Application Service Series

Address Book Management System

Administrator's Manual

Document Version: 02

Release Date: 2025-10-10

NEWROCK

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

1 Contents

1 Contents....1
2 Contents of Figures....5
3 Contents of Tables....8
4 Modifying Record....9
5 Preamble....10
5.1 About this Manual....10
5.2 Document User....10
6 Products Description....11
6.1 AS Address Book Management System....11
6.2 System Features....12
7 Application Scenario....13
7.1 Enterprise communications management....13
7.2 Cross-departmental and cross-platform collaboration....13
7.3 Large-scale user support and resource optimization....14
7.4 Flexible permissions and security management....14
8 AS Series Software Deployment and Installation....15
8.1 Pre-Installation Environment Configuration....15

8.1.1 List of Files Required for Installation....16
8.1.2 Create User Accounts....17
8.1.3 Granting sudo privileges to users....18
8.2 Installing NewLync-AS (Single-Machine Deployment)....18
8.3 Install NewLync-AS (Dual-Server Deployment)....21
8.4 Firewall Configuration....24
8.5 Accessing and Logging into the NewLync-AS Management System Platform....26
8.6 Import License....27
8.7 AS Series License Features Overview....29
8.8 Function Comparison Table....32
9 Configuring AS....33
9.1 Organizational Structure....33
9.1.1 Membership and Sectors....33
9.1.2 Address Book Settings....39
9.1.3 LDAP....40
9.1.3.1 Enabling the LDAP server....40
9.1.3.2 LDAP Schema Settings....41
9.1.3.3 LDAP client configuration....42
9.1.3.4 Creating an LDAP account....44
9.1.3.5 Contacts Permissions Management....46

9.1.3.6 Add an LDAP server to the phone 49
9.1.3.6.1 Fanvil Phone (using the V61W model as an example) ... 49
9.1.3.6.2 Yealink Phone 51
9.1.3.6.3 HuaWei Phone 52
9.1.3.7 Quickly search cloud contact list members via the phone (Using the NRP1312 phone as an example) 53
9.2 User Groups 54
9.3 Enterprise Settings 54
9.3.1 Corporate Information 54
9.3.2 Administrative Authority 56
9.3.2.1 Transfer creator 56
9.3.2.2 Add Super Administrator 56
9.3.2.3 Add Administrator 57
10 Alerts 59
10.1 Alarm Log 59
10.2 Alarm settings 60
11 System Settings 62
11.1 Authorization Information 62
11.2 Data Maintenance 64
11.3 System settings 66
11.4 Recording Node Function 67

12. Appendix..... 70

12.1 Communications Matrix 70

12.2 Glossary.....71

2 Contents of Figures

Figure 1 AS management system login screen 27
Figure 2 Getting the License Request File 28
Figure 3 Import License.....29
Figure 4 Checking License Status 29
Figure 5 AS Trial License Interface.....30
Figure 6 New sectors 33
Figure 7 Setting up department heads 34
Figure 8 Editorial office 34
Figure 9 Import Export Members.....35
Figure 10 Import Export Members.....35
Figure 11 Download Template.....36
Figure 12 Uploading departmental information.....36
Figure 13 Download Template.....37
Figure 14 Adding Members 37
Figure 15 Modify member information 38
Figure 16 Name modification settings 39
Figure 17 Position grading 40

Figure 18 Position grading 40
Figure 19 Enabling the LDAP server 41
Figure 20 LDAP Schema Configuration 42
Figure 21 LDAP client configuration interface 43
Figure 22 LDAP client account configuration screen 44
Figure 23 Add Account 44
Figure 24 Modifying the LDAP account 44
Figure 25 Edit LADP account 45
Figure 26 Edit LDAP account screen 45
Figure 27 Edit LDAP Account Interface 46
Figure 28 Fanvil Phone Configuration LDAP Interface. 49
Figure 29 Configure LDAP Parameters for Yealink Phones 51
Figure 30 NRP Phone Contact Search Interface 53
Figure 31 Modify basic enterprise information 55
Figure 32 Transfer creator 56
Figure 33Add Super Administrator 57
Figure 34 Add Administrator 57
Figure 35 Edit Administrator Privileges 58
Figure 36 Alarm log interface 59
Figure 37 Alarm Event Settings 60
Figure 38 Sending Mail Settings 61

Figure 39 Getting the License Request ID 63

Figure 40 Import License 63

Figure 41 Check if the License file is imported correctly 64

Figure 42 Data Maintenance Interface 65

Figure 43 System setup interface 66

Figure 44 Add Node 67

Figure 45 Edit Node 68

Figure 46 Deleting nodes 69

3 Contents of Tables

Table 1 Compatibility Requirements Table 16
Table 2 Number of concurrent recordings supported 16
Table 3 Installation File Information Sheet 17
Table 4 Firewall Port List 25
Table 5 Function Comparison Table 32
Table 6 Explanation of the Modify Member Information screen 38
Table 7 LDAP Server Parameters 41
Table 8 LDAP Configuration Definitions 43
Table 9 Edit LDAP Account Interface Definitions 45
Table 10 Edit LDAP Account Interface Definition 47
Table 11 Multi-level Permission Control Definition 47
Table 12 Configure LDAP Parameters for Fanvil Phones 51
Table 13 Configure LDAP Parameters for Yealink Phones 52
Table 14 Configure LDAP Parameters for HuaWei Phones 52
Table 15 Enterprise Basic Information Interface Definition 55
Table 16 Adding an Administrator Interface Definition 58
Table 17 Data Maintenance Interface Definitions 65

4 Modifying Record

Document Version 02 (2025-10-10)

Update LDAP configuration content.

Document Version 01 (2025-01-10)

Full Version.

5 Preamble

5.1 About this Manual

This manual is designed to help businesses and individual users fully utilize the features and benefits of the AS Address Book Management System. The manual covers product overviews, operating instructions, and practical application scenarios in a clear, well-structured format for first-time users and system administrators.

5.2 Document User

- IT administrator: responsible for the deployment and daily maintenance of the system to ensure stable and efficient system operation.
- Enterprise managers: Optimize resource management and personnel collaboration efficiency by analyzing address book data to enhance organizational operations and management capabilities.
- Technical support engineers: solve all kinds of technical problems encountered by users and provide professional advice.

6 Products Description

6.1 AS Address Book Management System

AS Address Book Management System is an enterprise-level address book management solution focused on meeting the organizational structure and phone book management needs of large-scale enterprises and organizations. The system provides efficient organizational structure management, user rights allocation and multi-terminal collaboration functions. Through strong compatibility and flexible deployment, the system can be adapted to a variety of enterprise environments, helping enterprises optimize internal communication and resource management.

The system includes the following core functions:

- ✓ Organizational structure management: support the management of multi-level organizational structure, without limiting the number of levels.
- ✓ Address Book Permission Management: Allows access to the address book to be set by department or individual, supports whitelist function to protect sensitive information.
- ✓ Third-party system interfacing: Support LDAP protocol interfacing.

6.2 System Features

- Large-scale user support: The system is designed to support an unlimited number of users to meet the needs of large groups and institutions for complex organizational structures and large-scale address book management.
- High compatibility and multi-terminal collaboration: support PC terminal, APP terminal and mainstream phone terminal to work together to realize full scene coverage. Compatible with a variety of mainstream phone brands (such as Huawei, Yealink, Hanlong, square, Cisco, etc.), support for the old equipment, reduce the cost of investment in the enterprise.
- Flexible rights management: provide grouping rights allocation function, can be assigned access rights by department, position, user.

7 Application Scenario

7.1 Enterprise communications management

AS Address Book Management System provides comprehensive address book management features to help organizations centrally manage employee contact information. The system supports intelligent categorization and filtering based on department, position and other information, which facilitates quick querying and updating of employees' contact information.

7.2 Cross-departmental and cross-platform collaboration

AS address book management system not only supports PC terminal and APP terminal, but also compatible with mainstream phone terminals, helping enterprises to realize full-scene coverage to meet the communication needs of different work scenarios. Whether at their desks or on the move, employees are able to access and update their address book information at any time from different devices. The high compatibility of the system allows it to work seamlessly with existing equipment and systems, reducing equipment replacement costs for organizations.

7.3 Large-scale user support and resource optimization

AS address book management system is designed to support large-scale user management and meet the needs of large groups and organizations in address book management. Regardless of the increase in the number of employees in the organization, the system can provide stable and efficient support to ensure the accuracy and real-time update of address book data. With centralized address book management, enterprises can effectively optimize internal communication processes and improve information sharing efficiency. At the same time, the system also provides a whitelist function to protect sensitive information and further enhance enterprise data security.

7.4 Flexible permissions and security management

In order to meet the permission needs of different departments and employees, AS Address Book Management System provides flexible permission assignment function. Administrators can assign access rights to different users by department, position, or individual, ensuring that people at different levels can only access address book data relevant to their work. Such permission setting not only improves data security, but also effectively avoids unrelated personnel from accessing sensitive information, thus enhancing the information protection capability within the enterprise.

8 AS Series Software Deployment and Installation

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

8.1 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

8.1.1 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.xxxxxxxxxxxxxx.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

8.1.2 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.

8.1.3 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.



8.2 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.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. 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
```

8.3 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.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. 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
```

8.4 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
```

8.5 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.

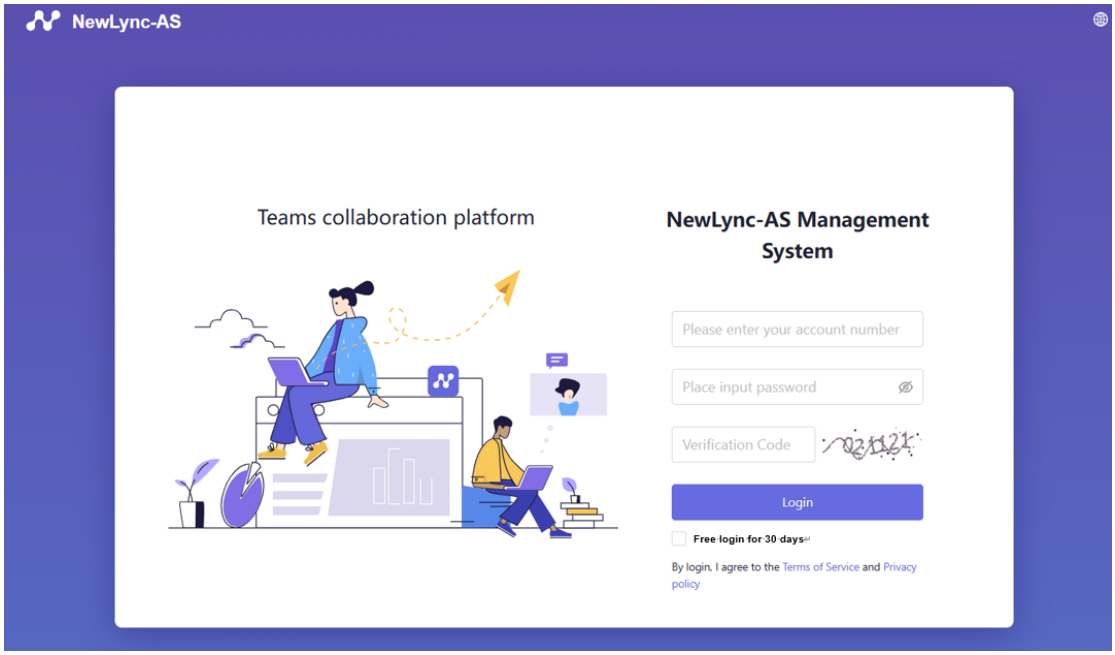


Figure 1 AS management system login screen

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.

8.6 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).

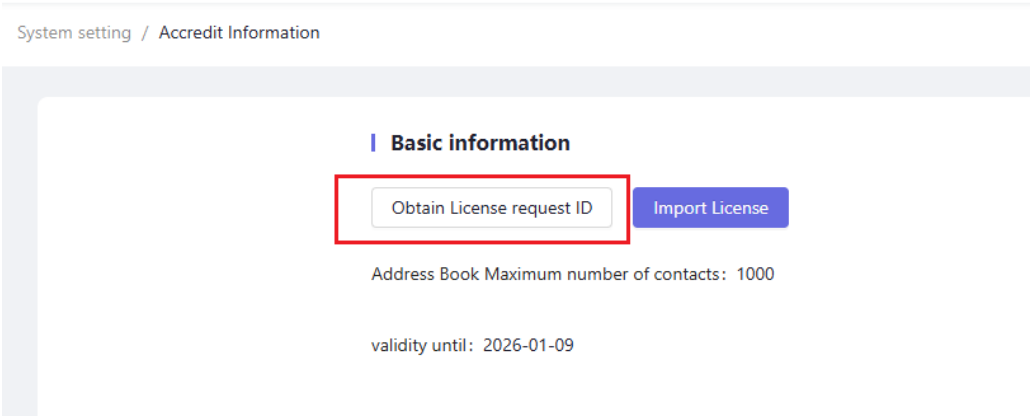


Figure 2 Getting the License Request File

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:

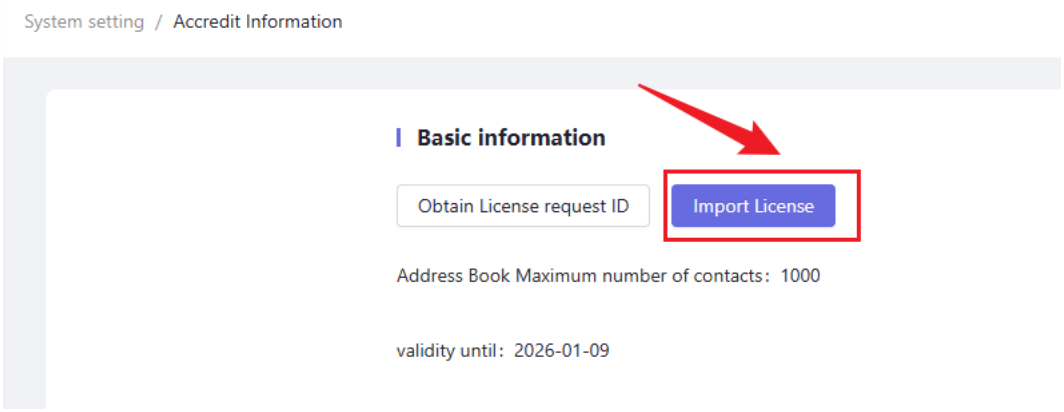


Figure 3 Import License

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.

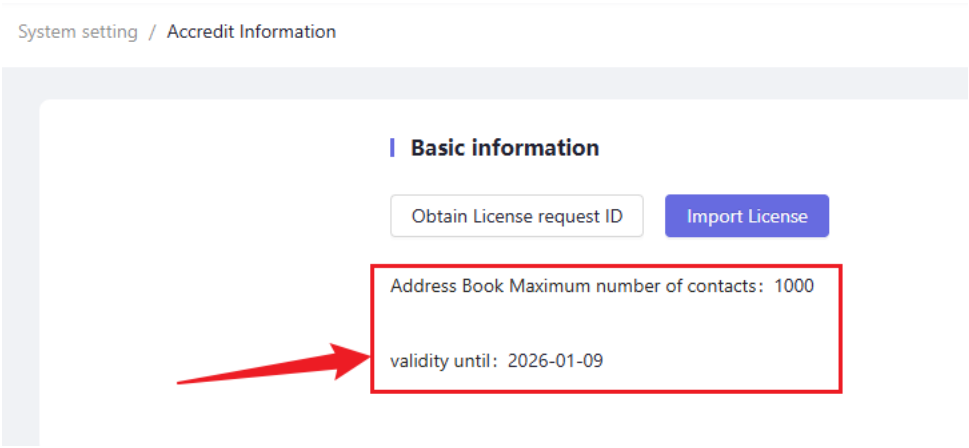


Figure 4 Checking License Status

8.7 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.

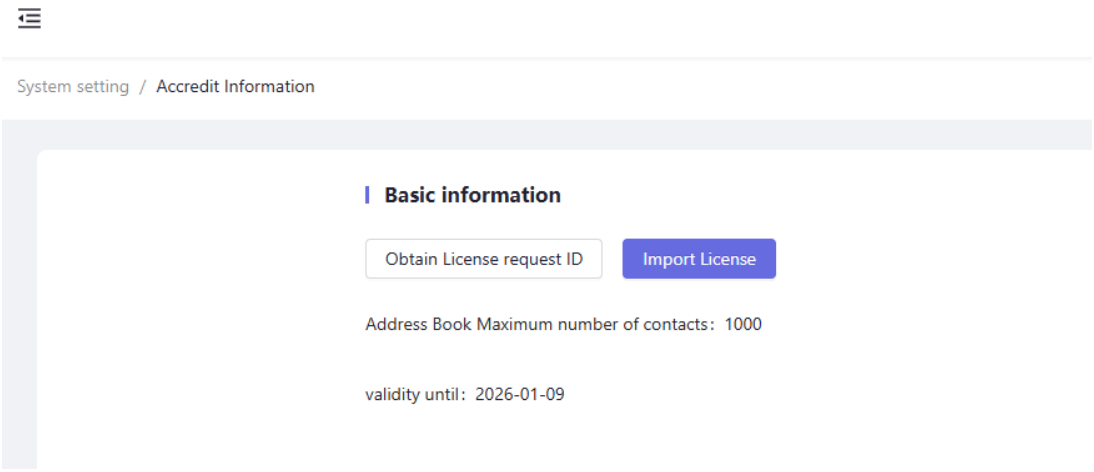


Figure 5 AS Trial License Interface

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.

8.8 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

9 Configuring AS

9.1 Organizational Structure

9.1.1 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.

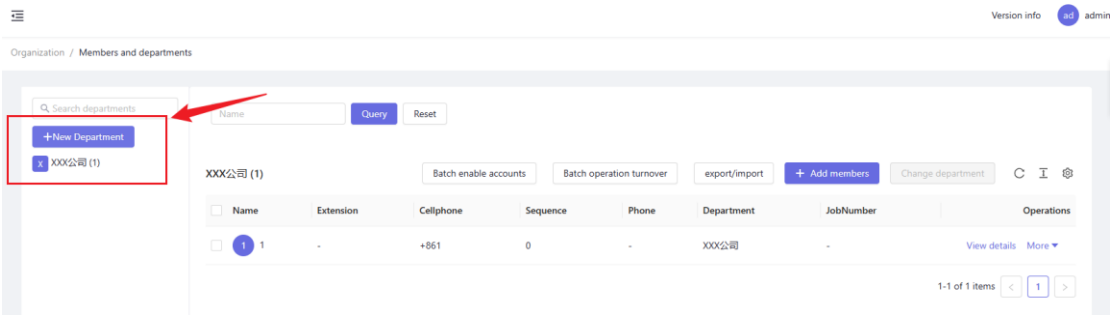


Figure 6 New sectors

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

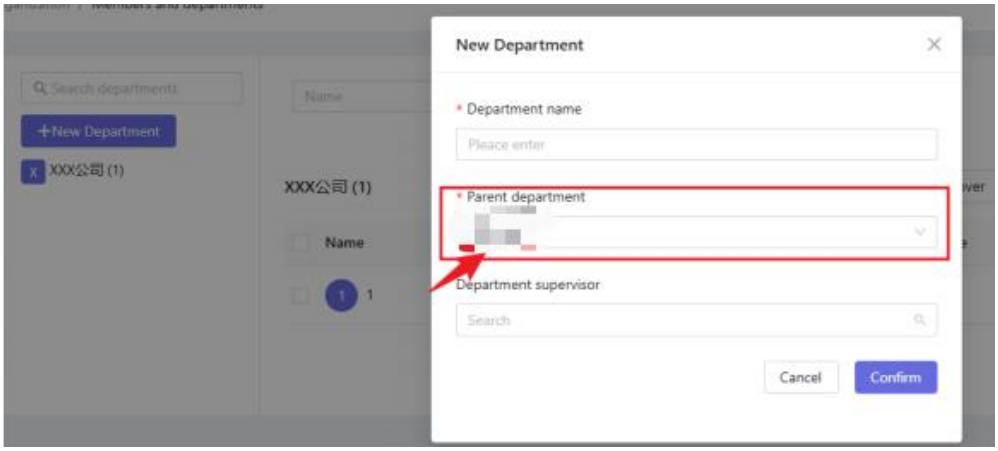


Figure 7 Setting up department heads

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.

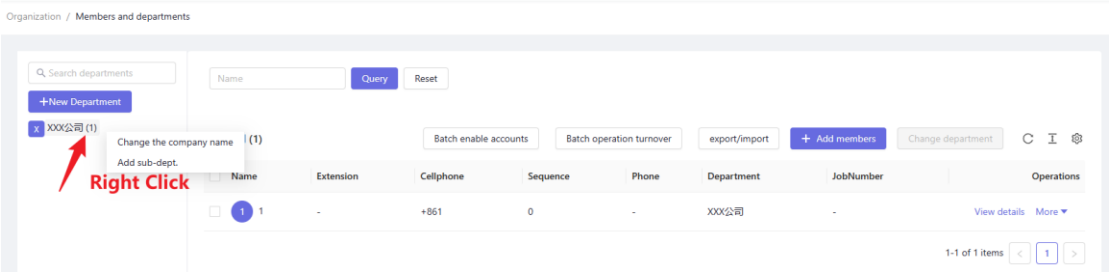


Figure 8 Editorial office

Import Export Membership

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

Step.2 Click Import Export.

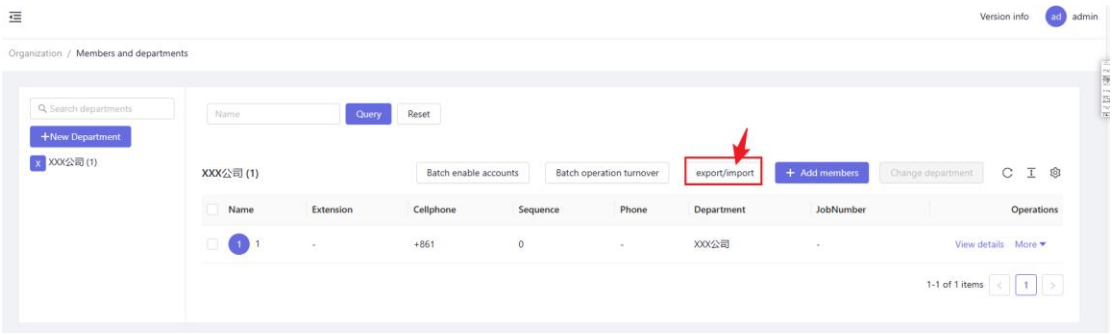


Figure 9 Import Export Members

Step.3 Click Export Members to export all members.

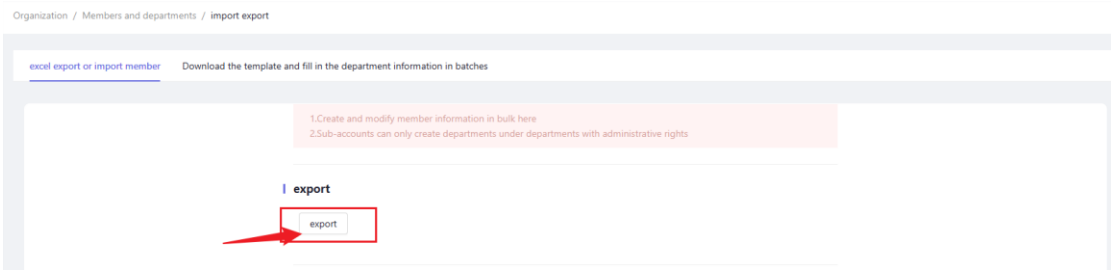


Figure 10 Import Export Members

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 Forum structure.

Import Export Department

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

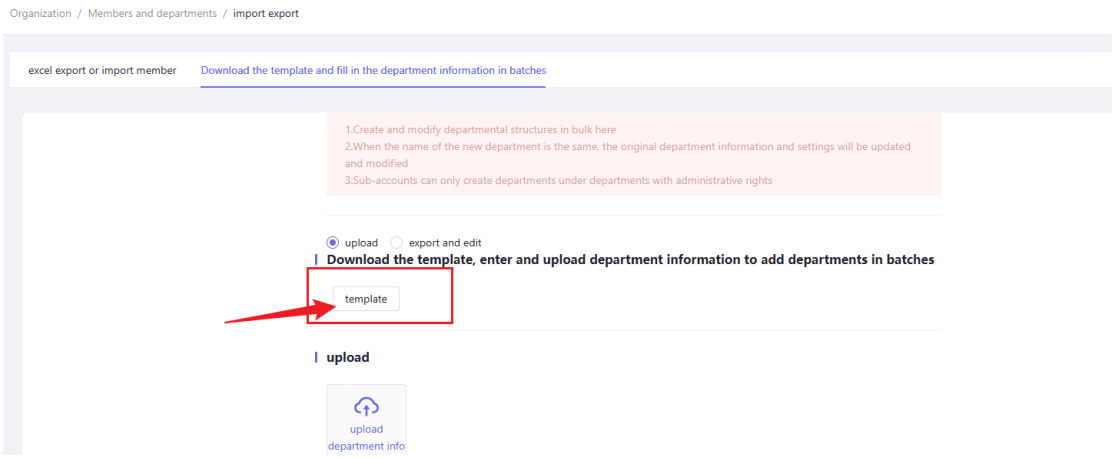


Figure 11 Download Template

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

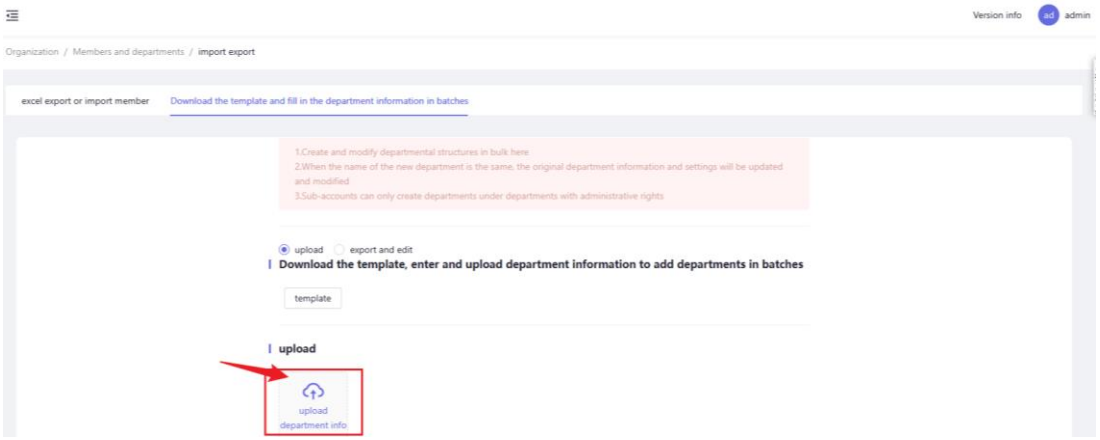


Figure 12 Uploading departmental information

Step.3 Export and modify departments

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

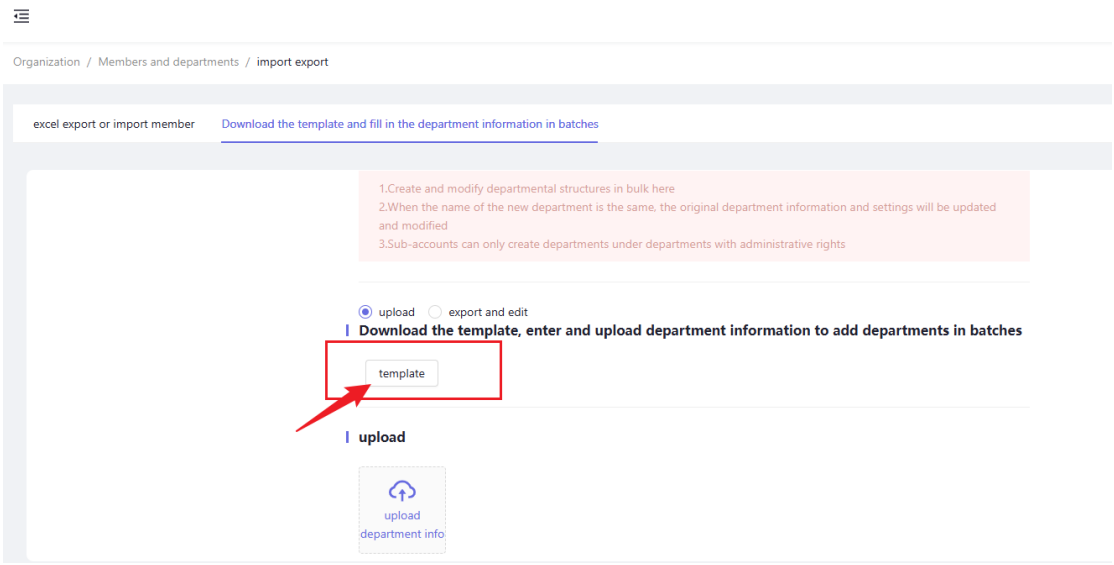


Figure 13 Download Template

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.

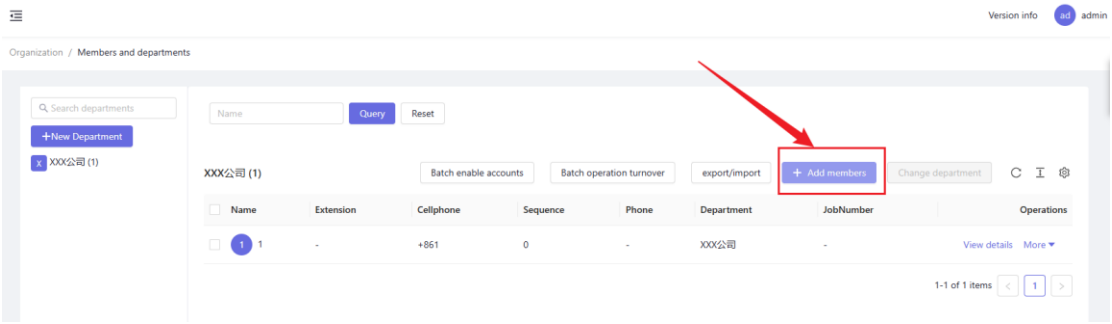


Figure 14 Adding Members

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.

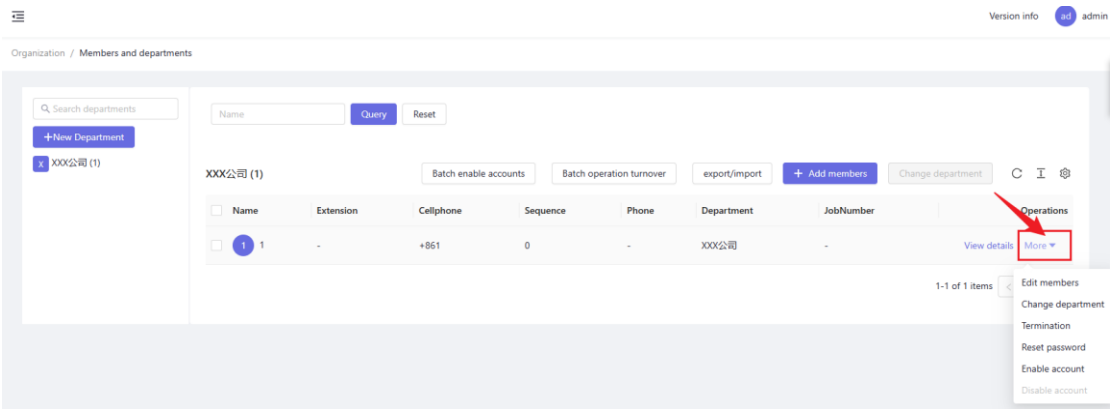


Figure 15 Modify member information

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 differentiate between different employees and is an important identifier of an employee's identity.

Table 6 Explanation of the Modify Member Information screen

9.1.2 Address Book Settings

Navigate to Organizational Structure > Address Book Settings, which provides address book-related setting options that allow administrators to flexibly configure the display and modification permissions for member information.

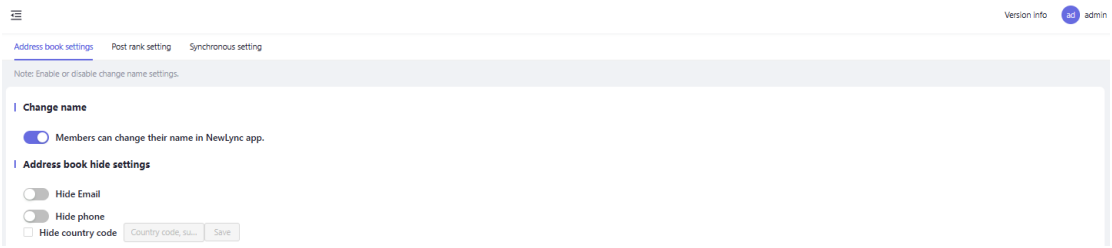


Figure 16 Name modification settings

When this option is enabled, regular members can change their name information autonomously through the client.

Address Book Hidden Settings

1.Hide Email: When enabled, members' email addresses in the address book will be hidden.

2.Hidden cell phone：When enabled, members' cell phone numbers in the address book will be hidden.

3. Hide Country Code：When enabled, the phone numbers displayed in the address book will not contain international area codes, which are supported to be set independently.

Position grading

This interface is used to set up the member's position and grade information, which facilitates the enterprise to clearly display the employee's organizational hierarchy and job duties in the address book. Administrators can select positions and set

grades for employees.

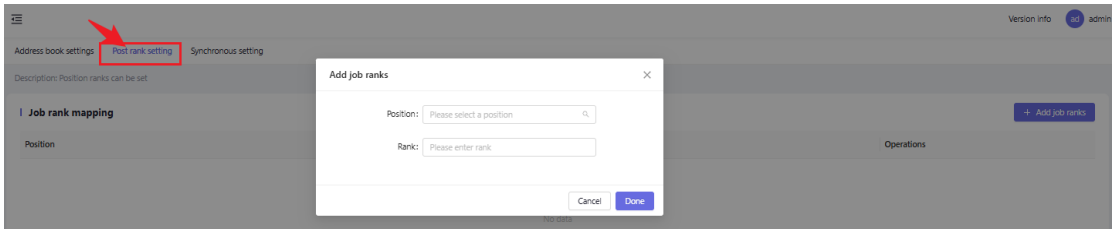


Figure 17 Position grading

Synchronized Organizational Structure

Click Sync Settings, select the sync source, and click Sync Now to directly sync the organization structure.

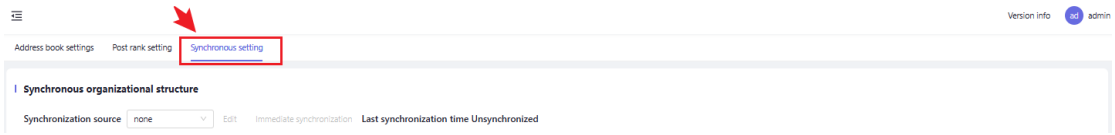


Figure 18 Position grading

9.1.3 LDAP

The Contacts system supports the use of LDAP with IP phones to provide a convenient cloud-based address book service for IP phones. LDAP is compatible with the LDAP v3 protocol. Users can select the v3 version when configuring LDAP on the phone to achieve seamless integration. In addition, Address Book also supports UC Address Book for Huawei phones and Remote Address Book for Yealink phones, ensuring a consistent and smooth address book access experience across different brands of devices.

9.1.3.1 Enabling the LDAP server

1. Navigate to click Organizational Structure->LDAP.
2. Click the LDAP Client Configuration tab and click Enable LDAP.

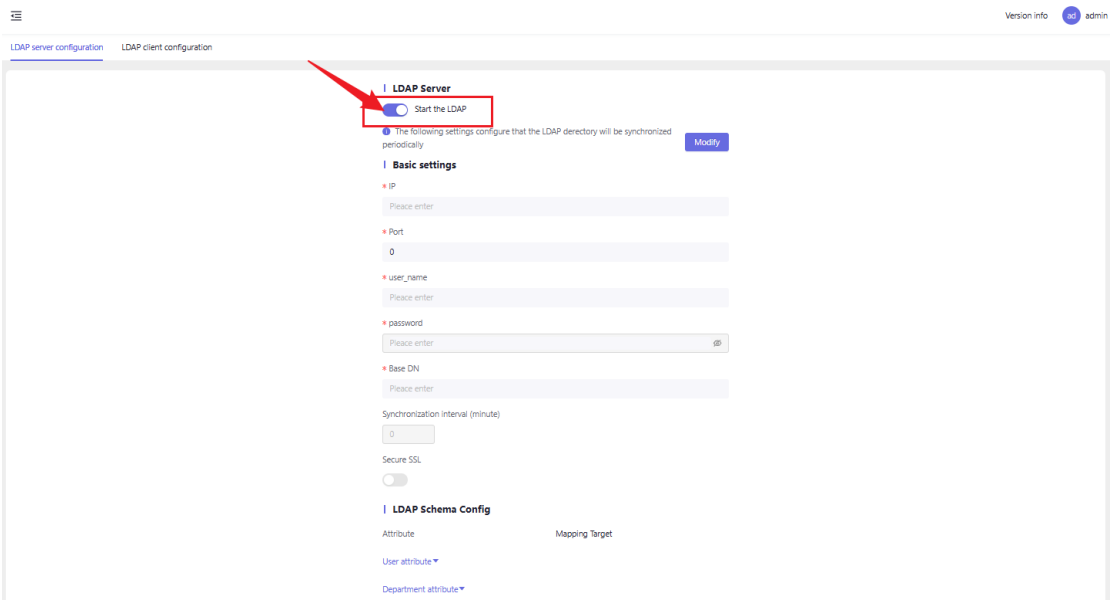


Figure 19 Enabling the LDAP server

Item	Definition
LDAP server	The address of the LDAP server used for the connection.
Ports	The port number used to communicate with the LDAP server.
User ID	The username used for authentication.
Password	The starting location for synchronizing data from the LDAP directory tree.
Synchronization interval	The data synchronization interval between the Address Book and the LDAP server.
SSL encryption	Enable or disable SSL encrypted communication.

Table 7 LDAP Server Parameters

9.1.3.2 LDAP Schema Settings

LDAP Schema Configuration Used to define the data field mapping relationship between the address book and the LDAP server. The administrator fills in the appropriate content based on the employee's information.

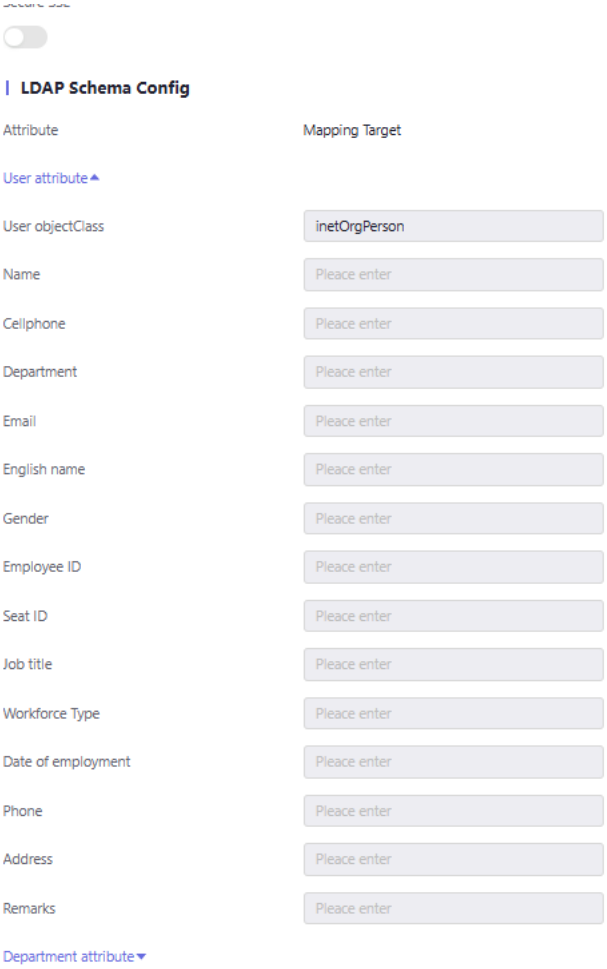


Figure 20 LDAP Schema Configuration

9.1.3.3 LDAP client configuration

Contacts Management System interfaces with enterprise LDAP servers through LDAP client functionality, providing efficient data synchronization and management capabilities for contacts. Support standard LDAP v3 protocol, flexible configuration of server address, port, Base DN, user name and password, etc. Meanwhile, LDAP data can be accurately synchronized to address book through field mapping relationship (such as name, department, cell phone, email, etc.). The system is compatible with most of the phones on the market (including Yealink, Square, Huawei, etc.), and supports SSL encrypted communication to ensure data security, which is suitable for enterprise-level address book management needs.

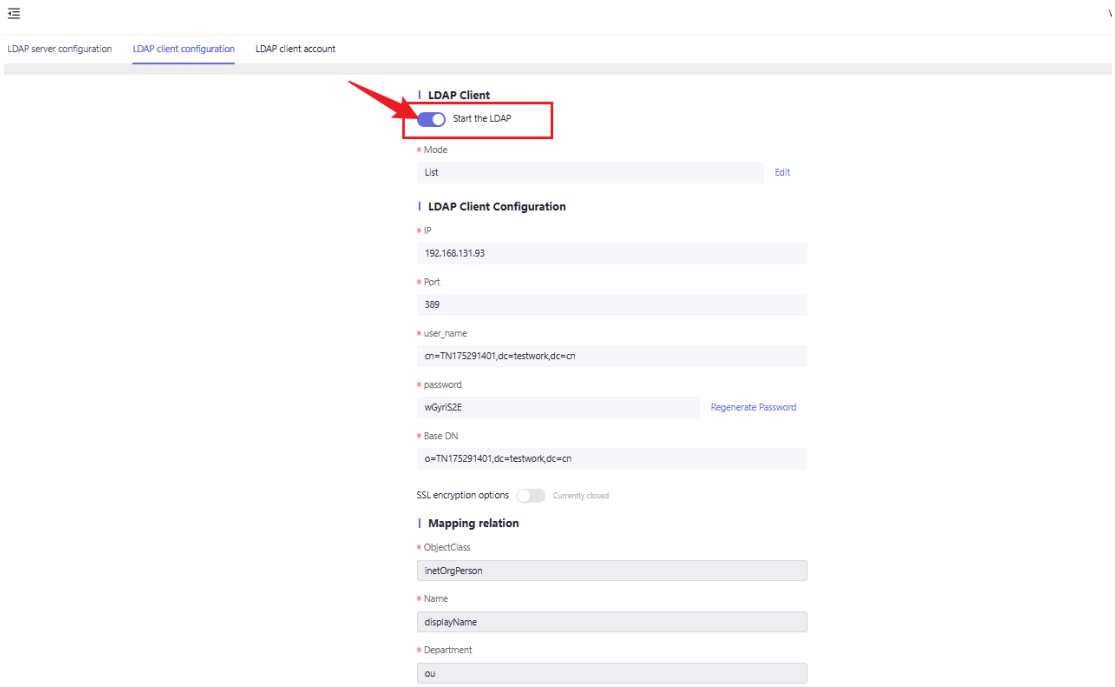


Figure 21 LDAP client configuration interface

Item	Definition
Address Book Architecture	Displays the architecture (Schema) configuration currently used by the LDAP client. The schema defines the mapping relationship between LDAP data fields and system address book fields.
LDAP server	Specifies the LDAP server address to be used for the connection.
ports	LDAP communication port.
user ID	The authentication account of the LDAP client.
Password	The password that accompanies the above username.
Base DN	Defines the starting path for LDAP data synchronization.
SSL encryption options	Select whether to enable SSL encryption.

Table 8 LDAP Configuration Definitions

9.1.3.4 Creating an LDAP account

1. Go to the admin backend and click Organization Structure->LDAP.

2. Click the LDAP Client Account stab and click+ Add Account.

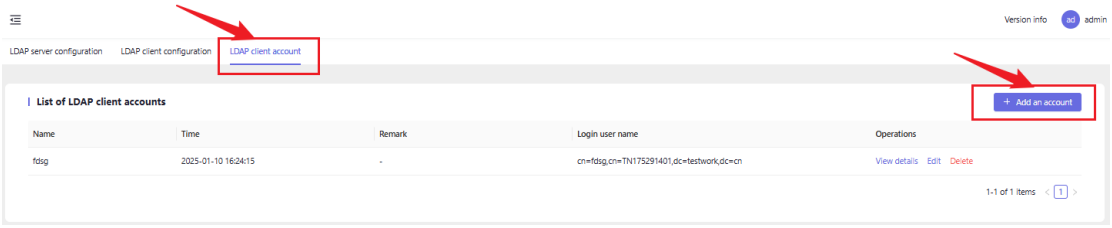


Figure 22 LDAP client account configuration screen

3. Enter a name and notes in the pop-up window. The name must be letters and numbers, ten characters or less.

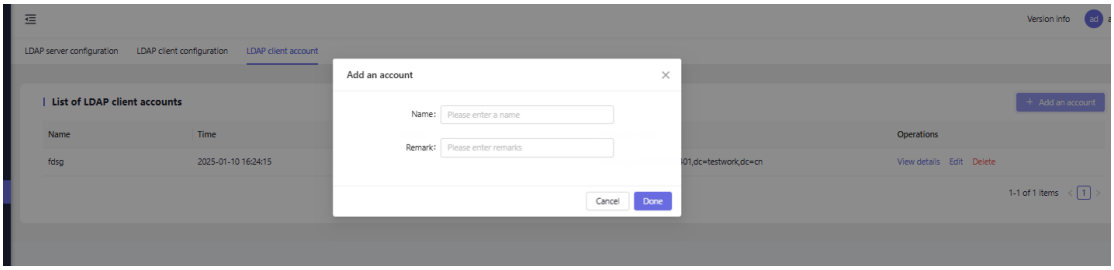


Figure 23 Add Account

4. Click Edit to configure visible departments and see the entire enterprise by default.

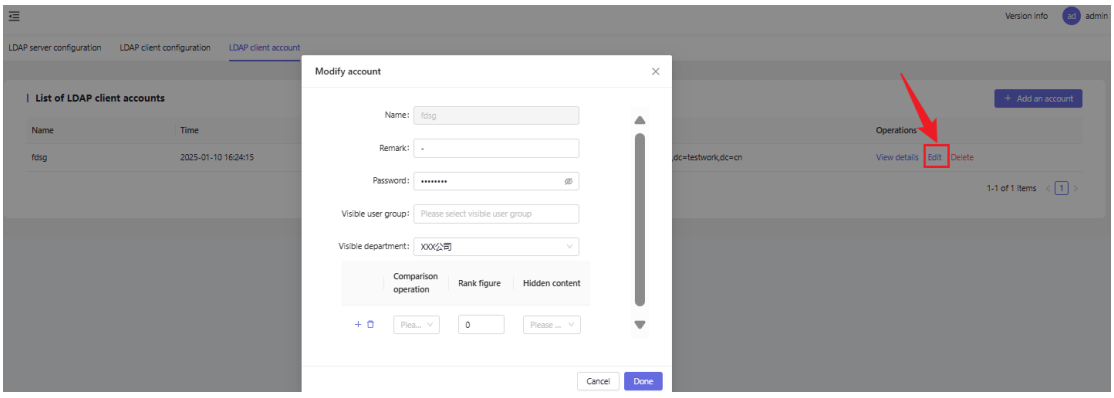


Figure 24 Modifying the LDAP account

5. Click View Details to see the LDAP account information. The LDAP function requires three pieces of information, Base DN, login username and password. Yealink phones can also choose to use the remote address book, and Huawei phones can choose to use the UC address book.

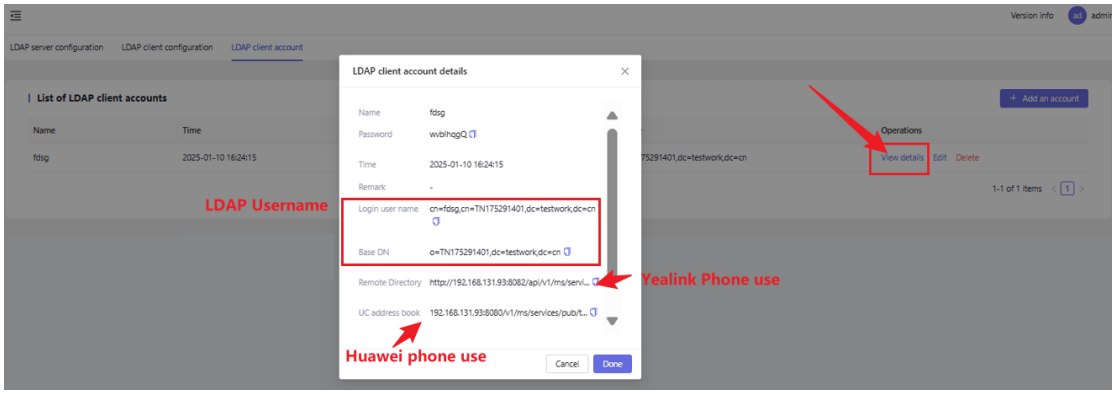


Figure 25 Edit LADP account

Click Edit LDAP Account to modify the account information.

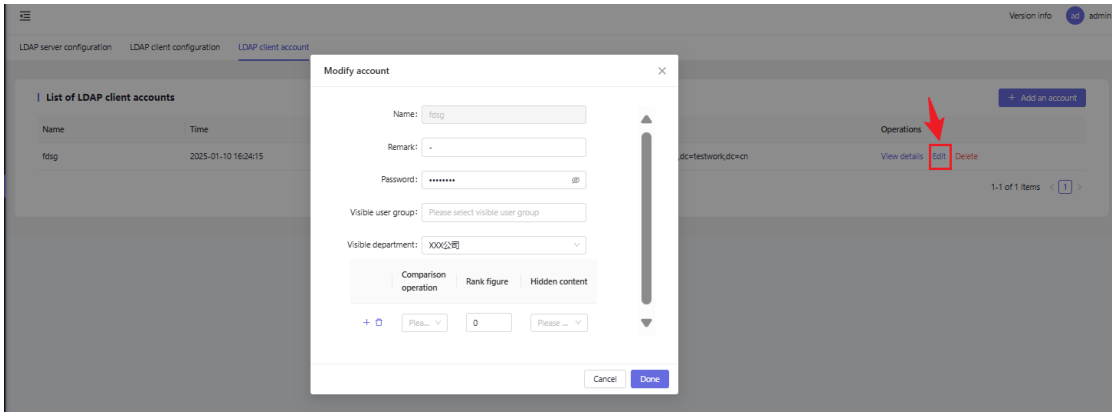


Figure 26 Edit LDAP account screen

Item	Definition
Name	Sets the name of the user or department that identifies the configuration object.
Remark	Can be filled in with additional explanatory information.
Password	Configure the user's access password.
Visible user group	Specify the range of user groups that this user or department can access, with support for selecting specific user groups from a drop-down menu.
Visible sector	Sets the range of departments that can be viewed by this user or department.

Table 9 Edit LDAP Account Interface Definitions

9.1.3.5 Contacts Permissions Management

After logging in, navigate to LDAP > LDAP Client Accounts and click Edit. You can modify LDAP account information and manage permissions for the LDAP address book. The address book supports flexible permission management based on department, user group, and rank rules (greater than, equal to, less than). You can set visibility scopes for different departments or user groups, and control which members' information should be hidden or displayed using rank rules.

For example: You can restrict visibility to only members within the same department, or hide contact information for higher-ranking personnel. This approach safeguards privacy while maintaining efficient and orderly communication.

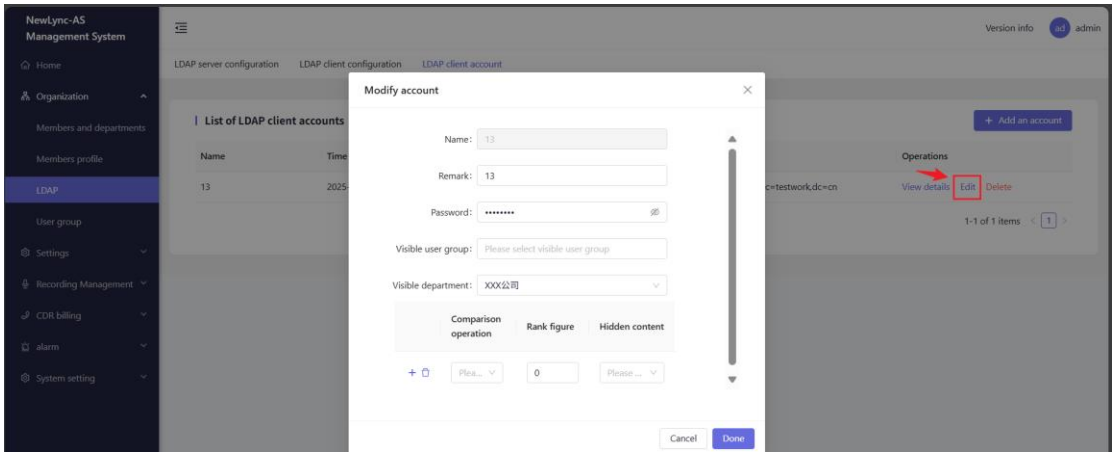


Figure 27 Edit LDAP Account Interface

Item	Definition
Name	Set the name of the user or department.
Remark	Additional notes may be entered here.
Password	Configured access password.
Visible user	Specify the scope of user groups that this user or department

group	can access.
Visible department	Set the scope of departments that this user or department can view.

Table 10 Edit LDAP Account Interface Definition

Multi-level Permission Management

When setting address book hiding rules, you can intelligently control which contacts to hide by combining comparison operators (greater than, greater than or equal to, less than) with job level numbers. For example: - Selecting “greater than (>)” and entering the rank number 5 will hide contact information for members with ranks greater than 5. - Selecting “equal to (=)” will hide only members with ranks equal to 5. - Selecting “less than (<)” will hide members with ranks less than 5.

Item	Definition
greater than	Hide member information for roles greater than N.
less than	Hide member information for roles below level N.
Equal to	Hide member information where rank equals N.
Rank figure r	The rank value of a user or department.
Hidden Content	Specify the types of information to hide in the address book. Options include hiding all information or hiding only mobile/extension numbers.

Table 11 Multi-level Permission Control Definition

For example:

Rule ①: > 7 → Hide contact information for senior management;

Rule ②: = 5 → Hide contact information for department heads;

Rule ③: < 2 → Hide contact information for interns and assistants.

Through multi-layered rule combinations, hierarchical and role-based protection of

address book information can be implemented within the same system, meeting diverse security and privacy management requirements.



Job levels and visible user groups cannot be used simultaneously.

9.1.3.6 Add an LDAP server to the phone

This section guides users on how to configure the LDAP cloud address book on the phone, enabling the device to connect to the LDAP server and synchronize cloud-based address book data.

9.1.3.6.1 Fanvil Phone (using the V61W model as an example)

After logging in, navigate to Contacts > Cloud Contacts.

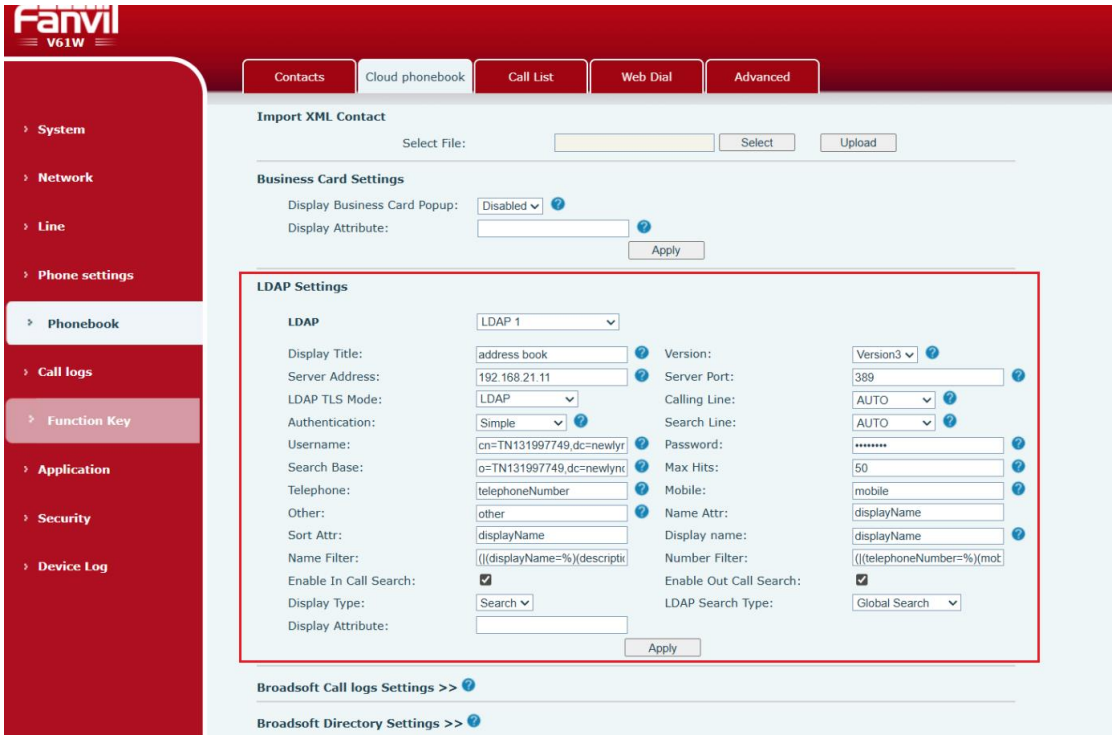


Figure 28 Fanvil Phone Configuration LDAP Interface.

Item	Definition
LDAP	Select the LDAP server you need to configure or update from the dropdown menu.
Display Title	Set the display name for the LDAP configuration on the interface. Required field.
Version	Select LDAP version.
Server Address	Enter the IP address of the LDAP server to enable the

Item	Definition
	device to connect correctly to the target LDAP server. Required field.
Server port	Enter the port used by the LDAP server. Required field.
LDAP Encrypted Transport Mode	Select the encryption method for LDAP protocol transmission.
Dialing Line	Select the dialing method; the default is AUTO.
Authentication Method	Configure the authentication method when setting up an LDAP connection.
Check Route	Select the route query method; the default is AUTO.
Username	Enter the username required for LDAP authentication, See Section 9.1.3.4: Creating LDAP Accounts.
Password	Enter the password required for LDAP authentication, See Section 9.1.3.4: Creating LDAP Accounts.
Search Base	Set the starting directory path for LDAP queries, See Section 9.1.3.4: Creating LDAP Accounts.
Maximum number of clicks	Limit the maximum number of entries returned by LDAP queries.
Office phone	Configure the office phone number field stored in LDAP
Mobile phone	Configure the mobile phone number field stored in LDAP.
Others	Configure the fields in LDAP for storing additional information.
Name Attribute	Configure the fields in LDAP that store user identification information.
Sorting Attributes	Configure the sorting criteria field for query results to arrange the returned data in the specified order.

Item	Definition
Display Name	Configure the display name field stored in LDAP.
Name Filter	Set the filter criteria used for LDAP queries.
Number Filtering	Set the filter criteria for using LDAP numbers.
Enable Call Query	Enable or disable the call query feature.
Enable Outbound Query	Enable or disable call inquiries initiated from the device.
Display Type	Configure the display format for query results, allowing selection of different display formats.
LDAP Search Types	Configure the search scope for LDAP queries.
Display Properties	Configure the specific fields to be displayed in the query results.

Table 12 Configure LDAP Parameters for Fanvil Phones

9.1.3.6.2 Yealink Phone

After logging in, navigate to Contacts > Remote Address Book.

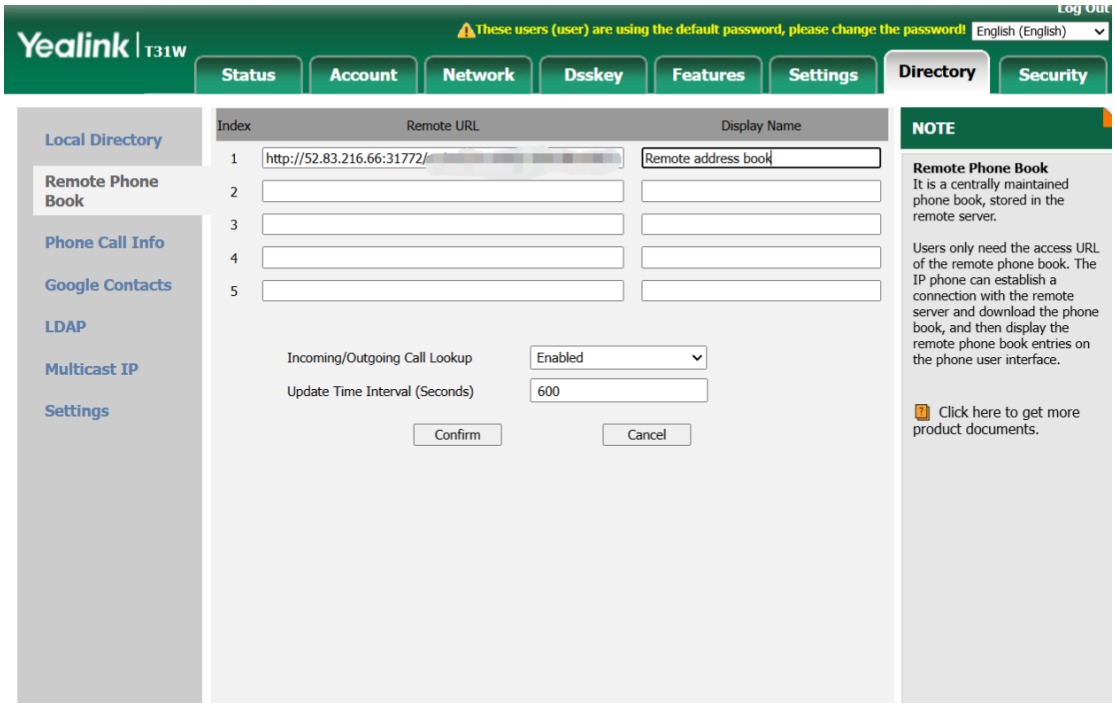


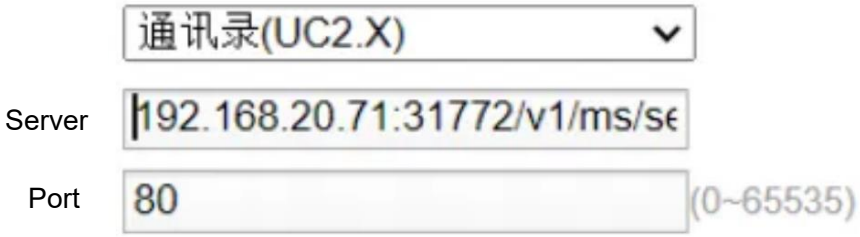
Figure 29 Configure LDAP Parameters for Yealink Phones

Item	Definition
Remote URL	Configure the remote URL address for the LDAP server, See Section 9.1.3.4: Creating LDAP Accounts.
Display Name	Configure the name displayed on the phone's screen. The display name can be a user, department, or device identifier used to distinguish and identify different devices or users.
Incoming/Outgoing Number Matching	Configure how the device matches and identifies numbers for incoming or outgoing calls.
Update Interval (seconds)	Configure the time interval, in seconds, for the device to retrieve data or perform actions from a remote URL.

Table 13 Configure LDAP Parameters for Yealink Phones

9.1.3.6.3 HuaWei Phone

After logging in, navigate to Server > Advanced Server > Address Book.



Item	Definition
Address Book Server	Select the address book server from the dropdown menu.
Server	Enter the address and path of the address book server, See Section 9.1.3.4: Creating LDAP Accounts.
Port	Configure the port number for the address book server, within the range of 0 to 65535.

Table 14 Configure LDAP Parameters for HuaWei Phones

9.1.3.7 Quickly search cloud contact list members via the phone (Using the NRP1312 phone as an example)

After configuring the LDAP server on the phone, users can directly search for and access member information in the LDAP cloud directory from the phone.

Taking the NRP1312 phone as an example:

The name filtering rule is enabled in LDAP settings:

(|(displayName=%)(description=%)), meaning matching occurs based on either the display name or description field.

When contacts “Zhang San” and “Zhang Liu” exist in the address book, after the phone completes the LDAP download, users can search by pressing the search button on the phone and entering the initials (first letters of the name):

Pressing “z” displays “Zhang San” and “Zhang Liu” on the screen;

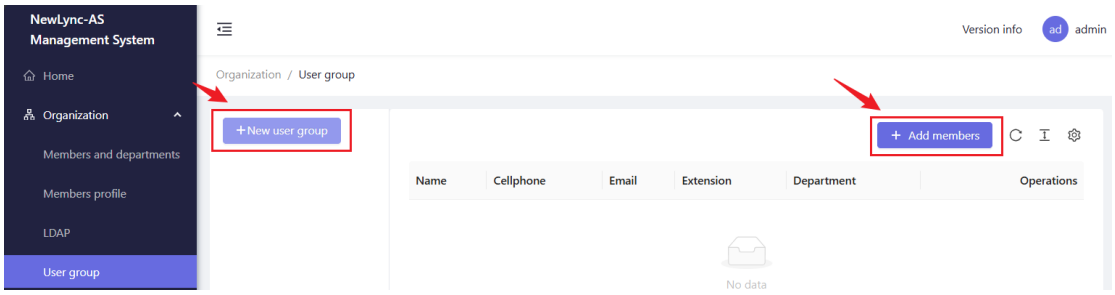
Pressing “zl” displays only “Zhang Liu” on the screen.



Figure 30 NRP Phone Contact Search Interface

9.2 User Groups

Navigate to Organization Structure > User Groups. This interface allows administrators to create user groups and configure group members. Once members are added to a user group, their contact information within that group will be uniformly hidden, preventing others from viewing their details in the address book. If you wish to grant specific users or departments access to view these hidden members' information, navigate to LDAP > LDAP Client Accounts. Under Visible User Groups, specify the scope of accessible user groups. This feature enables flexible control over which member information is externally visible, meeting privacy and security management needs across various scenarios.



9.3 Enterprise Settings

9.3.1 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.

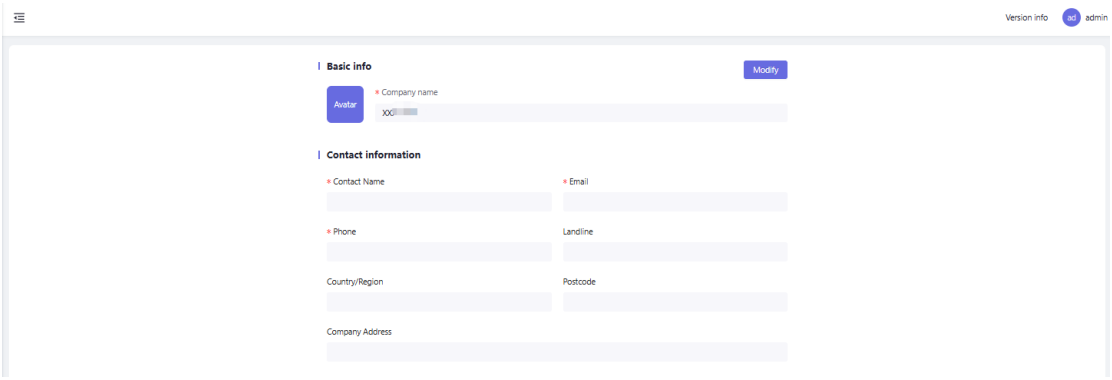


Figure 31 Modify basic enterprise information

Item	Definition
Company identification	To display the company name, you need to fill in or select the official 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.
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 15 Enterprise Basic Information Interface Definition

9.3.2 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.

9.3.2.1 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.

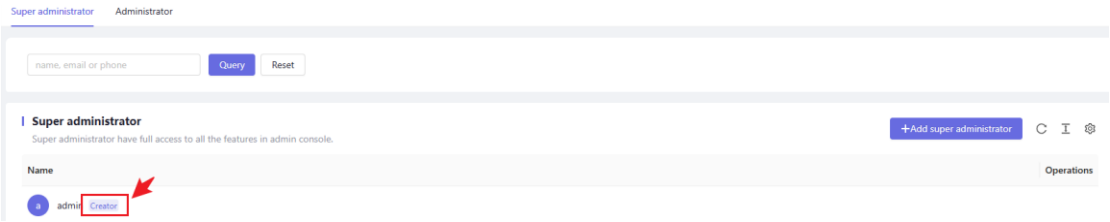


Figure 32 Transfer creator

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.

9.3.2.2 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.

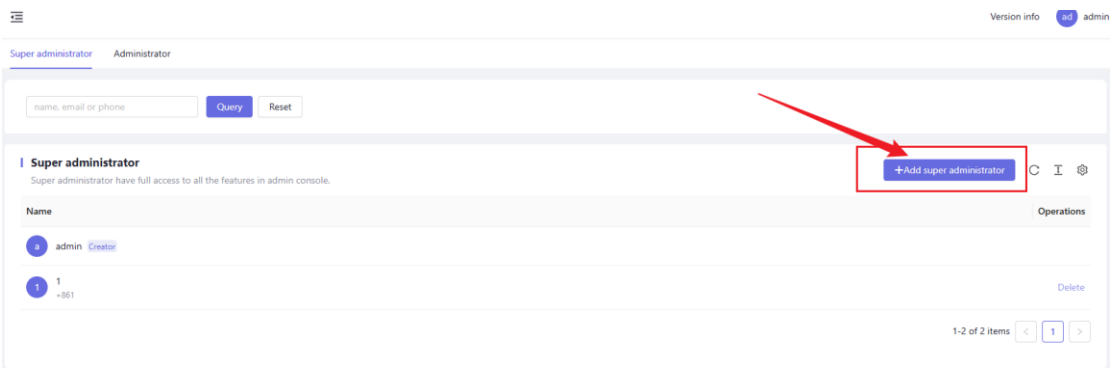


Figure 33Add Super Administrator

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.

9.3.2.3 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.

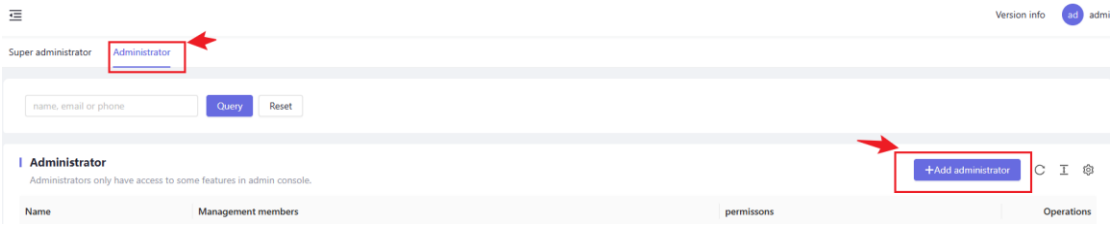


Figure 34 Add Administrator

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	The administrator needs to set the scope of that administrator's

Item	Definition
management	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 16 Adding an Administrator Interface Definition

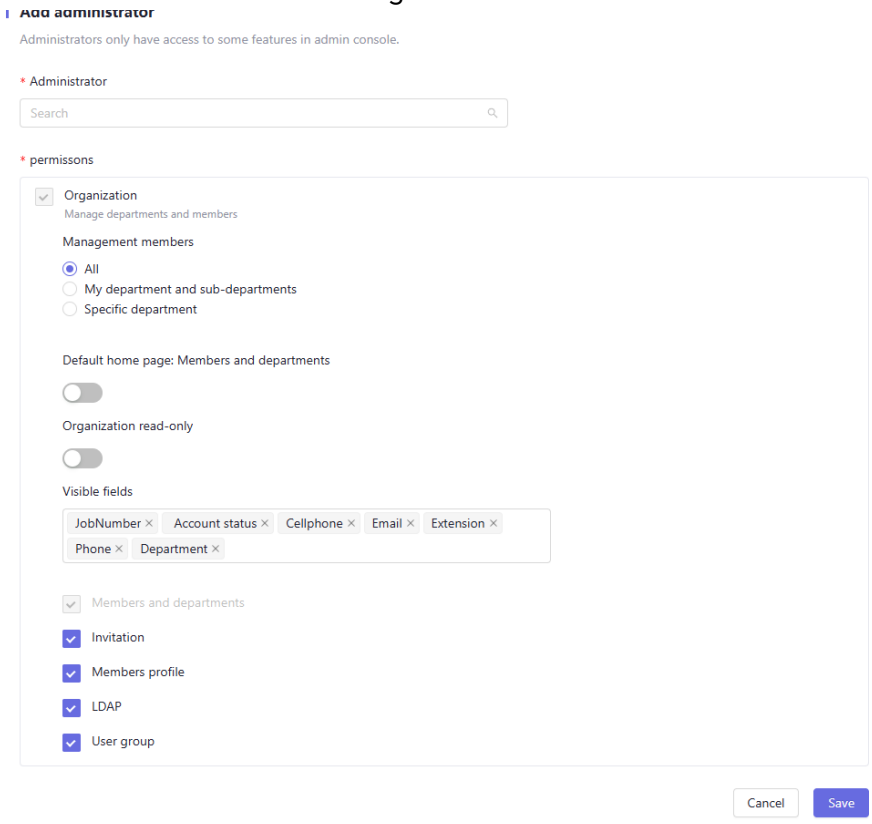


Figure 35 Edit Administrator Privileges

Step.4 Click Save to complete the addition.

10 Alerts

10.1 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 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.

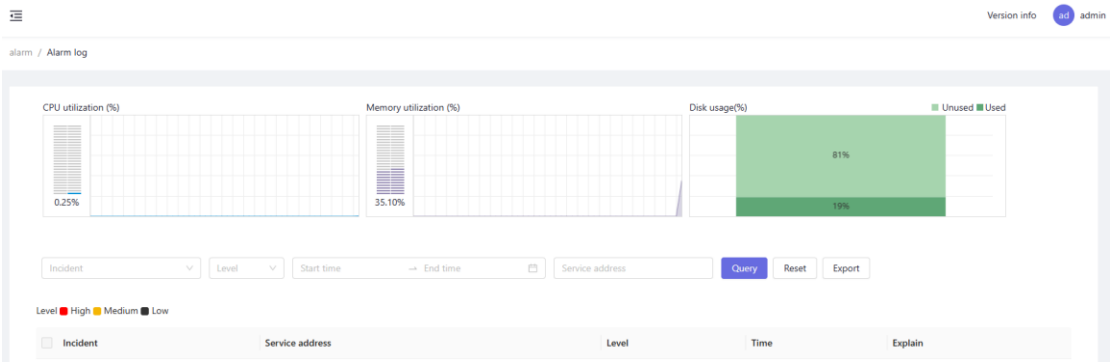


Figure 36 Alarm log interface

10.2Alarm 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 longtime 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.

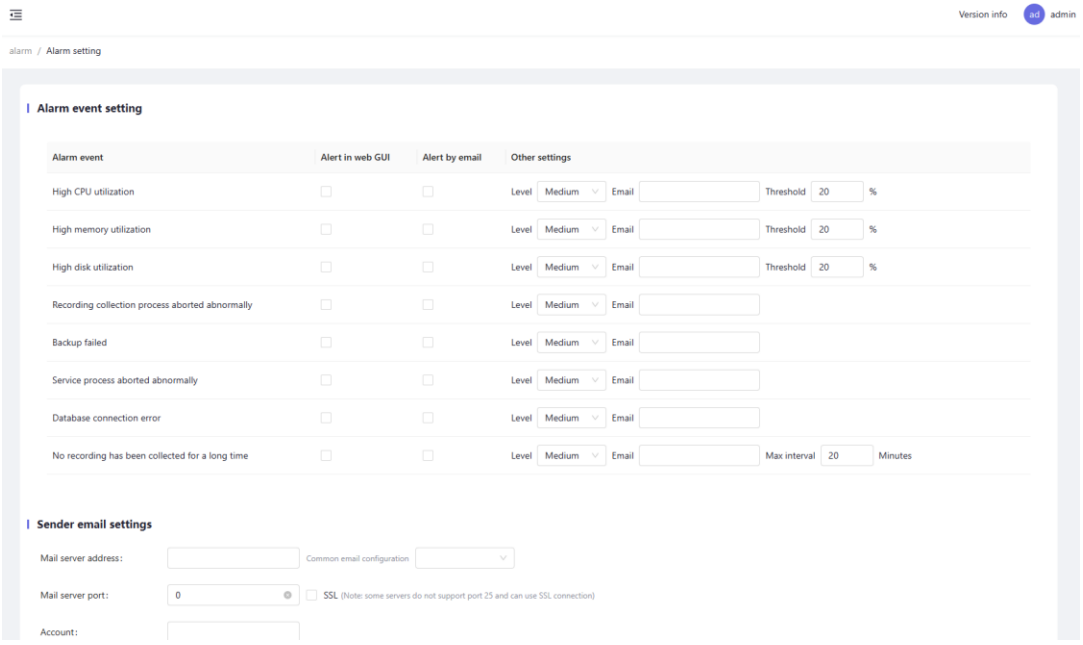


Figure 37 Alarm Event Settings

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.

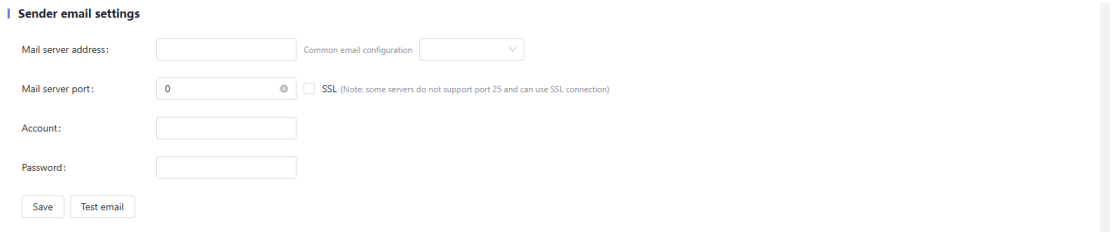


Figure 38 Sending Mail Settings

11 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.

11.1 Authorization Information

After completing the installation of the AS Series NL-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 NL-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.

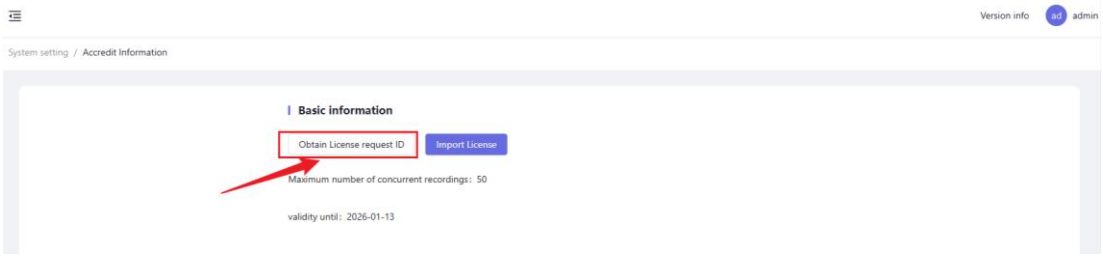


Figure 39 Getting the License Request ID

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:

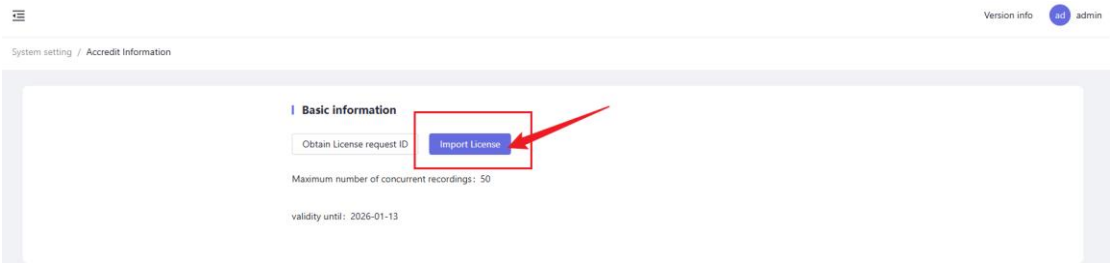


Figure 40 Import License

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.

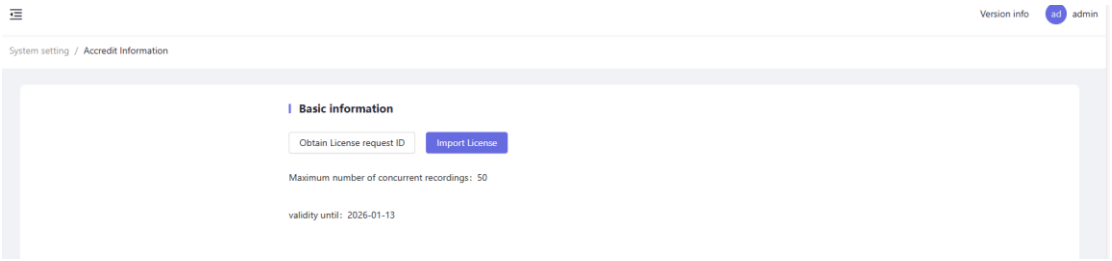


Figure 41 Check if the License file is imported correctly

11.2 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.

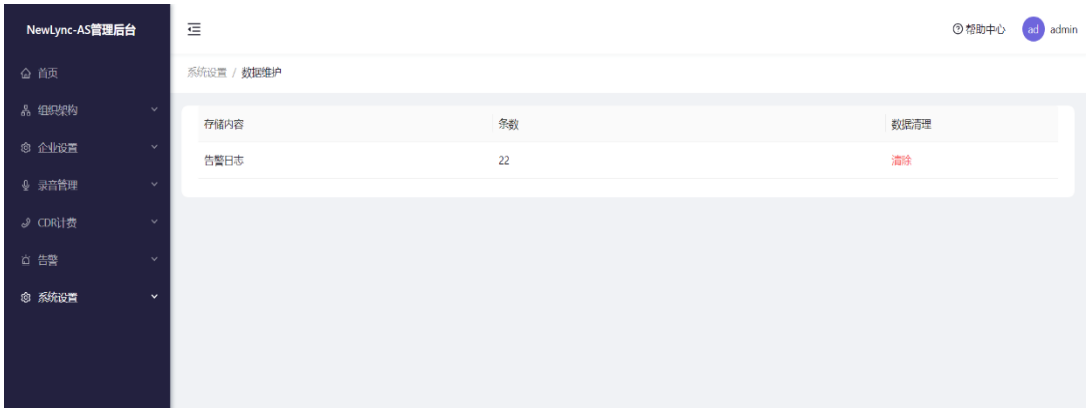


Figure 42 Data Maintenance Interface

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 17Data Maintenance Interface Definitions

Step.1 Select the time period to be cleaned and click Confirm.

After confirming the purge operation, the system perForum data purging 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.

Note Backup data: Before performing data cleaning operation, it is recommended to backup important data to avoid data loss due to accidental deletion.
Regular maintenance: It is recommended to check and maintain the system data regularly to ensure efficient and stable operation of the system.

11.3 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.

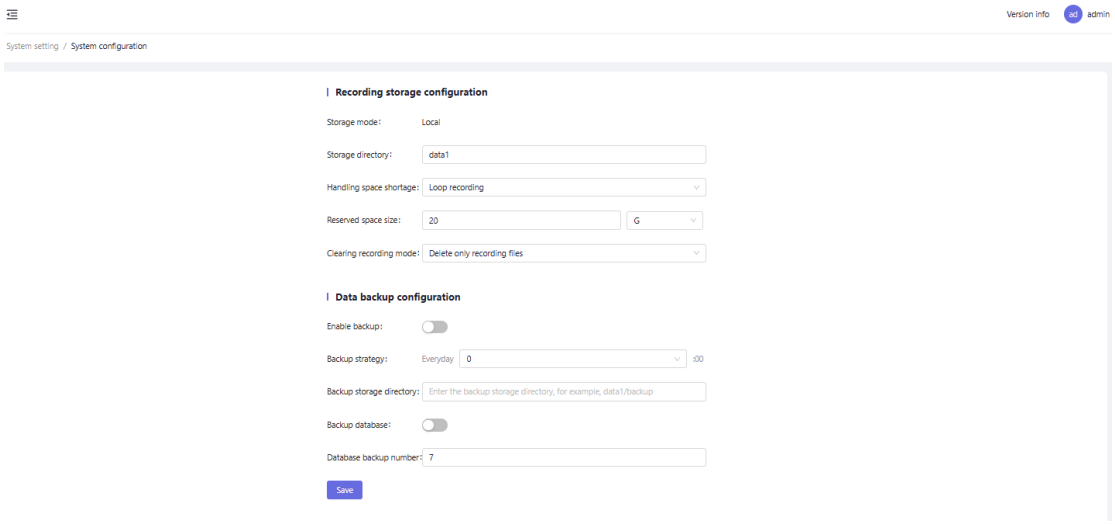


Figure 43 System setup interface

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 space to be reserved
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

11.4 Recording Node Function

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.

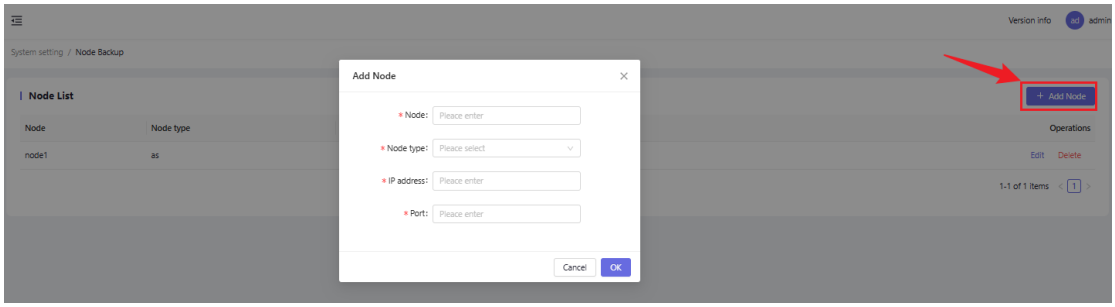


Figure 44 Add Node

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

Edit Node

Click Edit Node to modify the configured node parameters.

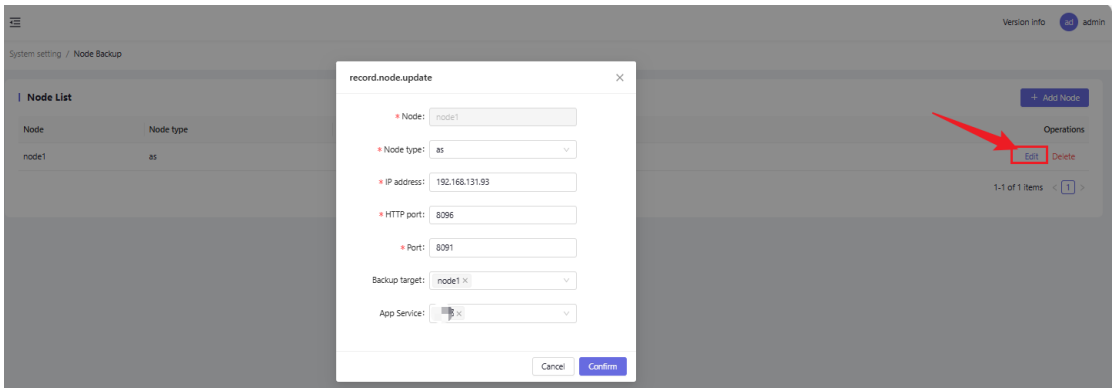


Figure 45 Edit Node

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 nodes
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 nodes

Click Delete to delete the current node.

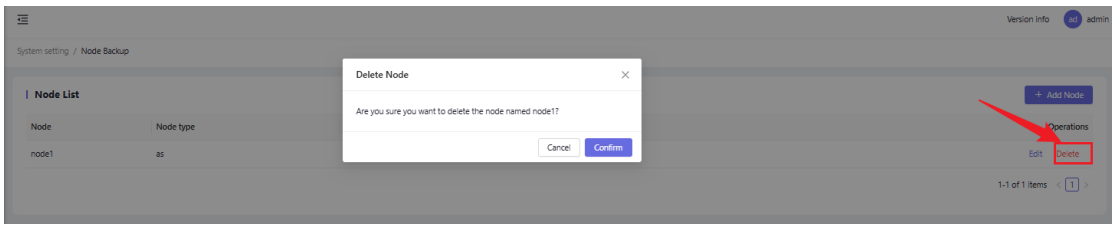


Figure 46 Deleting nodes

12. Appendix

12.1 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	Pact	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.

12.2 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.
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/video switching device.