Application Service Series

Recording Management System

Administrator's Manual

Document Version: 01

Release Date: 2025-01-06

Copyright © 2025 New Rock Technologies, Inc. All Rights Reserved.

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

New Rock Technologies, Inc

Website: en.newrocktech.com

Email: global@newrocktech.com

Contents

Contents 1
Contents of Figures 3
Contents of Tables 6
Modifying Record 8
1. Preamble 9
1.1 About this Manual 9
1.2 Document Users 9
2. Products 10
2.1 Product positioning 10
2.2 System Features 10
3. Application Scenario 12
4. NewLync-AS Series Software Deployment 14
4.1 Pre-Installation Environment Configuration 14
4.1.1 List of Files Required for Installation 15
4.1.2 Create User Accounts 15
4.1.3 Granting sudo privileges to users 16
4.2 Installing NewLync-AS (Single-Machine Deployment) 17
4.3 Install NewLync-AS (Dual-Server Deployment) 19
4.4 Firewall Configuration 21
4.5 Accessing and Logging into the Management System Platform 23
4.6 Add Recording Node 24
4.7 Configure OM Remote Recording 25
4.8 Import License 28
4.9 AS Series License Features Overview 30

4.10 Function Comparison Table 33

5. Configuring AS 34

5.1 Organizational structure 34

5.1.1 Membership and sectors 34

5.2 Enterprise Settings 39

5.2.1 Corporate Information 39

5.2.2 Administrative authority 40

6. Recording Management 44

6.1 Recording Inquiry 44

6.2 Recording settings 50

6.3 Operation Log Management 53

6.4 Statistical analysis interface 55

7. Alerts 61

7.1 Alarm Log 61

7.2 Alarm settings 61

8. System settings 63

8.1 Device Management Interface 63

8.2 Recording Configuration 68

8.3 Authorization Information 76

8.4 Data Maintenance 78

8.5 System settings 79

8.6 Recording Node Functionality 80

9. Appendices 82

9.1 Communications Matrix 82

9.2 Glossary 84

9.3 Common Problems 85

Contents of Figures

Figure 1 AS management system login screen....24
Figure 2 Add Recording Node....25
Figure 3 Add OM device....26
Figure 4 Configure OM Remote Recording....27
Figure 5 Configure OM Remote Recording 2....27
Figure 6 Getting the License Request File....28
Figure 7 Import License....29
Figure 8 Checking License Status....30
Figure 9 AS Trial License Interface....31
Figure 10 New sectors....34
Figure 11 Setting up department heads....35
Figure 12 Editorial office....35
Figure 13 Import Export Members....36
Figure 14 Import Export Members....36
Figure 15 Download Template....36
Figure 16 Uploading departmental information....37
Figure 17 Download Template....37
Figure 18 Adding Members....38

Figure 19 Modify member information....38

Figure 20 Modify basic enterprise information....39

Figure 21 Transfer creator....41

Figure 22 Add Super Administrator....41

Figure 23 Add Administrator....42

Figure 24 Edit Administrator Privileges....43

Figure 25 Recording query interface....44

Figure 26 Steps to download all data....45

Figure 27 Exporting query data....46

Figure 28 Filter more search criteria....46

Figure 29 Query recording management details....47

Figure 30 Whitelist editing screen....52

Figure 31 Whitelist List....53

Figure 32 Operation log query....53

Figure 33 Detailed statistical data table....57

Figure 34 Pie Figure presentation....58

Figure 35 Selection of statistical dimensions graph....59

Figure 36 Customized Report Statistical Analysis Figure....59

Figure 37 Filter screen with more conditions....60

Figure 38 Alarm log interface....61

Figure 39 Alarm Event Settings....62

Figure 40 Sending Mail Settings 62

Figure 41 Device management interface 63

Figure 42 Edit device operation interface 64

Figure 43 Device management editing interface 66

Figure 44 Device management interface 66

Figure 45 Add Device 67

Figure 46 Add application Interface 68

Figure 47 Add Node Interface 69

Figure 48 Add Device Interface 70

Figure 49 Add OMX Device Interface 72

Figure 50 Enable Remote Recording Interface on OM 73

Figure 51 Enable Remote Recording Interface on OM 2 73

Figure 52 Unified Communications Platform Tenant Configuration Interface . 74

Figure 53 Getting the License Request ID 76

Figure 54 Import License 77

Figure 55 Check if the License file is imported correctly 77

Figure 56 Data Maintenance Interface 78

Figure 57 Recording storage interface 79

Figure 58 Add Node 80

Figure 59 Edit Node 80

Figure 60 Deleting nodes 81

Contents of Tables

Table 1 Compatibility Requirements Table 15

Table 2 Number of concurrent recordings supported 15

Table 3 Installation File Information Sheet 15

Table 4 Firewall Port List 22

Table 5 Function Comparison Table 33

Table 6 Explanation of the Modify Member Information screen 39

Table 7 Enterprise Basic Information Interface Definition 40

Table 8 Adding an Administrator Interface Definition 42

Table 9 Search criteria for recording queries 45

Table 10 Recording Detail Definition 47

Table 11 Encryption Configuration Definitions 51

Table 12 Set Date 55

Table 13 Bar Figure Definition 56

Table 14 Filter call statistics 57

Table 15 Detailed Statistical Data Table Filter Definitions 58

Table 16 More Conditional Filter Definitions 60

Table 17 Editing Device Operator Interface Definitions 65

Table 18 Add Application Interface Definition 69

Table 19 Node Add Interface 70

Table 20 Add Device Interface 71

Table 21 Add OMX Device Interface Definition 72

Table 22 Configure recording report parameters on the unified communications platform 75

Table 23 Data Maintenance Interface Definitions 78

Modifying Record

Document Version 01 (2025-01-06)

Full Version

1. Preamble

1.1 About this Manual

This manual is a guide document created to help businesses and individual users maximize their use of the AS Recording Management System. The manual describes in detail the product introduction, operation methods and application scenarios for initial users and managers.

1.2 Document Users

- IT Administrator: Responsible for the deployment, configuration and daily maintenance of the recording system to ensure that the system runs stably and efficiently and is able to respond to technical problems that may arise in a timely manner.
- Enterprise managers: With the data analysis and statistical functions provided by the recording system, optimize the enterprise's communication costs, improve operation strategies, and enhance overall management efficiency.
- Technical support engineers: solve all kinds of technical problems encountered by users and provide professional advice.

2. Products

The AS Series Recording is an efficient and professional enterprise-grade recording management system that provides organizations with a comprehensive communications recording, storage and management solution. Through this system, enterprises can centralize the storage and management of call recordings, while providing flexible data query, statistical analysis and authority control, to meet the high standard demand for communication transparency and security compliance.

2.1 Product positioning

Recording system is aimed at medium and large enterprises and organizations that need communication compliance management, data security protection and efficient analysis capabilities, and is widely used in finance, politics, law and public security, energy and power, transportation, aerospace and other industries. The system focuses on recording management, supports high concurrent recording processing and multi-terminal cooperative operation, meets strict industry regulatory standards, and provides flexible deployment options (single-point, multi-node and cluster deployment).

2.2 System Features

- ✓ Powerful recording management capabilities.
- ✓ Support WAV, MP3 and other mainstream recording formats to meet diversified business needs.
- ✓ Provides multi-level recording management functions such as audition, download and permission assignment to ensure data security and privacy protection.
- ✓ Supports recording query and permission configuration by department and user for efficient management.
- ✓ Multiple security measures, including encrypted storage, permission control,

logging, etc., ensure that data is not tampered with.

- ✓ High-performance concurrent recording capability.
- ✓ The system is designed to support high concurrent recordings with stable performance to meet large-scale enterprise usage scenarios.
- ✓ Flexible adjustment of hardware configuration according to business needs, supporting small to large-scale concurrent recording deployment.
- ✓ Powerful statistics and analysis.
- ✓ Provide customized report generation tools to support daily, monthly, annual reports and sub-departmental statistical analysis functions.
- ✓ Supports single-point, multi-node and cluster deployment to meet the needs of flexible enterprise expansion.

3. Application Scenario

Compliance-critical industries

The system is designed to meet the compliance requirements of businesses and organizations for communication recording. In industries such as finance, law, public safety, energy and other industries with stringent regulatory requirements for compliance, communication recordings need to be stored for long periods of time and be traceable. The Recording system ensures that communications are recorded in accordance with industry compliance standards and legal and regulatory requirements through the encrypted storage of recordings, permission levels and log auditing capabilities.

Large-scale communication management scenarios

For large enterprises or organizations that are cross-regional and cross-departmental, the system is able to support highly concurrent recording processing and meet the needs under complex network architectures through flexible distributed deployment. Its centralized recording storage and management capability, together with the customized permission assignment mechanism, can efficiently serve the communication management needs of large-scale user groups.

Data Analysis and Optimization Scenarios

Recording provides powerful data statistics and analysis functions, supporting multi-dimensional recording analysis by department, user and time period. The reports generated by the system can assist the enterprise management to optimize the communication strategy, improve internal work efficiency, and at the same time provide data basis for decision support.

Security and Privacy Protection Scenario

In an environment that focuses on the privacy and security of communication data, the system provides all-around data security protection for the enterprise through multiple encrypted storage, fine-grained privilege configuration, and log auditing to avoid the leakage of sensitive information. The alarm mechanism of the system can monitor the abnormal operation in real time to further guarantee the security of communication recording.

Scenarios for Flexible Deployment Requirements

Recording supports single-point deployment, multi-node deployment, and cluster deployment, which is suitable for a wide range of business requirements from small to large enterprises. Whether centrally managed or distributed, the system can be flexibly configured to adapt to an organization's changing business scale.

Complex Privilege Management Scenarios

Multi-departmental and multi-level management needs usually exist within an enterprise. The Recording system meets the needs of enterprises for fine-grained permissions in the use and sharing of recording data and improves the efficiency of internal collaboration through hierarchical permission configuration and group management functions.

4. NewLync-AS Series Software Deployment

This chapter provides a detailed overview of the entire installation process, including system requirements, pre-deployment preparations, installation steps, initial configuration, and firewall settings.

4.1 Pre-Installation Environment Configuration

Please prepare the installation environment according to the following instructions to ensure a smooth system installation.

CPU Requirements

Details:

Specification	At least 8 cores
CPU Frequency	At least 2.4 GHz

The system requires a minimum of an 8-core CPU with a clock speed of at least 2.4 GHz to support the concurrent operations of the recording system. The greater the number of CPU cores and the higher the clock speed, the better the system's multitasking capabilities and response speed will be.

Memory Requirements

Memory Requirements	At least 16GB

At least 16GB of memory is required to ensure smooth system operation and robust data processing capabilities. The larger the memory capacity, the stronger the system's ability to handle a large number of concurrent tasks.

Disk Requirements

It is recommended to reserve sufficient storage space for MP3 and WAV format data to accommodate potential future growth needs. Based on our testing, 1GB of storage

space can hold approximately 290 hours of MP3 recordings or about 18 hours of WAV recordings.

Compatibility Requirements

CPU	Kunpeng（ARM）、Phytium（ARM）、HYGON、ZhaoXin、Intel（X86）
Operating System	KylinOS V10、KylinOS、EulerOS、 UOS、Red Hat、Ubuntu
Database	KingbaseES、Dameng、KDMDB、TiDB、Cassandra、CouchDB

Table 1 Compatibility Requirements Table

Recommended Configurations

Number of concurrent recordings	Recommended CPU cores	Recommended CPU frequency	Recommended memory size
50	8-core	2.4GHz	16GB
800	16-core	2.4GHz	64GB

Table 2 Number of concurrent recordings supported

4.1.1 List of Files Required for Installation

This section lists the core files required prior to installing the NewLync-AS series system. To ensure a smooth installation process, please verify that the installation packages listed below have been downloaded and their integrity confirmed.

File name
nlkas.xxxxxxxxxxxxxxx.tar.gz（The filename includes the version number and release date, and will be updated with the release of new version installation packages）

Table 3 Installation File Information Sheet

4.1.2 Create User Accounts

Prerequisite: The operator must possess superuser (root) privileges.

1. To start a terminal session: Type `ssh username@serverdomaine`, press the spacebar, enter the server password, then press the spacebar again.

```
PS C:\Users\user> ssh npms@192.168.191.168
npms@192.168.191.168's password:
```

2. Switch to the root user.

3. Add a user account: Execute the following command as the system root user to create a new user account named ‘nlk’. Replace <username> with the desired username for the user you wish to create:

```
adduser <username>
```

4. Assign passwords to new users:

```
passwd <username>
```

5. When prompted for a “New Password,” enter the new password you wish to set.

6. Confirm new password:

Next, the system will prompt you to “Re-enter the new password:” for confirmation. Re-enter the password you just set to complete the password setup.

4.1.3 Granting sudo privileges to users

Use the visudo command to grant sudo privileges to specified users, enabling them to execute commands requiring elevated privileges.

1. Enter the visudo command and execute it:

```
visudo
```

2. Locate the root entry in the sudoers file:

In the text editor, locate the section regarding root user privileges, as shown below:

```
## Allow root to run any commands anywhere

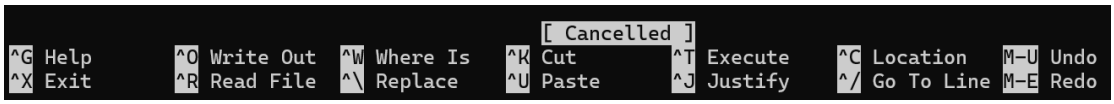
root    ALL=(ALL)       ALL
```

3. Add sudo privileges for this user under the root entry:

Immediately following the root user permission entry, add the following content:

```
nlk    ALL=(ALL)       ALL
```

After entering the command, press Ctrl+X to exit.



4.2 Installing NewLync-AS (Single-Machine Deployment)

This section provides detailed steps for deploying NewLync-AS on a single Linux machine, covering the entire process from preparing the deployment directory to configuring and executing the installation script.

1. Switch to the nlk user account:

If you are not currently logged in as the nlk user, you must first switch to that user.

Execute the following command to switch users:

```
su - nlk
```

2. Create the deployment directory: After opening the terminal or connecting to the server, create a new directory to store the NewLync-AS installation files:

```
mkdir deploy
```

3. Switch to the newly created deployment directory:

```
cd deploy
```

4. Upload the installation package to the deployment directory.

5. Extract the installation files:

```
tar -zxf nlkas.xxxxxxxxxxxx.tar.gz
```

File names may change with version updates. Please ensure that the file name within the command is replaced with the current installation file name.

6. Post-completion verification: Confirm that the file has been successfully

decompressed:

```
ll
```

After entering the command, you will see a list of the newly extracted files and directories.

7. Prepare the ENV file on the server:

```
./installV2.sh newenv
```

8. Modify the env file according to the specific environment:

Item	Definition
adparam_mode=local	No changes required.
adparam_hostname	Enter this device's IP address
secondary_hostname	Leave blank
adparam_ldap_domain	LDAP domain, modify according to actual circumstances
adparam_ladp_password	LDAP password, modify as needed based on actual circumstances
adparam_s3_key	S3 Protocol ID, modify as needed based on actual circumstances
adparam_s3_secret	S3 Protocol ID, modify as needed based on actual circumstances
MY_IS_SECOND=no	No changes required.

9. Run script: Used to install Docker, enable IPv4 forwarding, configure the system environment, and prepare for subsequent installations.

```
./installV2.sh install
```

10. Logout: After completing the installation script, execute the logout operation to close the current terminal session.

```
exit
```

11. Relogin: After logging out, please reconnect to the server to ensure all environment variables and configuration updates take effect. Use the following command to relogin to the server, replacing your.server.com with your server address.

```
ssh nlk@your.server.com
```

12. Re-execute the installation script: After logging back in, navigate to the directory containing installV2.sh. Run the following command to execute the installation script again and complete the installation.

```
cd deploy
./installV2.sh install
```

4.3 Install NewLync-AS (Dual-Server Deployment)

This section provides detailed steps for installing NewLync-AS Dual-Machine in a Linux environment, covering the entire process from preparing the deployment directory to configuring and executing the installation script.

1. Switch to the nlk user account:

If you are not currently logged in as the nlk user, you must first switch to that user. After opening a terminal or connecting to the server, execute the following command to switch users:

```
su - nlk
```

2. Create deployment directory： Create deployment directory:

After connecting to both servers, create a deploy directory on each machine to store the NewLync-AS installation files:

```
mkdir deploy
```

3. Both servers have been switched to the newly created deployment directory:

```
cd deploy
```

4. Both servers uploaded the installation package to the deployment directory.

5. Extract the NewLync-AS installation files on both servers:

```
tar -zxf nlkas.xxxxxxxxxxx.tar.gz
```

File names may change with version updates. Please ensure that the file name within the command is replaced with the current installation file name.

6. Verify upon completion:

Confirm that the files have been successfully extracted on both servers:

```
[nlk@localhost nlkas]# ll
```

After entering the command, you will see a list of the newly extracted files and directories.

7. Prepare the ENV file on the first server:

```
./installV2.sh newenv
```

8. Modify the env file according to the specific environment:

Item	Definition
adparam_mode=local	No changes required.
adparam_hostname	Enter this device's IP address.
secondary_hostname	Enter the backup machine's IP address.
adparam_ldap_domain	LDAP domain, modify according to actual circumstances.
adparam_ladp_password	LDAP password, modify as needed.
adparam_s3_key	S3 protocol ID, modify according to actual circumstances.
adparam_s3_secret	S3 protocol key, modify according to actual circumstances.
MY_IS_SECOND=no	No changes needed.

9. After executing the following command on the first server to generate the environment for the second server, it will be automatically copied to the second

server:

```
./installV2.sh setup_secondary_server_env
```

10. Both servers execute the script:

```
./installV2.sh install
```

11. Log out.

After completing the installation script, perform the exit operation on both servers to close the current terminal session.

```
exit
```

12. Please log in again.

After logging out, please reconnect to both servers to ensure all environment variables and configuration updates take effect. Use the following command to log back into the server, replacing your.server.com with your server address:

```
ssh nlk@your.server.com
```

13. Re-execute the installation script: After logging back in, navigate to the directory containing installV2.sh. On both servers, run the following command to re-execute the installation script and complete the installation:

```
cd deploy
./installV2.sh install
```

14. Import Authorization: Log in to the AS management backend using the IP address of the first server, export the License ID, apply for authorization, and then import it.

15. Restart nlkas on another server.

```
docker-compose restart nlkms
```

4.4 Firewall Configuration

This section details how to configure the firewall to support the full functionality of the NewLync-AS series services. Ensure that the corresponding ports are opened to allow

the services to operate normally.

Port number	Protocol	Description
8082	tcp	Access for the NewLync-AS series management page.
1311	udp	Data transmission for OM remote recording.
7070	tcp	Reporting for OM CDR Data.
389	tcp	Network communication for LDAP services.

Table 4 Firewall Port List

1. Open the management page port for the NewLync-AS series.

Open port 1311/tcp for OM remote recording:

```
firewall-cmd --zone=public --add-port=1311/udp --permanent
```

2. Open the OM remote recording port.

Open port 8082/UDP for accessing the NewLync-AS series management page:

```
firewall-cmd --zone=public --add-port=8082/tcp --permanent
```

3. Open the OM CDR reporting port.

Open port 7070/TCP for OM CDR reporting:

```
firewall-cmd --zone=public --add-port=7070/tcp --permanent
```

4. Open the LDAP service port.

Open port 389/tcp for LDAP service:

```
firewall-cmd --zone=public --add-port=389/tcp --permanent
```

5. Apply and reload firewall rules.

Apply all changes and reload the firewall to make the settings take effect:

```
firewall-cmd --reload
```

6. Verify that ports are open.

```
firewall-cmd --zone=public --list-ports
8082/tcp 1311/udp 7070/tcp 389/tcp
```

4.5 Accessing and Logging into the NewLync-AS Management System Platform

After completing the installation and configuration of the NewLync-AS management system, administrators need to access the management platform to configure and manage the system. The detailed steps are as follows:

1. Open your web browser:

On your computer, launch any web browser, such as Google Chrome, Mozilla Firefox, or Microsoft Edge.

2. Enter the management platform address:

In the browser's address bar, enter the URL for the NewLync-AS Management System Platform: http://[server IP address]:[port number].

Example: http://192.168.131.58:8082, then press Enter to access the site.

3. Log in to the management platform:

On the login page, you will need to enter the credentials for your administrator account. Please use the following default login information:

- User name: enter your user name in the 'User name' input box, default user name：sysadmin
- Password: Enter your password in the 'Password' input box, default password：as28N24@pw

In addition, you can choose to log in with your cell phone number:

- Cell Phone Number: Enter your cell phone number in the 'Cell Phone Number' input box and enter the verification code received in the 'Verification Code' input box.

Once you have entered these credentials, click "Login" to enter the management platform.

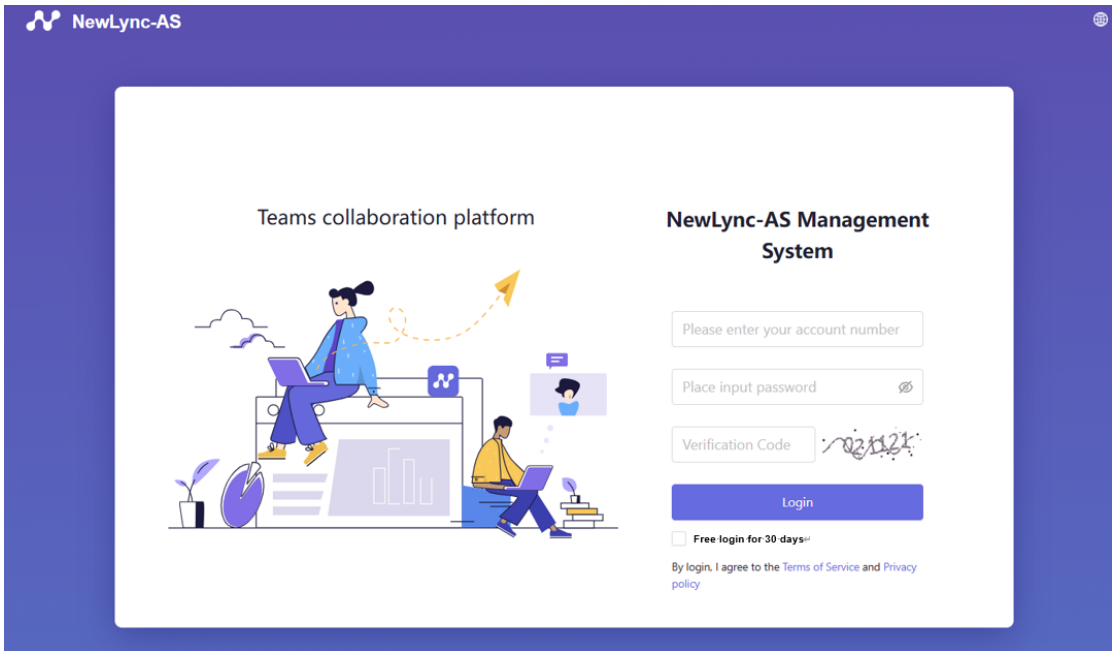


Figure 1 AS management system login screen

Note Keep your login credentials confidential and use them only on trusted devices. For system security, it is recommended to change the default password immediately after your first login.

4.6 Add Recording Node

After installation, add a recording node by navigating to the NewLync-AS management backend and selecting > Recording Node, then click Add Node.

Web address: http://192.168.130.58:8082 (Modify according to the actual server IP address)

Default account and password: sysadmin/as28N24@pw

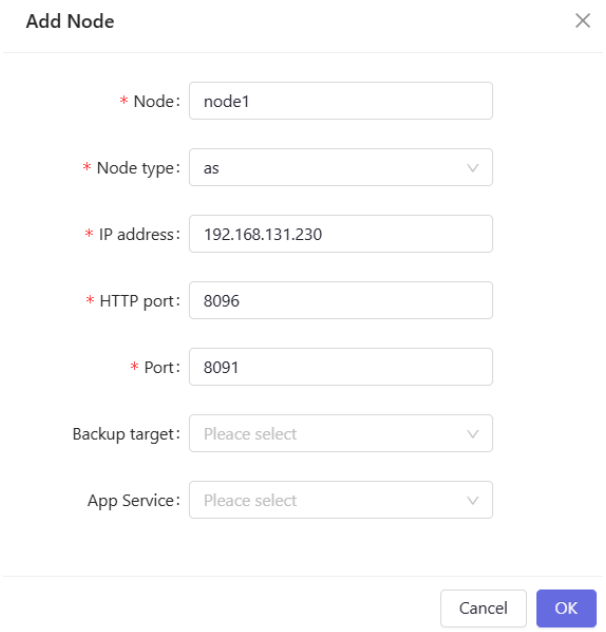


Figure 2 Add Recording Node

Item	Definition
Node Name	Default input node1.
Node Type	Select as.
IP address	Enter the current server IP address.
HTTP port	Default input 8096.
Port	Enter 8091.
Application Services	Select the application. The default application created during installation is internal. Select internal.
Backup target	Not selected.
Alarm Switch	Enable as needed; alerts will be sent when space is insufficient.

4.7 Configure OM Remote Recording

Access the NewLync-AS management backend at http://192.168.130.58:8082 (modify according to the actual server IP address).

Default Account and Password：sysadmin/as28N24@pw

1. Add OM device

Step.1. Select the department; it is recommended to select the entire company.

Step.2. Select the application service created when adding the recording node from the application services at the bottom.

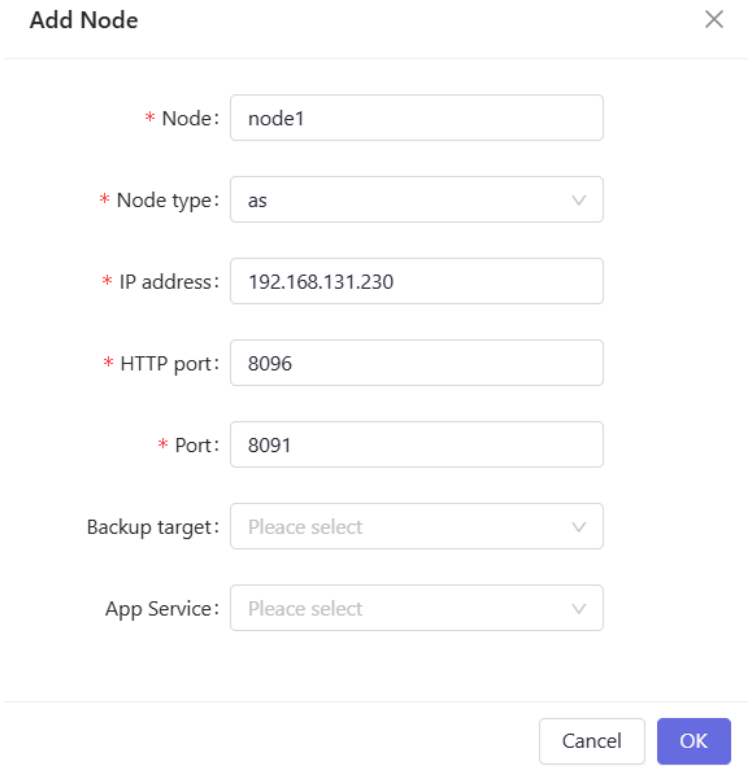


Figure 3 Add OM device

Item	Definition
Name	Fill in as needed. For example: node1
Department	Required. If uncertain, select the entire team.
Equipment Type	Select the OM/MX or OMX device based on the type of equipment being added.
MAC address	Enter the MAC address of the device.
FSP Security Code	Enter the FSP security code.
Recording Cache Address	Select and enter the recording cache address.
Local CDR Cache	Check to enable local CDR caching.
Application Services	Select the default internal.

2. Configure OM Remote Recording

Log in to the web interface, navigate to Application Services > Recording/Voicemail, configure remote recording, and enter the recording server address: 192.168.131.230:1311 (modify according to the actual server IP in your deployment).

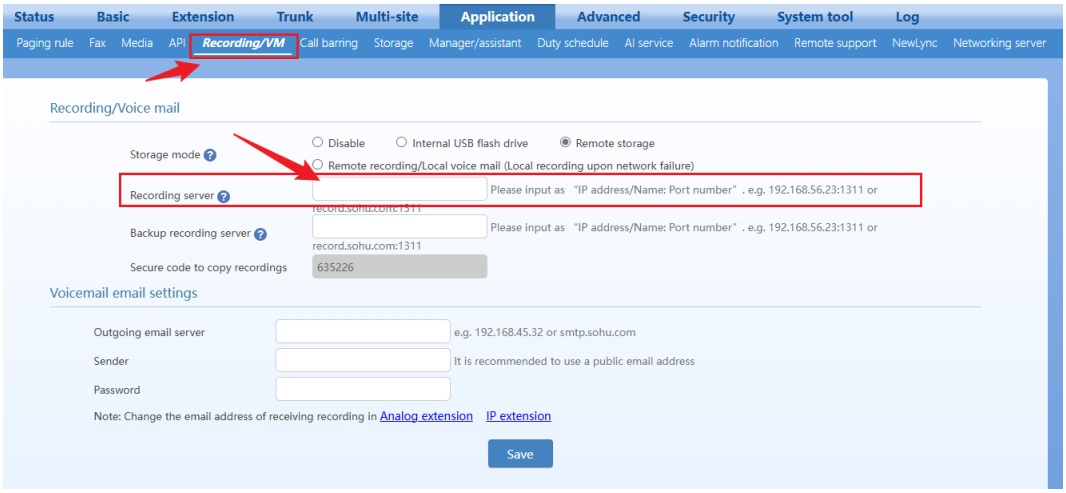


Figure 4 Configure OM Remote Recording

3. Enable call recording for the OM extension

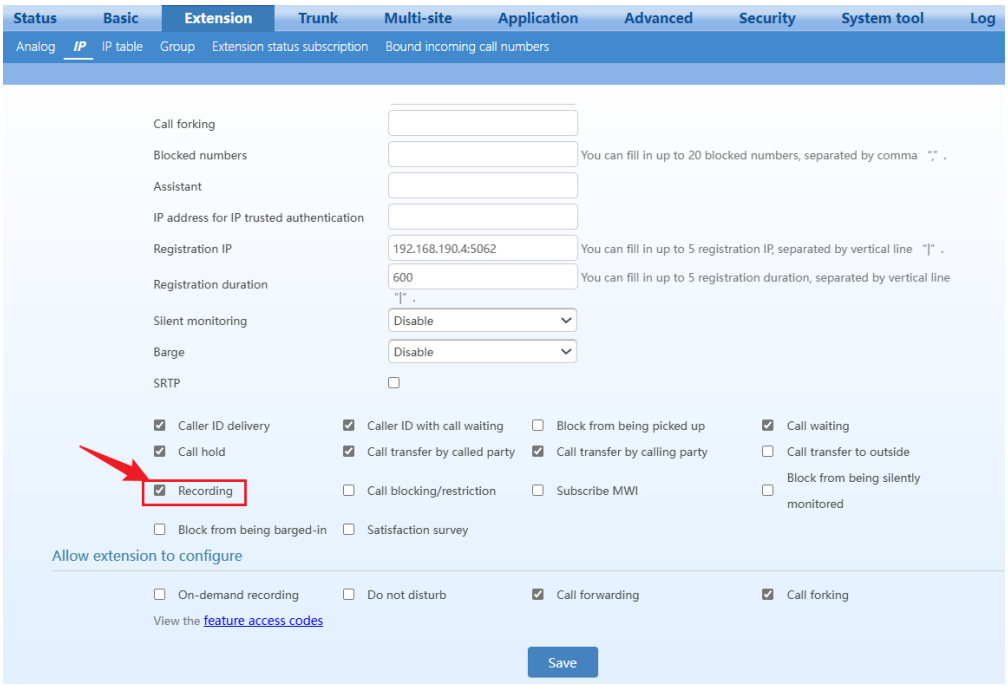


Figure 5 Configure OM Remote Recording 2

Recording Parameter Configuration

192.168.130.55 is the OM IP (modify according to your OM address). After logging into the OM web interface, enter the following command in your browser:

http://192.168.130.55/xml?method=gw.config.set&id698=0x008F

Finally, restart OM to complete the configuration.

4.8 Import License

After completing the installation and configuration of the NewLync-AS Series NL-Recording system, it defaults to a trial license. The next step is to import the License to activate and enable the system's full functionality. Please contact your distributor to obtain the appropriate License. Once you have the License, follow the steps below to import it correctly.

Obtain License request file:

Step.1 Log in to the NewLync-AS NL-Recording system management platform.

Step.2 Navigate to > System Settings > License Information. Click “Get License Request ID” to generate the License Request file (.csr file).

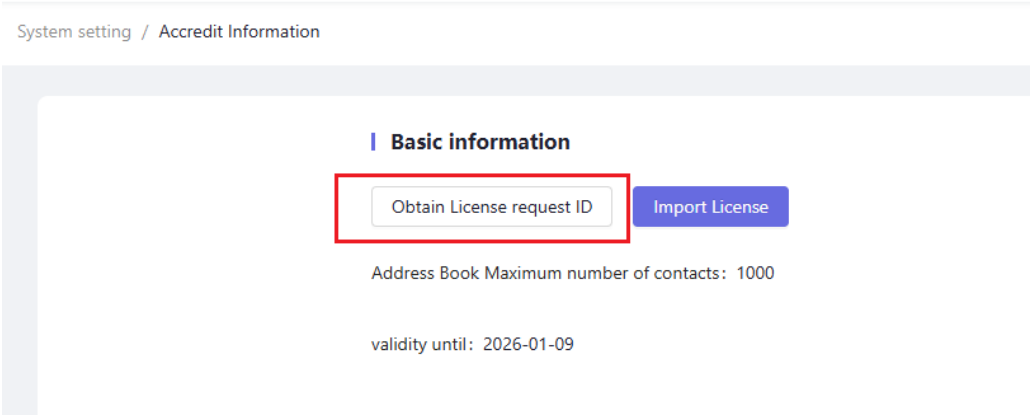


Figure 6 Getting the License Request File

Step.3 Save the generated .csr file to your local computer as prompted. This file must be sent to your distributor to obtain the corresponding license.

Submit a license request and receive the license file

Step.1 Send the .csr file to your supplier or New Rock. They will generate the corresponding license file based on the number of services you purchased.

Step.2 After processing your request, the supplier will send you a document containing the official license.

Import License File:

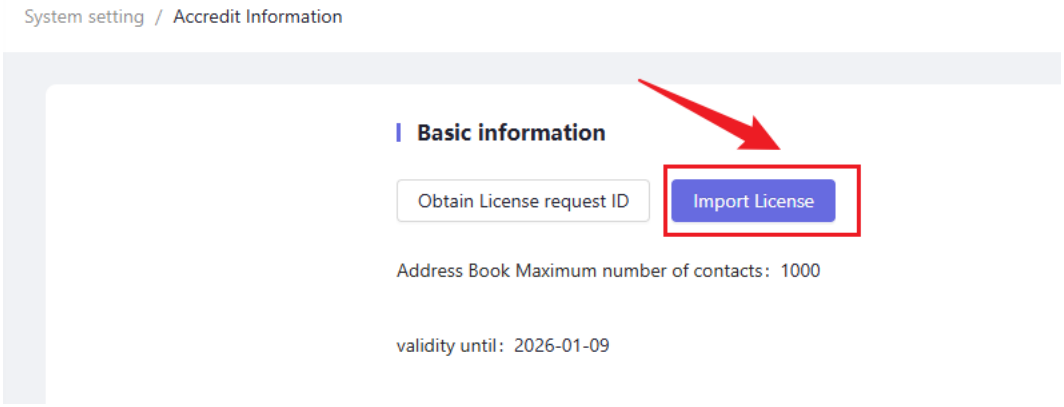


Figure 7 Import License

Step.1 Click “Import License”.

Step.2 In the pop-up window, browse and select your License file.

Step.3 After selecting the file, click “Open” to upload it. The system will automatically process and verify the validity of the License file.

Step.4 Verify License Status.

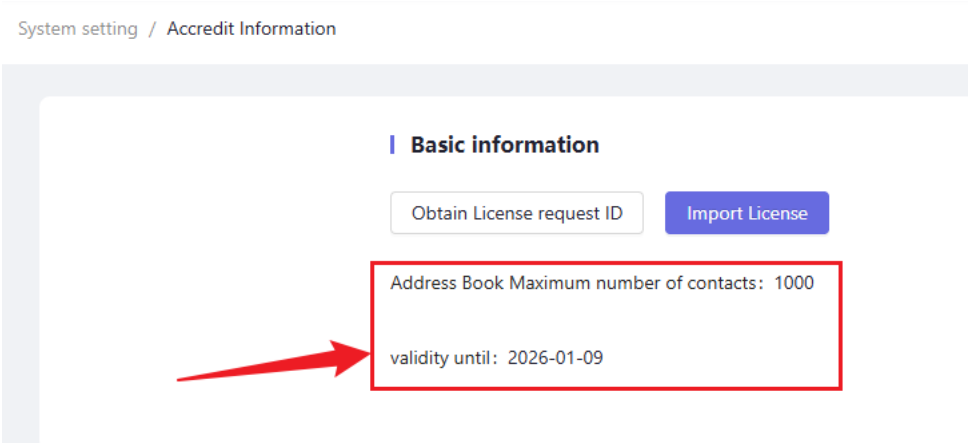


Figure 8 Checking License Status

4.9 AS Series License Features Overview

The AS series of management systems offers four authorization modes to meet the diverse communications management needs of enterprise users. After initial installation, the system defaults to a trial license mode with some functionality limitations. Enterprise users can contact the distributor to purchase an official license, which supports personalization (functionality, concurrency, maximum number of contacts) to fully unlock the full functionality. The following is a detailed description of the functions and features of the four authorizations:

I. AS Trial License

The system defaults to a trial license, under which the number of address book administrators is limited and only the basic organization structure and member management functions are supported. The recording function has a limited maximum number of concurrencies, which cannot meet the demand for large-scale recording. The trial period for the function is 7 days. For enterprise trial and functionality evaluation only.

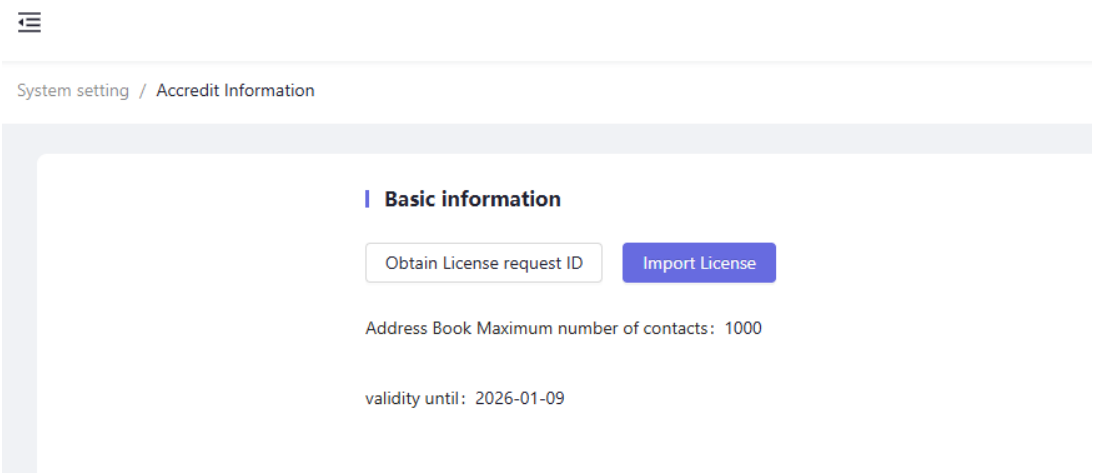


Figure 9 AS Trial License Interface

II. AS Recording System License

Core Functions: Provide storage, query and playback management of call recording, support recording acquisition and storage, support encrypted and non-encrypted storage modes, and provide recording statistical analysis and alarm functions to meet multi-dimensional data management needs.

Applicable industries: Mainly used in finance, customer service, public prosecutors and law enforcement and other industries, need to record, archive and playback the customer call scenarios.

III. AS billing system authorization

Core Functions: Support call record (CDR) collection and management, filter call records according to departments or members, manage call cost calculation, generate bills according to call duration, location, type, etc., and support personalized rate settings. Ideal for large-scale call centers or enterprise communications expense management.

Applicable industries: call centers, communication service providers, mainly used for call billing, bill management and communication expense accounting.

IV. AS Address Book System License

Core Functions: Used to manage the information and organizational structure of enterprise employees, support LDAP protocol docking, support for a variety of phones (including Yealink, Direction, Huawei and other internal communications).

Support employee information query and organization management.

Applicable industries: HR, administration and IT departments for scenarios that require efficient management of company address book, employee and departmental information.

Concurrent authorization of recordings and authorization of a maximum number of communicators

Users can purchase recording concurrent license and address book number limit license separately according to their needs, to enhance the maximum number of concurrent use of the system at the same time and the maximum number of address book users, to ensure that the system can still run stably during the peak period of use. When the enterprise in the subsequent expansion, you can contact the channel provider to upgrade the license on the existing basis.

4.10 Function Comparison Table

Feature Module	Contacts Authorization	Recording Authorization	Billing Authorization
Support Organizational Structure Management	✅	✅	✅
Support User Permission Level Management	✅	✅	✅
LDAP Protocol Integration	✅		
Recording Collection and Storage Management		✅	
Recording Permission Control (Whitelist, etc.)		✅	
Support Recording Statistics and Alerts		✅	
Support Multi-Node Recording Backup		✅	
Support Call Record Statistics			✅
Support CDR Collection and Management			✅
Support Billing Report Output			✅
Support Call Rate Calculation and Tiered Billing			✅
Support API Interface Integration	✅	✅	✅
Support Domestic Servers and Operating Systems (New China)	✅	✅	✅
Support Statistical Report Output	✅	✅	✅
Support Sensitive Information Hiding (Recording/CDR)		✅	✅
Compatible with OM/OMX/MX Devices	✅	✅	✅
Support NewLync2.0 Collaboration Platform	✅	✅	✅
Support Log Backup and Recovery	✅	✅	✅
Support Call Detail Record Encryption		✅	✅
Support Departmental Statistical Analysis	✅	✅	✅
Support Large-Scale Concurrent Access	✅	✅	✅

Table 5 Function Comparison Table

5. Configuring AS

This guide describes everything from basic user login, day-to-day administrative operations, system monitoring, data backup and recovery, and security and troubleshooting. Help system administrators and technicians use the system effectively, ensure stable operation, and maintain system security.

5.1 Organizational structure

5.1.1 Membership and sectors

Administrators can add members directly in the admin backend, or via a corporate invitation code. Directly added members are inactivated by default and cannot log in to the client, you can enable the automatic activation function in the operation and maintenance platform.

Add department

Step.1 Go to the AS administration backend and click Organizational Structure > Members & Departments.

Step.2 Click +New Department on the left side of the page.

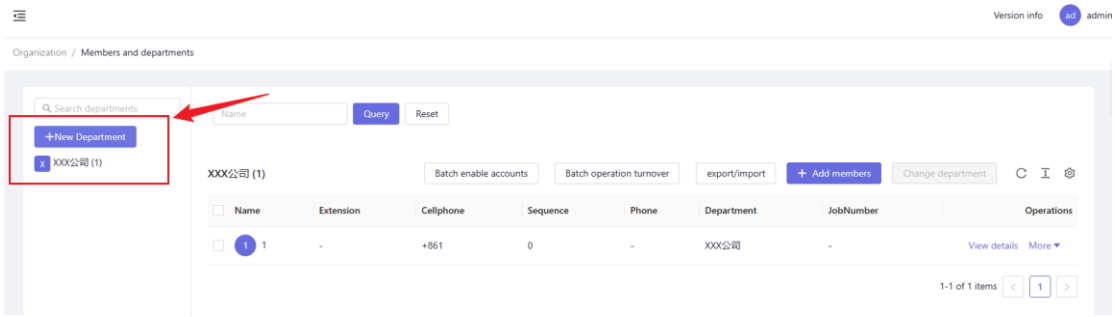


Figure 10 New sectors

Step.3 Enter the department name in the pop-up window, select the parent department, and set the department head (optional).

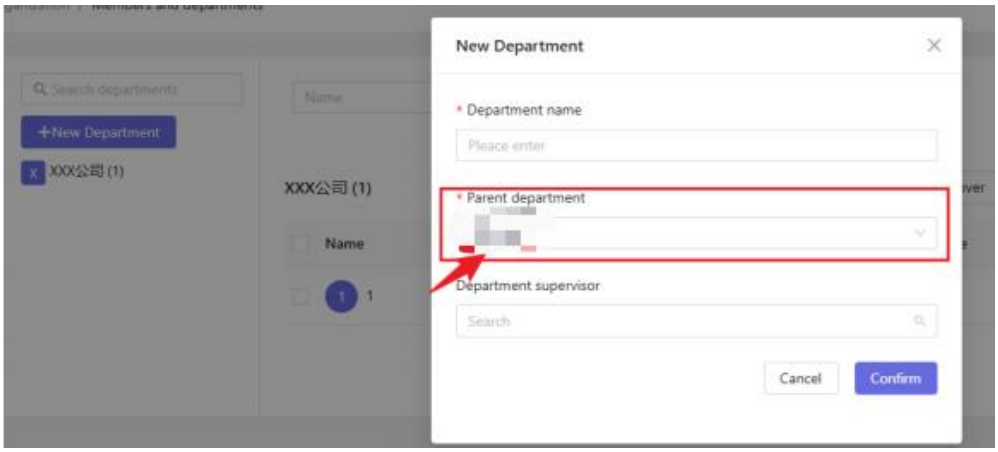


Figure 11 Setting up department heads

Step.4 Click Confirm to create successfully.

Step.5 Right mouse button on a department name allows you to edit the department, add sub-departments, move down, and delete the department. Only empty departments can be deleted, so remove the members in the department before deleting it.

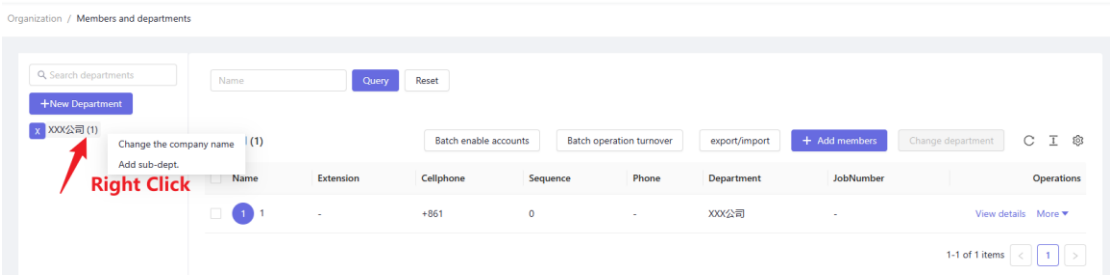


Figure 12 Editorial office

Import Export Membership

Step.1 Go to the AS administration backend and click Organizational Structure > Members & Departments.

Step.2 Click Import Export.

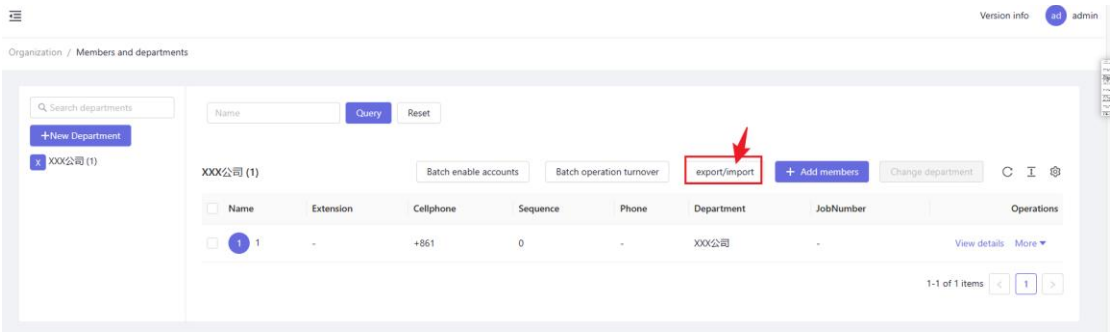


Figure 13 Import Export Members

Step.3 Click Export Members to export all members.

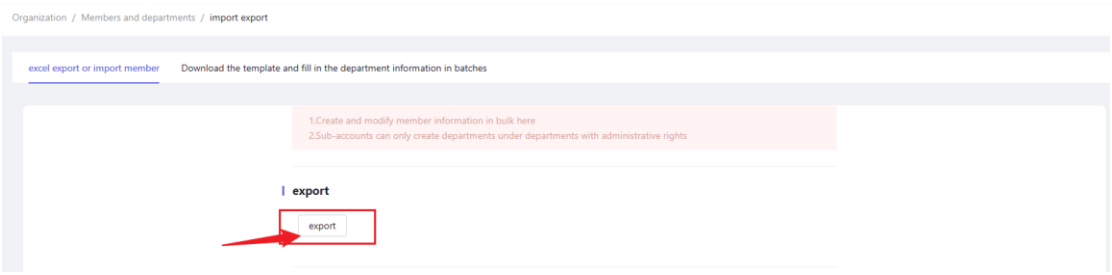


Figure 14 Import Export Members

Step.4 Click Download Template and the browser automatically downloads an excel template. Edit the template, add member information, save, and then click Upload Staff Information to upload the edited form. Be careful not to modify the table structure.

Import Export Department

Step.1 Download the template, enter departmental information and then upload it to add departments in batch.

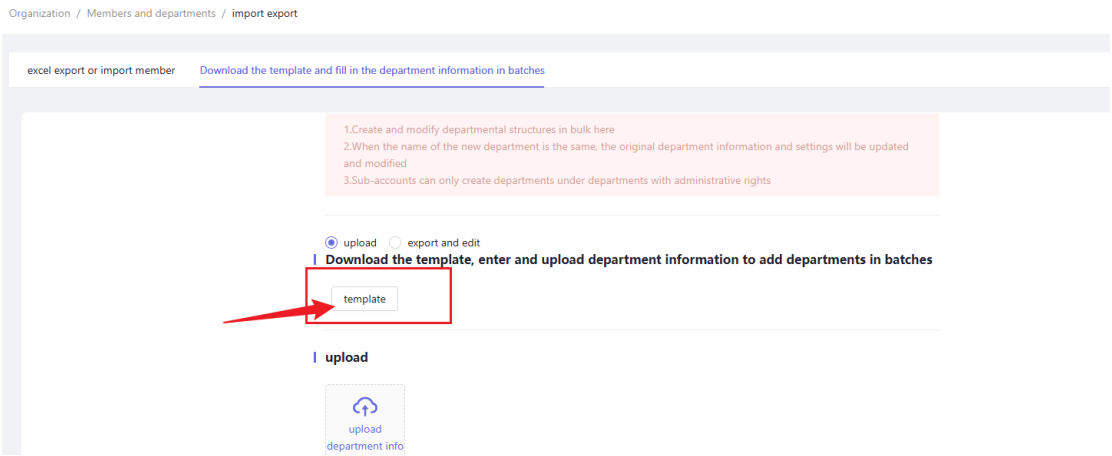


Figure 15Download Template

Step.2 Follow the form prompts and click Upload Department Information after completing the form.

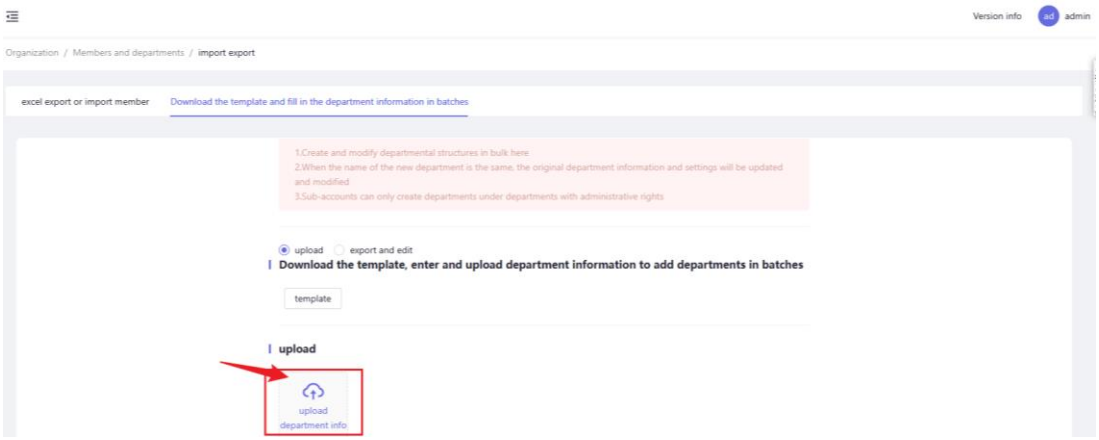


Figure 16 Uploading departmental information

Step.3 Export and modify departments

Click to download the template, enter department information and upload it to add departments in bulk.

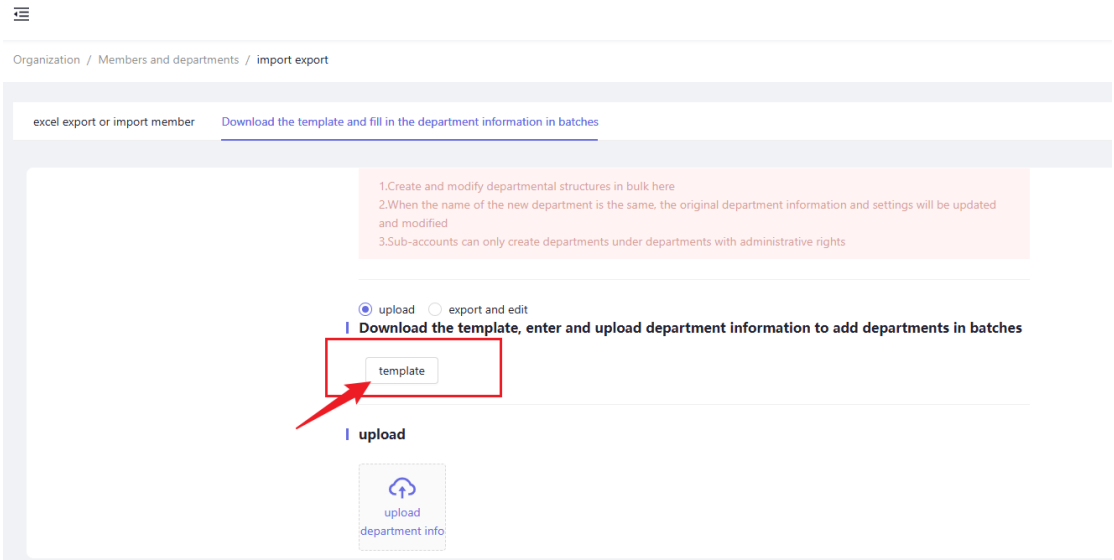


Figure 17 Download Template

Add Member

Step.1 Go to the AS administration backend and click Organizational Structure > Members & Departments.

Step.2 Click +Add Member on the Members page.

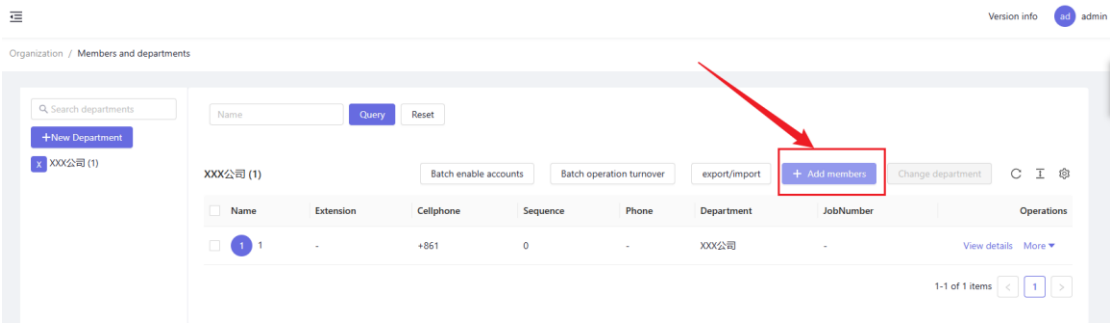


Figure 18 Adding Members

Step.3 Fill in the pop-up window with basic information such as name, cell phone, department, email and extension. Fill in at least one cell phone and email address.

Step.4 Click Finish to add successfully.

Step.5 Click More in the member list to modify member information, change departments, operate departures, reset passwords, and suspend accounts.

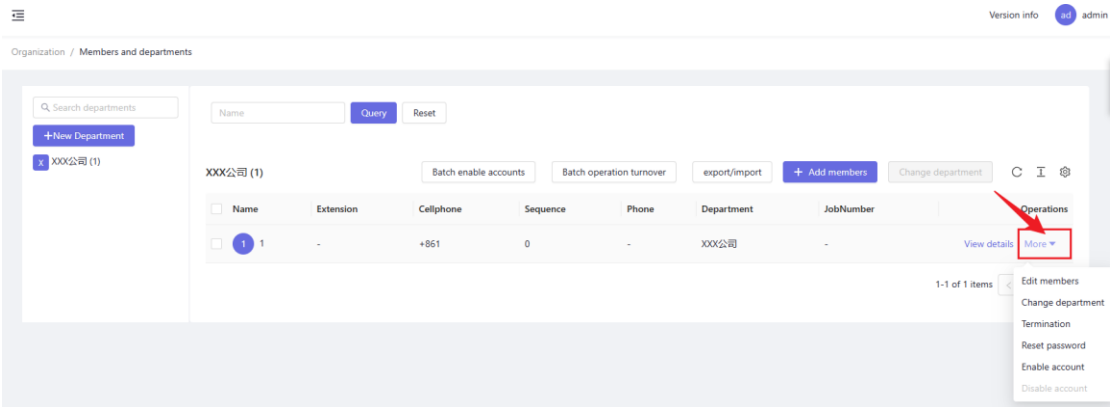


Figure 19 Modify member information

Batch Enable Accounts and Batch Operate Separations

Step .1 Click on Bulk Enable Accounts and enter your login name (currently supports cell phone, email, and extension logins)

Step .2 Enter your login password

Step .3 Check Enable response permissions and click OK to save.

Item	Definition
Name and surname	This field is used to display or enter the employee's name. Users can query or update basic employee information based on this field.
Extension	Employee's extension number.
Cell phone	Employee's cell phone number.
Private plane	Employee's landline number.
Sectoral	The department to which the employee belongs. Administrators or users with privileges can use this field to view the departmental affiliation of an employee, or to perform departmental transfers.
Job title	The job number is used to distinguish between different employees and is an important identifier of the employee's identity.

Table 6 Explanation of the Modify Member Information screen

5.2 Enterprise Settings

5.2.1 Corporate Information

Go to the admin backend and click Enterprise Settings>Enterprise Information to view the enterprise information. Click Modifying the upper right corner to modify the enterprise information, with an asterisk for required fields.

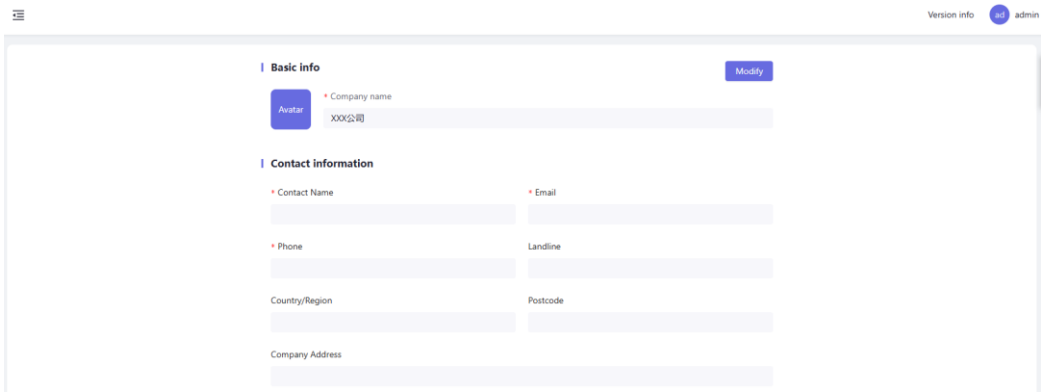


Figure 20 Modify basic enterprise information

Item	Definition
Company	To display the company name, you need to fill in or select the official

identification	name of the company. Ensure that the name of the company is the same as the one registered in the system for subsequent management and inquiries.
Contact e-mail	The e-mail address of the primary contact. This mailbox is used to receive external notifications from the organization or to make contact.
Contact person's cell phone	The cell phone number of the primary contact for emergency communication or contact with someone outside the company.
Private plane	The landline phone number of the business.
Country or area	The administrator needs to fill in the country or region where the company is located. This information helps determine the legal, tax and other compliance requirements of the company's location.
Zip code	The postal code of the company's address. Zip codes help to ensure that mail or packages are correctly mailed to the company's address.
Business address	The complete office address of the company, including the street, city, country or region where it is located. This information is used for company communications and business-related geolocation identification.

Table 7 Enterprise Basic Information Interface Definition

5.2.2 Administrative authority

There are three roles in the admin backend permissions, Creator, Super Administrator and Administrator. There is only one creator with all permissions to transfer. Super Administrators are created by the creator, and there can be more than one, with all the permissions except that you can't manage Super Administrators and creators. Administrators are created by super administrators and can customize the scope of permissions.

9.2.2.1 Transfer creator

Step .1 Go to the admin backend and click Enterprise Settings>Manage Permissions.

Step .2 Find the creator on the Super Admin page and click Transfer.

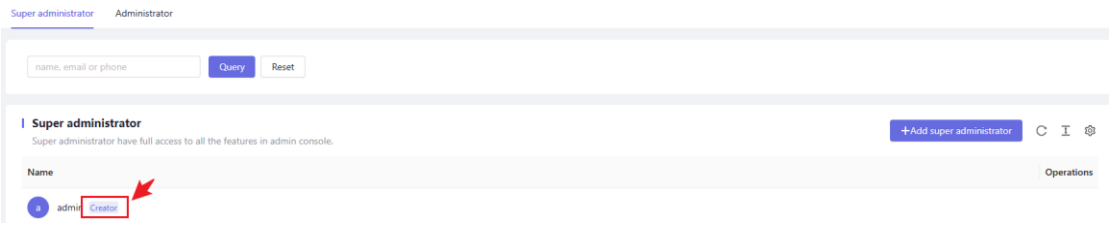


Figure 21 Transfer creator

Step .3 Enter keywords in the pop-up window, search for the member you want to transfer to, and click Select.

Step .4 Click Submit to complete the transfer.

9.2.2.2 Add Super Administrator

Step .1 Go to the AS administration backend and click Enterprise Settings>Manage Privileges.

Step .2 Click +Add Super Administrator on the Super Administrator page.

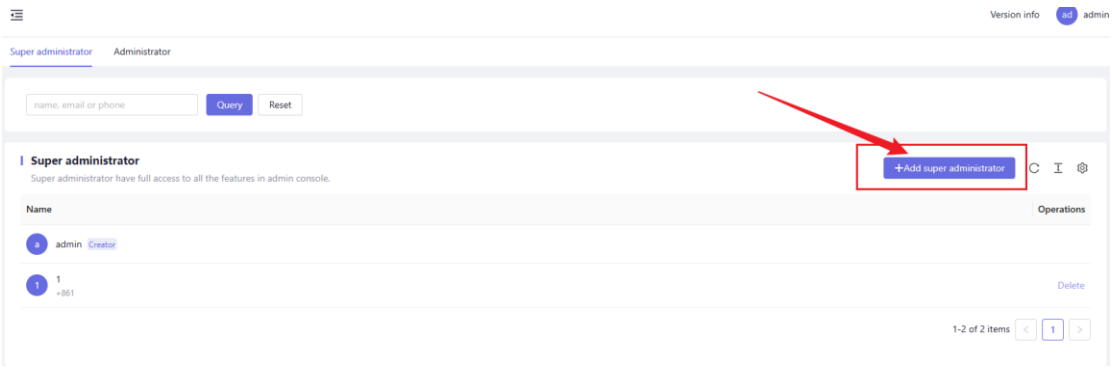


Figure 22 Add Super Administrator

Step .3 Enter a keyword in the pop-up window, search for members, and then click Selected.

Step .4 Click Submit to complete the creation.

9.2.2.3 Add Administrator

Step .1 Go to the AS administration backend and click Enterprise

Settings>Manage Privileges.

Step .2 Click+Add Administrator on the Administrator page.

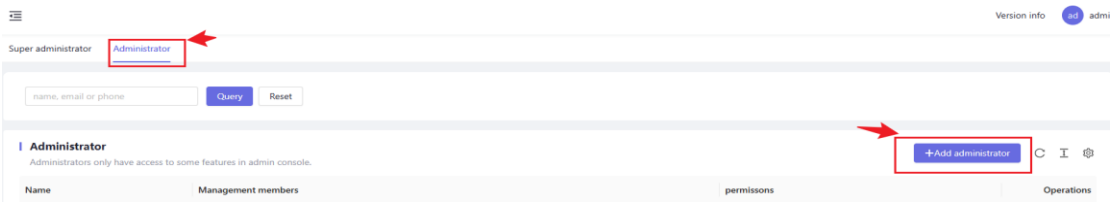


Figure 23 Add Administrator

Step .3 Enter keywords in the pop-up window to search for members to add as administrators, and then check the permission range.

Item	Definition
Name and surname	The administrator needs to fill in the name of the new administrator. This field is used to identify the administrator as an individual and to ensure that information about each administrator in the system is clearly identifiable.
Scope of management	The administrator needs to set the scope of that administrator's administrative privileges and decide which departments that administrator can manage. This field is used to control the assignment of permissions.
Scope of one's jurisdiction	The appropriate permissions granted to the new administrator.
Manipulate	The administrator needs to define the actions that can be performed on this administrator account. Examples include enabling, disabling, modifying or deleting administrator information. This field is used to manage the account status and related settings for this administrator.

Table 8 Adding an Administrator Interface Definition

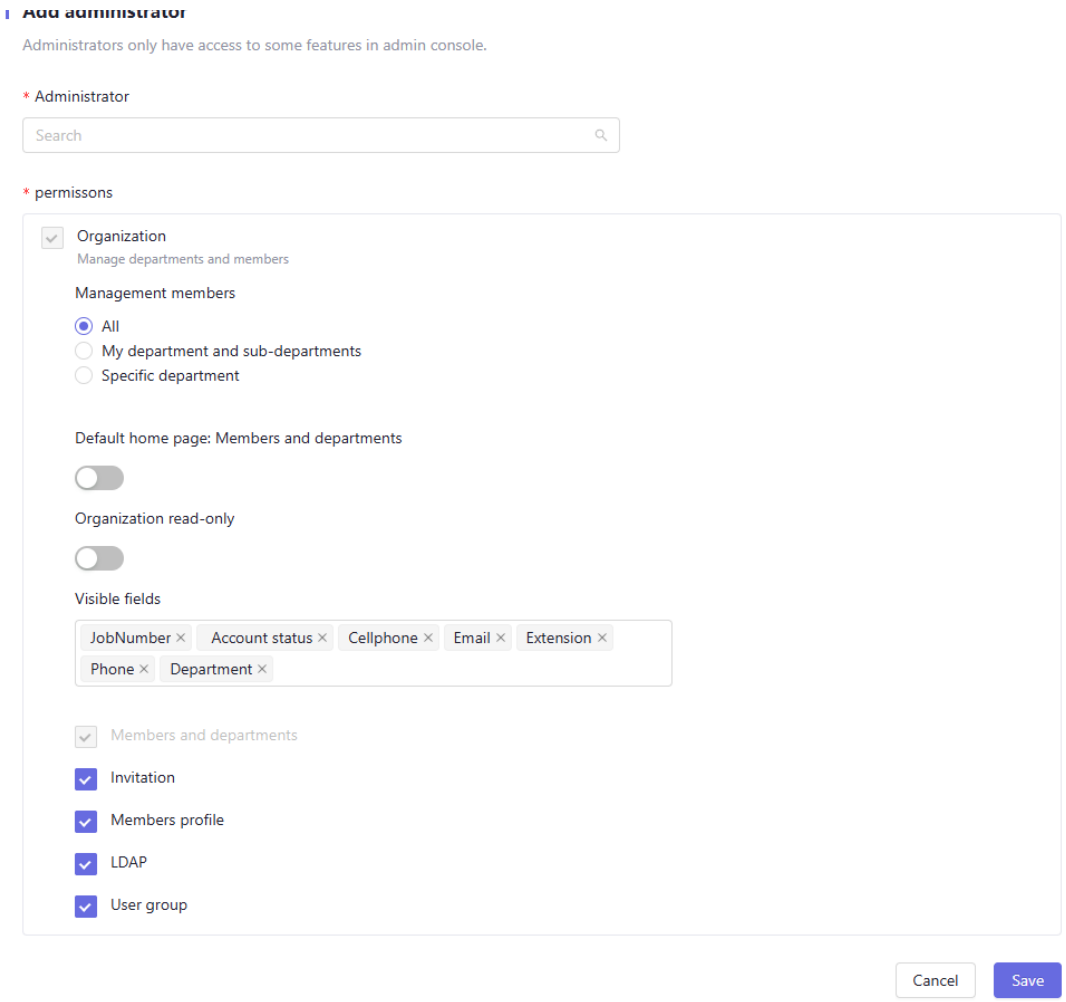


Figure 24 Edit Administrator Privileges

Step .4 Click Save to complete the addition.

6. Recording Management

The Recording Management Module of the AS Recording System is an efficient recording processing and storage solution designed specifically for enterprises, integrating recording capture, storage, querying, privilege control and security encryption. The module supports centralized management of recording files in multiple audios formats and provides a flexible permission assignment mechanism, allowing users to quickly retrieve, audition or download recordings by department or member. With powerful statistical analysis functions, it can generate multi-dimensional reports, and at the same time, it supports encrypted storage and backup recovery of recording files.

6.1 Recording Inquiry

The Recording Query operation allows users to retrieve call recordings and voice messages from the system based on specific criteria.

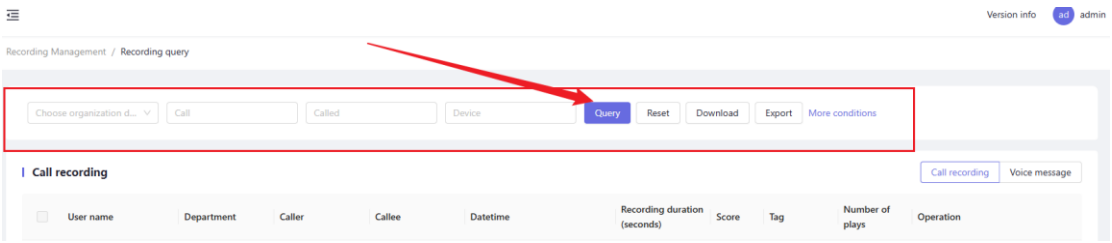


Figure 25 Recording query interface

Step .1 Navigate to the Recording Management > Recording Inquiry screen.

Step .2 Fill in the search criteria:

Item	Definition
Select Organization or Department	Select the department you want to search for in the "Organizational Departments" drop-down menu.
Caller	In the "Caller" input box, enter the caller number you want to query.
Called	Enter the called number in the "Called" input box.

Installations	In the "Device" input box, enter the name of the device you want to query.

Table 9 Search criteria for recording queries

Step .3 Click the "Search" button, the system will display the list of recordings according to the input conditions.

The query result is reset:

To reset the search criteria, click the "Reset" button to clear all current search information.

Download audio files

Click on the "Download" button. The system pops up a confirmation dialog box, prompting "Do you want to download all the data?". The system pops up a confirmation dialog box prompting "Do you want to download all the data?". The user confirms the download by selecting "OK".

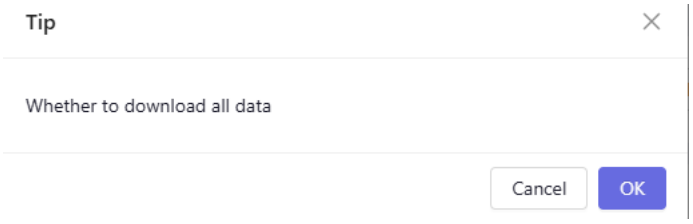


Figure 26 Steps to download all data

Saving of documents. Users can save the downloaded zip file to a specified location on their computer. The file name will be automatically generated by the system according to the actual downloaded content.

Exporting query data

Step .1 The user clicks the "Export Data" button on the screen. The system pops up a prompt box asking if the user does want to export all the data.

Step .2 The user clicks "OK" to confirm the export of the entire query result.

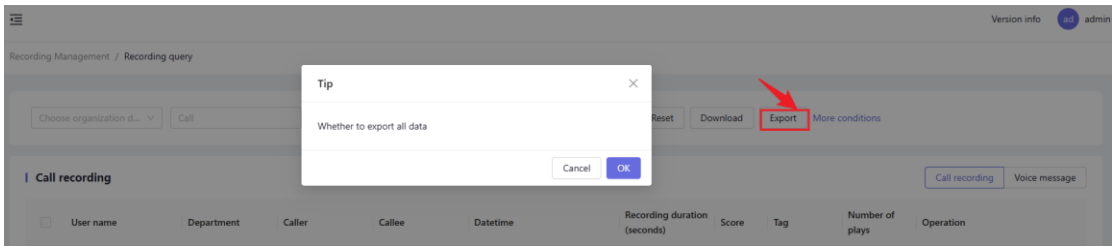


Figure 27 Exporting query data

More search terms

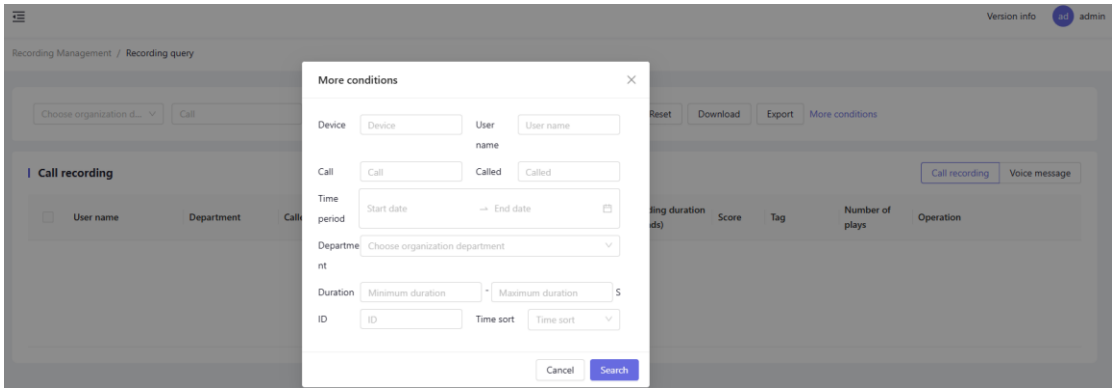


Figure 28 Filter more search criteria

Step .1 Click for more conditions.

Step .2 Configure advanced search parameters.

Step .3 After setting all the advanced search criteria, click the "Query" button to continue or "Cancel" button to exit the advanced search.

In the Recording Management screen, the Call Recording and Voice Message functions allow users to perform the same set of actions to manage and review call recordings.

View Details

Both "Call Recording" and "Voice Message" interface support to view recording management details.

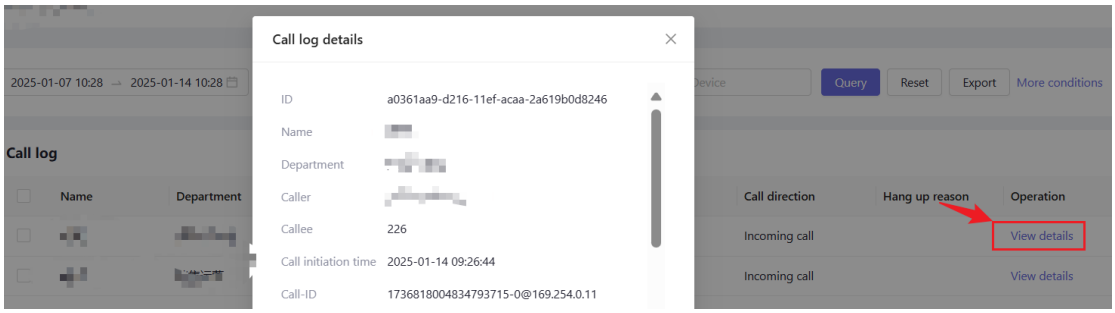


Figure 29 Query recording management details

Item	Definition
Id	Unique recording identifier to distinguish each recording or message.
User ID	The name of the user account associated with the recording.
Extension number	The extension number from which the recording came.
Sectoral	The department to which the user belongs.
Caller ID	The phone number that initiated the call.
Called number	The phone number to receive the call.
Dates	The date and time stamp of the recording.
Installations	The ID of the device on which the recording is performed.
Recording duration	The specific time the call or message lasted.
Filename	The name of the file in which the recording is stored.
Encrypted or not	Displays whether the recording file is encrypted or not.
Score	The quality of the recording is rated.
Number of times it has been played	Number of times the file was played
Backup recording	Recordings are backed up to show the backup recordings here.
Tab	Categorized labels for recording files for easy management and searching.

Table 10 Recording Detail Definition

playback of recorded sound

After clicking Play Call Recording or Voice Message, the following functions appear at the bottom of the page:

1. Playable

Click the Play button in the Call Recordings or Voice Messages list to play the selected recording immediately. During playback, you can use the slider at the bottom of the screen to adjust the playback progress.

2. score (of student's work)

The recording quality can be rated while the recording is playing. Click on the rating button After that, select a rating from 1 to 10 to assess the quality of the recording, where 1 means the lowest quality and 10 means the highest quality. After selecting a score, the corresponding number will be displayed next to the score button, confirming your scoring choice.

3. Tab

To facilitate subsequent retrieval or categorization, users can add tags to the recordings. Click the Add Tags button After that, enter the tag in the pop-up dialog box and click Add. If you need to remove an added tag, click on it again to cancel it.

4. Volume adjustment:

Users can adjust the playback volume by clicking the volume button on the interface.

Playlist

Click the + number, the selected recording will be added to the playlist. The number next to the playlist icon increases with the number of recordings added. To remove a recording from a playlist, click the × button next to the corresponding recording in the playlist.

Playlists in order

In the Recording Management System, users can build a playlist to control the playback order of recording files.

1. Add to Playlist: Click on any recording next to the + next to any recording to add it to the playlist. The playlist will list the recordings in the order they were added, and the number next to the list icon indicates the number of recordings in the list.
2. Sequential Playback Control: In the playlist, the recordings will be played back sequentially in the order they were added. Users can control the playback process with the play and pause buttons at the bottom of the playback console, or select a specific recording to play directly.
3. Manage Playlists: Users can freely manage the recording entries in the playlists. To remove a recording from the playlist, simply click the × button next to that recording entry in the playlist. This operation does not delete the recording file, only removes it from the current playlist.

Download Recordings

The system allows users to download selected call recordings or voice messages to a local device.

Step .1 Click the download icon next to the recording you wish to download.

Step .2 In the dialog box, select the path where you wish to save the recording file.

Step .3 After confirming the save location, click "Save" to start the download.

Delete Recordings

Only the Creator role has permission to delete recordings. Users can delete call recordings or voice messages from the system that are no longer needed. This operation is not reversible.

Step .1 Click the Delete button next to the recording you want to delete.

Step .2 A dialog box will pop up asking for the reason for deletion

Step .3 Enter the reason for deletion in the text box provided.

Step .4 Fill in the reason and click "OK" to execute the deletion, or click "Cancel" to terminate the operation if you change your mind.

Note Only the Creator role has the permission to delete recordings; the Super Administrator and Administrator roles do not have this permission.

Batch selection of recordings

Users can select records by checking the checkbox next to the call record. After selecting a record, the system displays the number of selected records at the top of the screen.

Note Deleting a recording is a permanent operation and once deleted, it cannot be recovered.

Before performing a deletion operation, make sure that you have backed up any important recordings or have been authorized accordingly.

6.2 Recording settings

This section describes in detail how to configure recording settings in the AS Series Recording System.

6.2.1 Recording encryption configuration

Recording encryption is an important feature to ensure that call recordings remain confidential during storage and transmission on the server. Administrators can enable or disable recording encryption as needed and update encryption keys as necessary to ensure security when downloading files.

Step .1 Navigate to Login to Recording Management > Recording Settings

Step .2 Encryption Configuration

Item	Definition
activate encryption	Select "Encryption" to enable end-to-end encryption protection. After encryption, all recording files stored on the server will be encrypted, effectively preventing unauthorized access and leakage of data. To download these files, you need to unzip them using an encryption key.
Disable encryption	Recording files will be stored in the system in a non-encrypted format, which is less secure.

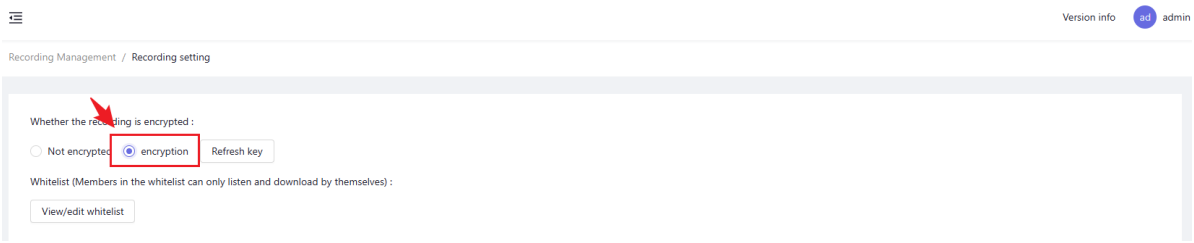
Table 11Encryption Configuration Definitions

After selecting Encrypted or Unencrypted, the system will automatically update and apply the selected configuration.

Key management:

Activate encryption settings: In the "Encrypt recording or not" section, select the "Encrypt" option, and the interface will display the "Refresh key" button.

- Refresh the encryption key:
  - By clicking on "Refresh Key" you can generate a new encryption key to ensure a higher level of data protection.
  - A pop-up dialog box will ask if you want to refresh the key, select OK to update, or cancel to keep the existing key.
- Confirm the key refresh:
  - A pop-up dialog box will ask "Do you want to refresh the key?", offering the options "OK" and "Cancel".
  - After selecting OK, the system will automatically process the key update.
  - The system will process the key update and display a message "Refresh Successful" when it is completed, and the system will automatically manage the encryption key.



Note Once encryption is enabled, all recording files, both new and existing, are automatically encrypted.

6.2.2 whitelisting

The whitelisting feature allows administrators to specify which users or departments can access recording files.

Step .1 Whitelist setup access:

On the "Recording Settings" screen, click "View/Edit Whitelist" to enter the Whitelist management interface.

Step .2 Edit whitelist:

Click on the "Edit" button to open the "Select Members" dialog box. Expand the list of departments, select the members you want to add to the whitelist, and check the appropriate checkboxes.

Step .3 Confirm the member and save.

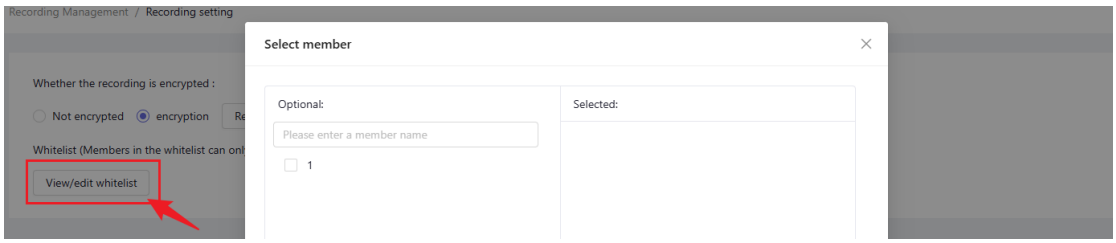


Figure 30 Whitelist editing screen

Whitelist member management:

View Whitelist Members: Successfully added members will be displayed in the Whitelist list.

Remove member operation:

Using the "Close" button: Clicking the "Close" button next to a member's entry will remove that member from the whitelist.

Using the ⊗ Icons: The list of members provides ⊗ icon, clicking on which will also remove the corresponding member. When clicked, the system will remove the member from the whitelist and update the list

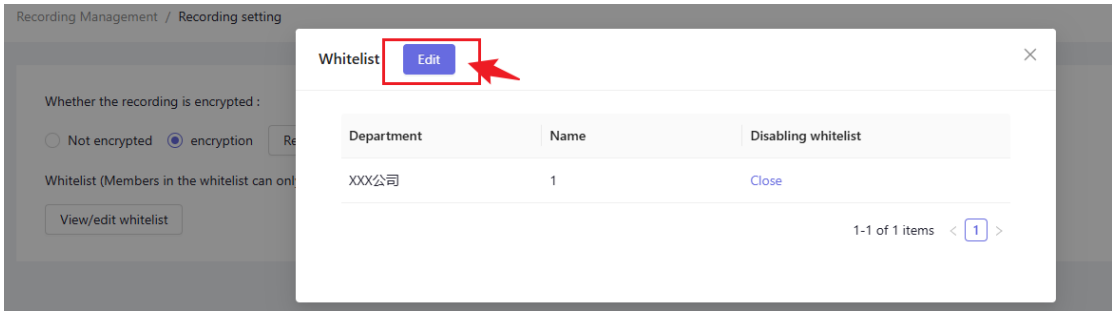


Figure 31 Whitelist List

Note The whitelisting feature allows authorized users listed in the whitelist to download and audition recording files. This ensures that only explicitly authorized users can perform these operations. The Delete Recordings feature is limited to the Creator role; whitelisted users do not have permission to delete recording files. This setting ensures system security and rigorous data management against unauthorized deletion operations.

6.3 Operation Log Management

The management platform supports querying detailed operation logs.

6.3.1 Operation log query

Administrators can query operation logs based on specific time frames and other key parameters.

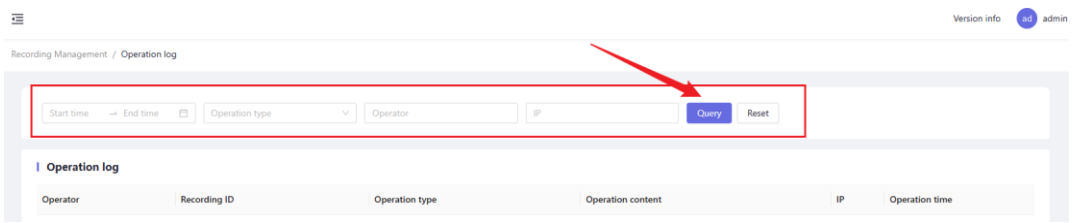


Figure 32 Operation log query

Step .1 Setting the query time range

Locate the time selection area at the top of the log query screen, click on the date selection box, and select the "Start Time" and "End Time".

Step .2 Selecting the type of operation

Click on the Action Type drop-down menu to list the available action types, including Tagging, Rating, Playing, Downloading, and Deleting, and select an action type in order to filter and view the records of a specific type of action.

Step .3 Enter operator name

Type the name of a specific user in the "Operator" input box to view the user's operation records. This step helps to filter the operation records of a specific user, which facilitates detailed user behavior analysis.

Step .4 Enter the IP address:

Enter the IP address of the user's computer on which the operation is to be performed in the "IP" input box.

Step .5 Execute the query:

Click the "Query" button at the bottom of the interface, the system will perform the search of operation logs according to the specified conditions, and after the search is completed, the operation logs will be displayed in the list, so that the administrator can further analyze them.

Reset query conditions

Click the "Reset" button to restore the query conditions to the initial state, and the interface will display all the operation logs again.

6.3.2 View a list of operation logs

The query result will be displayed in the Operation Log List screen, listing in detail all the operation records that meet the query criteria.

Item	Definition
Operator	Displays the name of the user performing the operation

Recording ID	Provides a unique identifier for the recording file associated with the operation
Type of operation	Displays the types of actions performed by the user, such as tagging, rating, playing, downloading, deleting
Operation content	Describes the specific actions performed by the user
IP address	Displays the IP address of the user's computer on which the operation is being performed
Operating time	Displays the exact date and time when the operation took place

6.4 Statistical analysis interface

This chapter details how to use statistical analysis tools to evaluate and analyze recording data. The interface provides administrators with a powerful toolset for monitoring and analyzing call activity and usage trends over time, which in turn helps optimize resource allocation and improve service efficiency.

6.4.1 Daily, monthly and annual statistical analysis

This section describes in detail how to use the Daily, Monthly, and Annual Report functions in the AS system for call data statistics and analysis.

Step .1 Select Report Type

The user selects the desired type of report: daily, monthly or annual by using the tabbed buttons at the top of the interface.

Step .2 Setting the date

Item	Definition
Daily	The user is required to select a specific year, month and day
Monthly bulletin	Users need to select a specific year and month
Annual report	The user only needs to select the specific year

Table 12 Set Date

After selecting a date, the system automatically loads and displays call data for the selected time range.

histogram

Item	Definition
Exhalation versus Inhalation	The Figure visualizes the number of outgoing and incoming calls per hour on the selected date by means of blue and green bar graphs.
Total call duration vs. average call duration	Total Talk Time: The purple line runs through the bar graph, and the total talk time for each point in time is indicated by a circle marked on the purple line in seconds. Average talk time: indicated by a light red dotted line, the average talk time per hour is clearly identified by circling the time point in seconds.

Table 13 Bar Figure Definition

Interactive features

When the user hovers the mouse over a point in time on the Figure, the system automatically displays an information box next to the mouse, providing detailed data on outbound call volume, inbound call volume, total call duration, and average call duration for that point in time, which helps the user to conduct in-depth analysis of call activities.

View detailed statistics

On the right side of the statistical analysis screen, the user can view a detailed data table showing call statistics under filtered conditions.

Filtering call statistics

Item	Definition
Total Talk Time	Sort by total length of call

Ascending/Descending	
Average talk time ascending/descending	Sort by average length of each call
Call out ascending/descending order	Sorting based on the number of incoming inbound calls received
Call out ascending/descending order	Sorting based on the number of outbound calls initiated

Table 14 Filter call statistics

The table includes call statistics for different categories, and users can choose to view different types of call data from the drop-down menu at the top.

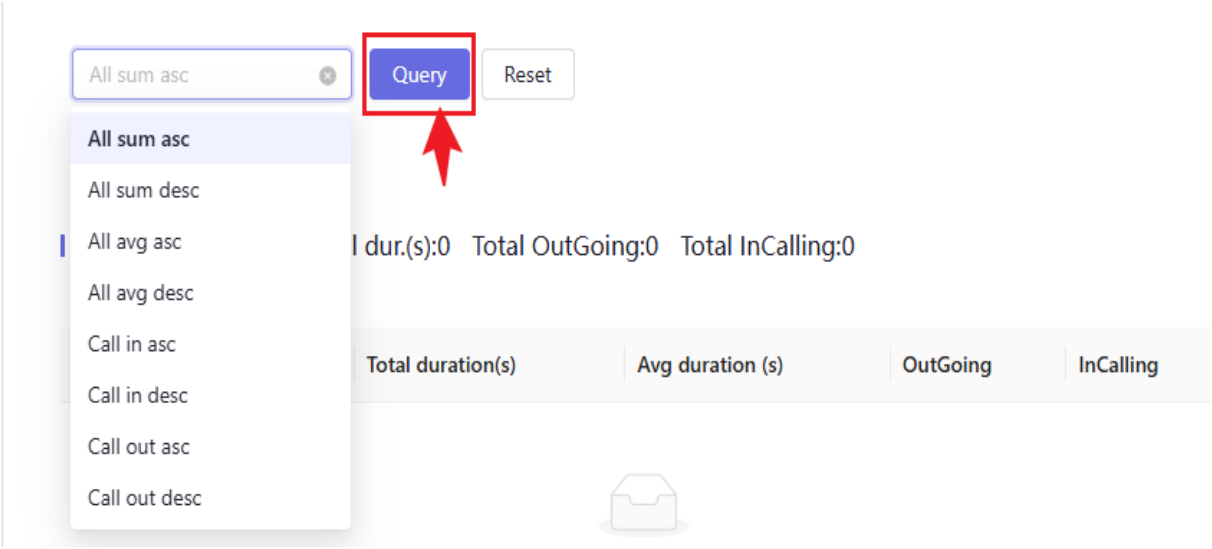


Figure 33 Detailed statistical data table

Item	Definition
Total talk time	Displays the total duration of all calls
Average talk time	Shows the average length of each call
Breathe out	Displays the number of outbound calls initiated

Incoming call	Displays the number of incoming inbound calls received

Table 15 Detailed Statistical Data Table Filter Definitions

6.4.2 Analysis of subsector call statistics

In AS, departmental call statistics can be visualized through the "departmental report", using pie Figures to visually represent the percentage of call duration of each department.

Report Type Selection

At the top of the screen, the user can select this type of statistical report by clicking on the "Segment Report" button.

data visualization

The system displays a pie Figure in which each sector represents a department, and the size of the sector indicates the proportion of the total number of call hours for that department.

Detailed Data Display

The specific call duration data for each sector is labeled in red on the sectors of the pie Figure, providing a clear indication of the values.

The red label on the pie Figure ("undefined"), showing the specific call length value, indicates the specific call length for each department.

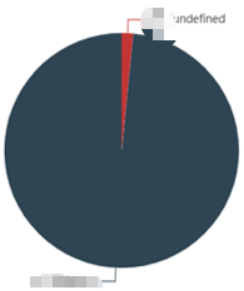


Figure 34 Pie Figure presentation

Dimension Selection

At the top of the Statistical Analysis screen, click on the Statistical Dimension Selector (a drop-down menu). Select the statistical dimension you need to view from the drop-down menu, and once selected, the pie Figure will update according to the selected

dimension, showing the percentage of call duration for different departments on the selected dimension.

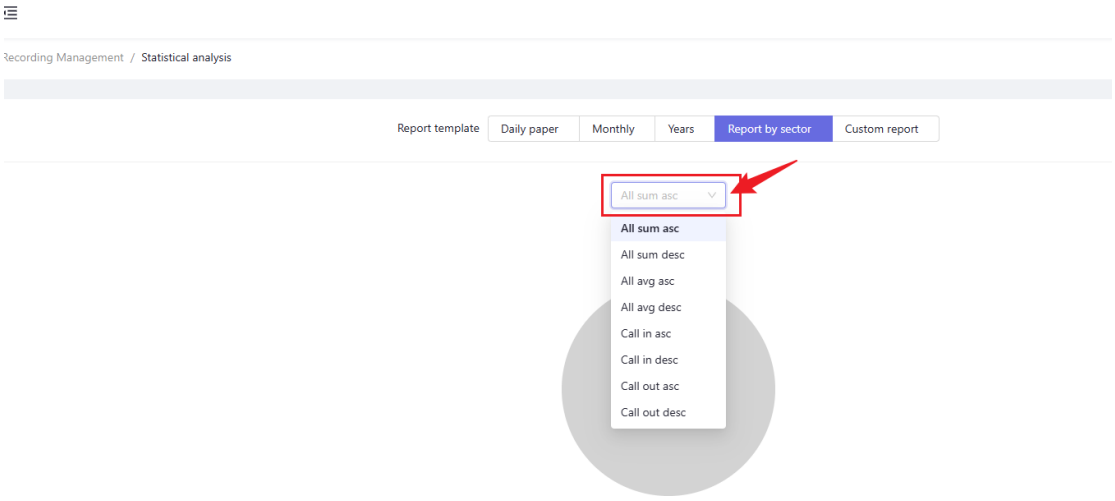


Figure 35 Selection of statistical dimensions graph

6.4.3 Customized reports for statistical analysis

Custom Report Statistical Analysis supports the use of filters to retrieve specific types of statistics.

Users can select the type of data they wish to display by clicking on "Select Type" in the drop-down menu at the top of the interface.

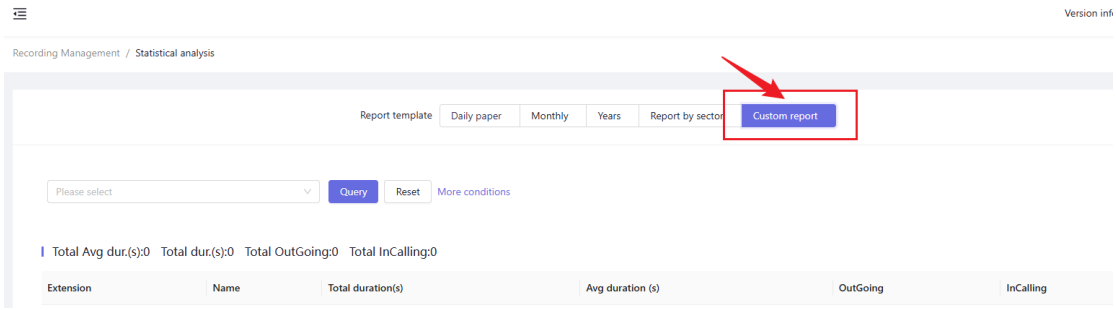


Figure 36 Customized Report Statistical Analysis Figure

Reset function

After clicking the "Reset" button, the table will reload and display all the original data without any filters.

More conditions

Users can click the "More Conditions" button on the interface to open a detailed

condition filtering dialog box to set the filtering conditions.

Item	Definition
Equipment/name	Enter a device name or associated identifier to filter call records associated with a specific device
Caller/called	Enter a phone number to locate relevant call data
The twelve two hour divisions of the day	Select a specific date range, from start date to end date, to filter call records
Sectoral	Select a department from the drop-down menu to limit the search results to call data for a specific department
Length of time	Set the minimum and maximum values for call duration to filter call records that meet the criteria
Extension number	Enter a specific extension number to find the call history for that extension

Table 16 More Conditional Filter Definitions

Screening

After the user has set all the required filtering conditions, click the "Query" button to apply these conditions, and the system will update the data display according to the specified filtering conditions.

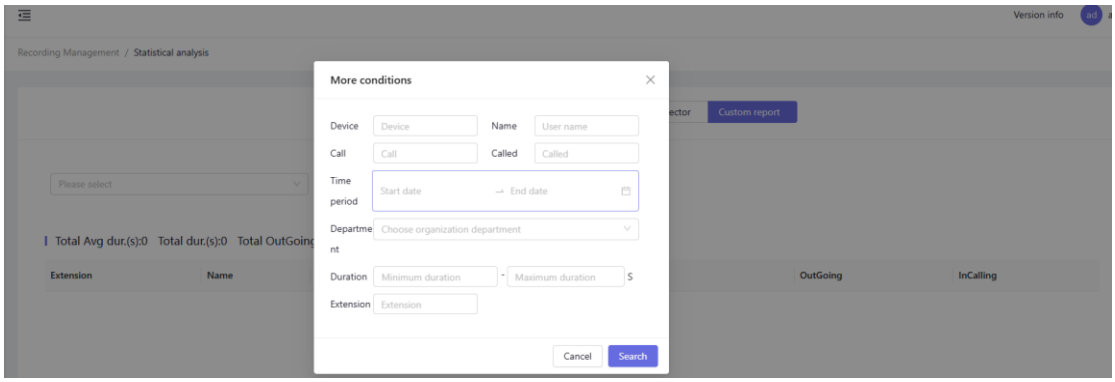


Figure 37 Filter screen with more conditions

7. Alerts

7.1 Alarm Log

The alarm management interface is used for real-time monitoring of system operation status and recording of alarm events to help users find and deal with potential problems in time. The interface is divided into two main parts: alarm logging and resource usage monitoring. The resource monitoring area displays key system performance indicators, including CPU usage, memory usage and disk usage, showing current resource consumption in numerical and graphical form. The alarm log section records all alarm events, categorized by "high", "medium" and "low" levels, displaying the type of event, the related service address, the time of occurrence and a detailed description, making it easy for users to quickly locate the problem. It is convenient for users to quickly locate the problem.

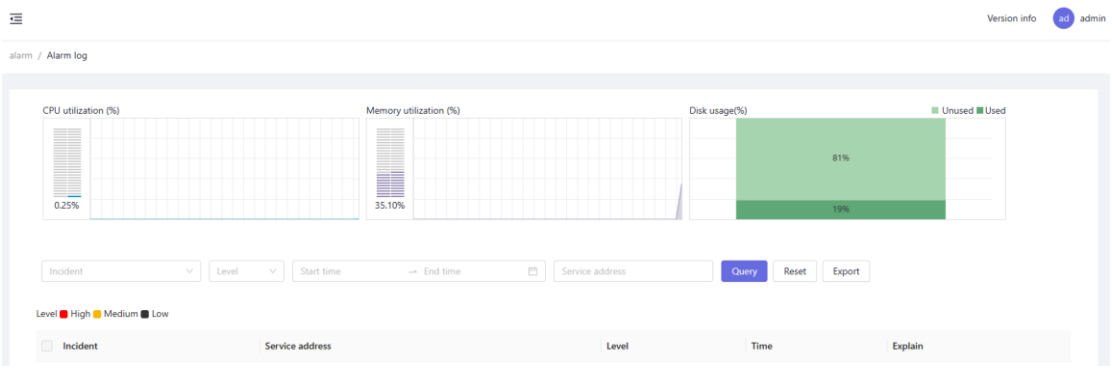


Figure 38 Alarm log interface

7.2 Alarm settings

The alarm event setting interface is used to flexibly configure the alarm rules and notification methods for system monitoring to ensure stable system operation. According to different scenarios, users can set up resource usage alarms such as high CPU occupancy, high memory occupancy, high storage space usage, etc., as well as program status alarms such as abnormal termination of the recording and acquisition

program, abnormal termination of the service program, and backup failure. In addition, it also supports monitoring of abnormal situations such as database connection errors and long time not receiving recording files, etc. Users can set alarm level, notification mailbox and specific threshold or time interval for each event. Through fine-grained alarm configuration, administrators can receive timely interface alerts or email notifications to effectively handle system exceptions.

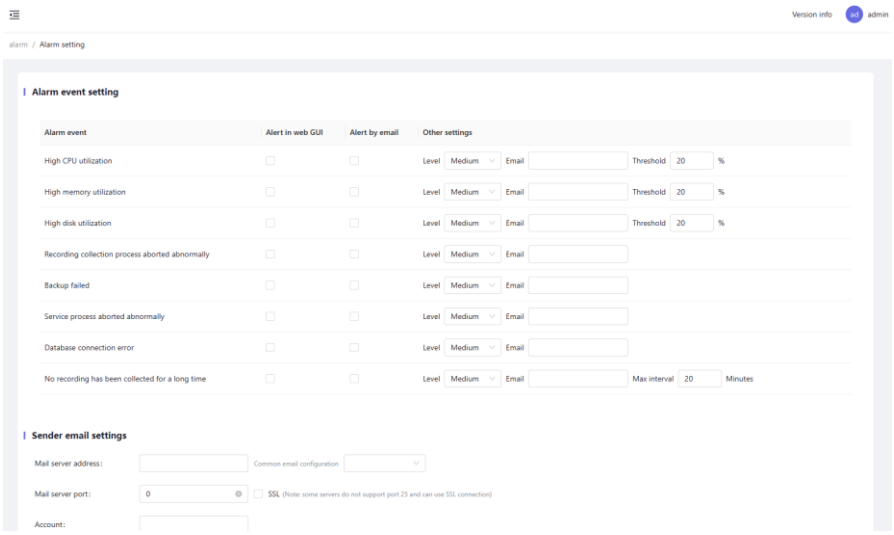


Figure 39 Alarm Event Settings

Sending mailbox setting is used to configure the mailbox information of the system to send alarm emails to ensure that the alarm notification can be sent to the relevant person in charge in time. Users can fill in the mailbox server address, select common mailbox configurations to simplify the setup process, and specify the mailbox server port number (SSL encrypted connection is supported to cope with the situation that some servers do not support port 25). Enter your email account and password to complete the authentication.

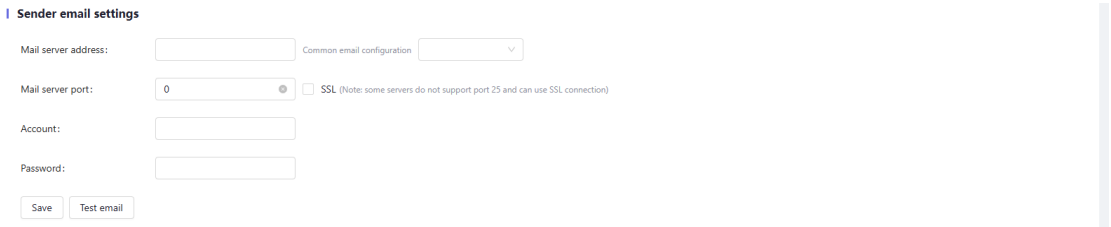


Figure 40 Sending Mail Settings

8. System settings

This section provides various global configuration and management features for the AS Series system. With this module, administrators can effectively manage devices, application services, license information, and data maintenance operations.

8.1 Device Management Interface

The Device Management section allows administrators to monitor and manage all devices in the system. This includes viewing the current status of the device, configuring device details, and performing necessary maintenance operations. The following are the specific steps for device management and the key features of the interface.

Step .1 Access the list of devices:

The system will display a list of devices with each device's name, MAC address, device type, FSP security code, recording cache address, and local CDR to save key information. Users can quickly understand the current status and basic configuration of the device through this list.

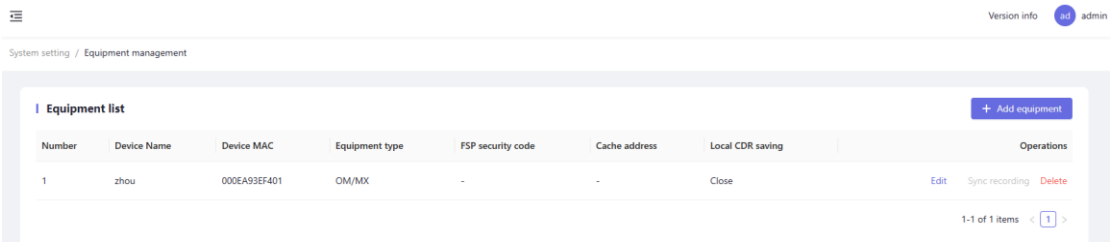


Figure 41 Device management interface

Step .2 Edit device information: Click the "Edit" button next to the device you want to edit to open the "Edit Device" dialog box.

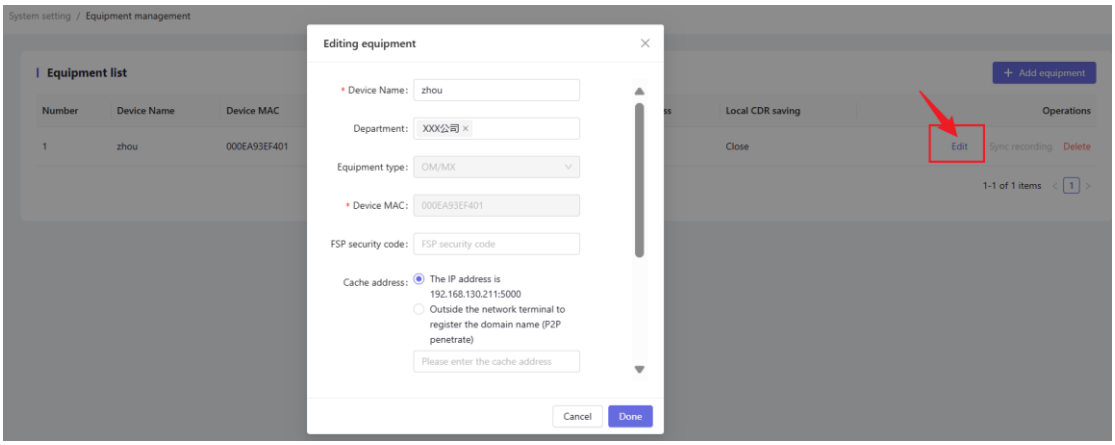


Figure 42 Edit device operation interface

Item	Definition
Equipment name	In the Device Name field, enter or modify the name of the device.
Sectoral	Fill in the appropriate departmental information here
Equipment type	Select the type of device from the Device Type drop-down menu. This field is grayed out in the interface and is not editable because the device type is determined when the device is added and cannot be changed in subsequent edits
MAC address	Enter or modify the MAC address of the device. This field is grayed out in the interface and is not editable because the MAC address is the unique identifier of the device, which is determined when the device is added and cannot be changed in subsequent edits
FSP security code	: The FSP (Field Security Protocol) security number is a security authentication code used to identify and verify the identity of a device. This number ensures that only authorized devices can access the system when the device requires specific secure communications or data exchange. If your device settings include FSP security, you will need to enter the correct security number in this field so that the system can confirm the legitimacy of the device and enable the appropriate security measures

Recording cache address	iP Address: You can choose to set the IP address of the device. Extranet Terminal Registration Domain Name: Alternatively, select Extranet Terminal Registration Domain Name (P2P Penetration) to allow devices to be accessed via the Internet without disclosing the device's real IP address, which improves security and simplifies remote access setup.
Default Time Zone	Select the time zone of the device from the drop-down menu
Get Interval	Fill in the interval time in minutes and set it according to your needs.
Synchronizing local CDR saves	Choose to turn this item on or off to determine whether Call Detail Records (CDRs) are saved to the device's local storage.
Select Application Services	This step lets you decide whether to enable application services. If enabled, you can select the desired local application service from the drop-down menu, e.g. local AS service

Table 17 Editing Device Operator Interface Definitions

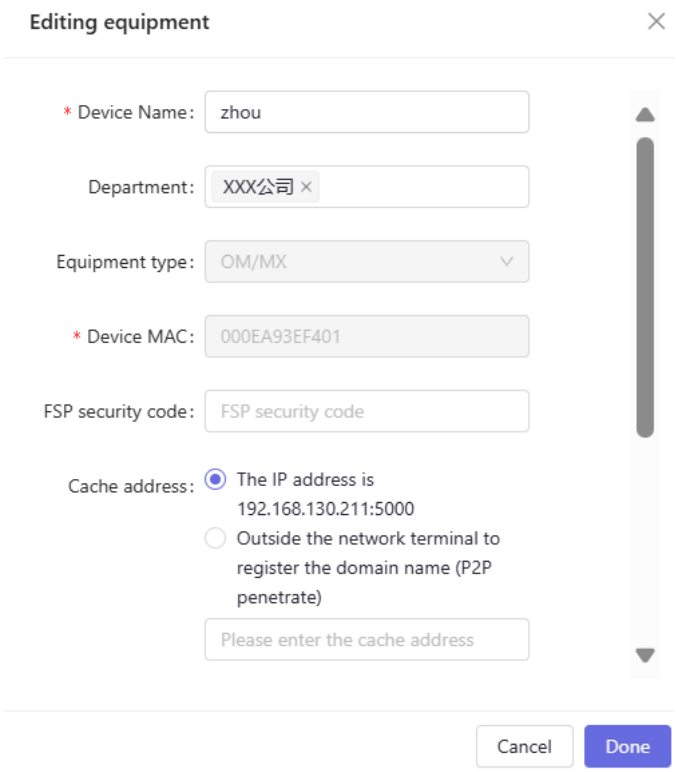


Figure 43 Device management editing interface

Step .3 Apply or cancel changes.

Step .4 Add device.

Administrators can register new hardware or software to the system by clicking the "+Add Device" button on the interface. This includes physical devices such as servers and switches, as well as software components such as OMX.

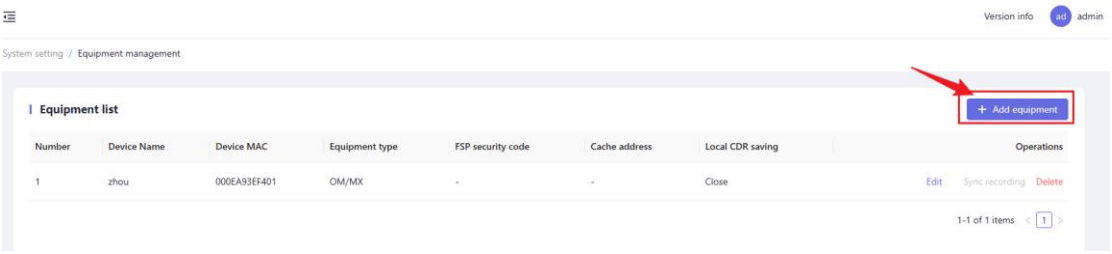


Figure 44 Device management interface

Administrators can register new devices to the system by clicking the "+Add Device" button on the interface.

Step .1 Click the "+Add Device" button to open the "Add Device" dialog box.

Step .2 Enter or select device details including name, department, device type (either hardware or software, e.g. OMX as a software component), MAC address, FSP security code, recording cache address, IP address, domain name of the

extranet endpoint registry, default time zone, fetch interval, local CDR saving and application services.

Step .3 After confirming that the information entered is correct, click the "Finish" button to save and register the new device.

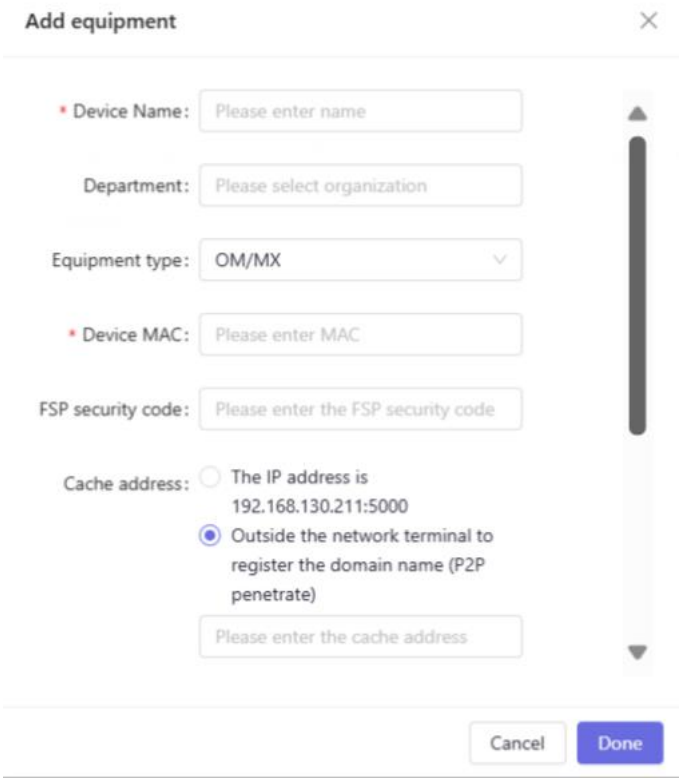


Figure 45 Add Device

Note In the "Add Device Type" option, "OM" and "OMX" are displayed. In fact, when you select the "OM" type, you can add not only OM devices but also MX devices. Selecting the "OM" type includes both OM and MX devices.

Remove the device:

Step .1 Select the device to be deleted in the device list.

Step .2 Click the "Delete" button next to the device and a confirmation dialog box will pop up.

Step .3 Confirm the deletion operation in the confirmation dialog and the device will be completely removed from the system, or select Cancel to terminate the

deletion operation.

8.2 Recording Configuration

NewLync manages recordings from both IPPBX and cloud PBX systems. Recordings are uploaded from IPPBX and cloud PBX to NewLync, where administrators can centrally view, playback, and download them. To enable recording and Call Detail Record (CDR) data upload and management, register each branch's OM IPPBX device to the NewLync AS platform. Simultaneously, ensure recording functionality is enabled for all extensions.

IPPBX Configuration Recording Upload

Step.1. Navigate to System Settings > Application Services, then click Add Application.

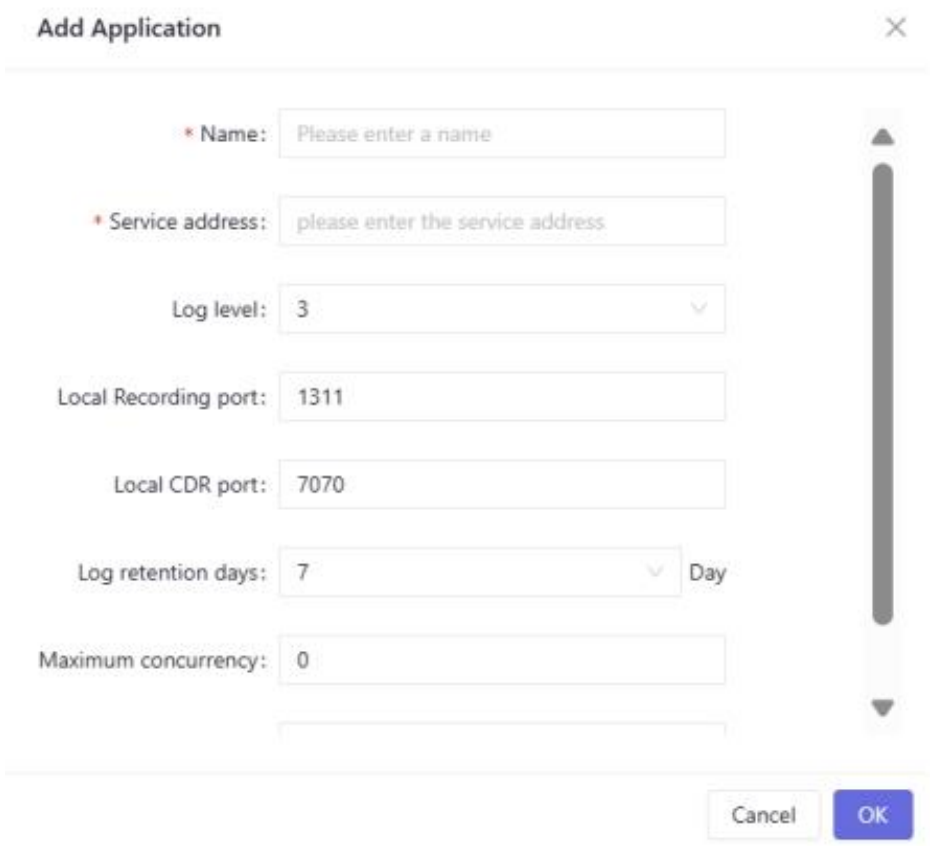


Figure 46 Add application Interface

Configuration options	Description
Name	Fill in as required
Server Address	The IP address of this server, in the format http://192.168.131.82:1311
Log Level	3
Local Recording port	1311
Local CDR port	7070
Log retention days	7
Maximum concurrency	After installation, the default is 5 concurrent connections. After importing the license file , change the concurrent connections to match the certificate .

Table 18 Add Application Interface Definition

Step.2. Navigate to System Settings > Recording Nodes, click Add Node, and select AS as the node type.

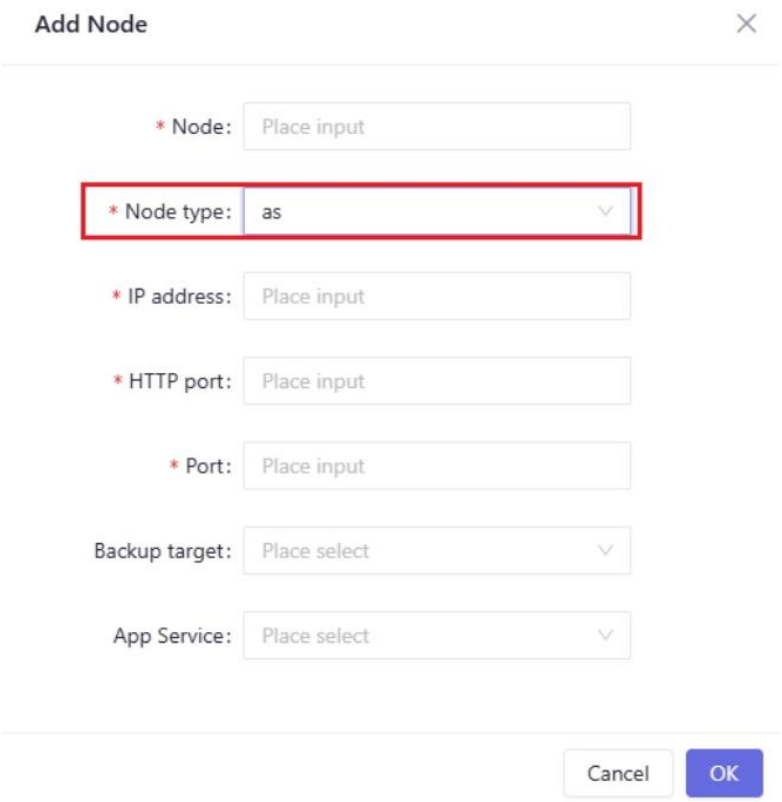


Figure 47Add Node Interface

Configuration options	Description
Node name	Enter local_node
Node type	Select as
IP address	The IP address of this server, in the format 192.168.131.82
HTTP port	80
Port	8091
Backup target	Empty
App service	Select the previously added service

Table 19 Node Add Interface

Step.3. Navigate to System Settings > Device Management, then click Add Device to add the corresponding OM/Unified Communications Platform (OMX) device.

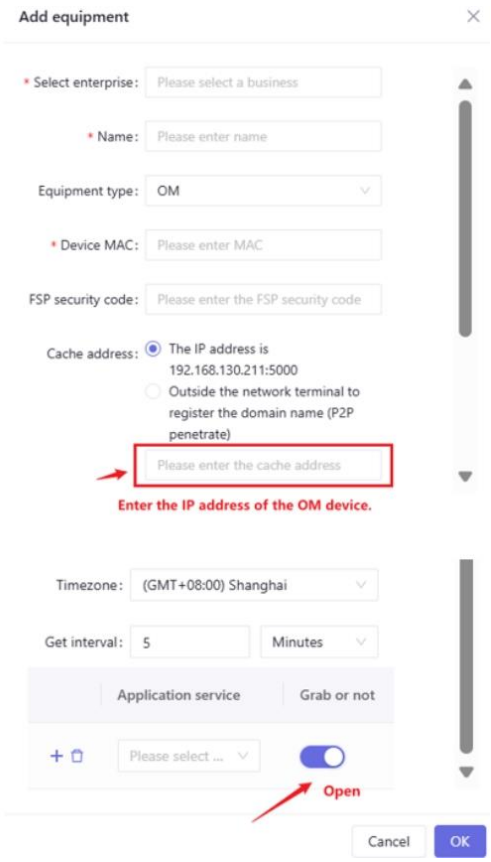


Figure 48 Add Device Interface

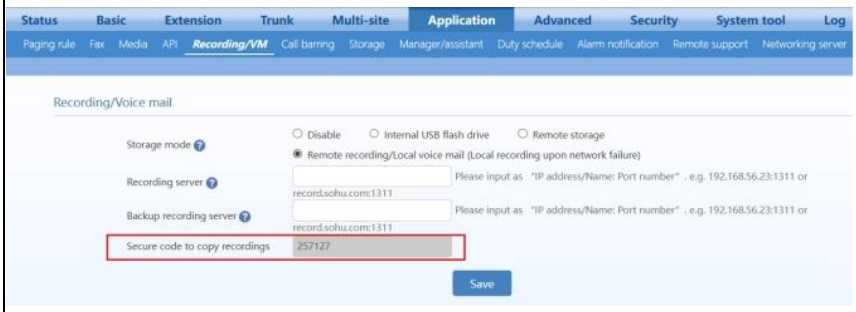
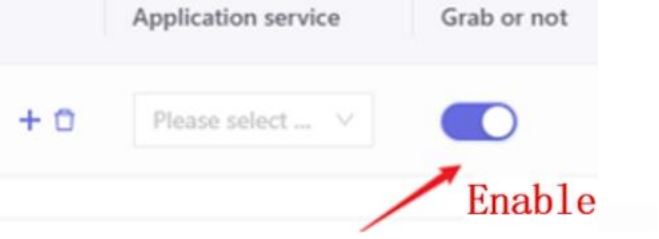
Configuration items	Description
Select enterprise	Select the affiliated enterprise or branch.
Name	Enter the device name. It is recommended to name it as "branch name + OM".
Equipment type	Select OM.
Device MAC	Enter the MAC address of the device.
FSP security code	Enter the FSP security code. After entering the OM device backend, navigate to >Application>Recording/VM, click the Remote recording/Local voice mail (Local recording upon network failure) option, and view the security code. 
Cache address	Select "The IP address" and enter the IP address of the OM device.
Timezone	Select the time zone where the device is located.
Get interval	Set the interval for data synchronization. We recommend 5 minutes.
Application service / Grab or not	Select the configured application service and enable Grab 

Table 20 Add Device Interface

Add OMX

Navigate to CDR Recording Management > Device Management, then click Add Device.

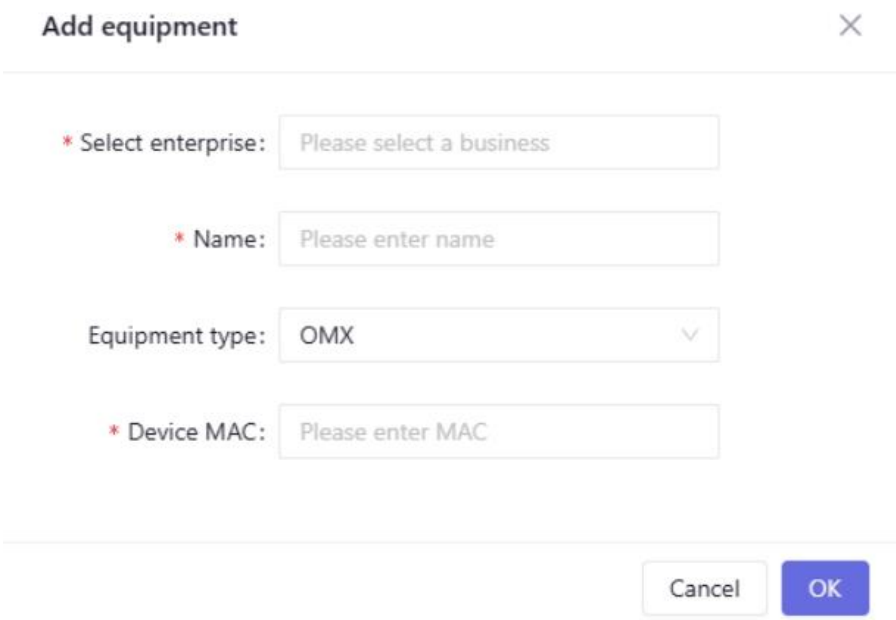


Figure 49 Add OMX Device Interface

Name	Definition
Select enterprise	Select the corresponding enterprise
Name	Fill in as required
Equipment type	Select OMX
Device MAC	Enter the tenant ID corresponding to the OMX tenant of the enterprise

Table 21 Add OMX Device Interface Definition

Step.4. Log in to OM WEB, click Application Services > Recording/Voicemail, enable Remote Recording, and enter the recording server address.

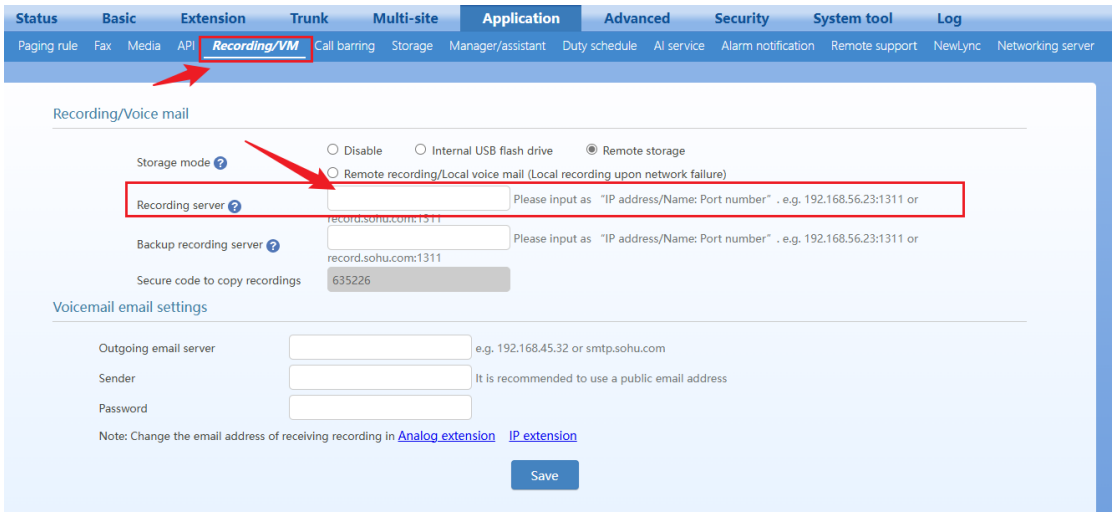


Figure 50 Enable Remote Recording Interface on OM

Step.5. Click Extension Settings > IP Extension to enable recording for the IP extension.

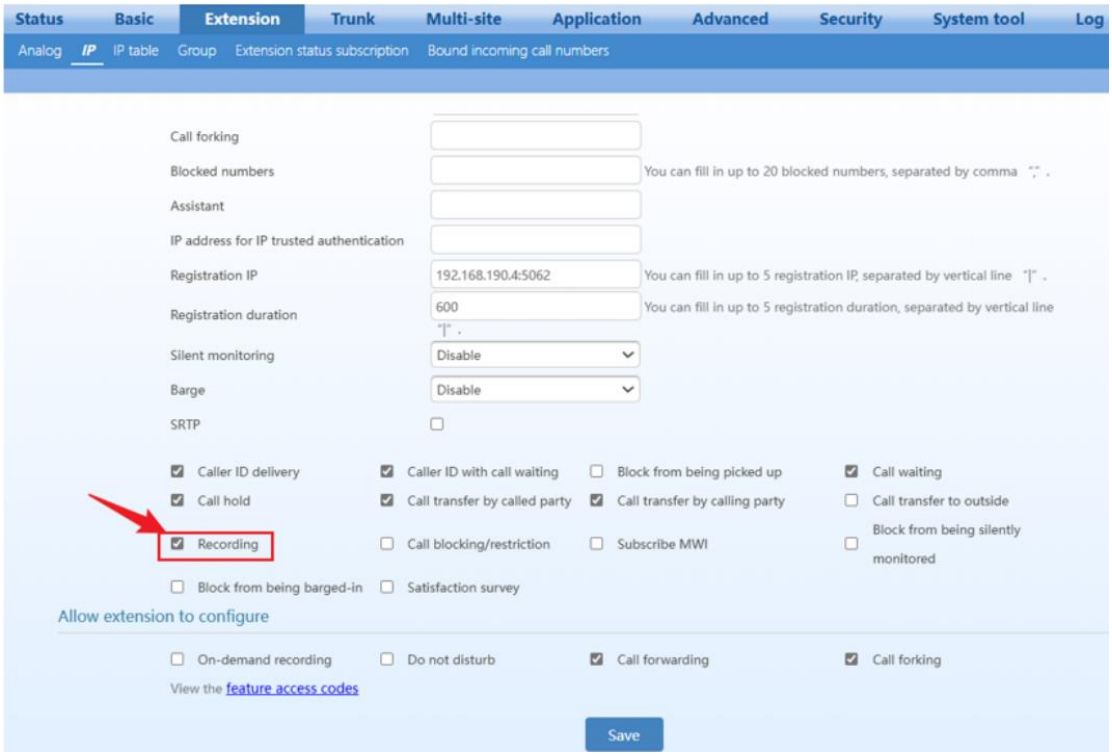


Figure 51 Enable Remote Recording Interface on OM 2

Configure the recording reporting function on the integrated communication platform

After registering the OM device on the SSC Operations Platform, you must also configure the recording reporting function on the Unified Communications Platform

(OMX) to ensure that call recordings are correctly transmitted back to the server for centralized management and storage.

Access the Unified Communications Platform Web interface: Use a browser to access the Unified Communications Platform Web interface. The URL is: http://192.168.130.71:8085 . (Modify according to the URL of the server you deployed.)

Step.1. Log in to the Unified Communications Platform Web interface: Enter the administrator account, password, and account name to log in.

Default username	superadmin
Default password	ShnewR0ck12
Default account name	master

Step.2. After logging in successfully, click the admin account in the top-right corner

Step.3. After entering the control center, click "Account" in the left-hand menu to access the tenant configuration page.

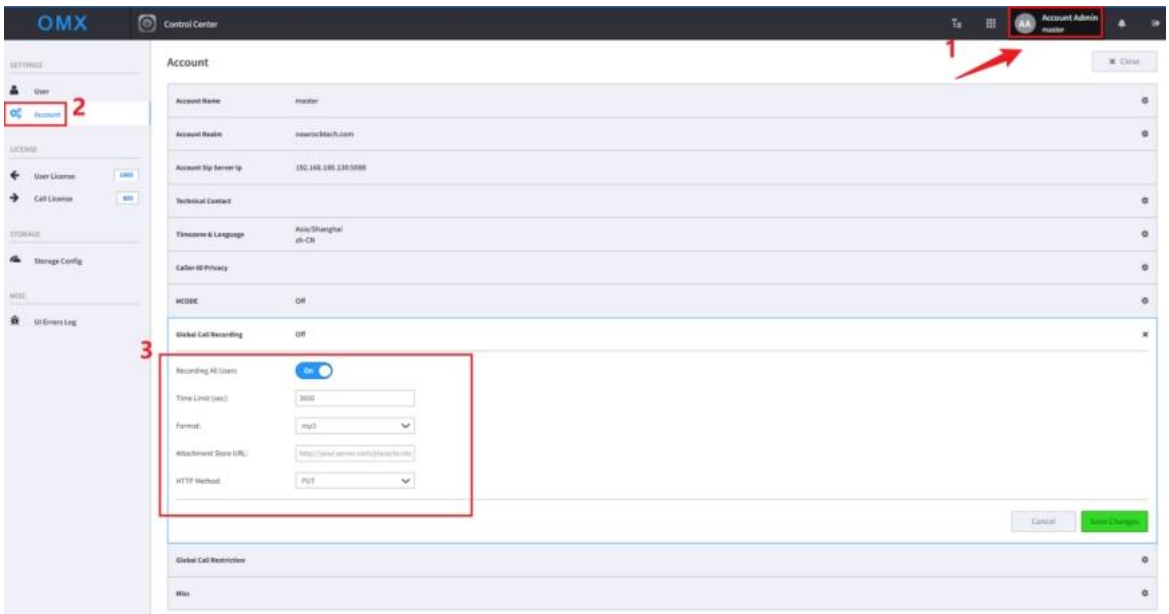


Figure 52 Unified Communications Platform Tenant Configuration Interface

Name	Definition
Record all users	It is recommended to enable this option, which indicates that the system will automatically record all extension calls. If you only need to enable recording for specific extensions, you can disable this option and enable it individually on the corresponding extension configuration page.
Time Limits(sec)	Default 3600
Format	Default mp3
Record URL: Storage URL	Change to your server's IP address, in the format http://192.168.131.82:8096/recording
HTTP Method	Select POST

Table 22 Configure recording report parameters on the unified communications platform

8.3 Authorization Information

After completing the installation of the AS Series Recording Management System, the next step is to import the License to activate and enable the full functionality of the system. License is the key to the operation of the system and ensures legal use of the software and access to its features. Please follow the steps below to import License correctly.

Get the License request file:

Step.1 Log in to the AS Recording System Administration Platform.

Step.2 Navigate to the "System Settings" section and select the "License Information" option.

Step.3 Click Get License Request ID to generate a license request file (.csr file). This file contains the system information necessary to request an official License file.

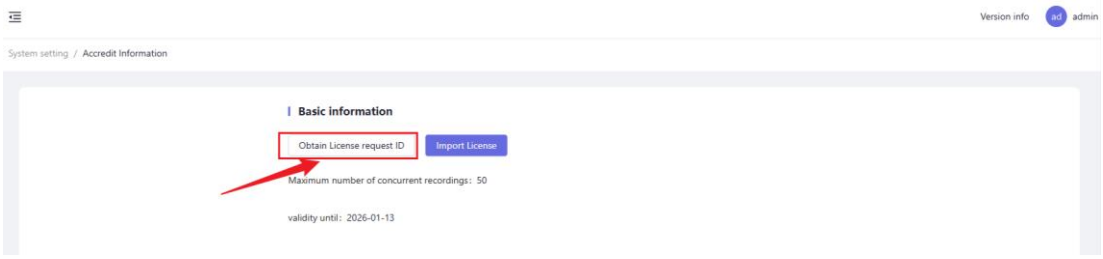


Figure 53 Getting the License Request ID

Step.4 Follow the prompts to save the resulting .csr file to your local computer, which will need to be sent to your distributor to obtain the appropriate License.

Submit a License request and receive the License file

Step.1 Send the .csr file to your supplier or to Newswire Communications. The License file is generated according to the number of services you have purchased.

Step.2 After processing your request, the supplier will send you a document

containing the official License.

Import the License file:

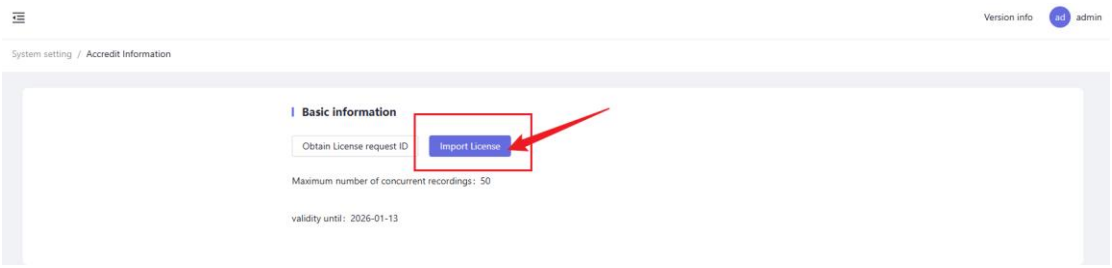


Figure 54 Import License

Step.1 Select Import License.

Step.2 In the pop-up window, browse and select your License file.

Step.3 After selecting the file, click "Open" to upload the file. The system will automatically process and verify the validity of the License file.

Verify the License status:

After the License file is uploaded, the system will automatically verify the validity of the License. If the system shows that the license is valid, it means that the license has been imported successfully and the system has been activated successfully. The page will display key information about the License, such as:

- Maximum number of concurrent recordings: 20
- Valid until: 2024-08-13

Verify that the License information displayed is what you expect and that the system features are activated correctly. If the display status is invalid or an error occurs, check that the License file is correct or contact your vendor for further support.

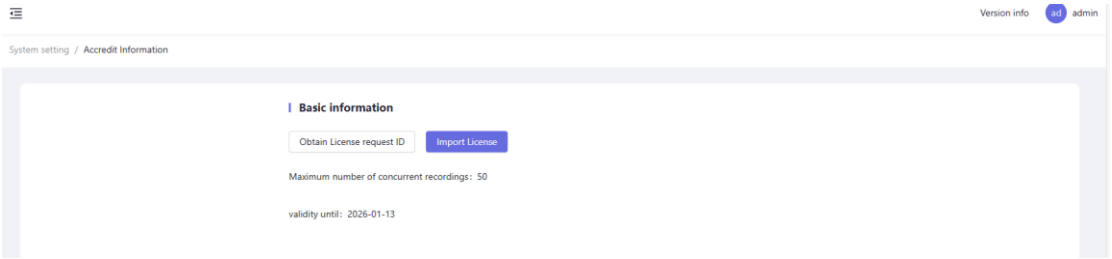


Figure 55 Check if the License file is imported correctly

8.4 Data Maintenance

Through the data maintenance interface, administrators can easily view and manage the data in the system and perform the necessary cleanup operations to ensure efficient system operation and effective data management.

Step.1 After logging in to the AS management background, click "System Settings" in the left menu, and then select "Data Maintenance" submenu to enter the Data Maintenance page.

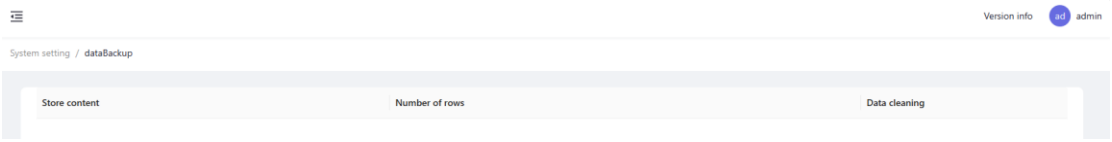


Figure 56 Data Maintenance Interface

Item	Definition
Stored content	Administrators can use this function to view all the data currently stored in the system and the corresponding data volume, and evaluate the storage status of the system.
View Entries	Displays the number of each type of data entry, helping administrators quickly understand the size and distribution of each type of data stored in the system.
Perform data cleansing	The Data Cleaning feature allows administrators to delete historical data that is no longer needed, optimizing system performance.

Table 23 Data Maintenance Interface Definitions

Step.2 Select the time period to be cleaned and click Confirm.

After confirming the cleanup operation, the system perTable data cleanup and updates the list of stored contents to show the latest number of data entries.

Step.3 After data cleansing is complete, the system will update the contents of the storage.

8.5 System settings

The system provides flexible recording storage and data backup functions to ensure the security of recording data and the stability of system operation. With a combination of local storage and backup policies, users can effectively manage storage space and quickly recover critical information in the event of unexpected data loss.

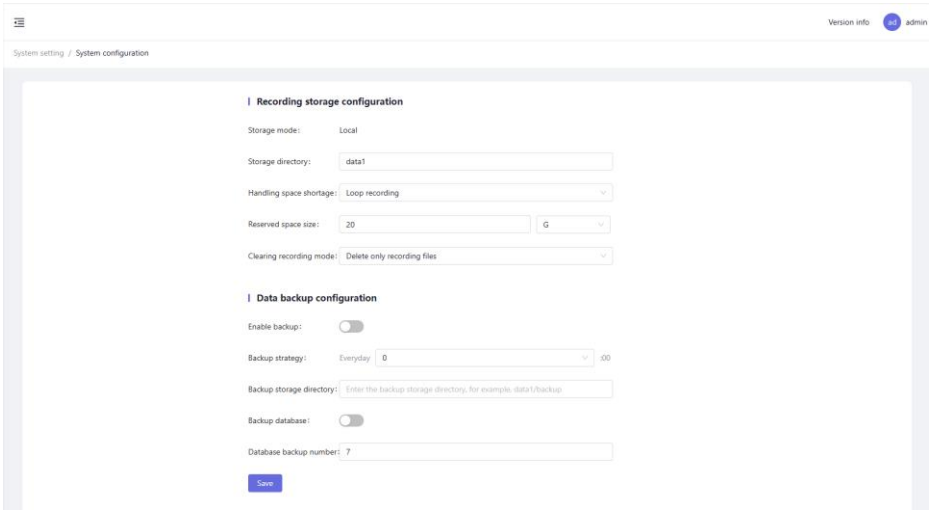


Figure 57 Recording storage interface

Item	Definition
Storage Mode	The current storage mode, which defaults to local storage.
Storage Catalog	Specified path for backup file storage
Handling of space shortages	Loop recording is currently supported
Size of space reserved	By presetting the minimum reserved space
Cleaning up the recording method	The system automatically cleans up the earliest recordings when there is insufficient space, ensuring the continuity and effectiveness of storage
Backup Strategy	Support daily scheduled backup, the default backup time for the whole point, can be adjusted according to demand
Backup Storage Catalog	Enter the storage directory, e.g. data1/backup

Database Backup	The system backs up the recording database on a regular basis and retains the latest backups (number of backups can be set on demand) to ensure data recoverability

8.6 Recording Node Functionality

The Recording Management System supports node list management, which is used to configure and maintain different types of nodes to meet the needs of backup and data management. Users can add, edit or delete nodes according to actual application scenarios.

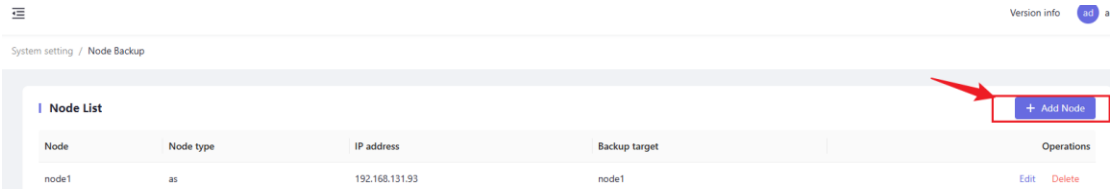


Figure 58 Add Node

Step.1 To add a node, navigate to Recording Node, click Add Node, and configure the parameters.

Edit Node

Click Edit Node to modify the configured node parameters.

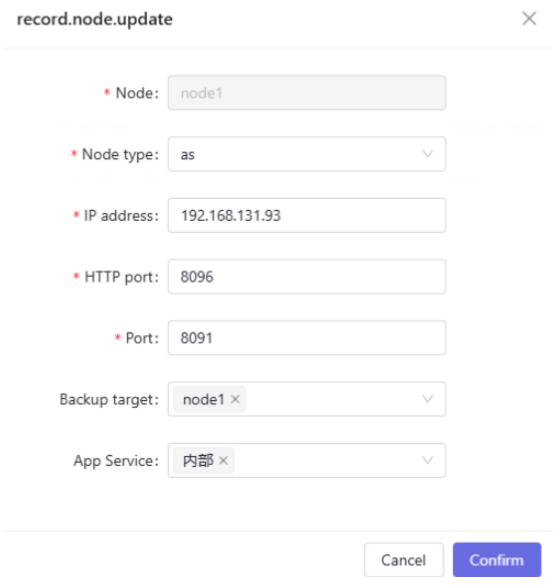


Figure 59 Edit Node

Node name; the name of the current node.

Node Type: Select the node type from the drop-down menu, the following node types are currently supported.

Item	Definition
as	Recording management system node
ftp	FTP protocol node for external storage and file transfer
http	HTTP protocol node for transferring data over the network

Other parameters

Item	Definition
IP address	Network address of the node for targeting of data transmission
ports	Port number of the current server
http	HTTP protocol node for transferring data over the network
Backup target	Name of the backup server

Delete node

Click Delete to delete the current node.

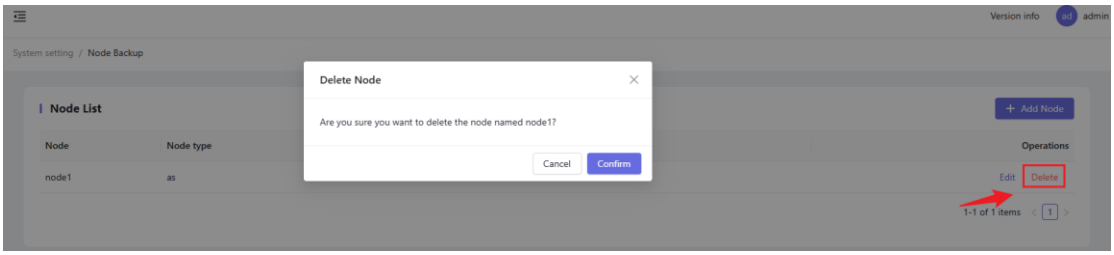


Figure 60 Deleting nodes

9. Appendices

This appendix section contains technical information related to the AS Series Recording System. The purpose is to provide network administrators and system engineers with the necessary reference material so that they can effectively manage and maintain their systems. The appendices include detailed documentation of the communications matrix, a glossary of terms, troubleshooting and frequently asked questions, and safety guidelines to help ensure that the various parts of the system are able to exchange data correctly and securely, as well as providing comprehensive information on the use and maintenance of the system.

9.1 Communications Matrix

The communication matrix is used to detail the communication configuration between individual devices in the network, including the IP addresses of the source and destination devices, port numbers, the type of protocol used, and the specific purpose of each port. The main purpose of this matrix is to ensure that data can be exchanged correctly and securely between different devices, making it easy for network administrators and system engineers to configure and maintain.

Serial number	Source system	Source ip	Destination system	Destination ip	Destination port	Protocols	Use
1	Management Computer	<Managing computers>	AS Server	<AS Server>	8082	TCP	Access to AS Management Page: Administrators access the management interface of the AS system through this port to perform system configuration and maintenance

							operations.
2	Management Computer	<Managing computers>	OM Server	<OM server>	1311	UDP	OM Remote Recording:The management computer communicates with the OM server through this port for remote recording function to ensure real-time transmission and storage of recording data.
3	Management Computer	<Managing computers>	OM Server	<OM server>	7070	TCP	OM CDR Upload: The management computer uploads Call Detail Records (CDR) data to the OM server through this port for easy recording and analysis.
4	Management Computer	<Managing computers>	OM Server	<OM server>	8080	TCP	OMX Upload Recording Records and CDR: This port is used to upload recording records and call detail records from the management computer to the OM server for centralized management and archiving.
5	Management Computer	<Managing computers>	OM Server	<OM server>	9000	TCP	OMX Upload Recording File: This port is used to upload recording files to the OM server to ensure centralized

							storage and management of recording data.
6	Management Computer	<Managing computers>	OM Server	<OM server>	3389	TCP	LDAP Service: The management computer accesses the LDAP service through this port for user authentication and directory services.

9.2 Glossary

The Glossary contains specialized terms and their explanations that appear in this manual and is used to assist the user in accurately understanding the technical expressions in the document.

Nomenclature	Definition
API (Application Programming Interface)	An API is a set of rules and tools that allow different programs to interact with each other, enabling software developers to create applications that can connect to other applications or services.
CDR (Call Detail Record)	CDR is a system that records detailed information (e.g., call length, start and end times, participant numbers) about each call activity and is used to analyze call data and calculate charges.
FSP(Field Safety Protocol)	FSP is a security protocol used to authenticate devices and ensure secure communication.
LDAP (Lightweight Directory Access Protocol)	LDAP helps computers find and manage people or device information such as e-mail addresses or printers on a network, and is commonly used for user and resource management within an organization.
RESTful	Describes a style of network architecture that manipulates resources on the network via standard HTTP methods (e.g., GET, POST, PUT, DELETE), often used in the design of APIs

	to support expressive state transfer of resources.
SSL (Security Layer Agreement)	SSL is a security protocol used to establish an encrypted connection over a computer network to ensure the security of data as it travels between the server and the client.
TCP (Transmission Control Protocol)	TCP is a network protocol that ensures that packets are transmitted accurately and without error through an acknowledgement and retransmission mechanism, and is suitable for applications that require high reliability, such as e-mail and file transfers.
UDP (User Datagram Protocol)	UDP is a fast network transport protocol that does not guarantee packet order or integrity, and the unit of transmission for UDP is called a "datagram". For video streaming and online gaming, where speed is more important than transmission reliability.
OM	The OM series converged communication platform is a new generation of Voice over IP core switching equipment
OMX	The OMX converged communication platform is a high-capacity audio and video switching device in the Newrock digital collaborative communication solution.
	is a Online Collaboration Office software developed by Communication Equipment Co.

9.3 Common Problems

In the course of using the AS Series Recording System, you may encounter some technical problems. To help administrators and technicians quickly resolve these issues, we have provided a detailed troubleshooting guide.

Question 1. Recordings are not displayed in the WEB-recording management interface

If you fail to see any recording files in the WEB-Recording management interface, please follow the troubleshooting guide below:

Step 1: Check the recording configuration on the OM: Make sure that the IP and port

configuration of the recording server is correct and the line recording function is enabled.

Step 2: Check the XML configuration of OM: Make sure the 'REC_FLAG' parameter is set to '0x8F' to enable the recording function.

Step 3: Verify the device configuration on the AS server: Verify that the OM device has been added to the AS server correctly and that the MAC address matches.

Step 4: Perform network packet capture: Use the 'tcpdump' tool on the AS server to perform network packet capture to check whether the UDP recording packets sent from port 1311 of the OM device successfully reach port 1311 of the recording server. Verify that the OM sends an end-of-recording packet containing MAC address information at the end of a call.