Core Network OMC Operation Manual

Version： 3.0

Date: 2023-12-18

Contents

1 About this manual

This document describes the hardware and software environment of the 5G core network management system, system functions, operation guides, and frequently asked questions (FAQs). It provides basic network management functions, such as configuration management, performance management, monitor management, security management, log management, trace management, UE management, MML management, and system management. It also provides a variety of optional functions.

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 spcifications 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

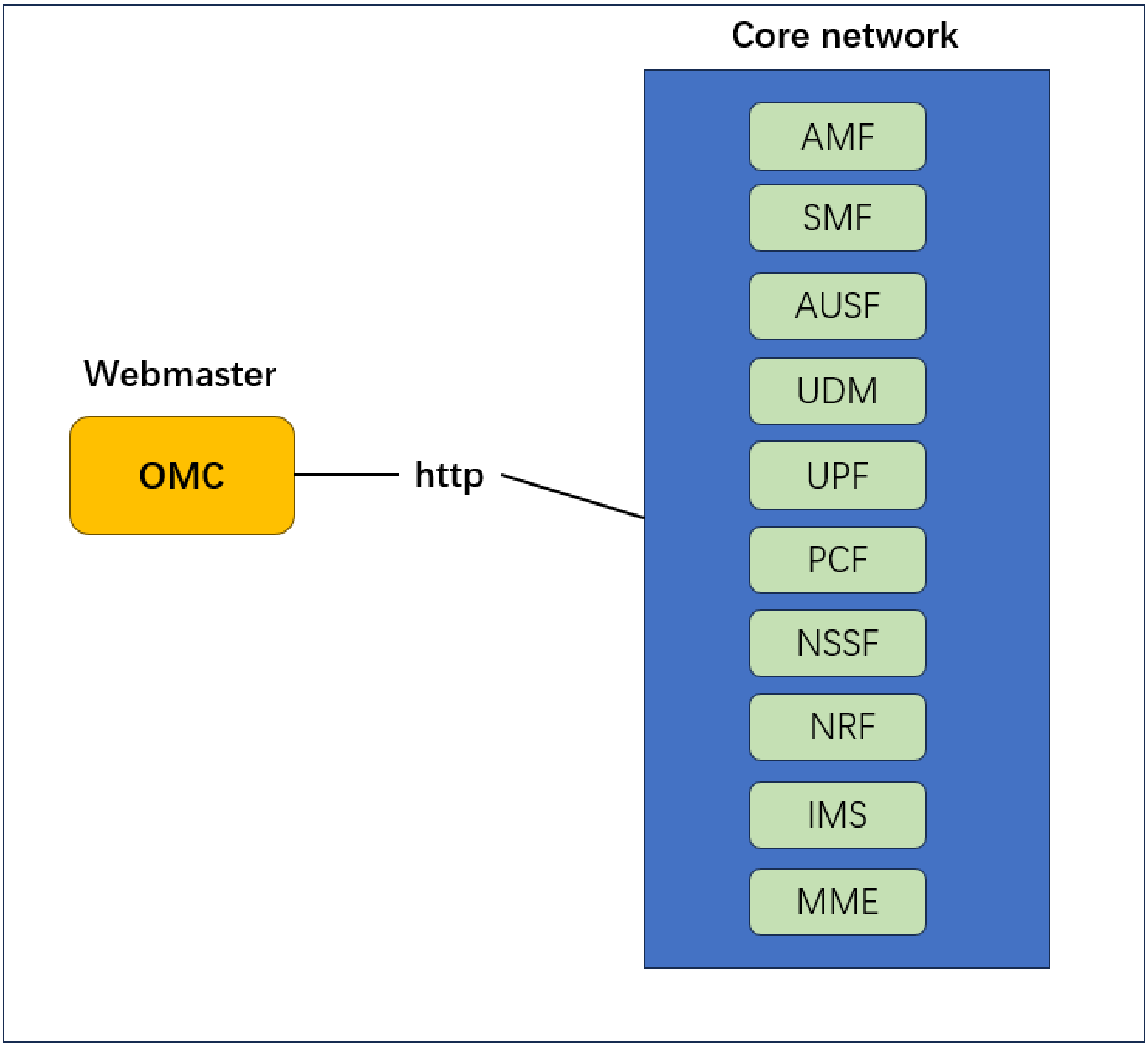
The software is shipped with the hardware and has been installed and tested before the delivery, so it will not be detailed here.

1.4 Software Uninstallation

The software and hardware of the system are integrated, so it is impossible to uninstall the software separately.

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, monitoring status, network element configuration, abnormal alarms, signaling tracking, 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.

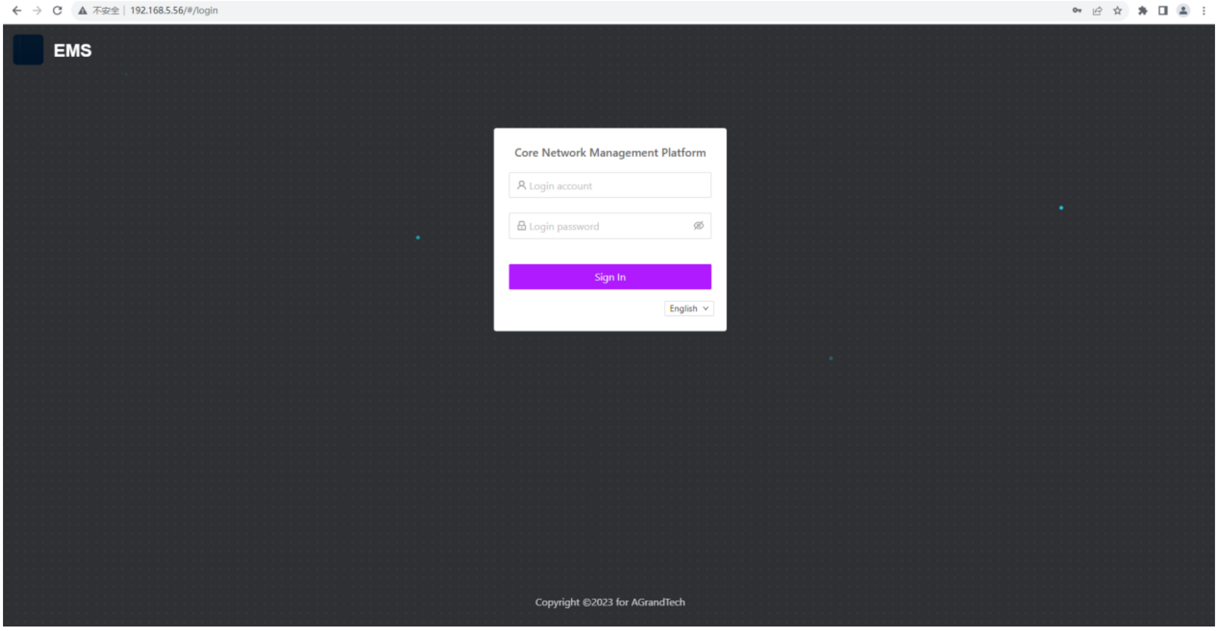
11. MME functions

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

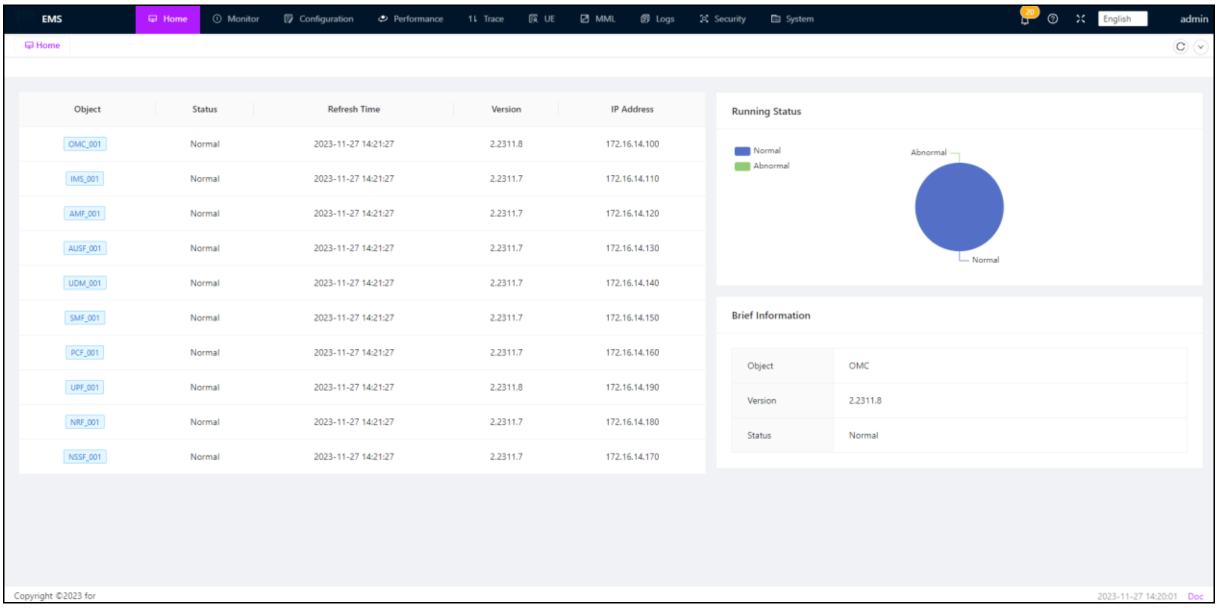

不安全 | 192.168.5.56/#/login
EMS
Core Network Management Platform
Login account
Login password
Sign In
English
Copyright ©2023 for AGrandTech

- 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, and IP address:



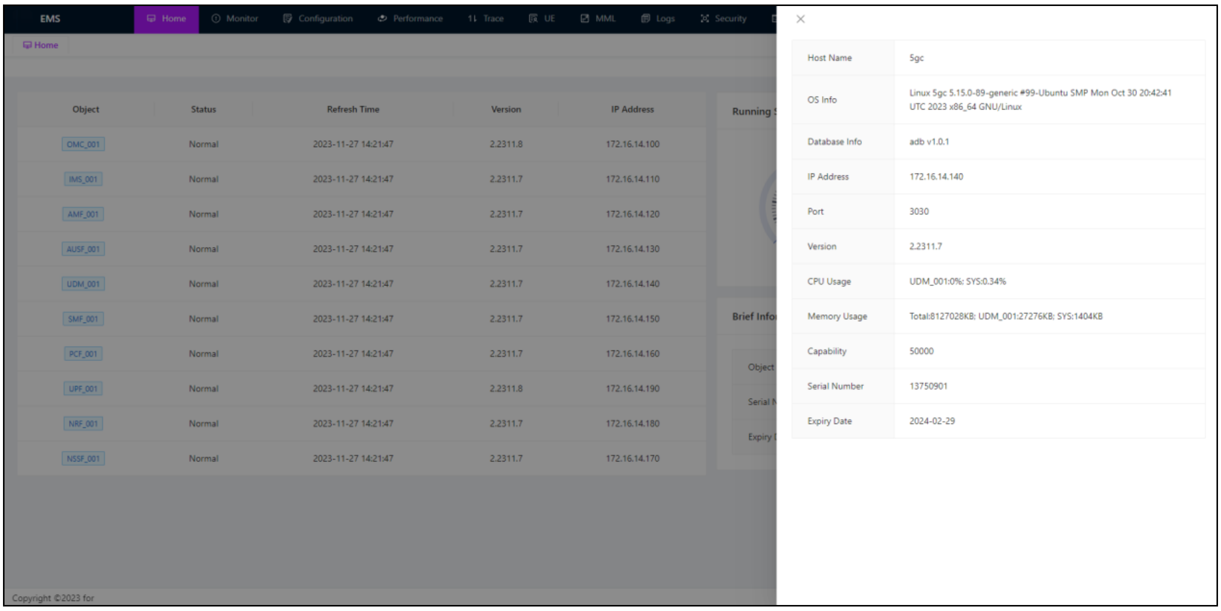
Object	Status	Refresh Time	Version	IP Address
OMC_001	Normal	2023-11-27 14:21:27	2.2311.8	172.16.14.100
IMS_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.110
AMF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.120
AUSF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.130
UDM_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.140
SMF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.150
PCF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.160
UPF_001	Normal	2023-11-27 14:21:27	2.2311.8	172.16.14.190
NRF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.180
NSSF_001	Normal	2023-11-27 14:21:27	2.2311.7	172.16.14.170

Brief Information

Object	OMC
Version	2.2311.8
Status	Normal

- 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, license serial number and validity period, operating system, database, IP, port, user capacity etc.

The network element status display will refresh every 10 seconds:



Object	Status	Refresh Time	Version	IP Address
OMC_001	Normal	2023-11-27 14:21:47	2.2311.8	172.16.14.100
IMS_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.110
AMF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.120
AUSF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.130
UDM_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.140
SMF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.150
PCF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.160
UPF_001	Normal	2023-11-27 14:21:47	2.2311.8	172.16.14.190
NRF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.180
NSSF_001	Normal	2023-11-27 14:21:47	2.2311.7	172.16.14.170

Host Name	5gc
OS Info	Linux 5gc 5.15.0-89-generic #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023 x86_64 GNU/Linux
Database Info	adb v1.0.1
IP Address	172.16.14.140
Port	3030
Version	2.2311.7
CPU Usage	UDM_001:0%; SYS:0.34%
Memory Usage	Total:8127028KB; UDM_001:27276KB; SYS:1404KB
Capability	50000
Serial Number	13750901
Expiry Date	2024-02-29

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 Type	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

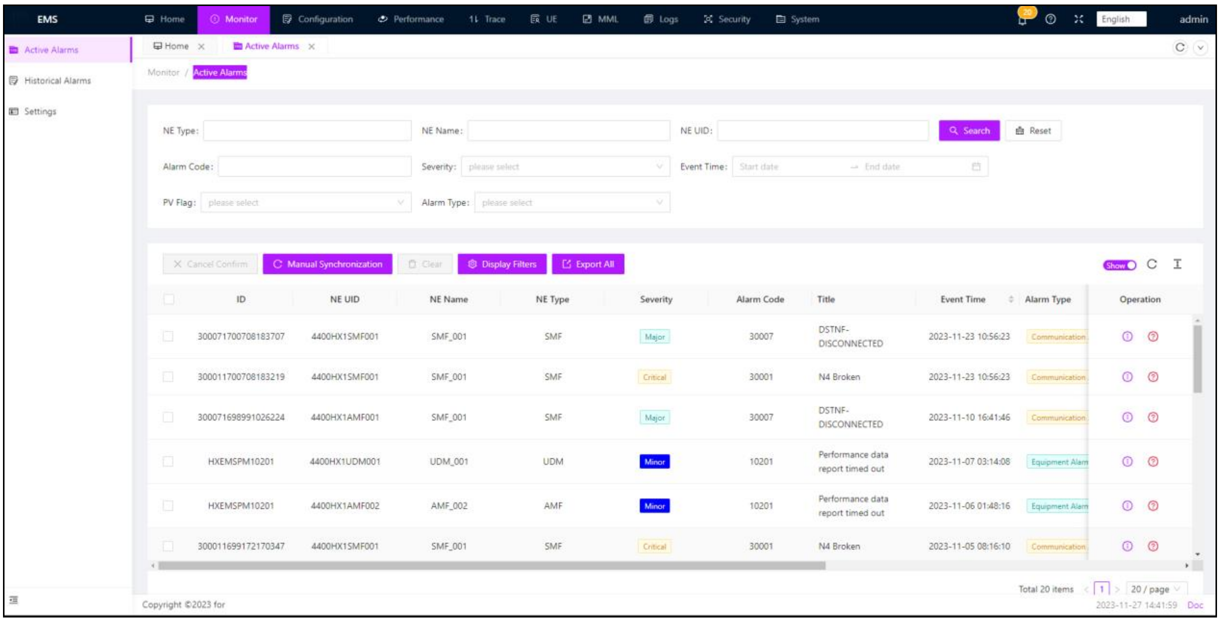
Name	Description
Communication Alarm	A fault on the communication system, such as a network cable disconnection or network equipment fault.
Equipment Alarm	A fault on the equipment
Processing Failure Alarm	An error or exception that occurs during processing, for example, the database is abnormal or the 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：

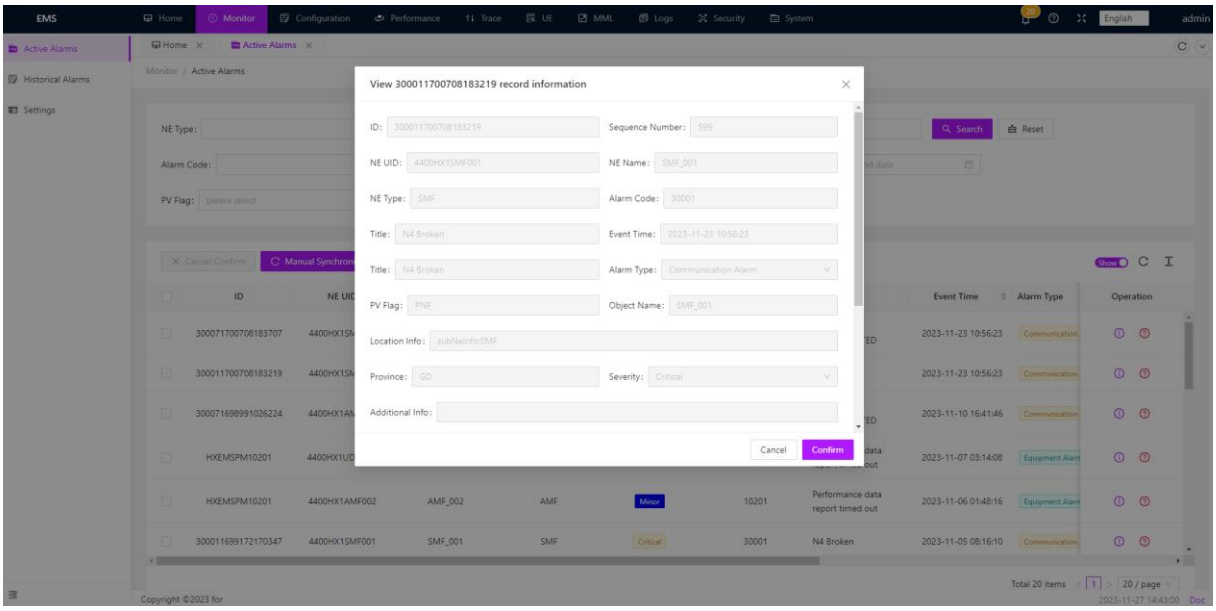


NE Type:
NE Name:
NE UID:
Alarm Code:
Severity: please select
Event Time: Start date → End date
PV Flag: please select
Alarm Type: please select

ID	NE UID	NE Name	NE Type	Severity	Alarm Code	Title	Event Time	Alarm Type	Operation
300071700708183707	4400HX1SMF001	SMF_001	SMF	Major	30007	DSTNF-DISCONNECTED	2023-11-23 10:56:23	Communication	ⓘ ⓘ
300011700708183219	4400HX1SMF001	SMF_001	SMF	Critical	30001	N4 Broken	2023-11-23 10:56:23	Communication	ⓘ ⓘ
300071698991026224	4400HX1AMF001	SMF_001	SMF	Major	30007	DSTNF-DISCONNECTED	2023-11-10 16:41:46	Communication	ⓘ ⓘ
HXEMSPM10201	4400HX1UDM001	UDM_001	UDM	Minor	10201	Performance data report timed out	2023-11-07 03:14:08	Equipment Alarm	ⓘ ⓘ
HXEMSPM10201	4400HX1AMF002	AMF_002	AMF	Minor	10201	Performance data report timed out	2023-11-06 01:48:16	Equipment Alarm	ⓘ ⓘ
300011699172170347	4400HX1SMF001	SMF_001	SMF	Critical	30001	N4 Broken	2023-11-05 08:16:10	Communication	ⓘ ⓘ

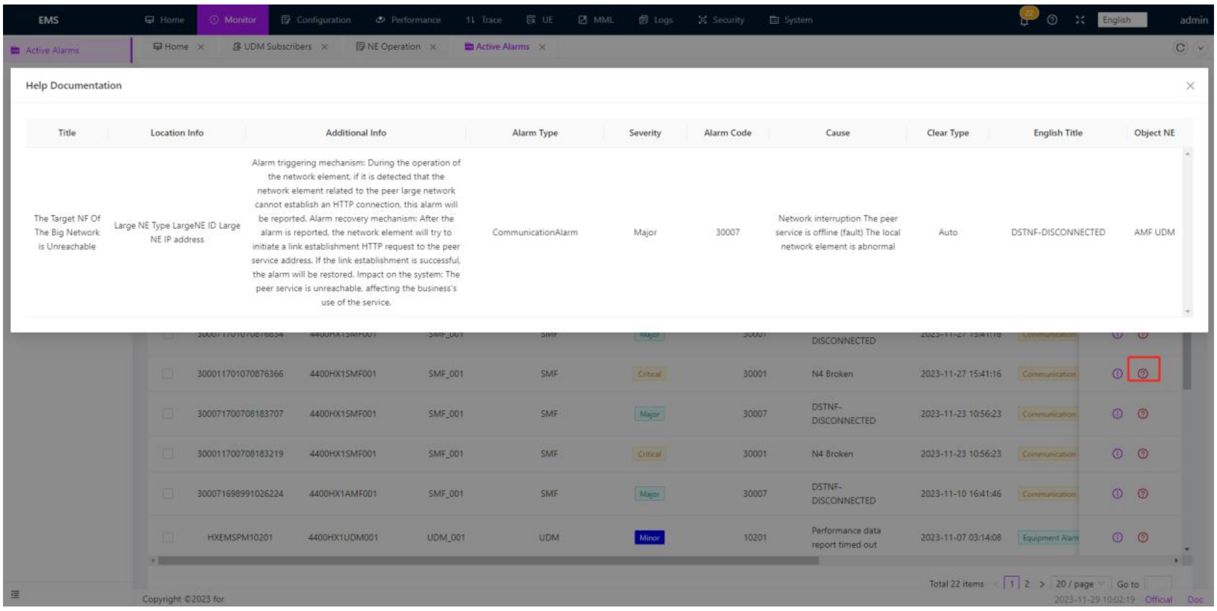
Total 20 items 1 20 / page
2023-11-27 14:41:59

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.



View 300011700708183219 record information

ID:	300011700708183219	Sequence Number:	599
NE UID:	4400HX1SMF001	NE Name:	SMF_001
NE Type:	SMF	Alarm Code:	30001
Title:	N4 Broken	Event Time:	2023-11-23 10:56:23
Title:	N4 Broken	Alarm Type:	Communication Alarm
PV Flag:	PNF	Object Name:	SMF_001
Location Info:	subNeInfo:SMF		
Province:	GD	Severity:	Critical
Additional Info:			



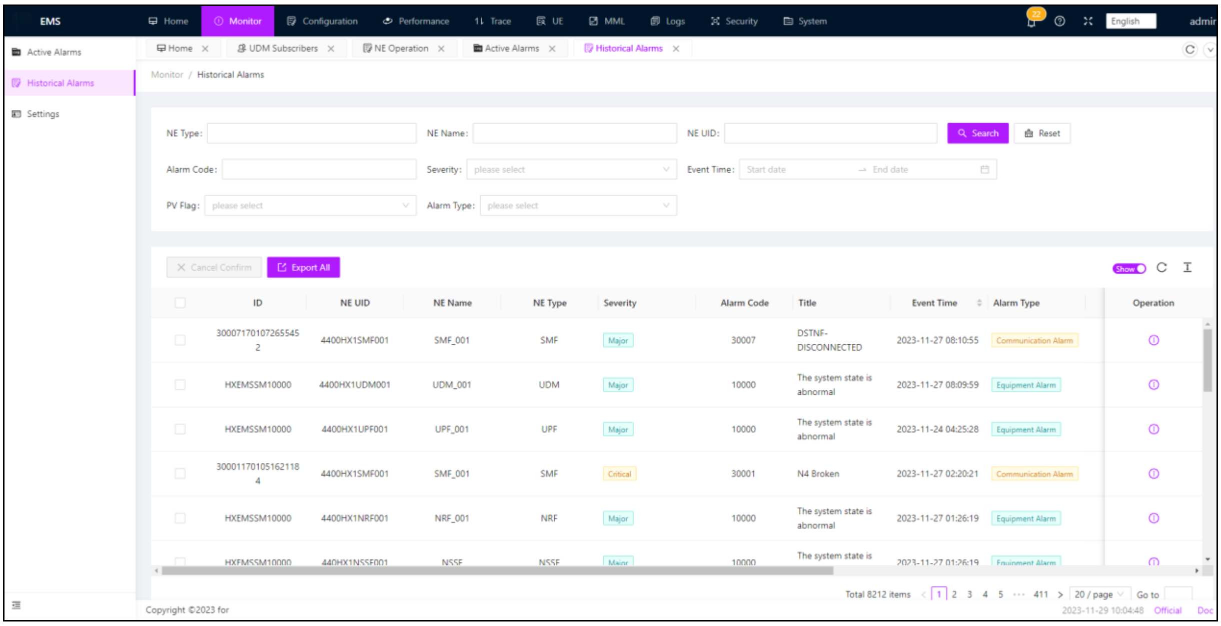
Help Documentation

Title	Location Info	Additional Info	Alarm Type	Severity	Alarm Code	Cause	Clear Type	English Title	Object NE
The Target NF Of The Big Network is Unreachable	Large NE Type LargeNE ID Large NE IP address	Alarm triggering mechanism: During the operation of the network element, if it is detected that the network element related to the peer large network cannot establish an HTTP connection, this alarm will be reported. Alarm recovery mechanism: After the alarm is reported, the network element will try to initiate a link establishment HTTP request to the peer service address. If the link establishment is successful, the alarm will be restored. Impact on the system: The peer service is unreachable, affecting the business's use of the service.	CommunicationAlarm	Major	30007	Network interruption The peer service is offline (fault) The local network element is abnormal	Auto	DSTNF-DISCONNECTED	AMF UDM

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.



NE Type: NE Name: NE UID:

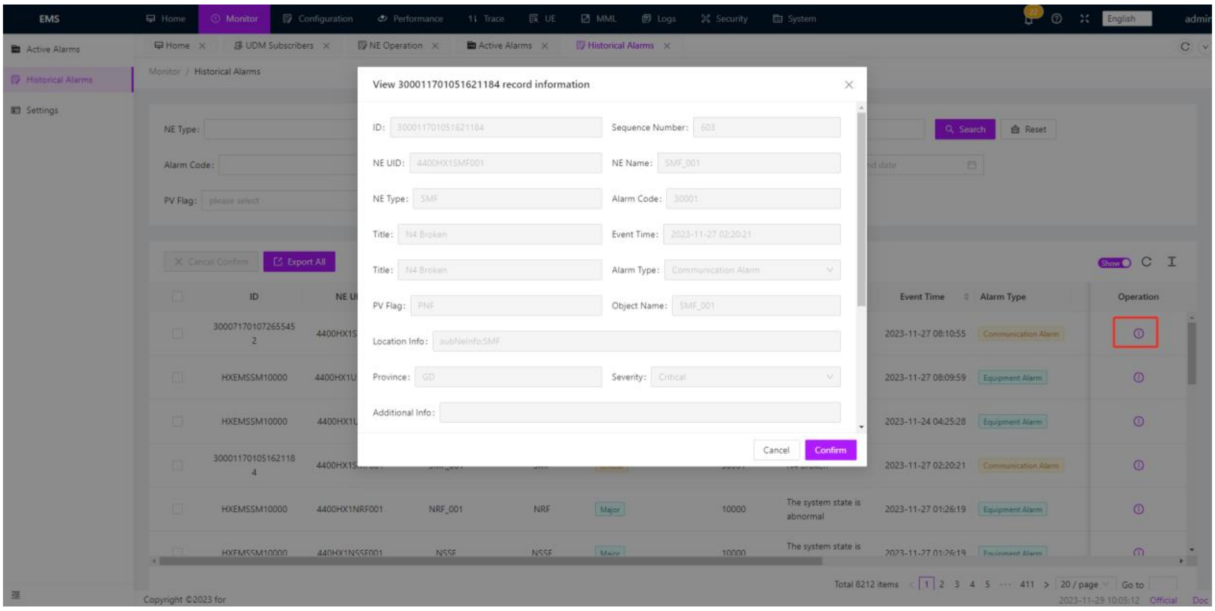
Alarm Code: Severity: please select Event Time: Start date → End date

PV Flag: please select Alarm Type: please select

ID	NE UID	NE Name	NE Type	Severity	Alarm Code	Title	Event Time	Alarm Type	Operation
300071701072655452	4400HX1SMF001	SMF_001	SMF	Major	30007	DSTNF-DISCONNECTED	2023-11-27 08:10:55	Communication Alarm	ⓘ
HXEMSSM10000	4400HX1UDM001	UDM_001	UDM	Major	10000	The system state is abnormal	2023-11-27 08:09:59	Equipment Alarm	ⓘ
HXEMSSM10000	4400HX1UPF001	UPF_001	UPF	Major	10000	The system state is abnormal	2023-11-24 04:25:28	Equipment Alarm	ⓘ
300011701051621184	4400HX1SMF001	SMF_001	SMF	Critical	30001	N4 Broken	2023-11-27 02:20:21	Communication Alarm	ⓘ
HXEMSSM10000	4400HX1NRF001	NRF_001	NRF	Major	10000	The system state is abnormal	2023-11-27 01:26:19	Equipment Alarm	ⓘ
HXEMSSM10000	440HX1NSSF001	NSSF	NSSF	Major	10000	The system state is	2023-11-27 01:26:19	Equipment Alarm	ⓘ

Total 8212 items < 1 2 3 4 5 ··· 411 > 20 / page Go to

Copyright ©2023 for 2023-11-29 10:04:48 Official Doc



View 300011701051621184 record information

ID: 300011701051621184 Sequence Number: 603

NE UID: 4400HX1SMF001 NE Name: SMF_001

NE Type: SMF Alarm Code: 30001

Title: N4 Broken Event Time: 2023-11-27 02:20:21

Title: N4 Broken Alarm Type: Communication Alarm

PV Flag: PNF Object Name: SMF_001

Location Info: subNeInfo:SMF

Province: GD Severity: Critical

Additional Info:

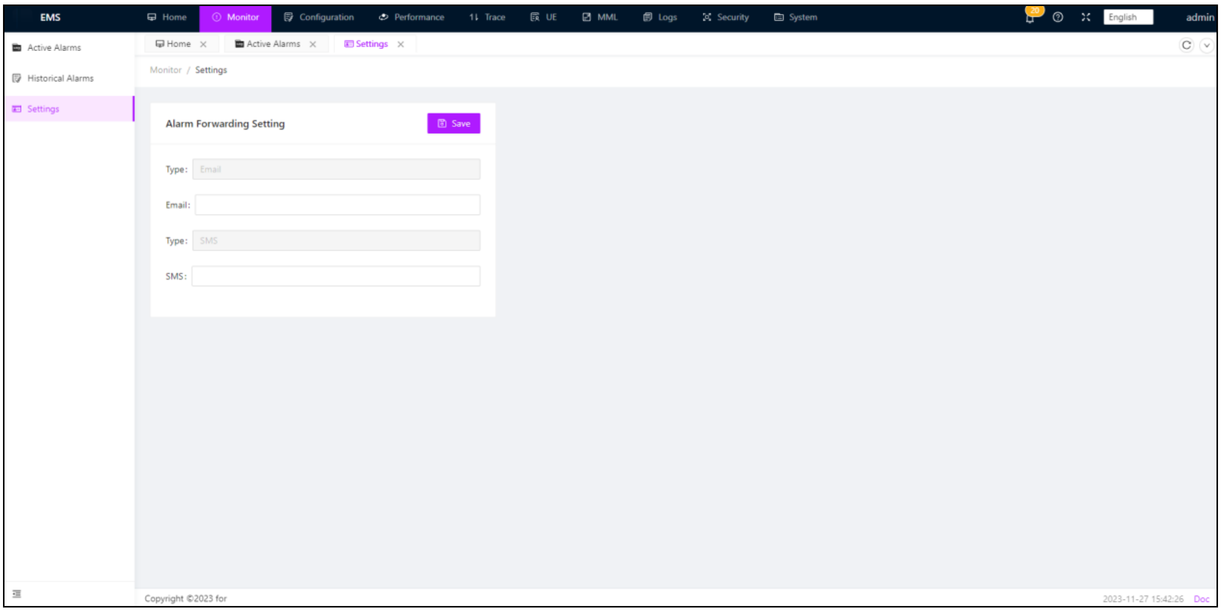
3.3.3 Settings

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.



Alarm Forwarding Setting

Type: Email

Email:

Type: SMS

SMS:

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.

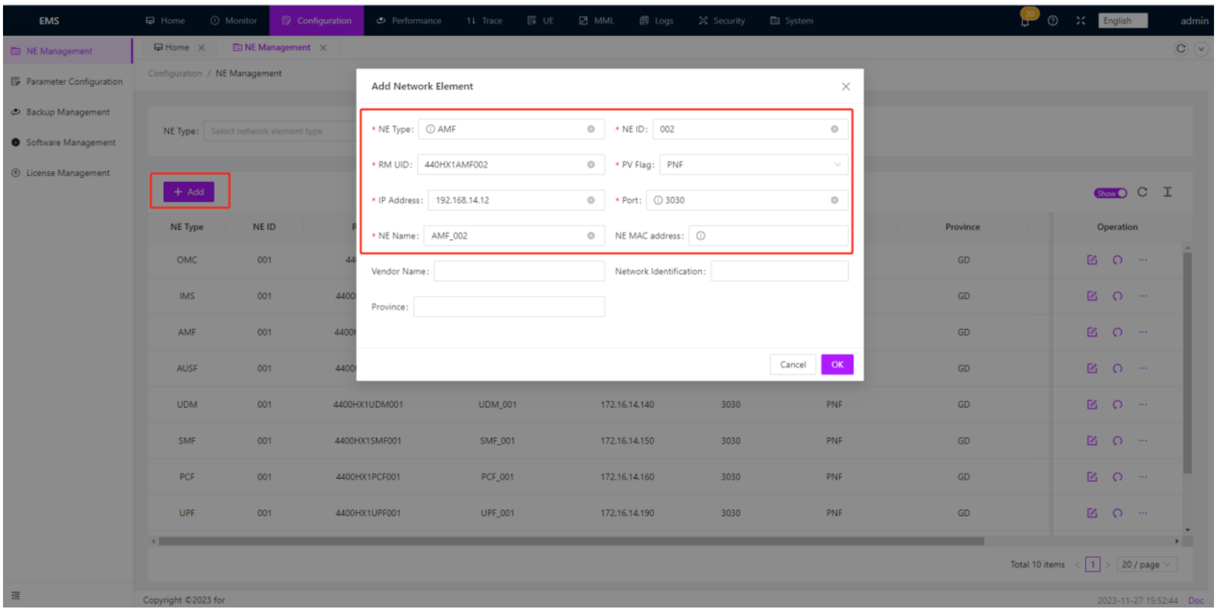
3.4.1 NE Management

This function allows you to add, delete, and modify NE information, restart, start, and stop NE, export and import NE configurations on the OMC.

Click on **+ Add** 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



NE Type: Select network element type

Add Network Element

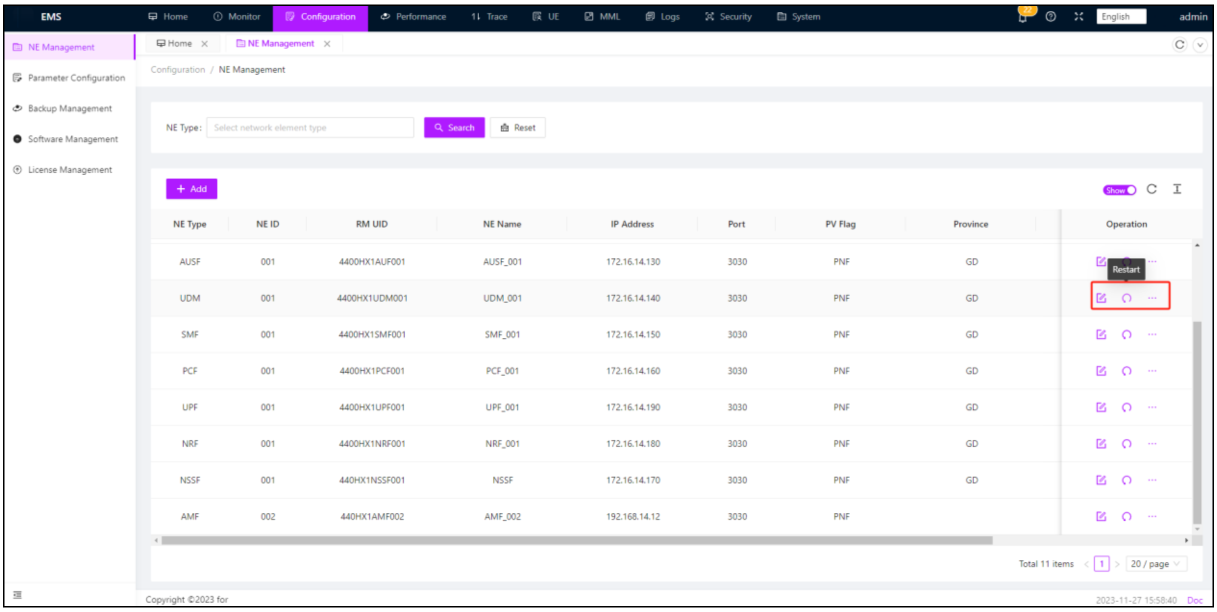
* NE Type: AMF	* NE ID: 002
* RM UID: 440HX1AMF002	* PV Flag: PNF
* IP Address: 192.168.14.12	* Port: 3030
* NE Name: AMF_002	NE MAC address:
Vendor Name:	Network Identification:
Province:	

Cancel OK

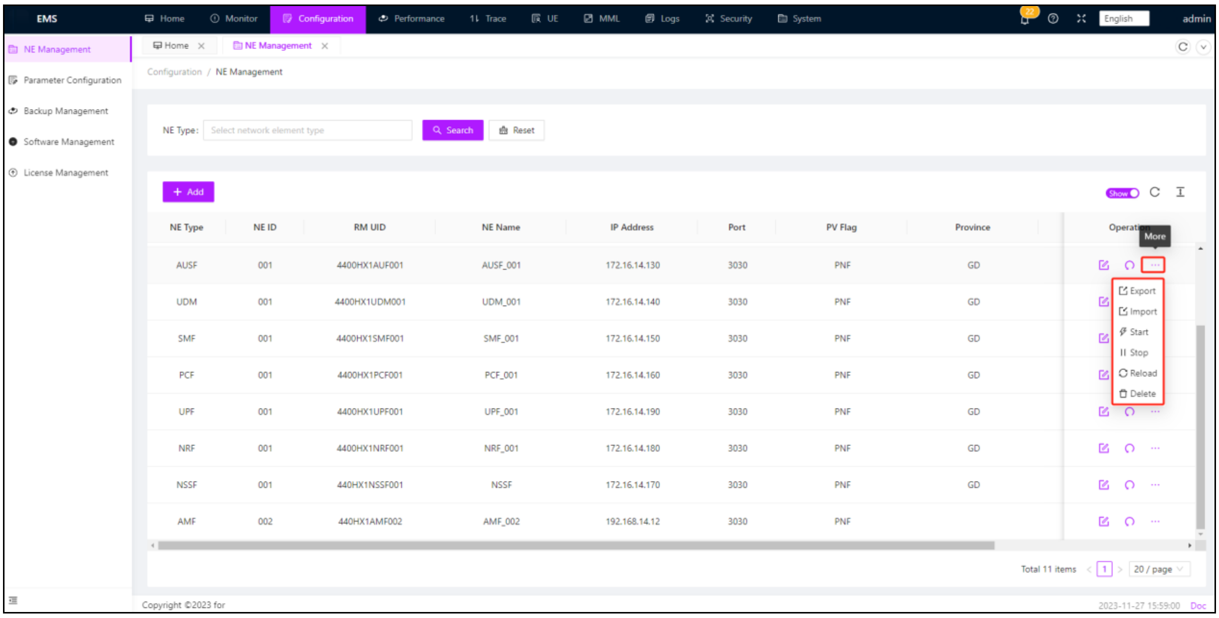
NE Type	NE ID	R					Province	Operation
OMC	001	44					GD	
IMS	001	4400					GD	
AMF	001	4400					GD	
AUSF	001	4400					GD	
UDM	001	4400HX1UDM001	UDM_001	172.16.14.140	3030	PNF	GD	
SMF	001	4400HX1SMF001	SMF_001	172.16.14.150	3030	PNF	GD	
PCF	001	4400HX1PCF001	PCF_001	172.16.14.160	3030	PNF	GD	
UPF	001	4400HX1UPF001	UPF_001	172.16.14.190	3030	PNF	GD	

Total 10 items 1 20 / page

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.



NE Type	NE ID	RM UID	NE Name	IP Address	Port	PV Flag	Province	Operation
AUSF	001	4400HX1AUF001	AUSF_001	172.16.14.130	3030	PNF	GD	
UDM	001	4400HX1UDM001	UDM_001	172.16.14.140	3030	PNF	GD	
SMF	001	4400HX1SMF001	SMF_001	172.16.14.150	3030	PNF	GD	
PCF	001	4400HX1PCF001	PCF_001	172.16.14.160	3030	PNF	GD	
UPF	001	4400HX1UPF001	UPF_001	172.16.14.190	3030	PNF	GD	
NRF	001	4400HX1NRF001	NRF_001	172.16.14.180	3030	PNF	GD	
NSSF	001	440HX1NSSF001	NSSF	172.16.14.170	3030	PNF	GD	
AMF	002	440HX1AMF002	AMF_002	192.168.14.12	3030	PNF		

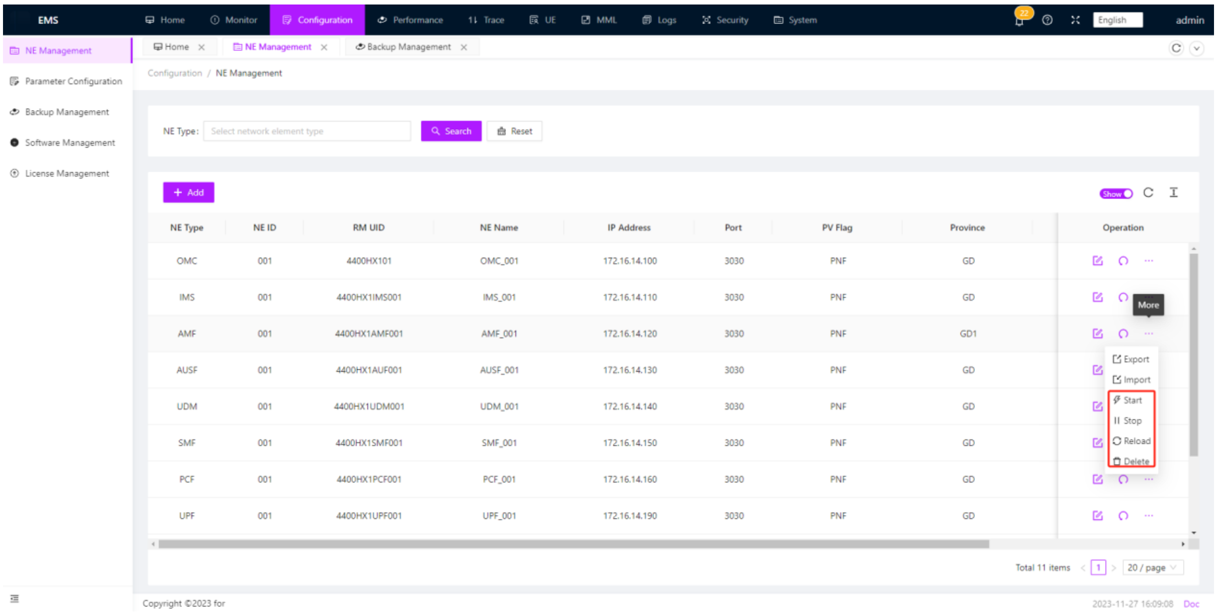


NE Type	NE ID	RM UID	NE Name	IP Address	Port	PV Flag	Province	Operation
AUSF	001	4400HX1AUF001	AUSF_001	172.16.14.130	3030	PNF	GD	
UDM	001	4400HX1UDM001	UDM_001	172.16.14.140	3030	PNF	GD	
SMF	001	4400HX1SMF001	SMF_001	172.16.14.150	3030	PNF	GD	
PCF	001	4400HX1PCF001	PCF_001	172.16.14.160	3030	PNF	GD	
UPF	001	4400HX1UPF001	UPF_001	172.16.14.190	3030	PNF	GD	
NRF	001	4400HX1NRF001	NRF_001	172.16.14.180	3030	PNF	GD	
NSSF	001	440HX1NSSF001	NSSF	172.16.14.170	3030	PNF	GD	
AMF	002	440HX1AMF002	AMF_002	192.168.14.12	3030	PNF		

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

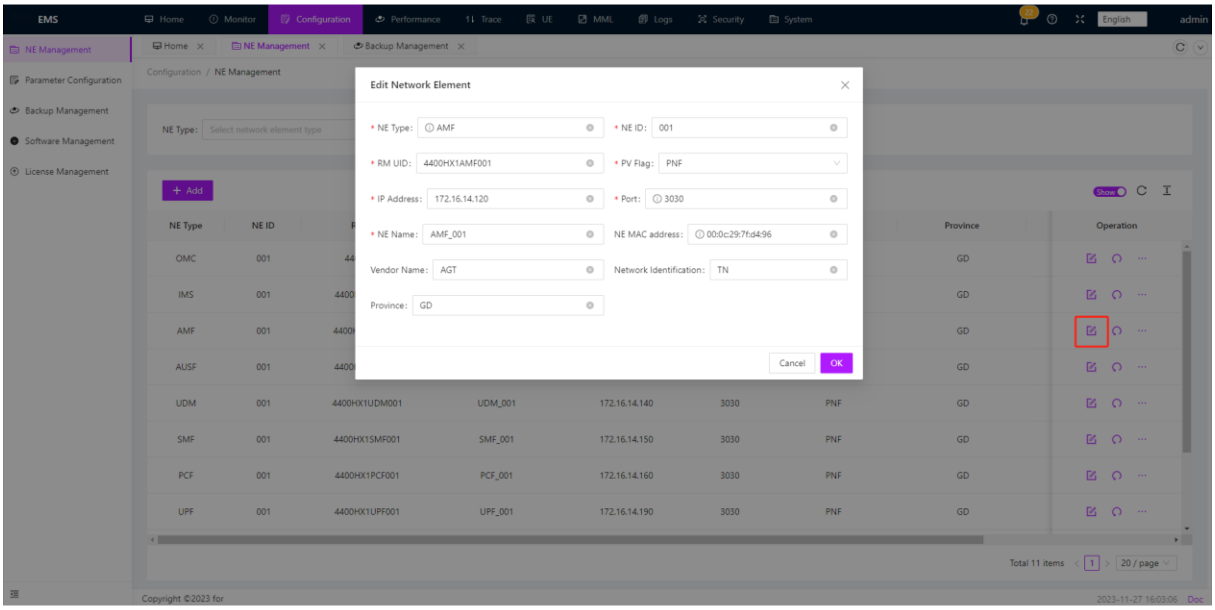
The operator can click "Start" in "More" to start running the network element, click "Stop" to stop running the network element, click "Reload" to reset the network element parameters, and click "Delete" to delete the network element.



NE Type: Select network element type

NE Type	NE ID	RM UID	NE Name	IP Address	Port	PV Flag	Province
OMC	001	4400HX101	OMC_001	172.16.14.100	3030	PNF	GD
IMS	001	4400HX1IMS001	IMS_001	172.16.14.110	3030	PNF	GD
AMF	001	4400HX1AMF001	AMF_001	172.16.14.120	3030	PNF	GD1
AUSF	001	4400HX1AUF001	AUSF_001	172.16.14.130	3030	PNF	GD
UDM	001	4400HX1UDM001	UDM_001	172.16.14.140	3030	PNF	GD
SMF	001	4400HX1SMF001	SMF_001	172.16.14.150	3030	PNF	GD
PCF	001	4400HX1PCF001	PCF_001	172.16.14.160	3030	PNF	GD
UPF	001	4400HX1UPF001	UPF_001	172.16.14.190	3030	PNF	GD

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



Edit Network Element

* NE Type: AMF
* NE ID: 001
* RM UID: 4400HX1AMF001
* PV Flag: PNF
* IP Address: 172.16.14.120
* Port: 3030
* NE Name: AMF_001
NE MAC address: 00:0c:29:7f:d4:96
Vendor Name: AGT
Network Identification: TN
Province: GD

3.4.2 Parameter Configuration

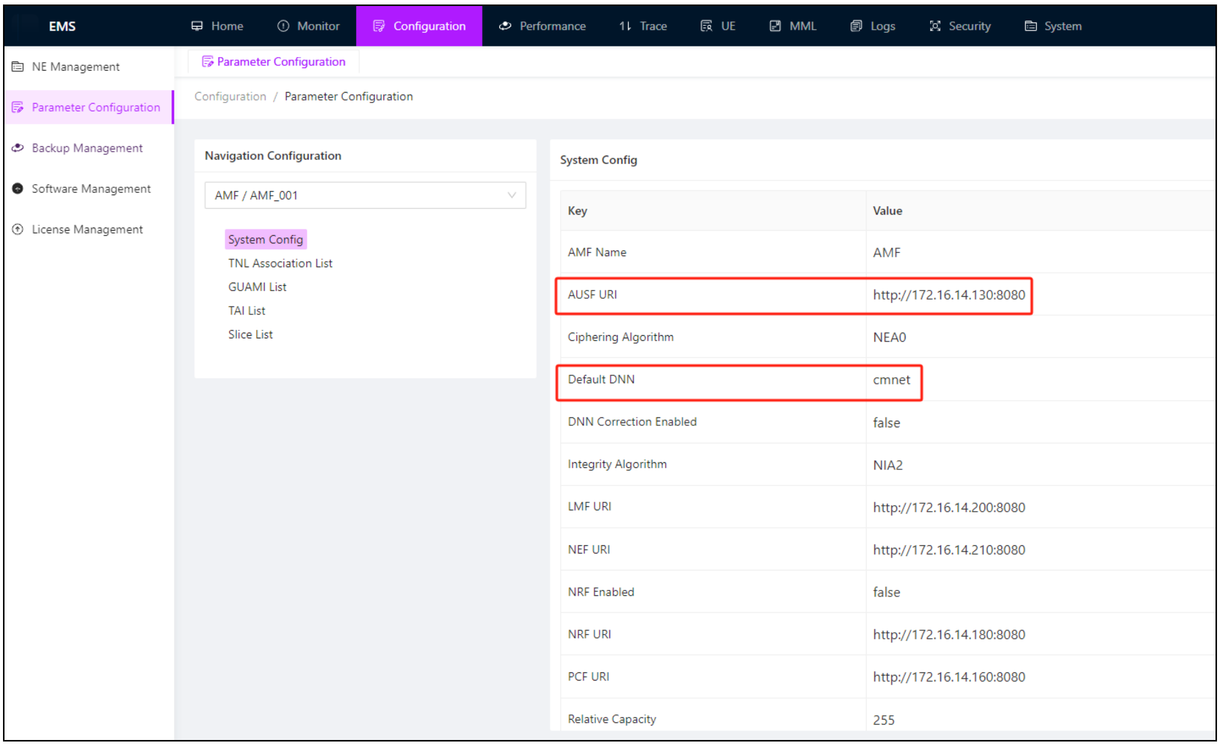
This function corresponds to the parameter configuration of each NE. The operator can add, modify, and delete certain parameter of NE through this function.

The configurations in parameter configuration correspond to the parameters in the NE configuration file. After the modifications are made, the modifications in the configuration file will take effect immediately.

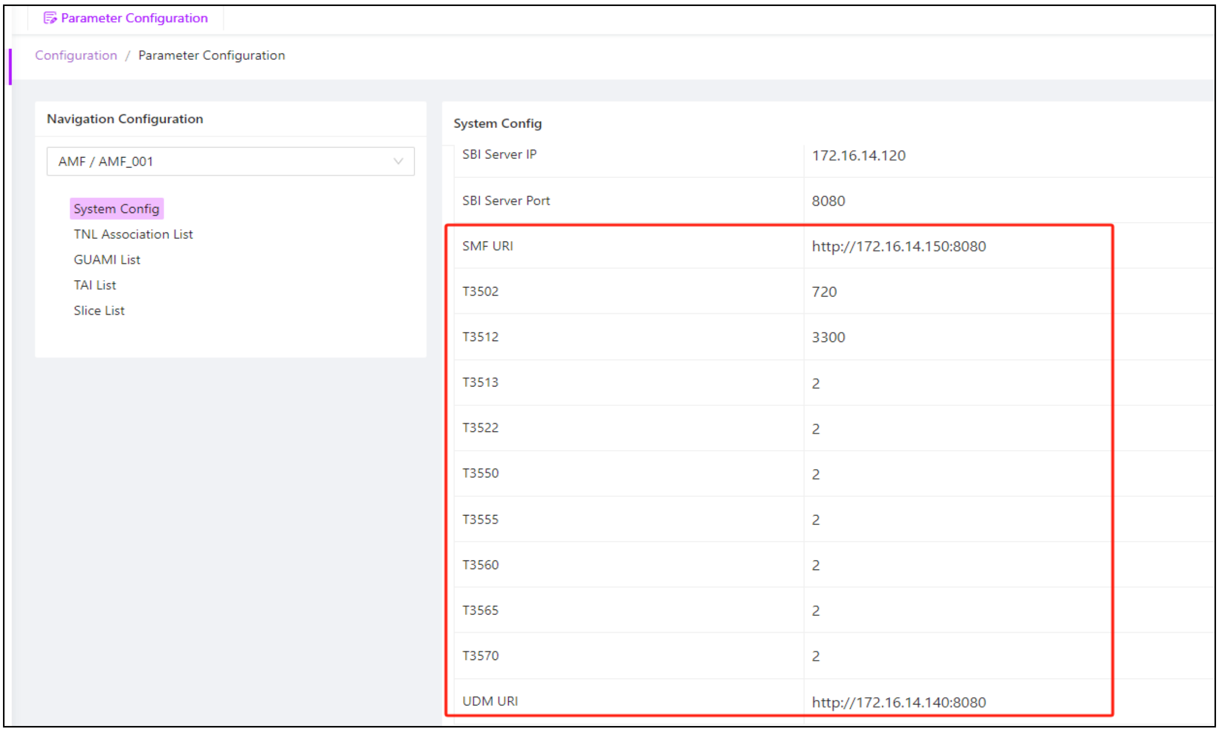
The following are examples of common NE configuration modification, when you want to modify, when the mouse hovers on a specific value, the modification mark will appear, click it to modify, or there will be a modification mark on the right side of some places, click ✎ to modify.

3.4.2.1 AMF

1、**System Config**: in the System Config of the AMF, the AUSF URI and 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.



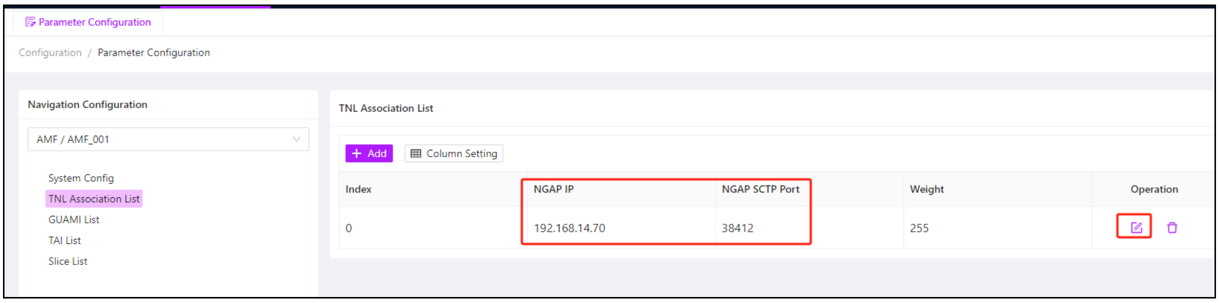
Key	Value
AMF Name	AMF
AUSF URI	http://172.16.14.130:8080
Ciphering Algorithm	NEA0
Default DNN	cmnet
DNN Correction Enabled	false
Integrity Algorithm	NIA2
LMF URI	http://172.16.14.200:8080
NEF URI	http://172.16.14.210:8080
NRF Enabled	false
NRF URI	http://172.16.14.180:8080
PCF URI	http://172.16.14.160:8080
Relative Capacity	255



System Config

SBI Server IP	172.16.14.120
SBI Server Port	8080
SMF URI	http://172.16.14.150:8080
T3502	720
T3512	3300
T3513	2
T3522	2
T3550	2
T3555	2
T3560	2
T3565	2
T3570	2
UDM URI	http://172.16.14.140:8080

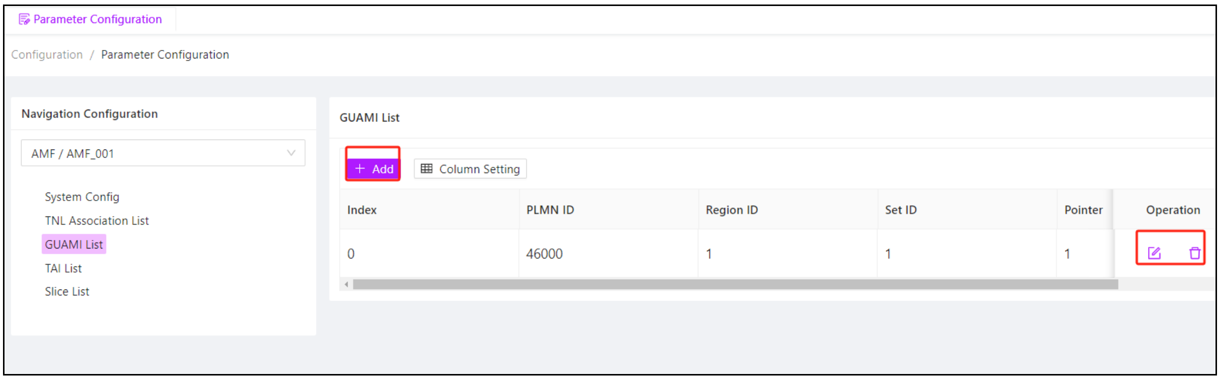
2、**TNL Association List**: in the TNL Association List, you can modify the N2 IP and NGAP SCTP Port, which are used to interconnect with gNB.



TNL Association List

Index	NGAP IP	NGAP SCTP Port	Weight	Operation
0	192.168.14.70	38412	255	

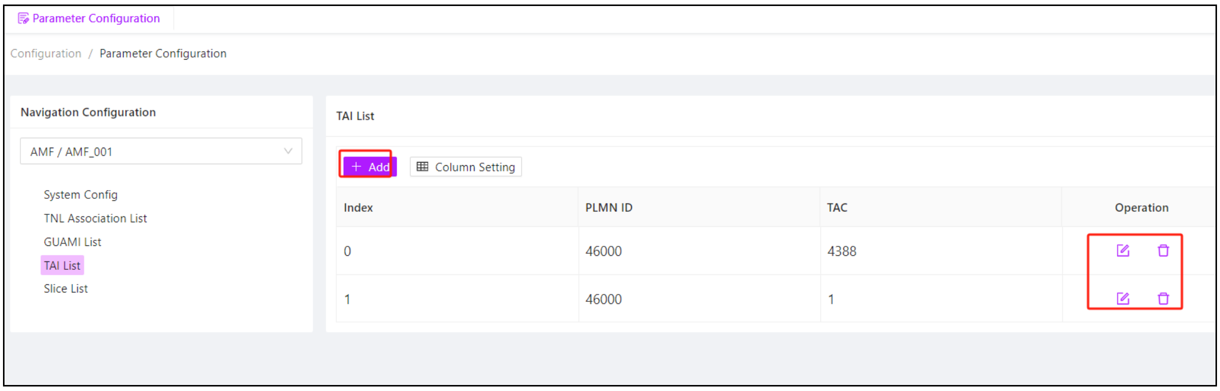
3、**GUAMI List:** GUAMI List can be modified, added, and deleted. When a user device attempts to access or manage mobility, the network determines the required AMF based on the AMF ID in the GUAMI list and routes the relevant control signaling to the corresponding AMF.



GUAMI List

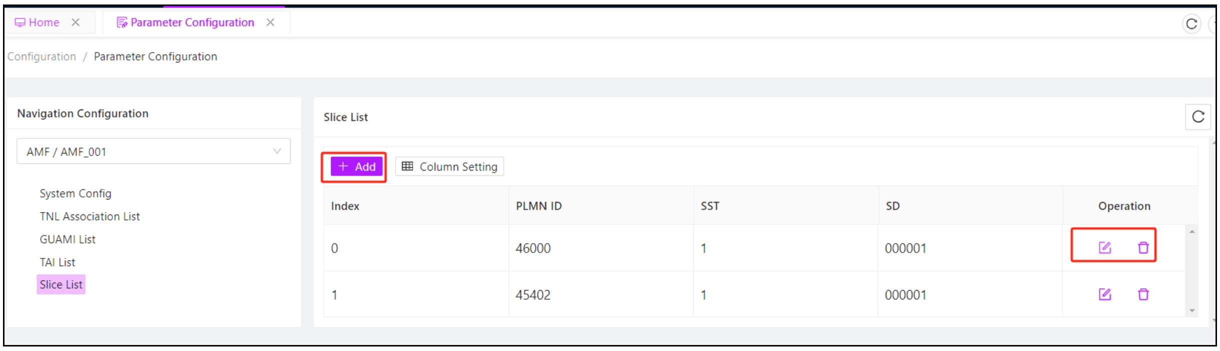
Index	PLMN ID	Region ID	Set ID	Pointer	Operation
0	46000	1	1	1	

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.



Index	PLMN ID	TAC	Operation
0	46000	4388	
1	46000	1	

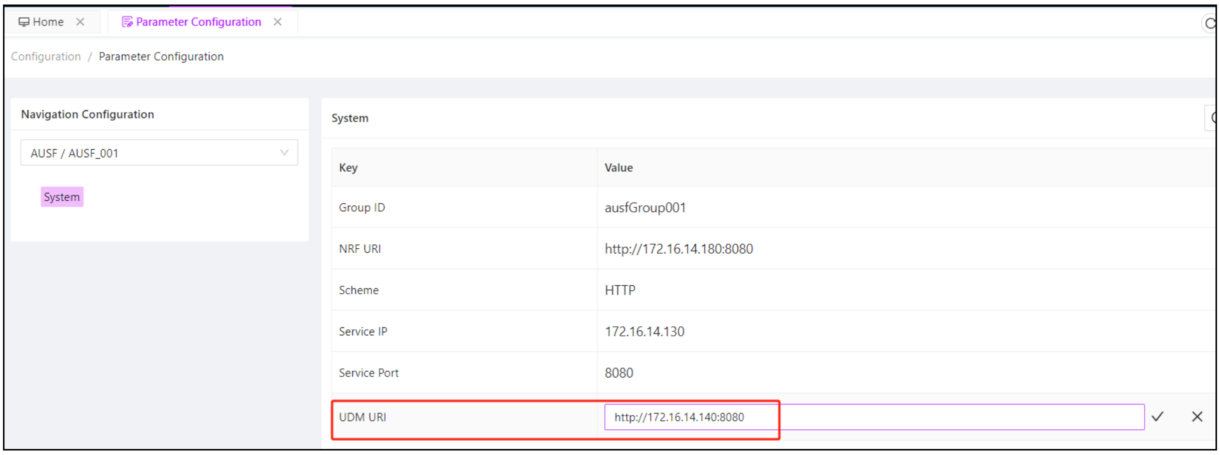
5、**Slice List**: In the Slice List, you can modify the slice information corresponding to the PLMN, which is the slice that the AMF allows to access



Index	PLMN ID	SST	SD	Operation
0	46000	1	000001	
1	45402	1	000001	

3.4.2.2 AUSF

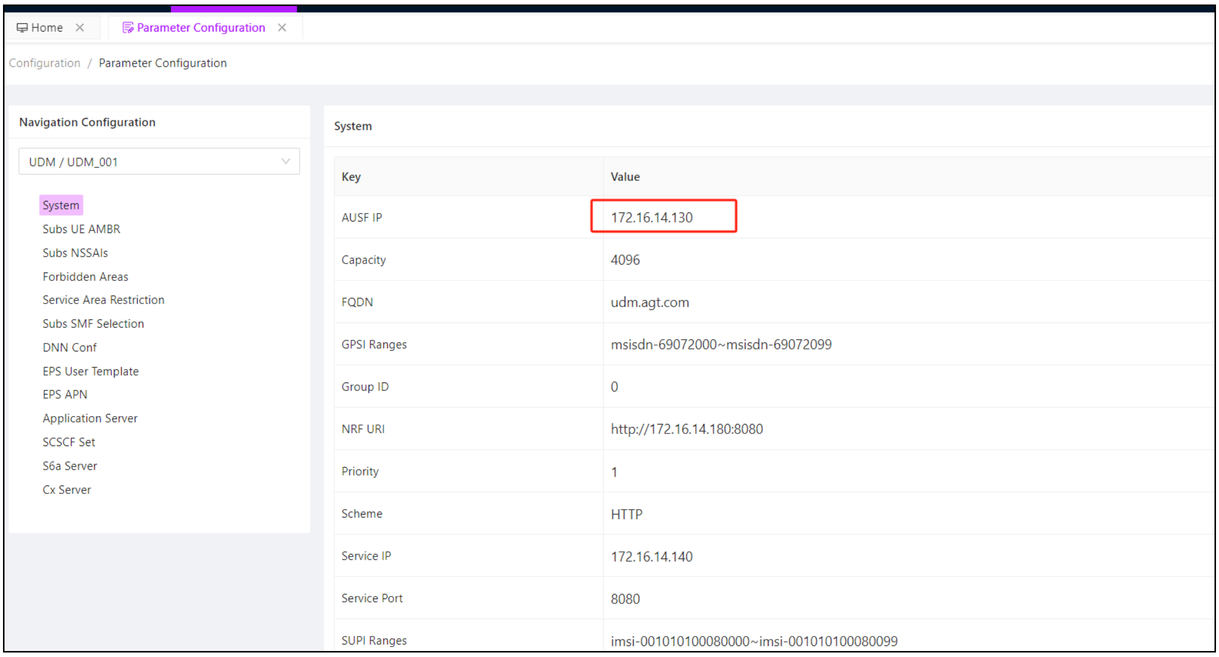
1、**System**:In the AUSF configuration file, change the UDM URI and configure the UDM IP address for interconnection with the AUSF:



Key	Value
Group ID	ausfGroup001
NRF URI	http://172.16.14.180:8080
Scheme	HTTP
Service IP	172.16.14.130
Service Port	8080
UDM URI	http://172.16.14.140:8080

3.4.2.3 UDM

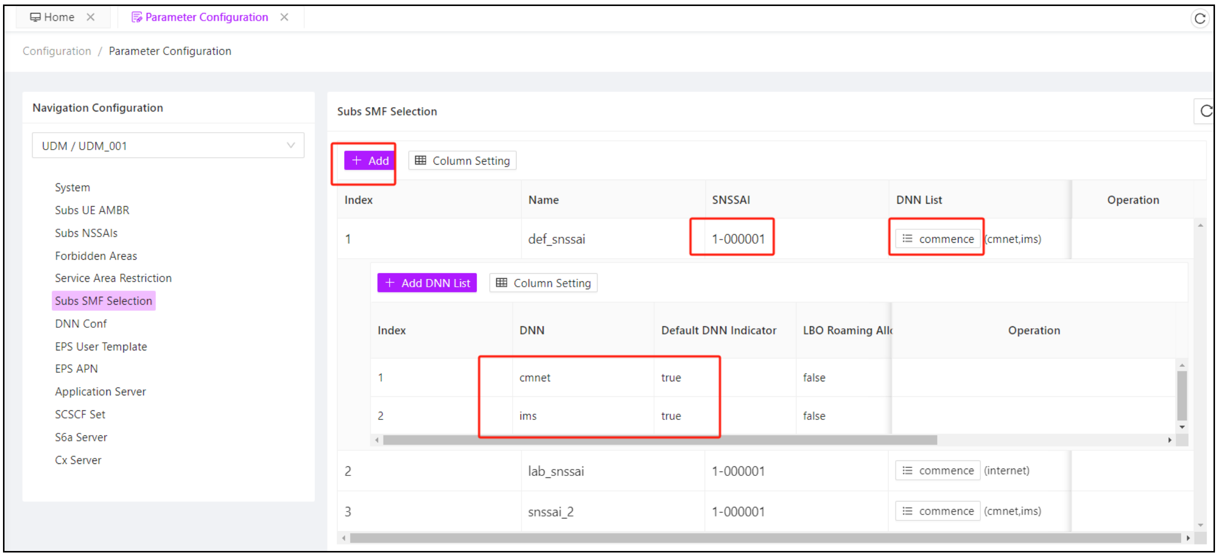
1、**System**: the operator mainly modifies the AUSF IP here



System

Key	Value
AUSF IP	172.16.14.130
Capacity	4096
FQDN	udm.agt.com
GPSI Ranges	msisdn-69072000~msisdn-69072099
Group ID	0
NRF URI	http://172.16.14.180:8080
Priority	1
Scheme	HTTP
Service IP	172.16.14.140
Service Port	8080
SUPI Ranges	imsi-001010100080000~imsi-001010100080099

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

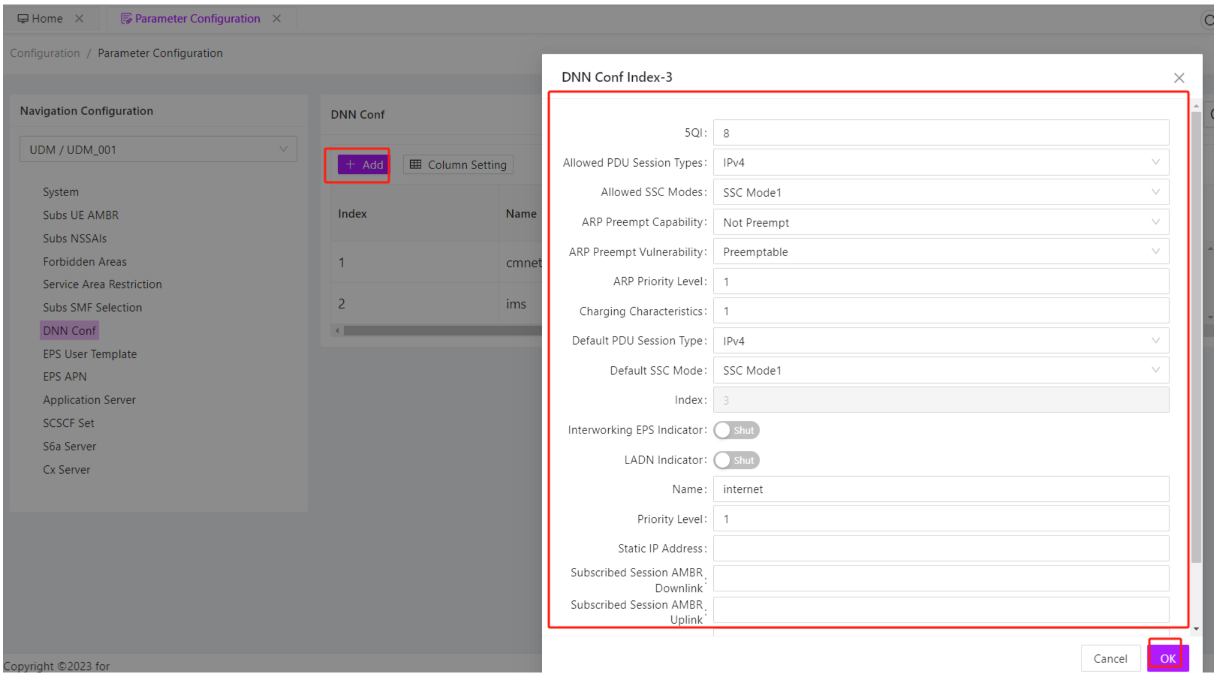


Subs SMF Selection

Index	Name	SNSSAI	DNN List	Operation
1	def_snssai	1-000001	commence (cmnet,ims)	
2	lab_snssai	1-000001	commence (internet)	
3	snssai_2	1-000001	commence (cmnet,ims)	

Index	DNN	Default DNN Indicator	LBO Roaming Allo	Operation
1	cmnet	true	false	
2	ims	true	false	

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.

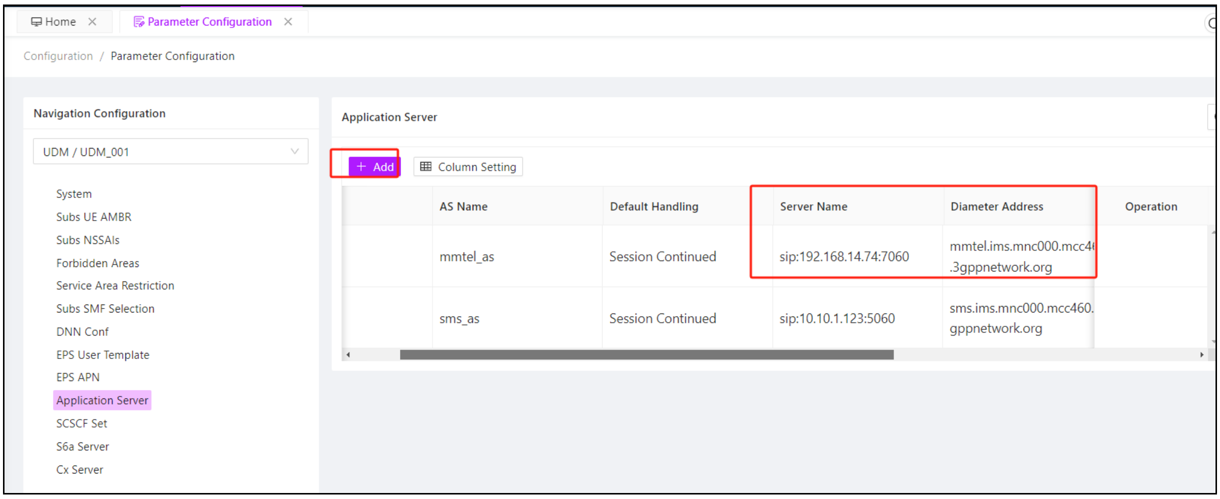


Index	Name
1	cmnet
2	ims

DNN Conf Index-3

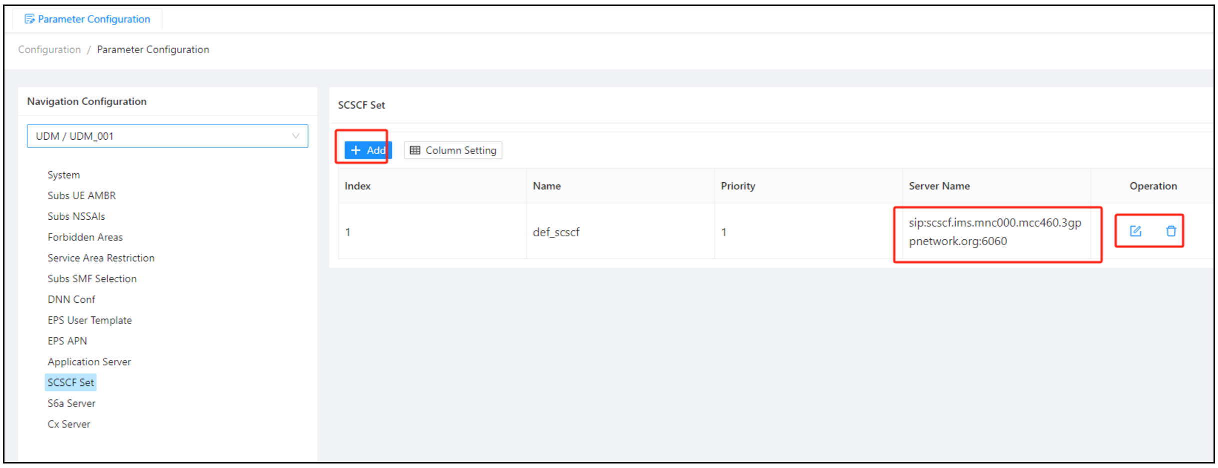
5QI:	8
Allowed PDU Session Types:	IPv4
Allowed SSC Modes:	SSC Mode1
ARP Preempt Capability:	Not Preempt
ARP Preempt Vulnerability:	Preemptable
ARP Priority Level:	1
Charging Characteristics:	1
Default PDU Session Type:	IPv4
Default SSC Mode:	SSC Mode1
Index:	3
Interworking EPS Indicator:	Shut
LADN Indicator:	Shut
Name:	internet
Priority Level:	1
Static IP Address:	
Subscribed Session AMBR Downlink:	
Subscribed Session AMBR Uplink:	

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.



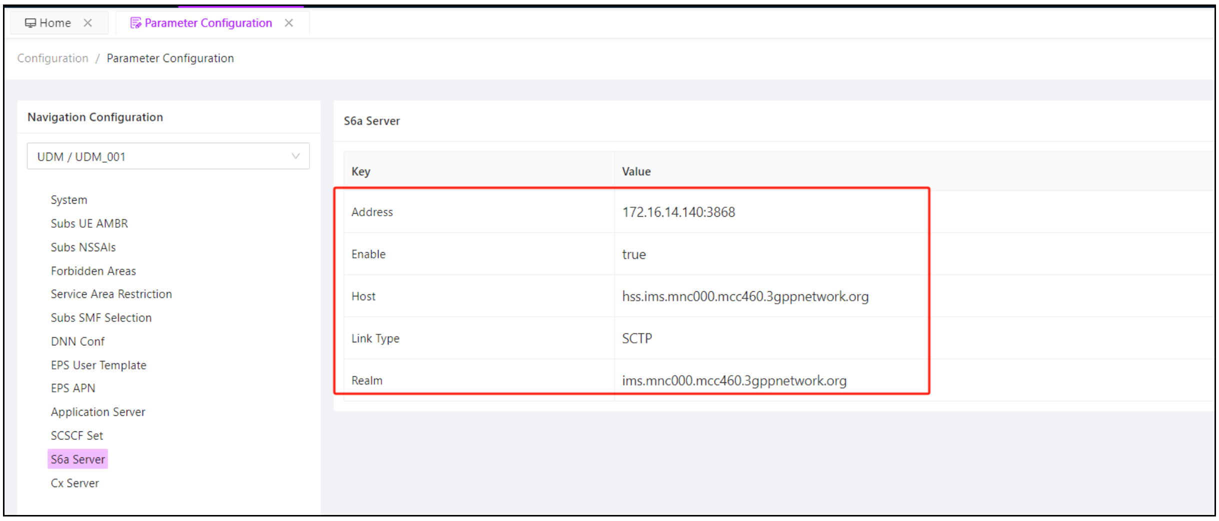
AS Name	Default Handling	Server Name	Diameter Address	Operation
mmtel_as	Session Continued	sip:192.168.14.74:7060	mmtel.ims.mnc000.mcc4(.3gppnetwork.org	
sms_as	Session Continued	sip:10.10.1.123:5060	sms.ims.mnc000.mcc460. gppnetwork.org	

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



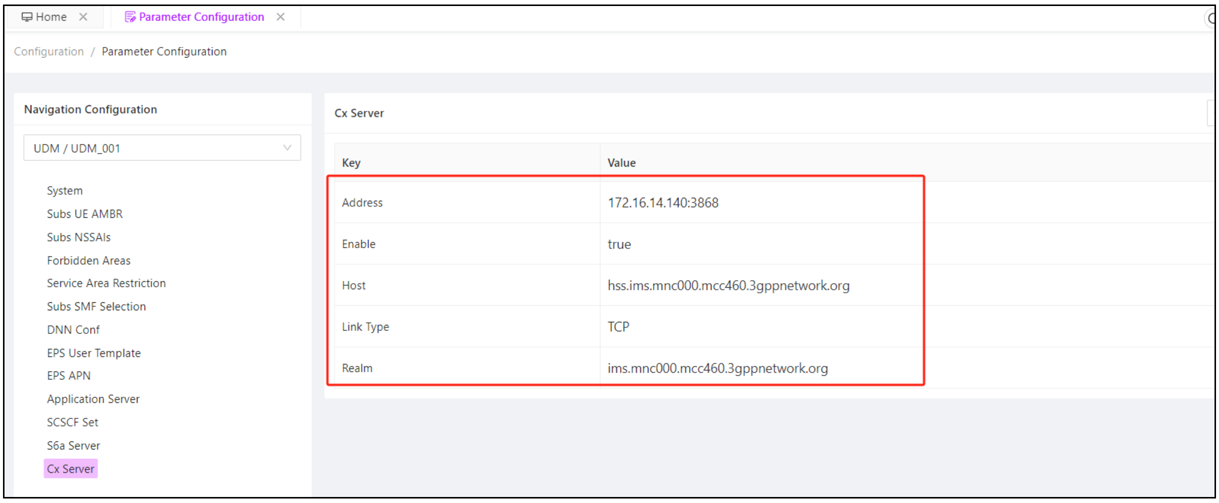
Index	Name	Priority	Server Name	Operation
1	def_scscf	1	sip:scscf.ims.mnc000.mcc460.3gppnetwork.org:6060	

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



Key	Value
Address	172.16.14.140:3868
Enable	true
Host	hss.ims.mnc000.mcc460.3gppnetwork.org
Link Type	SCTP
Realm	ims.mnc000.mcc460.3gppnetwork.org

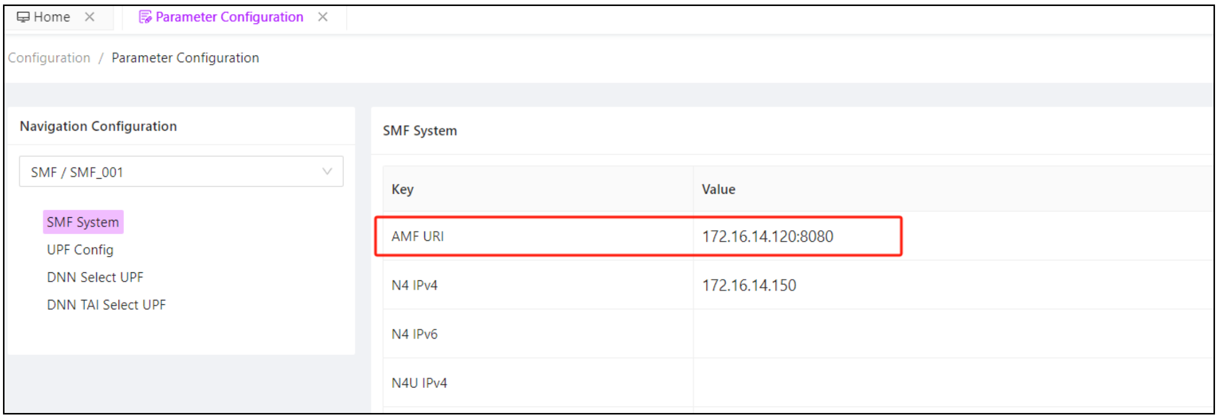
7、**Cx Server:** the operator mainly switches on the Cx port corresponding to the IMS and changes the corresponding host



Key	Value
Address	172.16.14.140:3868
Enable	true
Host	hss.ims.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	ims.mnc000.mcc460.3gppnetwork.org

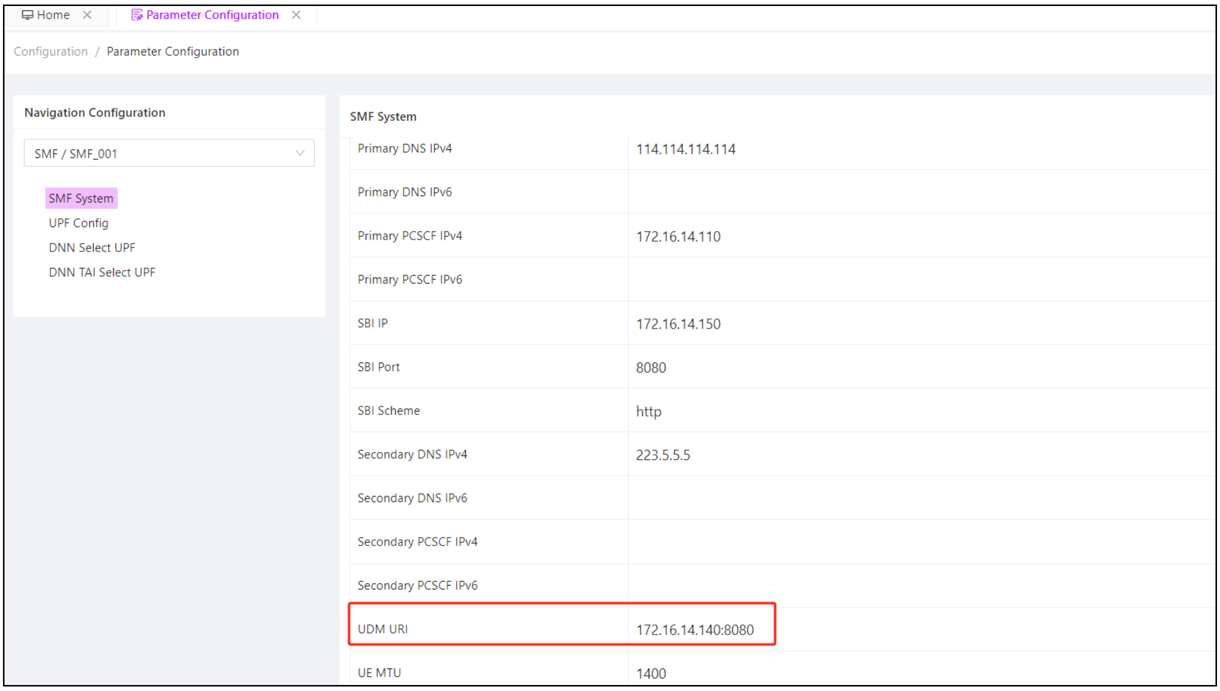
3.4.3.4 SMF

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



SMF System

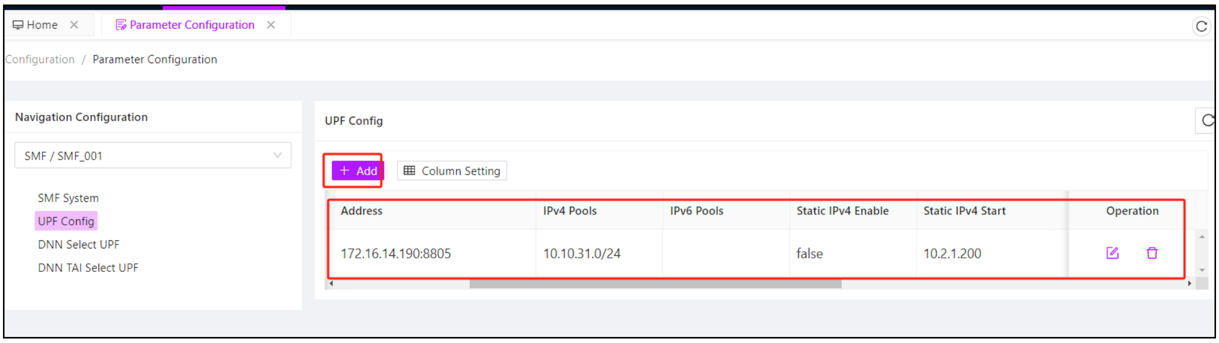
Key	Value
AMF URI	172.16.14.120:8080
N4 IPv4	172.16.14.150
N4 IPv6	
N4U IPv4	



SMF System

Primary DNS IPv4	114.114.114.114
Primary DNS IPv6	
Primary PCSCF IPv4	172.16.14.110
Primary PCSCF IPv6	
SBI IP	172.16.14.150
SBI Port	8080
SBI Scheme	http
Secondary DNS IPv4	223.5.5.5
Secondary DNS IPv6	
Secondary PCSCF IPv4	
Secondary PCSCF IPv6	
UDM URI	172.16.14.140:8080
UE MTU	1400

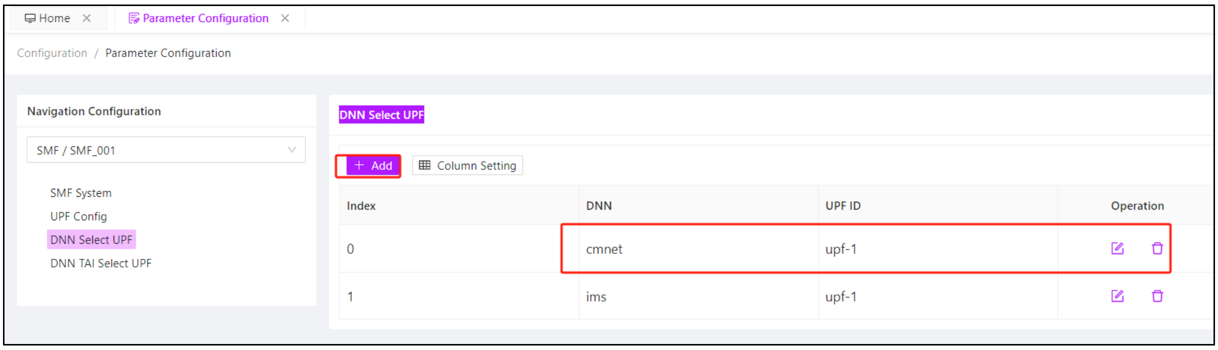
2、**UPF Config**: the operator can configure the UPF IP corresponding to the SMF in UPF config, set the IP address pool assigned to the UE, and set the static IP address.



UPF Config

Address	IPv4 Pools	IPv6 Pools	Static IPv4 Enable	Static IPv4 Start	Operation
172.16.14.190:8805	10.10.31.0/24		false	10.2.1.200	

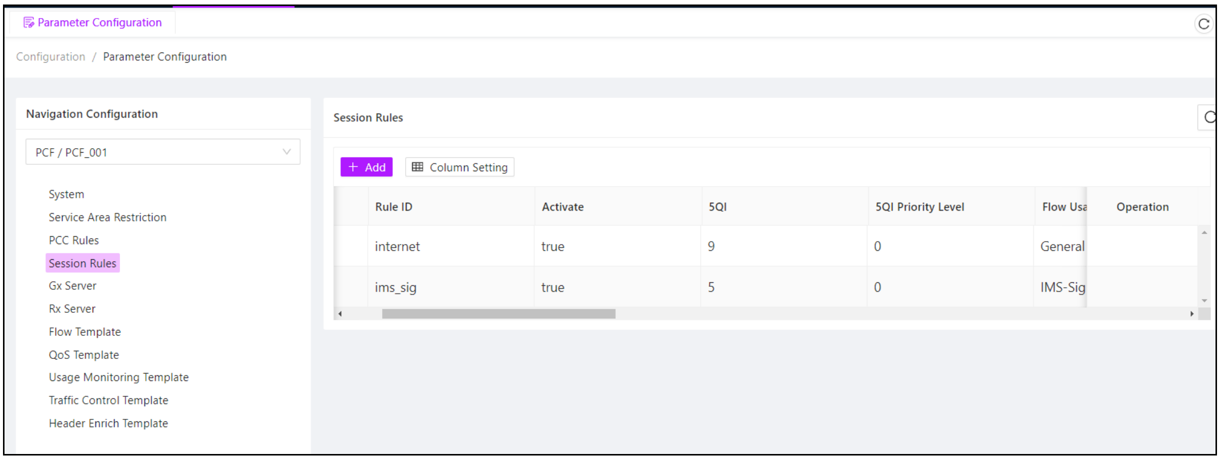
3、**DNN Select UPF**: the operator can configure different DNN to correspond to different UPF.



Index	DNN	UPF ID	Operation
0	cmnet	upf-1	
1	ims	upf-1	

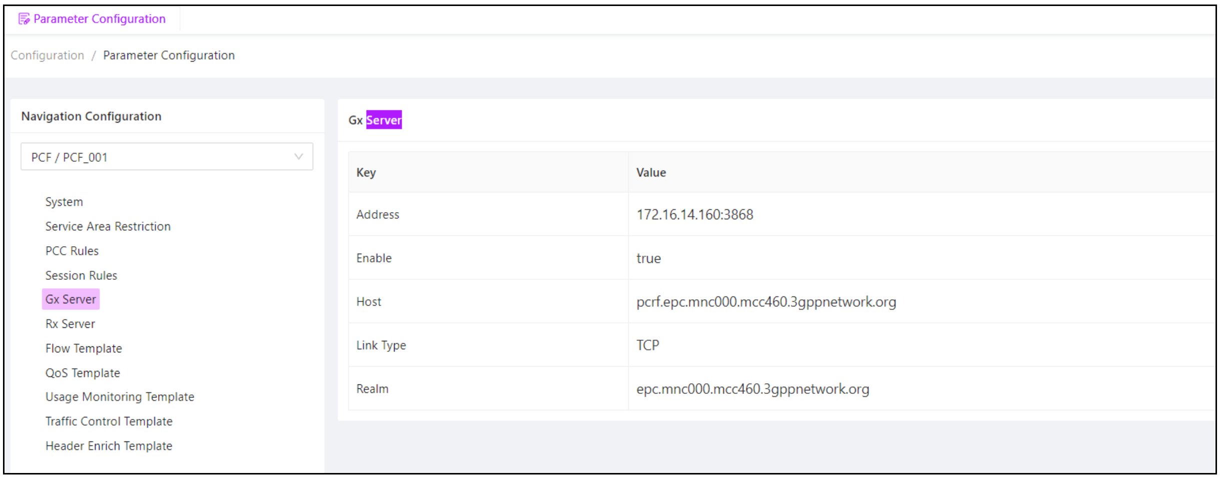
3.4.4.5 PCF

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



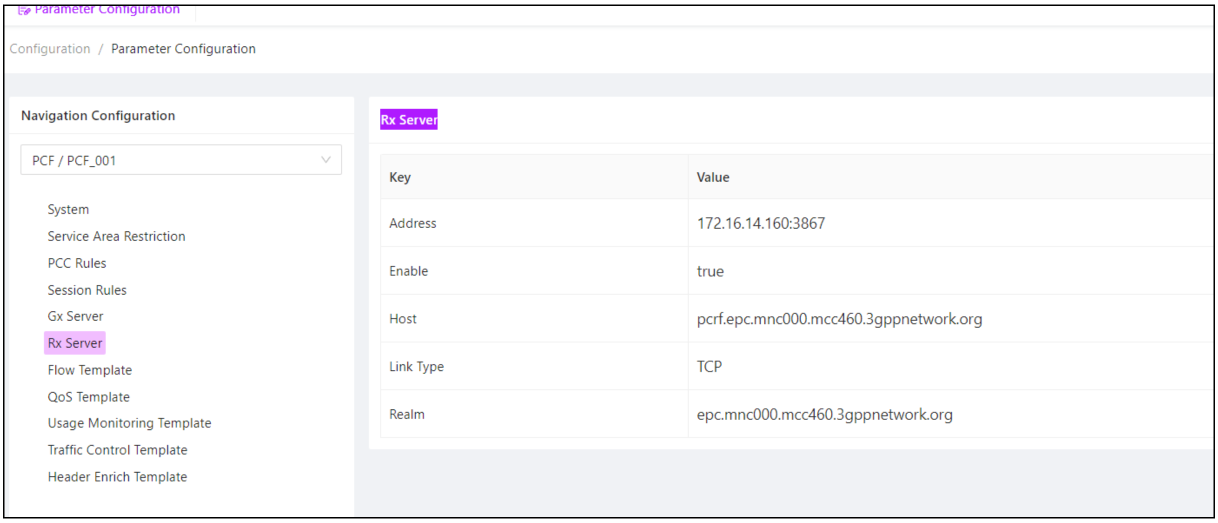
Rule ID	Activate	5QI	5QI Priority Level	Flow Usa	Operation
internet	true	9	0	General	
ims_sig	true	5	0	IMS-Sig	

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



Key	Value
Address	172.16.14.160:3868
Enable	true
Host	pcrf.epc.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	epc.mnc000.mcc460.3gppnetwork.org

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



Parameter Configuration

Configuration / Parameter Configuration

Navigation Configuration

PCF / PCF_001

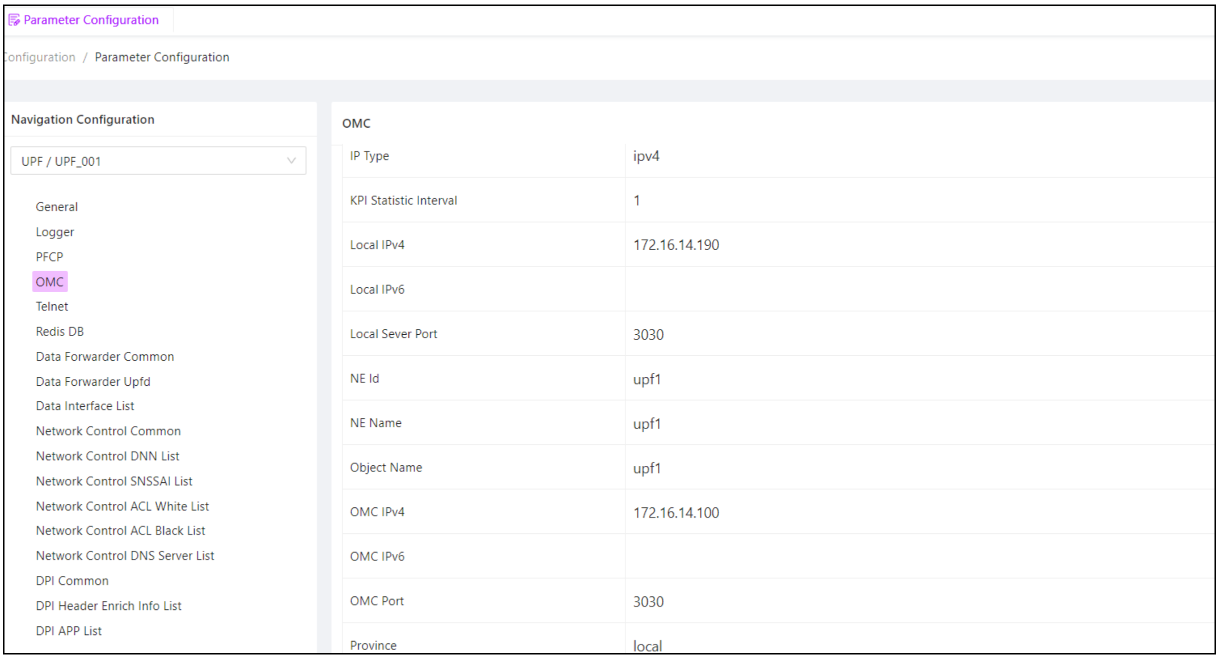
- System
- Service Area Restriction
- PCC Rules
- Session Rules
- Gx Server
- Rx Server
- Flow Template
- QoS Template
- Usage Monitoring Template
- Traffic Control Template
- Header Enrich Template

Rx Server

Key	Value
Address	172.16.14.160:3867
Enable	true
Host	pcrf.epc.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	epc.mnc000.mcc460.3gppnetwork.org

3.4.4.6 UPF

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



Parameter Configuration

onfiguration / Parameter Configuration

Navigation Configuration

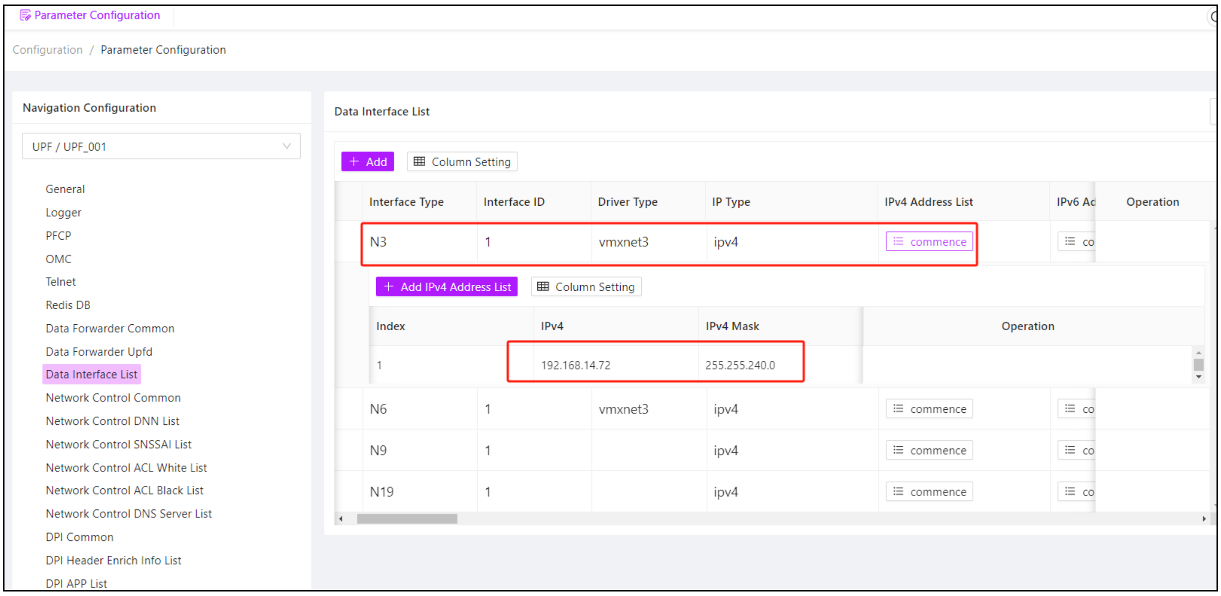
UPF / UPF_001

- General
- Logger
- PFCP
- OMC
- Telnet
- Redis DB
- Data Forwarder Common
- Data Forwarder Upfd
- Data Interface List
- Network Control Common
- Network Control DNN List
- Network Control SNSSAI List
- Network Control ACL White List
- Network Control ACL Black List
- Network Control DNS Server List
- DPI Common
- DPI Header Enrich Info List
- DPI APP List

OMC

IP Type	ipv4
KPI Statistic Interval	1
Local IPv4	172.16.14.190
Local IPv6	
Local Sever Port	3030
NE Id	upf1
NE Name	upf1
Object Name	upf1
OMC IPv4	172.16.14.100
OMC IPv6	
OMC Port	3030
Province	local

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.



Data Interface List

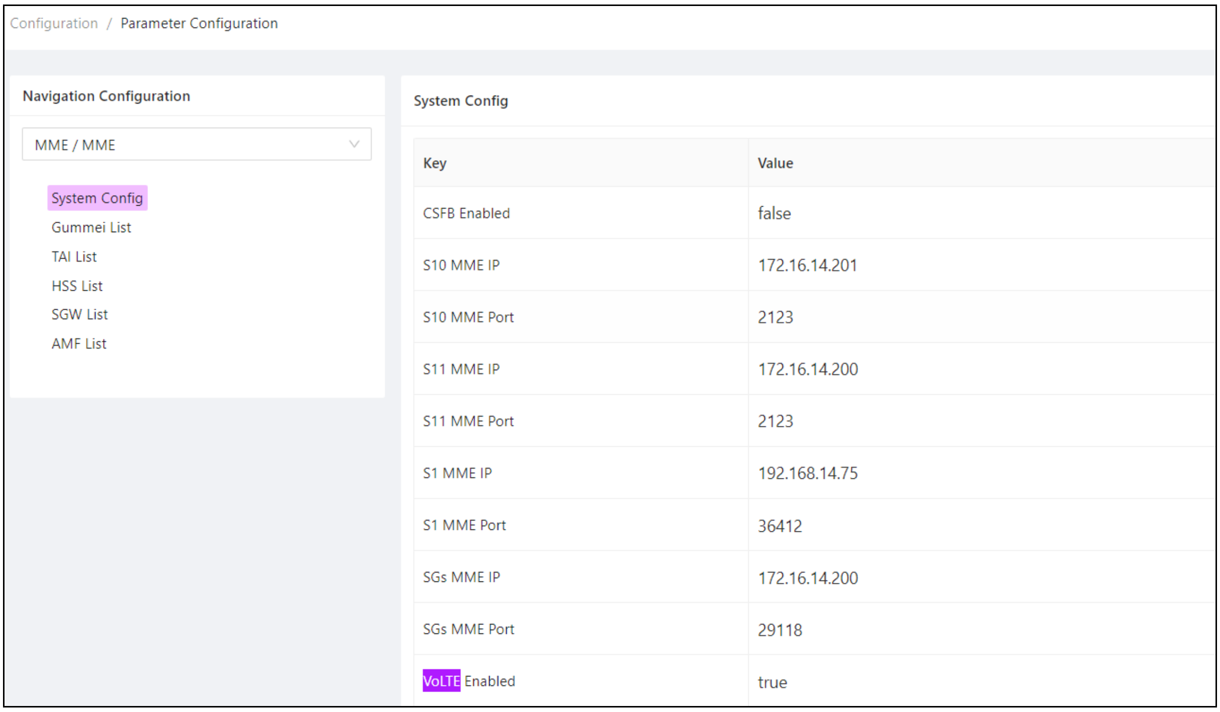
Interface Type	Interface ID	Driver Type	IP Type	IPv4 Address List	IPv6 Ac	Operation
N3	1	vmxnet3	ipv4	commence	co	

Index	IPv4	IPv4 Mask	Operation
1	192.168.14.72	255.255.240.0	

Interface Type	Interface ID	Driver Type	IP Type	IPv4 Address List	IPv6 Ac	Operation
N6	1	vmxnet3	ipv4	commence	co	
N9	1		ipv4	commence	co	
N19	1		ipv4	commence	co	

3.4.4.7 MME

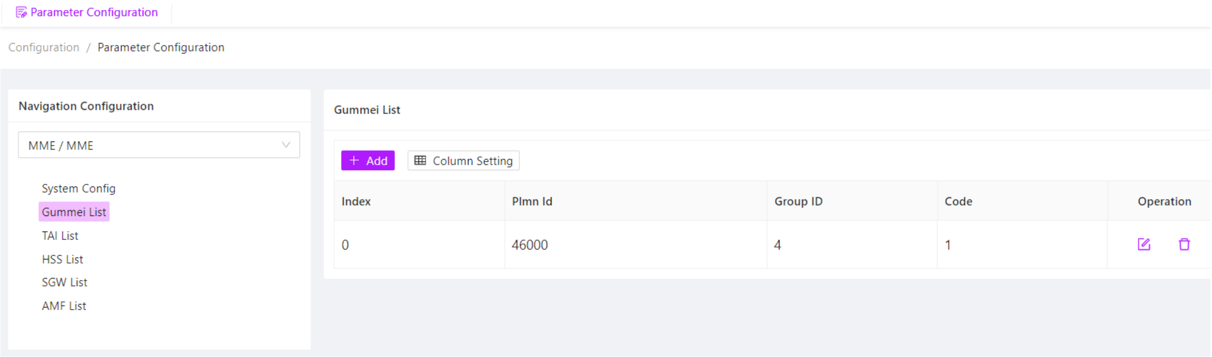
1、**System Config:** The operator mainly configures the IP and ports of S10, S11, S1, SGs, and VoLTE switches can be configured



System Config

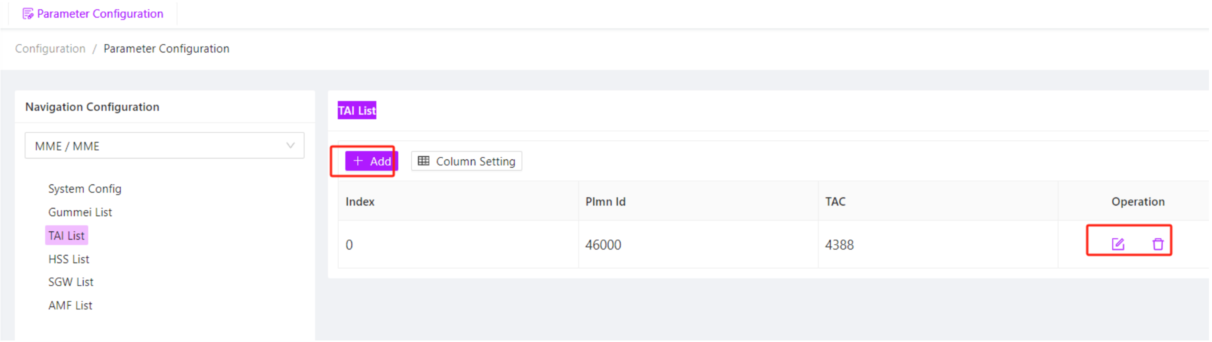
Key	Value
CSFB Enabled	false
S10 MME IP	172.16.14.201
S10 MME Port	2123
S11 MME IP	172.16.14.200
S11 MME Port	2123
S1 MME IP	192.168.14.75
S1 MME Port	36412
SGs MME IP	172.16.14.200
SGs MME Port	29118
VoLTE Enabled	true

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



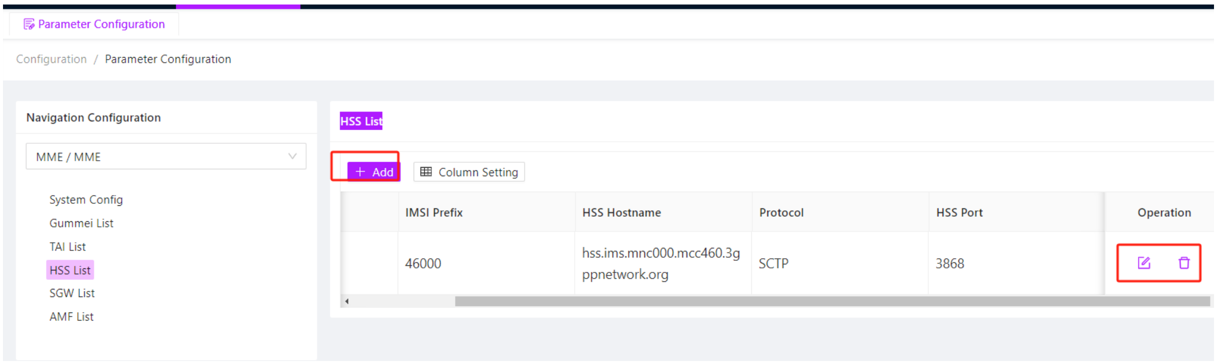
Index	Plmn Id	Group ID	Code	Operation
0	46000	4	1	

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



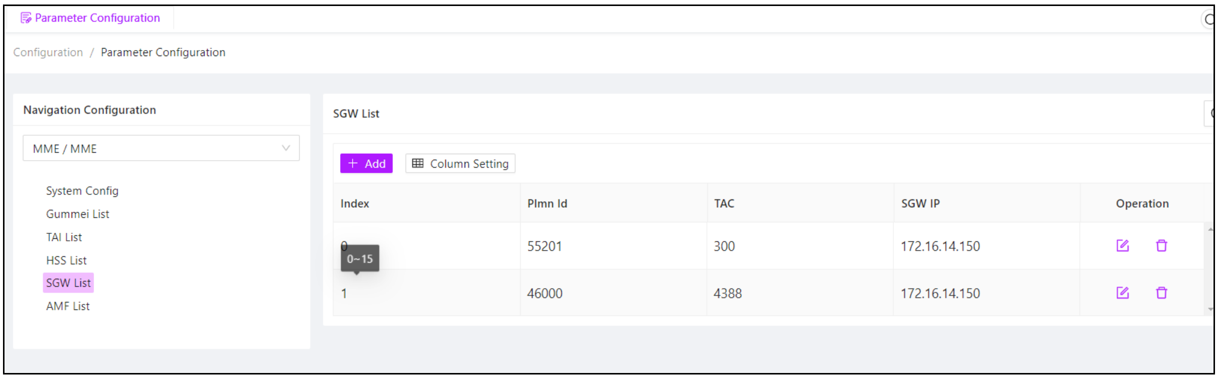
Index	Plmn Id	TAC	Operation
0	46000	4388	

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



IMSI Prefix	HSS Hostname	Protocol	HSS Port	Operation
46000	hss.ims.mnc000.mcc460.3gppnetwork.org	SCTP	3868	

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



Parameter Configuration

Configuration / Parameter Configuration

Navigation Configuration

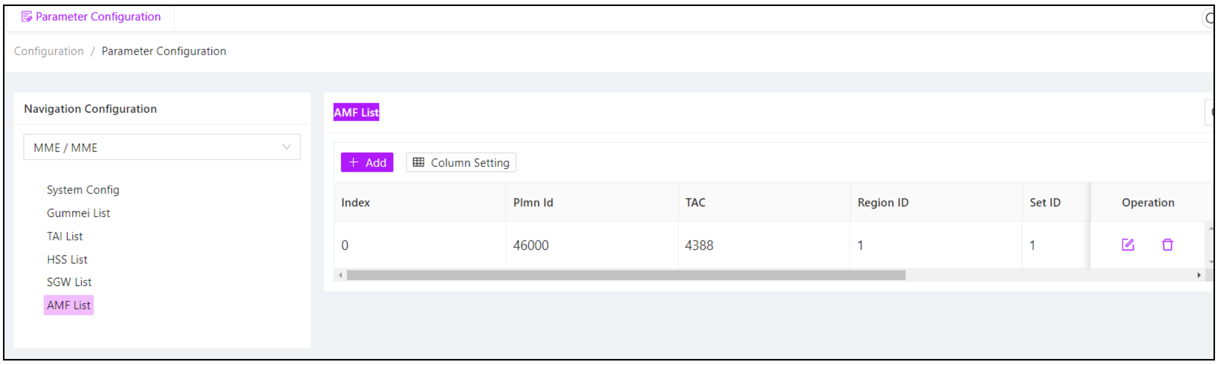
MME / MME

- System Config
- Gummei List
- TAI List
- HSS List
- SGW List
- AMF List

SGW List

Index	Plmn Id	TAC	SGW IP	Operation
0	55201	300	172.16.14.150	
1	46000	4388	172.16.14.150	

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.



Parameter Configuration

Configuration / Parameter Configuration

Navigation Configuration

MME / MME

- System Config
- Gummei List
- TAI List
- HSS List
- SGW List
- AMF List

AMF List

Index	Plmn Id	TAC	Region ID	Set ID	Operation
0	46000	4388	1	1	

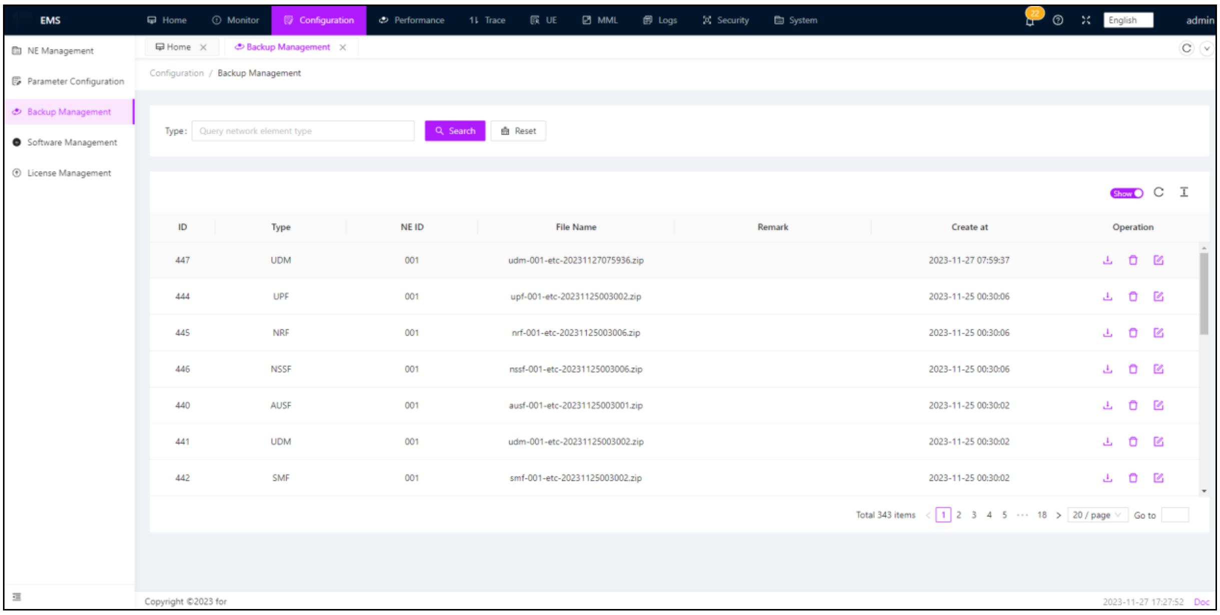
3.4.3 Backup Management

Backup management is to back up and restore NE configuration files. NE backup is very important to provide system redundancy, fault tolerance, and recovery capabilities to ensure high network availability and reliability.

NE backup management usually includes automatic system backup and manual backup:

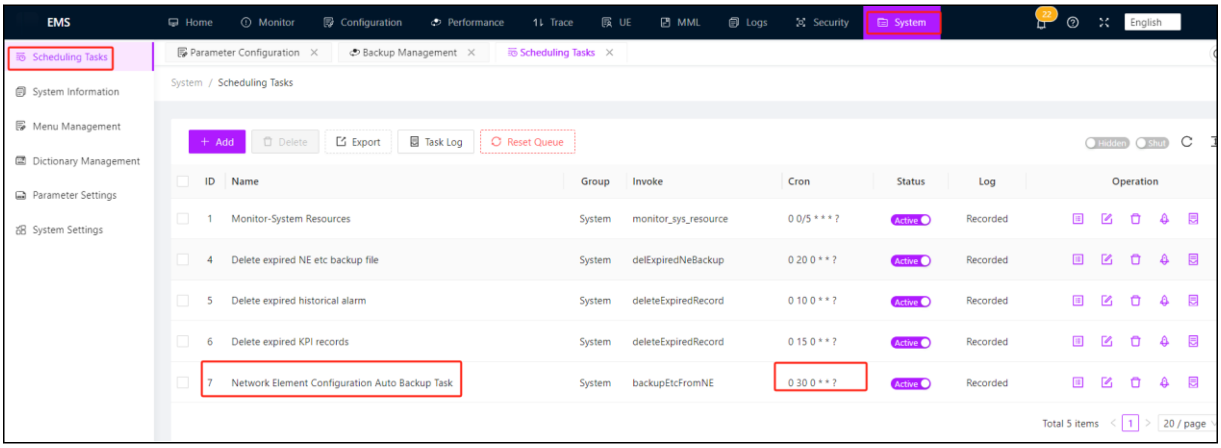
Manual backup: After manual backup, you can export NEs in NE management. The exported configuration file will be displayed in backup management.

Automatic backup: In automatic backup, the system implements automatic backup and schedule management of NE backup. You can configure a backup task under the scheduling task in system configuration. Currently, the configuration file of each NE is backed up at 00:30 every day.



ID	Type	NE ID	File Name	Remark	Create at	Operation
447	UDM	001	udm-001-etc-20231127075936.zip		2023-11-27 07:59:37	
444	UPF	001	upf-001-etc-20231125003002.zip		2023-11-25 00:30:06	
445	NRF	001	nrf-001-etc-20231125003006.zip		2023-11-25 00:30:06	
446	NSSF	001	nssf-001-etc-20231125003006.zip		2023-11-25 00:30:06	
440	AUSF	001	ausf-001-etc-20231125003001.zip		2023-11-25 00:30:02	
441	UDM	001	udm-001-etc-20231125003002.zip		2023-11-25 00:30:02	
442	SMF	001	smf-001-etc-20231125003002.zip		2023-11-25 00:30:02	

Total 343 items < 1 2 3 4 5 ··· 18 > 20 / page Go to



☐	ID	Name	Group	Invoke	Cron	Status	Log	Operation
☐	1	Monitor-System Resources	System	monitor_sys_resource	0 0/5 * * * ?	Active	Recorded	
☐	4	Delete expired NE etc backup file	System	delExpiredNeBackup	0 20 0 * * ?	Active	Recorded	
☐	5	Delete expired historical alarm	System	deleteExpiredRecord	0 10 0 * * ?	Active	Recorded	
☐	6	Delete expired KPI records	System	deleteExpiredRecord	0 15 0 * * ?	Active	Recorded	
☐	7	Network Element Configuration Auto Backup Task	System	backupEtcFromNE	0 30 0 * * ?	Active	Recorded	

Total 5 items < 1 > 20 / page

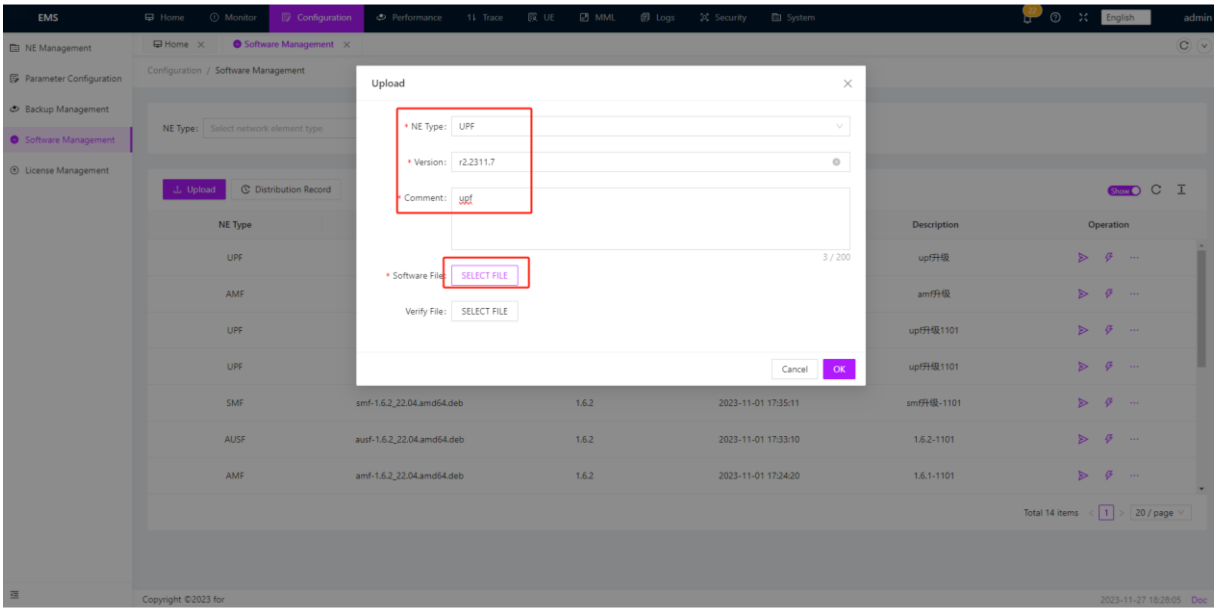
3.4.4 Software Management

Software management is to manage and upgrade the software of each network element in the network, and ensure the stability of the network and the smooth upgrade of functions. In a network, network element upgrades are very important, bringing new features and performance improvements, while also fixing known issues and vulnerabilities. The main functions include:

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

Rollback and downgrade management: If a problem or unexpected situation occurs during the software upgrade, the rollback and downgrade policies must be in place. The corresponding NE can be rolled back

Operation: Upload ->Distribute ->Activate/Rollback



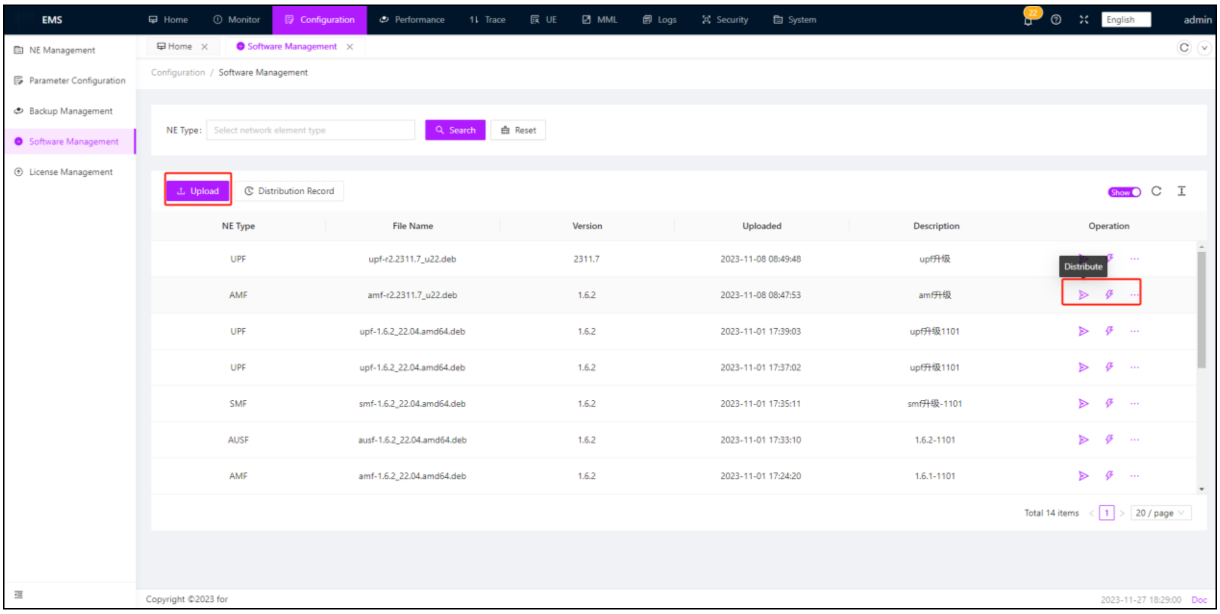
Upload

- * NE Type: UPF
- * Version: r2.2311.7
- * Comment: upf
- 3 / 200
- * Software File: SELECT FILE
- Verify File: SELECT FILE

Cancel OK

NE Type				Description	Operation
UPF				upf升级	
AMF				amf升级	
UPF				upf升级1101	
UPF				upf升级1101	
SMF	smf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:35:11	smf升级-1101	
AUSF	ausf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:33:10	1.6.2-1101	
AMF	amf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:24:20	1.6.1-1101	

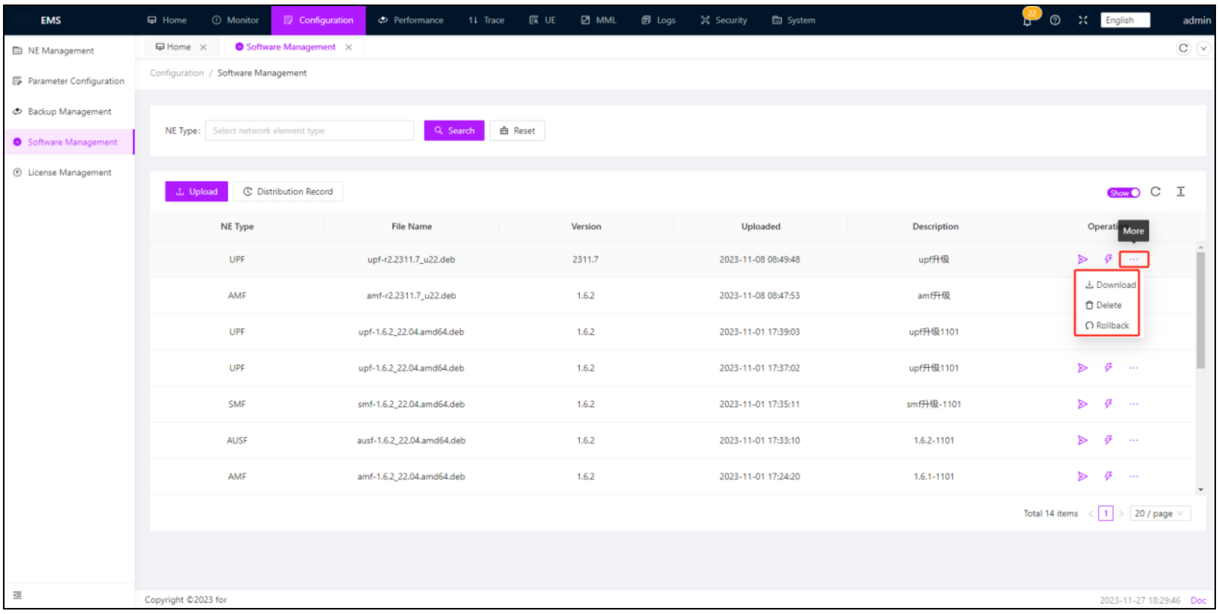
Total 14 items 1 20 / page



NE Type: Select network element type

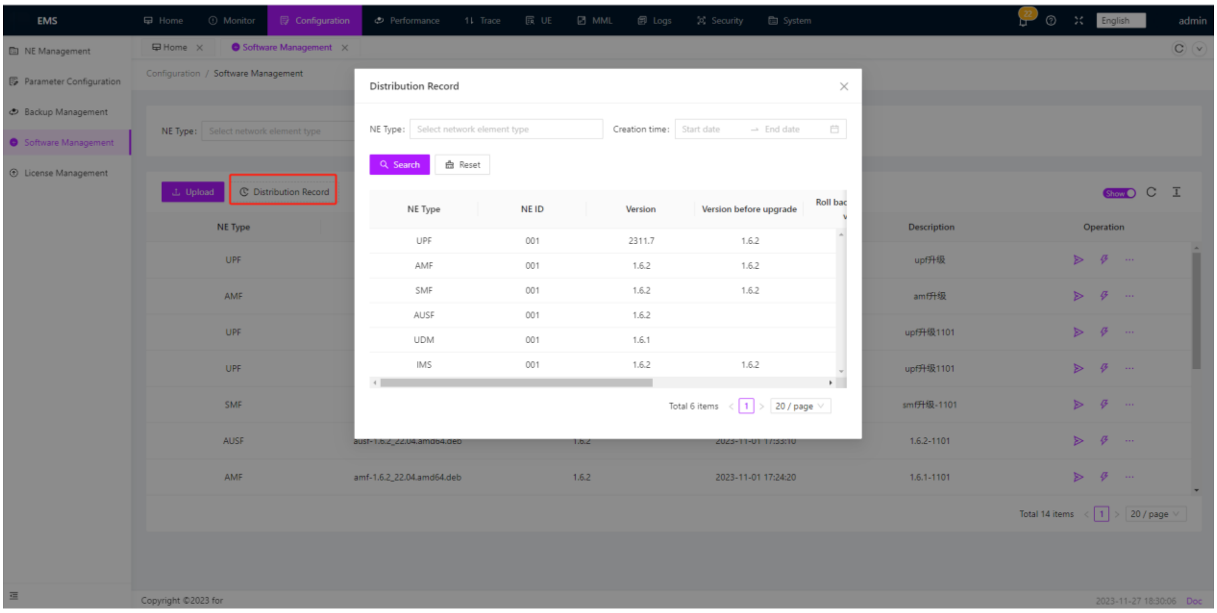
NE Type	File Name	Version	Uploaded	Description	Operation
UPF	upf-r2.2311.7_u22.deb	2311.7	2023-11-08 08:49:48	upf升级	
AMF	amf-r2.2311.7_u22.deb	1.6.2	2023-11-08 08:47:53	amf升级	
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:39:03	upf升级1101	
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:37:02	upf升级1101	
SMF	smf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:35:11	smf升级-1101	
AUSF	ausf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:33:10	1.6.2-1101	
AMF	amf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:24:20	1.6.1-1101	

Total 14 items 1 20 / page



NE Type	File Name	Version	Uploaded	Description	Operation
UPF	upf-r2.2311.7_u22.deb	2311.7	2023-11-08 08:49:48	upf升级	
AMF	amf-r2.2311.7_u22.deb	1.6.2	2023-11-08 08:47:53	amf升级	
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:39:03	upf升级1101	
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:37:02	upf升级1101	
SMF	smf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:35:11	smf升级-1101	
AUSF	ausf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:33:10	1.6.2-1101	
AMF	amf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:24:20	1.6.1-1101	

Can view the distribution records of each network element



NE Type	NE ID	Version	Version before upgrade	Roll bac v
UPF	001	2311.7	1.6.2	
AMF	001	1.6.2	1.6.2	
SMF	001	1.6.2	1.6.2	
AUSF	001	1.6.2		
UDM	001	1.6.1		
IMS	001	1.6.2	1.6.2	

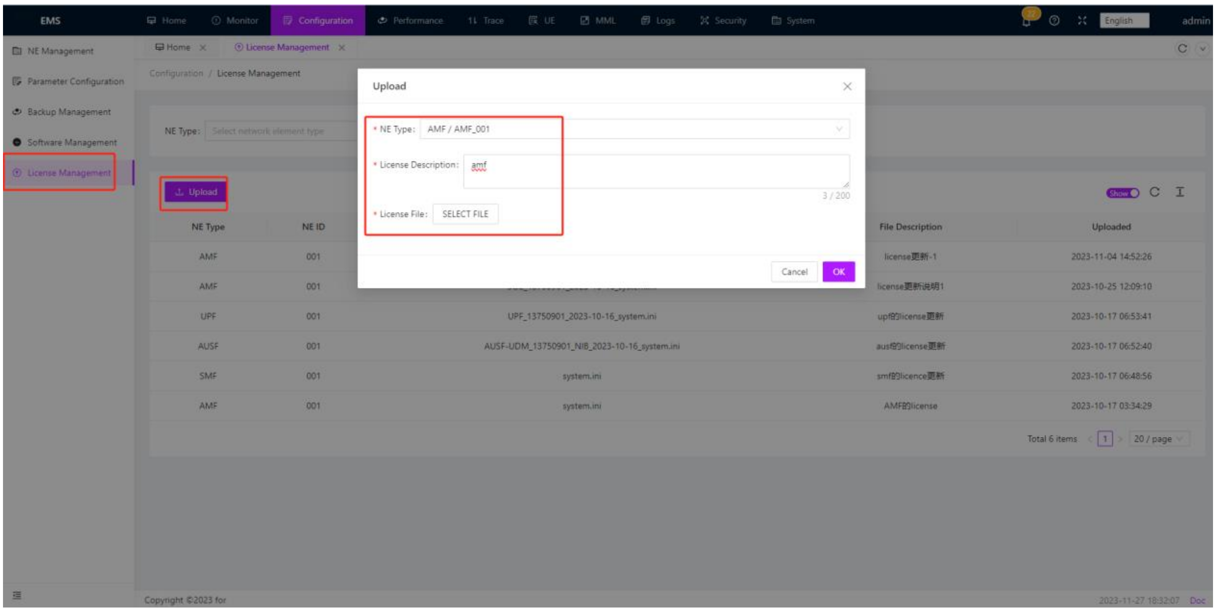
3.4.5 License Management

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.



Upload

* NE Type: AMF / AMF_001

* License Description: amf

3 / 200

* License File: SELECT FILE

NE Type	NE ID		File Description	Uploaded
AMF	001		license更新-1	2023-11-04 14:52:26
AMF	001	[illegible]	license更新说明1	2023-10-25 12:09:10
UPF	001	UPF_13750901_2023-10-16_system.ini	upf的license更新	2023-10-17 06:53:41
AUSF	001	AUSF-UDM_13750901_NIB_2023-10-16_system.ini	ausf的license更新	2023-10-17 06:52:40
SMF	001	system.ini	smf的licence更新	2023-10-17 06:48:56
AMF	001	system.ini	AMF的license	2023-10-17 03:34:29

Total 6 items 1 20 / page

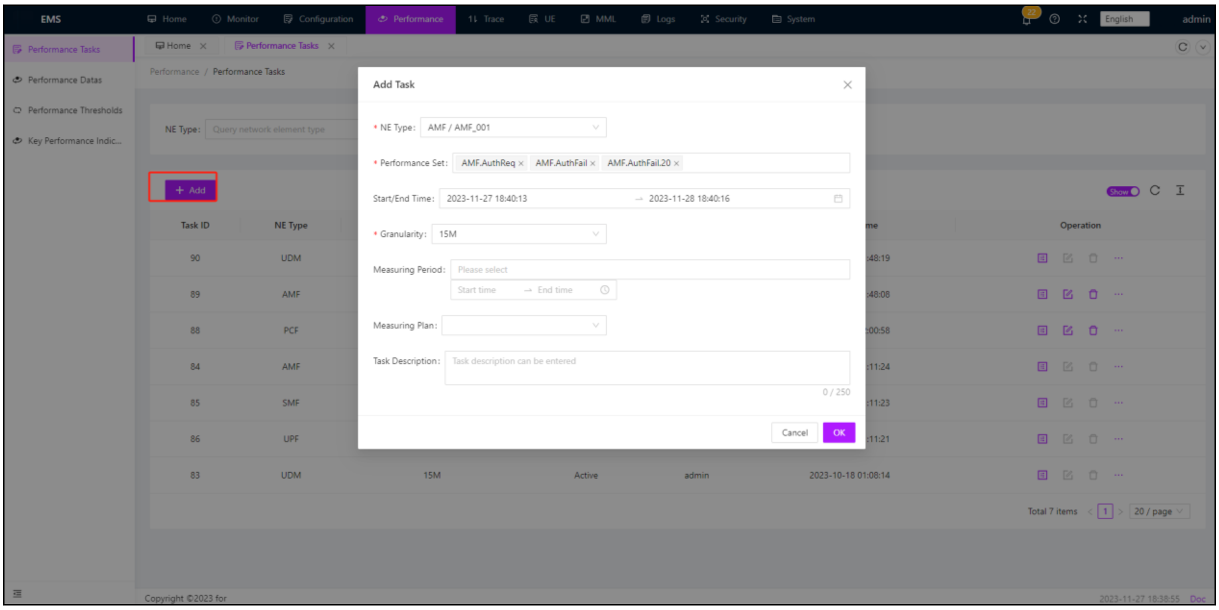
3.5 Performance

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.



Add Task

* NE Type: AMF / AMF_001

* Performance Set: AMF.AuthReq × AMF.AuthFail × AMF.AuthFail.20 ×

Start/End Time: 2023-11-27 18:40:13 → 2023-11-28 18:40:16

* Granularity: 15M

Measuring Period: Please select

Start time → End time

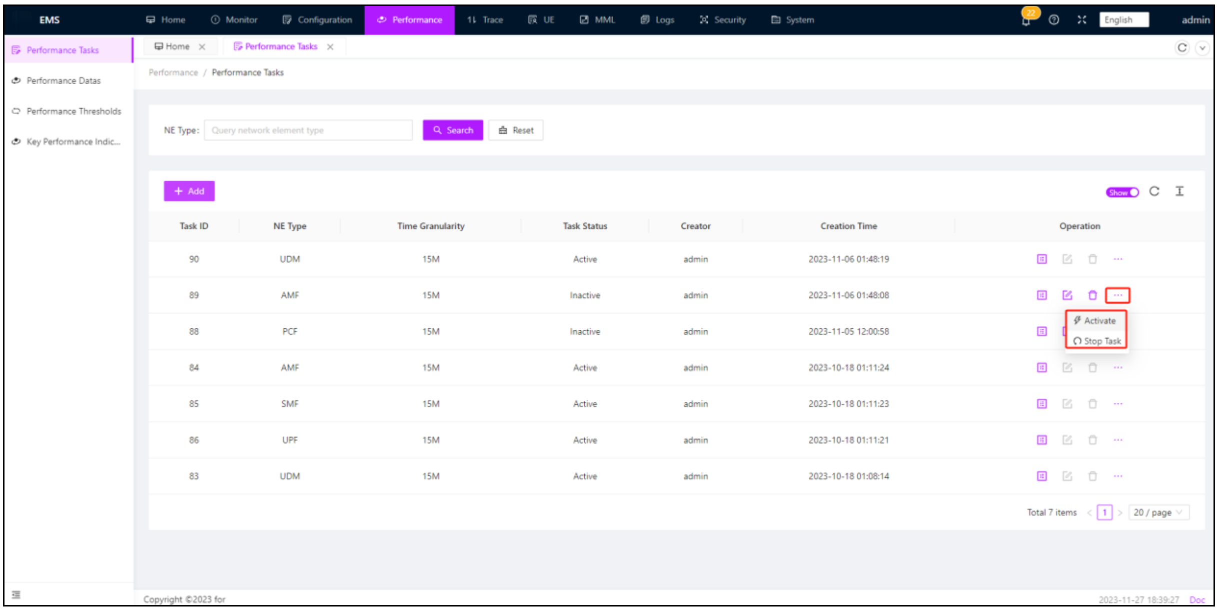
Measuring Plan:

Task Description: Task description can be entered

0 / 250

Cancel OK

Copyright ©2023 for

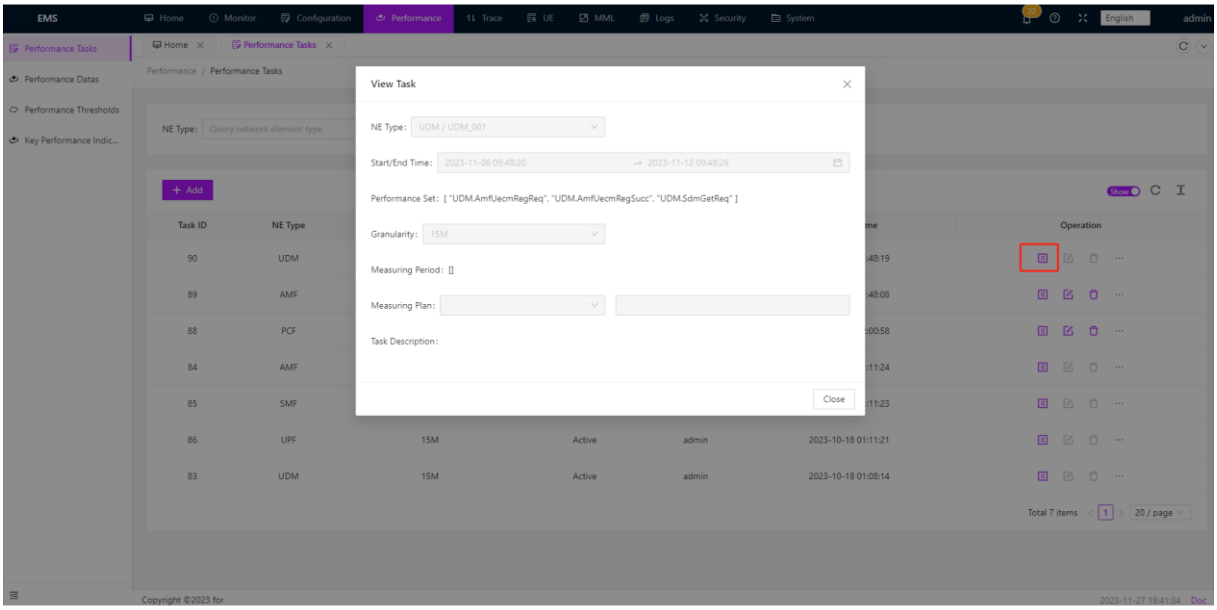


NE Type: Query network element type

Task ID	NE Type	Time Granularity	Task Status	Creator	Creation Time	Operation
90	UDM	15M	Active	admin	2023-11-06 01:48:19	
89	AMF	15M	Inactive	admin	2023-11-06 01:48:08	
88	PCF	15M	Inactive	admin	2023-11-05 12:00:58	
84	AMF	15M	Active	admin	2023-10-18 01:11:24	
85	SMF	15M	Active	admin	2023-10-18 01:11:23	
86	UPF	15M	Active	admin	2023-10-18 01:11:21	
83	UDM	15M	Active	admin	2023-10-18 01:08:14	

Total 7 items 1 20 / page

Copyright ©2023 for 2023-11-27 18:39:27 Doc



View Task

NE Type: UDM / UDM_001

Start/End Time: 2023-11-06 09:48:20 → 2023-11-12 09:48:26

Performance Set: ["UDM.AmfUecmRegReq", "UDM.AmfUecmRegSucc", "UDM.SdmGetReq"]

Granularity: 15M

Measuring Period: []

Measuring Plan:

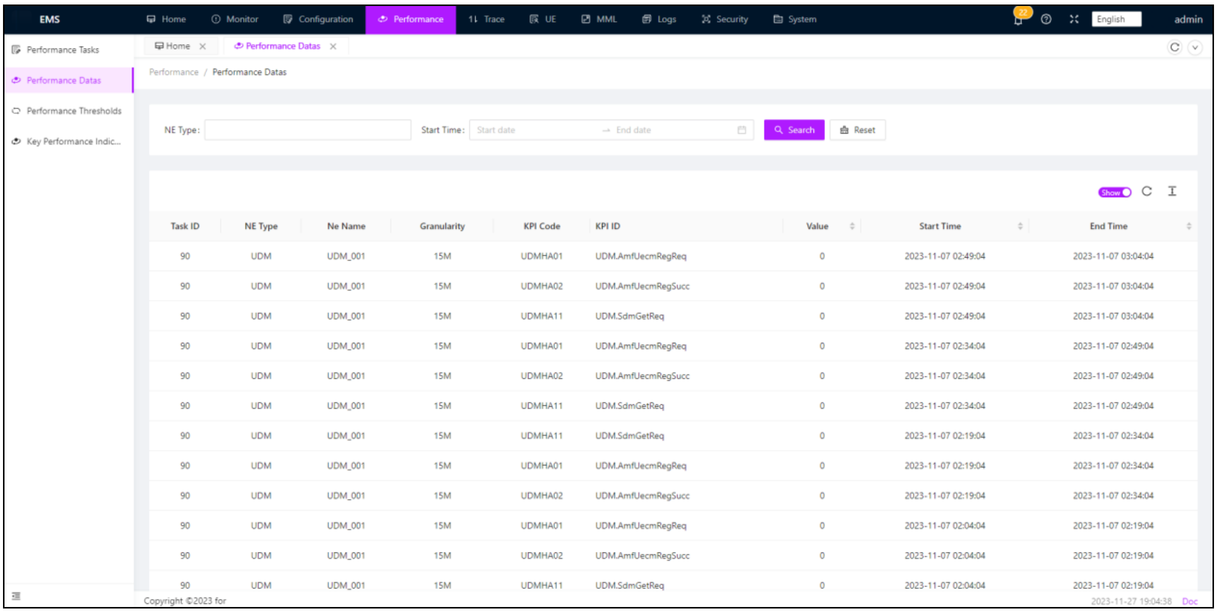
Task Description:

Close

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:



NE Type:

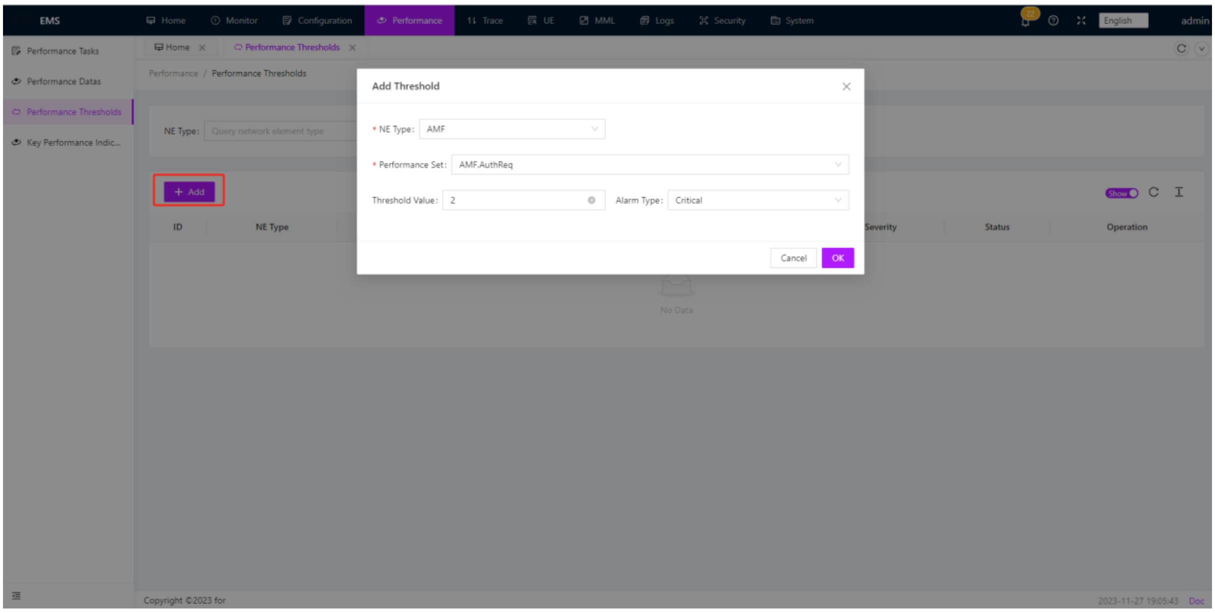
Start Time: Start date → End date

Task ID	NE Type	Ne Name	Granularity	KPI Code	KPI ID	Value	Start Time	End Time
90	UDM	UDM_001	15M	UDMHA01	UDM.AmfUecmRegReq	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDMHA02	UDM.AmfUecmRegSucc	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDMHA11	UDM.SdmGetReq	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDMHA01	UDM.AmfUecmRegReq	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDMHA02	UDM.AmfUecmRegSucc	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDMHA11	UDM.SdmGetReq	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDMHA11	UDM.SdmGetReq	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDMHA01	UDM.AmfUecmRegReq	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDMHA02	UDM.AmfUecmRegSucc	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDMHA01	UDM.AmfUecmRegReq	0	2023-11-07 02:04:04	2023-11-07 02:19:04
90	UDM	UDM_001	15M	UDMHA02	UDM.AmfUecmRegSucc	0	2023-11-07 02:04:04	2023-11-07 02:19:04
90	UDM	UDM_001	15M	UDMHA11	UDM.SdmGetReq	0	2023-11-07 02:04:04	2023-11-07 02:19:04

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



Add Threshold

* NE Type: AMF

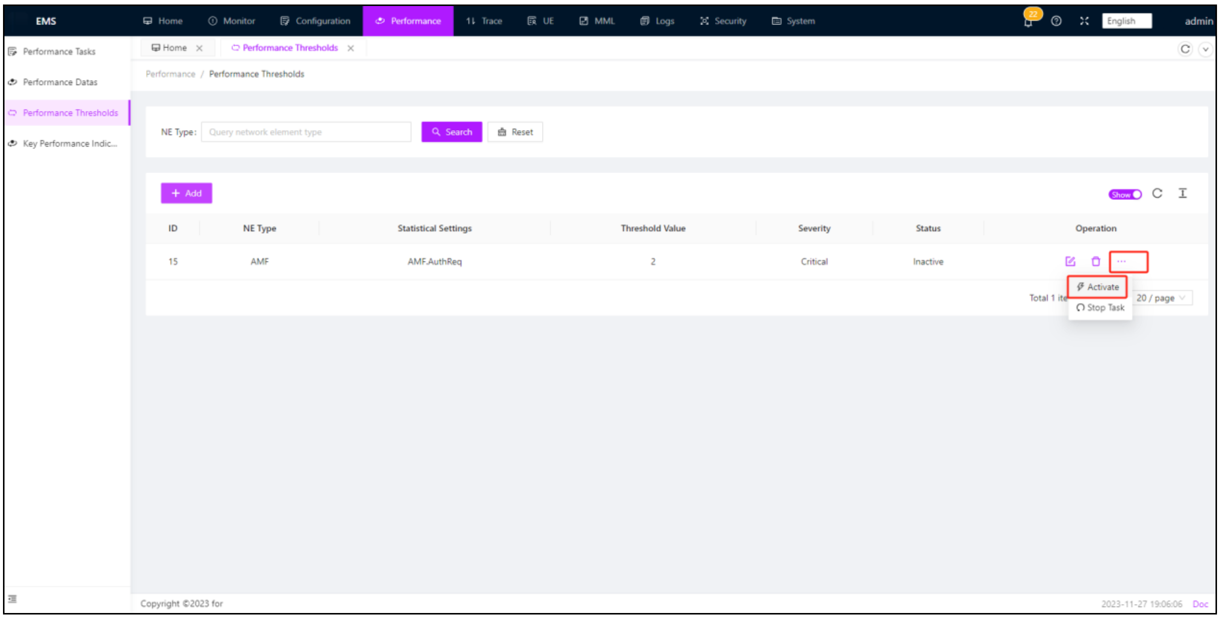
* Performance Set: AMF.AuthReq

Threshold Value: 2

Alarm Type: Critical

Cancel OK

Activate after successfully adding tasks

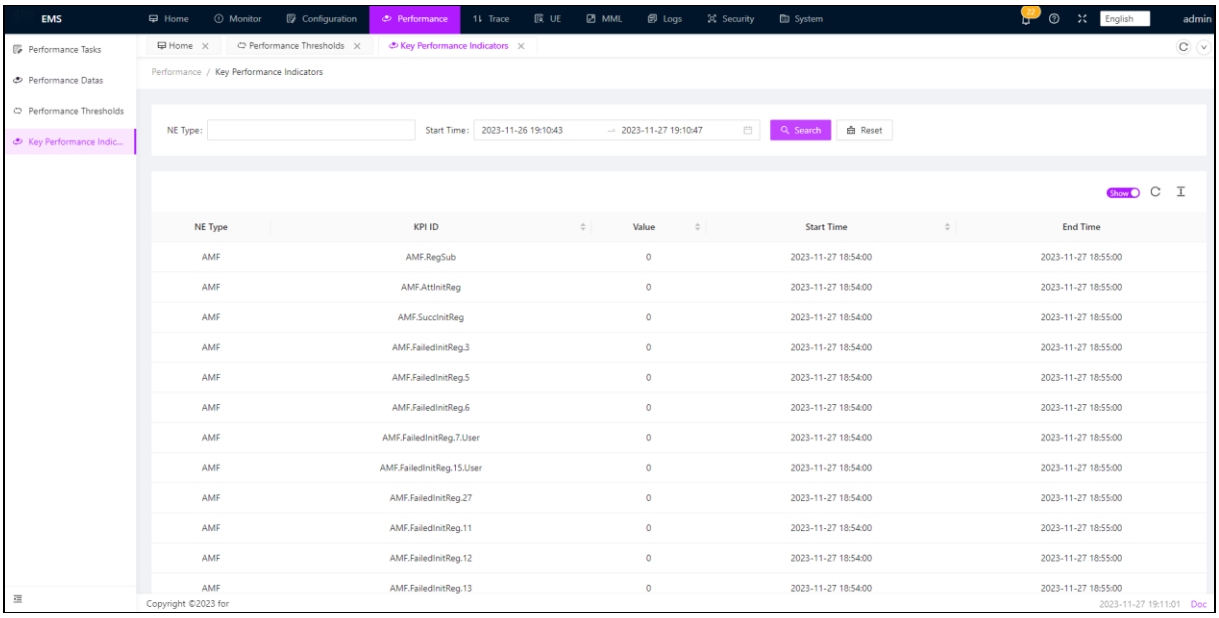


NE Type: Query network element type

ID	NE Type	Statistical Settings	Threshold Value	Severity	Status	Operation
15	AMF	AMF.AuthReq	2	Critical	Inactive	

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.



NE Type:

Start Time: 2023-11-26 19:10:43 → 2023-11-27 19:10:47

NE Type	KPI ID	Value	Start Time	End Time
AMF	AMF.RegSub	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.AttInitReg	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.SuccInitReg	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.3	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.5	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.6	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.7.User	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.15.User	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.27	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.11	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.12	0	2023-11-27 18:54:00	2023-11-27 18:55:00
AMF	AMF.FailedInitReg.13	0	2023-11-27 18:54:00	2023-11-27 18:55:00

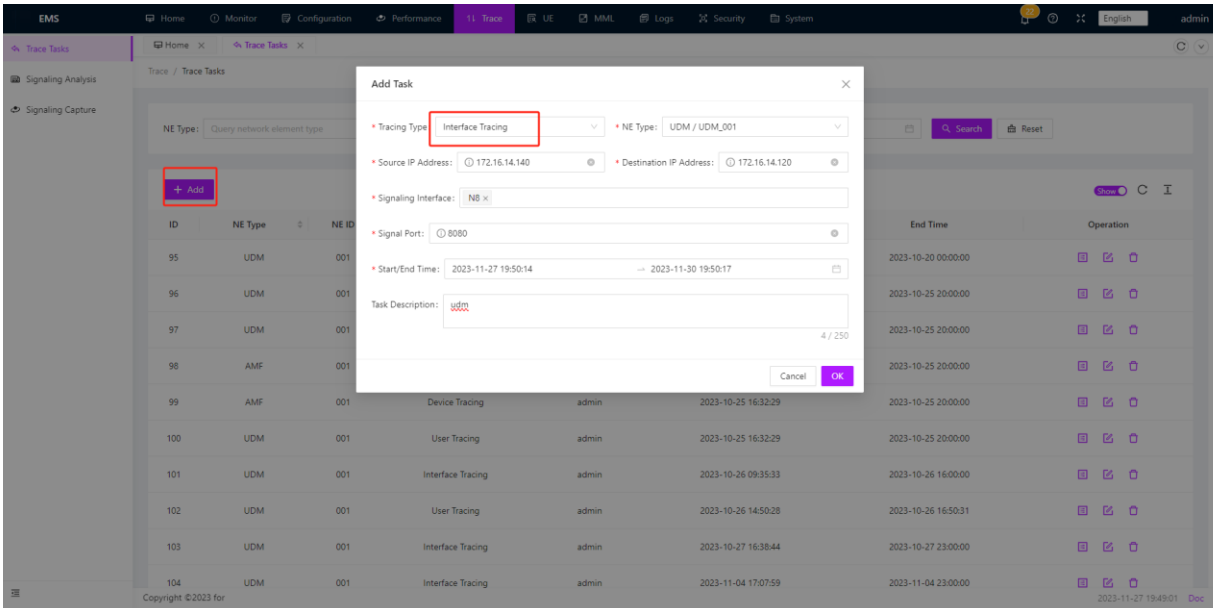
3.6 Trace

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：



Add Task

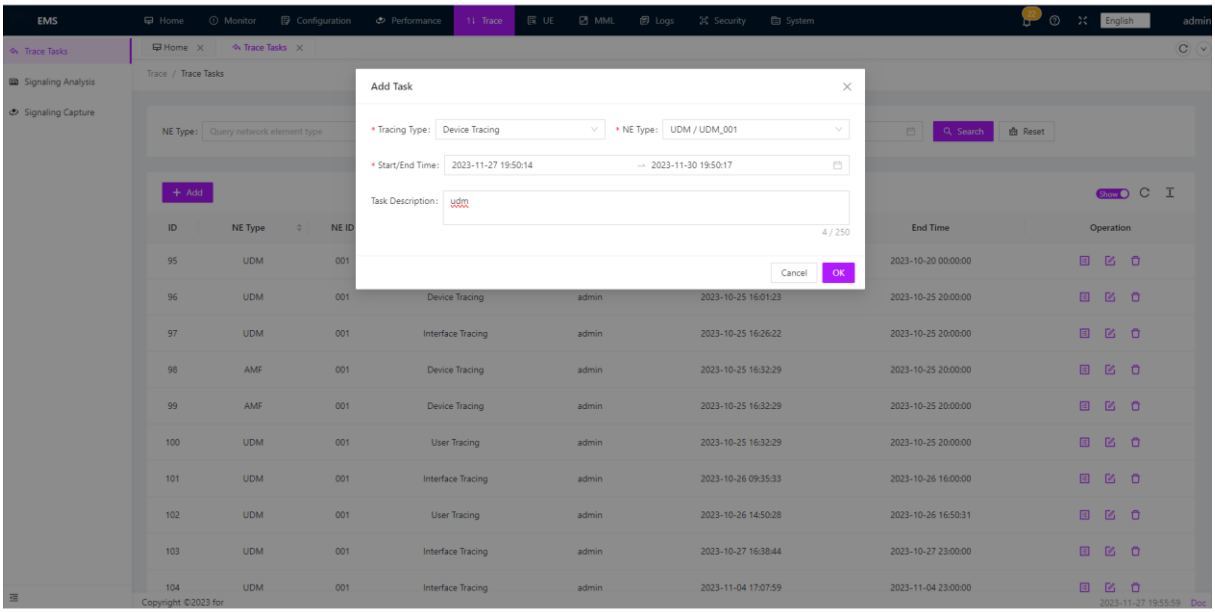
- * Tracing Type: Interface Tracing
- * NE Type: UDM / UDM_001
- * Source IP Address: 172.16.14.140
- * Destination IP Address: 172.16.14.120
- * Signaling Interface: N8 ×
- * Signal Port: 8080
- * Start/End Time: 2023-11-27 19:50:14 → 2023-11-30 19:50:17
- Task Description: udm

4 / 250

Cancel OK

ID	NE Type	NE ID				End Time	Operation
95	UDM	001				2023-10-20 00:00:00	
96	UDM	001				2023-10-25 20:00:00	
97	UDM	001				2023-10-25 20:00:00	
98	AMF	001				2023-10-25 20:00:00	
99	AMF	001	Device Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
100	UDM	001	User Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
101	UDM	001	Interface Tracing	admin	2023-10-26 09:35:33	2023-10-26 16:00:00	
102	UDM	001	User Tracing	admin	2023-10-26 14:50:28	2023-10-26 16:50:31	
103	UDM	001	Interface Tracing	admin	2023-10-27 16:38:44	2023-10-27 23:00:00	
104	UDM	001	Interface Tracing	admin	2023-11-04 17:07:59	2023-11-04 23:00:00	

Device Tracing:



NE Type: Query network element type

Add Task

* Tracing Type: Device Tracing

* NE Type: UDM / UDM_001

* Start/End Time: 2023-11-27 19:50:14 → 2023-11-30 19:50:17

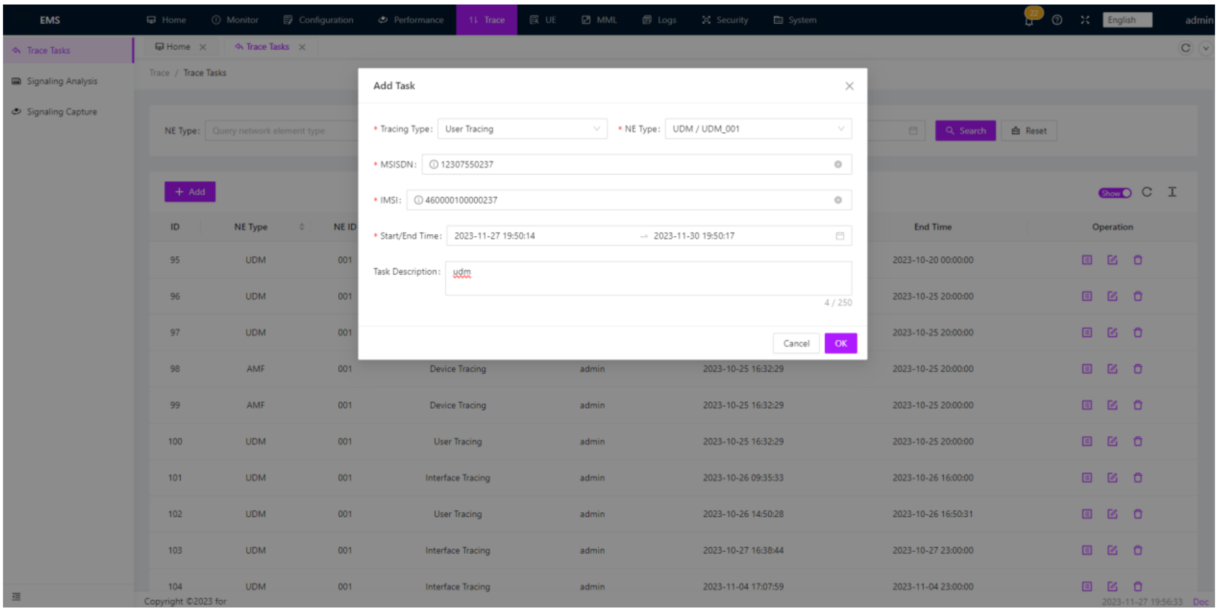
Task Description: udm

4 / 250

Cancel OK

ID	NE Type	NE ID				End Time	Operation
95	UDM	001				2023-10-20 00:00:00	
96	UDM	001	Device Tracing	admin	2023-10-25 16:01:23	2023-10-25 20:00:00	
97	UDM	001	Interface Tracing	admin	2023-10-25 16:26:22	2023-10-25 20:00:00	
98	AMF	001	Device Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
99	AMF	001	Device Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
100	UDM	001	User Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
101	UDM	001	Interface Tracing	admin	2023-10-26 09:35:33	2023-10-26 16:00:00	
102	UDM	001	User Tracing	admin	2023-10-26 14:50:28	2023-10-26 16:50:31	
103	UDM	001	Interface Tracing	admin	2023-10-27 16:38:44	2023-10-27 23:00:00	
104	UDM	001	Interface Tracing	admin	2023-11-04 17:07:59	2023-11-04 23:00:00	

User Tracing:



NE Type: Query network element type

Add Task

* Tracing Type: User Tracing

* NE Type: UDM / UDM_001

* MSISDN: 12307550237

* IMSI: 460000100000237

* Start/End Time: 2023-11-27 19:50:14 → 2023-11-30 19:50:17

Task Description: udm

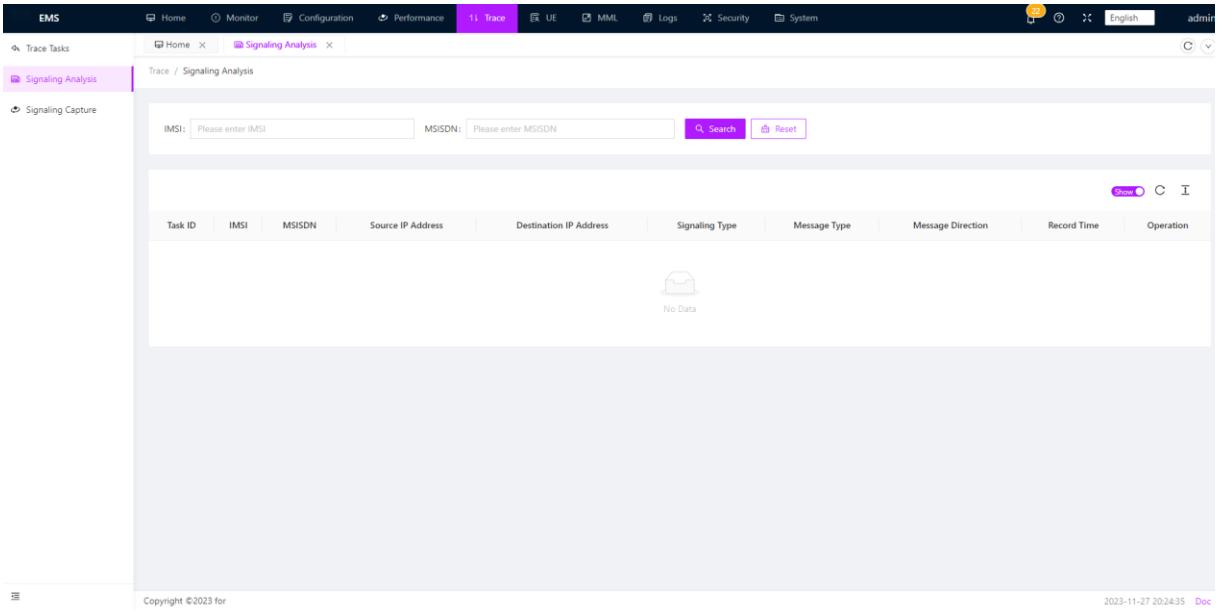
4 / 250

Cancel OK

ID	NE Type	NE ID				End Time	Operation
95	UDM	001				2023-10-20 00:00:00	
96	UDM	001				2023-10-25 20:00:00	
97	UDM	001				2023-10-25 20:00:00	
98	AMF	001	Device Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
99	AMF	001	Device Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
100	UDM	001	User Tracing	admin	2023-10-25 16:32:29	2023-10-25 20:00:00	
101	UDM	001	Interface Tracing	admin	2023-10-26 09:35:33	2023-10-26 16:00:00	
102	UDM	001	User Tracing	admin	2023-10-26 14:50:28	2023-10-26 16:50:31	
103	UDM	001	Interface Tracing	admin	2023-10-27 16:38:44	2023-10-27 23:00:00	
104	UDM	001	Interface Tracing	admin	2023-11-04 17:07:59	2023-11-04 23:00:00	

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)



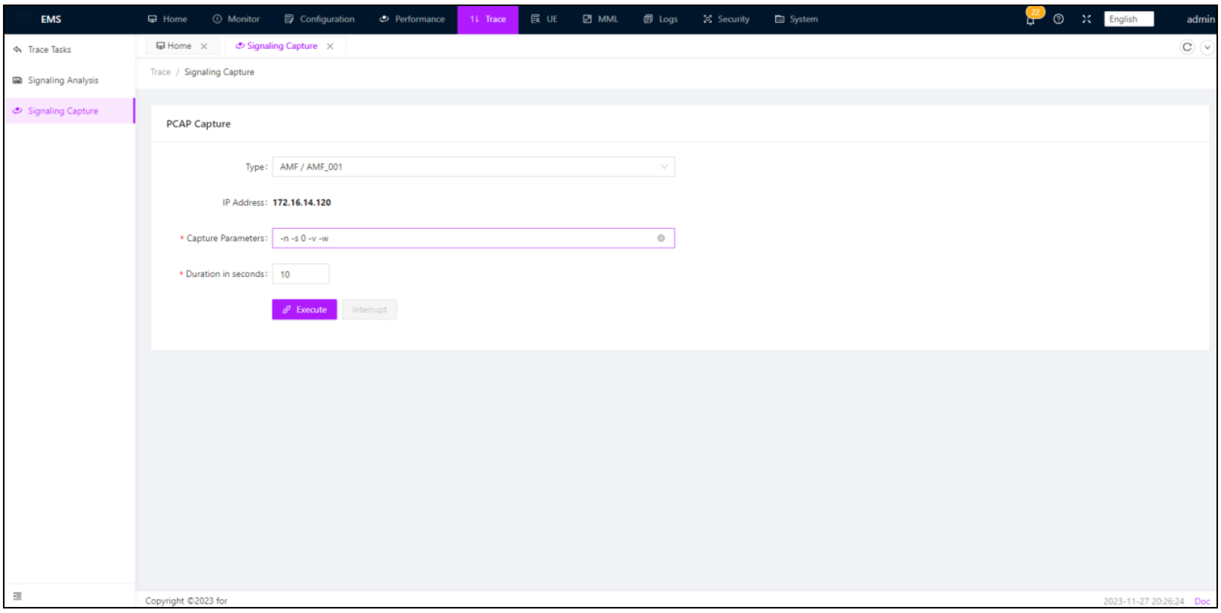
IMSI: Please enter IMSI MSISDN: Please enter MSISDN

Task ID	IMSI	MSISDN	Source IP Address	Destination IP Address	Signaling Type	Message Type	Message Direction	Record Time	Operation

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.



PCAP Capture

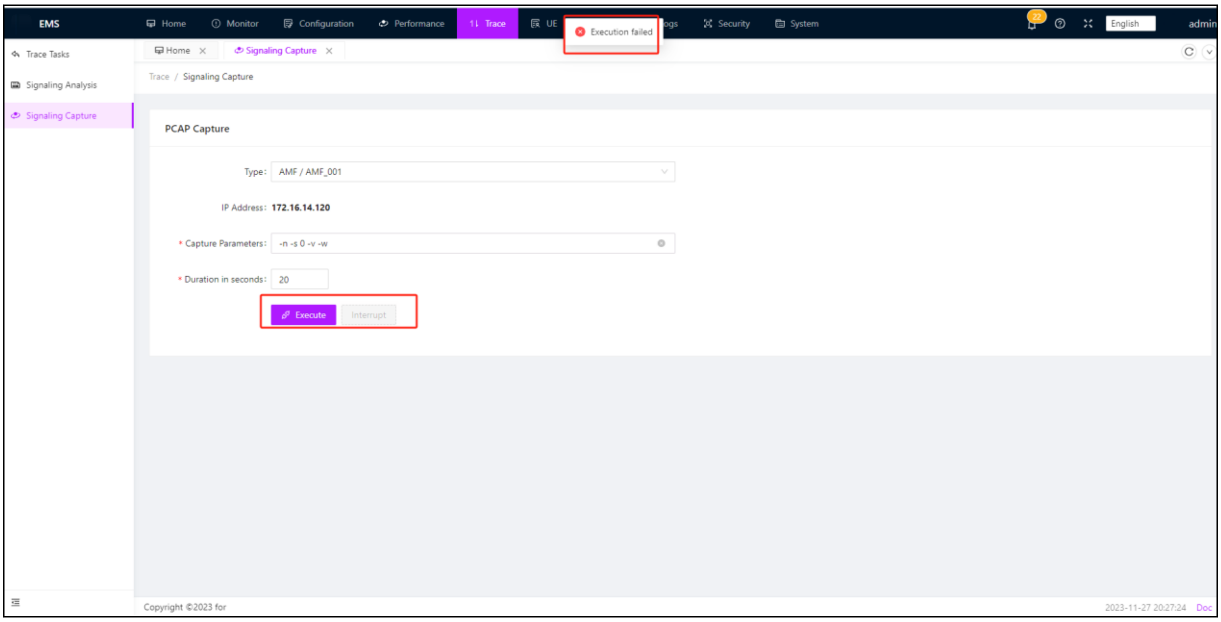
Type: AMF / AMF_001

IP Address: 172.16.14.120

* Capture Parameters: -n -s 0 -v -w

* Duration in seconds: 10

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



PCAP Capture

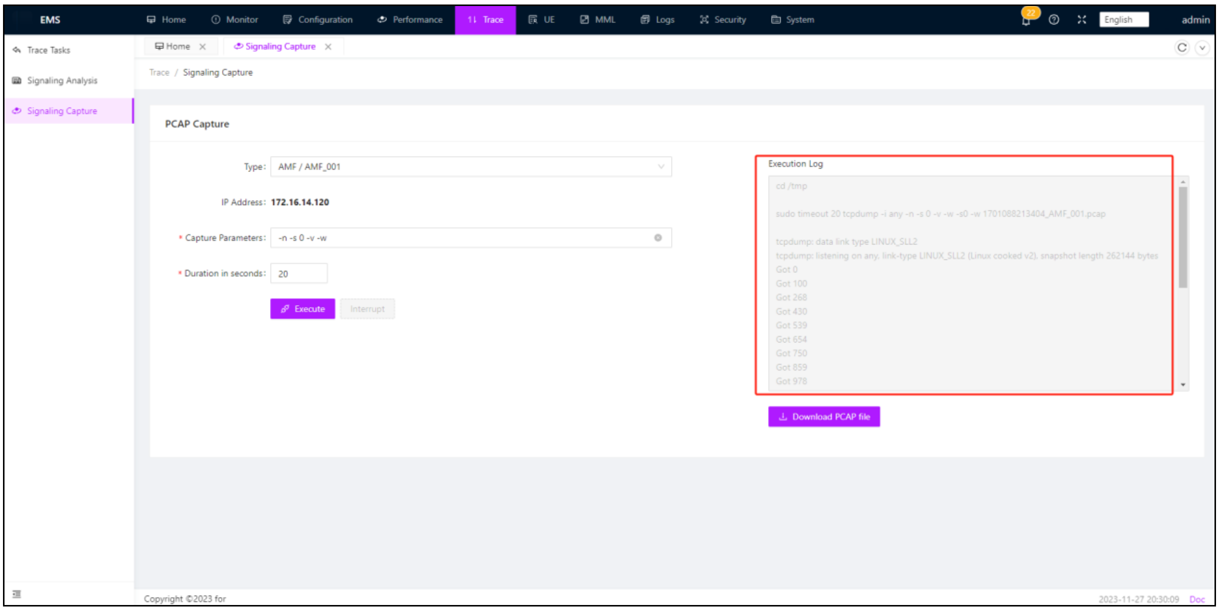
Type: AMF / AMF_001

IP Address: 172.16.14.120

* Capture Parameters: -n -s 0 -v -w

* Duration in seconds: 20

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.



PCAP Capture

Type: AMF / AMF_001

IP Address: 172.16.14.120

* Capture Parameters: -n -s 0 -v -w

* Duration in seconds: 20

Execution Log

```
cd /tmp

sudo timeout 20 tcpdump -i any -n -s 0 -v -w -s0 -w 1701088213404_AMF_001.pcap

tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
Got 0
Got 100
Got 268
Got 430
Got 539
Got 654
Got 750
Got 859
Got 978
```

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

3.7 UE

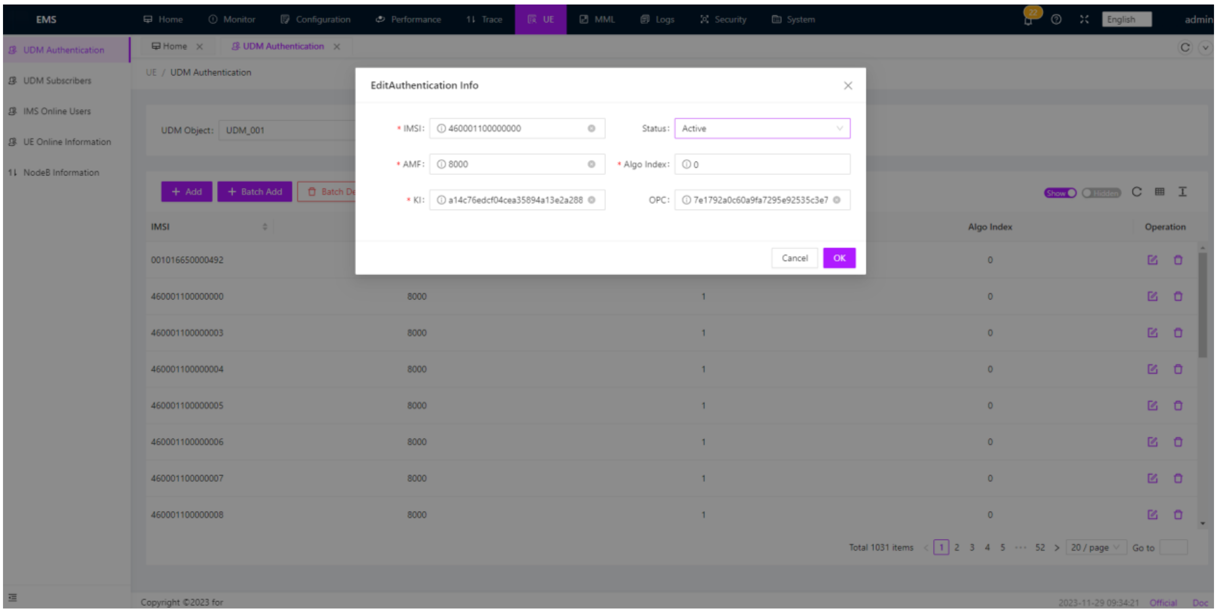
Core network terminal management refers to the management and control of terminal devices in the core network to ensure the security and smooth operation of the network. The core network terminal management includes the UDM authentication and UDM subscribers in the User data management (UDM), and the 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 Object: UDM_001

EditAuthentication Info

* IMSI: 460001100000000
Status: Active
* AMF: 8000
* Algo Index: 0
* KI: a14c76edcf04cea35894a13e2a288
OPC: 7e1792a0c60a9fa7295e92535c3e7

Cancel OK

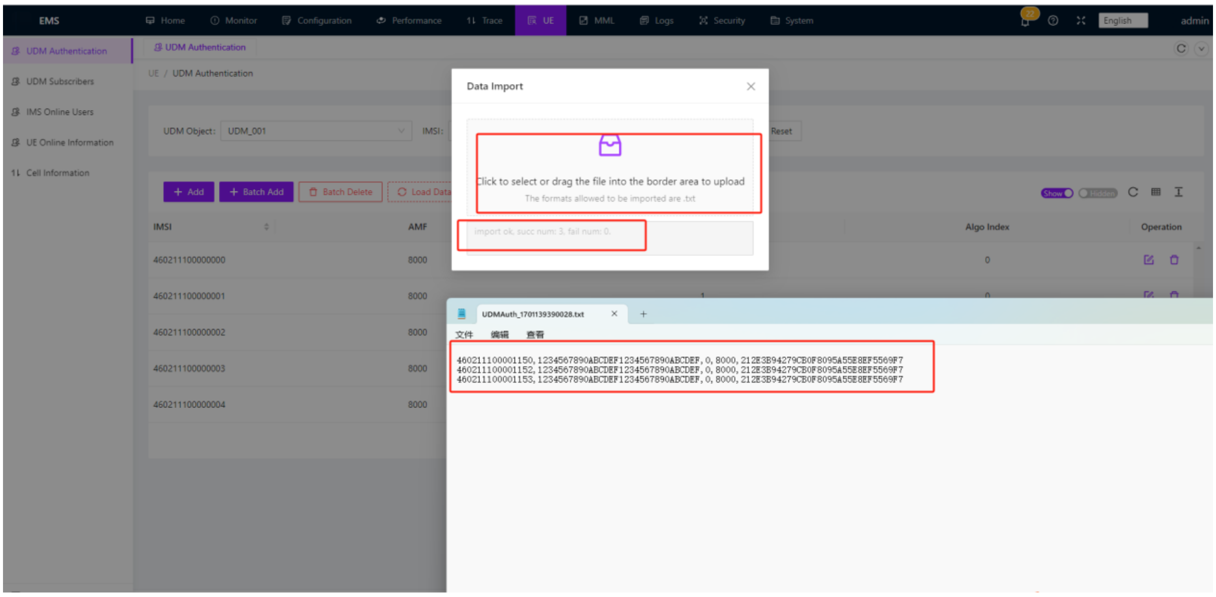
IMSI			Algo Index	Operation
001016650000492			0	✎ 🗑
460001100000000	8000	1	0	✎ 🗑
460001100000003	8000	1	0	✎ 🗑
460001100000004	8000	1	0	✎ 🗑
460001100000005	8000	1	0	✎ 🗑
460001100000006	8000	1	0	✎ 🗑
460001100000007	8000	1	0	✎ 🗑
460001100000008	8000	1	0	✎ 🗑

Total 1031 items < 1 2 3 4 5 ··· 52 > 20 / page Go to

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.



Click to select or drag the file into the border area to upload

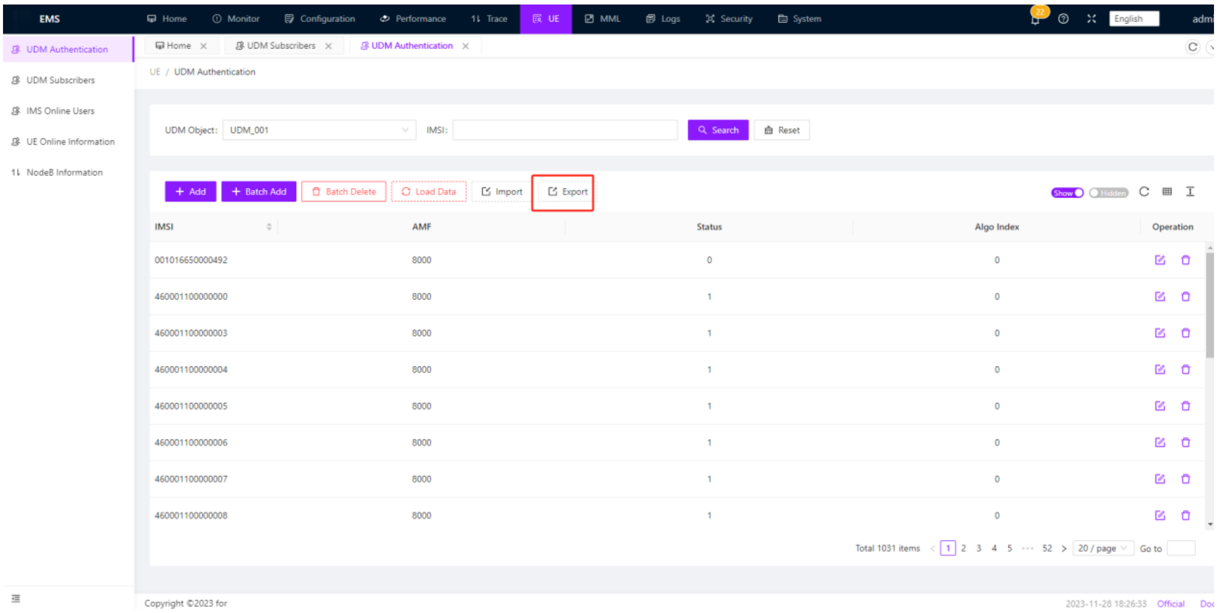
The formats allowed to be imported are .txt

import ok, succ num: 3, fail num: 0.

IMSI	AMF	Algo Index	Operation
460211100000000	8000	0	
460211100000001	8000	0	
460211100000002	8000		
460211100000003	8000		
460211100000004	8000		

```
460211100001150, 1234567890ABCDEF1234567890ABCDEF, 0, 8000, 212E3B94279CB0F8095A55E8EF5569F7
460211100001152, 1234567890ABCDEF1234567890ABCDEF, 0, 8000, 212E3B94279CB0F8095A55E8EF5569F7
460211100001153, 1234567890ABCDEF1234567890ABCDEF, 0, 8000, 212E3B94279CB0F8095A55E8EF5569F7
```

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



UDM Object: UDM_001

IMSI:

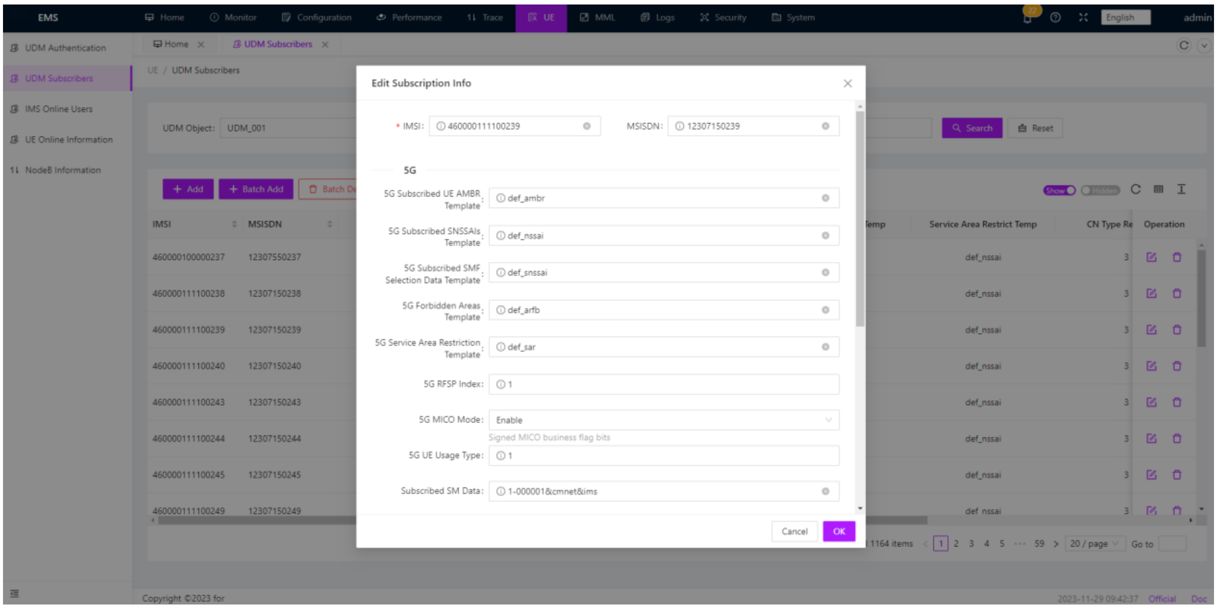
IMSI	AMF	Status	Algo Index	Operation
001016650000492	8000	0	0	
460001100000000	8000	1	0	
460001100000003	8000	1	0	
460001100000004	8000	1	0	
460001100000005	8000	1	0	
460001100000006	8000	1	0	
460001100000007	8000	1	0	
460001100000008	8000	1	0	

Total 1031 items < 1 2 3 4 5 ··· 52 > 20 / page Go to

3.7.2 UDM Subscribers

The UDM Subscribers is the user information of terminal devices stored in the User Data management (UDM). These data include the user's IMSI, MSISDN, SM-DATA, 4G static IP, 4G Context LIST, etc., for the core network to identify users and service management. The core network terminal management can add, modify and delete the user data, single or batch, to ensure the integrity and update of user information.

- Click on the right edit button to view more detailed user data and make modifications, such as modifying static IP data.



Edit Subscription Info

* IMSI: 460000111100239   MSISDN: 12307150239

5G

5G Subscribed UE AMBR Template: def_ambr

5G Subscribed SNSSAIs Template: def_nssai

5G Subscribed SMF Selection Data Template: def_snssai

5G Forbidden Areas Template: def_arfb

5G Service Area Restriction Template: def_sar

5G RFSP Index: 1

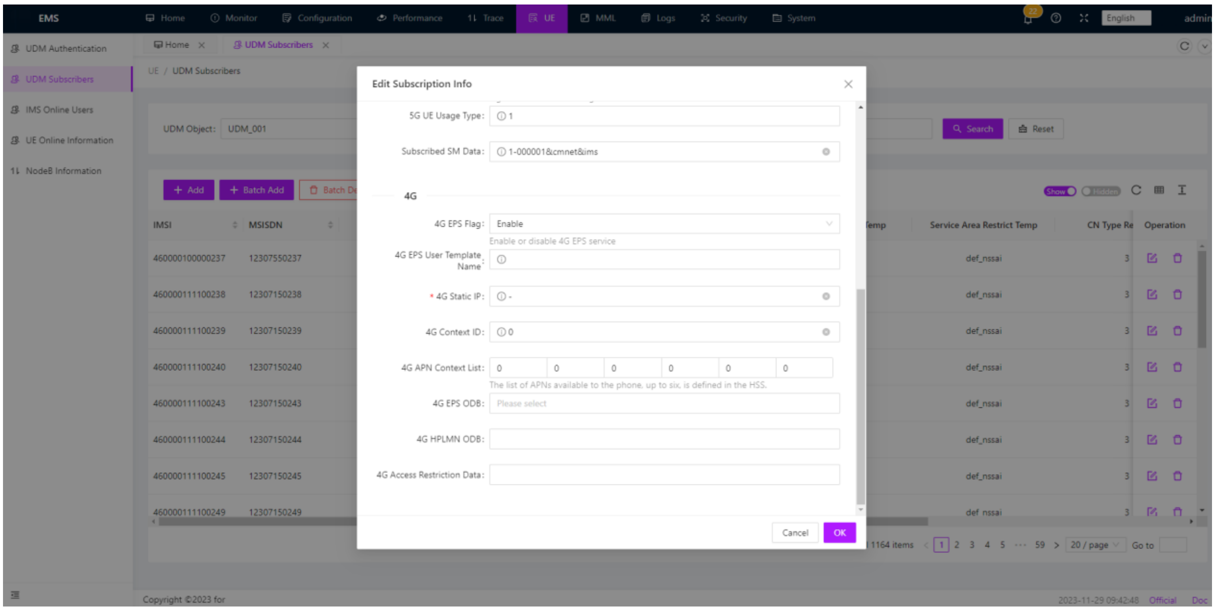
5G MICO Mode: Enable

Signed MICO business flag bits

5G UE Usage Type: 1

Subscribed SM Data: 1-000001&cmnet&ims

Cancel OK



Edit Subscription Info

5G UE Usage Type: 1

Subscribed SM Data: 1-000001&cmnet&ims

4G

4G EPS Flag: Enable

Enable or disable 4G EPS service

4G EPS User Template Name:

* 4G Static IP: -

4G Context ID: 0

4G APN Context List: 0 0 0 0 0 0

The list of APNs available to the phone, up to six, is defined in the HSS.

4G EPS ODB: Please select

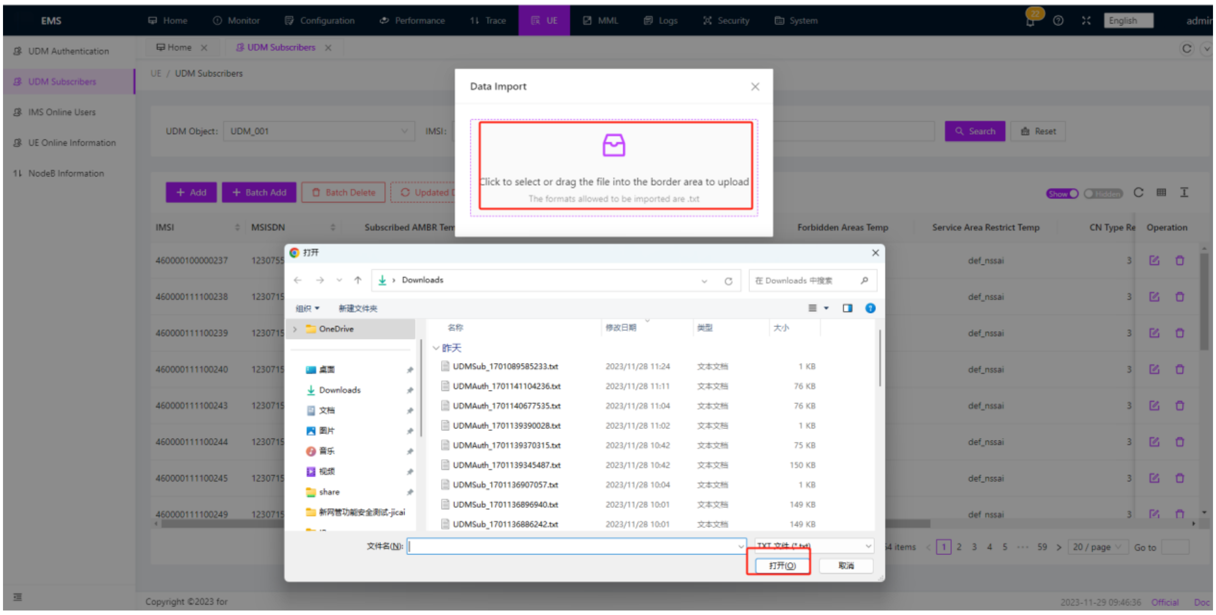
4G HPLMN ODB:

4G Access Restriction Data:

Cancel OK

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.



Data Import

Click to select or drag the file into the border area to upload

The formats allowed to be imported are .txt

打开

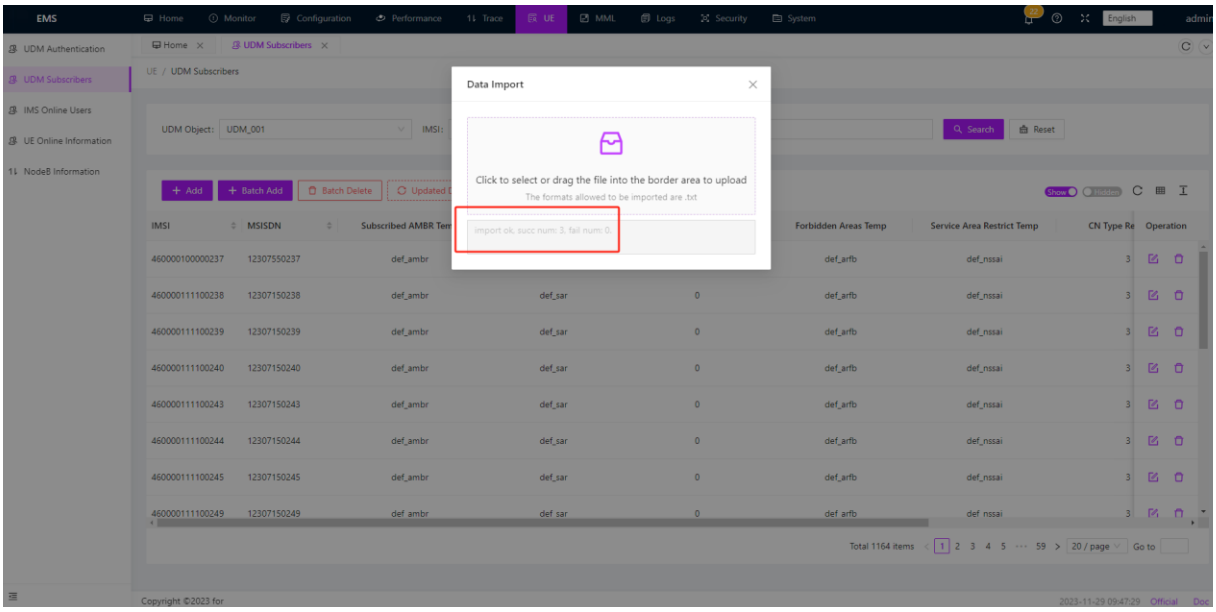
Downloads

昨天

名称	修改日期	类型	大小
UDMSub_1701089585233.txt	2023/11/28 11:24	文本文档	1 KB
UDMAuth_1701141104236.txt	2023/11/28 11:11	文本文档	76 KB
UDMAuth_1701140677535.txt	2023/11/28 11:04	文本文档	76 KB
UDMAuth_1701139390028.txt	2023/11/28 11:02	文本文档	1 KB
UDMAuth_1701139370315.txt	2023/11/28 10:42	文本文档	75 KB
UDMAuth_1701139345487.txt	2023/11/28 10:42	文本文档	150 KB
UDMSub_1701136907057.txt	2023/11/28 10:04	文本文档	1 KB
UDMSub_1701136896940.txt	2023/11/28 10:01	文本文档	149 KB
UDMSub_1701136886242.txt	2023/11/28 10:01	文本文档	149 KB

文件名(N):

TXT 文件 (*.txt)



Data Import

Click to select or drag the file into the border area to upload

The formats allowed to be imported are .txt

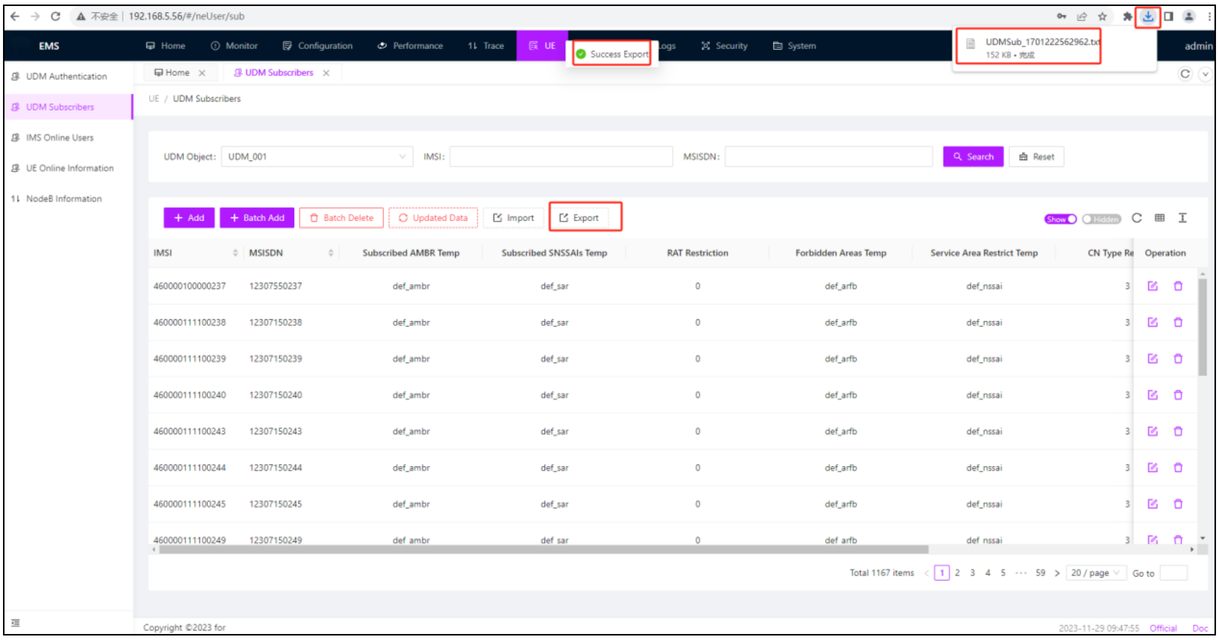
import ok, succ num: 3, fail num: 0.

UDM Object: UDM_001

IMSI	MSISDN	Subscribed AMBR Temp			Forbidden Areas Temp	Service Area Restrict Temp	CN Type Re
460000100000237	12307550237	def_ambr			def_arfb	def_nssai	3
460000111100238	12307150238	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100239	12307150239	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100240	12307150240	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100243	12307150243	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100244	12307150244	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100245	12307150245	def_ambr	def_sar	0	def_arfb	def_nssai	3
460000111100249	12307150249	def_ambr	def_sar	0	def_arfb	def_nssai	3

Total 1164 items

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



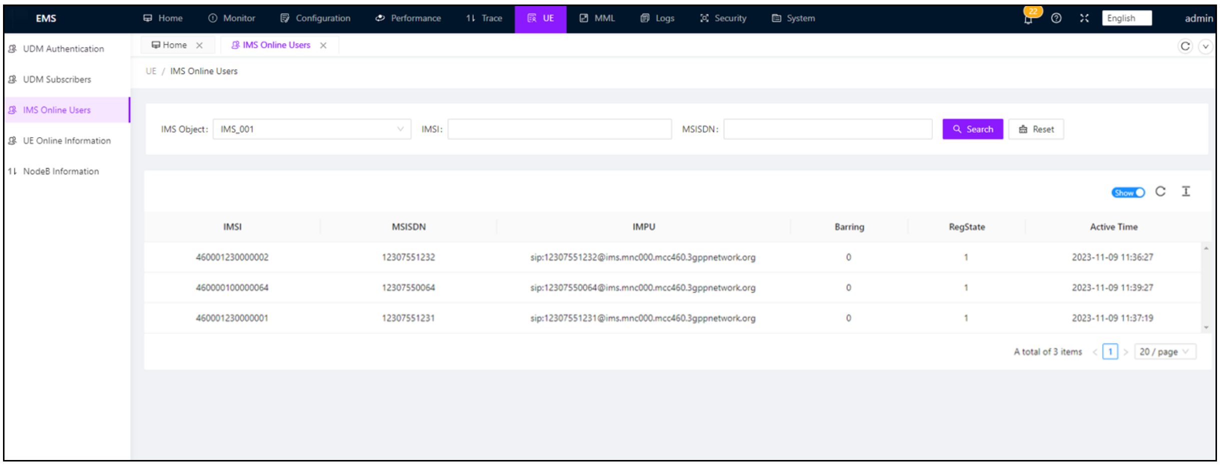
UDM Object: UDM_001 IMSI: MSISDN:

IMSI	MSISDN	Subscribed AMBR Temp	Subscribed SNSSAIs Temp	RAT Restriction	Forbidden Areas Temp	Service Area Restrict Temp	CN Type Re	Operation
460000100000237	12307550237	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100238	12307150238	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100239	12307150239	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100240	12307150240	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100243	12307150243	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100244	12307150244	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100245	12307150245	def_ambr	def_sar	0	def_arfb	def_nssai	3	
460000111100249	12307150249	def_ambr	def_sar	0	def_arfb	def_nssai	3	

Total 1167 items < 1 2 3 4 5 ··· 59 > 20 / page Go to

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.



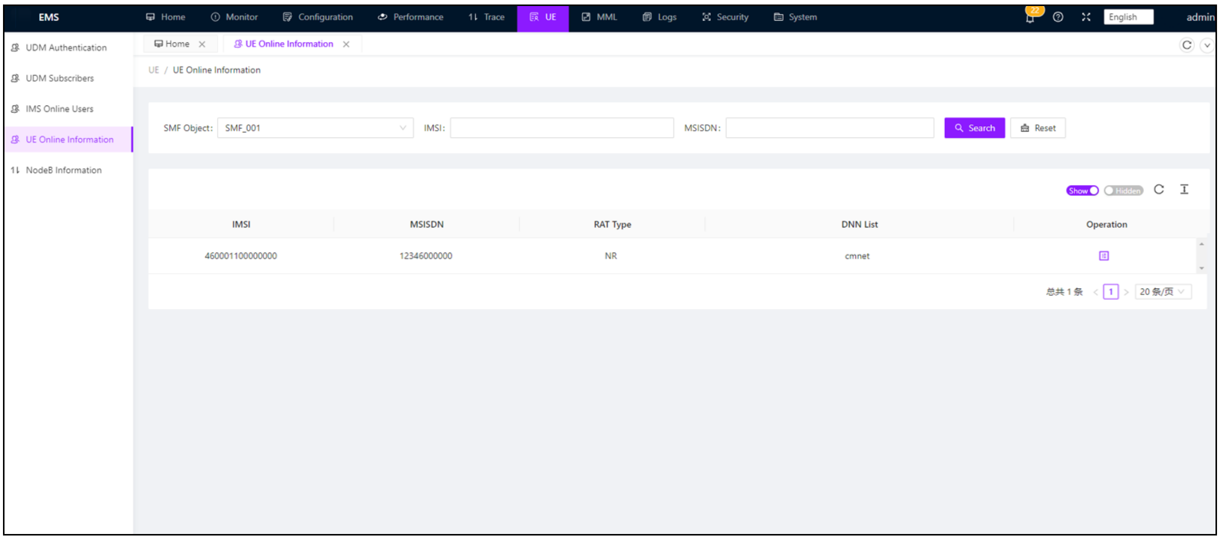
IMS Object: IMS_001 IMSI: MSISDN:

IMSI	MSISDN	IMPU	Barring	RegState	Active Time
460001230000002	12307551232	sip:12307551232@ims.mnc000.mcc460.3gppnetwork.org	0	1	2023-11-09 11:36:27
460000100000064	12307550064	sip:12307550064@ims.mnc000.mcc460.3gppnetwork.org	0	1	2023-11-09 11:39:27
460001230000001	12307551231	sip:12307551231@ims.mnc000.mcc460.3gppnetwork.org	0	1	2023-11-09 11:37:19

A total of 3 items < 1 > 20 / page

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



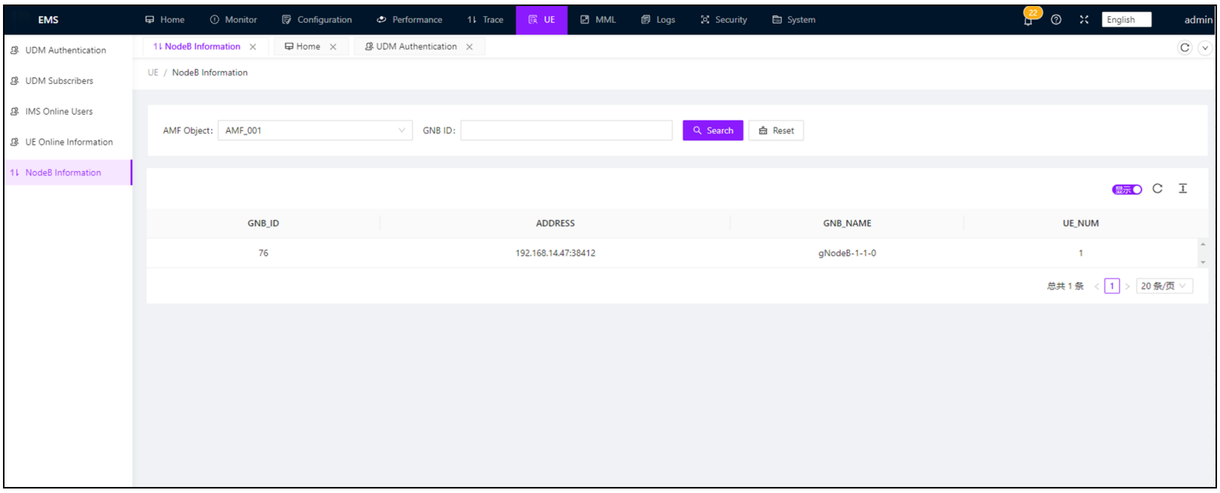
SMF Object: SMF_001 IMSI: MSISDN:

IMSI	MSISDN	RAT Type	DNN List	Operation
460001100000000	12346000000	NR	cmnet	

总共 1 条 < 1 > 20 条/页

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.



AMF Object: AMF_001 GNB ID:

GNB_ID	ADDRESS	GNB_NAME	UE_NUM
76	192.168.14.47:38412	gNodeB-1-1-0	1

总共 1 条 < 1 > 20 条/页

3.8 MML

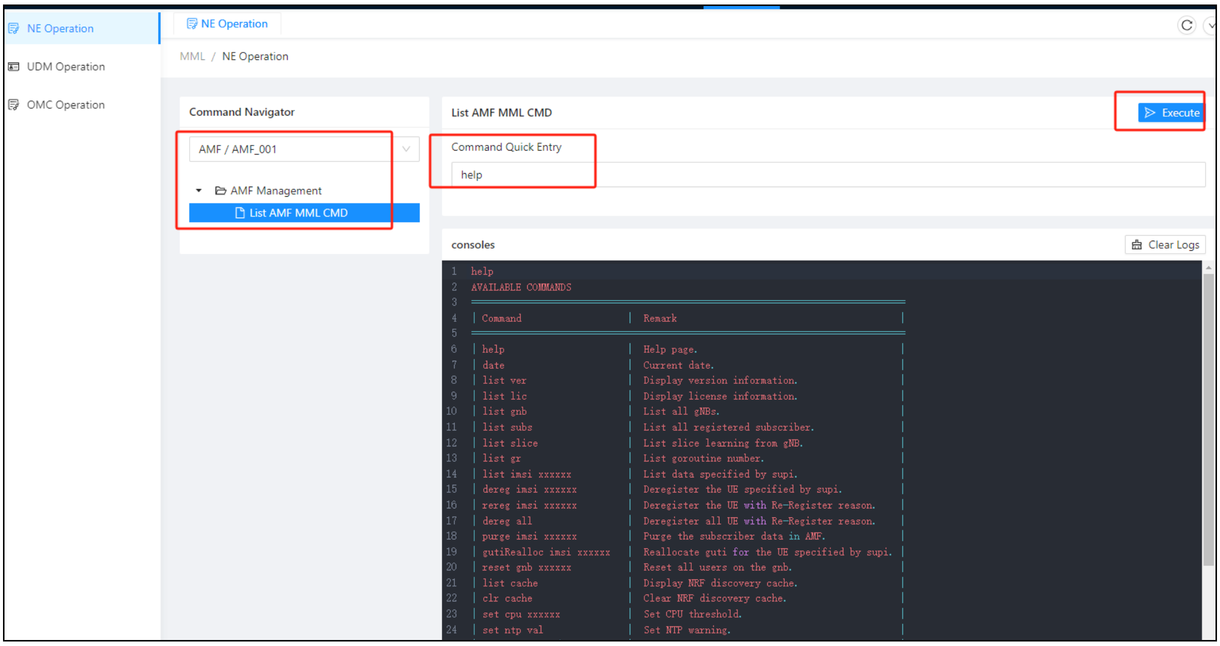
MML (Man-Machine Language) management refers to the method of managing and configuring various parts of the core network by using specific command languages. MML management covers NE operation, UDM operation, and OMC operation.

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

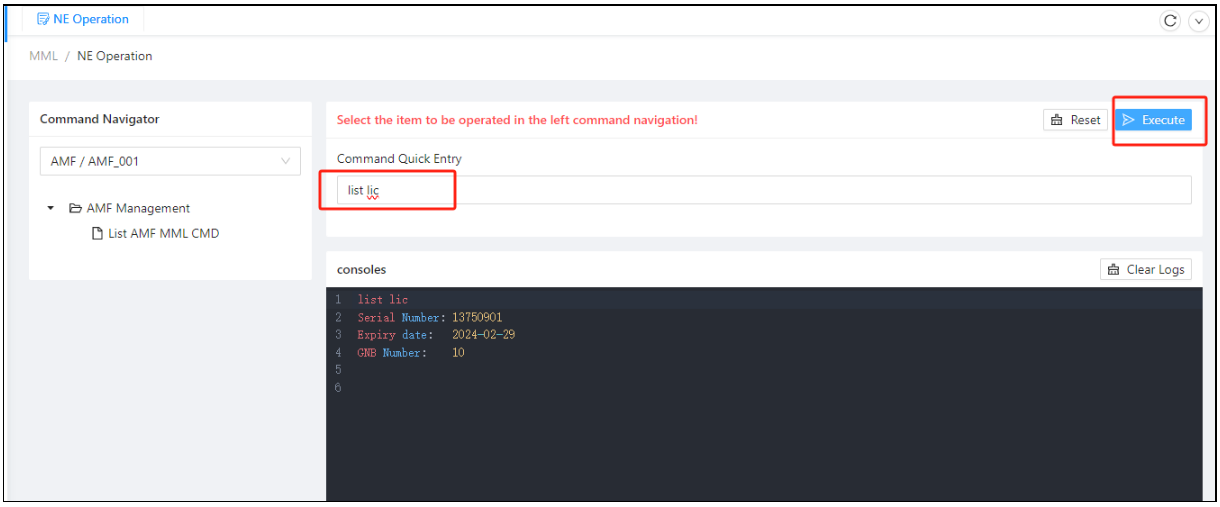
NE manage and configure core network elements through MML commands. Network element operations can query and configure the data information of each network element, such as querying the license information and version information of the network element, querying the access base station information in 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 explanation~~s~~ 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.



Command Quick Entry: help

```
help
AVAILABLE COMMANDS
================================================================
| Command                  | Remark                              |
================================================================
| help                     | Help page.                          |
| date                     | Current date.                       |
| list ver                 | Display version information.        |
| list lic                 | Display license information.        |
| list gnb                 | List all gNBs.                      |
| list subs                | List all registered subscriber.     |
| list slice               | List slice learning from gNB.       |
| list gr                  | List goroutine number.              |
| list imsi xxxxxx         | List data specified by supi.        |
| dereg imsi xxxxxx        | Deregister the UE specified by supi. |
| rereg imsi xxxxxx        | Deregister the UE with Re-Register reason. |
| dereg all                | Deregister all UE with Re-Register reason. |
| purge imsi xxxxxx        | Purge the subscriber data in AMF.   |
| gutiRealloc imsi xxxxxx  | Reallocate guti for the UE specified by supi. |
| reset gnb xxxxxx         | Reset all users on the gnb.         |
| list cache               | Display NRF discovery cache.        |
| clr cache                | Clear NRF discovery cache.          |
| set cpu xxxxxx           | Set CPU threshold.                  |
| set ntp val              | Set NTP warning.                    |
```



Select the item to be operated in the left command navigation!

Command Quick Entry: list lic

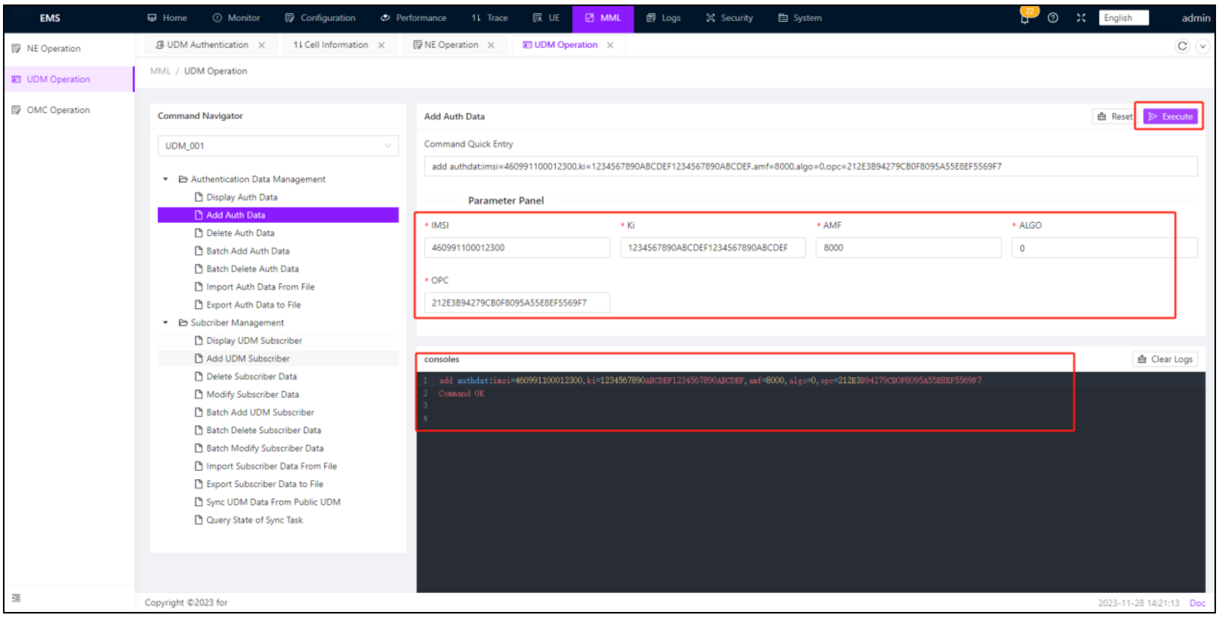
```
list lic
Serial Number: 13750901
Expiry date:   2024-02-29
GNB Number:    10
```

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.

Add UDM Auth data as follows:



Add Auth Data

Command Quick Entry

```
add authdat:imsi=460991100012300,ki=1234567890ABCDEF1234567890ABCDEF,amf=8000,algo=0,opc=212E3B94279CB0F8095A55E8EF5569F7
```

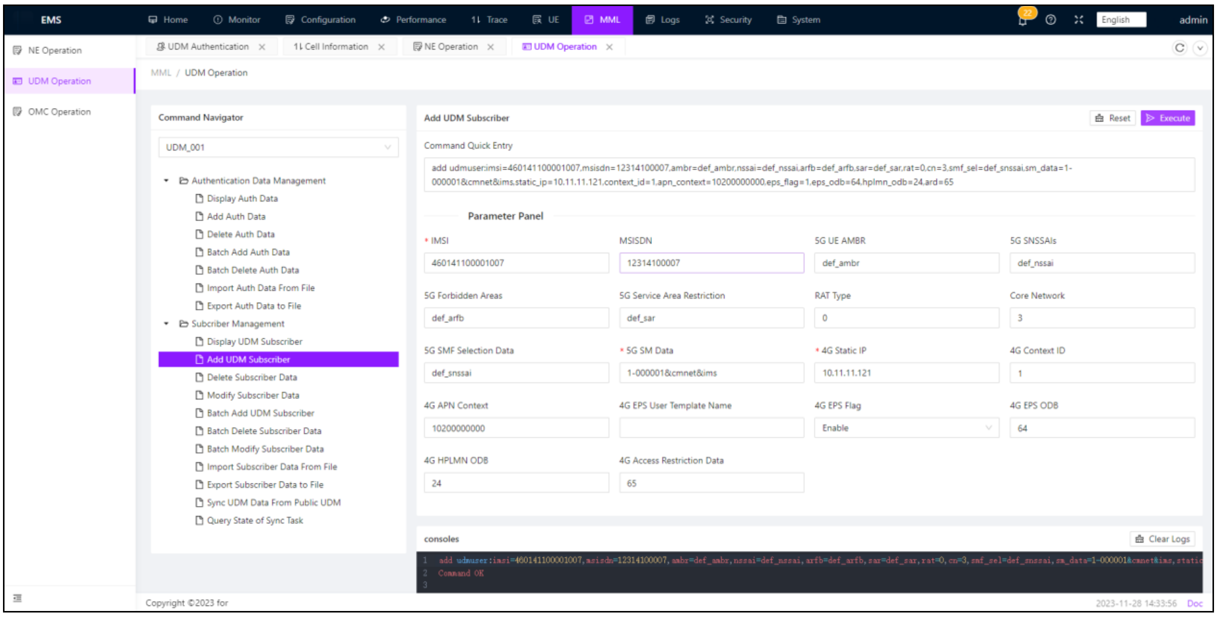
Parameter Panel

- * IMSI: 460991100012300
- * Ki: 1234567890ABCDEF1234567890ABCDEF
- * AMF: 8000
- * ALGO: 0
- * OPC: 212E3B94279CB0F8095A55E8EF5569F7

consoles

```
add authdat:imsi=460991100012300,ki=1234567890ABCDEF1234567890ABCDEF,amf=8000,algo=0,opc=212E3B94279CB0F8095A55E8EF5569F7
Command OK
```

Add UDM Subscriber data as follows:



Add UDM Subscriber

Command Quick Entry

```
add udmuser:imsi=460141100001007,msisdn=12314100007,ambr=def_ambr,nssai=def_nssai,arfb=def_arfb,sar=def_sar,rat=0,cn=3,smf_sel=def_snssai,sm_data=1-000001&cmnet&ims,static_ip=10.11.11.121,context_id=1,apn_context=10200000000,eps_flag=1,eps_odb=64,hplmn_odb=24,ard=65
```

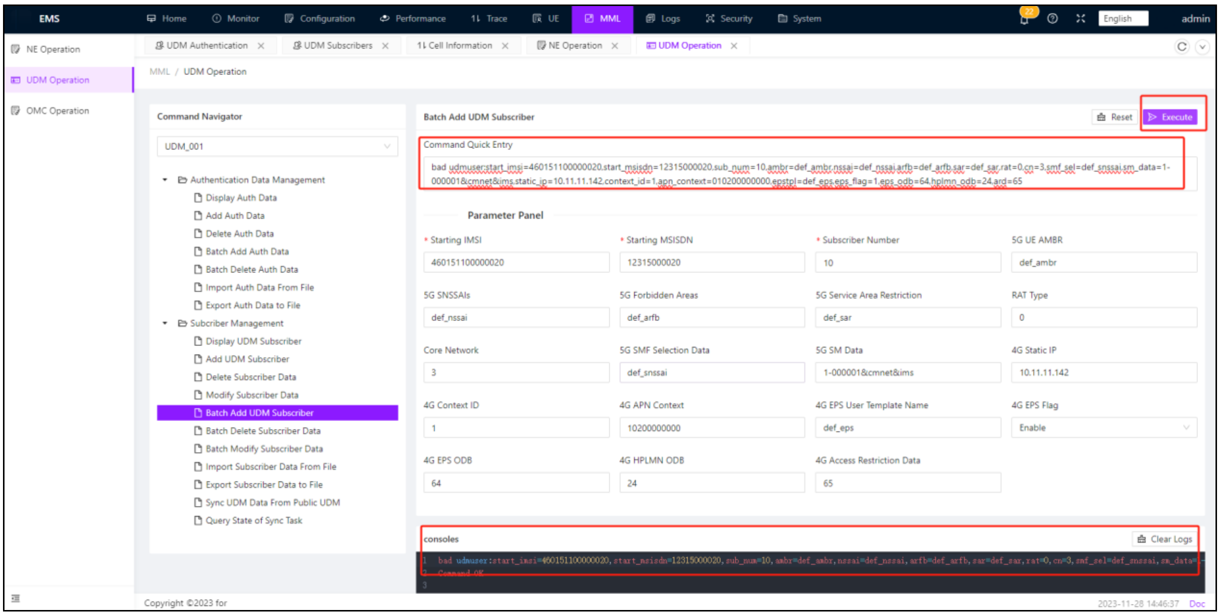
Parameter Panel

* IMSI 460141100001007	MSISDN 12314100007	5G UE AMBR def_ambr	5G SNSSAIs def_nssai
5G Forbidden Areas def_arfb	5G Service Area Restriction def_sar	RAT Type 0	Core Network 3
5G SMF Selection Data def_snssai	* 5G SM Data 1-000001&cmnet&ims	* 4G Static IP 10.11.11.121	4G Context ID 1
4G APN Context 10200000000	4G EPS User Template Name	4G EPS Flag Enable	4G EPS ODB 64
4G HPLMN ODB 24	4G Access Restriction Data 65		

consoles

```
add udmuser:imsi=460141100001007,msisdn=12314100007,ambr=def_ambr,nssai=def_nssai,arfb=def_arfb,sar=def_sar,rat=0,cn=3,smf_sel=def_snssai,sm_data=1-000001&cmnet&ims,static
Command OK
```

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



Batch Add UDM Subscriber

Command Quick Entry

```
bad udmuser:start_imsi=460151100000020,start_msisdn=12315000020,sub_num=10,ambr=def_ambr,nssai=def_nssai,arfb=def_arfb,sar=def_sar,rat=0,cn=3,smf_sel=def_snssai,sm_data=1-000001&cmnet&ims,static_ip=10.11.11.142,context_id=1,apn_context=010200000000,epstpl=def_eps,eps_flag=1,eps_odb=64,hplmn_odb=24,ard=65
```

Parameter Panel

* Starting IMSI	* Starting MSISDN	* Subscriber Number	5G UE AMBR
460151100000020	12315000020	10	def_ambr
5G SNSSAIs	5G Forbidden Areas	5G Service Area Restriction	RAT Type
def_nssai	def_arfb	def_sar	0
Core Network	5G SMF Selection Data	5G SM Data	4G Static IP
3	def_snssai	1-000001&cmnet&ims	10.11.11.142
4G Context ID	4G APN Context	4G EPS User Template Name	4G EPS Flag
1	10200000000	def_eps	Enable
4G EPS ODB	4G HPLMN ODB	4G Access Restriction Data	
64	24	65	

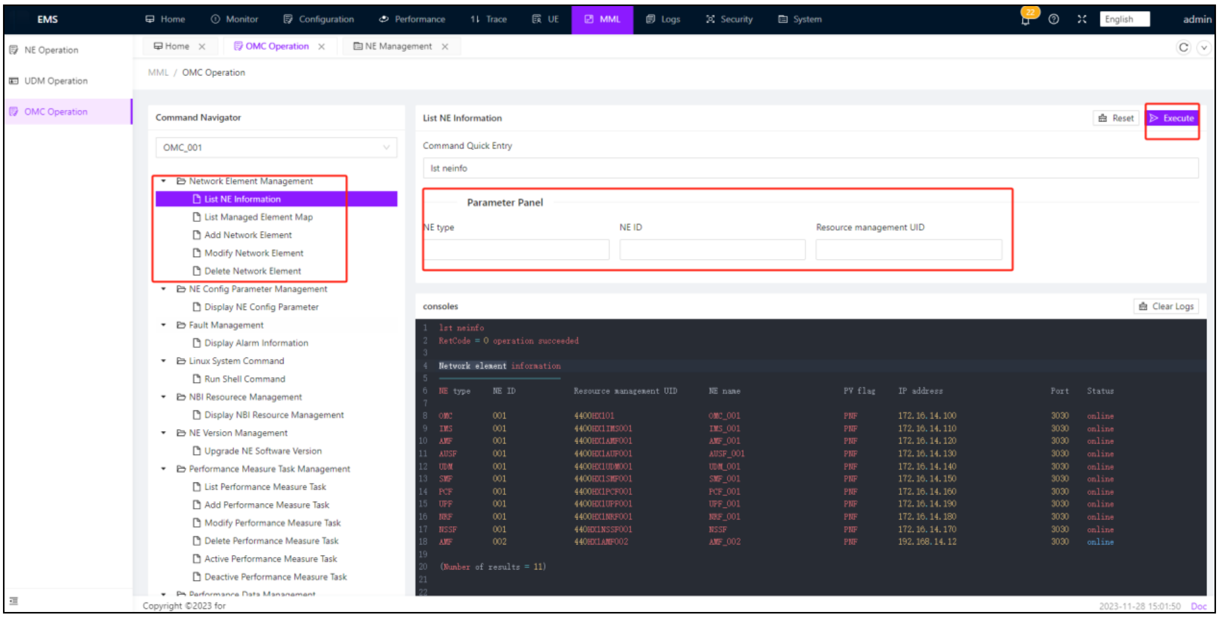
consoles

```
bad udmuser:start_imsi=460151100000020,start_msisdn=12315000020,sub_num=10,ambr=def_ambr,nssai=def_nssai,arfb=def_arfb,sar=def_sar,rat=0,cn=3,smf_sel=def_snssai,sm_data=
Command OK
```

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:



List NE Information

Command Quick Entry

```
lst neinfo
```

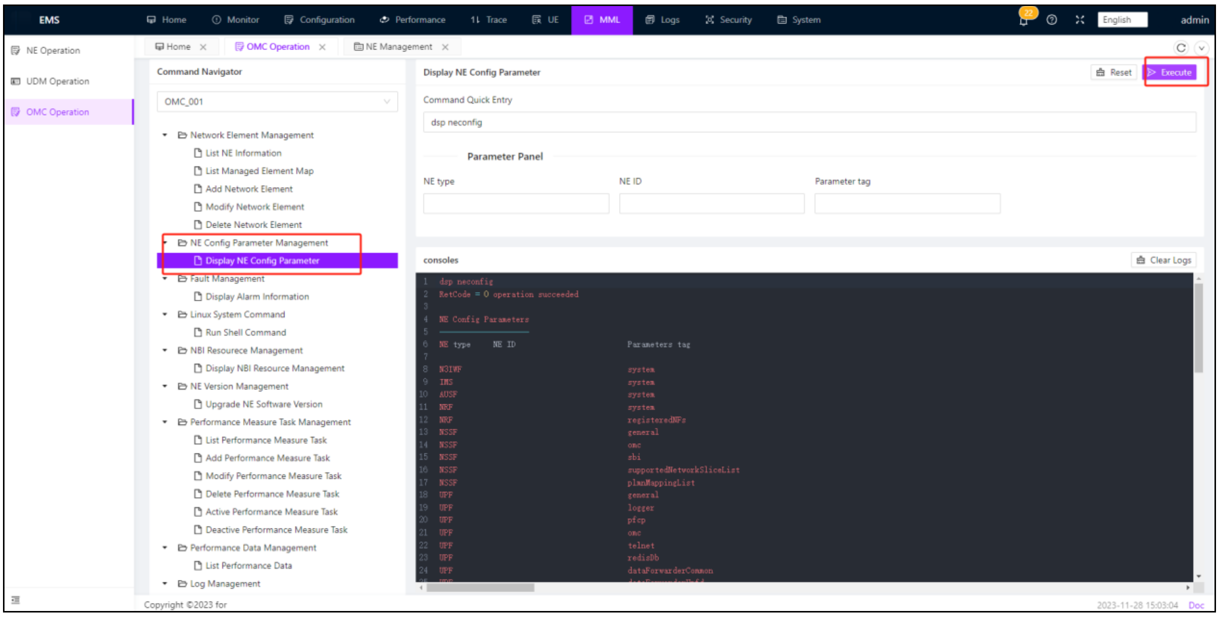
Parameter Panel

NE type	NE ID	Resource management UID

consoles

```
lst neinfo
RetCode = 0 operation succeeded

Network element information

NE type    NE ID       Resource management UID    NE name          PV flag    IP address       Port    Status

OMC        001         4400HX101                  OMC_001          PNF        172.16.14.100    3030    online
IMS        001         4400HX1IMS001              IMS_001          PNF        172.16.14.110    3030    online
AMF        001         4400HX1AMF001              AMF_001          PNF        172.16.14.120    3030    online
AUSF       001         4400HX1AUF001              AUSF_001         PNF        172.16.14.130    3030    online
UDM        001         4400HX1UDM001              UDM_001          PNF        172.16.14.140    3030    online
SMF        001         4400HX1SMF001              SMF_001          PNF        172.16.14.150    3030    online
PCF        001         4400HX1PCF001              PCF_001          PNF        172.16.14.160    3030    online
UPF        001         4400HX1UPF001              UPF_001          PNF        172.16.14.190    3030    online
NRF        001         4400HX1NRF001              NRF_001          PNF        172.16.14.180    3030    online
NSSF       001         440HX1NSSF001              NSSF             PNF        172.16.14.170    3030    online
AMF        002         440HX1AMF002               AMF_002          PNF        192.168.14.12    3030    online

(Number of results = 11)
```

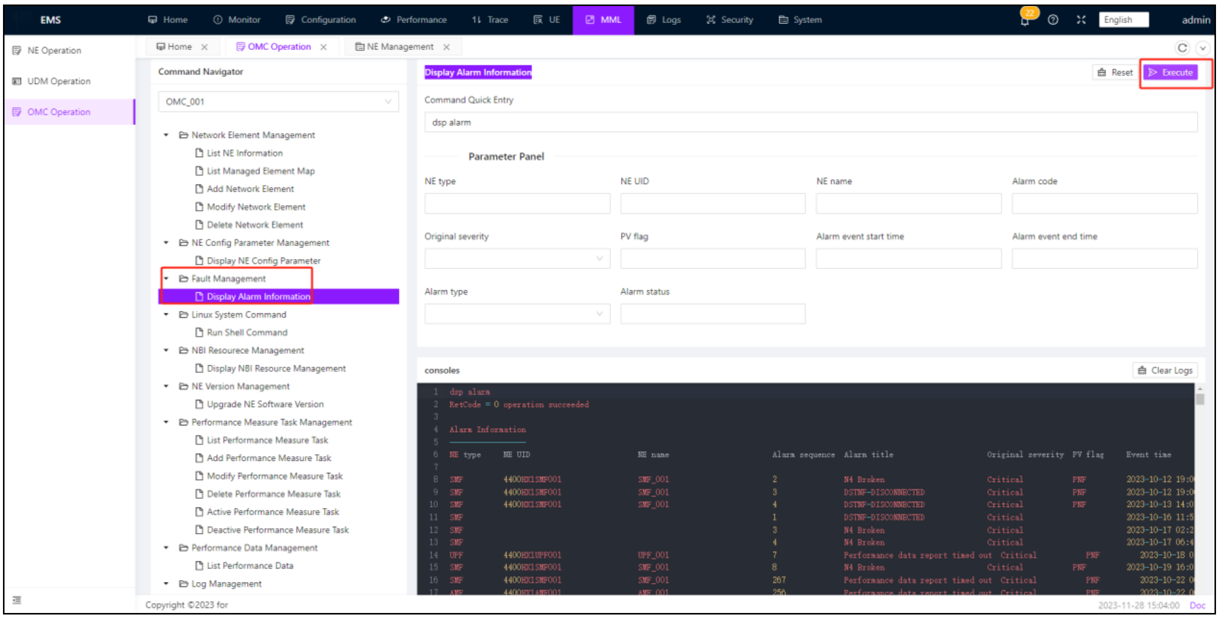
NE Config Parameter Management:



Command Quick Entry: dsp neconfig

```
dsp neconfig
RetCode = 0 operation succeeded

NE Config Parameters

NE type     NE ID                     Parameters tag

N3IWF                                 system
IMS                                   system
AUSF                                  system
NRF                                   system
NRF                                   registeredNFs
NSSF                                  general
NSSF                                  omc
NSSF                                  sbi
NSSF                                  supportedNetworkSliceList
NSSF                                  plmnMappingList
UPF                                   general
UPF                                   logger
UPF                                   pfcp
UPF                                   omc
UPF                                   telnet
UPF                                   redisDb
UPF                                   dataForwarderCommon
```

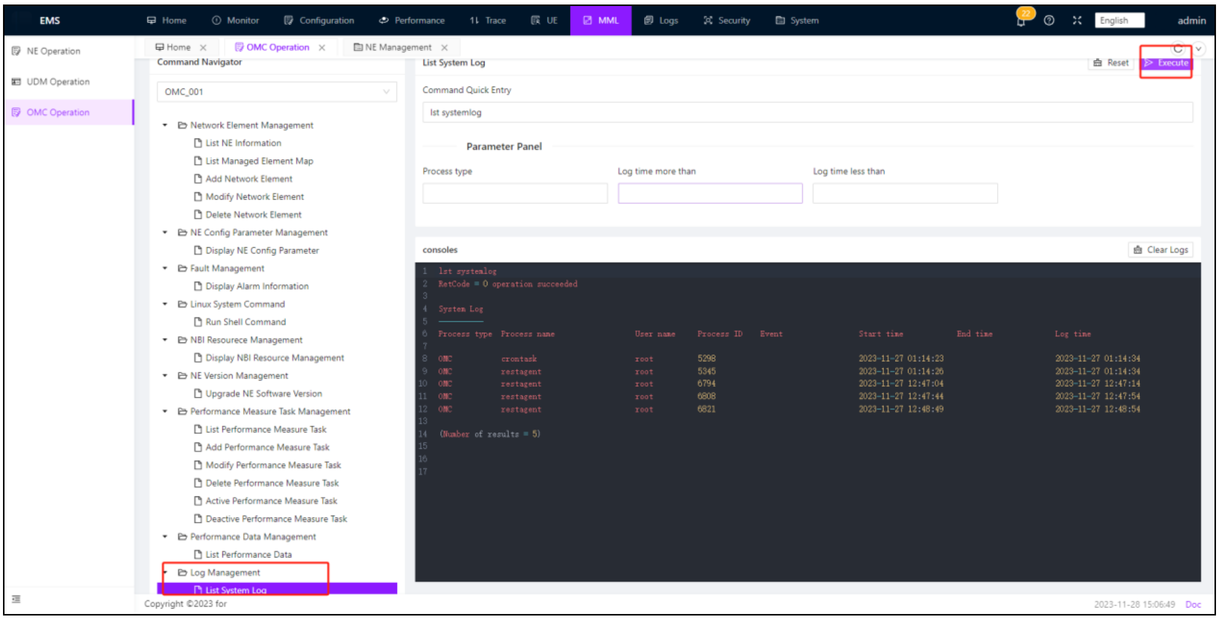
Fault Management:



Command Quick Entry: dsp alarm

```
dsp alarm
RetCode = 0 operation succeeded

Alarm Information

NE type    NE UID              NE name              Alarm sequence  Alarm title                   Original severity  PV flag   Event time

SMF        4400HX1SMF001       SMF_001              2               N4 Broken                     Critical           PNF       2023-10-12 19:0
SMF        4400HX1SMF001       SMF_001              3               DSTNF-DISCONNECTED            Critical           PNF       2023-10-12 19:0
SMF        4400HX1SMF001       SMF_001              4               DSTNF-DISCONNECTED            Critical           PNF       2023-10-13 14:0
SMF                                                 1               DSTNF-DISCONNECTED            Critical                     2023-10-16 11:5
SMF                                                 3               N4 Broken                     Critical                     2023-10-17 02:2
SMF                                                 4               N4 Broken                     Critical                     2023-10-17 06:4
UPF        4400HX1UPF001       UPF_001              7               Performance data report timed out  Critical         PNF       2023-10-18 0
SMF        4400HX1SMF001       SMF_001              8               N4 Broken                     Critical           PNF       2023-10-19 16:0
SMF        4400HX1SMF001       SMF_001              267             Performance data report timed out  Critical         PNF       2023-10-22 0
AMF        4400HX1AMF001       AMF_001              256             Performance data report timed out  Critical         PNF       2023-10-22 0
```

Log Management:



OMC_001

List System Log

Command Quick Entry: lst systemlog

Process type:

Log time more than:

Log time less than:

```
lst systemlog
RetCode = 0 operation succeeded

System Log
──────────
Process type  Process name         User name   Process ID   Event        Start time           End time         Log time

OMC           crontask             root        5298                      2023-11-27 01:14:23                   2023-11-27 01:14:34
OMC           restagent            root        5345                      2023-11-27 01:14:26                   2023-11-27 01:14:34
OMC           restagent            root        6794                      2023-11-27 12:47:04                   2023-11-27 12:47:14
OMC           restagent            root        6808                      2023-11-27 12:47:44                   2023-11-27 12:47:54
OMC           restagent            root        6821                      2023-11-27 12:48:49                   2023-11-27 12:48:54

(Number of results = 5)
```

3.9 Logs

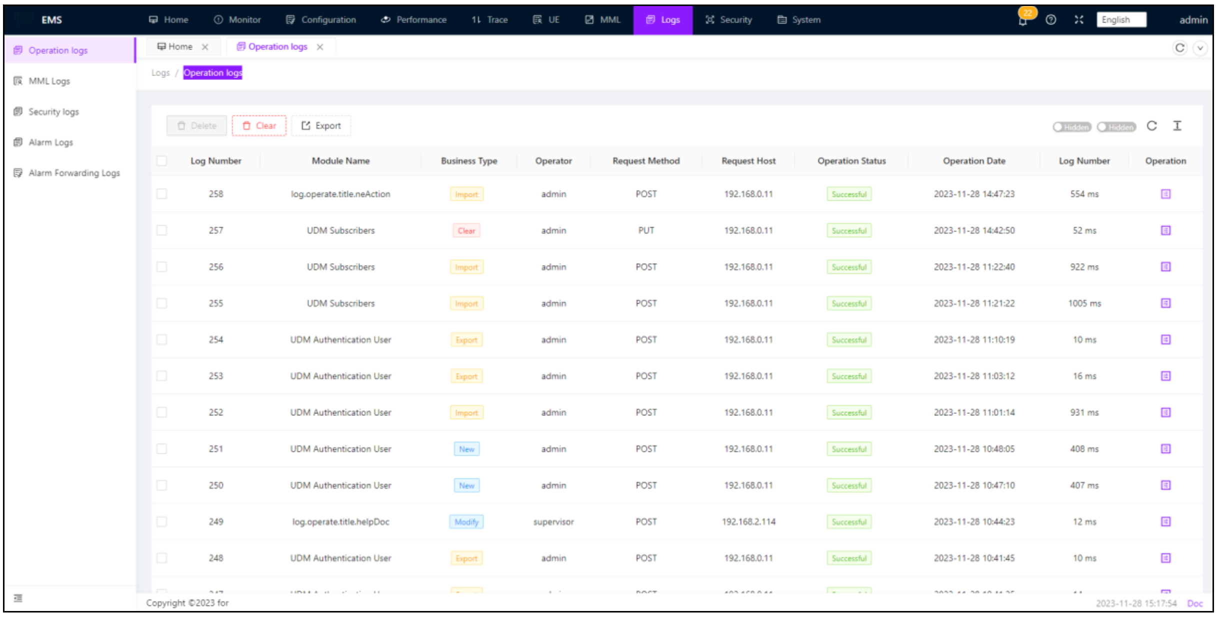
Core network Logs management is a critical part of network uptime maintenance, allowing managers to track the status of various parts of the core network, record potential problems, and perform troubleshooting and performance analysis. Logs management covers operation logs, MML logs, security logs, alarm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

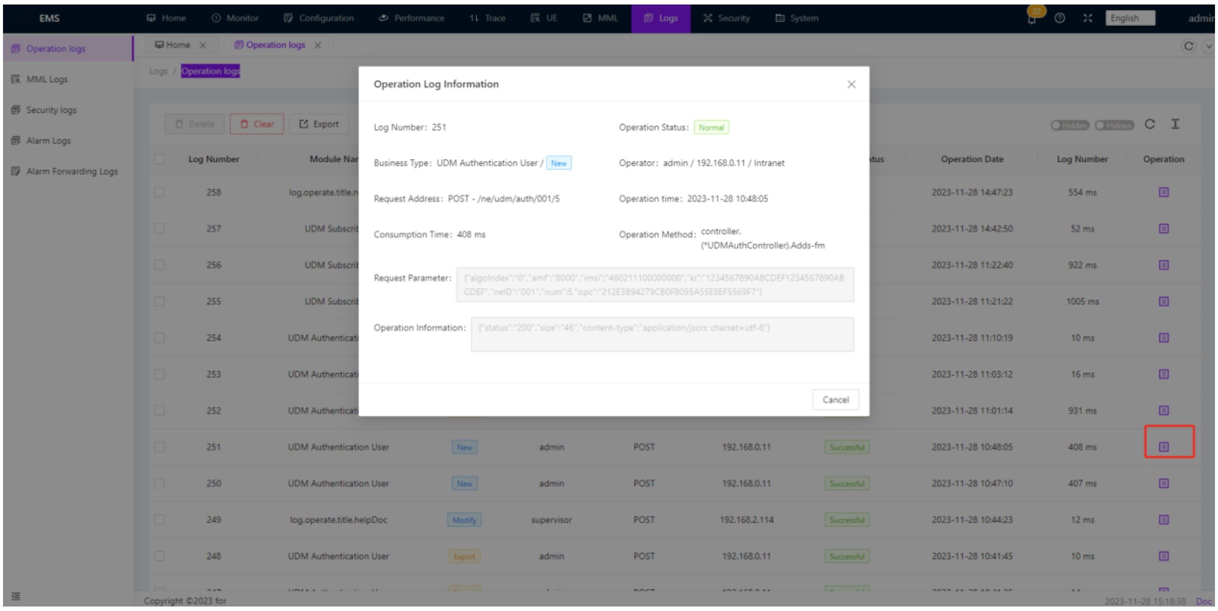
3.9.1 Operation logs

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.



Log Number	Module Name	Business Type	Operator	Request Method	Request Host	Operation Status	Operation Date	Log Number	Operation
258	log.operate.title.neAction	Import	admin	POST	192.168.0.11	Successful	2023-11-28 14:47:23	554 ms	
257	UDM Subscribers	Clear	admin	PUT	192.168.0.11	Successful	2023-11-28 14:42:50	52 ms	
256	UDM Subscribers	Import	admin	POST	192.168.0.11	Successful	2023-11-28 11:22:40	922 ms	
255	UDM Subscribers	Import	admin	POST	192.168.0.11	Successful	2023-11-28 11:21:22	1005 ms	
254	UDM Authentication User	Export	admin	POST	192.168.0.11	Successful	2023-11-28 11:10:19	10 ms	
253	UDM Authentication User	Export	admin	POST	192.168.0.11	Successful	2023-11-28 11:03:12	16 ms	
252	UDM Authentication User	Import	admin	POST	192.168.0.11	Successful	2023-11-28 11:01:14	931 ms	
251	UDM Authentication User	New	admin	POST	192.168.0.11	Successful	2023-11-28 10:48:05	408 ms	
250	UDM Authentication User	New	admin	POST	192.168.0.11	Successful	2023-11-28 10:47:10	407 ms	
249	log.operate.title.helpDoc	Modify	supervisor	POST	192.168.2.114	Successful	2023-11-28 10:44:23	12 ms	
248	UDM Authentication User	Export	admin	POST	192.168.0.11	Successful	2023-11-28 10:41:45	10 ms	



Operation Log Information

Log Number: 251

Operation Status: Normal

Business Type: UDM Authentication User / New

Operator: admin / 192.168.0.11 / Intranet

Request Address: POST - /ne/udm/auth/001/5

Operation time: 2023-11-28 10:48:05

Consumption Time: 408 ms

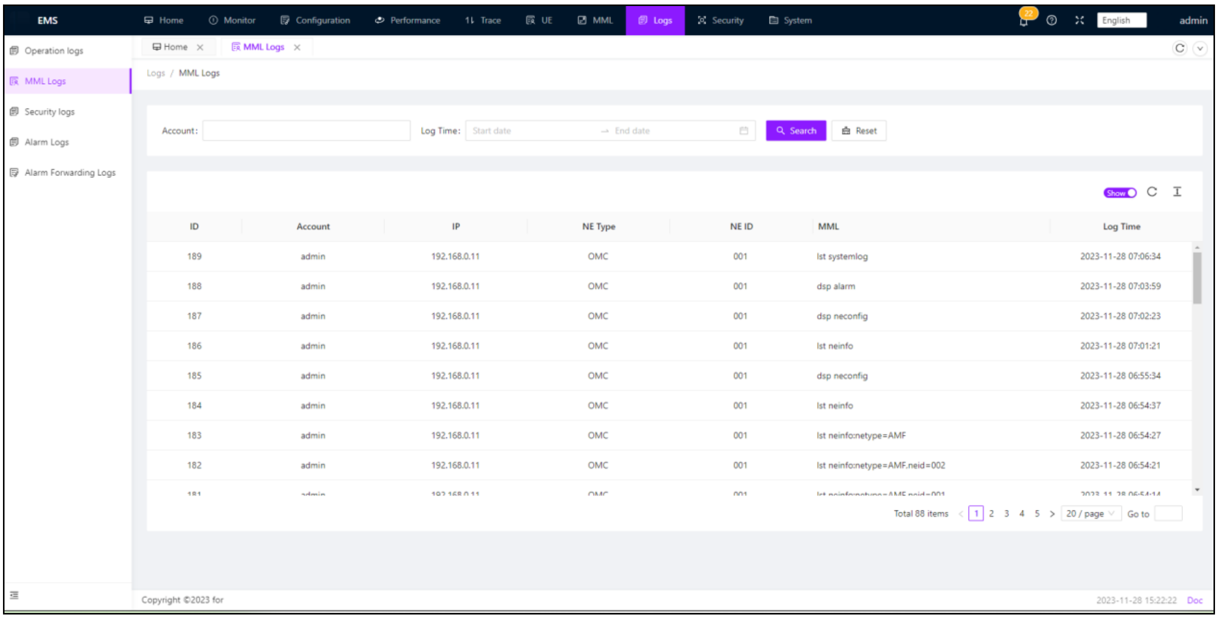
Operation Method: controller.(*UDMAuthController).Adds-fm

Request Parameter: {"algoIndex":"0","amf":"8000","imsi":"460211100000000","ki":"1234567890ABCDEF1234567890ABCDEF","neID":"001","num":5,"opc":"212E3B94279CB0F8095A55E8EF5569F7"}

Operation Information: {"status":"200","size":"46","content-type":"application/json; charset=utf-8"}

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.



Account:

Log Time: Start date → End date

ID	Account	IP	NE Type	NE ID	MML	Log Time
189	admin	192.168.0.11	OMC	001	lst systemlog	2023-11-28 07:06:34
188	admin	192.168.0.11	OMC	001	dsp alarm	2023-11-28 07:03:59
187	admin	192.168.0.11	OMC	001	dsp neconfig	2023-11-28 07:02:23
186	admin	192.168.0.11	OMC	001	lst neinfo	2023-11-28 07:01:21
185	admin	192.168.0.11	OMC	001	dsp neconfig	2023-11-28 06:55:34
184	admin	192.168.0.11	OMC	001	lst neinfo	2023-11-28 06:54:37
183	admin	192.168.0.11	OMC	001	lst neinfo:netype=AMF	2023-11-28 06:54:27
182	admin	192.168.0.11	OMC	001	lst neinfo:netype=AMF.neid=002	2023-11-28 06:54:21
181	admin	192.168.0.11	OMC	001	lst neinfo:netype=AMF.neid=001	2023-11-28 06:54:14

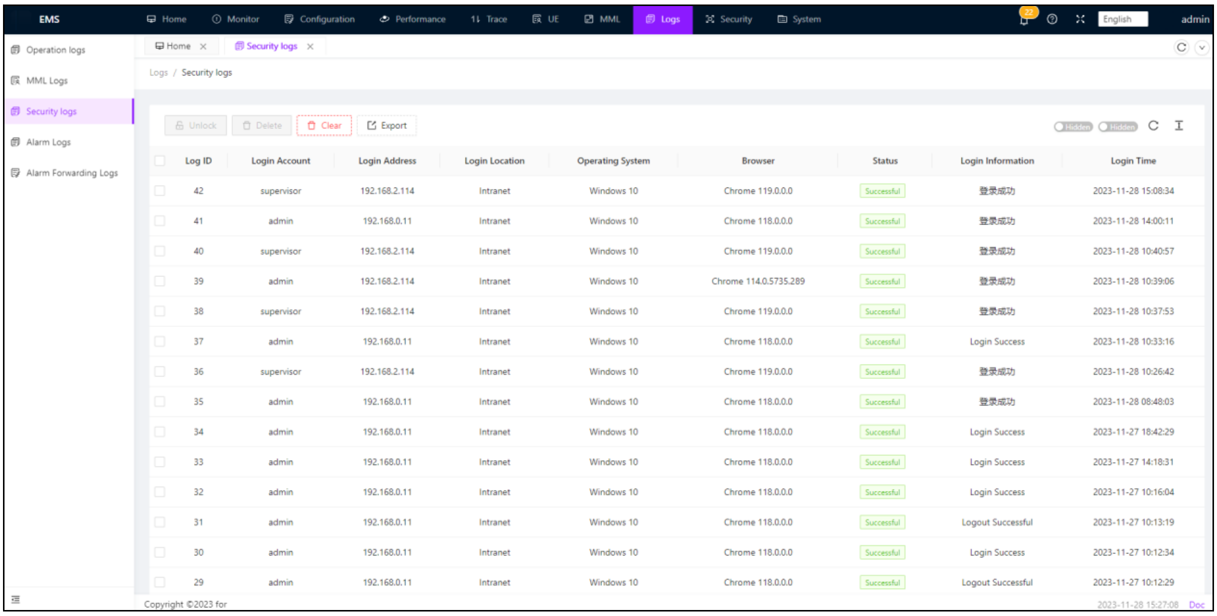
Total 88 items < 1 2 3 4 5 > 20 / page Go to

Copyright ©2023 for

2023-11-28 15:22:22 Doc

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.



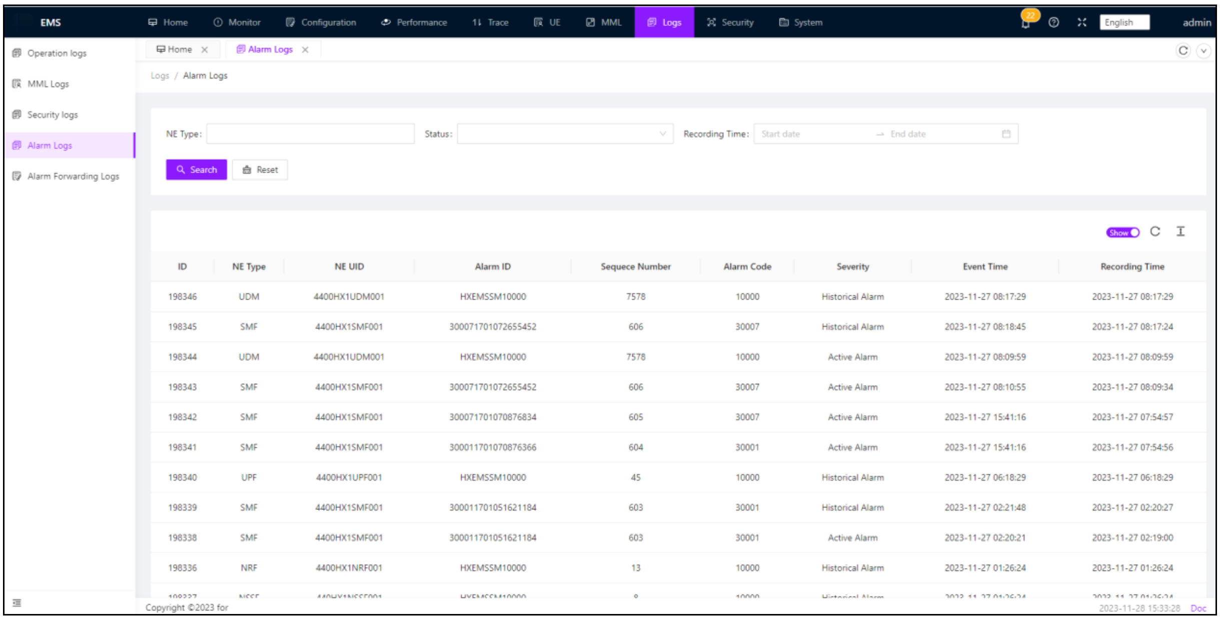
□	Log ID	Login Account	Login Address	Login Location	Operating System	Browser	Status	Login Information	Login Time
□	42	supervisor	192.168.2.114	Intranet	Windows 10	Chrome 119.0.0.0	Successful	登录成功	2023-11-28 15:08:34
□	41	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	登录成功	2023-11-28 14:00:11
□	40	supervisor	192.168.2.114	Intranet	Windows 10	Chrome 119.0.0.0	Successful	登录成功	2023-11-28 10:40:57
□	39	admin	192.168.2.114	Intranet	Windows 10	Chrome 114.0.5735.289	Successful	登录成功	2023-11-28 10:39:06
□	38	supervisor	192.168.2.114	Intranet	Windows 10	Chrome 119.0.0.0	Successful	登录成功	2023-11-28 10:37:53
□	37	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Login Success	2023-11-28 10:33:16
□	36	supervisor	192.168.2.114	Intranet	Windows 10	Chrome 119.0.0.0	Successful	登录成功	2023-11-28 10:26:42
□	35	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	登录成功	2023-11-28 08:48:03
□	34	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Login Success	2023-11-27 18:42:29
□	33	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Login Success	2023-11-27 14:18:31
□	32	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Login Success	2023-11-27 10:16:04
□	31	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Logout Successful	2023-11-27 10:13:19
□	30	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Login Success	2023-11-27 10:12:34
□	29	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	Successful	Logout Successful	2023-11-27 10:12:29

Copyright ©2023 for

2023-11-28 15:27:08 Doc

3.9.4 Alarm Logs

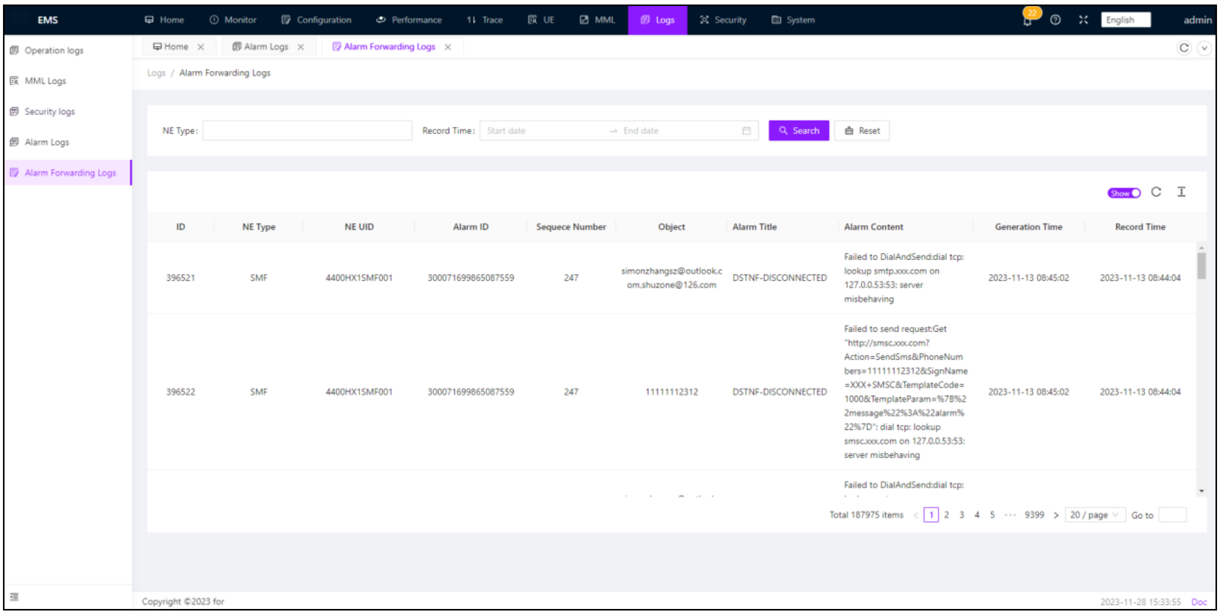
Alarm logs record all information about system faults, exceptions, or important events, including activation alarms and historical alarms, so that O&M personnel can quickly locate and rectify existing problems.



ID	NE Type	NE UID	Alarm ID	Sequece Number	Alarm Code	Severity	Event Time	Recording Time
198346	UDM	4400HX1UDM001	HXEMSSM10000	7578	10000	Historical Alarm	2023-11-27 08:17:29	2023-11-27 08:17:29
198345	SMF	4400HX1SMF001	300071701072655452	606	30007	Historical Alarm	2023-11-27 08:18:45	2023-11-27 08:17:24
198344	UDM	4400HX1UDM001	HXEMSSM10000	7578	10000	Active Alarm	2023-11-27 08:09:59	2023-11-27 08:09:59
198343	SMF	4400HX1SMF001	300071701072655452	606	30007	Active Alarm	2023-11-27 08:10:55	2023-11-27 08:09:34
198342	SMF	4400HX1SMF001	300071701070876834	605	30007	Active Alarm	2023-11-27 15:41:16	2023-11-27 07:54:57
198341	SMF	4400HX1SMF001	300011701070876366	604	30001	Active Alarm	2023-11-27 15:41:16	2023-11-27 07:54:56
198340	UPF	4400HX1UPF001	HXEMSSM10000	45	10000	Historical Alarm	2023-11-27 06:18:29	2023-11-27 06:18:29
198339	SMF	4400HX1SMF001	300011701051621184	603	30001	Historical Alarm	2023-11-27 02:21:48	2023-11-27 02:20:27
198338	SMF	4400HX1SMF001	300011701051621184	603	30001	Active Alarm	2023-11-27 02:20:21	2023-11-27 02:19:00
198336	NRF	4400HX1NRF001	HXEMSSM10000	13	10000	Historical Alarm	2023-11-27 01:26:24	2023-11-27 01:26:24

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.



ID	NE Type	NE UID	Alarm ID	Sequece Number	Object	Alarm Title	Alarm Content	Generation Time	Record Time
396521	SMF	4400HX1SMF001	300071699865087559	247	simonzhangsz@outlook.com,shuzone@126.com	DSTNF-DISCONNECTED	Failed to DialAndSend:dial tcp: lookup smtp.xxx.com on 127.0.0.53:53: server misbehaving	2023-11-13 08:45:02	2023-11-13 08:44:04
396522	SMF	4400HX1SMF001	300071699865087559	247	11111112312	DSTNF-DISCONNECTED	Failed to send request:Get "http://smsc.xxx.com?Action=SendSms&PhoneNumbers=11111112312&SignName=XXX+SMSC&TemplateCode=1000&TemplateParam=%7B%22message%22%3A%22alarm%22%7D": dial tcp: lookup smsc.xxx.com on 127.0.0.53:53: server misbehaving	2023-11-13 08:45:02	2023-11-13 08:44:04
							Failed to DialAndSend:dial tcp:		

3.10 Security

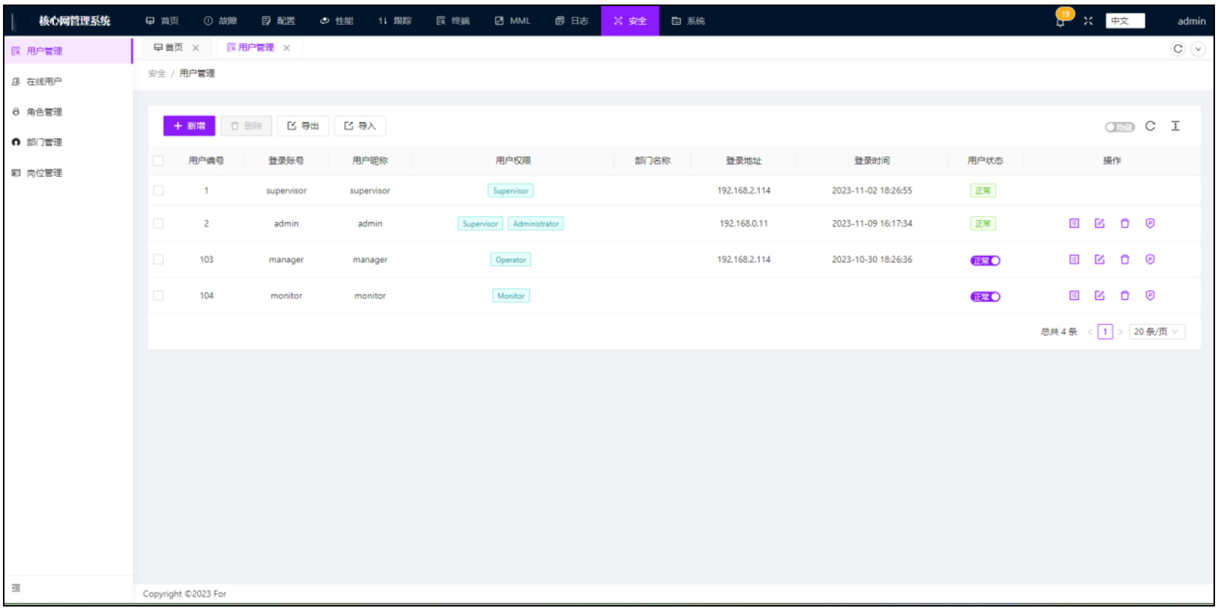
Core network security management refers to the management and permission control of users on the core network to ensure network security and protect the system from unauthorized access or malicious attacks. Core network security management includes user management, online user management, role management, 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.

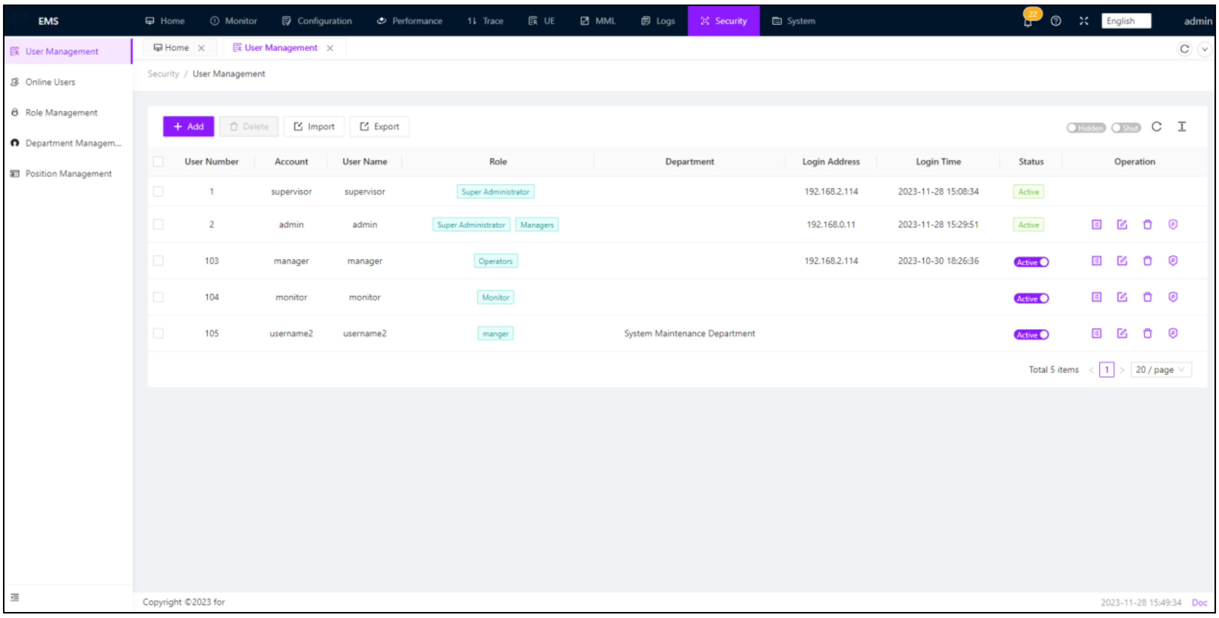
.



□	用户编号	登录账号	用户昵称	用户权限	部门名称	登录地址	登录时间	用户状态	操作
□	1	supervisor	supervisor	Supervisor		192.168.2.114	2023-11-02 18:26:55	正常	
□	2	admin	admin	Supervisor Administrator		192.168.0.11	2023-11-09 16:17:34	正常	
□	103	manager	manager	Operator		192.168.2.114	2023-10-30 18:26:36	正常	
□	104	monitor	monitor	Monitor				正常	

总共 4 条 < 1 > 20 条/页

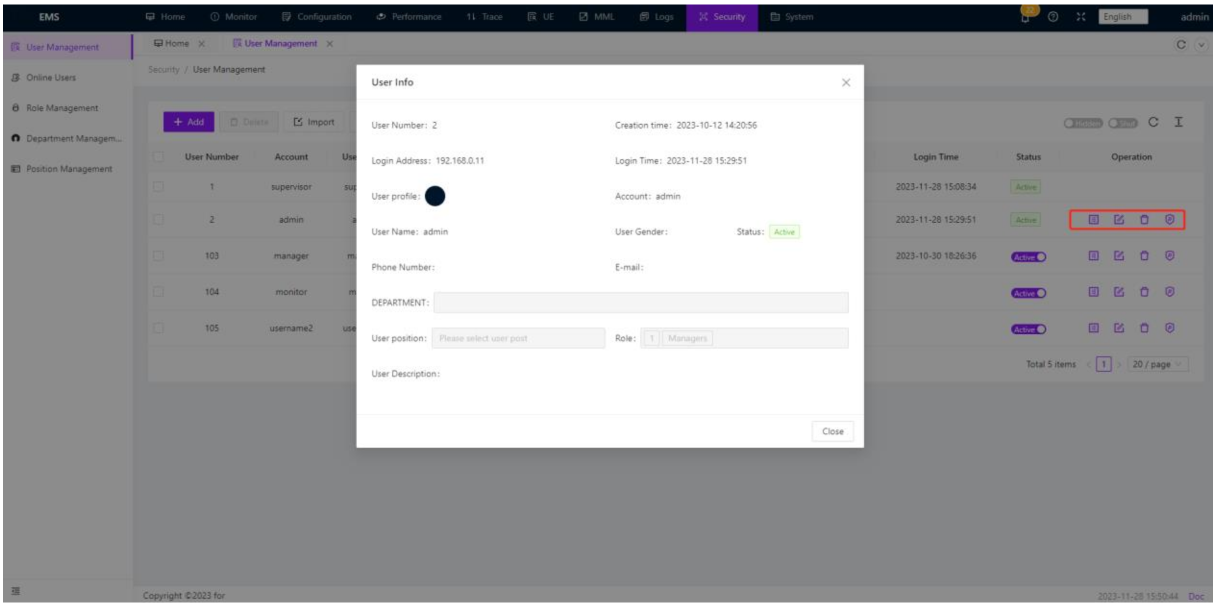
Click “Add” to add a logged-in user. Different user positions can be set according to needs, and different user permissions can be added. For specific permissions, please refer to Role Management：



User Number	Account	User Name	Role	Department	Login Address	Login Time	Status	Operation
1	supervisor	supervisor	Super Administrator		192.168.2.114	2023-11-28 15:08:34	Active	
2	admin	admin	Super Administrator Managers		192.168.0.11	2023-11-28 15:29:51	Active	
103	manager	manager	Operators		192.168.2.114	2023-10-30 18:26:36	Active	
104	monitor	monitor	Monitor				Active	
105	username2	username2	manger	System Maintenance Department			Active	

Total 5 items 1 20 / page

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:



User Info

User Number: 2

Creation time: 2023-10-12 14:20:56

Login Address: 192.168.0.11

Login Time: 2023-11-28 15:29:51

User profile:

Account: admin

User Name: admin

User Gender:

Status: Active

Phone Number:

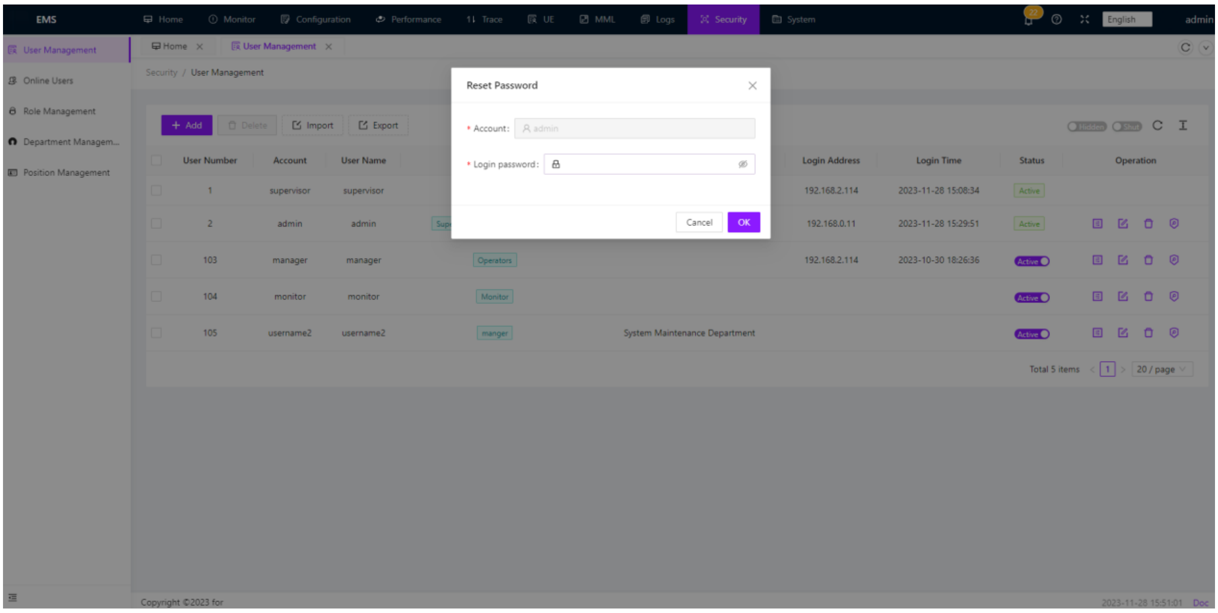
E-mail:

DEPARTMENT:

User position: Please select user post

Role: 1 Managers

User Description:



Reset Password

* Account: admin

* Login password:

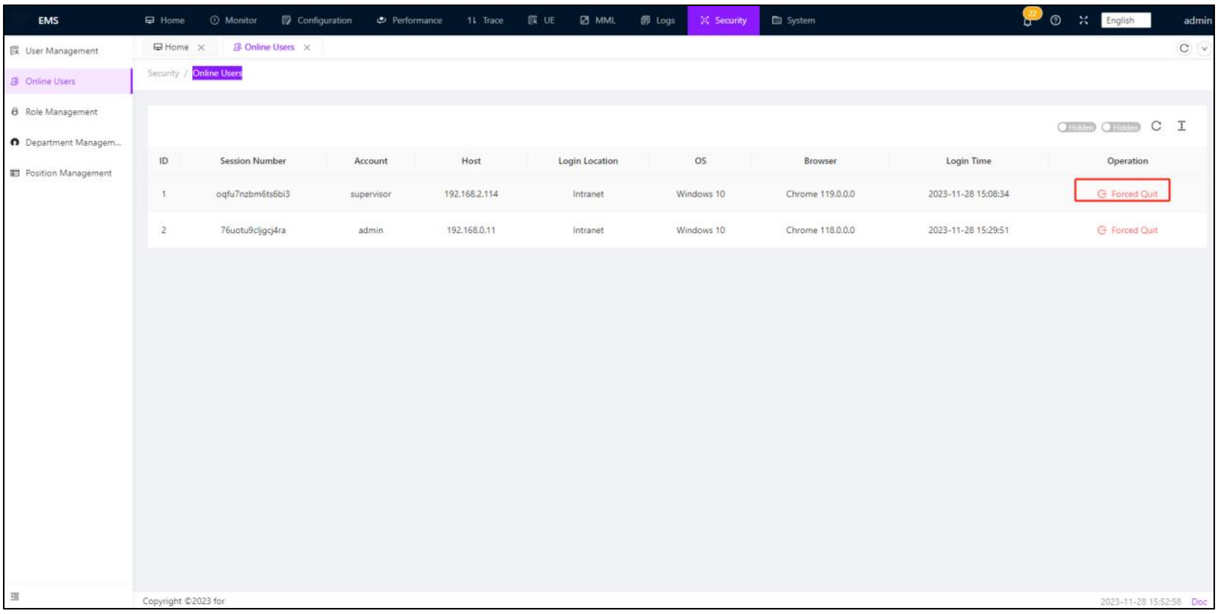
Cancel OK

User Number	Account	User Name			Login Address	Login Time	Status	Operation
1	supervisor	supervisor			192.168.2.114	2023-11-28 15:08:34	Active	
2	admin	admin	Sup		192.168.0.11	2023-11-28 15:29:51	Active	
103	manager	manager	Operators		192.168.2.114	2023-10-30 18:26:36	Active	
104	monitor	monitor	Monitor				Active	
105	username2	username2	manger	System Maintenance Department			Active	

Total 5 items < 1 > 20 / page

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.

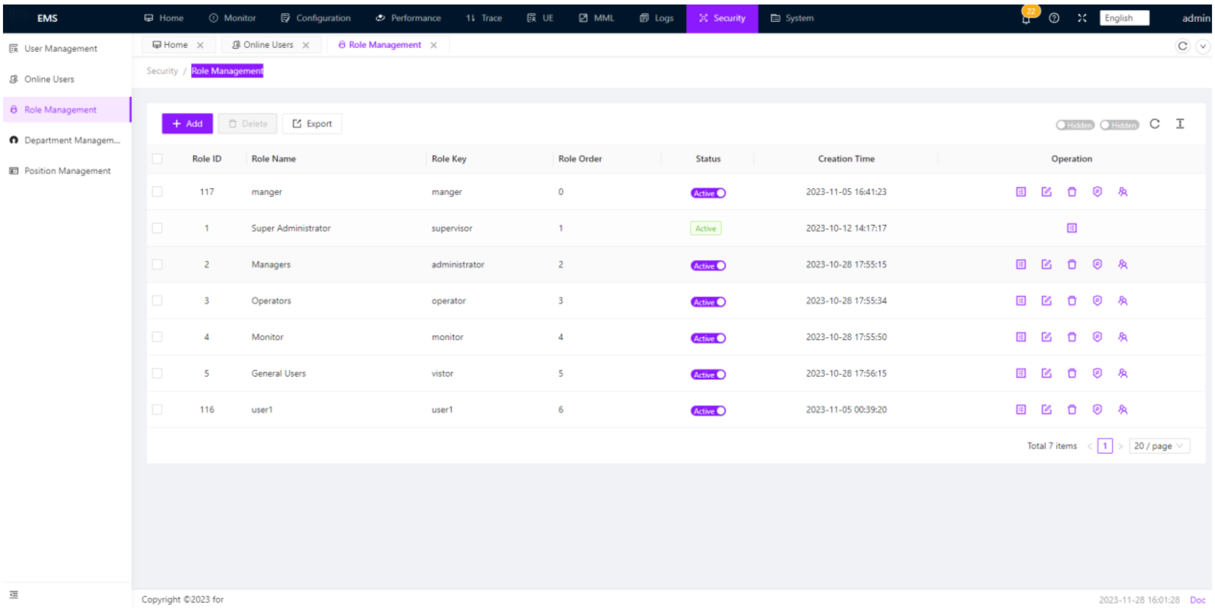


ID	Session Number	Account	Host	Login Location	OS	Browser	Login Time	Operation
1	oqfu7nzbm6ts6bi3	supervisor	192.168.2.114	Intranet	Windows 10	Chrome 119.0.0.0	2023-11-28 15:08:34	Forced Quit
2	76uotu9cljgcj4ra	admin	192.168.0.11	Intranet	Windows 10	Chrome 118.0.0.0	2023-11-28 15:29:51	Forced Quit

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.

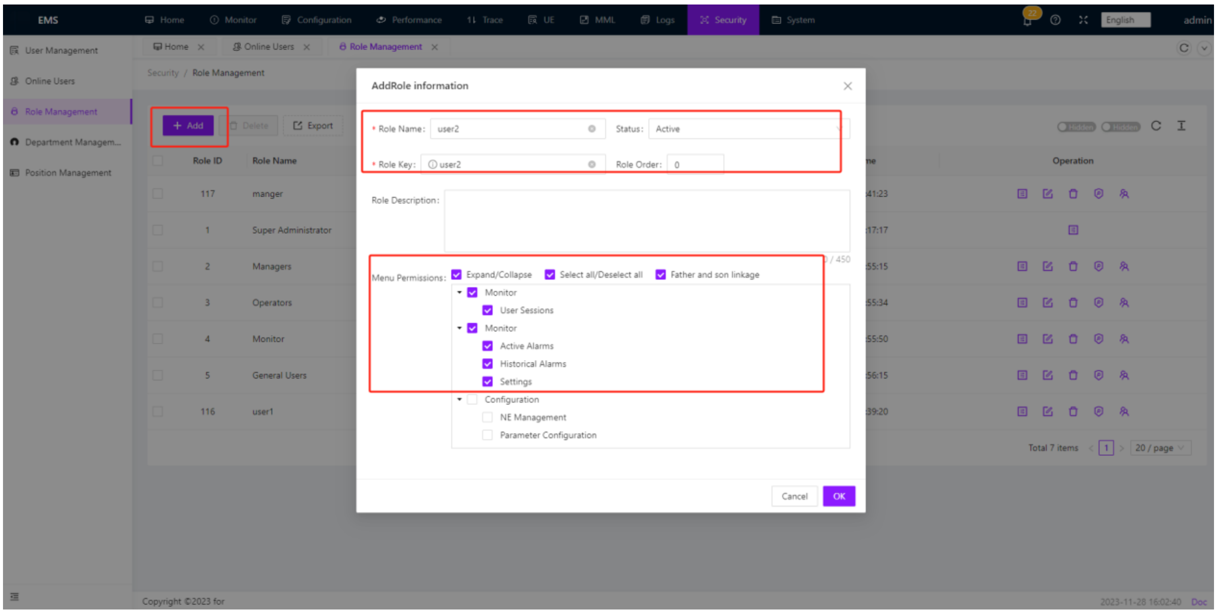
The operator can view role related information and perform operations such as adding, deleting, and modifying. The operator can also add role permission sets:



Role ID	Role Name	Role Key	Role Order	Status	Creation Time	Operation
117	manger	manger	0	Active	2023-11-05 16:41:23	
1	Super Administrator	supervisor	1	Active	2023-10-12 14:17:17	
2	Managers	administrator	2	Active	2023-10-28 17:55:15	
3	Operators	operator	3	Active	2023-10-28 17:55:34	
4	Monitor	monitor	4	Active	2023-10-28 17:55:50	
5	General Users	vistor	5	Active	2023-10-28 17:56:15	
116	user1	user1	6	Active	2023-11-05 00:39:20	

Total 7 items 1 20 / page

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



AddRole information

* Role Name: user2 Status: Active

* Role Key: user2 Role Order: 0

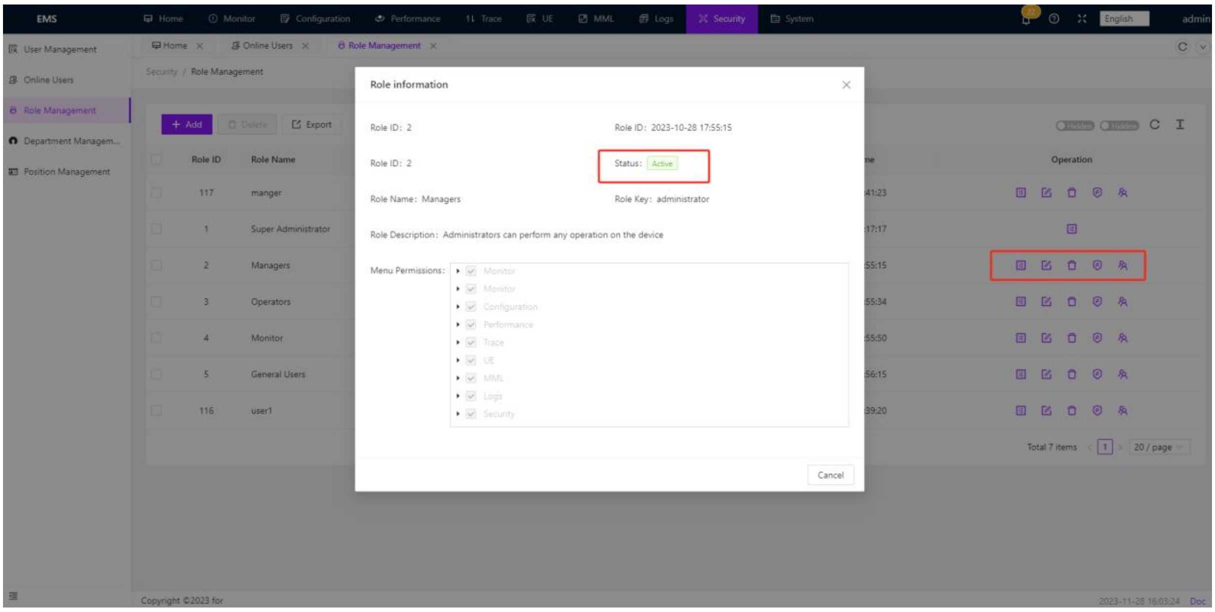
Role Description:

0 / 450

Menu Permissions: ☑ Expand/Collapse ☑ Select all/Deselect all ☑ Father and son linkage

- ☑ Monitor
  - ☑ User Sessions
- ☑ Monitor
  - ☑ Active Alarms
  - ☑ Historical Alarms
  - ☑ Settings
- □ Configuration
  - □ NE Management
  - □ Parameter Configuration

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:



Role information

Role ID: 2

Role ID: 2023-10-28 17:55:15

Role ID: 2

Status: Active

Role Name: Managers

Role Key: administrator

Role Description: Administrators can perform any operation on the device

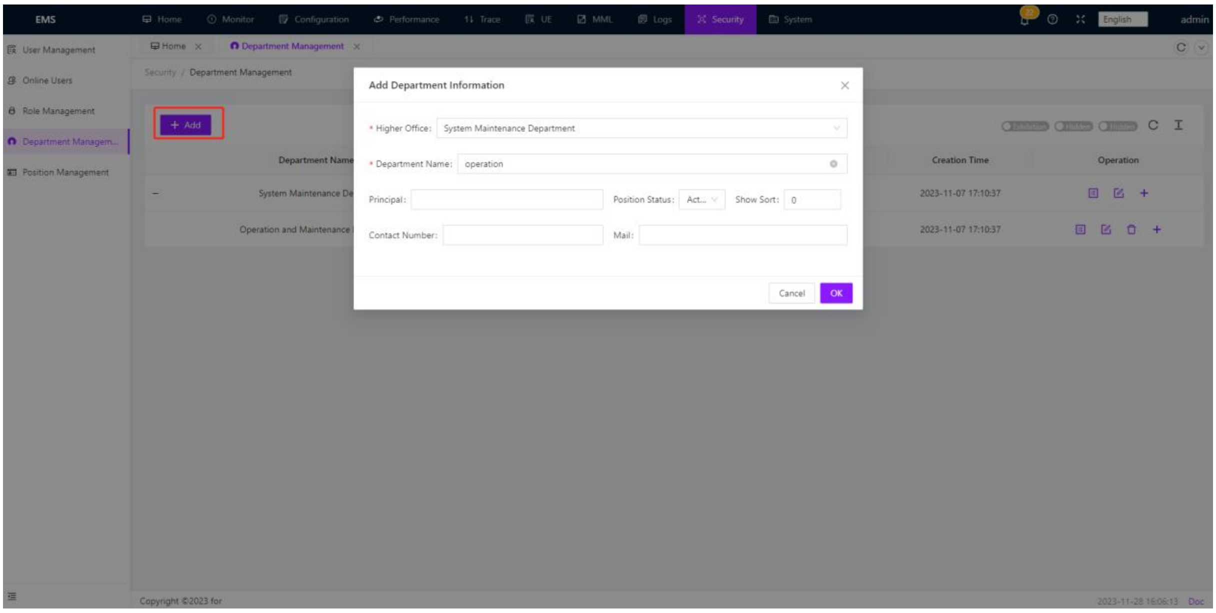
Menu Permissions:
- ☑ Monitor
- ☑ Monitor
- ☑ Configuration
- ☑ Performance
- ☑ Trace
- ☑ UE
- ☑ MML
- ☑ Logs
- ☑ Security

Cancel

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:



Add Department Information

* Higher Office: System Maintenance Department

* Department Name: operation

Principal:

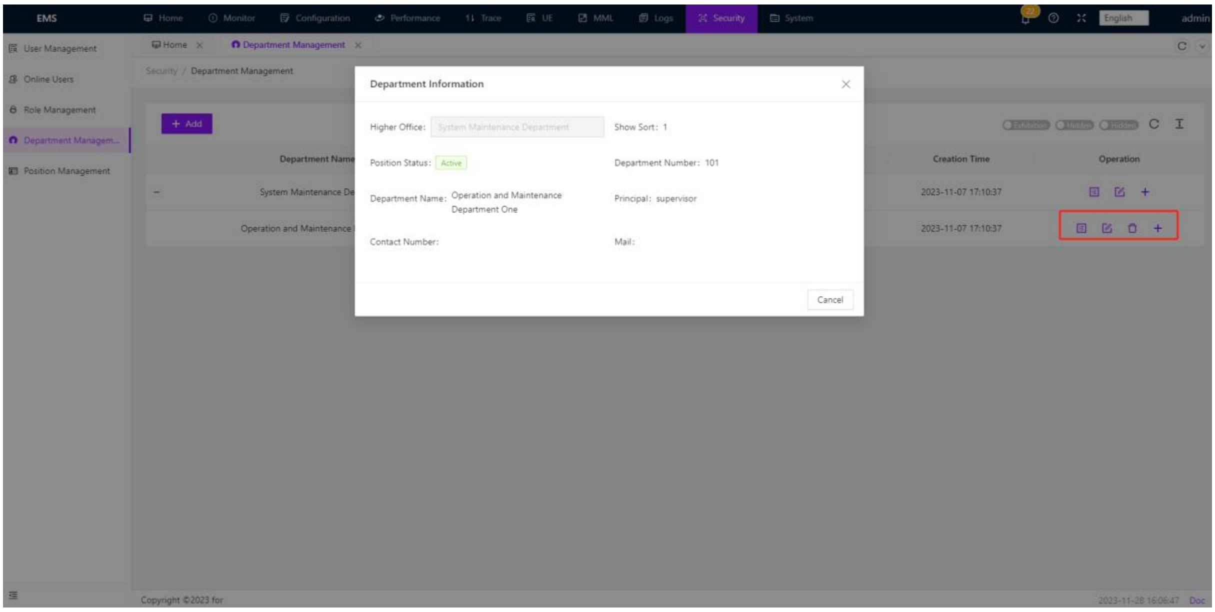
Position Status: Act...

Show Sort: 0

Contact Number:

Mail:

Cancel OK



Department Information

Higher Office: System Maintenance Department
Show Sort: 1
Position Status: Active
Department Number: 101
Department Name: Operation and Maintenance Department One
Principal: supervisor
Contact Number:
Mail:

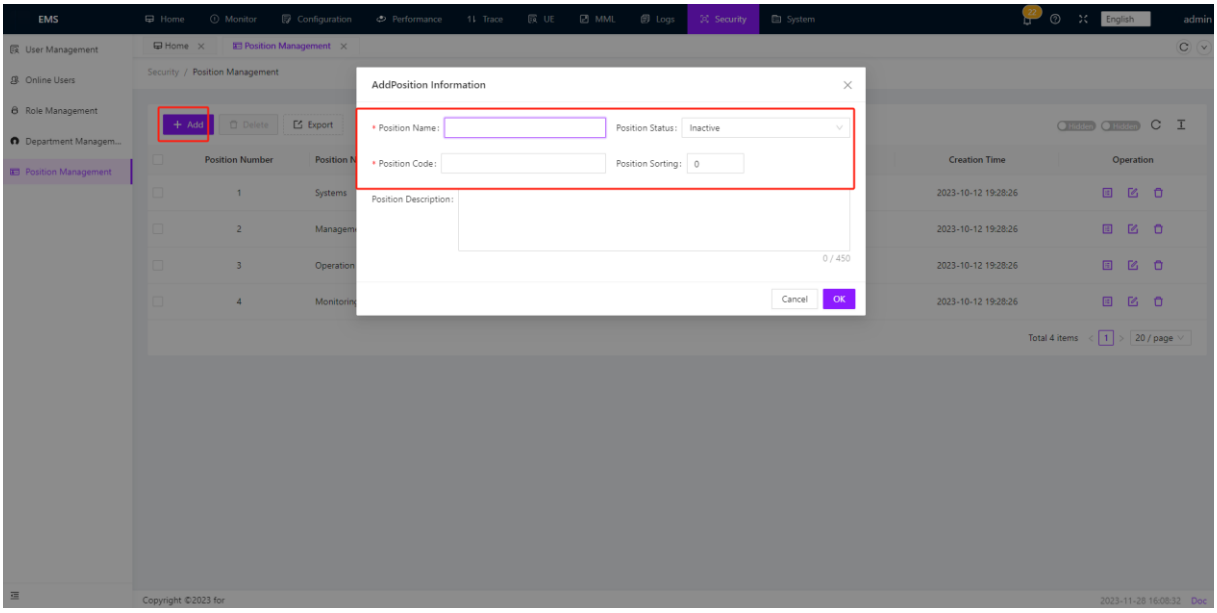
Cancel

Department Name	Creation Time
System Maintenance De	2023-11-07 17:10:37
Operation and Maintenance	2023-11-07 17:10:37

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:



AddPosition Information

* Position Name:
Position Status: Inactive
* Position Code:
Position Sorting: 0
Position Description:
0 / 450

Cancel
OK

Position Number	Position N	Creation Time
1	Systems	2023-10-12 19:28:26
2	Managem	2023-10-12 19:28:26
3	Operation	2023-10-12 19:28:26
4	Monitorin	2023-10-12 19:28:26

Total 4 items 1 20 / page

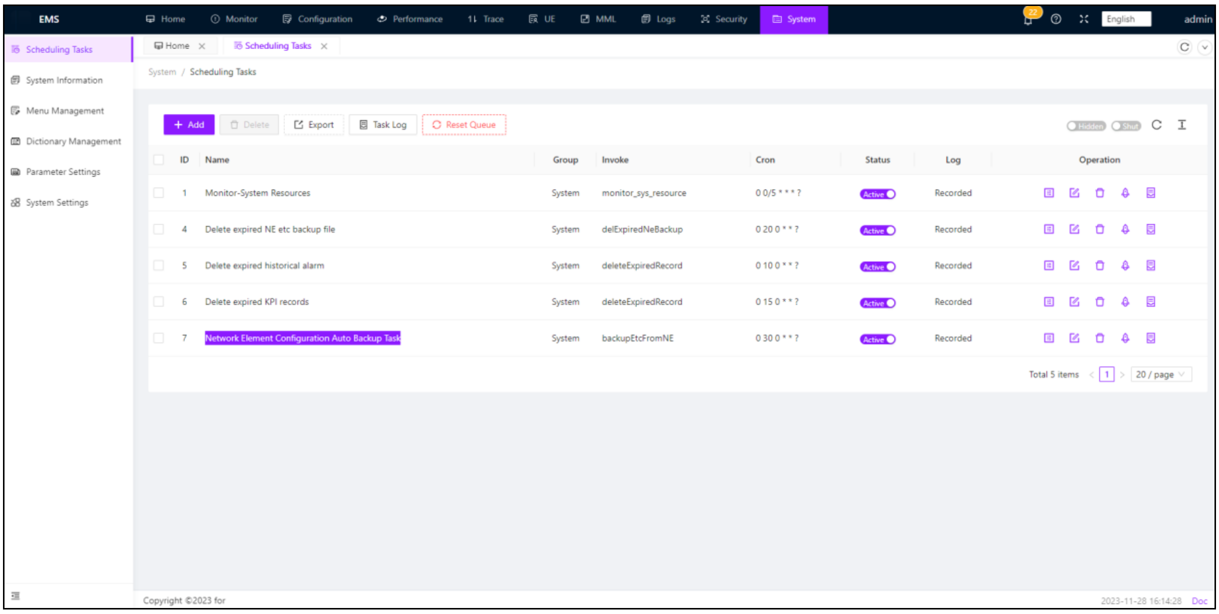
3.11 System

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.

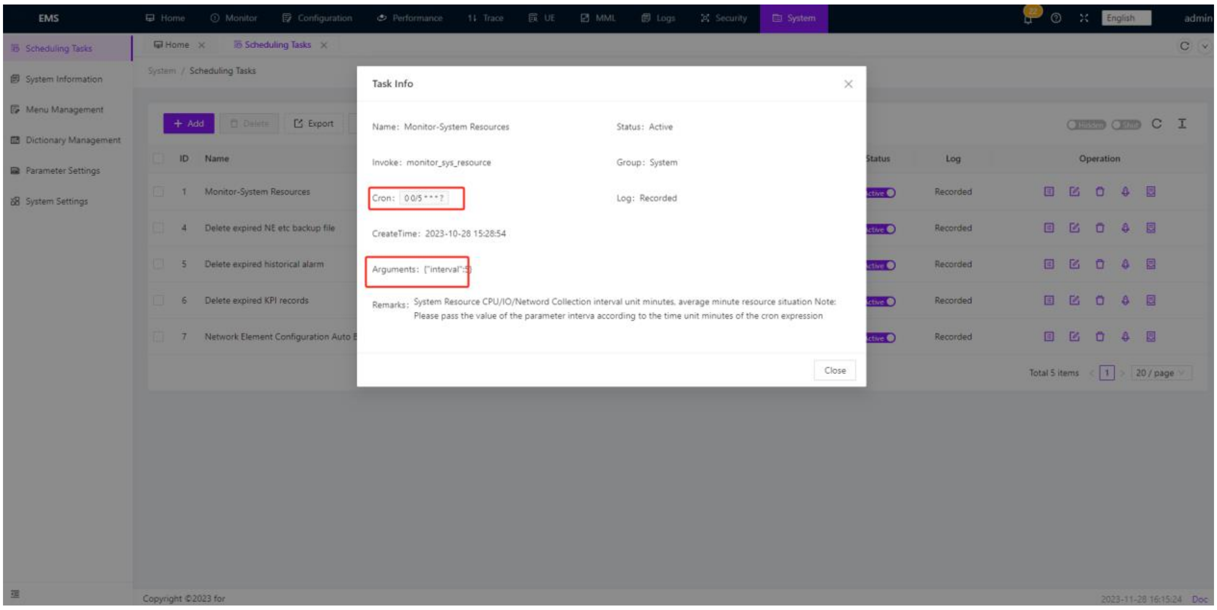
3.11.1 Scheduling Tasks

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.



ID	Name	Group	Invoke	Cron	Status	Log	Operation
1	Monitor-System Resources	System	monitor_sys_resource	0 0/5 * * * ?	Active	Recorded	
4	Delete expired NE etc backup file	System	delExpiredNeBackup	0 20 0 * * ?	Active	Recorded	
5	Delete expired historical alarm	System	deleteExpiredRecord	0 10 0 * * ?	Active	Recorded	
6	Delete expired KPI records	System	deleteExpiredRecord	0 15 0 * * ?	Active	Recorded	
7	Network Element Configuration Auto Backup Task	System	backupEtcFromNE	0 30 0 * * ?	Active	Recorded	

- 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.



Task Info

Name: Monitor-System Resources

Status: Active

Invoke: monitor_sys_resource

Group: System

Cron: 0 0/5 * * * ?

Log: Recorded

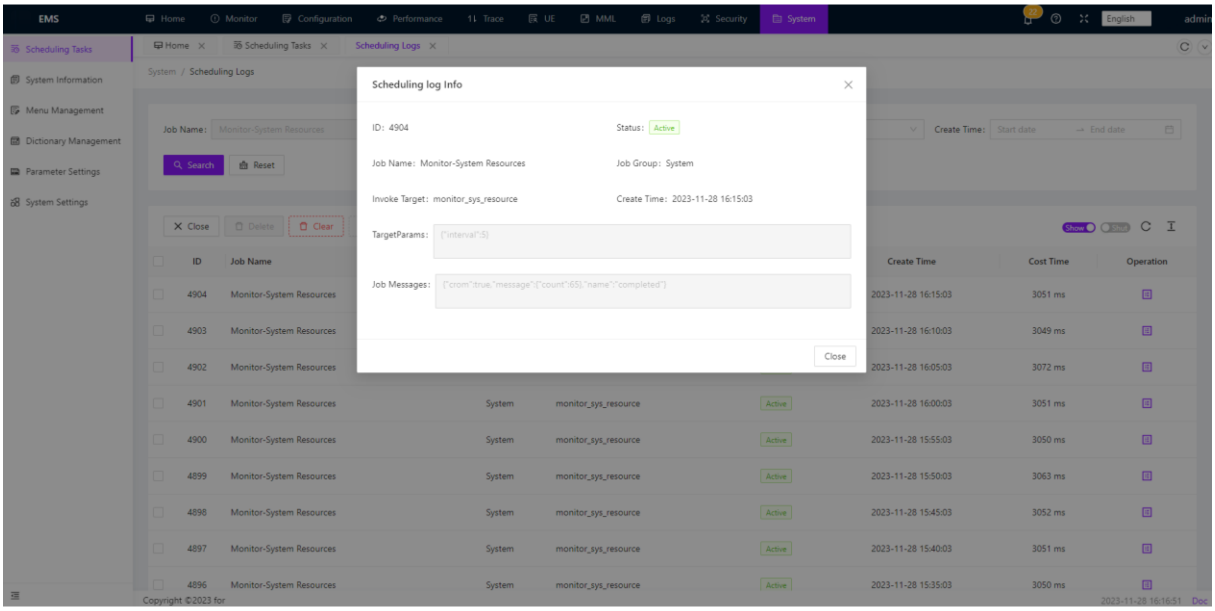
CreateTime: 2023-10-28 15:28:54

Arguments: {"interval":5}

Remarks: System Resource CPU/IO/Netword Collection interval unit minutes, average minute resource situation Note: Please pass the value of the parameter interva according to the time unit minutes of the cron expression

Close

ID	Name	Status	Log	Operation
1	Monitor-System Resources	ctive	Recorded	
4	Delete expired NE etc backup file	ctive	Recorded	
5	Delete expired historical alarm	ctive	Recorded	
6	Delete expired KPI records	ctive	Recorded	
7	Network Element Configuration Auto E	ctive	Recorded	



Job Name: Monitor-System Resources

Create Time: Start date → End date

Scheduling log Info

ID: 4904

Status: Active

Job Name: Monitor-System Resources

Job Group: System

Invoke Target: monitor_sys_resource

Create Time: 2023-11-28 16:15:03

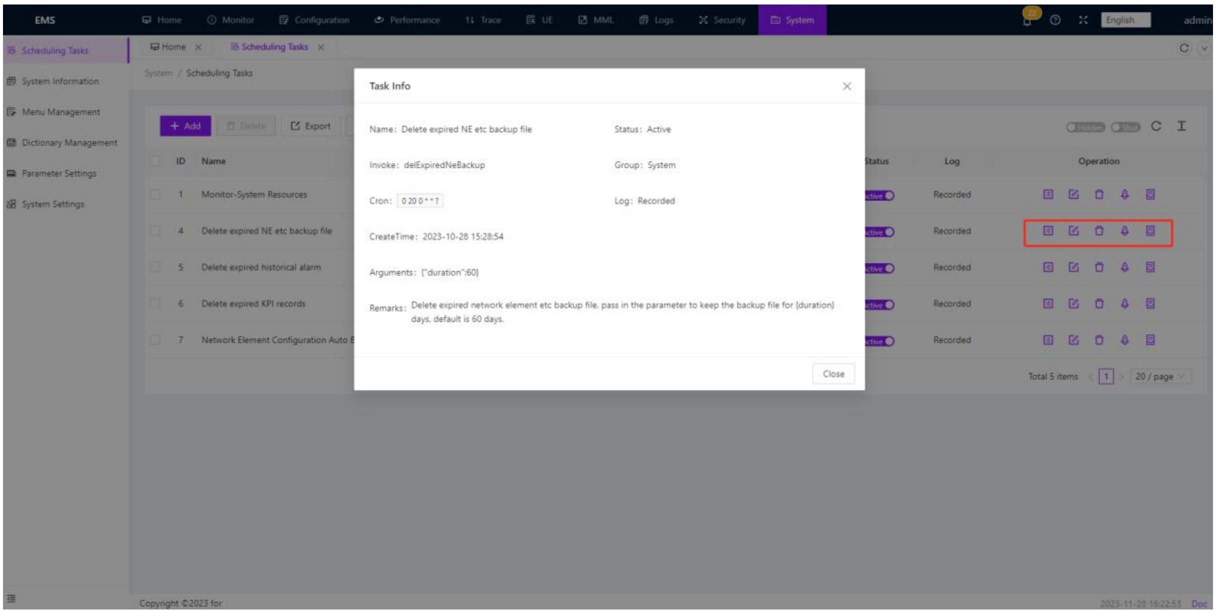
TargetParams: {"interval":5}

Job Messages: {"crom":true,"message":{"count":65},"name":"completed"}

Close

ID	Job Name				Create Time	Cost Time	Operation
4904	Monitor-System Resources				2023-11-28 16:15:03	3051 ms	
4903	Monitor-System Resources				2023-11-28 16:10:03	3049 ms	
4902	Monitor-System Resources				2023-11-28 16:05:03	3072 ms	
4901	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 16:00:03	3051 ms	
4900	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 15:55:03	3050 ms	
4899	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 15:50:03	3063 ms	
4898	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 15:45:03	3052 ms	
4897	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 15:40:03	3051 ms	
4896	Monitor-System Resources	System	monitor_sys_resource	Active	2023-11-28 15:35:03	3050 ms	

- 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



ID	Name	Status	Log
1	Monitor-System Resources	Active	Recorded
4	Delete expired NE etc backup file	Active	Recorded
5	Delete expired historical alarm	Active	Recorded
6	Delete expired KPI records	Active	Recorded
7	Network Element Configuration Auto E	Active	Recorded

Total 5 items 1 20 / page

Task Info

Name：Delete expired NE etc backup file

Status：Active

Invoke：delExpiredNeBackup

Group：System

Cron：0 20 0 * * ?

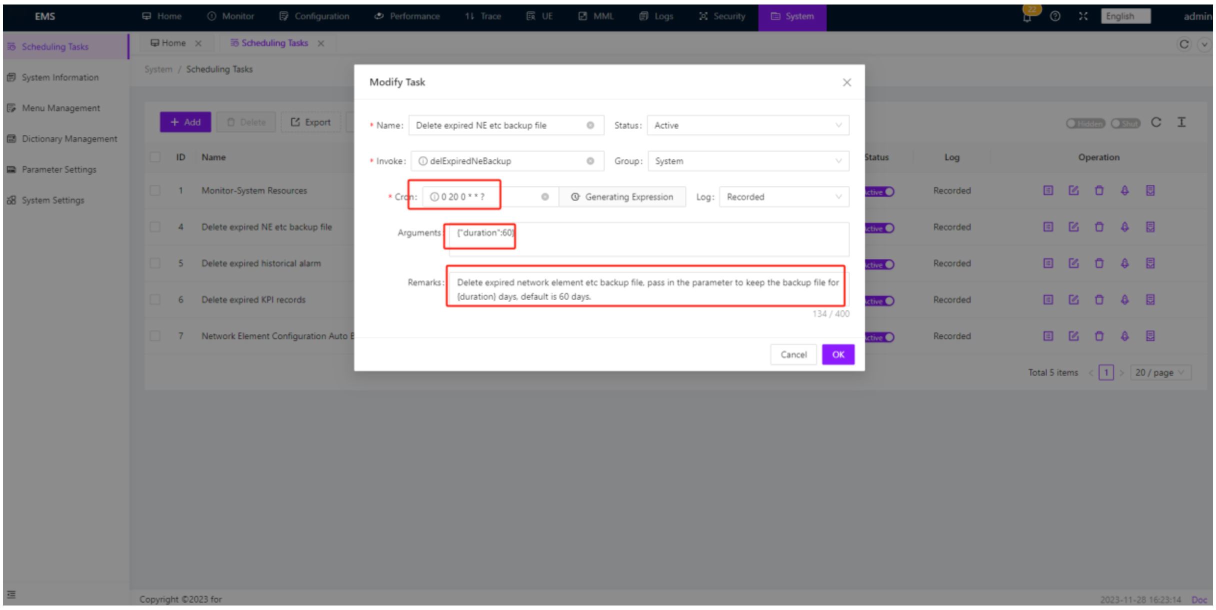
Log：Recorded

CreateTime：2023-10-28 15:28:54

Arguments：{"duration":60}

Remarks：Delete expired network element etc backup file, pass in the parameter to keep the backup file for {duration} days, default is 60 days.

Close



ID	Name	Status	Log
1	Monitor-System Resources	Active	Recorded
4	Delete expired NE etc backup file	Active	Recorded
5	Delete expired historical alarm	Active	Recorded
6	Delete expired KPI records	Active	Recorded
7	Network Element Configuration Auto E	Active	Recorded

Total 5 items 1 20 / page

Modify Task

* Name：Delete expired NE etc backup file

Status：Active

* Invoke：delExpiredNeBackup

Group：System

* Cron：0 20 0 * * ? Generating Expression

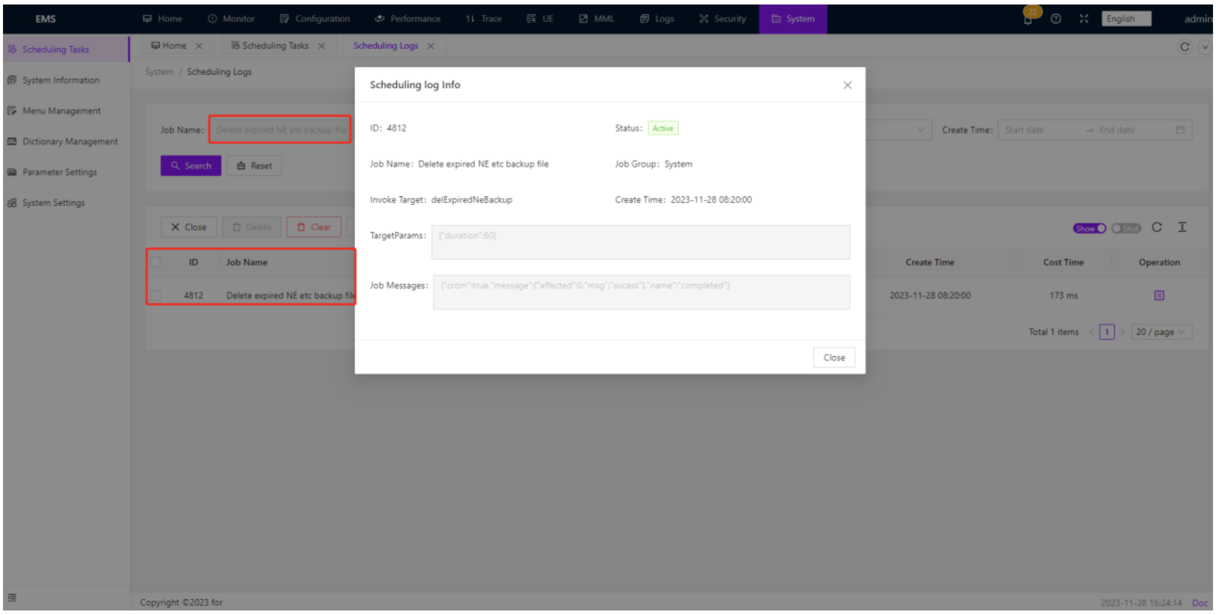
Log：Recorded

Arguments：{"duration":60}

Remarks：Delete expired network element etc backup file, pass in the parameter to keep the backup file for {duration} days, default is 60 days.

134 / 400

Cancel OK



Job Name: Delete expired NE etc backup file

ID	Job Name	Create Time	Cost Time	Operation
4812	Delete expired NE etc backup fil	2023-11-28 08:20:00	173 ms	

Total 1 items 1 20 / page

Scheduling log Info

ID: 4812

Status: Active

Job Name: Delete expired NE etc backup file

Job Group: System

Invoke Target: delExpiredNeBackup

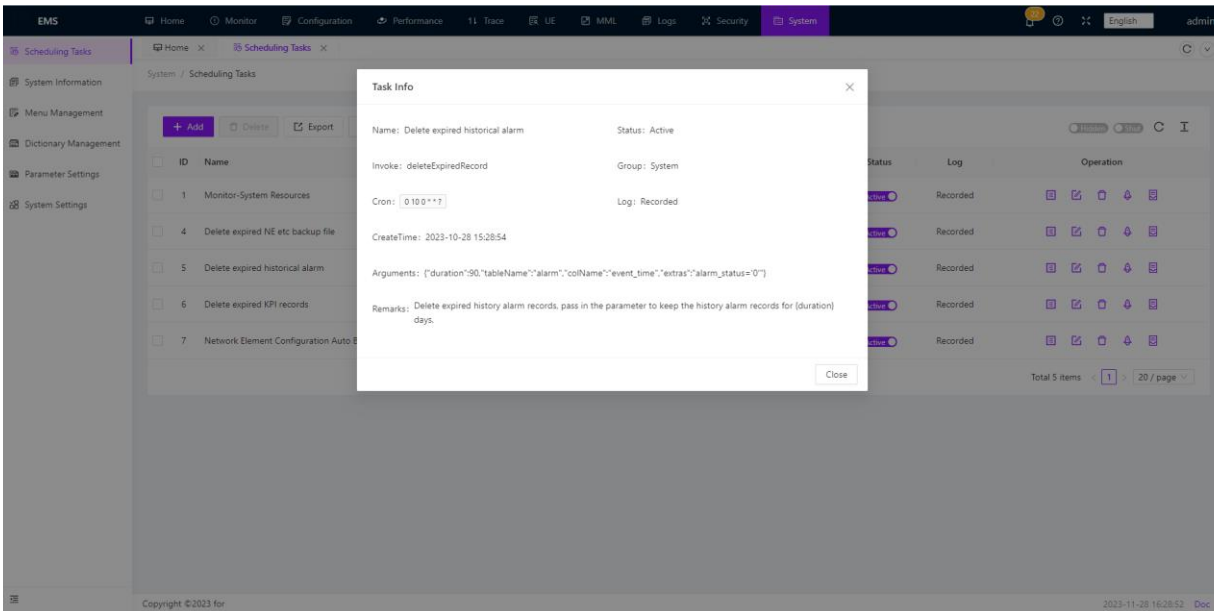
Create Time: 2023-11-28 08:20:00

TargetParams: {"duration":60}

Job Messages: {"crom":true,"message":{"affected":0,"msg":"sucess"},"name":"completed"}

Close

- 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.



ID	Name	Status	Log	Operation
1	Monitor-System Resources	Active	Recorded	
4	Delete expired NE etc backup file	Active	Recorded	
5	Delete expired historical alarm	Active	Recorded	
6	Delete expired KPI records	Active	Recorded	
7	Network Element Configuration Auto E	Active	Recorded	

Total 5 items 1 20 / page

Task Info

Name: Delete expired historical alarm

Status: Active

Invoke: deleteExpiredRecord

Group: System

Cron: 0 10 0 * * ?

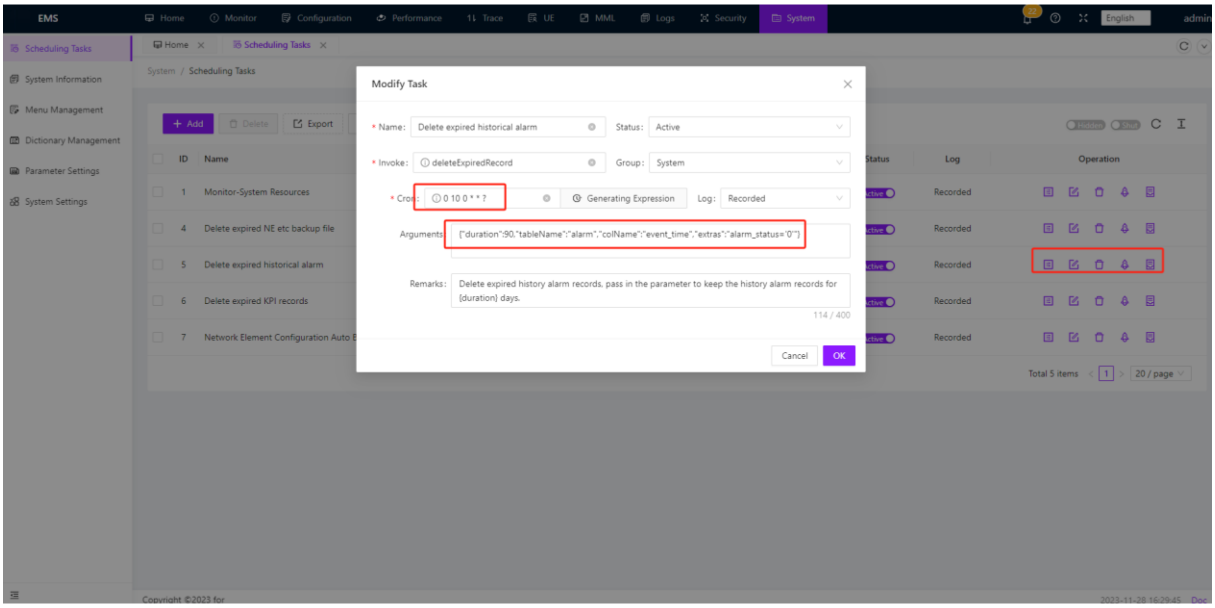
Log: Recorded

CreateTime: 2023-10-28 15:28:54

Arguments: {"duration":90,"tableName":"alarm","colName":"event_time","extras":"alarm_status='0'"}

Remarks: Delete expired history alarm records, pass in the parameter to keep the history alarm records for {duration} days.

Close



Modify Task

* Name: Delete expired historical alarm

Status: Active

* Invoke: deleteExpiredRecord

Group: System

* Cron: 0 10 0 * * ?

Generating Expression

Log: Recorded

Arguments: {"duration":90,"tableName":"alarm","colName":"event_time","extras":"alarm_status='0'"}

Remarks: Delete expired history alarm records, pass in the parameter to keep the history alarm records for {duration} days.

114 / 400

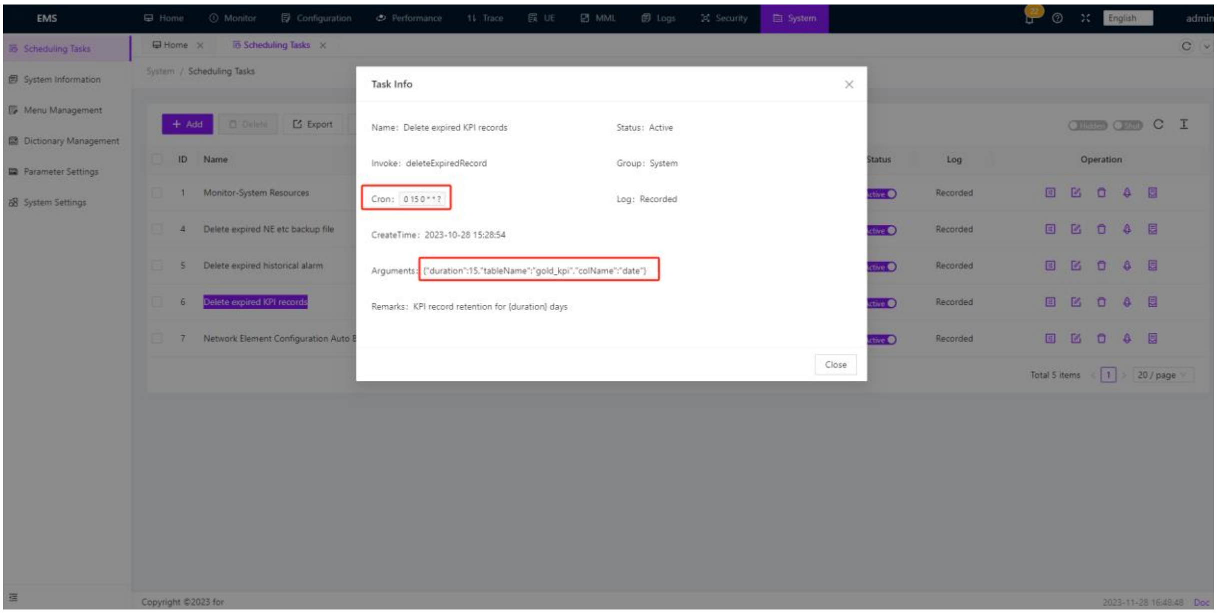
ID	Name	Log
1	Monitor-System Resources	Recorded
4	Delete expired NE etc backup file	Recorded
5	Delete expired historical alarm	Recorded
6	Delete expired KPI records	Recorded
7	Network Element Configuration Auto B	Recorded

Total 5 items 1 20 / page

Copyright ©2023 for

2023-11-28 16:29:45 Doc

- 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.



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"}

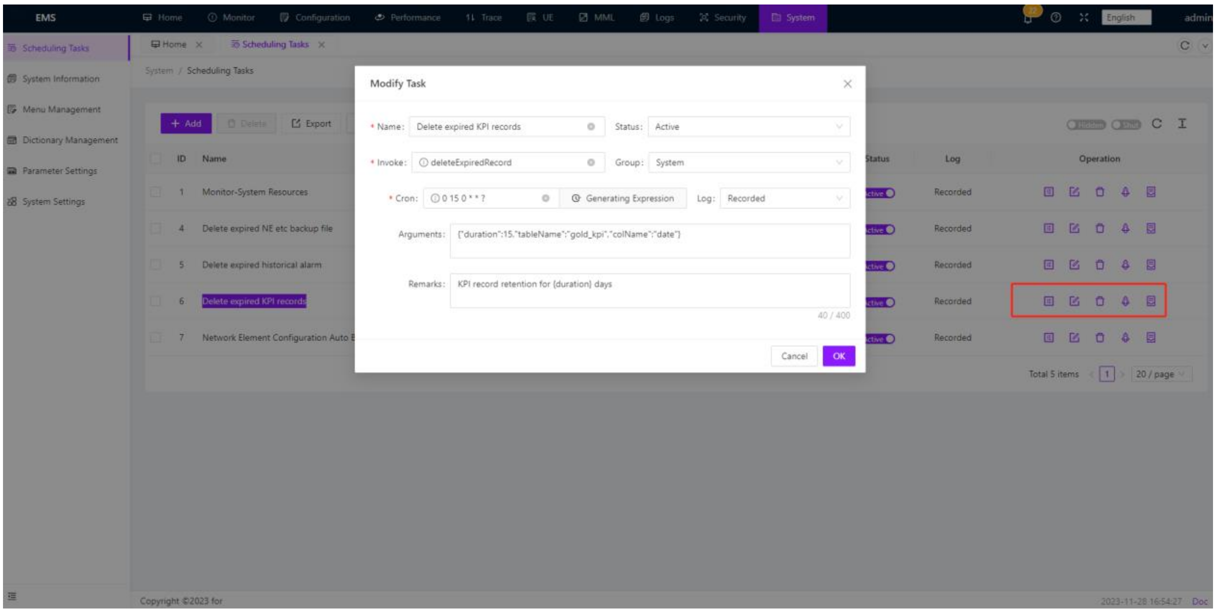
Remarks: KPI record retention for {duration} days

ID	Name	Log
1	Monitor-System Resources	Recorded
4	Delete expired NE etc backup file	Recorded
5	Delete expired historical alarm	Recorded
6	Delete expired KPI records	Recorded
7	Network Element Configuration Auto B	Recorded

Total 5 items 1 20 / page

Copyright ©2023 for

2023-11-28 16:48:48 Doc



ID	Name	Status	Log
1	Monitor-System Resources	Active	Recorded
4	Delete expired NE etc backup file	Active	Recorded
5	Delete expired historical alarm	Active	Recorded
6	Delete expired KPI records	Active	Recorded
7	Network Element Configuration Auto B	Active	Recorded

Total 5 items 1 20 / page

Modify Task

* Name: Delete expired KPI records Status: Active

* Invoke: deleteExpiredRecord Group: System

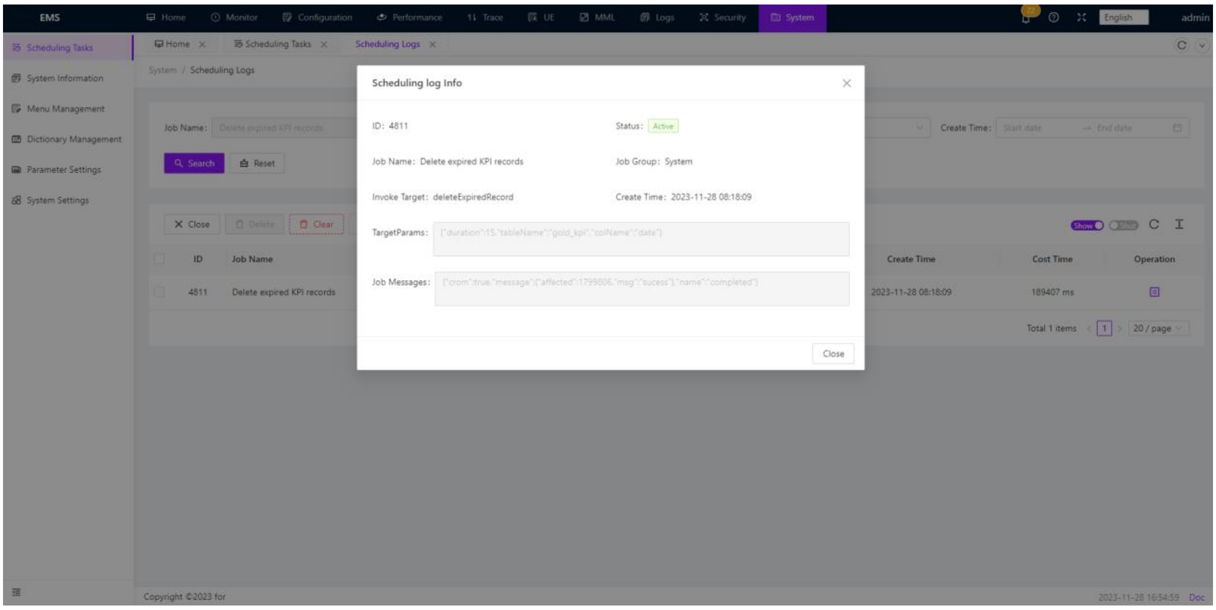
* Cron: 0 15 0 * * ? Generating Expression Log: Recorded

Arguments: {"duration":15,"tableName":"gold_kpi","colName":"date"}

Remarks: KPI record retention for {duration} days

40 / 400

Cancel OK



ID	Job Name	Create Time	Cost Time
4811	Delete expired KPI records	2023-11-28 08:18:09	189407 ms

Total 1 items 1 20 / page

Scheduling log Info

ID: 4811 Status: Active

Job Name: Delete expired KPI records Job Group: System

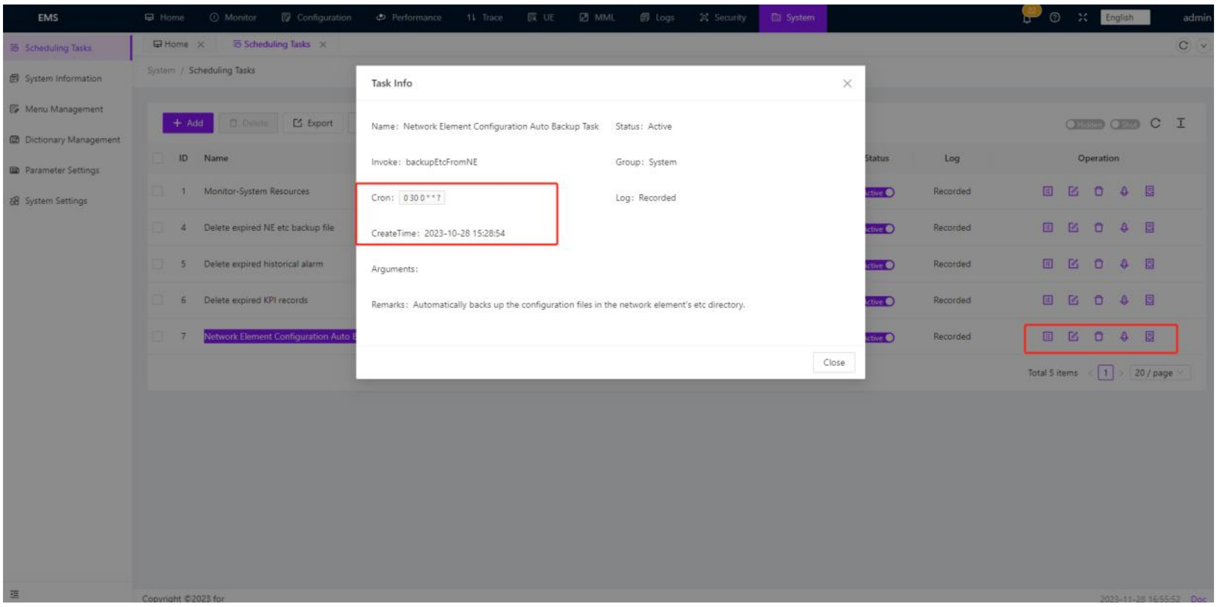
Invoke Target: deleteExpiredRecord Create Time: 2023-11-28 08:18:09

TargetParams: {"duration":15,"tableName":"gold_kpi","colName":"date"}

Job Messages: {"crom":true,"message":{"affected":1799806,"msg":"sucess"},"name":"completed"}

Close

- 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.



Task Info

Name: Network Element Configuration Auto Backup Task

Status: Active

Invoke: backupEtcFromNE

Group: System

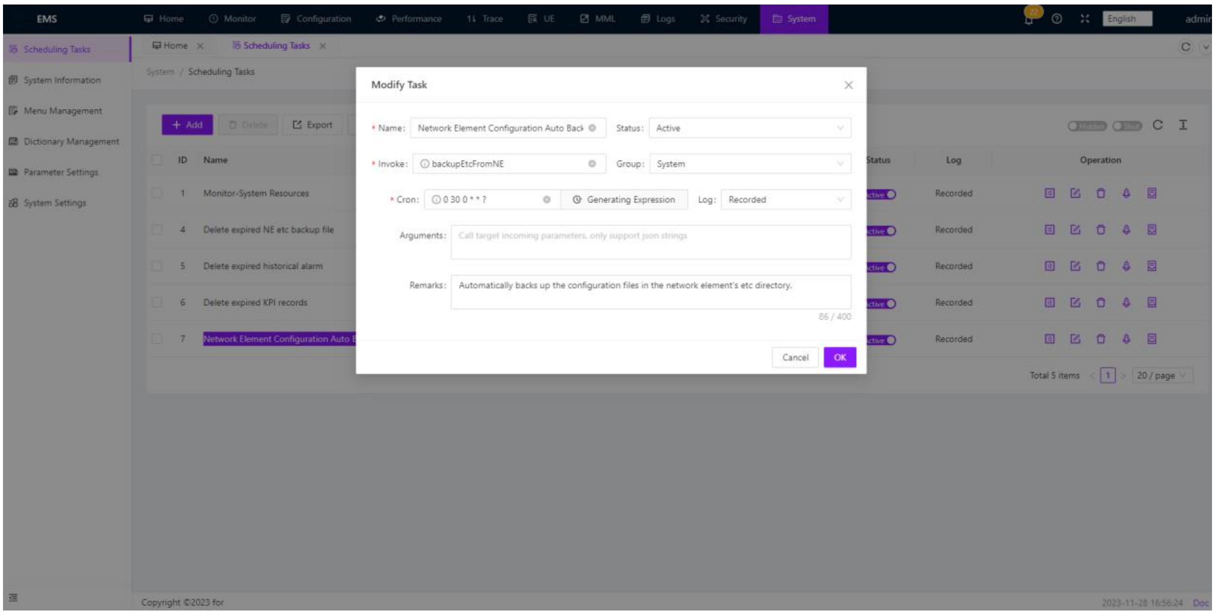
Cron: 0 30 0 * * ?

Log: Recorded

CreateTime: 2023-10-28 15:28:54

Arguments:

Remarks: Automatically backs up the configuration files in the network element's etc directory.



Modify Task

* Name: Network Element Configuration Auto Back

Status: Active

* Invoke: backupEtcFromNE

Group: System

* Cron: 0 30 0 * * ?

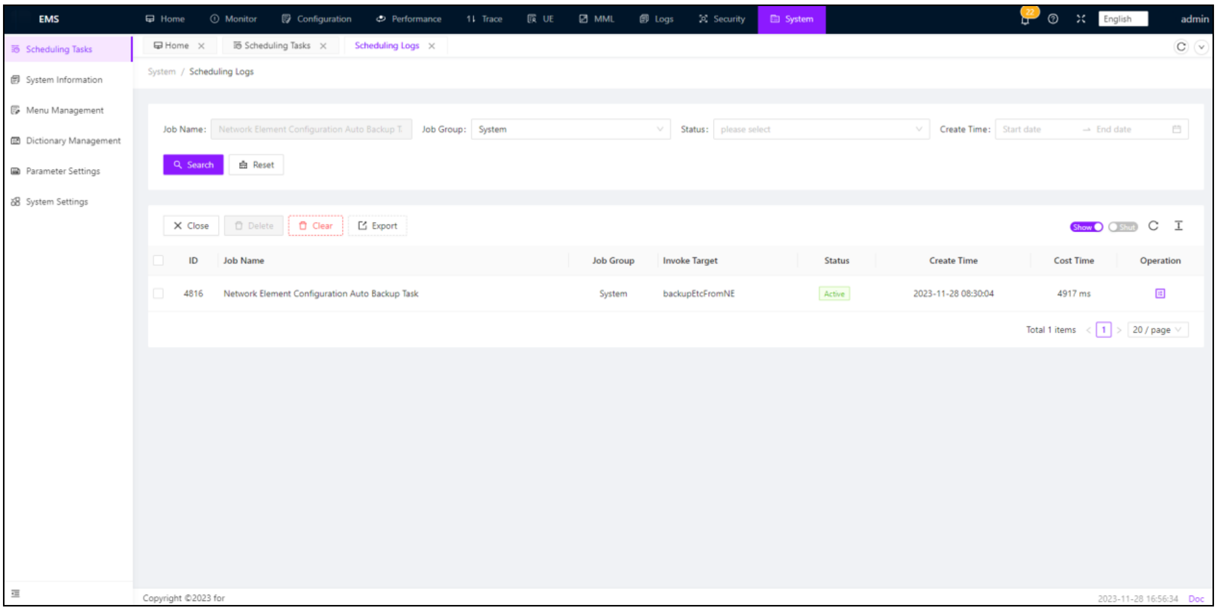
Generating Expression

Log: Recorded

Arguments: Call target incoming parameters, only support json strings

Remarks: Automatically backs up the configuration files in the network element's etc directory.

86 / 400



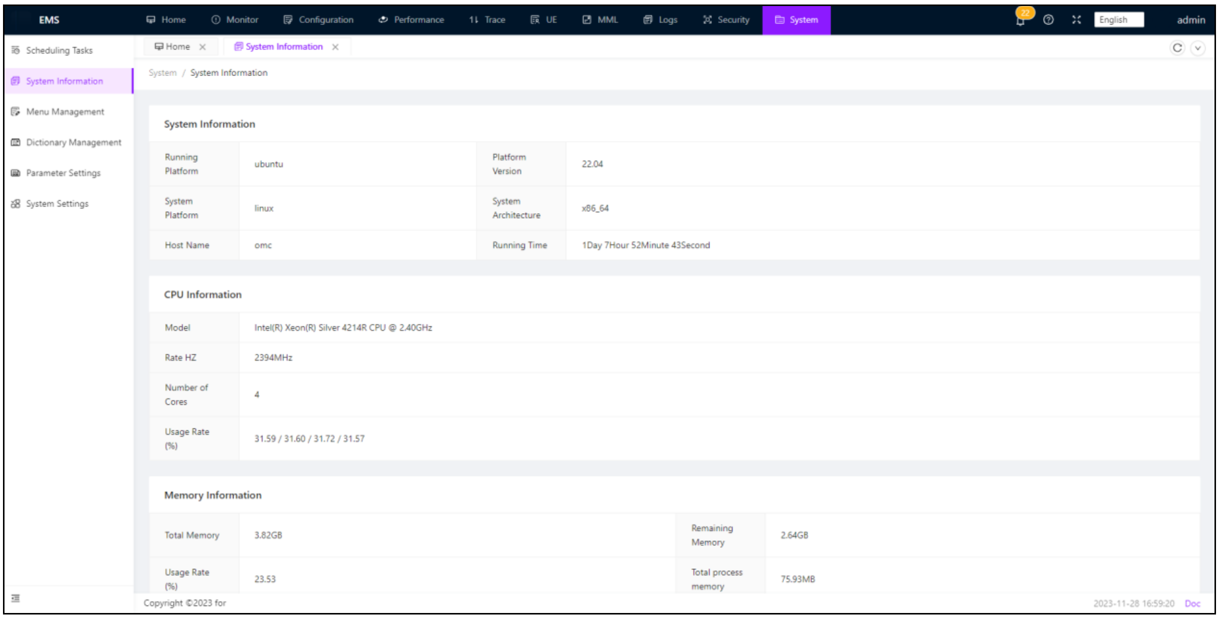
Job Name: Network Element Configuration Auto Backup T Job Group: System Status: please select Create Time: Start date → End date

ID	Job Name	Job Group	Invoke Target	Status	Create Time	Cost Time	Operation
4816	Network Element Configuration Auto Backup Task	System	backupEtcFromNE	Active	2023-11-28 08:30:04	4917 ms	

Total 1 items < 1 > 20 / page

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.



System Information

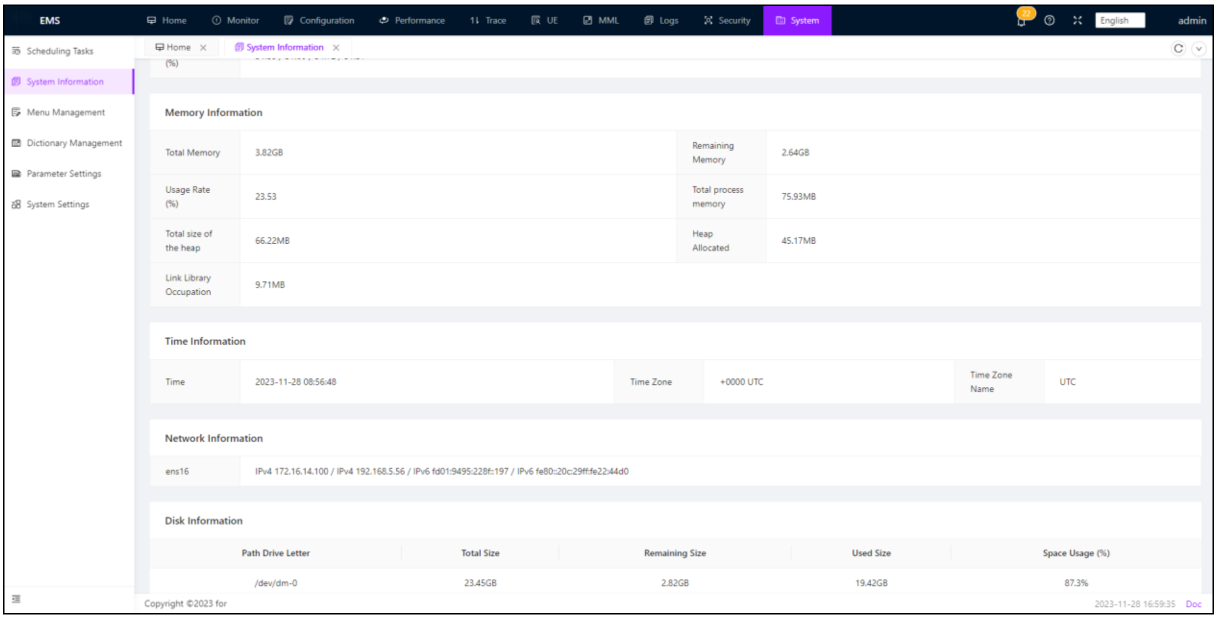
Running Platform	ubuntu	Platform Version	22.04
System Platform	linux	System Architecture	x86_64
Host Name	omc	Running Time	1Day 7Hour 52Minute 43Second

CPU Information

Model	Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz
Rate HZ	2394MHz
Number of Cores	4
Usage Rate (%)	31.59 / 31.60 / 31.72 / 31.57

Memory Information

Total Memory	3.82GB	Remaining Memory	2.64GB
Usage Rate (%)	23.53	Total process memory	75.93MB



(%)

Memory Information

Total Memory	3.82GB	Remaining Memory	2.64GB
Usage Rate (%)	23.53	Total process memory	75.93MB
Total size of the heap	66.22MB	Heap Allocated	45.17MB
Link Library Occupation	9.71MB		

Time Information

Time	2023-11-28 08:56:48	Time Zone	+0000 UTC	Time Zone Name	UTC

Network Information

ens16	IPv4 172.16.14.100 / IPv4 192.168.5.56 / IPv6 fd01:9495:228f::197 / IPv6 fe80::20c:29ff:fe22:44d0

Disk Information

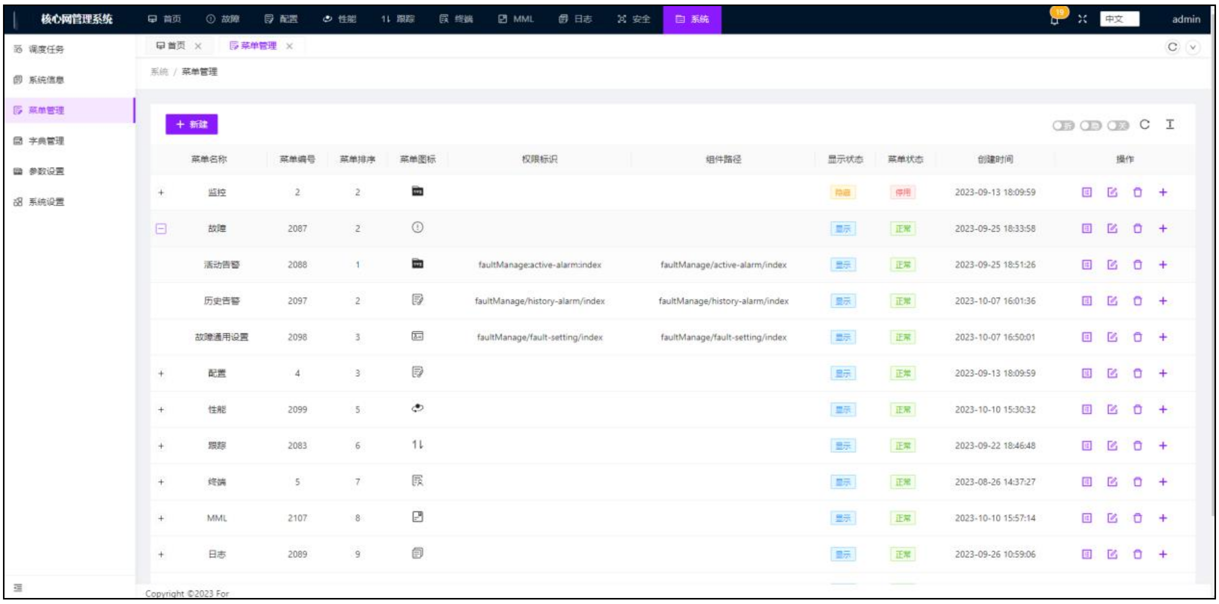
Path Drive Letter	Total Size	Remaining Size	Used Size	Space Usage (%)
/dev/dm-0	23.45GB	2.82GB	19.42GB	87.3%

Copyright ©2023 for

2023-11-28 16:59:35 Doc

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.



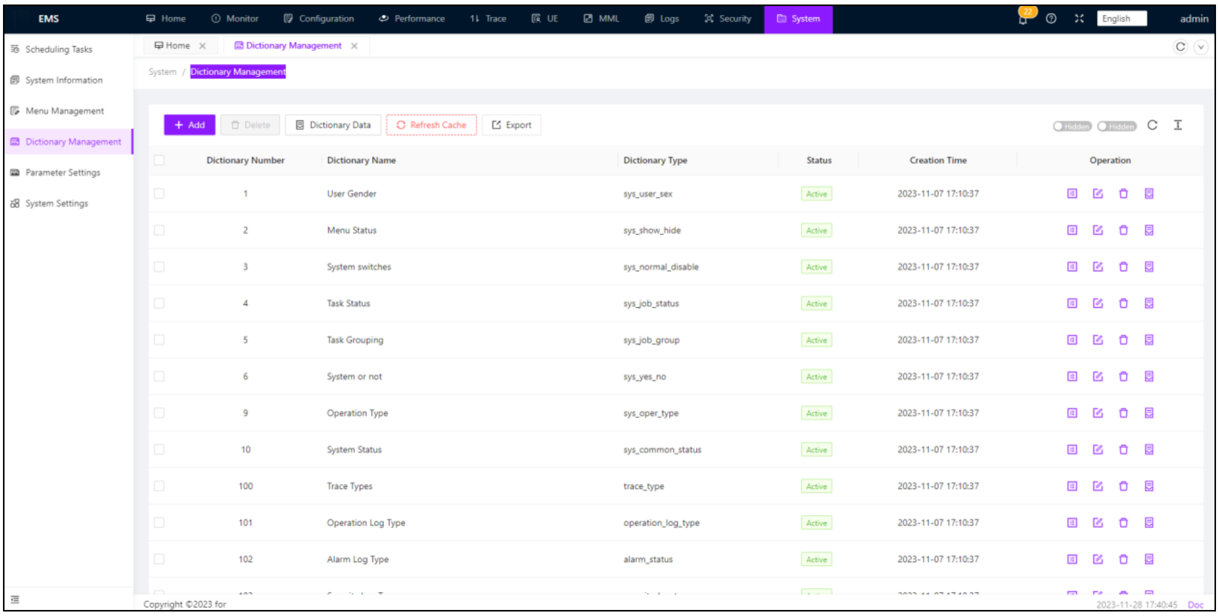
系统 / 菜单管理

	菜单名称	菜单编号	菜单排序	菜单图标	权限标识	组件路径	显示状态	菜单状态	创建时间	操作
+	监控	2	2				隐藏	停用	2023-09-13 18:09:59	
−	故障	2087	2				显示	正常	2023-09-25 18:33:58	
	活动告警	2088	1		faultManage:active-alarm:index	faultManage/active-alarm/index	显示	正常	2023-09-25 18:51:26	
	历史告警	2097	2		faultManage/history-alarm/index	faultManage/history-alarm/index	显示	正常	2023-10-07 16:01:36	
	故障通用设置	2098	3		faultManage/fault-setting/index	faultManage/fault-setting/index	显示	正常	2023-10-07 16:50:01	
+	配置	4	3				显示	正常	2023-09-13 18:09:59	
+	性能	2099	5				显示	正常	2023-10-10 15:30:32	
+	跟踪	2083	6				显示	正常	2023-09-22 18:46:48	
+	终端	5	7				显示	正常	2023-08-26 14:37:27	
+	MML	2107	8				显示	正常	2023-10-10 15:57:14	
+	日志	2089	9				显示	正常	2023-09-26 10:59:06	

Copyright ©2023 For

3.11.4 Dictionary Management

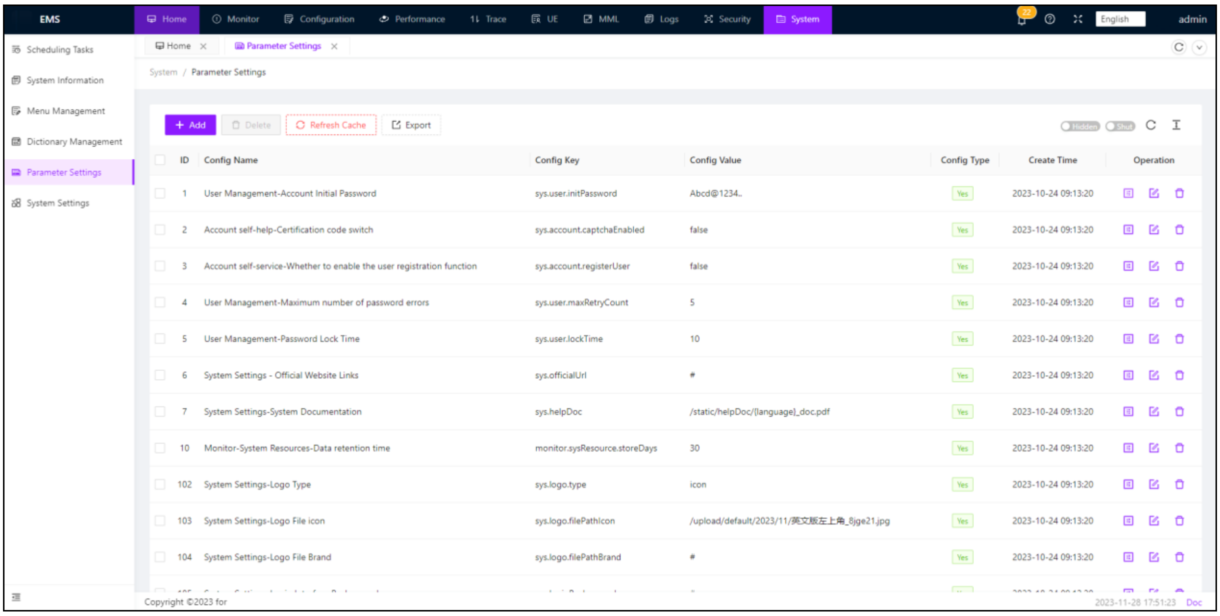
Dictionary management is used to manage dictionary data in the core network system. Administrators can add, modify, and delete dictionary data to ensure the accuracy and consistency of data in the core network system. Dictionary management can also help to realize the classification and standardization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



Dictionary Number	Dictionary Name	Dictionary Type	Status	Creation Time
1	User Gender	sys_user_sex	Active	2023-11-07 17:10:37
2	Menu Status	sys_show_hide	Active	2023-11-07 17:10:37
3	System switches	sys_normal_disable	Active	2023-11-07 17:10:37
4	Task Status	sys_job_status	Active	2023-11-07 17:10:37
5	Task Grouping	sys_job_group	Active	2023-11-07 17:10:37
6	System or not	sys_yes_no	Active	2023-11-07 17:10:37
9	Operation Type	sys_oper_type	Active	2023-11-07 17:10:37
10	System Status	sys_common_status	Active	2023-11-07 17:10:37
100	Trace Types	trace_type	Active	2023-11-07 17:10:37
101	Operation Log Type	operation_log_type	Active	2023-11-07 17:10:37
102	Alarm Log Type	alarm_status	Active	2023-11-07 17:10:37

3.11.5 Parameter Settings

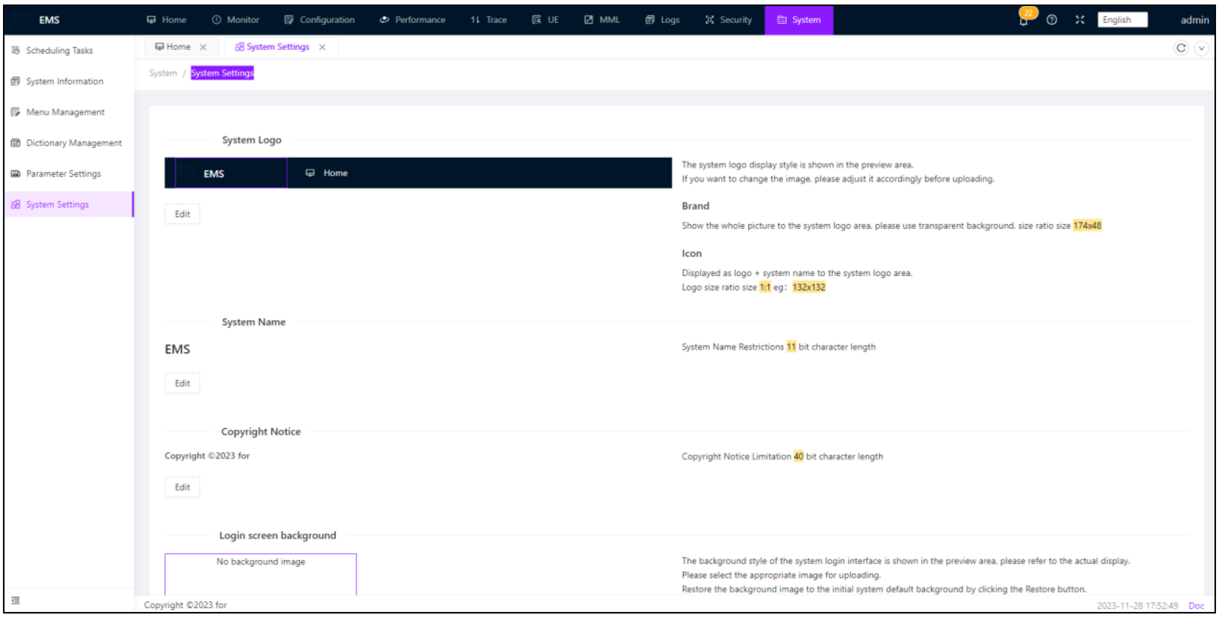
Parameter Settings allow the administrator to configure and adjust parameters of the core network system. These parameters can affect the functional performance and performance of the system. Administrators can adjust the parameters based on actual requirements to optimize system running and meet service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



□	ID	Config Name	Config Key	Config Value	Config Type	Create Time	Operation
□	1	User Management-Account Initial Password	sys.user.initPassword	Abcd@1234..	Yes	2023-10-24 09:13:20	
□	2	Account self-help-Certification code switch	sys.account.captchaEnabled	false	Yes	2023-10-24 09:13:20	
□	3	Account self-service-Whether to enable the user registration function	sys.account.registerUser	false	Yes	2023-10-24 09:13:20	
□	4	User Management-Maximum number of password errors	sys.user.maxRetryCount	5	Yes	2023-10-24 09:13:20	
□	5	User Management-Password Lock Time	sys.user.lockTime	10	Yes	2023-10-24 09:13:20	
□	6	System Settings - Official Website Links	sys.officialUrl	#	Yes	2023-10-24 09:13:20	
□	7	System Settings-System Documentation	sys.helpDoc	/static/helpDoc/{language}_doc.pdf	Yes	2023-10-24 09:13:20	
□	10	Monitor-System Resources-Data retention time	monitor.sysResource.storeDays	30	Yes	2023-10-24 09:13:20	
□	102	System Settings-Logo Type	sys.logo.type	icon	Yes	2023-10-24 09:13:20	
□	103	System Settings-Logo File icon	sys.logo.filePathIcon	/upload/default/2023/11/英文版左上角_8jge21.jpg	Yes	2023-10-24 09:13:20	
□	104	System Settings-Logo File Brand	sys.logo.filePathBrand	#	Yes	2023-10-24 09:13:20	

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.



System Logo

The system logo display style is shown in the preview area.
If you want to change the image, please adjust it accordingly before uploading.

Brand

Show the whole picture to the system logo area, please use transparent background, size ratio size 174x48

Icon

Displayed as logo + system name to the system logo area.
Logo size ratio size 1:1 eg: 132x132

System Name

EMS

System Name Restrictions 11 bit character length

Copyright Notice

Copyright ©2023 for

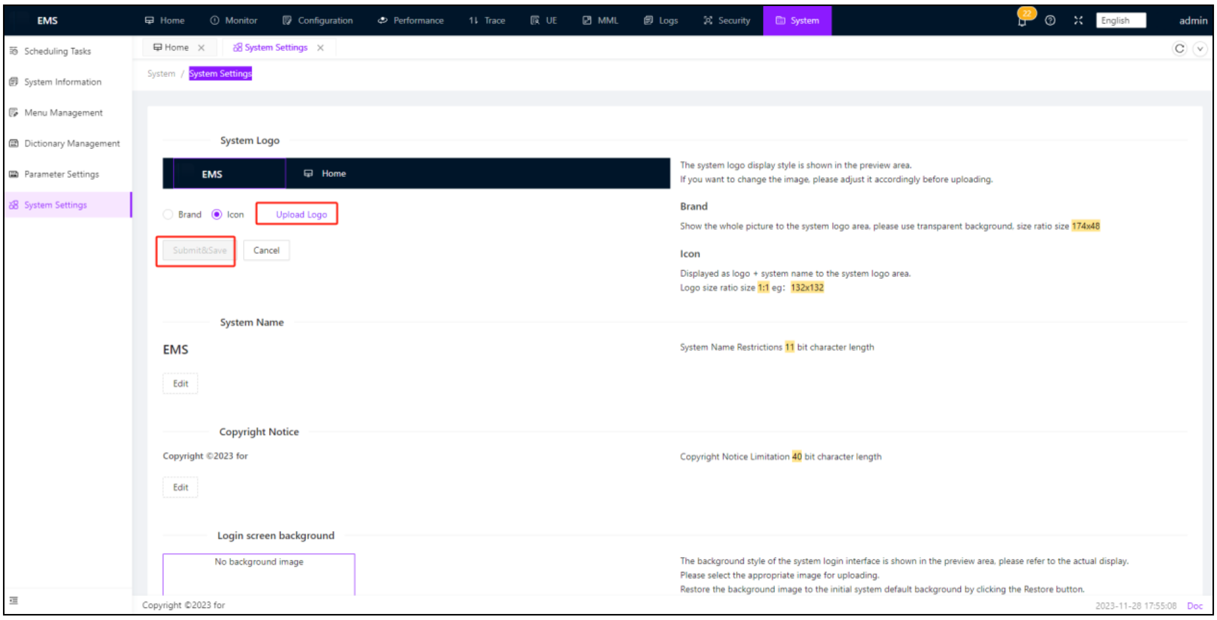
Copyright Notice Limitation 40 bit character length

Login screen background

No background image

The background style of the system login interface is shown in the preview area, please refer to the actual display.
Please select the appropriate image for uploading.
Restore the background image to the initial system default background by clicking the Restore button.

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



System Logo

The system logo display style is shown in the preview area.
If you want to change the image, please adjust it accordingly before uploading.

Brand

Show the whole picture to the system logo area, please use transparent background, size ratio size 174x48

Icon

Displayed as logo + system name to the system logo area.
Logo size ratio size 1:1 eg: 132x132

System Name

EMS

System Name Restrictions 11 bit character length

Copyright Notice

Copyright ©2023 for

Copyright Notice Limitation 40 bit character length

Login screen background

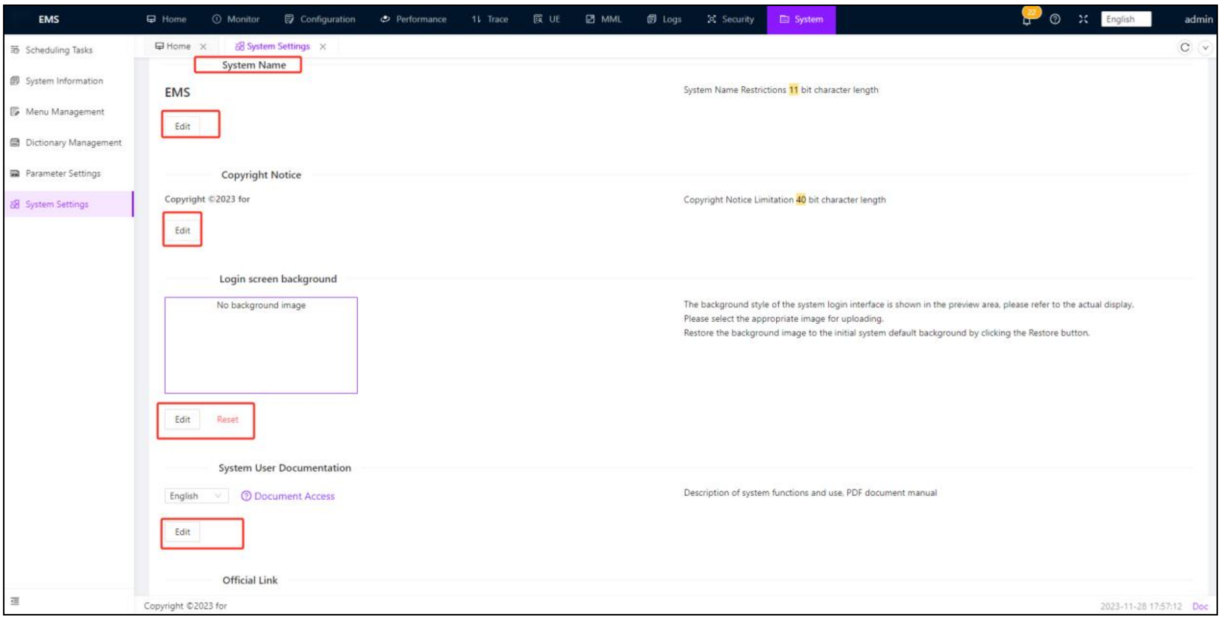
No background image

The background style of the system login interface is shown in the preview area, please refer to the actual display.
Please select the appropriate image for uploading.
Restore the background image to the initial system default background by clicking the Restore button.

Copyright ©2023 for

2023-11-28 17:55:08

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:



System Name

EMS

System Name Restrictions 11 bit character length

Copyright Notice

Copyright ©2023 for

Copyright Notice Limitation 40 bit character length

Login screen background

No background image

The background style of the system login interface is shown in the preview area, please refer to the actual display.
Please select the appropriate image for uploading.
Restore the background image to the initial system default background by clicking the Restore button.

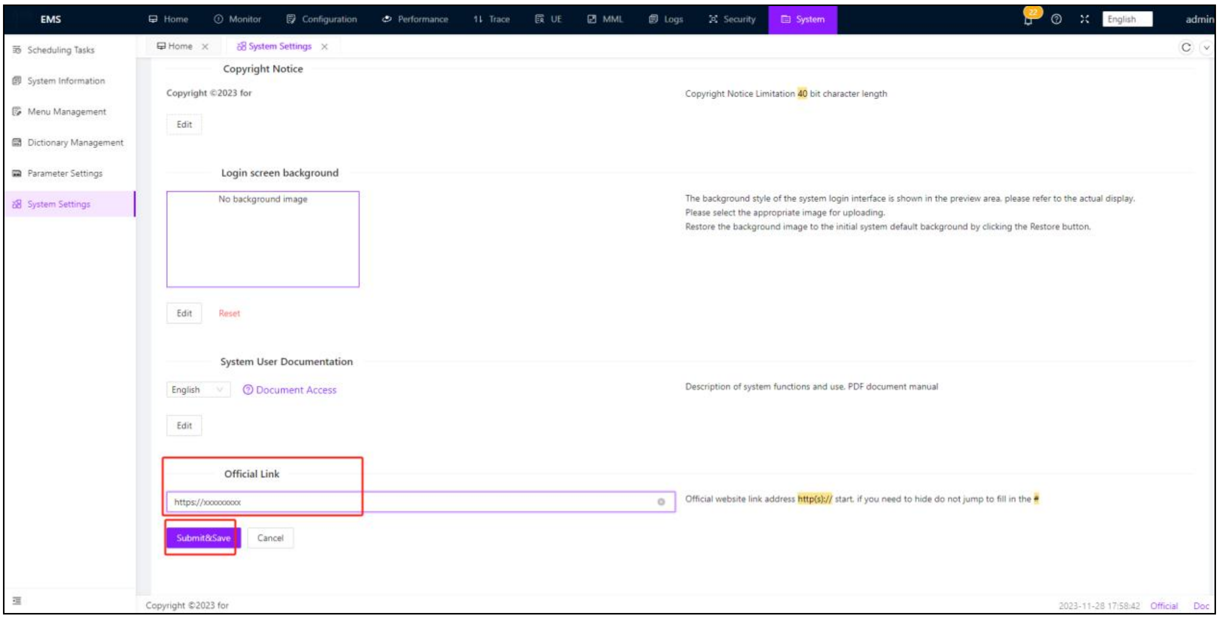
System User Documentation

Description of system functions and use, PDF document manual

Official Link

Copyright ©2023 for

2023-11-28 17:57:12



Copyright Notice

Copyright ©2023 for

Copyright Notice Limitation 40 bit character length

Login screen background

No background image

The background style of the system login interface is shown in the preview area. please refer to the actual display.
Please select the appropriate image for uploading.
Restore the background image to the initial system default background by clicking the Restore button.

System User Documentation

English

Document Access

Description of system functions and use. PDF document manual

Official Link

https://xxxxxxxxx

Official website link address http(s):// start. if you need to hide do not jump to fill in the #

Copyright ©2023 for

2023-11-28 17:58:42

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	Check if the OAM configuration switch on the

	added successfully	network element side is turned on
3	Core network function configuration operation	Refer to 5GC maintenance manual

7 Copyright Statement

This manual is the intellectual property of our company and is protected by law. No individual or company may engage in illegal piracy. The core network software products described in the manual are the intellectual property of our company and are protected by law. No individual or company may engage in illegal piracy and use.