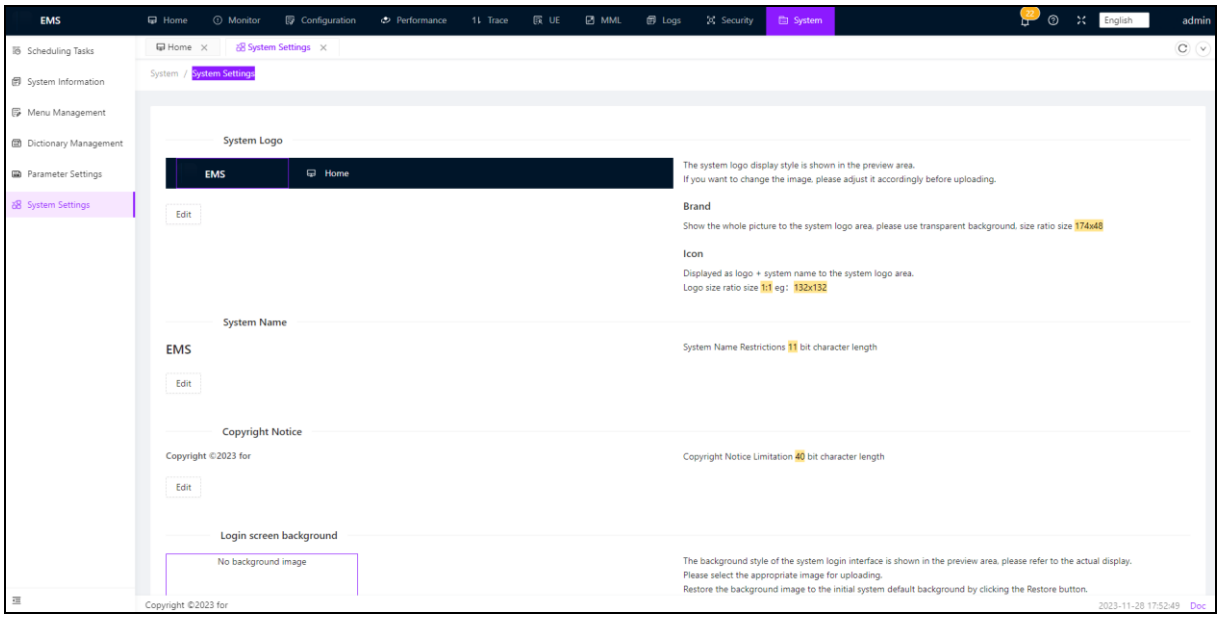
3.11.5 Parameter Settings

Parameter Settings allow the administrator to configure and adjust parameters of the core network system. These parameters can affect the functional performance and performance of the system. Administrators can adjust the parameters based on actual requirements to optimize system running and meet service requirements.

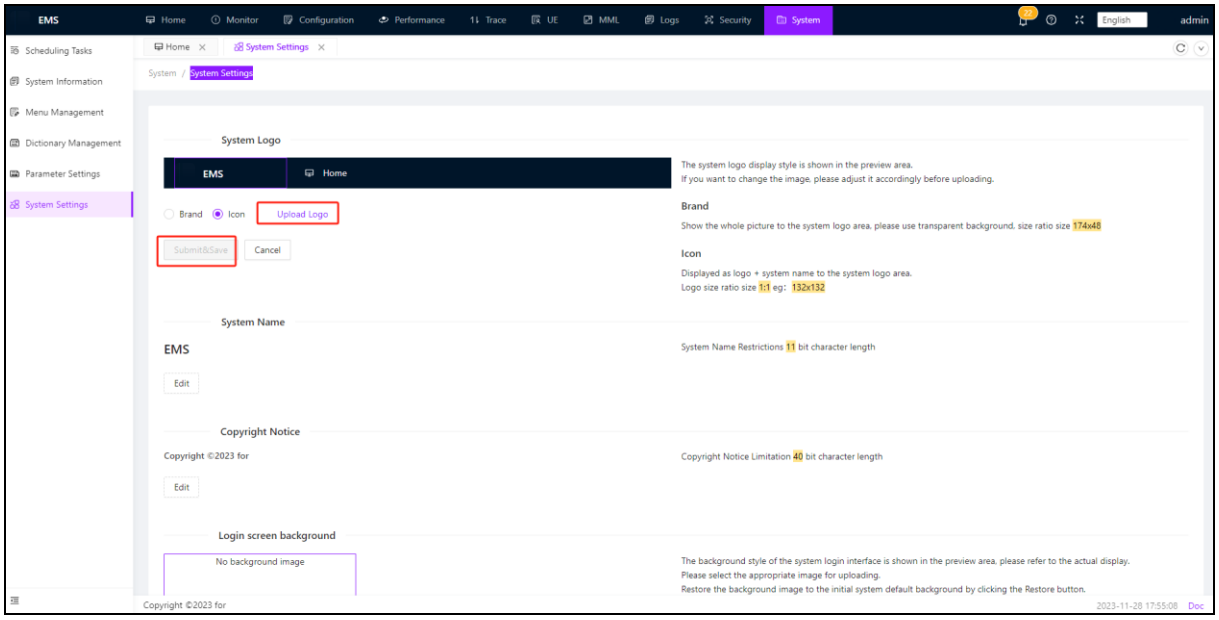


3.11.6 System Settings

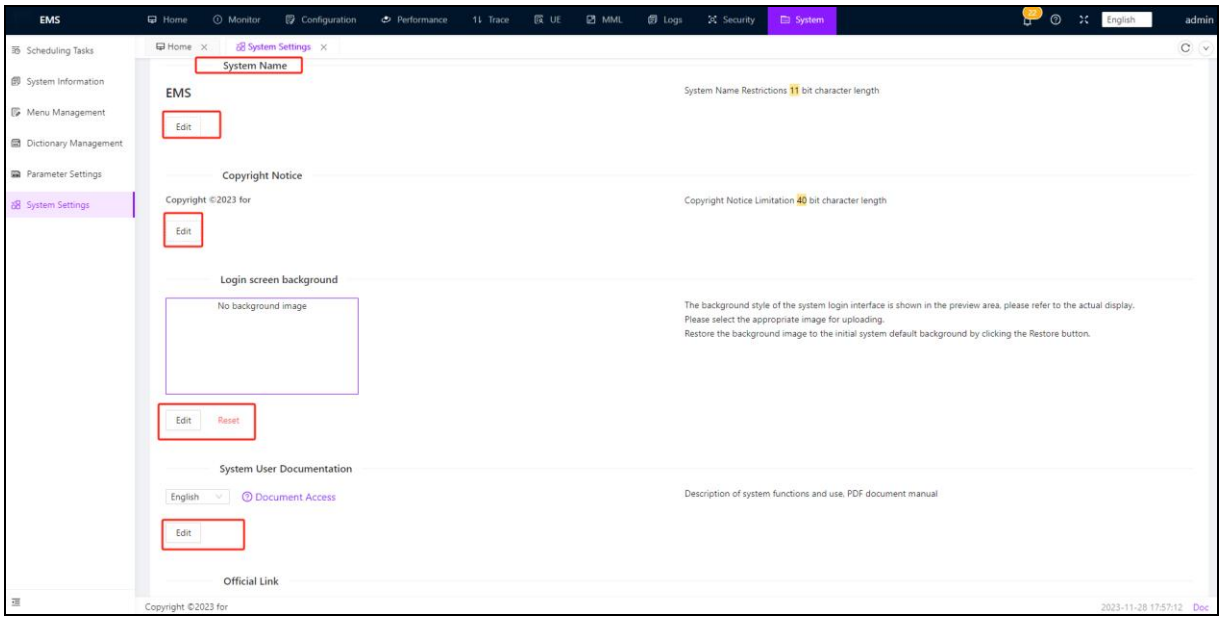
System Settings allow the administrator to modify and configure some basic Settings of the core network system. For example, you can modify the system LOGO and system name, set the copyright notice, configure the style and content of the login interface, and provide system usage documents and official website links. These Settings can be personalized to customize the management system, so that it meets the brand image of the enterprise and the needs of users.

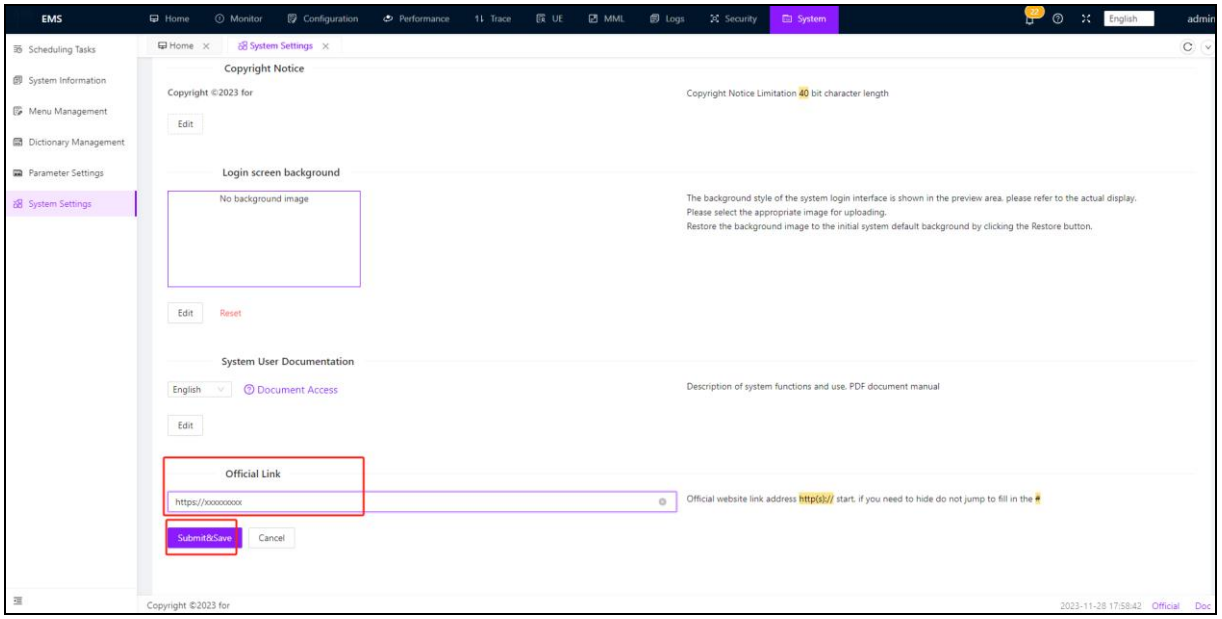


The operator can change the system logo by clicking "Edit"->"Upload Logo", selecting the logo image, and then clicking "Submit&Save" to change the logo



Below, The operator can modify the system name, modify the copyright statement, modify the background of the login interface, click edit and modify, and then click submit and save:





4 How to get help

You can contact our technical support and after-sales by phone or email.

5 The practices and principles of after-sales service for this software system

After the software is handed over to the user, our company will provide support and track after-sales service in accordance with the contract agreement. If there is no agreement, we will provide after-sales service in accordance with the relevant national

product regulations.

6 Frequently Asked Questions and Answers

SN	Problem	Solution
1	Partial browser operation and display abnormalities	Suggest using Google Chrome browser or Microsoft Edge (chrome kernel) version; Clear browser cache.
2	The network element cannot be added successfully	Check if the OAM configuration switch on the network element side is turned on
3	Core network function configuration operation	Refer to 5GC maintenance manual

7 Copyright Statement