

New Rock Technologies, Inc.

NewLync 2.0

Configuration and Operation Manual

Document Version: 02

Release Date: September 22, 2025



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.

Mail: global@newrocktech.com

Tel: 021-61202700 / 52217917

Document center: <https://en.newrocktech.com/DocumentCenter>

Table of Contents

Table of Contents	I
1 About This Document	1
2 NewLync 2.0 Product Introduction	2
3 Advantages of NewLync 2.0 over other legacy PBXs	4
4 NewLync 2.0 Integration Software Introduction	6
4.1.1 NewLync Operations and Maintenance System (SSC)	6
4.1.2 NewLync Management Backend (BSC)	7
4.1.3 NewLync Teams	8
5 NewLync 2.0 Disaster Recovery Solution Overview	9
6 NewLync and Unified Communications Platform Software Deployment and Installation Guide	13
6.1 Hardware Requirements	13
6.2 Hardware, Operating System, and Database Compatibility	13
6.3 Interactive Installation of the NewLync All-in-One System	14
6.3.1 Server Initialization Preparation	14
6.3.2 Prerequisites for Dual-Server Installation	15
6.3.3 Launch the Installation Wizard	16
6.4 IV. How to Change the IP Address or Domain Name for the Newlync 2.0 All-in- One Device	22
6.5 Recovery Installation Process (Expanding from Single Server to Dual Server)	27
7 NewLync Management Backend Configuration and Operation	32
7.1 Basic Operation	32

7.1.1 Log in	32
7.1.2 Change password	33
7.1.3 Switching teams	33
7.1.4 Global navigation	34
7.2 Organizational Structure	35
7.2.1 Membership and sectors	35
7.2.2 Invitation	40
7.2.3 Address Book Settings	41
7.3 LDAP	42
7.3.1 Enabling the LDAP server	42
7.3.2 LDAP Schema Settings	43
7.3.3 LDAP Client Configuration	44
7.3.4 Creating an LDAP account	45
7.3.5 Contacts Permissions Management	49
7.3.6 Add an LDAP server to the phone	52
7.3.7 Quickly search cloud contact list members via the phone (Using the NRP1312 phone as an example)	55
7.4 Cost Center	56
7.4.1 Value-added services and packages	56
7.4.2 Order Management	58
7.4.3 Account Management	58
7.5 Security	58
7.5.1 Security policy	58
7.5.2 Equipment management	59
7.5.3 Administrator log	59
7.6 Data Sheet	60
7.6.1 Equity data	60
7.7 Enterprise Settings	60

7.7.1 Corporate Information	60
7.7.2 API Services	61
7.7.3 Administrative authority	61
7.8 Meetings Management.....	64
7.8.1 Meeting data	64
7.8.2 Corporate meeting rooms	64
7.8.3 List of meetings	65
7.8.4 Conference settings	66
7.9 IPPBX Interconnect	67
7.9.1 OM Management	67
7.9.2 Extension management	69
7.9.3 Routing management	70
7.10 Cloud PBX Services.....	72
7.10.1 Centralized administration	72
7.10.1.1 Outbound Configuration	72
7.10.1.2 Outbound Inbound Configuration	76
7.10.2 Extension management	78
7.10.3 User group	79
7.10.4 IVR Voice Menu	84
7.10.5 Call queue	86
7.10.6 Enterprise Operations Management	88
7.10.7 NewLync Settings	88
7.10.8 Enabling Cloud PBX	89
7.11 Sound Recording Management.....	90
7.11.1 Recording Configuration	90
7.11.2 Sound Recording Inquiry	97
7.11.3 Recording settings	97
7.11.4 Operation log	98
7.11.5 Statistical analysis	98

7.12 CDR Billing	99
7.12.1 CDR Configuration	99
7.12.2 Call record	99
7.12.3 Statistical analysis	100
7.13 Billing center	101
7.13.1 Intend.....	101
7.13.2 Add Rate	101
7.13.3 Description of rates	103
7.14 Statement of Accounts.....	104
8 Common Problems.....	105
9 Glossary	107

1 About This Document

This manual is designed to provide detailed configuration and operation guides for enterprise IT administrators, system operation and maintenance engineers and technical support personnel to help efficiently manage and maintain NewLync 2.0, and to ensure safe and stable system operation. It covers system overview, installation and deployment, basic configuration, operation and maintenance management and troubleshooting.

2 NewLync 2.0 Product Introduction



NewLync 2.0 is a new-generation converged communication platform for the enterprise market, adopting microservices architecture and containerization technology, integrating voice, video, instant messaging (IM), enterprise address book, intelligent conferencing, and other communication modes to comprehensively improve the efficiency of enterprise collaboration. Its core advantage lies in high availability, flexible deployment and intelligent management, supporting both single-machine deployment and dual-machine hot standby solutions to meet the business needs of different enterprises.

For enterprises with high reliability requirements, NewLync 2.0 provides a dual-machine backup architecture, utilizing virtual IP technology and data synchronization mechanisms to ensure business continuity, and even if a single node fails, the system can be automatically recovered within 5 seconds to achieve highly available communication services. In addition, NewLync 2.0 is compatible with mainstream SIP devices and can be seamlessly integrated with enterprise HRM, OA, CRM and other systems to create an intelligent, full-scene enterprise communication solution.

At the management level, NewLync 2.0 integrates the NewLync O&M system (SSC) and

the NewLync management backend (BSC), providing comprehensive system configuration and management capabilities.

NewLync O&M system (SSC) is the central control system of the whole platform, through which administrators can carry out comprehensive monitoring, configuration and O&M of NewLync 2.0, including network settings, user management, service subscription and real-time monitoring, etc. Meanwhile, it also supports independent management of multiple enterprises or teams to meet the personalized needs of different organizations.

As a sub-platform of the O&M system, NewLync management backend (BSC) focuses on account and permission management within the enterprise, allowing enterprises to create independent management backends according to their own architecture and achieve fine-grained management of enterprise-level PBXs, extensions, routing, and user permissions through functions such as account management, organizational structure, permission configuration, IPPBX interconnection, and cloud PBX services.

NewLync 2.0 is suitable for a wide range of industries such as finance, manufacturing, government, energy, call centers, etc. It is especially suitable for enterprises with multiple branch offices, remote collaboration and high concurrent communication needs. Its converged communication capability supports cross-platform and multi-terminal interconnections, including IP phones, desktop clients, mobile applications, video conferencing systems, etc., realizing seamless connection between internal and external communications of enterprises. At the same time, the system provides value-added functions such as one multi-machine, call relay, and LDAP enterprise address book management, which help enterprises build a more intelligent, efficient, and secure communication network. NewLync 2.0 provides enterprises with a stable and reliable converged communication platform through its advanced architectural design, flexible deployment and perfect management system, which helps enterprises' digital transformation.

3 Advantages of NewLync 2.0 over other legacy PBXs

With the increasing demand for communication systems in modern businesses, cloud-based unified communication systems are becoming the preferred choice for organizations of all sizes. Traditional PBX systems are no longer able to meet current business needs, and organizations are looking for more efficient and flexible communication platforms. In this highly competitive market, NewLync 2.0 is the preferred solution for enterprise digital transformation due to its superior technical architecture, powerful integration capabilities and high availability compared to other traditional PBX systems.

High Availability and Disaster Tolerance

Most traditional PBX systems tend to rely on a single hardware device or a simple backup solution, which results in a long recovery time in the event of a failure and fails to ensure business continuity. NewLync 2.0 provides a dual-machine hot standby architecture, combined with virtual IP technology and data synchronization mechanism, to ensure that the system can be automatically recovered within 5 seconds when the main server fails to achieve highly available communication services.

Integration and Intelligent Functions

Traditional PBX systems lack intelligent features and underperform in terms of integration with existing enterprise systems. NewLync 2.0 seamlessly integrates with HRM, OA, CRM and other enterprise systems, realizing the efficient transfer of data flow within the enterprise and improving overall collaboration efficiency. At the same time, the system provides intelligent conference functions, breaking through the traditional PBX in conference management and intelligent office limitations.

Security and Privacy

Many traditional PBX systems have more basic security mechanisms, usually only transmission encryption, lacking comprehensive data protection. And the permission management function

is usually simple, unable to cope with complex enterprise security needs. NewLync 2.0 provides end-to-end encryption and fine-grained permissions management to secure all communication content. In addition, the system supports the state secret encryption configuration to meet the special needs of high security requirements of the industry (such as finance, government).

Performance and Scalability

Most traditional PBX systems are more limited in performance scaling, especially in the case of high concurrency, it is easy to overload the system, resulting in performance degradation. NewLync 2.0 adopts microservices architecture and containerized deployment with high performance and scalability to support high concurrent calls, concurrent video conferencing, and easily scale the system capacity according to enterprise needs.

4 NewLync 2.0 Integration Software Introduction

This chapter introduces the management system of NewLync 2.0, including the NewLync operation and maintenance system, the configuration interface of NewLync management backend, and the interface of NewLync Teams users' desktop and cell phone, which will help readers to understand the core functions of each system and their interrelationships. Subsequent chapters will explain the key features of the management system and how to use them in detail as they describe the NewLync 2.0 configuration steps so that administrators can better configure and maintain the system.

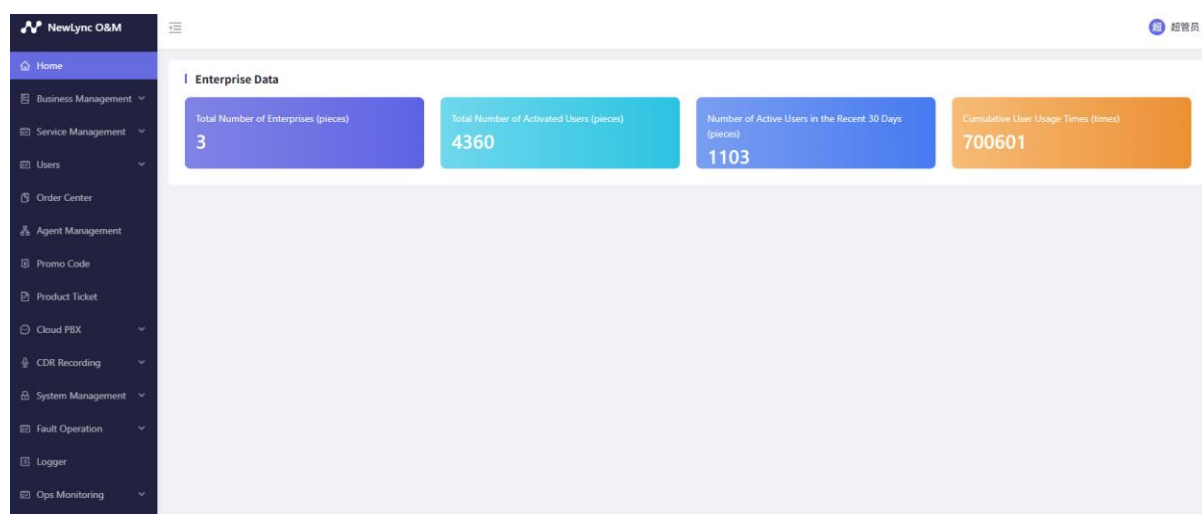
4.1.1 NewLync Operations and Maintenance System (SSC)

NewLync Ops is a comprehensive management platform responsible for the maintenance, configuration and operation of the system. As a central control system, administrators can carry out comprehensive control and configuration of the converged communication platform through this system to ensure stable operation of the system. At the same time, NewLync O&M system allows administrators to manage and configure different enterprises or teams independently to meet their needs and realize efficient O&M management.

KeyFeatures Include:

- ✓ System Configuration: Manage network settings, server configuration, etc.
- ✓ User Management: Add, delete and manage user accounts.
- ✓ Service Subscription: Subscribe to services such as Cloud PBX for your business account.
- ✓ Monitoring and Maintenance: Monitor the system status in real time and perform the necessary maintenance operations.

The following figure shows the service interface of the NewLync Ops system:



Service Interface of NewLync Ops System

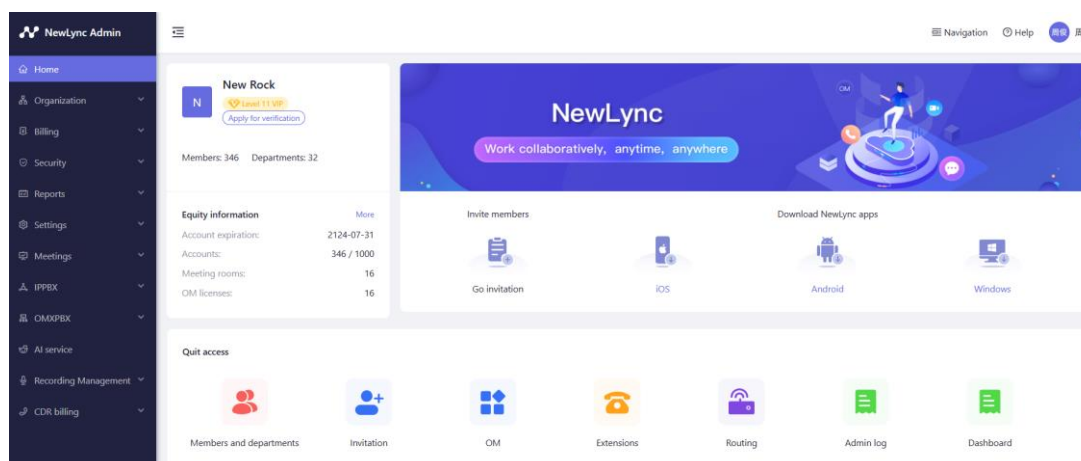
4.1.2 NewLync Management Backend (BSC)

The NewLync Management Backend is a sub-platform of the NewLync Ops system, dedicated to account and permission management within the organization. Each enterprise, subsidiary or business unit can have its own NewLync administration backend for independently managing its user and permission configuration. Group companies can set up independent management backgrounds for their subsidiaries, thus realizing efficient and independent user and authority management.

Key features include:

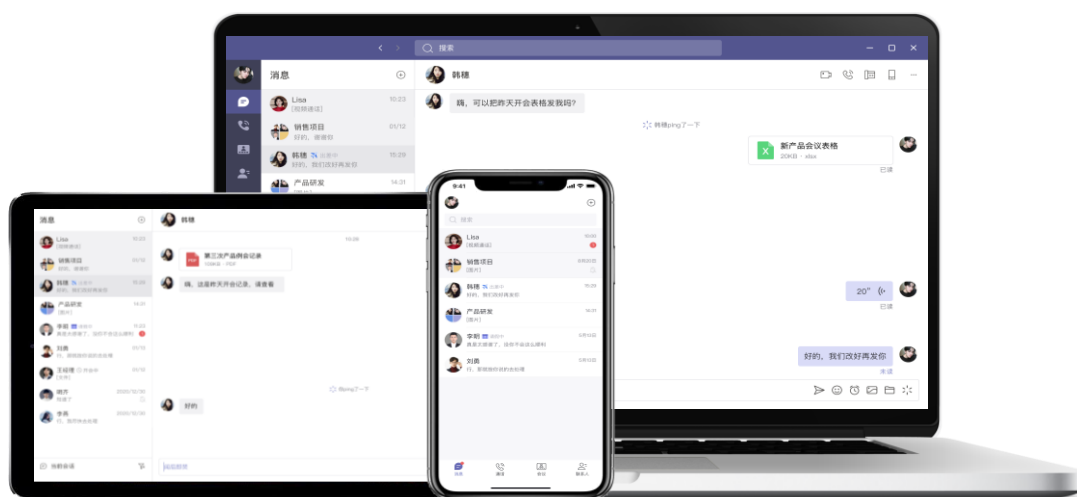
- ✓ **Account Management:** Create and manage corporate accounts, assign permissions.
- ✓ **Organizational Structure:** Create and manage departments, add and delete members.
- ✓ **Permission Configuration:** Assign different operating privileges to different users to ensure system security.
- ✓ **IPPBX Interconnect:** Manage OM, extension and routing settings.
- ✓ **Cloud PBX services:** Including dashboards, switchboard management, extension management, user groups, trunks and routing, IVR voice menus, call queues, enterprise O&M, NewLync setup, and more.

The following image shows the home screen of the NewLync administration backend:



Home screen of the NewLync administration backend

4.1.3 NewLync Teams



NewLync Teams is an enterprise-oriented online collaborative office software that integrates IM instant messaging, audio/video conferencing, multi-terminal collaboration, converged communications and more. Relying on New Rock nearly 20 years of industry accumulation, NewLync Teams innovatively integrates a variety of communication technologies to provide enterprises with a secure, efficient and intelligent collaboration experience. Through advanced intelligent communication solutions and professional services, NewLync Teams helps enterprises build a more convenient and stable communication platform, and comprehensively improve teamwork efficiency.

5 NewLync 2.0 Disaster Recovery Solution Overview

To ensure the high availability and business continuity of the enterprise communication system, NewLync 2.0 provides a comprehensive disaster recovery solution, adopting a dual-machine hot standby architecture, combined with data synchronization, load balancing, and an automatic failover mechanism, which enables rapid recovery of the system operation in the event of an abnormality in the servers or the network, minimizing the impact of business interruption.

1. Dual hot standby architecture

NewLync 2.0 utilizes a two-server Active-Standby architecture, where two servers (DC1 and DC2) take on the roles of the primary (Active) and standby (Standby) servers respectively. The two are efficiently switched through virtual IP technology (VIP) to ensure that when the main server is abnormal, the backup server can quickly take over the business to ensure the stable operation of the system.

1.1 Key technologies

- ✓ Virtual IP (VIP) mechanism: The master and backup servers share a virtual IP address, and the service traffic is always directed to this address, so there is no need to modify the terminal equipment configuration during the switching process.
- ✓ Keepalived monitoring mechanism: Real-time detection of server status to ensure that VIPs are bound to healthy servers and automatically switch to the backup server when the primary server fails.
- ✓ Heartbeat detection: The main and backup servers send heartbeat packets on a regular basis for state detection, once the main server is detected to be unavailable, the backup server can immediately take over the business.
- ✓ Automatic Load Balancing: Under normal conditions, the dual-machine architecture can share the communication load to enhance the overall system throughput capacity, and automatically adjust the traffic distribution in the event of failure to reduce the

pressure on a single point.

1.2 Failover process

- Normal operation of the main server: All business traffic is processed through the main server; the backup server is on standby and keeps data synchronized with the main server.
- Fault Detection: Keepalived and Heartbeat components detect state anomalies when the master server is abnormal (e.g., server down, network failure, etc.).
- Standby server takeover: The system is automatically migrated to the standby server and all services are resumed within 5 seconds without any additional operation by the user.
- Primary Server Recovery: Administrators can restart the primary server after troubleshooting and have it rejoin the cluster to resume dual hot standby mode.

2. Data synchronization and database redundancy

NewLync 2.0 utilizes Cassandra distributed database and MySQL master-slave replication mechanism to ensure that the data between the master and backup servers is always the same, so that even in the event of a failover, there will be no data loss or business interruption.

2.1 Cassandra Distributed Database Synchronization

- Multi-data center (DC1, DC2) architecture is adopted to ensure real-time synchronization of key data such as user configuration information and call records between two servers.
- Configure the Cassandra SEEDS mechanism so that DC1 and DC2 recognize each other and maintain data consistency.
- Ensure that the data write policy is correct for different servers to avoid data conflicts through the `cassandra-topology.properties` configuration file.

2.2 MySQL Master-Slave Replication

- The Master-Master mode ensures that the MySQL databases of both servers can be backed up to each other, i.e., if one server is down, the other server will still be able to provide complete data.
- Through the Binlog log replication mechanism, the database change records are

synchronized to the backup server in real time to ensure data consistency.

- When switching servers, the new master server can automatically load the latest database status to ensure that the service runs normally.

2.3 Uninterrupted call operations

- Established calls may be slightly affected in the event of a failure, but new calls can be resumed within 5 seconds.
- Adopts a SIP server dual registration mechanism that allows end devices to register on both DC1 and DC2 to improve availability.
- After the call data is synchronized, the SIP server can quickly restore the call state, reducing the impact on user perception.

3. Business Layer Disaster Recovery Program

In addition to server-level disaster recovery solutions, NewLync 2.0 also provides multiple disaster recovery mechanisms at the application layer to ensure the stability of enterprise communication services.

3.1 SIP server redundancy

- **Converged Communications Platform Server Dual Registration:** As a SIP server, the Converged Communications Platform supports dual-node registration, ensuring that IP phones, desktops, and mobile devices can be seamlessly switched between the primary and backup servers.
- **Automatic switching of outgoing lines:** When an outgoing line fails, the system can automatically select a backup line to ensure that outgoing calls are not interrupted.
- **Intelligent Routing:** Dynamically adjusts the registration policy of SIP terminals according to the server load to improve the call success rate.

3.2 Monitoring and Alerting Mechanisms

- **NewLync server status in real time,** including CPU load, memory utilization, network status, and more.
- **Automatic Failover:** When an abnormality is detected, the system automatically triggers failover and sends an alarm notification to the administrator.
- **Log analysis and fault location:** The system provides detailed log records to help administrators quickly troubleshoot problems and improve maintenance efficiency.

3.3 Client High Availability

- **One Number, Multiple Devices:** Users can log in to NewLync 2.0 on multiple devices (PCs, cell phones, IP phones) at the same time to achieve synchronization, and when one device drops out, it can be switched to the other device immediately.
- **Call Relay:** Users can freely switch between different devices to ensure communication anytime, anywhere.
- **LDAP Unified Address Book:** All user data is stored in the enterprise-level address book system and automatically synchronized to all clients, avoiding loss of address book due to equipment failure.

4. NewLync 2.0's disaster recovery solution is suitable for the following scenarios:

- **Key industries such as finance and energy:** 7×24 hours uninterrupted communication is required, and business continuity cannot be affected by server failure.
- **Multi-branch enterprises:** Headquarters and branches need to be managed in a unified manner, but local redundancy capability is required to ensure stable regional communications.
- **Large enterprises and call centers:** High concurrency business environment, must have automatic failover and business recovery capabilities.
- **Government and public services:** Higher security requirements, high availability and disaster recovery capabilities are needed to prevent unexpected interruptions.

NewLync 2.0 builds a stable and reliable disaster recovery solution through dual-machine hot standby, efficient data synchronization, intelligent load balancing and automatic failover. Whether it is a single machine failure, network outage, or SIP server abnormality, the system can quickly resume business, ensuring the continuity and high availability of enterprise communications.

6 NewLync and Unified Communications Platform Software Deployment and Installation Guide

This chapter provides a detailed guide to installing and deploying NewLync and the Unified Communications Platform software, covering environment preparation, system configuration, software installation, and related optimization settings. By following this guide, users can successfully complete the deployment of NewLync and the Unified Communications Platform step by step, ensuring stable system operation and meeting enterprise communication needs.

6.1 Hardware Requirements

Detailed Description:

Component	Requirement
CPU	Intel Core i5-8400 and above
Memory	16G DDR4 2666MHZ and above
Available disk space	128GSSD+1T and above

6.2 Hardware, Operating System, and Database Compatibility

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

6.3 Interactive Installation of the NewLync All-in-One System

6.3.1 Server Initialization Preparation

1. Install the Linux operating system and create the root account during the installation process.
2. When creating the root account in the UnionTech (UOS) system, you must select administrator privileges; when partitioning the disk, allocate all free space to the root directory, ensuring that both /home and the root directory have at least 200 GB of space.
3. Download the appropriate installation package based on the server architecture. The installation package version (x86 or ARM) must match; otherwise, installation will fail.
4. The latest integrated installation packages for NewLync 2.0 All-in-One are stored at the following path. Please obtain the latest version of the installation package from this path during installation:

Obtain the installation package	
Please contact your distributor or NewRock .	
Archive name: NewLync_2_0-v1.1-Ubuntu-XXXXX.tar.gz	
List of files after extraction	Description
OMX-4.3.140R067503-Ubuntu-x86_64-xingtang.tar.gz	OMX component installation package
newlync.single_all.x86_64.2.0.133xingtangR20260320.tar.gz	NewLync component installation package
readme.md	Installation Instructions
filelist.txt	Installation Package File List
server_prepare.sh	Server Pre-deployment Initialization Script
deploy_script/	Folder dedicated to deployment scripts,

	containing 4 scripts: install_sysinfo-monitor.sh (System monitoring installation script) export_log.sh (Log export script) install_wizard.sh (Core installation wizard script) getSysInfo.sh (system information retrieval script)
--	---

- After logging in with an administrator account, place the installation package in any directory. Running ``server_prepare.sh`` will automatically create the ``nlk`` user and set a password.
- Run the ``server_prepare.sh`` script to initialize the server. Follow the prompts and enter ``y`` to continue. The script will automatically create the ``nlk`` user, configure password-less ``sudo``, disable the firewall, disable SELinux, and enable IP forwarding.

```
[nlk@uos141 ~]$ ./server_prepare.sh
```
- The server will reboot once the script has finished executing.

6.3.2 Prerequisites for Dual-Server Installation

- The Linux operating system must be installed on both servers.
- Upload and extract the latest installation package to any directory on both servers; it is recommended to place it in the ``/home/nlk`` directory.
- On both servers, navigate to the root directory of the extracted files and run the pre-installation script ``server_prepare.sh``.
- After the script completes, both servers will automatically reboot. Wait for the reboot to finish before proceeding to the next installation steps.



For a single-server installation, the prerequisites need only be completed on one server; the requirements are the same.

6.3.3 Launch the Installation Wizard

After logging in to the host as the nlk user (the nlk login password is Newrock123!@#), navigate to the /home/nlk/deploy directory and run the ./install_wizard.sh script.

After the script runs, the terminal will display the “Newlync System Installation Wizard” interface; press Enter to confirm and start the installation.

```
[nlk@uos141 deploy]$ ./install_wizard.sh
=====
NewLync System Install Wizard
=====
Version: 1.1
Date: 2026-03-17

This wizard will help you configurate NewLync installation environment.
Please complete configures by tips.

Press Enter to start...
```

1. Selecting the TLS Certificate Type for the

1. The terminal will list three certificate type options. Select the desired certificate type (enter 1–3) and press Enter:

- Self-signed certificate: The system automatically generates the certificate, which is valid indefinitely. However, when accessing via the web, a warning will appear indicating that the connection is not secure.
- Newlync Official Certificate: Uses the certificate provided by Newlync. (Valid for one year)
- Custom Certificate: You must first name the client certificates server-customer.crt and server-customer.key and upload them to the /home/nlk/deploy directory

```
=====
Choose TLS Certificate Type
=====
1) Self-signed certificate - Auto generated by system
2) NewLync official certificate - Provided by NewLync
3) Customized certificate - Customized by yourself

Please input choice (1-3): 1
Selected: self-signed certificate
```

2. Installation Mode and Component Selection

1. Installation Mode: Select Standalone Installation or Dual-Master Installation. This installation uses Dual-Master Installation as an example: Enter 2, then press Enter to confirm:

```

=====
Choose Installation Mode
=====
1) Single Installation - Deploy all services on one server
2) Dual Installation - Deploy all services on two servers for higher performance

Please input choice (1-2): 2
Selected: dual installation

```

2. Deployment Mode: Select "New Installation" or "Restore Installation" (please refer to [6.7 Recovery Installation Process \(Expanding from Single Server to Dual Server\)](#)). For this example, we will use a new installation; enter 1 and press Enter to confirm:

```

=====
Choose Deployment Mode
=====
1) Fresh - Install all components as new server
2) Restore - Restore one server's data by backup data on the other server

Please input choice (1-2): 1
Selected: refresh

```

3. Component Selection: To perform a full installation of the NewLync+OMX all-in-one combination, enter 3 and press Enter to confirm:

```

=====
Choose Component (Single Choice)
=====
1) NewLync - One station cloud collaboration
2) OMX - Cloud PBX
3) NewLync-OMX - All-in-one combination

Please input choice (1-3): 3
Selected: NewLync-OMX

```

3. Enter your SSC maintenance login password

1. When entering your password for the first time, you can also simply press Enter (leaving it blank) to use the default password;
2. Enter your password again to confirm;
3. The system displays the message "SSC maintenance login password has been set successfully," indicating that the setup is complete.

```

=====
Get SSC Maintenance Login Password
=====
Please input ssc Maintenance login password (Keep null to use the default password):
Your system is not activated. Please activate as soon as possible for normal use.

Please input the ssc maintenance login password again to confirm:
Ssc maintenance login password is set successfully

```

4. Subnet Mask Configuration

1. If the Docker default subnet conflicts with the customer's private network subnet, enter 2

to specify a custom subnet; if there is no conflict, simply enter 1 to use the default subnet, then press Enter to confirm:

2. If you choose a custom subnet: Follow the prompts to enter the first two segments of the IPv4 subnet mask (e.g., 10.20)

```
=====
Configure Docker Subnet
=====
Will modify Docker default subnet?
1) Use default subnet
2) Customized subnet (Input the first two segments, while the rest two segments are always 0, mask is /16)

Please input choice (1-2): 2
Please input the first two segments of IPv4 subnet (Format: xxx.xxx): 10.50
Configured customized Docker subnet: 10.50.0.0/16
```

5. K8s Pod Subnet Configuration

Follow the prompts to modify the default subnet for the Pod. There are two options available:

1. Use the default subnet. If the default subnet conflicts with the customer's private network subnet, enter 2 to specify a custom subnet; if there is no conflict, simply enter 1 to use the default subnet, then press Enter to confirm:
2. Custom subnet (enter the first two segments; the last two segments are fixed at 0, and the subnet mask is /16). After entering the information, press Enter to confirm.

```
=====
Configure K8s Pod Subnet
=====
Will modify K8s pod default subnet?
1) Use default subnet (10.244.0.0/16)
2) Customized subnet (Input the first two segments, while the rest two segments are always 0, mask is /16)

Please input choice (1-2): 1
Default K8s pod subnet is used: 10.244.0.0/16
```

6. K8s Service Subnet Configuration

Follow the prompts to modify the default subnet for the K8s Service. There are two options available:

1. Use the default subnet. If the default subnet conflicts with the customer's private network subnet, enter 2 to specify a custom subnet; if there is no conflict, simply enter 1 to use the default subnet, then press Enter to confirm:
2. Custom subnet (enter the first two segments; the last two segments are fixed at 0, and the subnet mask is /16). After entering the information, press Enter to confirm.

```

=====
Configure K8s Service Subnet
=====
Will modify K8s service default subnet?
1) Use default subnet (10.96.0.0/16)
2) Customized subnet (Input the first two segments, while the rest two segments are always 0, mask is /16)

Please input choice (1-2): 1
Default K8s service subnet is used: 10.96.0.0/16

```

7. Network Interface and Domain Name Configuration

1. Network interface selection: The system will automatically scan all available network interfaces on the host and list them by number. Enter the corresponding number to select the business network interface, then press Enter to confirm. The system will then display the current IP address of that interface; enter "y" to confirm use of that IP.

```

=====
Choose Network Interface
=====
Scanning available network interfaces...
Id) Interface Name      IPv4 Address
-----
1) ens33                192.168.180.141

Please choose the network interface to deploy system (Its IPv4 address will be used)
Please input interface id (1-1): 1
Selected: Interface ens33, IP address 192.168.180.141
Confirm use this network interface and IP address? [y/n]: y

```

2. Configure Server Domain Name: Enter the host's custom domain name as prompted (as shown in the figure). If using the system's automatically generated default domain name, simply press Enter to confirm.

```

=====
Domain Configure
=====
Please configure domain for this server:
Default domain: nlk397-cloud.newlync.com

Domain will be used to access NewLync services, please confirm the correct configure
Please input domain [Press Enter directly to use default domain]: nlk141-cloud.newlync.com
Confirmed domain: nlk141-cloud.newlync.com

```

8. Dual-Master Deployment – Standby Server Configuration

1. For dual-master mode: Enter the standby server's business IP address as prompted, then press Enter to confirm. The system will automatically verify network connectivity with the standby server.
2. After verification passes, enter the standby server's domain name as prompted, or press Enter to use the default domain name. Ensure that the domain name suffixes for both servers are exactly the same.

```

=====
Dual Mode - The Secondary Server Configure
=====
Please input configure information of the secondary server

Reminder: Two servers will form a high performance cluster, their configure must be correct
Please input IPv4 address of the secondary server: 192.168.180.142
Checking if 192.168.180.142 is available...
✓ Server 192.168.180.142 is available
Confirmed IP of the secondary server: 192.168.180.142

Default domain of the secondary server: nlk417-cloud.newlync.com
Please input domain of the secondary server [Press enter directly to use default domain]: nlk142-cloud.newlync.com
Confirmed domain of the secondary server: nlk142-cloud.newlync.com
✓ Dual mode configure completed

```

9. Confirm Configuration and Proceed with Installation

1. The system will list all configuration details for this dual-server installation. After verifying that everything is correct, enter `y` to begin the installation. If you need to make changes, enter `n` to return to the configuration screen.

```

=====
Confirm & Save Configure
=====

Configure Summary
=====
Certificate type: Self-signed certificate
Docker subnet: 10.50.0.0/16
Installation mode: Dual mode
Deployment mode: Fresh
Selected components: NewLync-OMX
Network interface: ens33
Local IP: 192.168.180.141
Domain: nlk141-cloud.newlync.com
The secondary server's IP: 192.168.180.142
The secondary server's domain: nlk142-cloud.newlync.com
=====

Please confirm if above configure information is correct
Confirm and save configure? [y/n/q(exit)]: y
✓ Saved configure file in /tmp/prepare.env successfully

=====
Install wizard is configurated successfully
=====
Configure file path: /tmp/prepare.env

```

2. Follow the prompts to enter the passwords for the nlk accounts on both servers (the nlk password is Newrock123!@#). The system will automatically complete the installation. (This step is not required for single-server deployment.)

```

Press Enter to start installation...

Start to add ssh no password login
cp: 无法获取'/root/.ssh/known_hosts' 的文件状态(stat): 没有那个文件或目录
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/nlk/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
UOS Server 20 1070a
nlk@192.168.180.142's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'nlk@192.168.180.142'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/nlk/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
UOS Server 20 1070a
nlk@192.168.180.141's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'nlk@192.168.180.141'"
and check to make sure that only the key(s) you wanted were added.

UOS Server 20 1070a
id_rsa
UOS Server 20 1070a

```

- No manual intervention is required during the installation process. Service installation takes approximately 20 minutes. Ensure a stable network connection for the servers throughout the process and do not interrupt the operation.
- An installation report will be generated upon completion.

```

=====
NewLync Installation Summary
=====
Install time: 2026-03-19 17:15:17
Version: 2.0.132R20260317
OMX GA version: OMX-4.3.140R067503
Deploy IP: 192.168.180.143
Domain: nlk143-cloud.yyjr.com
TLS certificate type: Self-signed certificate
Deployment mode: Upgrade
-----
Dual mode configure:
  The secondary server's IP: 192.168.180.144
  The secondary server's domain: nlk144-cloud.yyjr.com
-----
Server information:
  CPU architecture: x86_64
  CPU cores: 8
  Memory: 15Gi
  Total disk space: 112G
  Available disk space: 66G
  Operating system: UOS Server 20
-----
Service status information:
This server CPU has 8 cores, memory is 15.1265GB
cassandra db ... ready
kamillo ... ready
janus ... ready
ldap ... ready
minio ... ready
restund ... ready
nlkas ... ready
k8s pods ... ready
Cluster Nodes:
IP1: 192.168.180.143
HOSTNAME1: omx1.newlync.com
IP2: 192.168.180.144
HOSTNAME2: omx2.newlync.com
OK! 192.168.180.143 is local ip.
docker-compose ps: OK
Container omx-rabbitmq: OK
Container omx-couchdb: OK
Container omx-haproxy: OK
Container omx-applications: OK
Container omx-ecallmgr: OK
Container omx-redis: OK
Container omx-media-fs: OK
Container omx-sip-km: OK
Container omx-syservice: OK
Container web-ui: OK
Container sipub: OK
omx-rabbitmq status: OK
omx-couchdb status: OK
OK! Node couchdb@omx1.newlync.com is active in omx-couchdb.
OK! Node couchdb@omx2.newlync.com is active in omx-couchdb.
omx-haproxy status: OK

```

10. Authorization and Activation

1. Obtain the machine codes: After OMX installation is complete, the machine codes for both servers will appear on the screen. Please record them for use in applying for authorization.

```

{"MachineID": "000C290B50B4X5JbXgKCRPUE7bPV0eILeCBWYvFzZYp+7UPwEXnQP65ns9bF0Kk+qg84uETt+bQ/FB3b1j fQAYoTX3XiaPozHZcdqa/NwITCF5YAcS3Im0EZPPxwzBVj qDc4ra"}
US Server 20.1070e
{"MachineID": "000C290492F6nF3n/pj1U7/UwJlaR6o3MqVnM/j+zRBXdv9sbmHzSzF+4eZpd15/Y1b810nPBpx6USVjWe leCytDZ0vWjHQcZI fNDEY4Yb4bzj P+huhnj3D3qPq3dKqeq/KDKeyDCGa"}
Done!
US Server 20.1070e
NAME IMAGE COMMAND SERVICE CREATED STATUS PORTS
omx-applications omx-applications:4.3.140R067503 "docker-entrypoint.sh" omx-applications 6 minutes ago Up 6 minutes (healthy)
omx-couchdb omx-couchdb:3.5.1 "docker-entrypoint.sh" omx-couchdb 7 minutes ago Up 7 minutes (healthy)
omx-ecallmgr omx-applications:4.3.140R067503 "docker-entrypoint.sh" omx-ecallmgr 6 minutes ago Up 6 minutes (healthy)
omx-haproxy omx-haproxy:2.4.24 "docker-entrypoint.sh" omx-haproxy 7 minutes ago Up 7 minutes (healthy)
omx-media-fs omx-media-fs:1.10.7-22 "docker-entrypoint.sh" omx-media-fs 6 minutes ago Up 6 minutes
omx-rabbitmq omx-rabbitmq:3.9.27 "docker-entrypoint.sh" omx-rabbitmq 8 minutes ago Up 8 minutes (healthy)
omx-redis omx-redis:1.0.2 "docker-entrypoint.sh" omx-redis 4 minutes ago Up 4 minutes (healthy) 127.0.0.1:6379->6379/tcp
omx-sip-km omx-sip-km:4.3.140R067503 "docker-entrypoint.sh" omx-sip-km 6 minutes ago Up 6 minutes
omx-syservice omx-applications:4.3.140R067503 "omx-syservices" omx-syservice 6 minutes ago Up 6 minutes
siphub siphub:latest "docker-entrypoint.s..." siphub 4 minutes ago Up 4 minutes 0.0.0.0:3000->3000/tcp, :::3000->3000/tcp, 9060/tcp, 0.0.0.0:9060->9060/udp, :::9060->9060/udp
web-ui web-ui:4.3.060128 "docker-entrypoint-n..." web-ui 4 minutes ago Up 4 minutes 443/tcp, 0.0.0.0:8085->80/tcp, :::8085->80/tcp
US Server 20.1070e
NAME IMAGE COMMAND SERVICE CREATED STATUS PORTS
omx-applications omx-applications:4.3.140R067503 "docker-entrypoint.sh" omx-applications 5 minutes ago Up 5 minutes (healthy)
omx-couchdb omx-couchdb:3.5.1 "docker-entrypoint.sh" omx-couchdb 7 minutes ago Up 7 minutes (healthy)
omx-ecallmgr omx-applications:4.3.140R067503 "docker-entrypoint.sh" omx-ecallmgr 5 minutes ago Up 5 minutes (healthy)
omx-haproxy omx-haproxy:2.4.24 "docker-entrypoint.sh" omx-haproxy 7 minutes ago Up 7 minutes (healthy)
omx-media-fs omx-media-fs:1.10.7-22 "docker-entrypoint.sh" omx-media-fs 6 minutes ago Up 6 minutes
omx-rabbitmq omx-rabbitmq:3.9.27 "docker-entrypoint.sh" omx-rabbitmq 8 minutes ago Up 7 minutes (healthy)
omx-redis omx-redis:1.0.2 "docker-entrypoint.sh" omx-redis 4 minutes ago Up 4 minutes (healthy) 127.0.0.1:6379->6379/tcp
omx-sip-km omx-sip-km:4.3.140R067503 "docker-entrypoint.sh" omx-sip-km 6 minutes ago Up 6 minutes
omx-syservice omx-applications:4.3.140R067503 "omx-syservices" omx-syservice 5 minutes ago Up 5 minutes 0.0.0.0:3000->3000/tcp, :::3000->3000/tcp, 9060/tcp, 0.0.0.0:9060->9060/udp, :::9060->9060/udp
siphub siphub:latest "docker-entrypoint.s..." siphub 4 minutes ago Up 4 minutes 0.0.0.0:3000->3000/tcp, :::3000->3000/tcp, 9060/tcp, 0.0.0.0:9060->9060/udp, :::9060->9060/udp
web-ui web-ui:4.3.060128 "docker-entrypoint-n..." web-ui 4 minutes ago Up 4 minutes 443/tcp, 0.0.0.0:8085->80/tcp, :::8085->80/tcp
US Server 20.1070e
no crontab for root
db_cluster_mon.sh is added as a daily task on omx1.newlync.com, database will be monitored
US Server 20.1070e
no crontab for root
db_cluster_mon.sh is added as a daily task on omx2.newlync.com, database will be monitored

```

2. Importing the license:

- Newlync Authorization: Import the codes in the "System Management - System Settings - Authorization Information" section of the SSC web interface on both servers.
- OMX Authorization: On the main server's SSC web interface, go to "Cloud PBX Management > OMX Management > OMX Authorization" and click "Upload" to upload the 3 license files.

6.4 IV. How to Change the IP Address or Domain Name for the Newlync 2.0 All-in-One Device

Modifying the IP address or domain name involves two scenarios: both servers are online, or only one server is online. Key requirements: Regardless of the scenario, only the host server should run the installation wizard script to complete the configuration update; do not restart the server; and ensure the domain name suffixes for both servers remain consistent. The specific steps are as follows:

Scenario 1: Both Servers Are Online – Modifying IP / Domain Name

This scenario applies when both servers are operating normally and you need to modify the IP, domain name, or both on both servers simultaneously. Both servers must complete the IP configuration changes, and only the host server should run the installation wizard to update the system configuration.

Step 1: Modify the IP configuration on both servers and apply the changes (perform on both)

1. Log in to the server as the nlk user, open the network configuration file (Ubuntu: `/etc/netplan/xxx.yaml`; UOS: `/etc/sysconfig/network-scripts/ifcfg-xxx`), and update the IP address, gateway, and subnet mask in the file to the new configuration based on your system type.

2. After making the changes, run the system-specific command to apply the IP settings.

Do not restart the server, as this will cause service failures:

- Ubuntu: `sudo netplan apply`
- UOS/CentOS systems: `sudo systemctl restart NetworkManager`

`sudo nmcli connection down ens33 && sudo nmcli connection up ens33`

3. Run the ``ip addr`` command to verify that the new IP address has taken effect and ensure network connectivity between the two machines.
4. If you need to modify the domain name, you can configure it directly in the subsequent installation wizard.

Step 2: Run the installation wizard on the host to update the configuration for both machines (host-only operation)

1. Log in to the host as the nlk user, navigate to the `/home/nlk/deploy` directory, and run the installation wizard script `install_wizard.sh`:

```
[nlk@uos141 deploy]$ ./install_wizard.sh
=====
NewLync System Install Wizard
=====
Version: 1.1
Date: 2026-03-17

This wizard will help you configure NewLync installation environment.
Please complete configures by tips.

Press Enter to start...
```

2. After the script starts, the system detects the existing configuration and prompts "Update IP/domain name configuration?" Enter ``y`` and press Enter to confirm.

```
You have already installed NewLync
Will update IP or domain configure? [y/n(exit)]: y
```

3. Enter the SSC maintenance password as prompted (if not modified, leave it blank and press Enter to use the default password).

```
Please input ssc Maintenance login password (Keep null to use the default password):
SSC maintenance login password is null, will use the default password instead
```

4. Proceed to complete the following steps in order: select the new network interface for the primary host, configure the new domain name for the primary host, enter the new IP address for the standby host, and configure the new domain name for the standby host. Ensure all information is accurate throughout the process.

```
=====
          Choose Network Interface
=====
Scanning available network interfaces...
Id) Interface Name      IPv4 Address
-----
1) ens33                192.168.180.143

Please choose the network interface to deploy system (Its IPv4 address will be used)
Please input interface id (1-1): 1
Selected: Interface ens33, IP address 192.168.180.143
Confirm use this network interface and IP address? [y/n]: y
=====
          Domain Configure
=====
Please configure domain for this server:
Default domain: nlk141-cloud.newlync.com

Domain will be used to access NewLync services, please confirm the correct configure
Please input domain [Press Enter directly to use default domain]: nlk143-cloud.yyjr.com
Confirmed domain: nlk143-cloud.yyjr.com
=====
          Dual Mode - The Secondary Server Configure
=====
Please input configure information of the secondary server
Old IP of the secondary server: 192.168.180.142

Reminder: Two servers will form a high performance cluster, their configure must be correct
Please input IPv4 address of the secondary server: 192.168.180.144
Checking if 192.168.180.144 is available...
✓ Server 192.168.180.144 is available
Confirmed IP of the secondary server: 192.168.180.144

Default domain of the secondary server: nlk142-cloud.newlync.com
Please input domain of the secondary server [Press enter directly to use default domain]: nlk144-cloud.yyjr.com
Confirmed domain of the secondary server: nlk144-cloud.yyjr.com
✓ Dual mode configure completed
```

5. Once configuration is complete, the system will generate a new configuration summary. Enter "y" to confirm the update; the system will automatically synchronize the new IP and domain name configurations across both machines and restart the relevant services (no manual intervention required).

```

=====
Configure Summary
=====
Certificate type: Self-signed certificate
Docker subnet: 10.50.0.0/16
Installation mode: Dual mode
Deployment mode: Upgrade
Selected components: NewLync-OMX
Network interface: ens33
Local IP: 192.168.180.143
Domain: nlk143-cloud.yyjr.com
The secondary server's IP: 192.168.180.144
The secondary server's domain: nlk144-cloud.yyjr.com
Old local IP: 192.168.180.141
Old domain: nlk141-cloud.newlync.com
The secondary server's old IP: 192.168.180.142
The secondary server's old domain: nlk142-cloud.newlync.com
=====

Please confirm if above configure information is correct
Confirm and save configure? [y/n/q(exit)]: y
✓ Saved configure file in /tmp/prepare.env successfully

=====
Install wizard is configured successfully
=====
Configure file path: /tmp/prepare.env

```

6. Once the update is complete, the terminal will display a message indicating that the configuration update was successful, matching the output of a fresh installation. You can verify that the service is functioning normally by accessing the new domain name.

Scenario 2: Only one server is online; only modify the IP address/domain name of the online server

This scenario applies when, after a dual-server installation is complete, you need to split the setup to use a single server independently (using only the primary or only the standby server) and must modify the IP of the server in use. Simply run the `install\_wizard.sh` script on the target server you wish to use. The procedure is identical to the dual-server configuration; during the configuration phase, you only need to enter the IP and domain name information of the other offline server.

Step 1: Modify the IP configuration on the online server and apply the changes (perform this step only on the online server)

Modify the IP configuration of the online server, execute the command to apply the changes (do not reboot), and verify that the new IP is functioning properly.

1. Log in to the server as the nlk user, open the network configuration file (Ubuntu: `/etc/netplan/xxx.yaml`; UOS: `/etc/sysconfig/network-scripts/ifcfg-xxx`), and update

the IP address, gateway, and subnet mask in the file to the new configuration according to your system type.

2. After making the changes, execute the system-specific command to apply the IP settings. Do not restart the server under any circumstances, as this will cause service failures:
 - Ubuntu: `sudo netplan apply`
 - UOS/CentOS systems: `sudo systemctl restart NetworkManager`
`sudo nmcli connection down ens33 && sudo nmcli connection up ens33`
3. Run the `ip addr` command to verify that the new IP address has taken effect, ensuring that the online server's IP is accessible while the other server's network connection is down.
4. If you need to modify the domain name, you can configure it directly in the subsequent installation wizard.

Step 2: Run the installation wizard on the online server to update the configuration (perform this step only on the online server)

1. Log in to the host as the `nlk` user, navigate to the `/home/nlk/deploy` directory, and run the installation wizard script `install_wizard.sh`:

```
[nlk@uos141 deploy]$ ./install_wizard.sh
=====
NewLync System Install Wizard
=====
Version: 1.1
Date: 2026-03-17

This wizard will help you configure NewLync installation environment.
Please complete configures by tips.

Press Enter to start...
```

2. Enter `y` to confirm the update of the IP/domain name configuration, then enter the SSC maintenance password (leave blank and press Enter).

```
You have already installed NewLync
Will update IP or domain configure? [y/n(exit)]: y

Please input ssc Maintenance login password (Keep null to use the default password):
SSC maintenance login password is null, will use the default password instead
```

3. Select the new network interface for the online server and configure the new IP address and domain name.

```

=====
Choose Network Interface
=====
Scanning available network interfaces...
Id) Interface Name      IPv4 Address
-----
1) ens33                192.168.180.143

Please choose the network interface to deploy system (Its IPv4 address will be used)
Please input interface id (1-1): 1
Selected: Interface ens33, IP address 192.168.180.143
Confirm use this network interface and IP address? [y/n]: y
=====

Domain Configure
=====
Please configure domain for this server:
Default domain: nlk141-cloud.newlync.com

Domain will be used to access NewLync services, please confirm the correct configure
Please input domain [Press Enter directly to use default domain]: nlk143-cloud.yyjr.com
Confirmed domain: nlk143-cloud.yyjr.com
=====

Dual Mode - The Secondary Server Configure
=====
Please input configure information of the secondary server
Old IP of the secondary server: 192.168.180.142

Reminder: Two servers will form a high performance cluster, their configure must be correct
Please input IPv4 address of the secondary server: 192.168.180.144
Checking if 192.168.180.144 is available...
✓ Server 192.168.180.144 is available
Confirmed IP of the secondary server: 192.168.180.144

Default domain of the secondary server: nlk142-cloud.newlync.com
Please input domain of the secondary server [Press enter directly to use default domain]: nlk144-cloud.yyjr.com
Confirmed domain of the secondary server: nlk144-cloud.yyjr.com
✓ Dual mode configure completed

```

4. When the system prompts you to enter the IP address or domain name of the other (offline) server, enter the original IP address or domain name of the offline server and press Enter to confirm (this must be entered even if the offline server cannot be verified).
5. After verifying that the configuration summary is correct, enter "y" to confirm the update. The system will then complete the IP/domain name configuration update for the online server.

6.5 Recovery Installation Process (Expanding from Single Server to Dual Server)

After an original two-server environment has been split into a single-server setup for a period of time, a new server (either a brand-new server or an existing standby server) must be added to re-establish a two-server high-availability environment with the existing single server. The IP address and domain name of the newly added server may differ from the original two-server configuration or remain consistent; both scenarios are supported by this procedure.

Prerequisites

- The existing single-server system is running normally, with no service abnormalities, and the SSC management interface is accessible.
- The new server has completed the Linux operating system installation and created the `nlk` user.
- The new server must remain powered off initially to ensure that its assigned IP address cannot be pinged on the network, thereby preventing configuration conflicts.

Step 1: Modify the configuration on the existing single-server system to add the new server's information (this step is performed only on the existing single-server system)

Update the dual-server configuration on the existing standalone server by entering the IP address or domain name of the new server. The procedure is the same as when modifying an IP address or domain name:

1. Log in to the host as the `nlk` user, navigate to the `/home/nlk/deploy` directory, and execute the installation wizard script `install\_wizard.sh`:
2. Follow the script prompts to enter "y" to confirm updating the IP/domain name configuration, and enter the server password (leave blank and press Enter).
3. If the existing single-node server does not require IP/domain name changes, simply select the original network interface to confirm the existing IP/domain name; if changes are needed, configure the new IP and domain name as prompted.
4. When the system prompts you to enter the IP address or domain name of another server, enter the planned IP address and domain name for the newly added server (the domain name suffix must match that of the existing standalone server), then press Enter to confirm.
5. After verifying that the configuration summary (existing server information + new server configuration information) is correct, enter "y" to confirm the update. The system will save the configuration without requiring a service restart.

Step 2: Preparations for the New Server (Performed only on the new server)

1. Power on the new server, ensure it is network-connected to the existing server, and configure it with the IP address specified in Step 1.
2. In the /home/nlk directory on the new server, upload the latest installation package and extract it.
3. In the root directory of the extracted files, enter the command `./server_prepare.sh` to run the pre-initialization script.
4. Follow the terminal prompts and enter "y" to confirm. Once the script completes, the new server will automatically reboot; wait for the reboot to finish.

Step 3: Perform a Restore Installation on the New Server (New Server Only)

1. After the new server restarts, log in as the nlk user and enter `cd /home/nlk/deploy` to navigate to the core deployment directory where the installation package was extracted.
2. Enter `./install_wizard.sh` to run the installation wizard script. After the Restore installation process starts, press Enter to enter the installation wizard.

```
[nlk@U05154 deploy]$ ./install_wizard.sh
=====
NewLync System Install Wizard
=====
Version: 1.1
Date: 2026-03-17

This wizard will help you configurate NewLync installation environment.
Please complete configures by tips.

Press Enter to start...
```

3. TLS Certificate Type Selection: Select the same certificate type as the existing standalone server (e.g., if the existing server uses a self-signed certificate, enter 1 for the new server as well), then press Enter to confirm.

```
=====
Choose TLS Certificate Type
=====
1) Self-signed certificate - Auto generated by system
2) NewLync official certificate - Provided by NewLync
3) Customized certificate - Customized by yourself

Please input choice (1-3): 1
Selected: self-signed certificate
```

4. Installation Mode Selection: Enter 2 to select dual-host installation, then press Enter to confirm.

```

=====
Choose Installation Mode
=====
1) Single Installation - Deploy all services on one server
2) Dual Installation - Deploy all services on two servers for higher performance

Please input choice (1-2): 2
Selected: dual installation

```

5. Deployment mode selection: Enter 2 to select Restore (reinstallation). This is a critical step; ensure the selection is correct, then press Enter to confirm.

```

=====
Choose Deployment Mode
=====
1) Fresh - Install all components as new server
2) Restore - Restore one server's data by backup data on the other server

Please input choice (1-2): 2
Selected: restore

```

6. Installation component selection: Select the same components as the existing standalone server, then press Enter to confirm.

```

=====
Choose Component (Single Choice)
=====
1) NewLync - One station cloud collaboration
2) OMX - Cloud PBX
3) NewLync-OMX - All-in-one combination

Please input choice (1-3): 3
Selected: NewLync-OMX

```

7. Network Interface Selection: Select the new server's business network port, enter the port number to select it, then enter 'y' to confirm.

```

=====
Choose Network Interface
=====
Scanning available network interfaces...
Id) Interface Name      IPv4 Address
-----
1) ens33                192.168.180.154

Please choose the network interface to deploy system (Its IPv4 address will be used)
Please input interface id (1-1): 1
Selected: Interface ens33, IP address 192.168.180.154
Confirm use this network interface and IP address? [y/n]: y

```

8. Local Domain Name Configuration: Enter the new server domain name (matching the suffix of the existing standalone server), then press Enter to confirm.

```

=====
Domain Configure
=====
Please configure domain for this server:
Default domain: nlk345-cloud.newlync.com

Domain will be used to access NewLync services, please confirm the correct configure
Please input domain [Press Enter directly to use default domain]: nlk154-cloud.yyds.com
Confirmed domain: nlk154-cloud.yyds.com

```

9. Existing standalone server configuration: Enter the service IP address of the existing operational standalone server, press Enter to confirm, and the system will automatically verify network connectivity with the existing standalone server.

```

=====
Dual Mode - The Secondary Server Configure
=====
Please input configure information of the secondary server

Reminder: Two servers will form a high performance cluster, their configure must be correct
Please input IPv4 address of the secondary server: 192.168.180.147
Checking if 192.168.180.147 is available...
✓ Server 192.168.180.147 is available
Confirmed IP of the secondary server: 192.168.180.147

```

10. Confirm Configuration Summary and Execute Restore: The system lists all configuration information for the Restore installation. After verifying that everything is correct, enter "y" to confirm. Once confirmed, press Enter to begin the restore installation.

```

Press Enter to start installation...

Start to add ssh no password login
cp: 无法获取'/root/.ssh/known_hosts' 的文件状态(stat): 没有那个文件或目录
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/nlk/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
UOS Server 20 1070a
nlk@192.168.180.147's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'nlk@192.168.180.147'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/nlk/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
UOS Server 20 1070a
nlk@192.168.180.154's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'nlk@192.168.180.154'"
and check to make sure that only the key(s) you wanted were added.

UOS Server 20 1070a
id_rsa
UOS Server 20 1070a

=====
Start to install NewLync components
=====
This server CPU has 8 cores, memory is 15.1265GB
----- start install yq -----
----- yq install success! -----
UOS Server 20 1070a
env
Restore backup server
Docker subnet is restored as 10.50.0.0/16
This server CPU has 8 cores, memory is 15.1265GB
Prepare env file

```

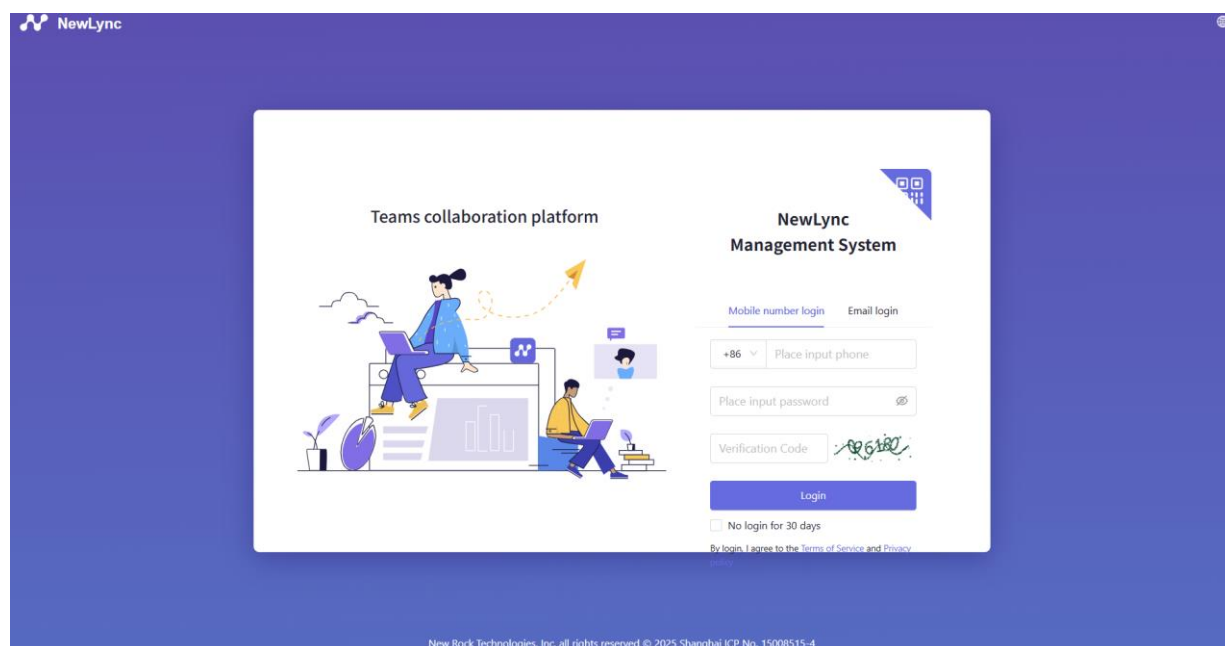
7 NewLync Management Backend Configuration and Operation

The management backend is the enterprise information management platform. The administrator logs into the admin backend for each enterprise configuration.

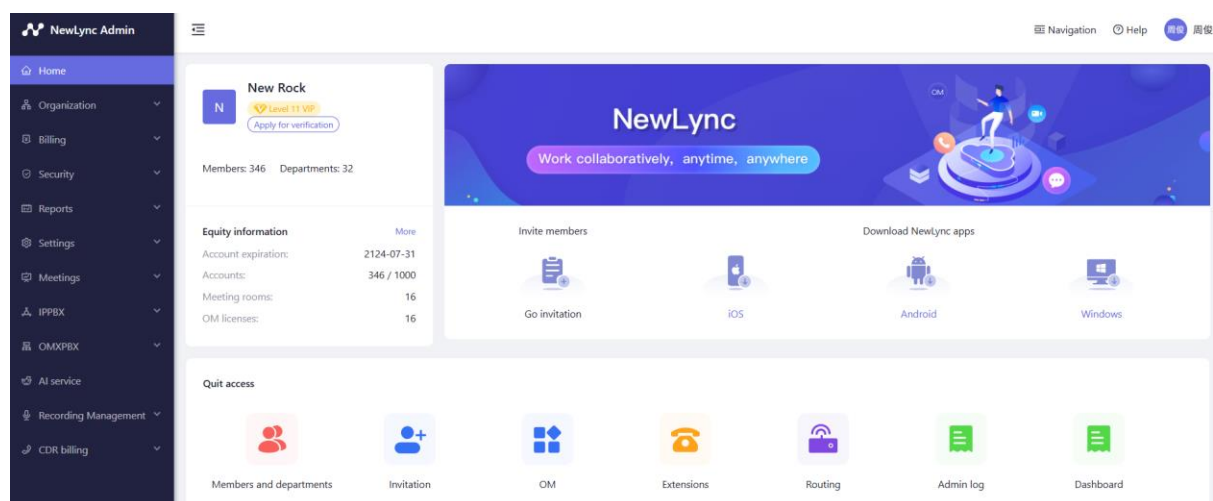
7.1 Basic Operation

7.1.1 Log in

Only Business Creators, Super Administrators and Administrators can log in to the admin backend. Enter the current environment's admin backend domain name in your browser to open the admin backend login page. There are three login methods, which are cell phone login, email login and client scanning login.

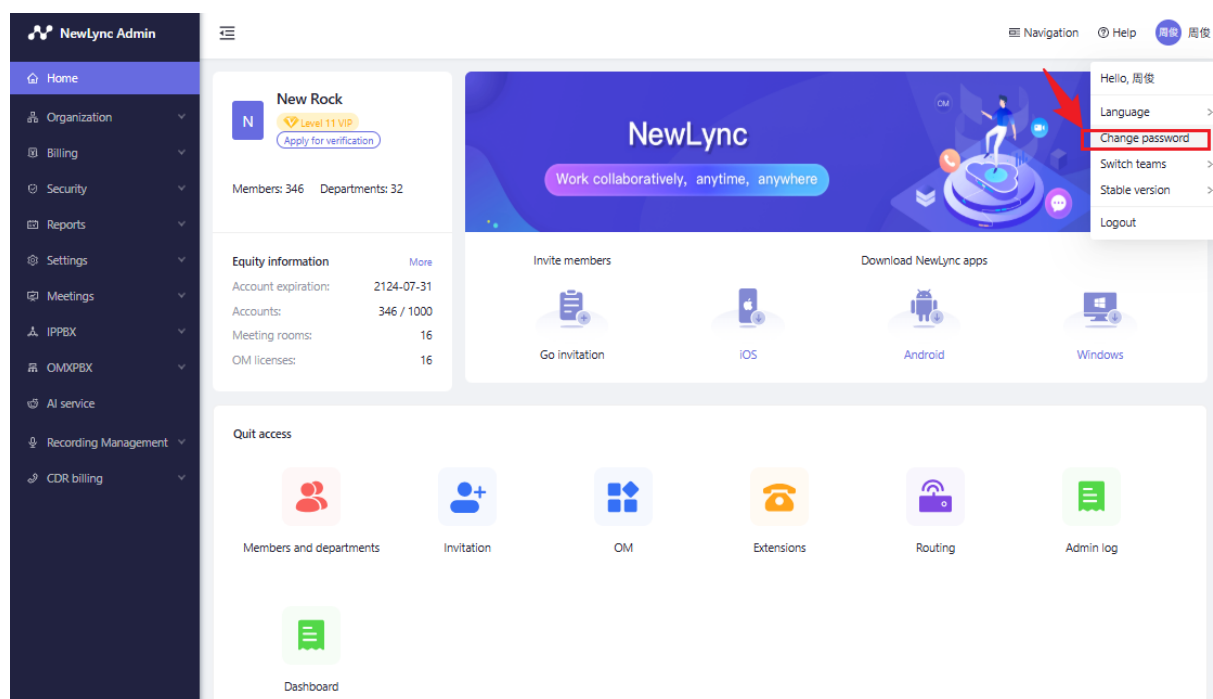


Successful login, enter the home page can see the basic information of the enterprise, enterprise rights and interests and common functions of the entrance.



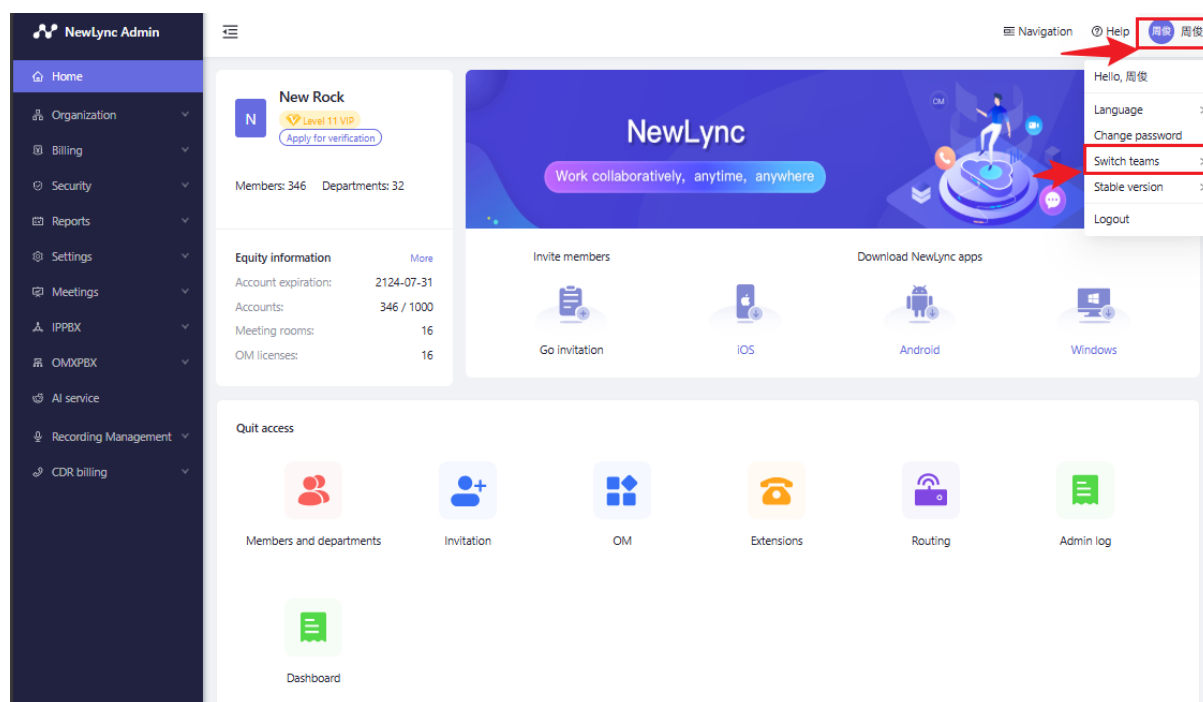
7.1.2 Change password

After logging in, click on the user's name in the upper right corner, click on Change Password and then enter your old and new passwords.



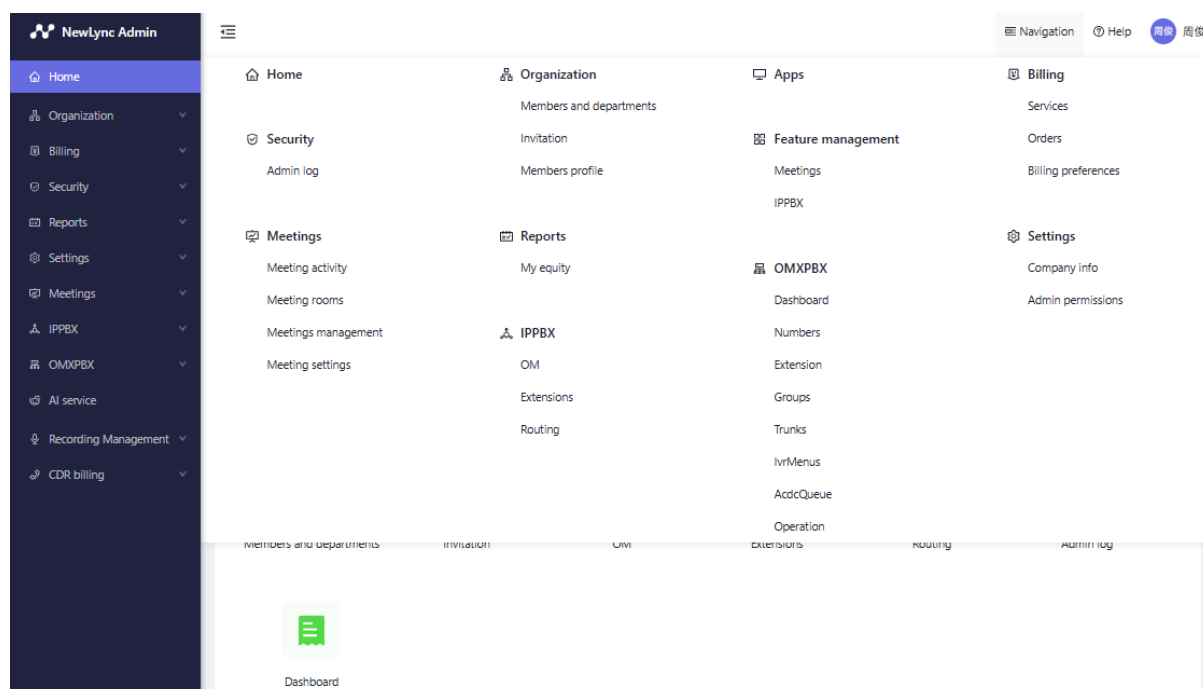
7.1.3 Switching teams

You can select the team when you log in, or you can click on the user name in the upper right corner after logging in and click Switch Team to select the team you need to switch to.



7.1.4 Global navigation

Click on Global Navigation in the upper right corner to quickly navigate to the appropriate function item.



7.2 Organizational Structure

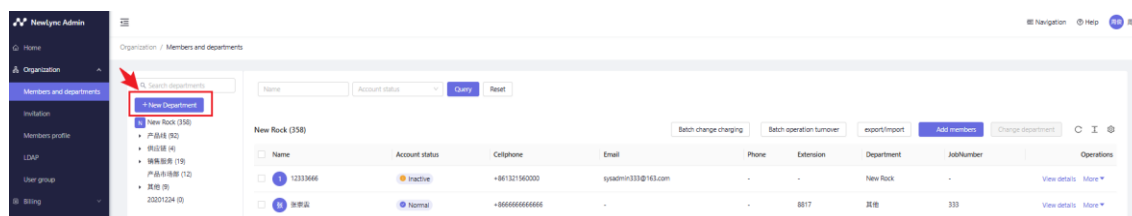
7.2.1 Membership and sectors

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

Add department

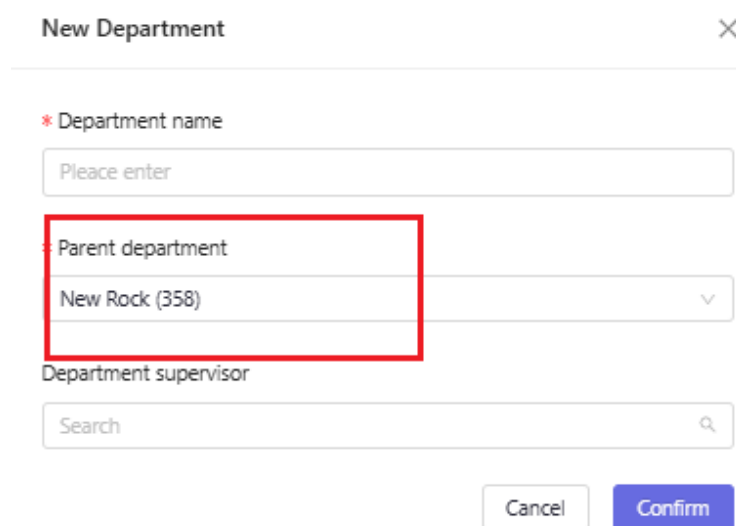
Step 1. Go to the NewLync admin backend and click Organization Structure > Members & Departments.

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



New sectors

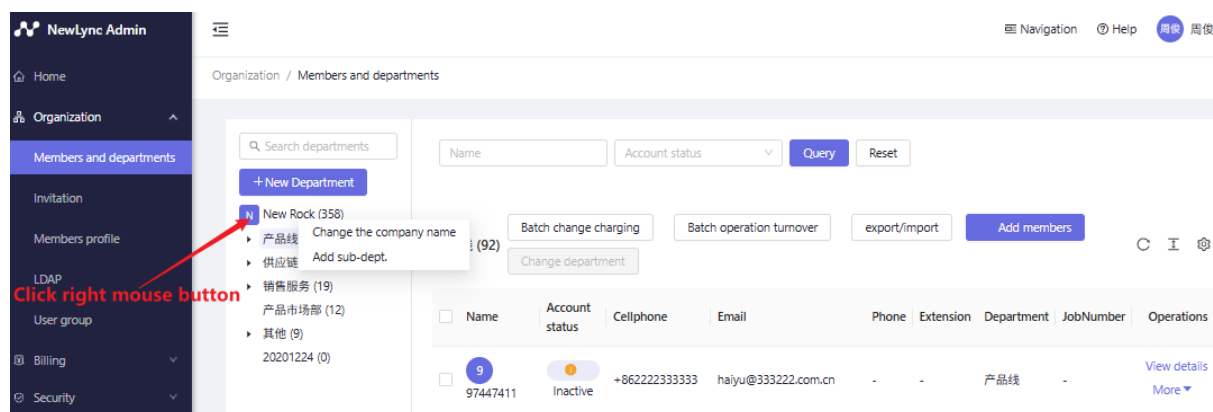
Step 3. Enter the department name in the pop-up window, select the parent department, and set the department head (optional).



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.

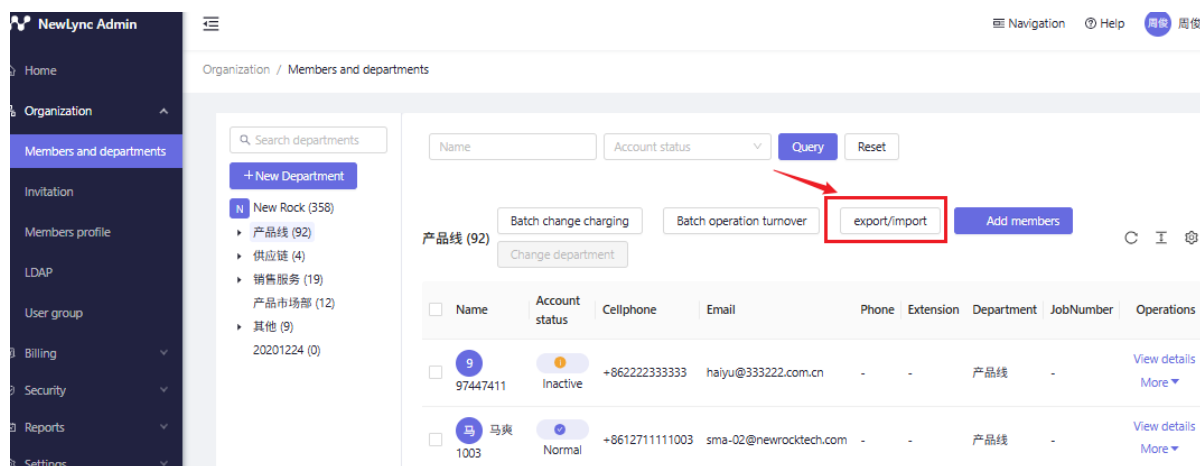


editorial department

Import & Export Membership

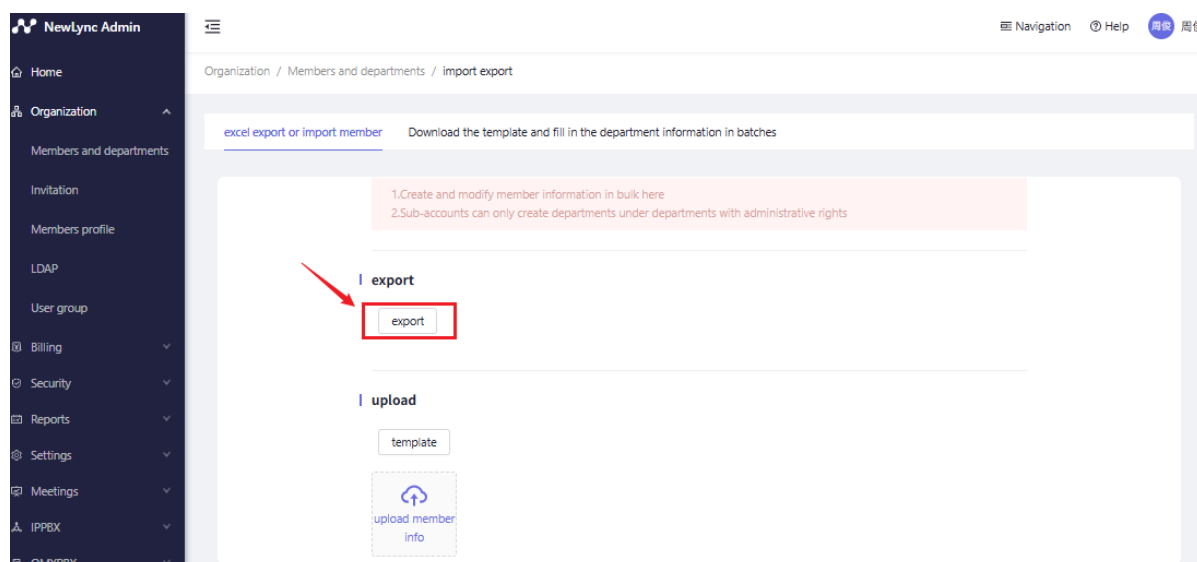
Step 1. Go to the NewLync admin backend and click Organization Structure > Members & Departments.

Step 2. Click Import Export.



Import Export Members

Step 3. Click Export Members to export all members.

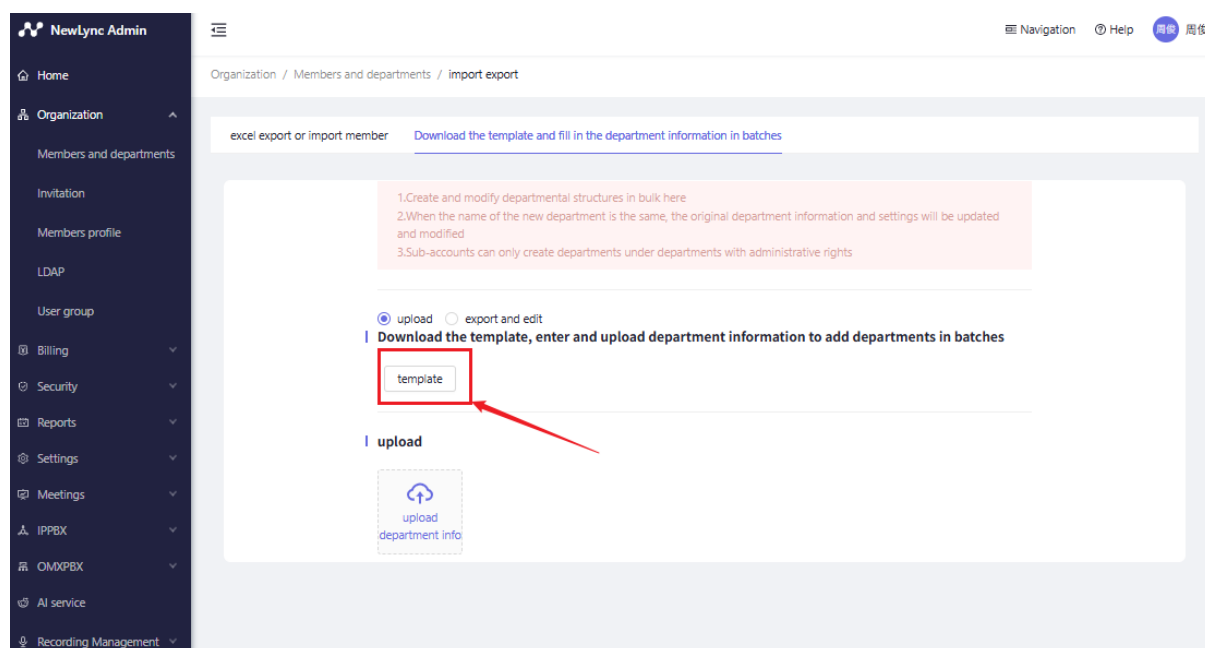


Import Export Members

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. Please be careful not to modify the table structure.

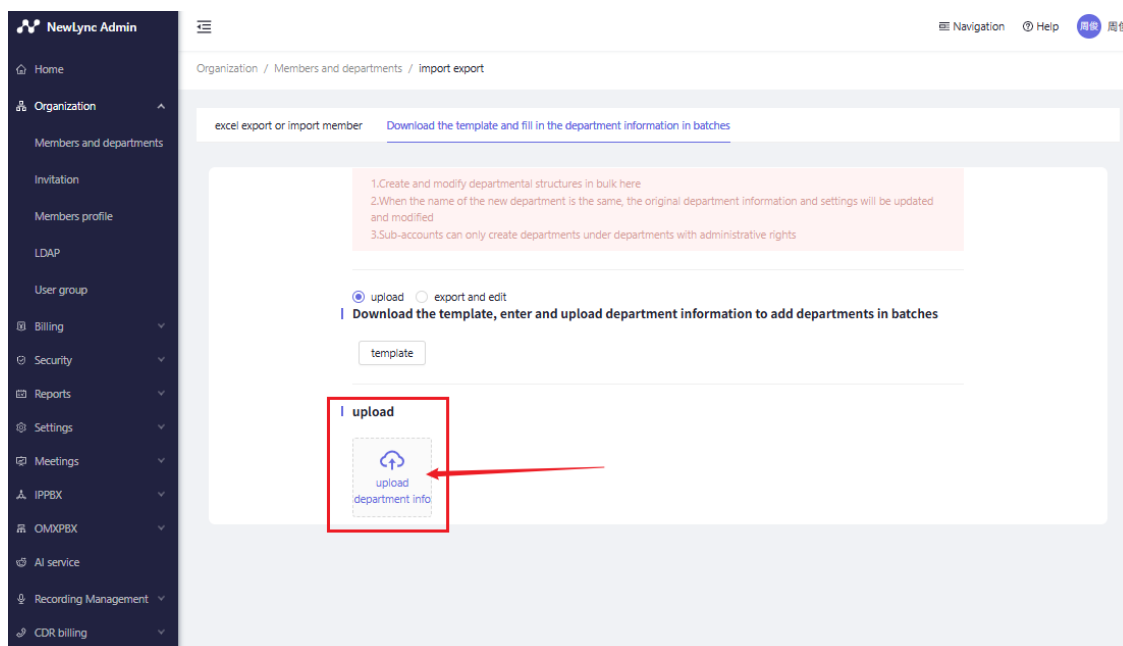
Import Export Department

Step 1. Download the template, enter department information and upload it to add departments in bulk.



Download Templates

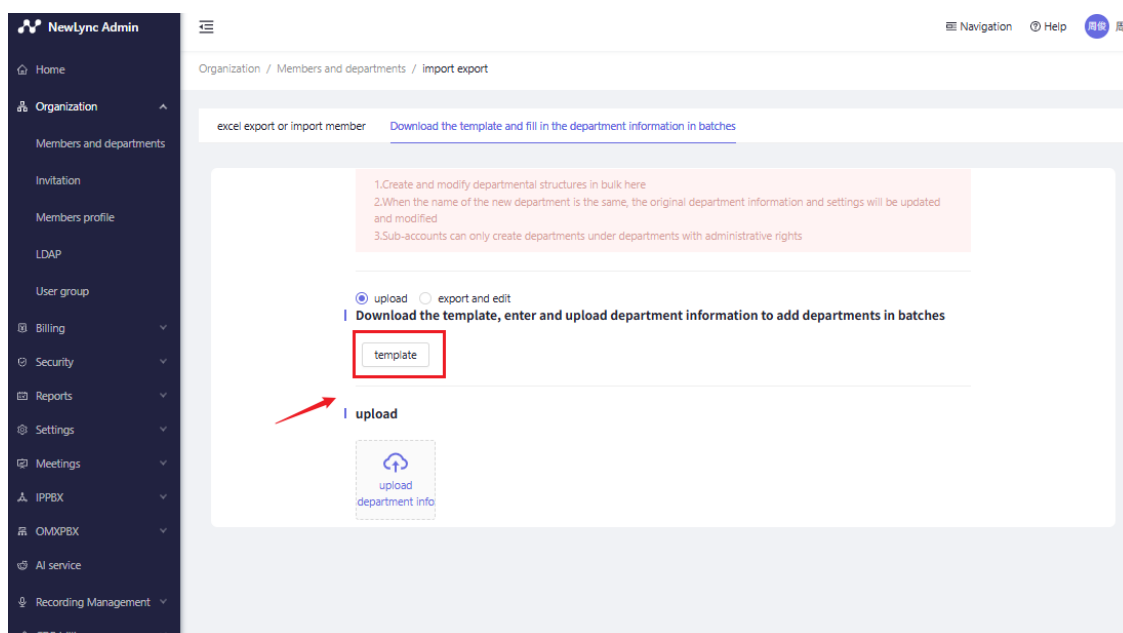
Step 2. Follow the form prompts and click Upload Department Information after completing the form.



Uploading departmental information

Export and modify departments

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

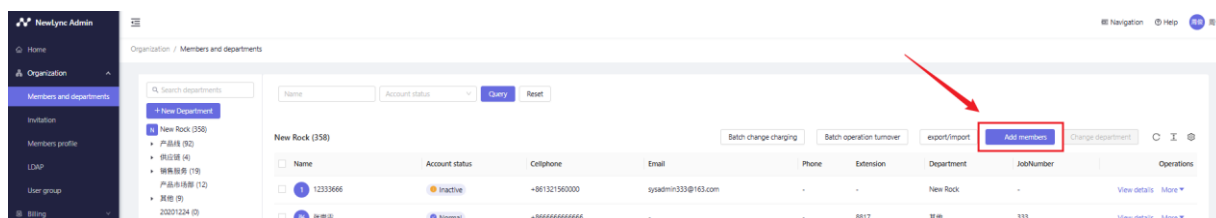


Download Templates

Add Member

Step 1. Go to the NewLync admin backend and click Organization Structure > Members & Departments.

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

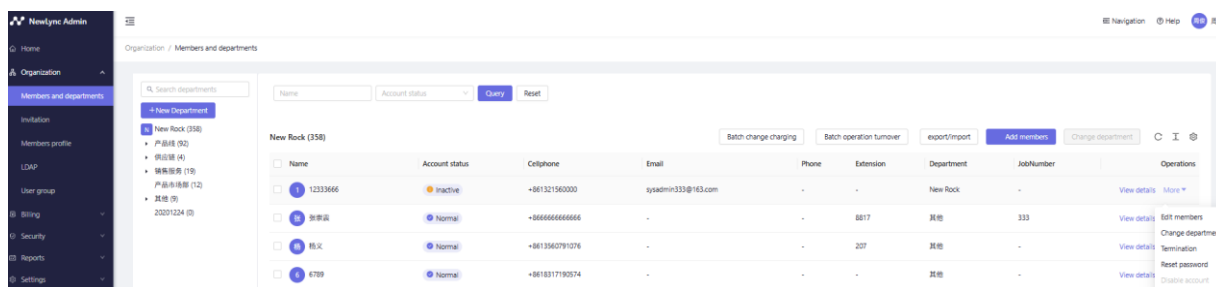


Add Member

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.



Modification of 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 the box to turn on the appropriate permissions and click OK to save.

Item	Definition
Name	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.

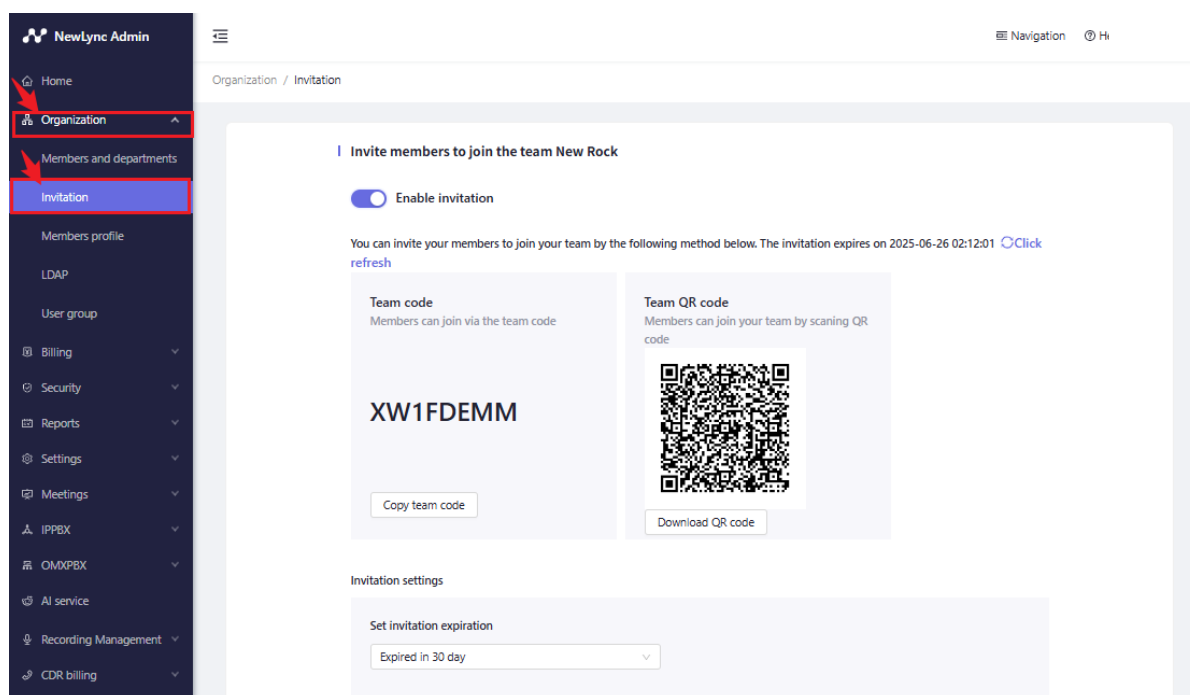
Cell phone	Employee's cell phone number.
Phone	Employee's landline number.
Department	The department to which the employee belongs. Administrators or users with privileges can use this field to view the departmental affiliation of an employee, or to perform departmental transfers.
Job number	The job number is used to distinguish between different employees and is an important identifier of the employee's identity.

Explanation of the Modify Member Information screen

7.2.2 Invitation

Step 1. Go to the NewLync admin backend and click Organizational Structure -> Invitation.

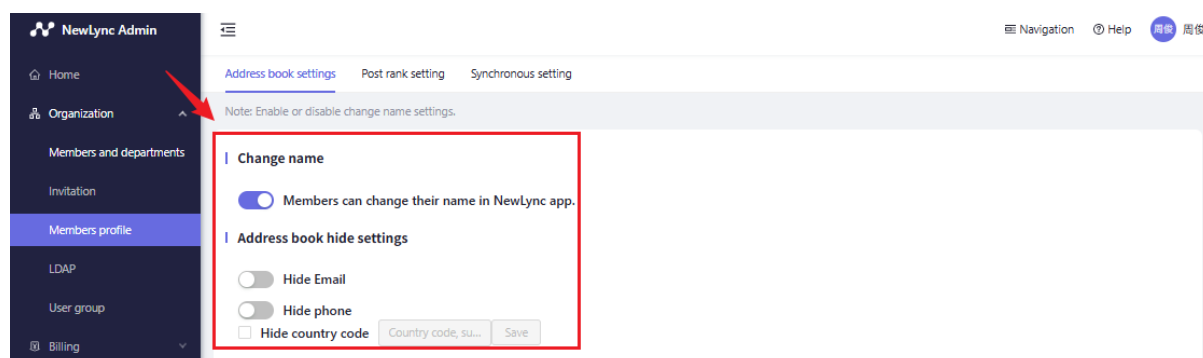
Step 2. Administrators can get the team code and team QR code on this page. Share the invitation information with members.



Step 3. Members download the client from the NewLync website, register for a NewLync account, and use the team code to join the organization during the registration process.

7.2.3 Address Book Settings

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



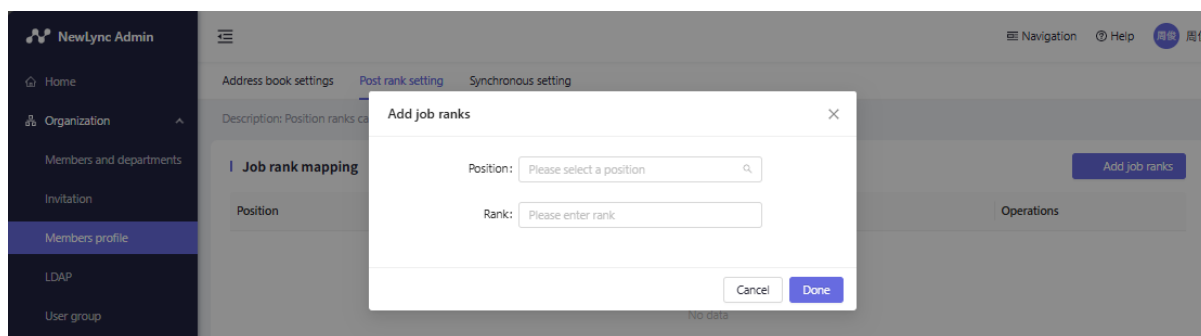
Name modification settings

Address Book Hidden Settings

Item	Define
Name modification settings	When this option is enabled, regular members can change their name information autonomously through the NewLync client.
Hide Mail	When enabled, members' email addresses in the address book will be hidden
Hidden phone	When enabled, members' cell phone numbers in the address book will be hidden
Hide country code	When enabled, the phone numbers displayed in the address book will not include the international area code, which can be set independently.

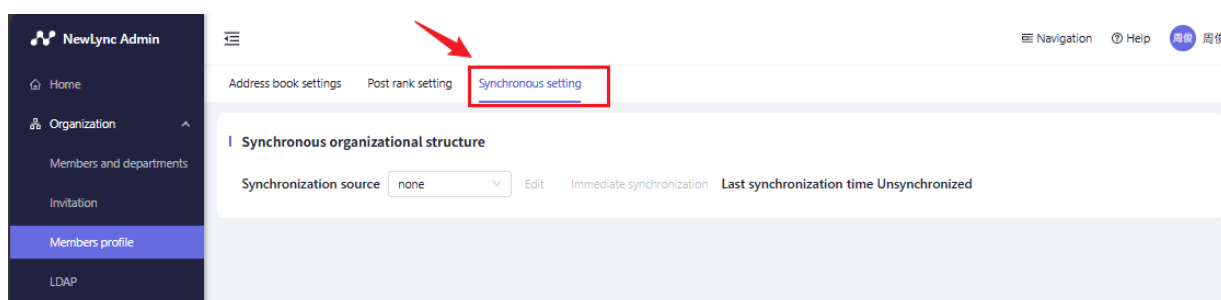
Position grading

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.



Synchronized Organizational Structure

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



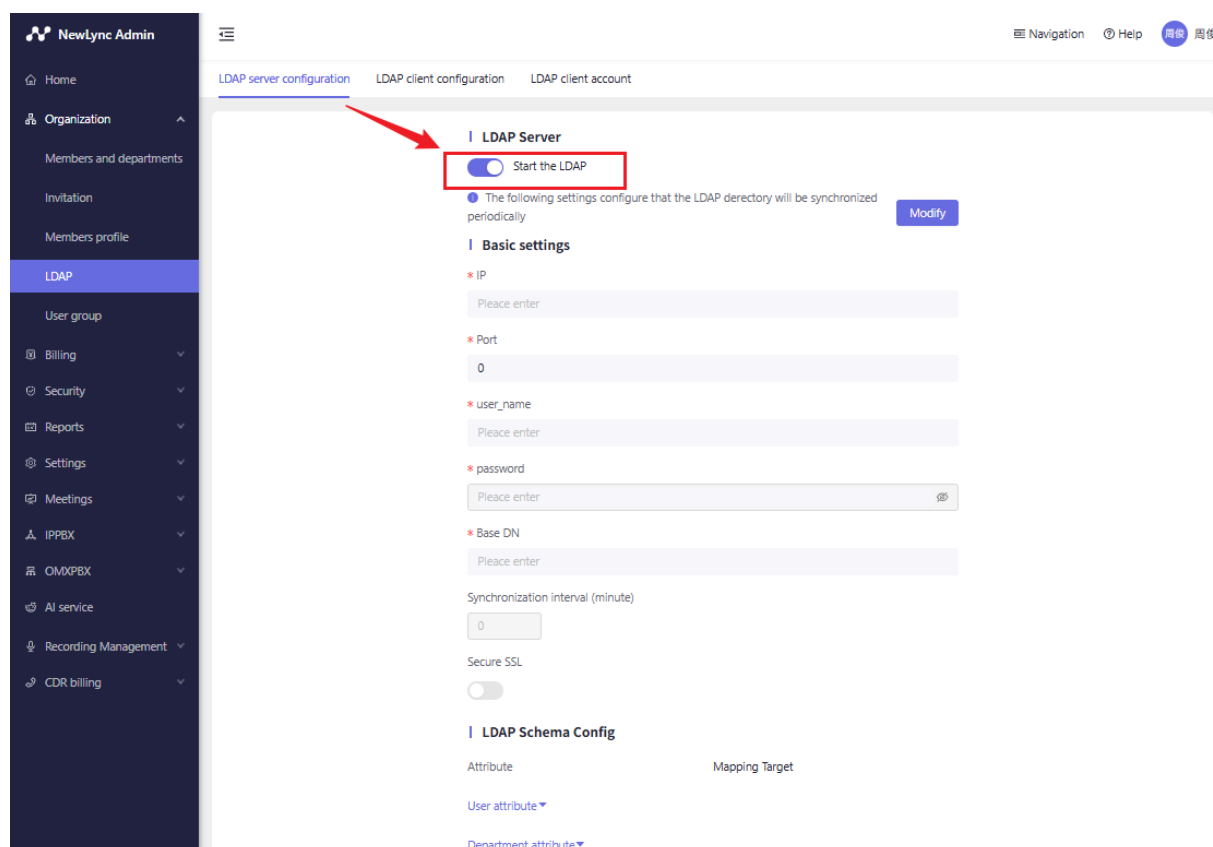
7.3 LDAP

The NewLync Contacts system supports the use of LDAP with IP phones to provide a convenient cloud-based address book service for IP phones. NewLync 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, NewLync 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.

7.3.1 Enabling the LDAP server

Navigate to click Organizational Structure->LDAP.

Step 1. Click the LDAP Client Configuration tab and click Enable LDAP.



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.
Cryptographic	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	Enables or disables SSL encrypted communication.

LDAP server parameters

7.3.2 LDAP Schema Settings

LDAP Schema Configuration Used to define the data field mapping relationship between the NewLync address book and the LDAP server. The administrator fills in the appropriate content

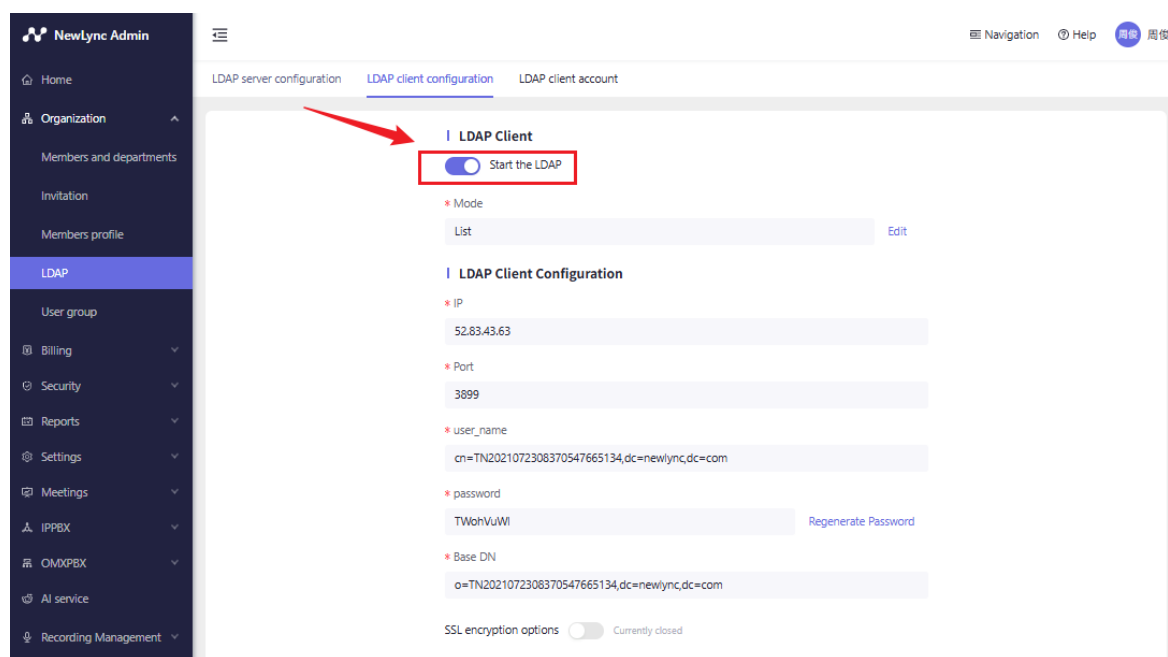
based on the employee's information.

Attribute	Mapping Target
LDAP Schema Config	
User attribute ▲	
User objectClass	inetOrgPerson
Name	Please enter
Cellphone	Please enter
Department	Please enter
Email	Please enter
English name	Please enter
Gender	Please enter
Employee ID	Please enter
Seat ID	Please enter
Job title	Please enter
Direct manager	Please enter
Workforce Type	Please enter
Date of employment	Please enter
Phone	Please enter
Address	Please enter
Remarks	Please enter
Department attribute ▼	

LDAP Schema Configuration

7.3.3 LDAP Client Configuration

NewLync 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.



LDAP Client Configuration Interface

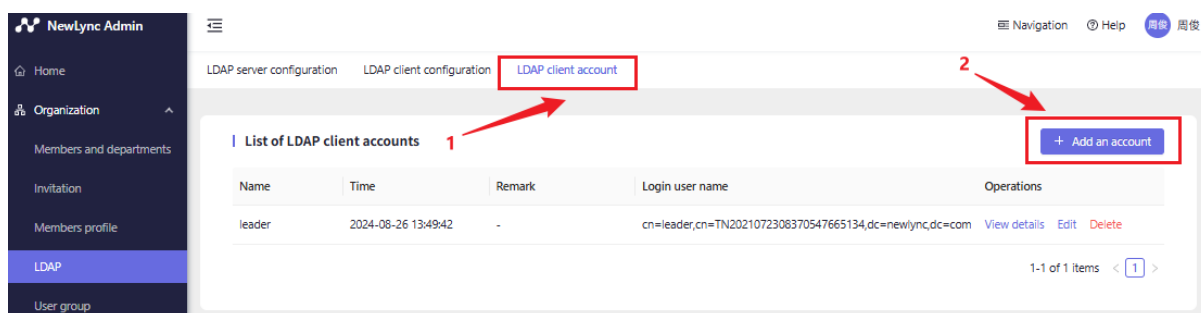
Item	Define
Address book architecture	Displays the architecture (Schema) configuration currently used by the LDAP client. The schema defines the mapping relationship between LDAP data fields and system address book fields.
LDAP server	Specifies the LDAP server address to be used for the connection.
Ports	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.

LDAP Configuration Definitions

7.3.4 Creating an LDAP account

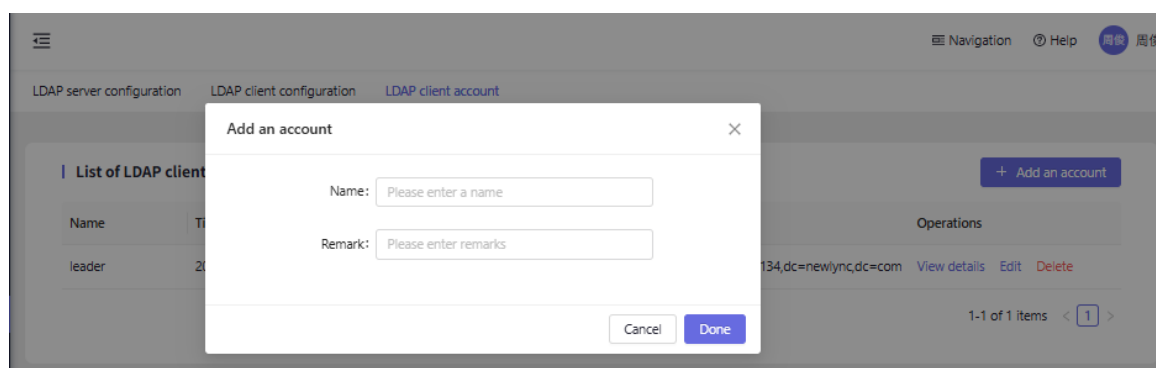
Step 1. Go to the NewLync administration backend and click Organizational Structure > LDAP.

Step 2. Click the LDAP Client Account tab and click + Add Account.



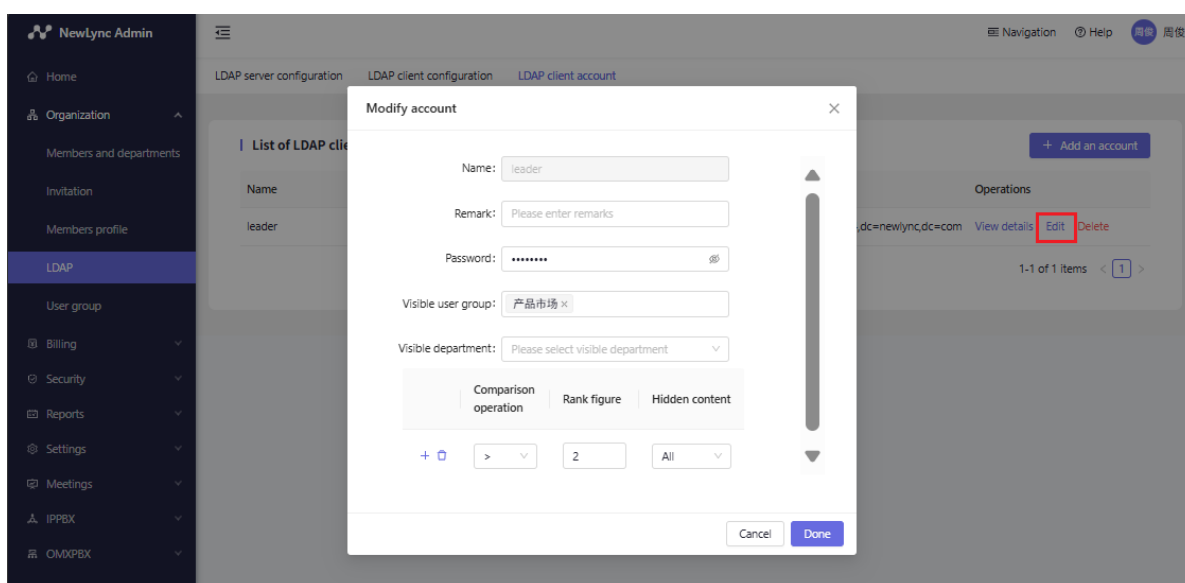
LDAP Client Account Configuration Screen

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



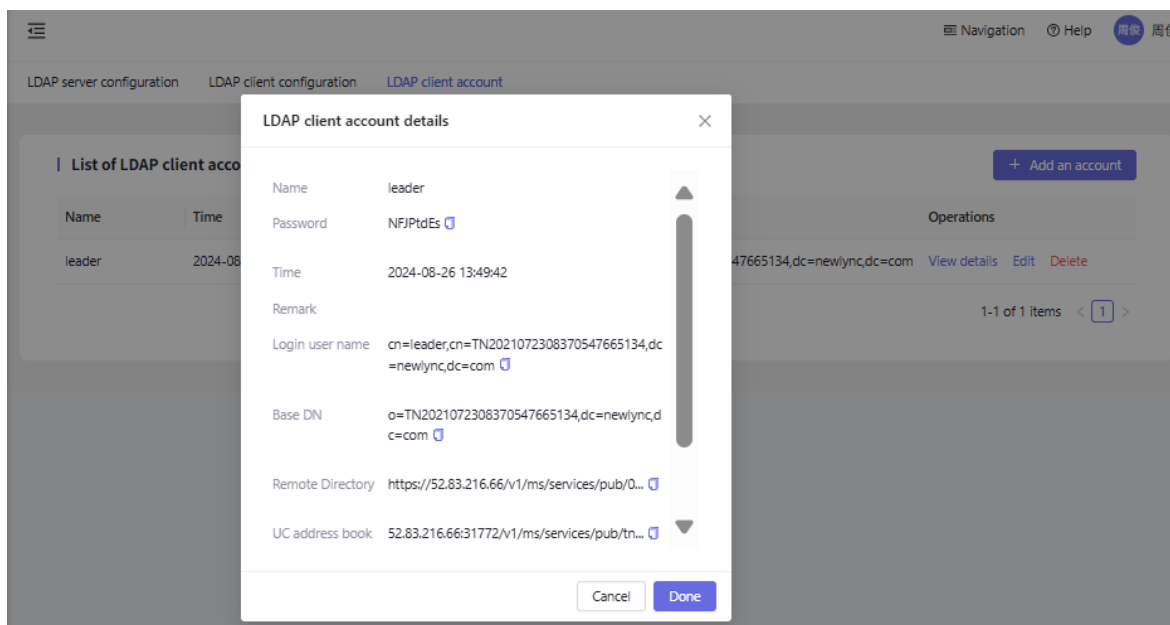
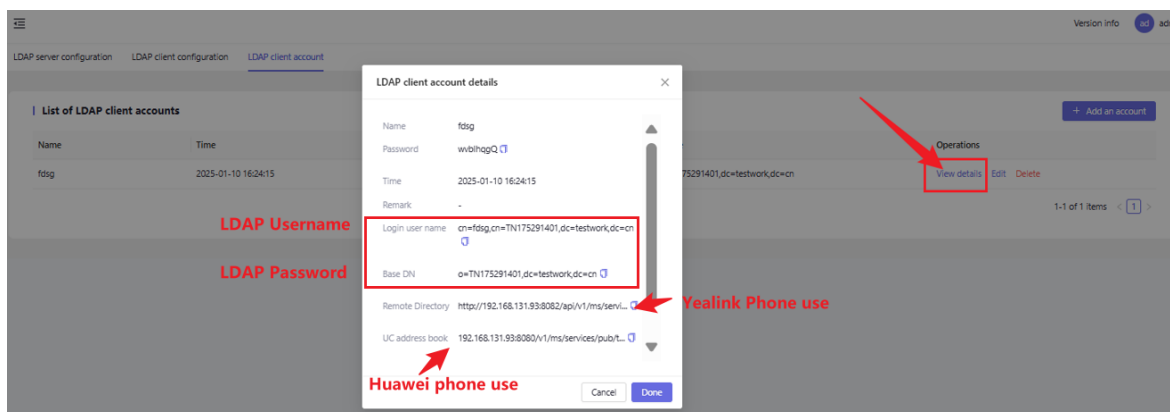
Add Account

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



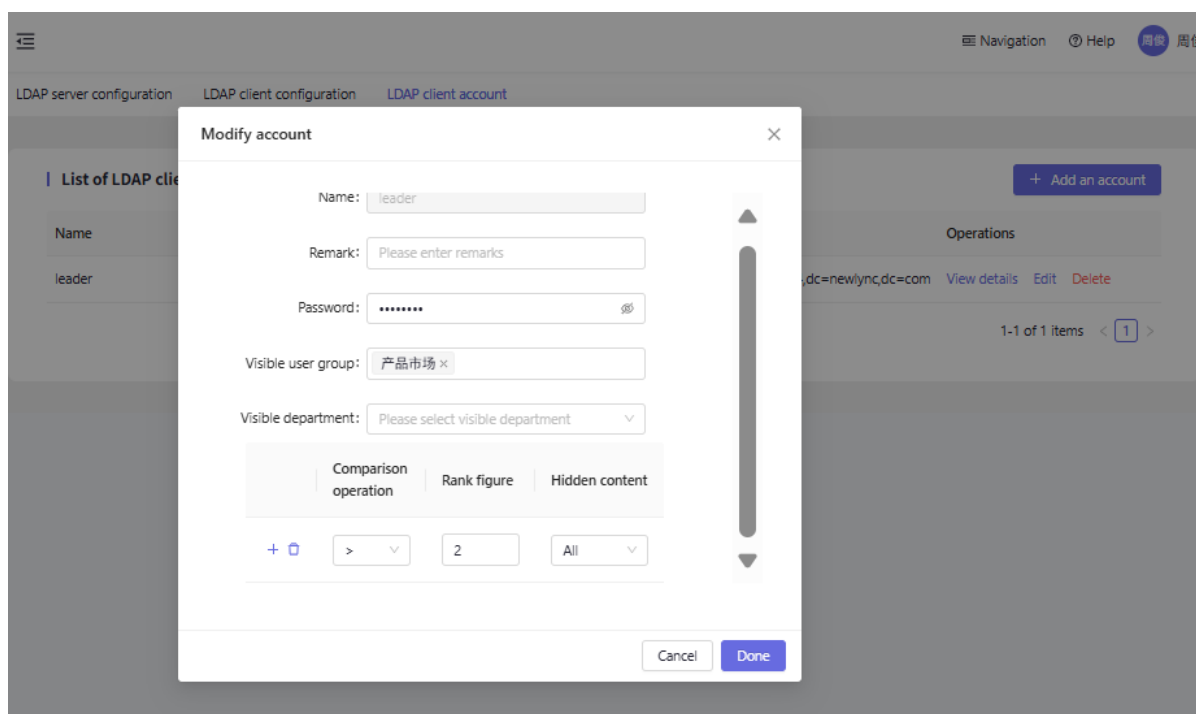
Modify the LDAP account

Step 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.



Edit LADP account

Step 6. Click Edit LDAP Account to modify the account information.



Edit LDAP Account Screen

Item	Define
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 Department	Sets the range of departments that can be viewed by this user or department.

Editing the LDAP Account Interface Definition

Comparison operation

The "Comparison Operation" function flexibly controls the visibility of contacts between users of different ranks by combining the "Rank Number" field with conditions such as greater than, less than or equal to.

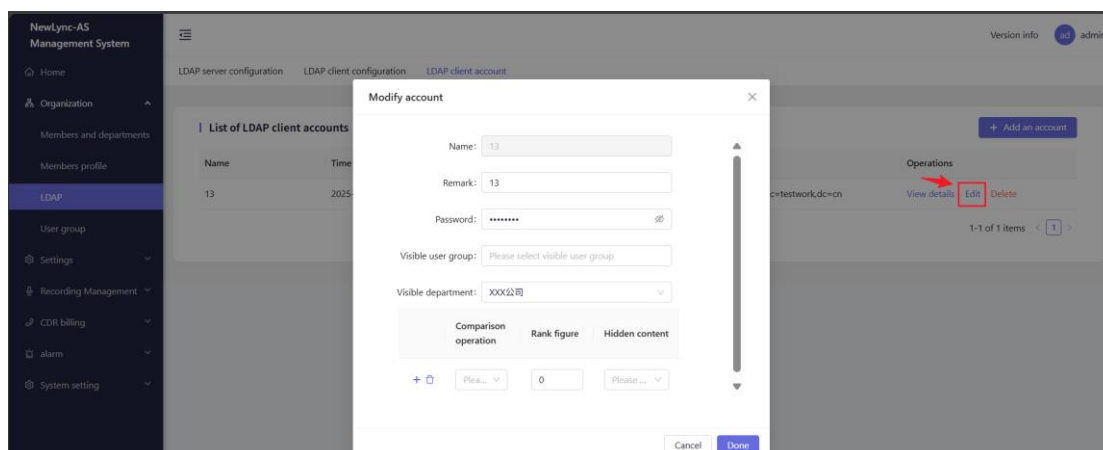
Item	Define
More than	Allows display of information only for users with a higher rank than the specified rank.
Less than	Allows display of information only for users who are lower than the specified rank.
Be tantamount to	Allows only user information with the same rank as specified to be displayed.
Grade figures	The value of the user's or department's rank.
Hidden content	Specify the type of content to be hidden in Address Book, support to hide all information, only hide cell phone/extension number.

Comparison Operation Definition

7.3.5 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.



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

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.

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.



Note

Job levels and visible user groups cannot be used simultaneously.

7.3.6 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.

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

After logging in, navigate to **Contacts > Cloud Contacts**.

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 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 9.3.4: Creating LDAP Accounts .
Password	Enter the password required for LDAP authentication, See Section 9.3.4: Creating LDAP Accounts .
Search Base	Set the starting directory path for LDAP queries, See Section 9.3.4: 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.
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.

Configure LDAP Parameters for Fanvil Phones

8.3.6.2 Yealink Phone

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

Yealink T31W

These users (user) are using the default password, please change the password!

English (English)

Log Out

Status Account Network Dsskey Features Settings Directory Security

Local Directory

Remote Phone Book

Phone Call Info

Google Contacts

LDAP

Multicast IP

Settings

Index	Remote URL	Display Name
1	http://52.83.216.66:31772/	Remote address book
2		
3		
4		
5		

Incoming/Outgoing Call Lookup: Enabled

Update Time Interval (Seconds): 600

Confirm Cancel

NOTE

Remote Phone Book
It is a centrally maintained phone book, stored in the remote server.

Users only need the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the phone book, and then display the remote phone book entries on the phone user interface.

Click here to get more product documents.

Configure LDAP Parameters for Yealink Phones

Item	Definition
Remote URL	Configure the remote URL address for the LDAP server, See Section 9.3.4: 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.
------------------------------	--

Configure LDAP Parameters for Yealink Phones

8.3.6.3 HuaWei Phone

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

Server

Port (0~65535)

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 9.3.4: Creating LDAP Accounts .
Port	Configure the port number for the address book server, within the range of 0 to 65535.

Configure LDAP Parameters for HuaWei Phones

7.3.7 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.



NRP Phone Contact Search Interface

7.4 Cost Center

7.4.1 Value-added services and packages

Navigate to the cost center, in this interface you can select the appropriate package, we provide you with flexible payment plans, at a fair price to provide high-quality products and services.

	Trial version	Basic Edition	Professional Edition	Custom Edition
021-61202700	Free trial for 3 months	Small teams of less than 50 people	Small and medium enterprises	Customized according to the enterprise demand
Team accounts	30single	50single	100single	Buy on demand
Enterprise meeting Rooms	1 Fixed meeting room(10)	1 Fixed meeting room(10)	1 Fixed meeting room(25)	Buy on demand
Meeting duration	40 minutes	Unlimited time	Unlimited time	Unlimited time
Security meetings	4 participant	6 participant	6 participant	Buy on demand
OM	None	1 OM-License (50)	1 OM-License (80E)	Buy on demand
Instant messaging	✓	✓	✓	✓
Audio and video call	✓	✓	✓	✓
Address book	✓	✓	✓	✓
Meeting management	✓	✓	✓	✓

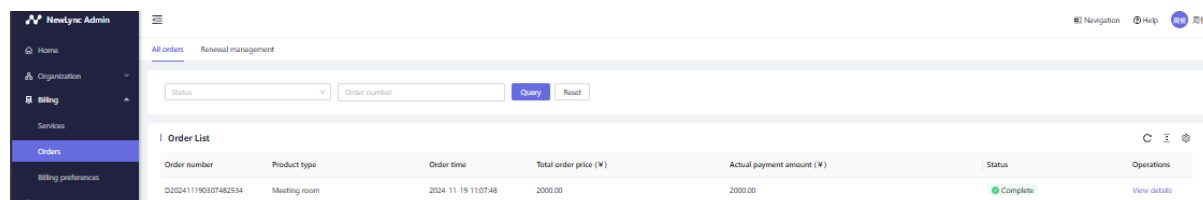
| Value-added services

[Renew](#)

	Account Each team can enjoy 30 team accounts for free trial version. If the account is insufficient, you can purchase more accounts. When a single purchase is more than 200 people, it will get some discount. Current 1000, accounts, remaining 854 available View detailed data Buy now
	OM devices Connecting to OM devices, NewLync app can call OM's extension or make outbound PSTN calls via OM, NewLync app also can be as the mobile extension for OM. 16 OM devices are currently connected View detailed data Apply for trial Buy now
	Enterprise meeting rooms Each team has a 10-participants instant meeting room, and enterprise meeting rooms can be purchased according to the needs of the team. Currently has 16 enterprise meeting rooms View detailed data Apply for trial Buy now
	Security meeting Trial customers default to 4 max participants, and paid customers default to 6 max participants. The number of max participants can be increased according to the needs of the team. Currently 8 max participants View detailed data Buy now
	Number of user access devices The account under the trial team is allowed to access max 3 devices for free, and the account under the paid team is allowed to access max 4 devices for free. The number of access devices can be purchased according to the needs of the team. Purchase additional 1500 access devices, remaining 667 available View detailed data Buy now
	Deployment service Deployment service provides product introduction and demonstrations, solution consulting, install and deploy service in your private servers. One-time free online deployment, please contact customer service for free online deployment. Buy now
	product.addserver.ai product.addserver.ai.tip product.addserver.ai.close View detailed data Buy now
	OMX NewLync+OMX converged communication platform, no need to purchase physical equipment Buy now

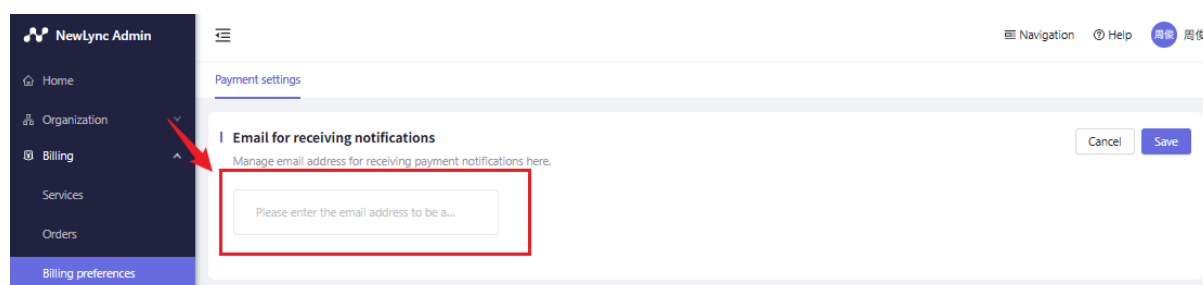
7.4.2 Order Management

Navigate to Order Management where you can check all your orders and pending renewal orders.



7.4.3 Account Management

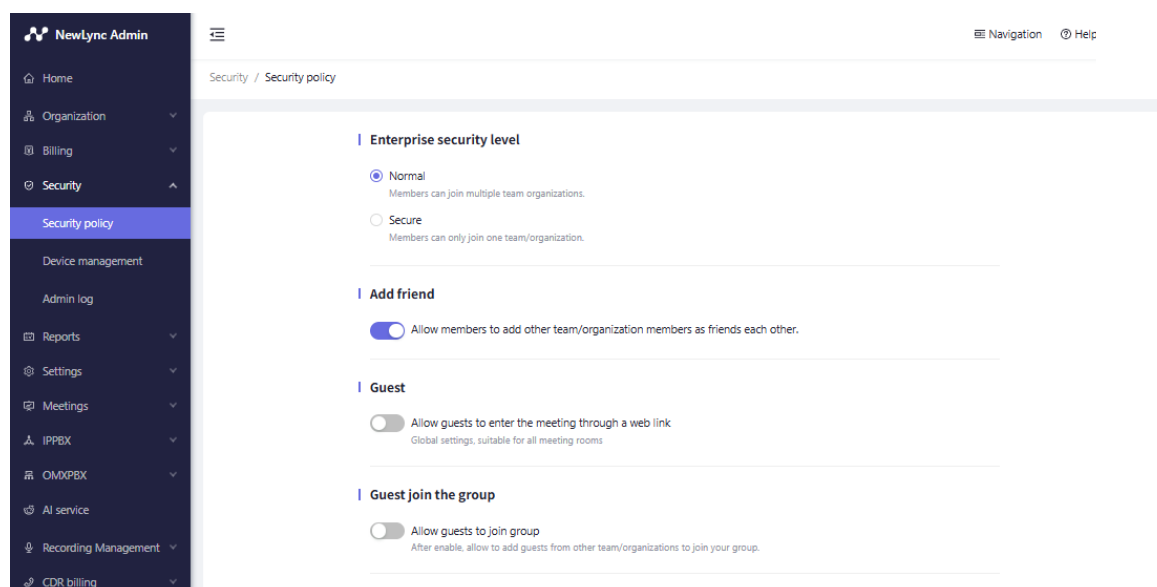
Navigate to Order Management > Billing preferences, where you can manage the email address to receive payment notifications.



7.5 Security

7.5.1 Security policy

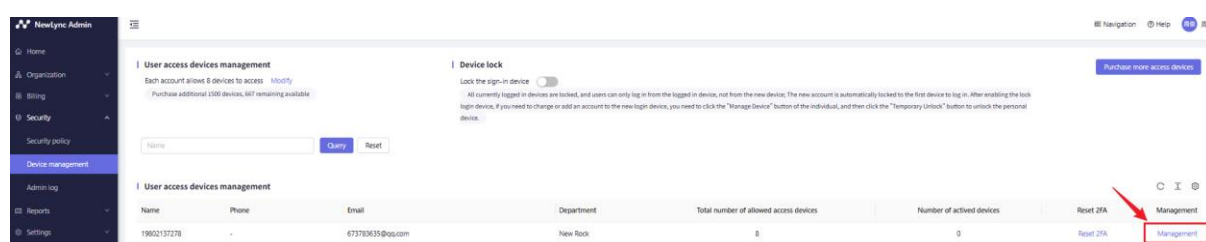
Go to the NewLync admin backend and click Security > Security Policies. This page allows you to configure various enterprise security policies.



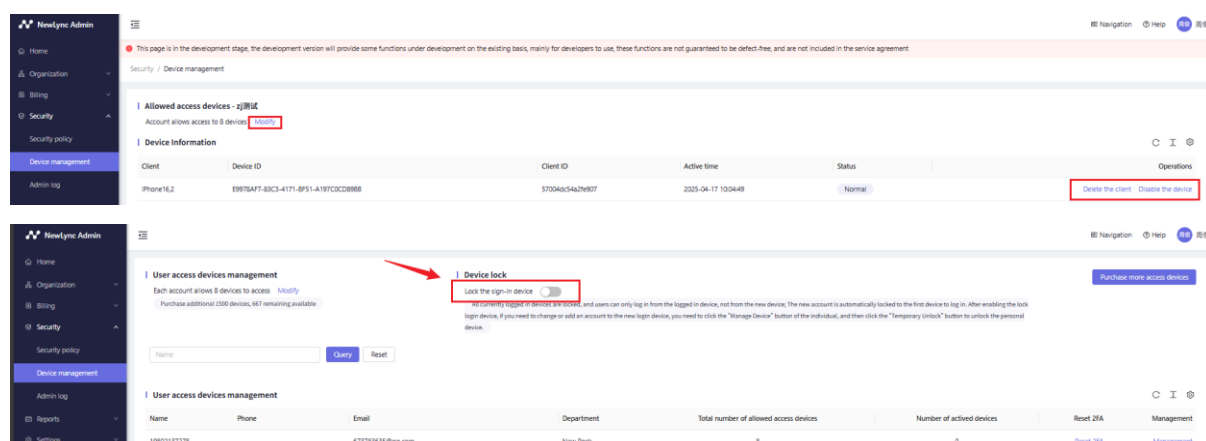
7.5.2 Equipment management

NewLync supports multiple endpoints, one account can log in to both desktop and mobile apps, or log in to multiple desktops or mobiles at the same time. In the device management page you can modify the number of terminals, delete terminals, disable terminals and lock devices.

Enter NewLync management background, click Security->Device Terminal, and then click Device Management to modify the number of terminals, delete terminals and disable terminals.

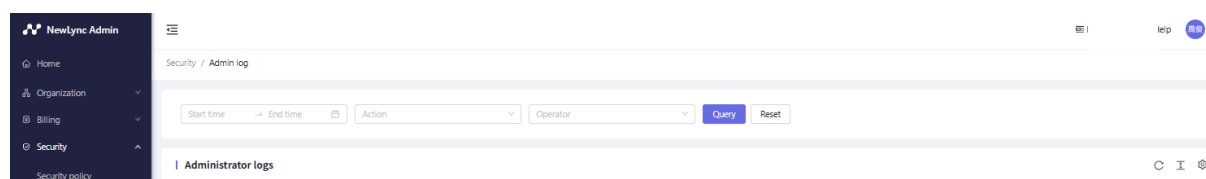


Click to turn on Locked Login Devices. Users can only log in from the device they are already logged in to, and cannot log in from a new device.



7.5.3 Administrator log

Enter the NewLync administration backend, click Security->Administrator Log. This page allows you to view the administrator operation log, which can be filtered by operation date and operation type.



7.6 Data Sheet

7.6.1 Equity data

Go to the NewLync admin backend and click Data Reports->Data Equity. This page allows you to view all the interests of the business and when they expire. Click Purchase in the upper right hand corner to purchase an entitlement, or contact our technical staff to assist you in extending your entitlement.

The screenshot displays the NewLync Admin interface. On the left, a dark sidebar contains a navigation menu with 'My equity' highlighted. The main content area shows four sections, each with a table of product types, counts, and expiration dates.

Account

Product type	Count	Expiration
Account	1000	2124-07-31 08:00:00

IPPBX (OM Licenses)

Product type	Count	Expiration
OM20G-NL	1	2025-12-31 08:00:00
OM20G-NL	1	2025-12-31 08:00:00
OM20G-NL	1	2025-12-31 08:00:00

Enterprise meeting rooms

Product type	Count	Expiration
Enterprise meeting room with max 10 participants	1	2025-07-31 08:00:00
Enterprise meeting room with max 25 participants	1	2024-07-29 08:00:00
Enterprise meeting room with max 10 participants	1	2024-10-13 08:00:00

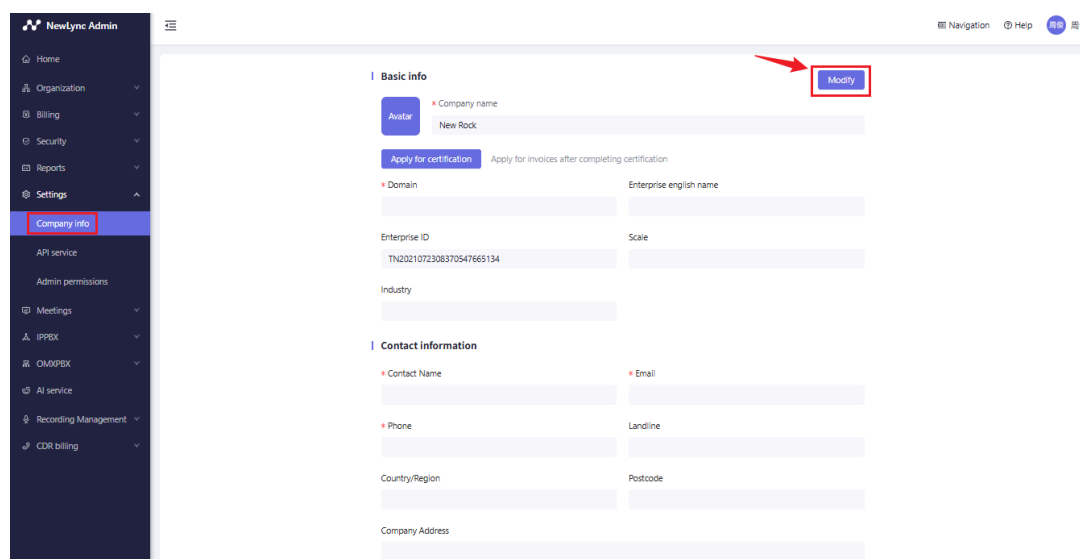
Security meeting

Product type	Count	Expiration
8 participants Security Meeting	Unlimited	2124-07-31 08:00:00

7.7 Enterprise Settings

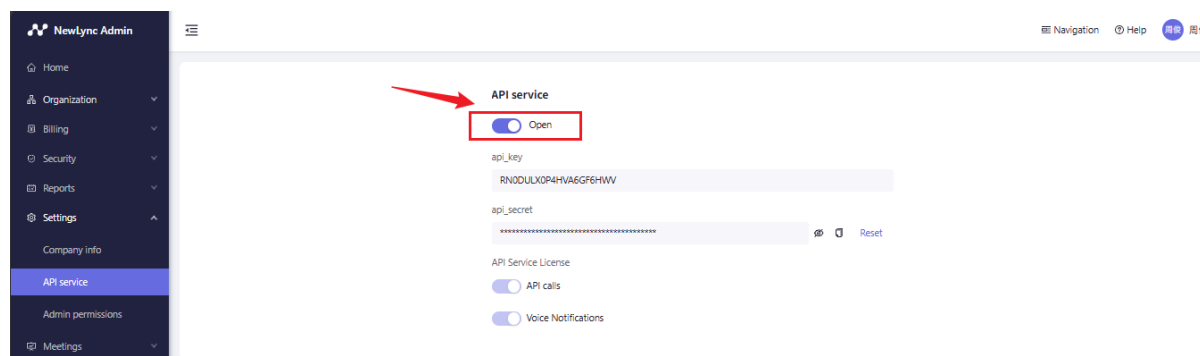
7.7.1 Corporate Information

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



7.7.2 API Services

Go to the NewLync admin backend and click Enterprise Settings->API Services to view the API service information. The API service is used to control cloud PBX calls, please contact New Rock support for details.



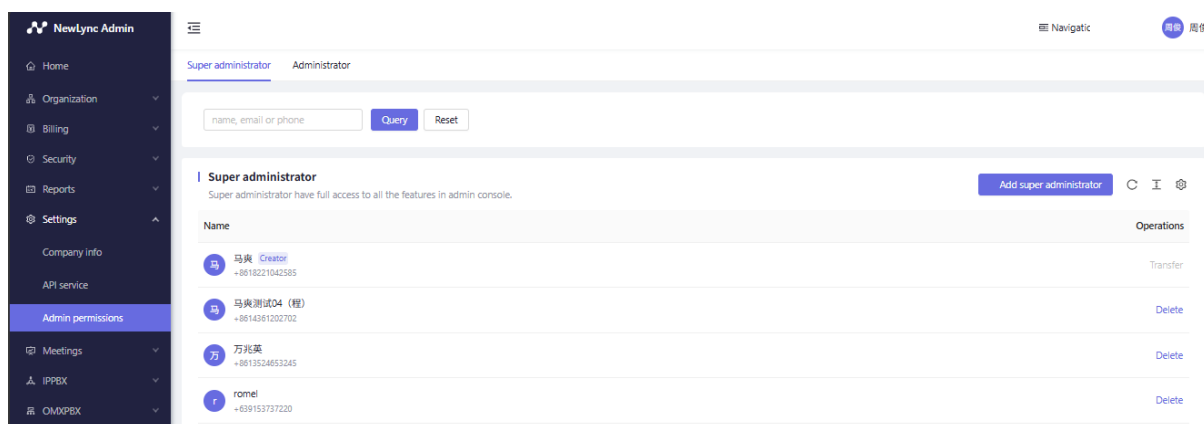
7.7.3 Administrative authority

There are three roles in the NewLync 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.

7.7.3.1 Transfer creator

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

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



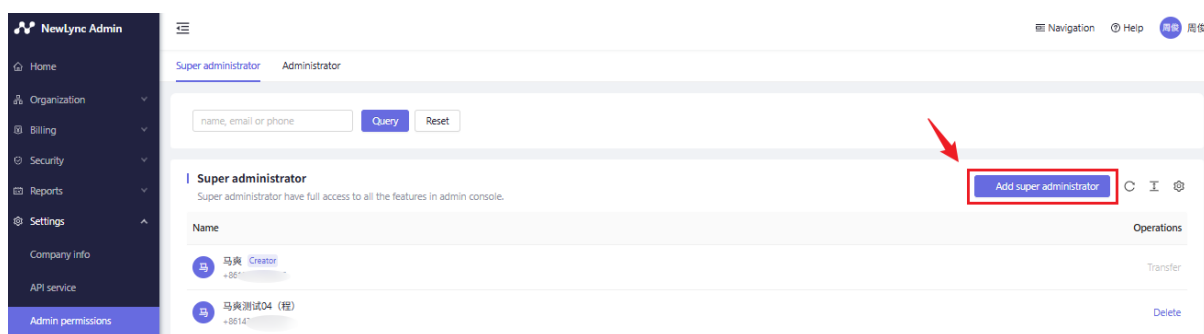
Step 3. Enter keywords in the pop-up window, search for the member you want to transfer to, and click Select.

Step 4. Click Submit to complete the transfer.

7.7.3.2 Add Super Administrator

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

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



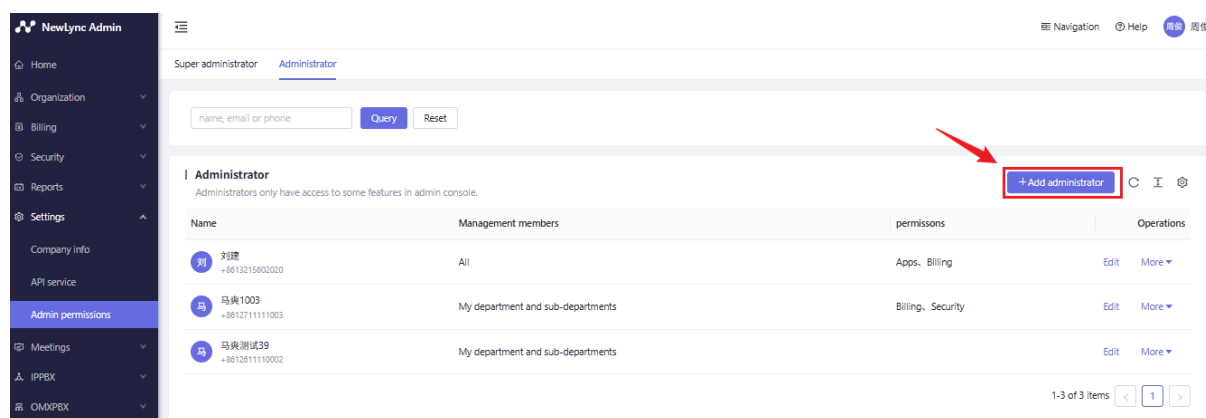
Step 3. Enter a keyword in the pop-up window, search for members, and then click Selected.

Step 4. Click Submit to complete the creation.

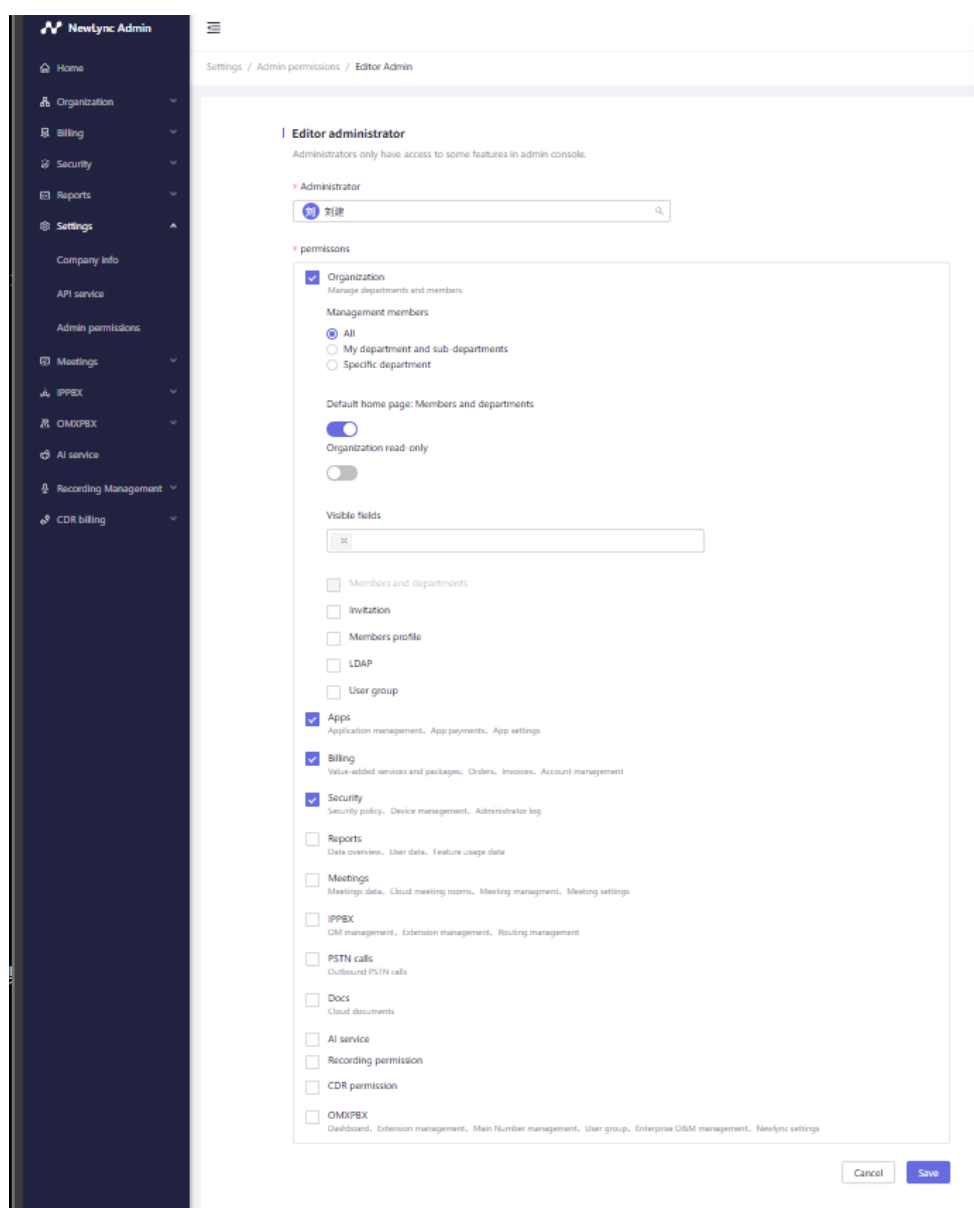
7.7.3.3 Add Administrator

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

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



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

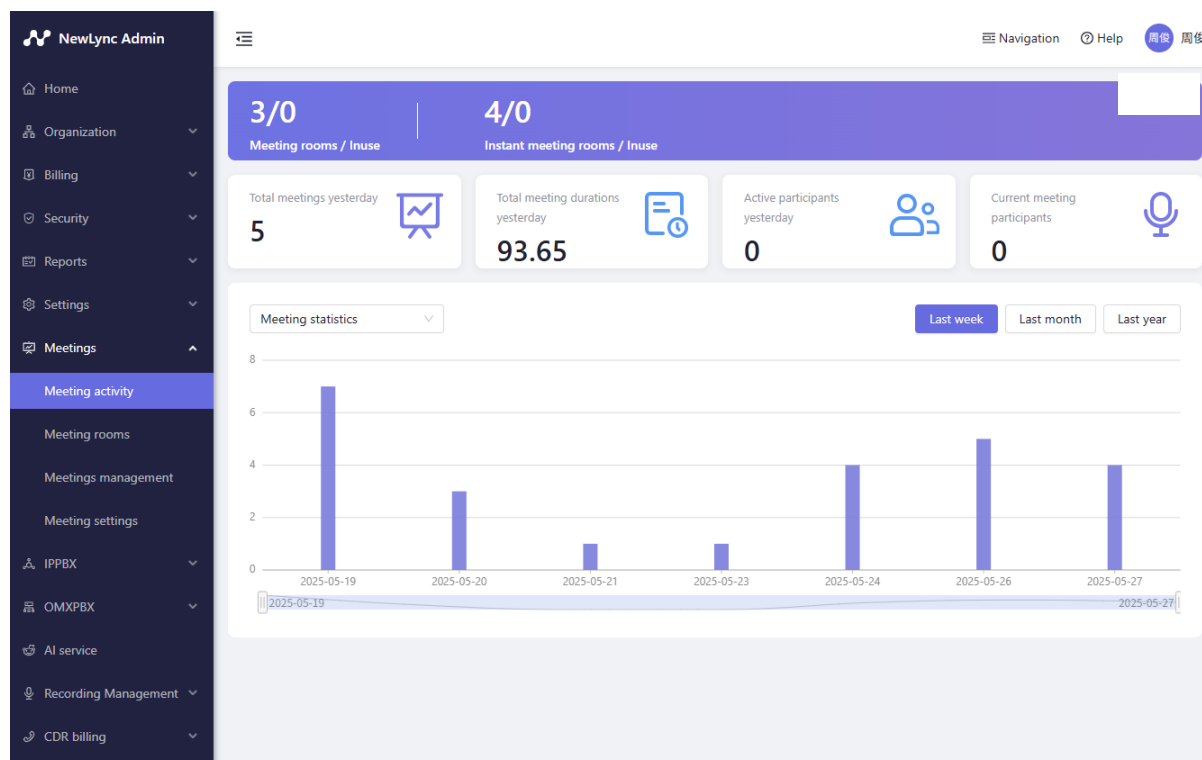


Step 4. Click Save to complete the addition.

7.8 Meetings Management

7.8.1 Meeting data

Go to the NewLync admin backend and click Meeting Management->Meeting Data . This page allows you to view conference room usage and conference room statistics. The slider below allows you to quickly filter the date range to count daily meetings, meeting length, and daily attendees.



7.8.2 Corporate meeting rooms

NewLync meeting rooms are categorized into corporate and instant meeting rooms. Meeting numbers for corporate meeting rooms are fixed and need to be purchased.

Step 1. Go to the NewLync admin backend and click Meeting Management -> Meeting Data .

All purchased corporate meeting rooms will be displayed on this page, if there are no available corporate meeting rooms, please contact a salesperson to purchase one.

Step 2. Click Details to view the meeting room password and host password, which is a random six-digit number that can be changed. Join the meeting at NewLync APP with the meeting number and room password, and become the host with the host password.

NewLync Admin

Home Organization Billing Security Reports Settings Meetings Meeting activity Meeting rooms Meetings management

Meetings / Meeting rooms

Room status Search meeting n... Query Reset

Enterprise meeting rooms Purchase Enable Disable

Meeting ID	Meeting room name	Start/Schedule meeting permissions	Room status	Meeting status	Max Participants	Expiration	Operations
9119444874	CEA会议		OK	Idle	25	2024-10-13	detail View Renewal
1622468652	Enterprise meeting room wi...	All	OK	Idle	10	2025-07-31	detail View Renewal

NewLync Admin

Home Organization Billing Security Reports Settings Meetings Meeting activity Meeting rooms Meetings management Meeting settings IPPBX OMPBX

Meetings / Meeting rooms / Room detail

Meeting room details Edit Disable Renewal

Meeting room status: OK

Meeting ID: 9119444874

Meeting room name: CEA会议

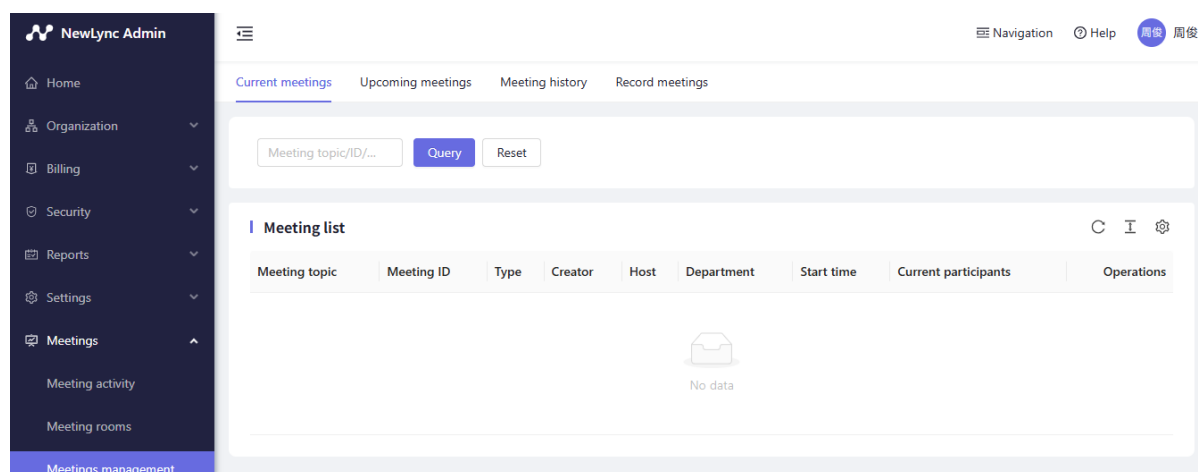
Timezone: (GMT+08:00) Shanghai

Start/Schedule meeting permissions: default、Jun Zhou测试号
Note: People without permissions cannot get host privileges

Meeting password: 888888

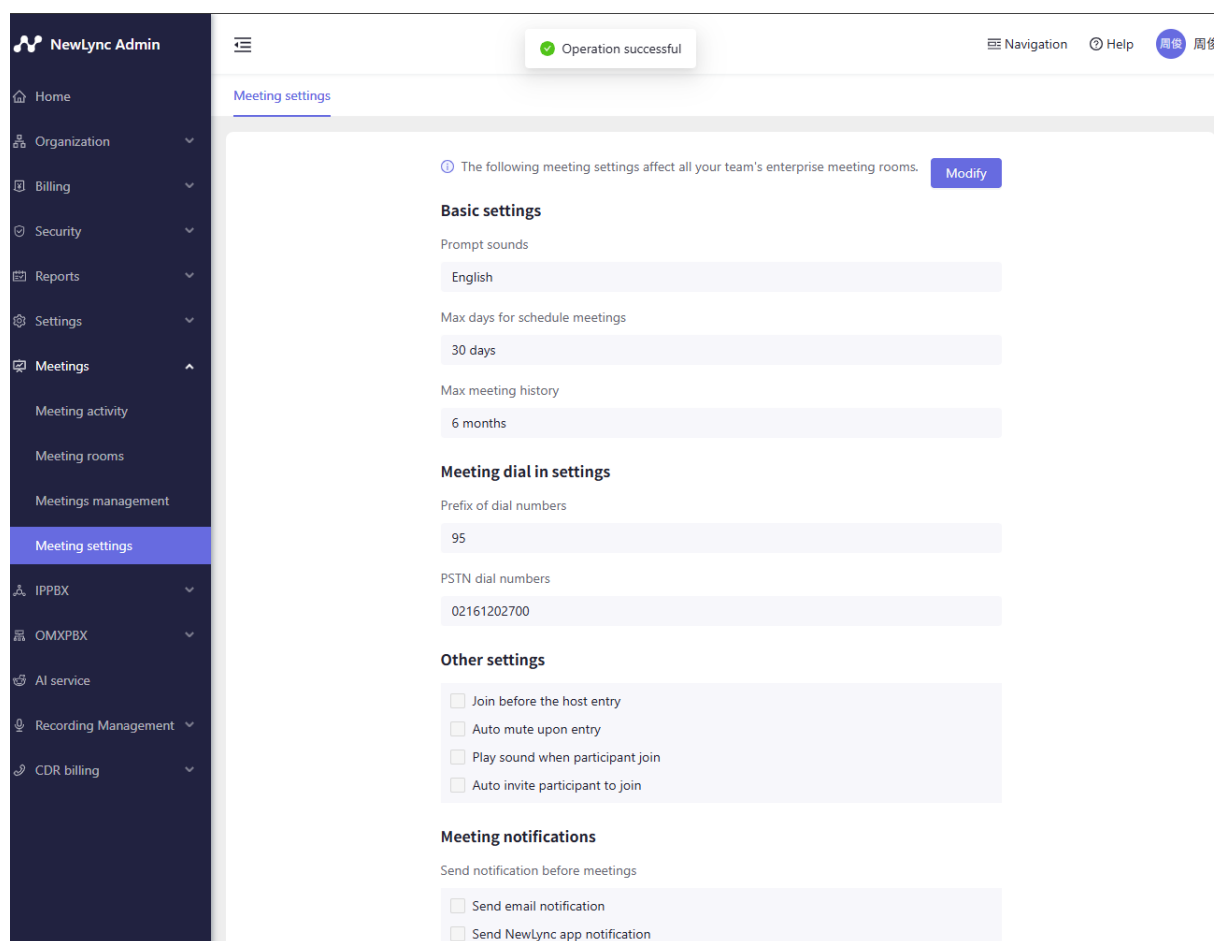
7.8.3 List of meetings

Go to the NewLync admin backend and click Meeting Management->Meeting List. This page allows you to view ongoing meetings, upcoming meetings, historical meetings, and meeting recording files. In the list of ongoing meetings, click Share to view the enrollment information in the pop-up window, copy it and share it to the same time by other means. Click End Meeting to force the meeting to end. The upcoming meeting is an appointment meeting, which is initiated on the NewLync APP.



7.8.4 Conference settings

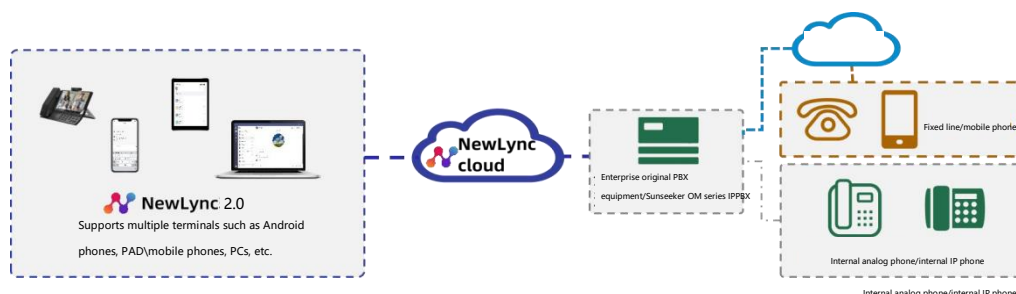
Go to the NewLync admin backend and click Meeting Management->Meeting Settings. Meeting settings are for all corporate meeting rooms under the organization and can be edited by clicking Modify in the upper right corner.



7.9 IPPBX Interconnect

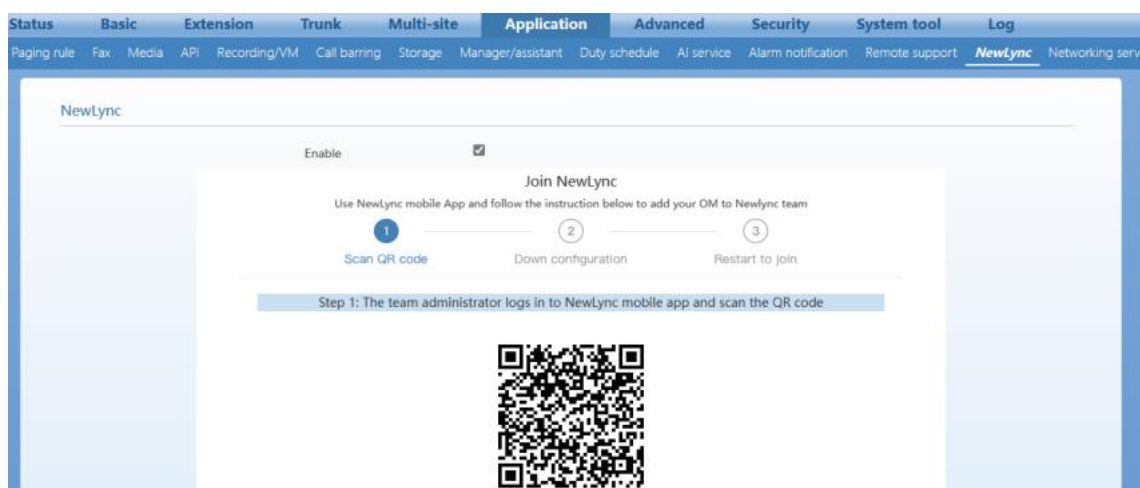
7.9.1 OM Management

After setting up the OM, you can make calls directly from the NewLync client, see the topology diagram below.

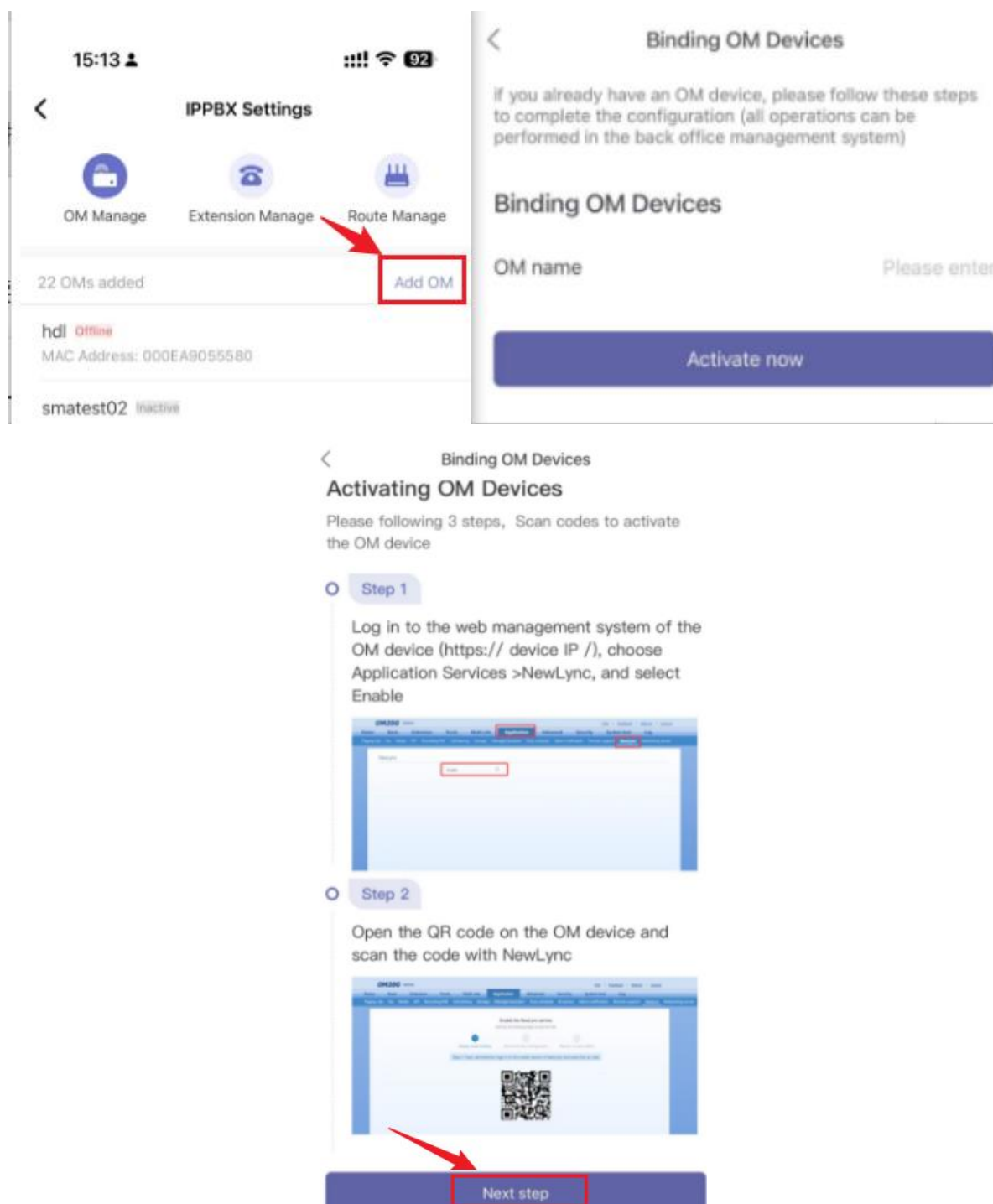


Adding OM devices

Step 1. Login to OM web management system, go to Application -> Cloud Co-working Service page, check Enable.



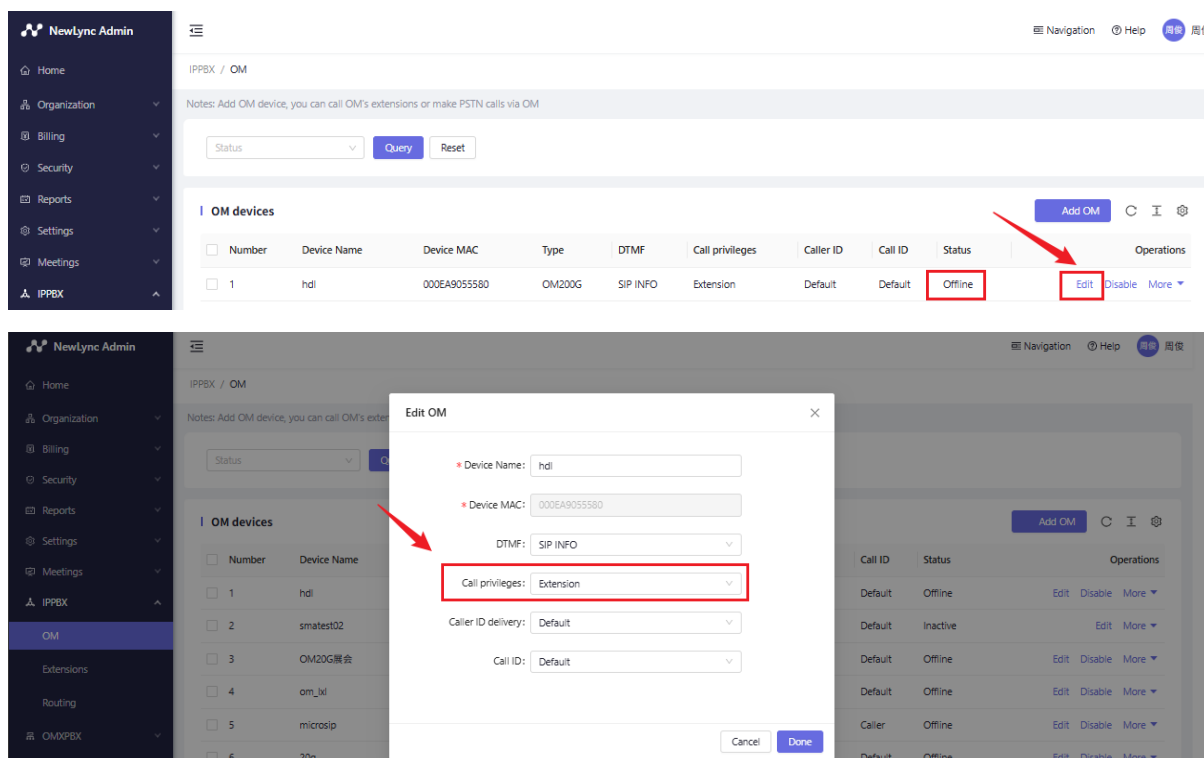
Step 2. The team administrator opens the NewLync mobile app, navigates to Settings->IPPBX Interconnect, clicks Add OM, enters the OM name, and then scans the code. To activate OM, scan the QR code in the previous step and follow the instructions to complete the addition.



Step 3. Click Finish on the Cloud Collaboration Services page, and then reboot the device. After the reboot is complete, the OM shows that it is registered, indicating that it was added successfully.

Configuring OM devices

Go to the NewLync management backend and click IPPBX Interconnection->OM Management. After successfully adding the OM, the OM status is online. Click Edit to configure OM, DTMF optional RFC2833 and SIPINFO, outbound authority defaults to extension, can only dial numbers up to 6 digits, change it to outbound to dial numbers above 6 digits.

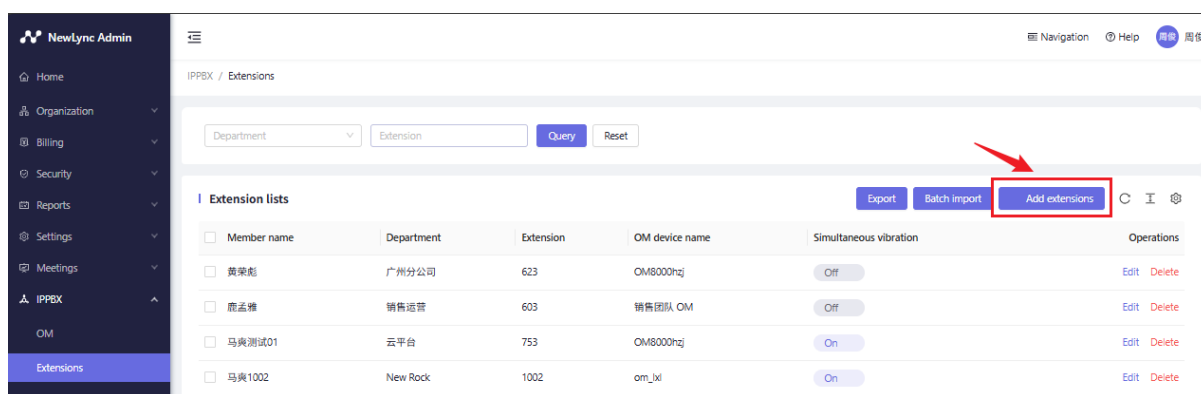


7.9.2 Extension management

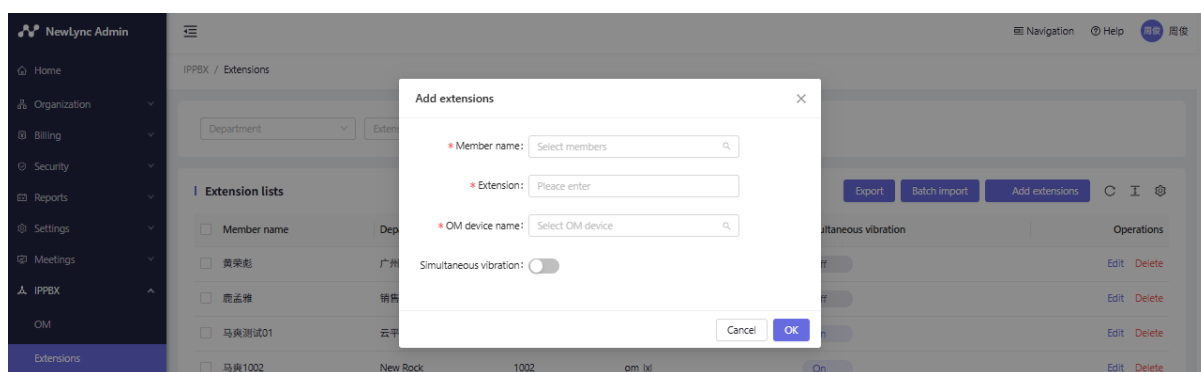
The extension here corresponds to the extension of OM, and after binding with the NewLync account, NewLync can make calls through the OM outside line, and can also call into the NewLync terminal through the same vibration.

Add Extension

Step 1. Go to NewLync management background, click IPPBX Interconnection->Extension Management, click +Add Extension.



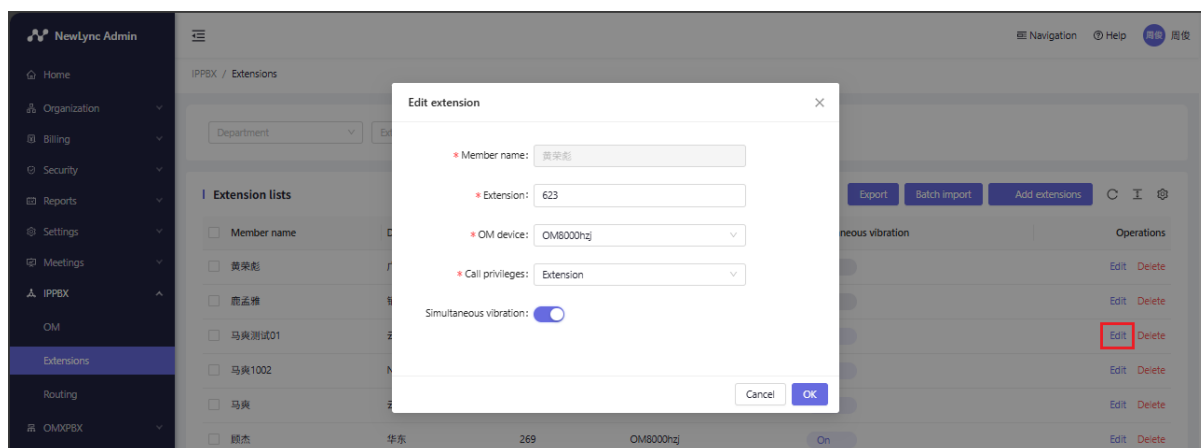
Step 2. Select NewLync user in the pop-up window, enter the OM corresponding extension number, select the corresponding OM, and turn on the same vibration.



Step 3. Click OK and the addition is complete.

Configuring extensions

Click Edit on the page to modify the extension binding information.



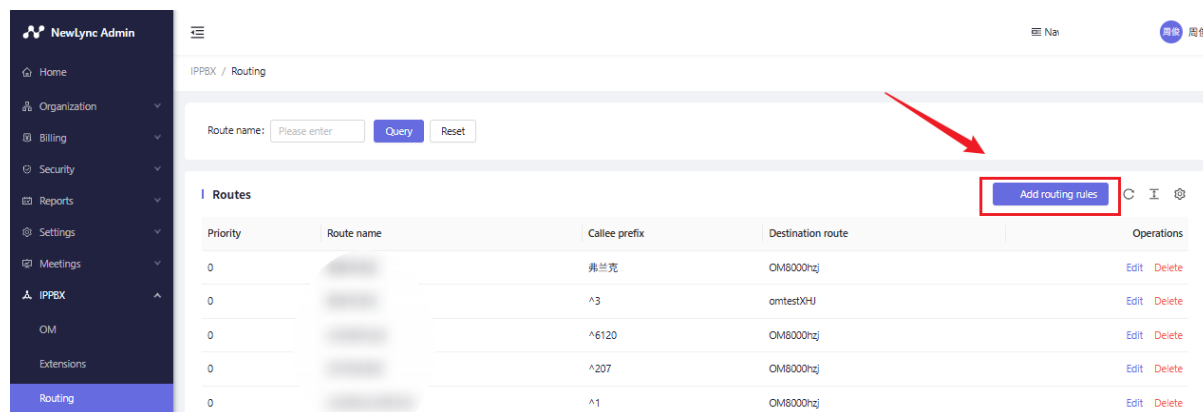
7.9.3 Routing management

NewLync supports adding multiple OMs, and calls are matched to OMs that are not available based on routing rules. The system automatically creates a default route pointing to the first

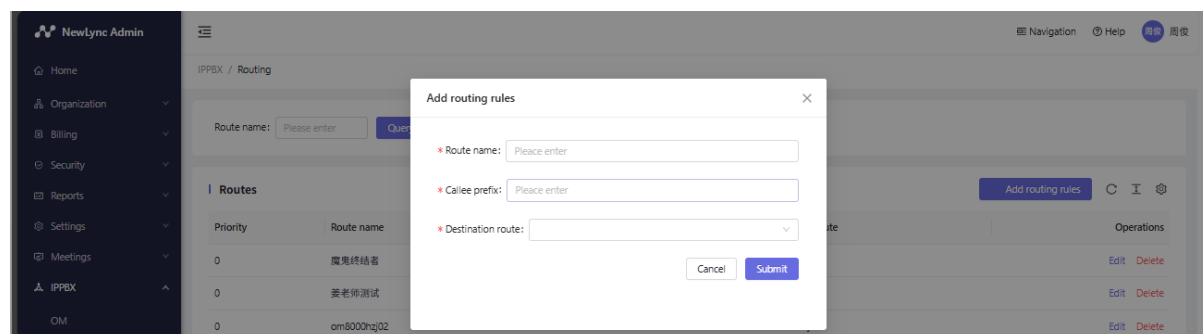
OM when you add it.

Add Route

Step 1. Go to the NewLync management background, click IPPBX Interconnection -> Routing Management, and click+ Add Routing Rule.



Step 2. Enter the route name, number prefix, and destination address in the pop-up window. The destination address is selected from the OMs that have been added.



Examples of common routing rules:

To match a specific number, such as 709, enter the prefix ^709\$ in front of the number in the rule;

Matches numbers starting with 7, prefixed with ^7 in the rule;

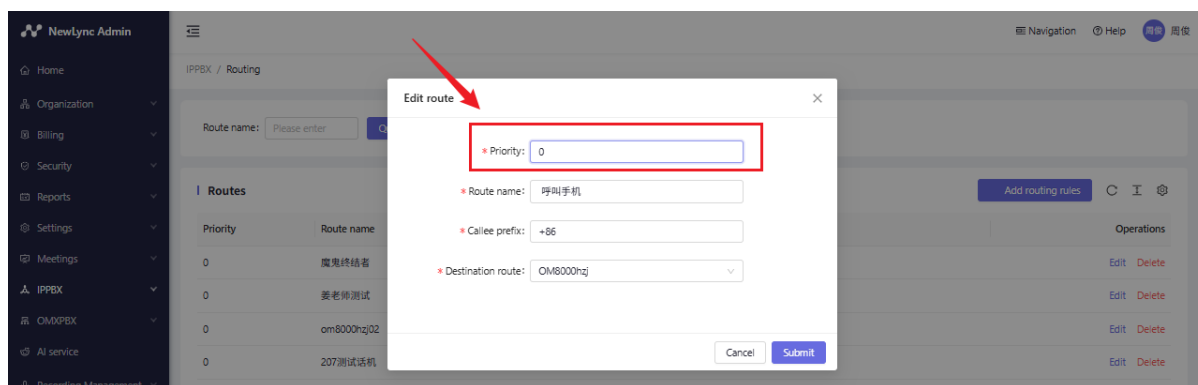
Matches 5-digit numbers starting with 7. The prefix in the rule is ^7[0-9]{4};

Matches 6- to 10-digit numbers starting with 76, prefixed in the rule as ^76[0-9]{4,8}.

Step 3. Click Submit to complete the addition.

Edit Route

Click Edit to modify the routing. Routing priority is a natural number, with 0 having the highest priority and larger numbers having lower priority.



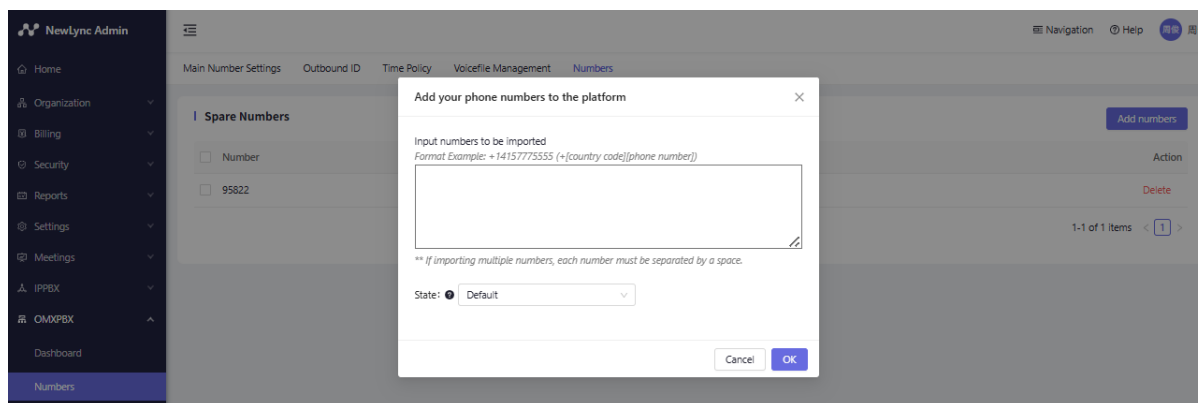
7.10 Cloud PBX Services

7.10.1 Centralized administration

7.10.1.1 Outbound Configuration

Adding a trunk number

Add a trunk number for assigning the number to a subscriber or switchboard or IVR in Cloud PBX Services > Trunk Numbers.

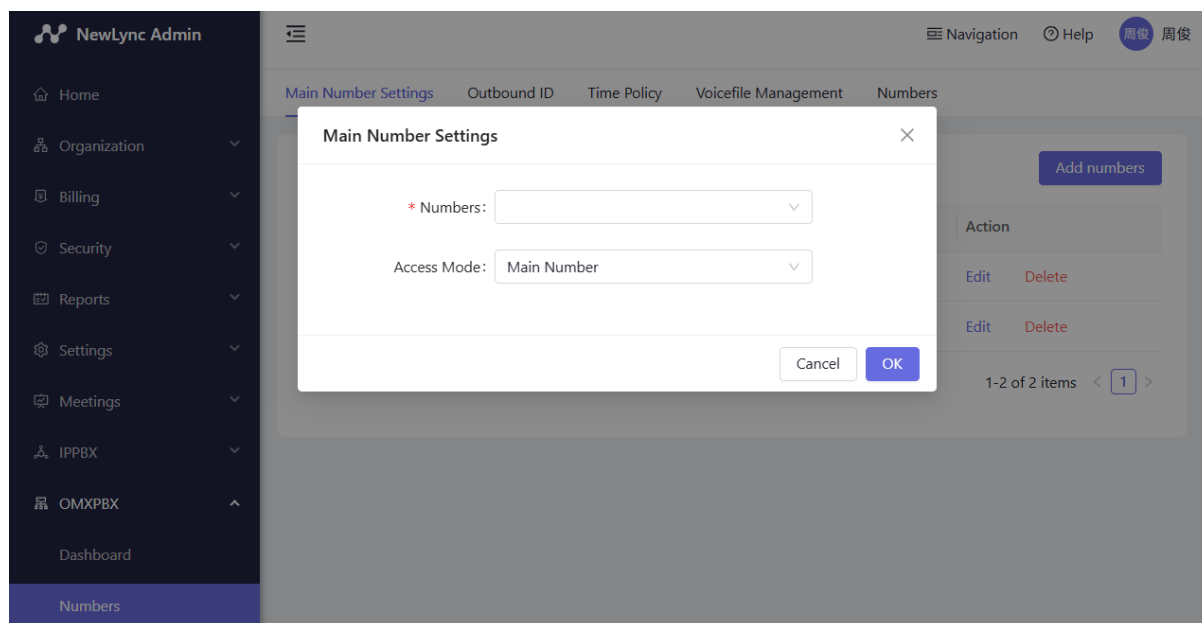


Add a switchboard number

Add the switchboard number in Cloud PBX Service->Switchboard Setup Number to assign a trunk number to the switchboard.

Inbound: Through this number you can call into the switchboard IVR and then dial the extension number to the corresponding user.

Outgoing: You can take this number as the outgoing call display number.



Adding an Outside Line Trunk

Add trunks in Cloud PBX Services > Trunks & Routing > Trunks.

Add Gateway

1) When not registering, authenticate via IP, peer-to-peer, the authentication domain is written as the IP of the gateway server, and the user name and password are filled in randomly;

2) When the gateway needs to be registered, enter the correct account and password, and then check Register to server in Advanced; when IMS support is needed, you need to check IMS support in Advanced;

Completion of relay additions

The screenshot shows the 'Creating a trunk' dialog box in the NewLync Admin interface. The dialog has a sidebar on the left with navigation links: Home, Organization, Billing, Security, Reports, Settings, Meetings, IPPBX, and OMXPBX. The main area contains the following fields:

- Name this Trunk:** A text input field with the placeholder 'Please enter'.
- Replace CallerID:** A text input field.
- Trunk Type:** A dropdown menu with 'Normal' selected.
- Gateways Strategy:** A dropdown menu with 'Sequential' selected.

Below these fields is a section titled 'Selected Gateways' which contains a table with the following headers: Gateway Server, Port, Authentication Username, and More. The table is currently empty, displaying 'No data' with a folder icon. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Adding call-out routes

Add an outbound route in Cloud PBX Services > Trunking & Routing > Outbound Routing.

The screenshot shows the 'Creating a route' dialog box in the NewLync Admin interface. The dialog has a sidebar on the left with navigation links: Home, Organization, Billing, Security, Reports, Settings, Meetings, IPPBX, and OMXPBX. The main area contains the following fields:

- Route Name:** A text input field.
- Prefix Number:** A text input field.
- Dod Route:** A dropdown menu with 'No' selected.
- Dialed Digits Length:** A dropdown menu with 'Not Care' selected.
- Prefix Remove Length:** A text input field with '0' entered.
- Prefix Add String:** A text input field.
- Caller Method:** A dropdown menu with '-None-' selected.
- Caller Id:** A dropdown menu with 'External' selected.
- Target Trunks:** A dropdown menu with '旺旺测试' selected.

At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Parameter description

Item	Define
Prefix number	Add different prefix numbers according to different relay gateways; for example, numbers beginning with 9 go to A relay, numbers beginning with 8 go to B relay
Match dialing length	For example, if you fill in 5, the length of the outgoing number is 5, you will go to this trunk
Delete prefix bits	Delete how many digits before the broadcasting number, generally used in conjunction with the prefix number; for example, dial 9 to go out to A trunk, but can't bring 9 when calling out, then fill in 1, delete the first 1 digit
Add prefix number	Called to add prefix content when dialing out; if there is both a deletion and an addition, the deletion is followed by an addition
Matching caller	1) "None" is defined as any calling number; 2) Match the caller number, then match this caller number to use this outgoing route; 3) Match the outbound grouping. You need to add a group to the outbound group; place multiple user extensions in this group; and use this outbound grouping when whenever a user in this group calls out;
Calling number selection	1) Subscriber Outside Number: It refers to the DID phone number of the subscriber (you need to turn on the Caller ID number in the subscriber function of the user interface; if Caller ID is not turned on or there is no DID, the switchboard number will be used, or if there is no DID, the extension number will be used); 2) Unified Outgoing Number: All users matched to the outgoing caller number are using the filled in this number; 3) Intercom number: When calling out, use this user's

	extension number;
Target relay	Which trunk will be used to route this outgoing call; multiple trunks are possible

7.10.1.2 Outbound Inbound Configuration

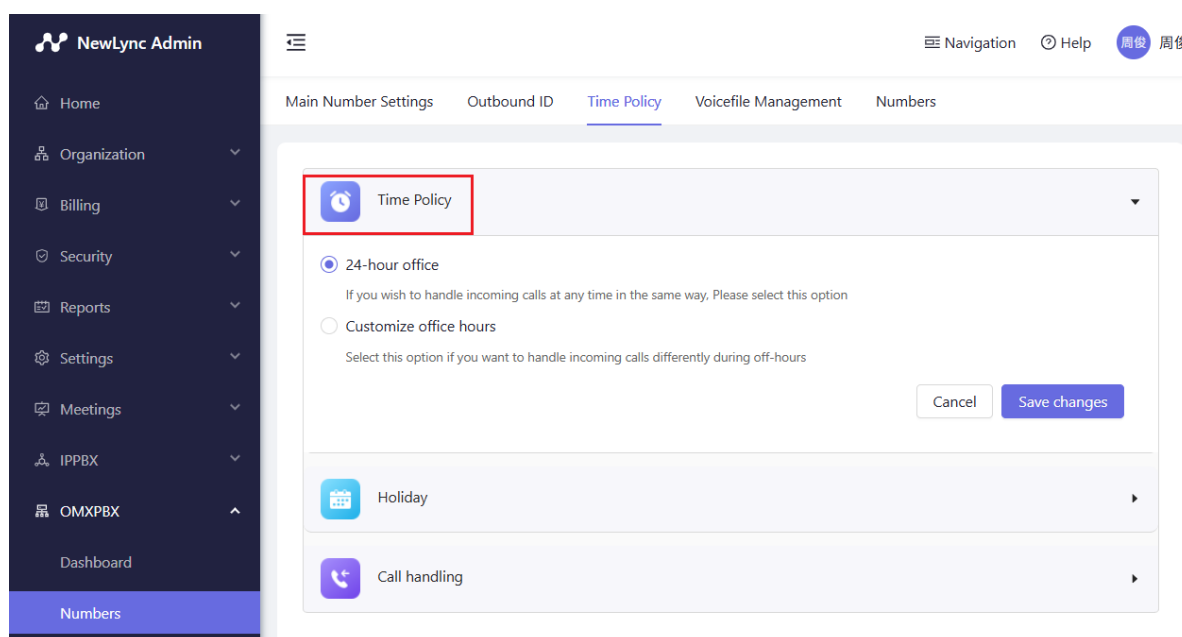
The way you can call into a cloud PBX

- 1) By dialing the switchboard number or IVR number and then dialing the corresponding extension number.
- 2) Dial the user's DID number.

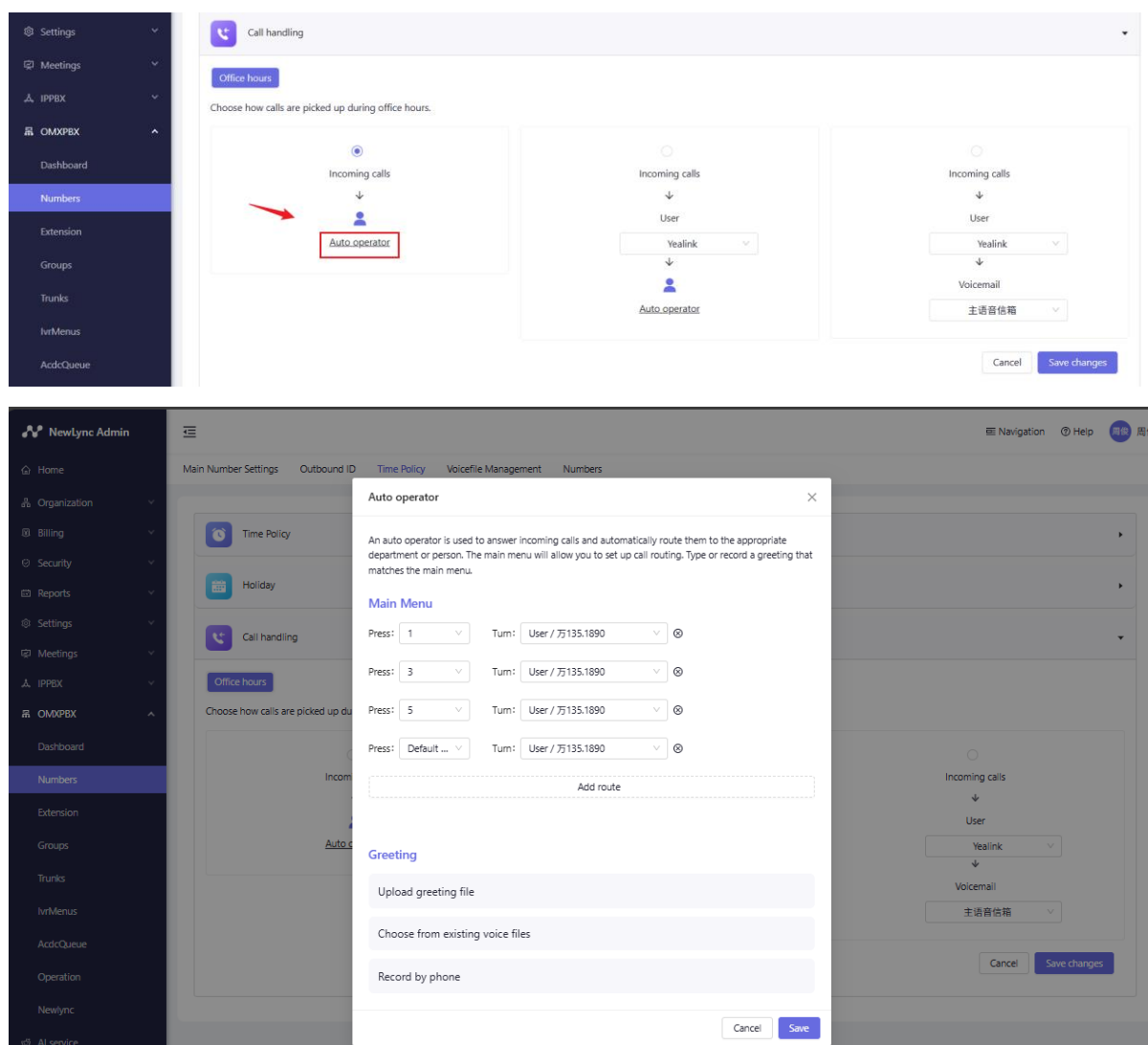
Step one. Configure the time policy

Configure time policies in Cloud PBX Services > Switchboard Management->Time Policies.

You can choose 24-hour office or customized office hours; you can realize, for example, office hours from 9 to 18, and off-duty hours beyond that, corresponding to different IVRs and playing different media.

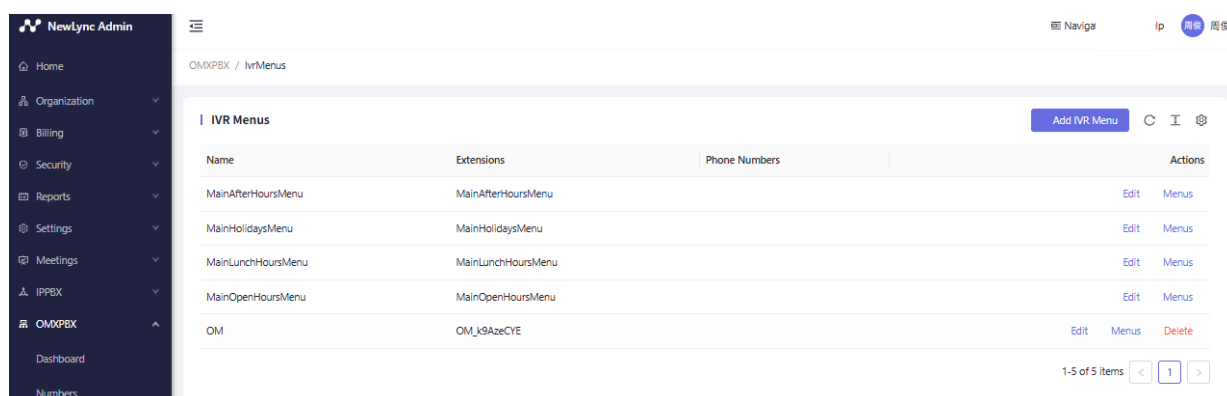


Configure call handling, select office hours, edit auto attendant, upload voice files, configure menu routing, and configure pressing numeric keys to go to different users. If the off-hours policy is customized to appear as an automated attendant during off-hours, you can upload voice prompts or configure menu routing.



Step 2. Configure IVR, configure IVR in the Cloud PBX Service->IVR Voice menu.

The four at the beginning of Main are IVRs for different time slots at the switchboard, followed by customized IVRs.



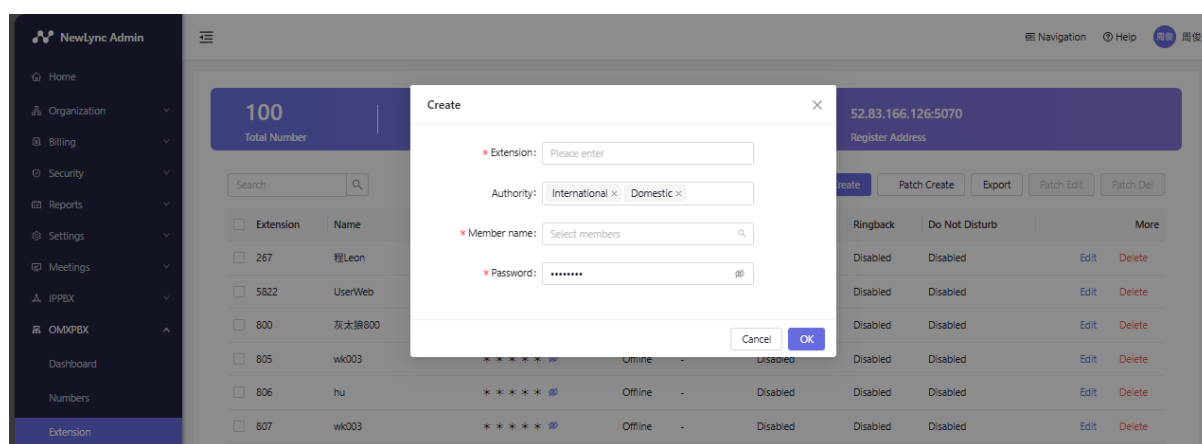
7.10.2 Extension management

Add Extension

Step 1. Go to the NewLync management backend and click Cloud PBX Service->Extension Management.

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

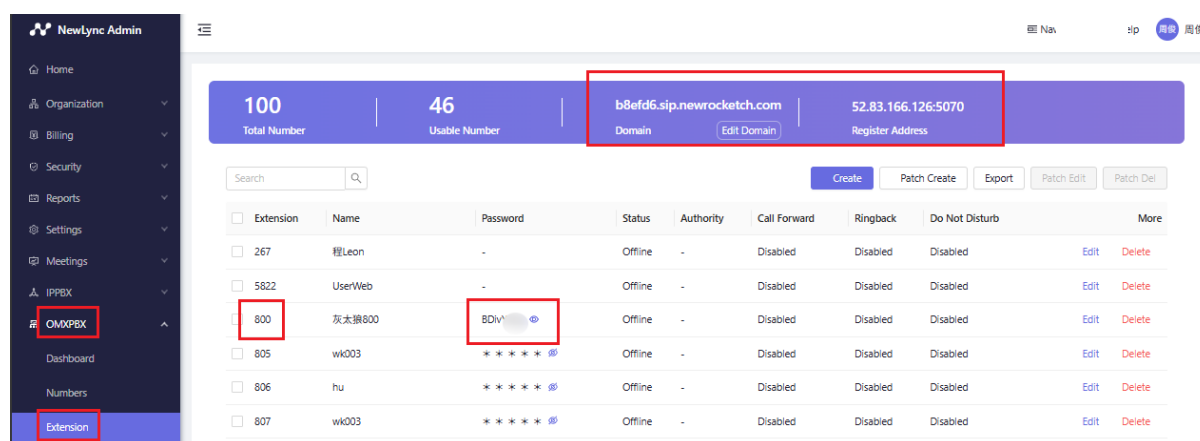
Step 3. In the pop-up window, enter the extension number, select the call-out permission, select the user, and enter the password. Employees can search for people in the organization structure or customize their additions. Once added successfully, you can register via IP Phones.



Step 4. Click Finish to add successfully.

Step 5. After adding, click Edit to configure various services for the extension, such as Recording, Color Ring, Call Forwarding, and so on.

You can register with an IP phone after adding it. In the example below the extension number is 1001, the password is 123456, the address is 192.168.190.210 and the domain is 9b30e.sip.newrocktech.com.



Step 6. Bind an extension to a NewLync account.

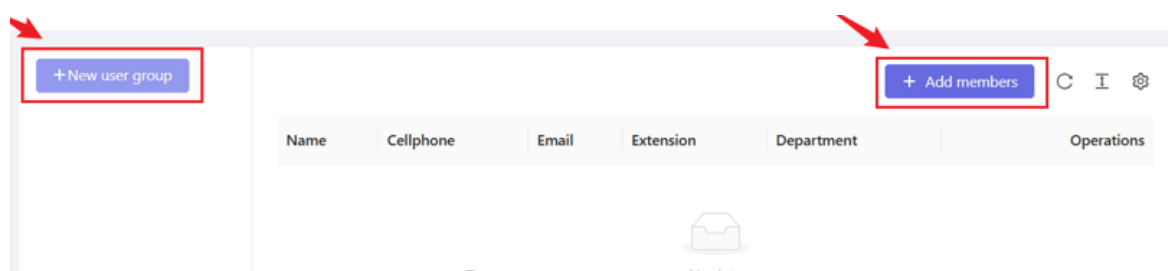
Parameter description

Item	Define
Extension number	Extension number of the created extension
User	Enter NewLync account to search for users
NewLync Synchronization	Calls received by an extension are synchronized to the NewLync account when it is turned on.

7.10.3 User group

Go to the NewLync administration backend, click Cloud PBX Services > Extension Management, and click + Add User Group. 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.

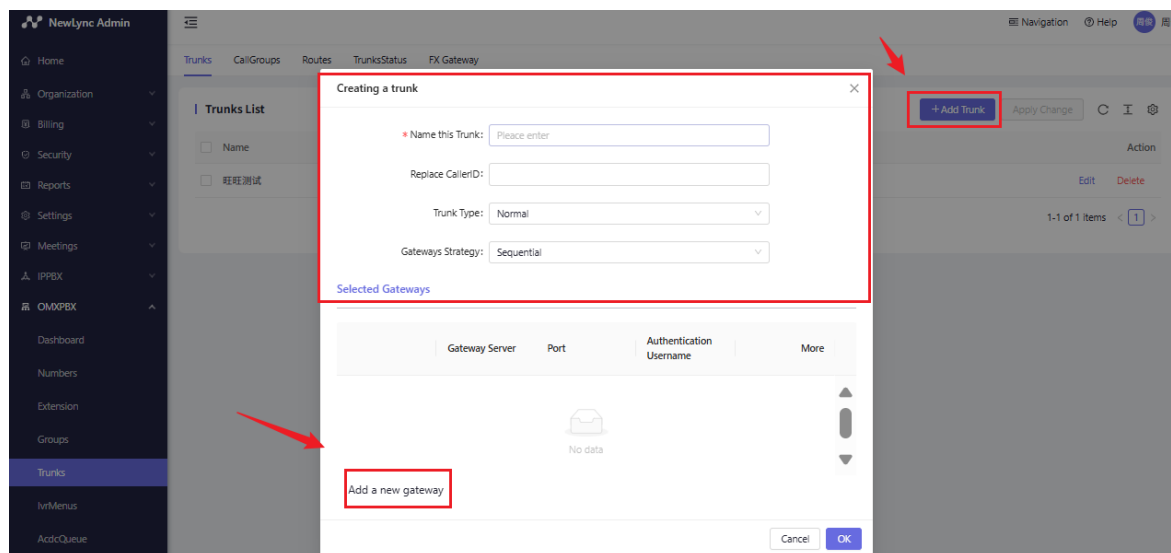


Parameter description

Item	Define
User group name	Customize user group names as required
Extension number	Customize the extension number according to your needs
User group member	In New User select

7.10.3.1 Add Relay

Navigate to Cloud PBX Services > Trunking & Routing. In the Trunking & Routing interface, users can create and manage trunk configurations, including parameters such as trunk type, gateway policy, authentication information, media stream settings, dialing prefixes, concurrent call restrictions, SIP codecs, and so on.

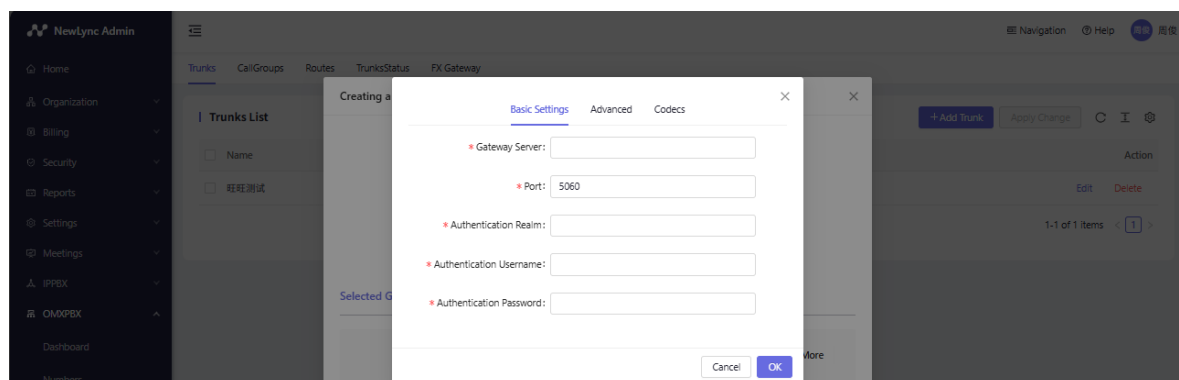


Item	Define
Name this relay.	Users need to configure a unique name for the trunk for subsequent management and querying
replace to show	User can choose whether to replace the external display number or not
Relay type	Ordinary Trunk: Used for regular SIP trunk lines to connect with carriers or IPPBX. Interconnection Trunking: Used for interconnection between different PBX systems within an enterprise, such as voice communication in multiple branch offices.
gateway strategy	Sequence: use the available gateways in the order of the gateway list Equalization: Even distribution of call loads among all gateways, suitable for traffic balancing policies DOD Exclusive: Each call is exclusive to a specific outbound DID

	number, suitable for enterprise outbound call management Local Priority: Prefer local carrier lines to reduce inter-regional or international call charges
--	--

7.10.3.2 Add new gateway

Users can add new SIP gateways to expand the available external line resources.



Item	Define
Gateway server	Information for configuring an external SIP gateway or PBX server
Ports	Usually 5060 (UDP/TCP) is used as the default SIP port, which can be adjusted according to the operator's requirements
Certification domain	Specify the SIP-registered domain name or IP address of the trunk line
Authentication user name	Username for SIP registration
Authentication code	Password for SIP registration

Advanced Options

✕

Basic Settings
Advanced
Codecs

Register: ☐ Charge Of Registration

Register Auth Name:

Streaming: ☐ Charge Of Streaming

Add Prefix:

IMS Support: ☐ IMS Support

Keep Alive (s):

Max Concurrent Calls:

Max Concurrent Inbound Calls:

Max Concurrent Outbound Calls:

Assign to Interface: Default ▼

Newlync Support: ☐ Newlync Support

SIP header CallerID Type: Remote-Party-ID ▼

SipMessage: + Add SIP Header

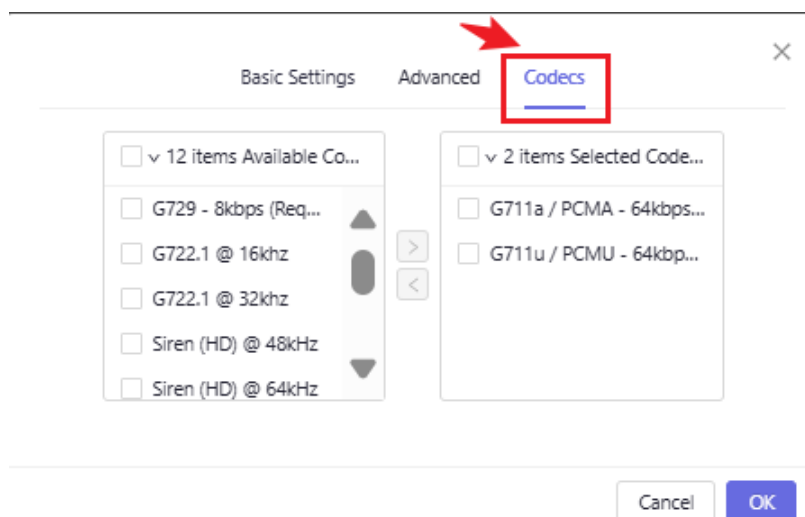
Cancel
OK

Item	Define
Register to server	Decide whether to enable the SIP enrollment process
Encrypted or not	Whether to enable encryption
Before adding dialing	Users can configure dialing prefixes for trunk lines
IMS Support	Check whether to support IMS-based VoIP communication
Alive message interval (sec)	Set the SIP OPTIONS or REGISTER alive interval to maintain the connection to the carrier server
Maximum number of concurrent calls	Define the maximum number of simultaneous calls allowed on this trunk to avoid exceeding bandwidth or carrier limits

Item	Define
Maximum number of concurrent inbound calls	Limit the number of simultaneous incoming calls to this trunk to control the call load
Maximum number of concurrent outgoing calls	Limit the number of simultaneous outgoing calls for this trunk to avoid occupying too many line resources
specified interface	Selecting a specific network interface
NewLync Support	This option determines whether NewLync compatibility mode is enabled to ensure interoperability with NewLync systems
Customized SIP message headers	Allows users to modify or add customized SIP headers as needed

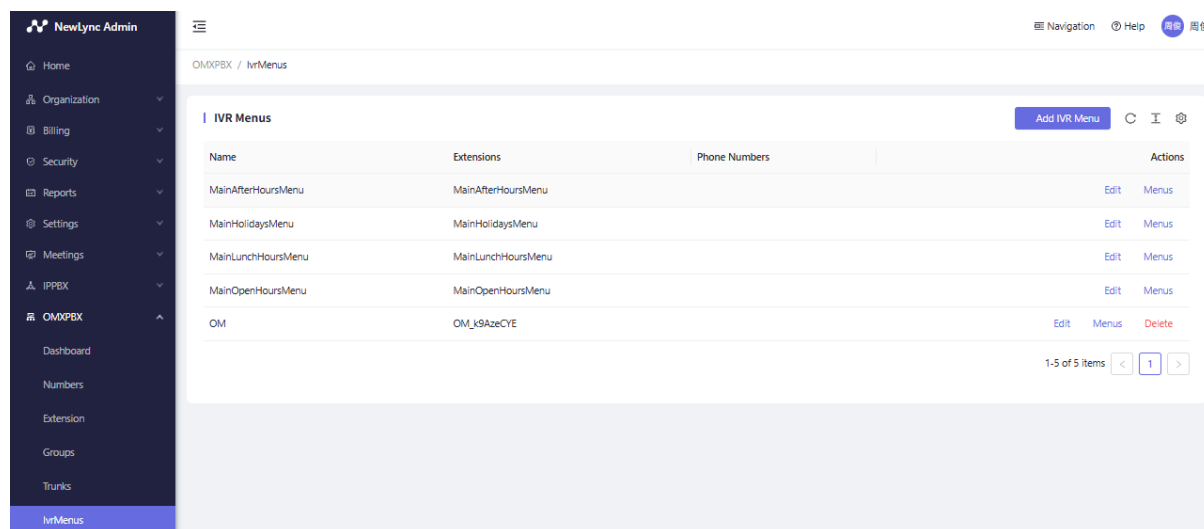
Codecs

Users can select the voice and video codecs supported by this trunk to improve call quality or save bandwidth.



7.10.4 IVR Voice Menu

Navigate to Cloud PBX Services > IVR Voice Menu, where the IVR Voice Menu screen allows users to configure the IVR (Interactive Voice Response) system's voice menus to automatically direct callers to self-service or transfer to the appropriate department.



Item	Define
Ivr name	The user needs to configure a unique name for the IVR menu
Extension number	This is used to set the extension number associated with the IVR menu
Prompt for recording password	For securing voice prompt recordings
Allow callers to dial extensions	Users can choose whether to allow callers to dial extension numbers directly from the IVR menu
Extension number length	Define the length of extension numbers allowed to be dialed
Greetings	The user can configure a welcome voice to be played when an incoming call enters the IVR menu

Advanced Settings

Creating an IVR Menu

Basic **Advanced**

Number of retries on mis: 2

Timeout for dialing (s): 10

Interdigit Timeout (s): 2

Whitelist of numbers: Regex

Blacklist of numbers: Regex

☐ Allow outside recording

☐ Suppress playing of Invalid Entry

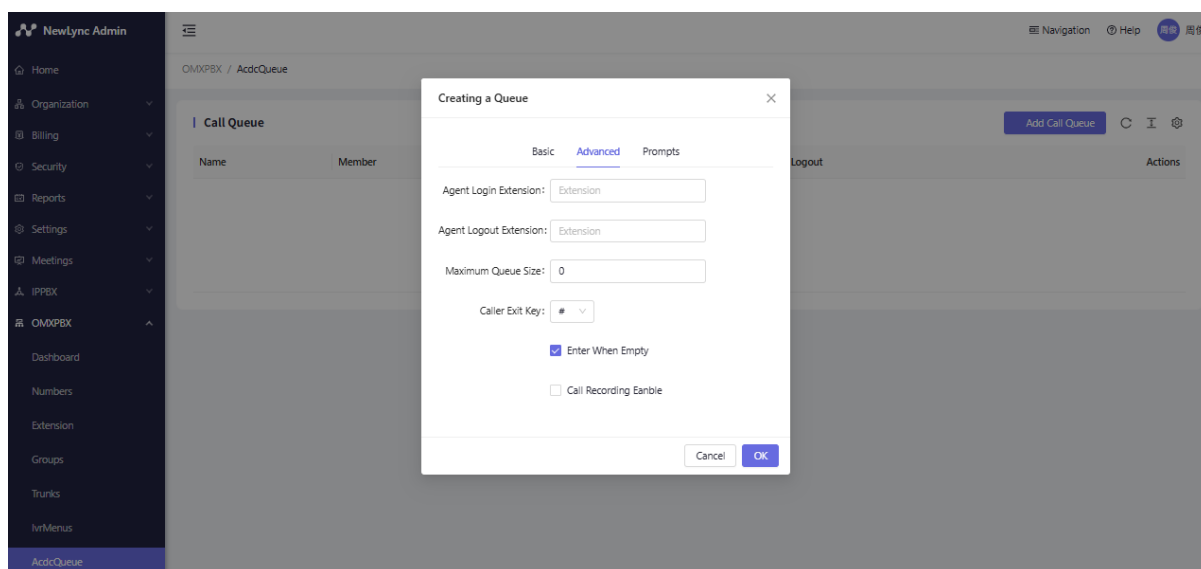
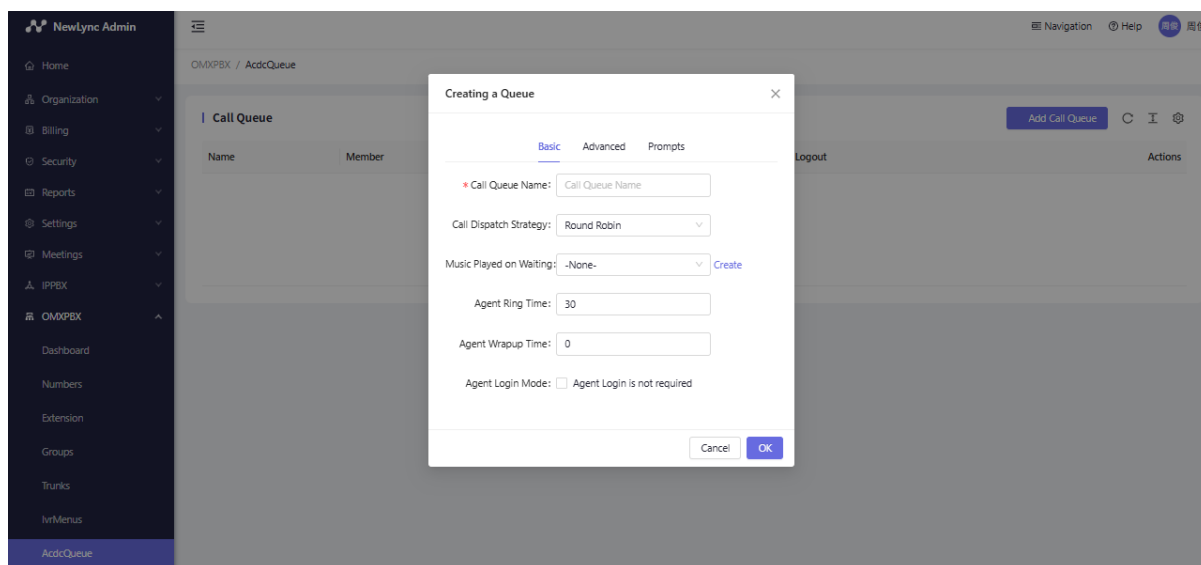
Cancel OK

Item	Define
Number of retries for error dialing	This field sets the maximum number of retries allowed by the IVR system when a user enters an invalid number
Dialing timeout	This field defines the maximum amount of time the IVR waits for the user to enter a keystroke
Inter-dial timeout	Set the maximum allowable interval between each digit when the user enters a number
Number whitelisting	Only the designated number can access this IVR menu
Number blacklisting	Block specific numbers from accessing the IVR menu
Allow external call-in recording	Select whether or not to allow voice recording after an external caller enters the IVR
Blocking invalid entries from playing	This option controls whether or not an error message is played when the user enters an invalid number

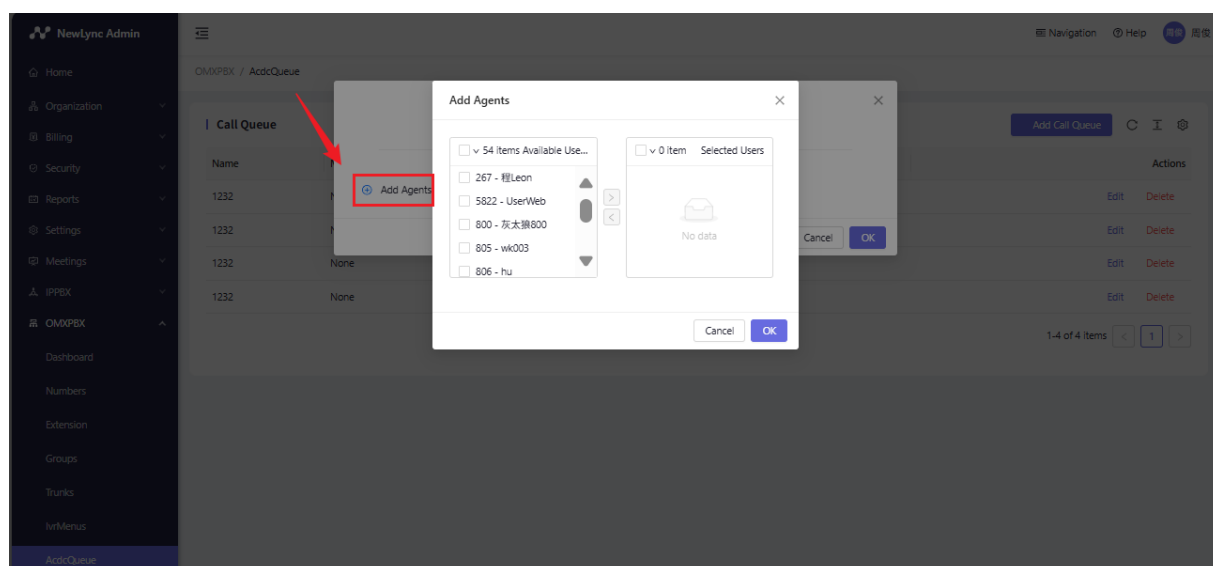
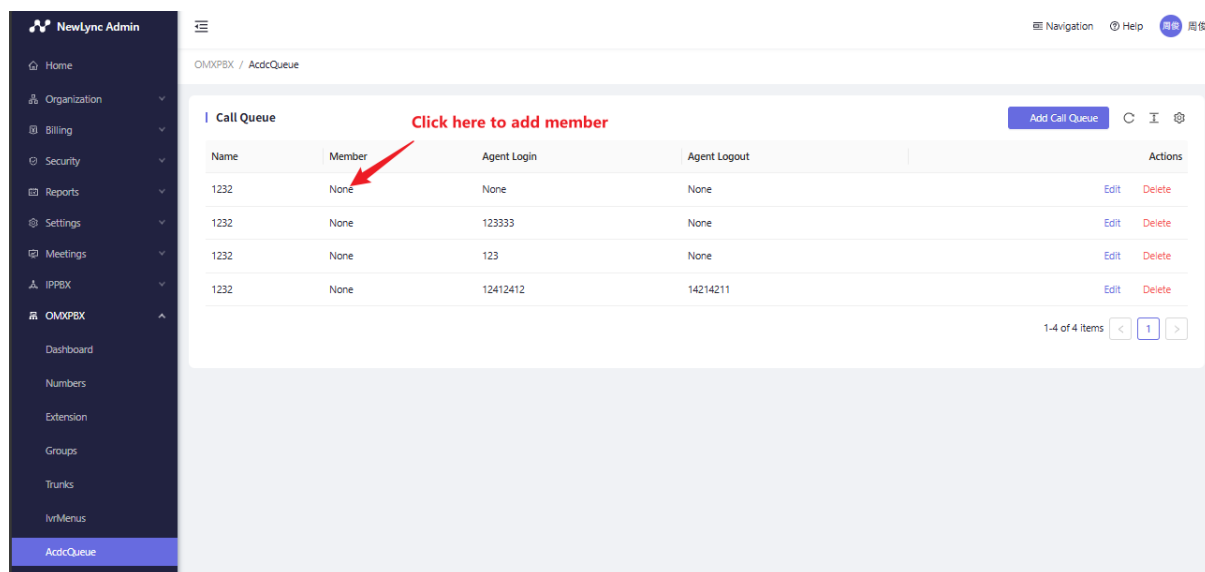
7.10.5 Call queue

Configure call queues in Cloud PBX Services->Call Queues. Distribute call flows by policy for all users in a call queue.

The round selection policy assigns calls to none of the users in turn; the most idle policy assigns calls to the least answered user. If the user is not signed in or is on a call it will not be assigned; you can configure a user in the call queue to pick up the call flow without signing in.

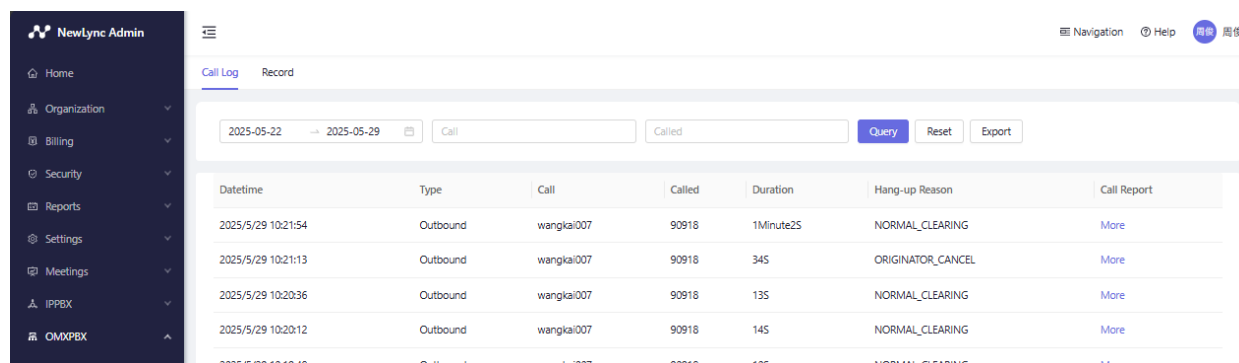


After the call queue is added click on the blank space below the seat member to add the seat member.



7.10.6 Enterprise Operations Management

Go to the NewLync management backend and click Cloud PBX Service->Enterprise O&M Management, this page allows you to view call logs and recordings.



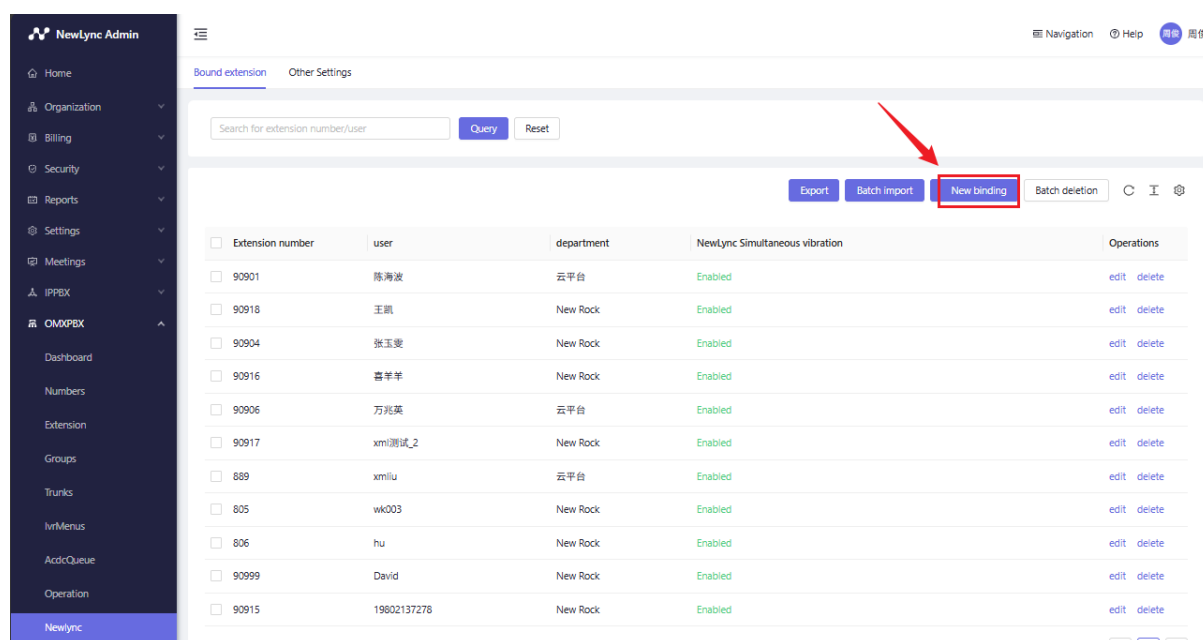
7.10.7 NewLync Settings

After the NewLync account is bound to an extension, you can dial cloud PBX extensions and outside lines through the NewLync APP.

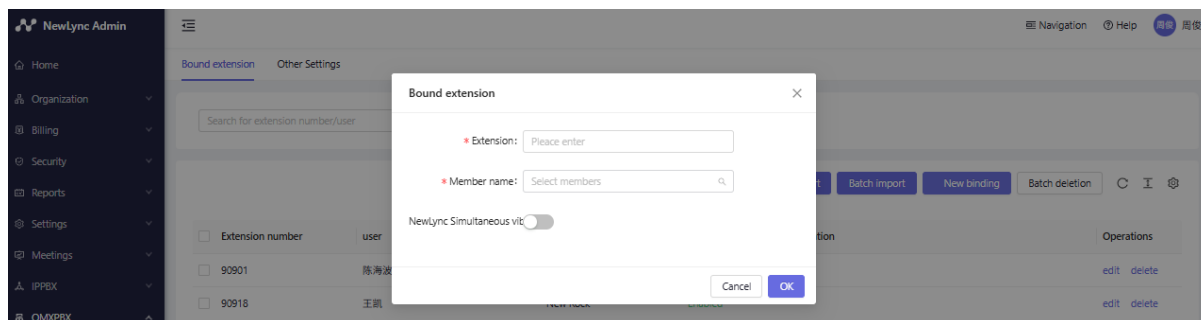
Bound extensions

Step 1. Go to the NewLync admin backend and click Cloud PBX Service->NewLync Settings.

Step 2. Click + New Binding on the Bind Extension page.

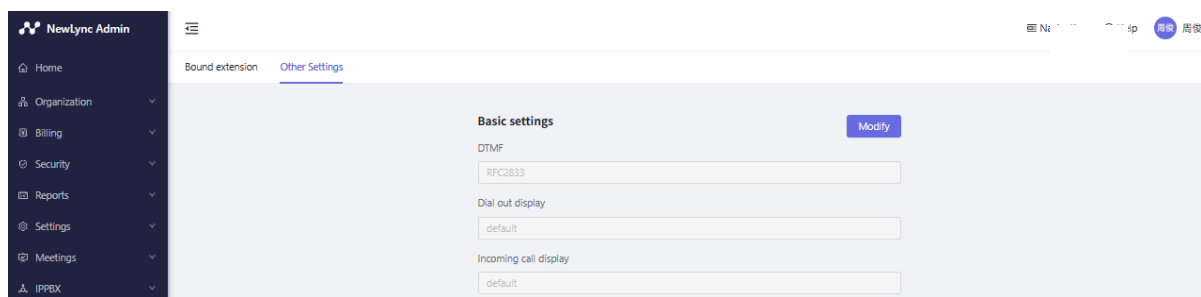


Step 3. Enter the extension number in the pop-up window and select the bound NewLync account to turn on simultaneous vibration.



Step 4. Click OK and the binding is complete.

Configure the DTMF method, caller ID and caller ID on the Other Settings page.



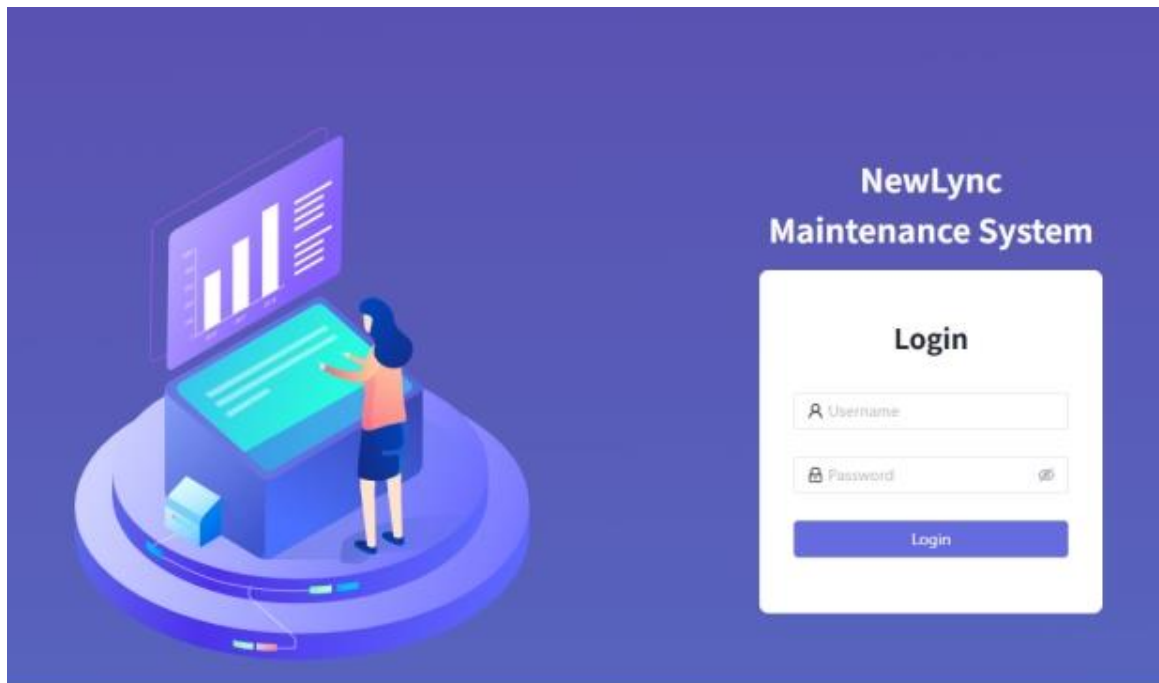
7.10.8 Enabling Cloud PBX

Go to the NewLync admin backend and click Cloud PBX Service->Dashboard. If the asset information pops up, it means it has been purchased. If the Cloud PBX service opening page pops up it is not purchased. Click Open Now to enter the service purchase page, enter the number of extensions and concurrency needed, and submit the order. To fulfill an order, please contact our sales team.

7.11 Sound Recording Management

7.11.1 Recording Configuration

Log in to the NewLync SSC Operations System



Step 1. Open a browser and access the following URL:

- <https://user-ssc.newlync.com>

Note that the "user" part of the URL should be replaced with the specific value provided by your company or system administrator.

Step 2. Enter your username and password to log in:

Default account	sysadmin
Default password	newlyncmgr2021

Step 3. Navigate to CDR Recording > Application Service, click Add to add an application service.

Add Application
✕

* **Name:**

* **Service address:**

Log level:

Local Recording port:

Local CDR port:

Log retention days: Day

Maximum concurrency:

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 .

Step 4. Navigate to > CDR Recording> Node Backup, click "Add Node," and select "AS" as the node type.

Add Node
✕

* Node:

* Node type: as ▼

* IP address:

* HTTP port:

* Port:

Backup target: ▼

App Service: ▼

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

Step 5. Navigate to CDR Recording > Equipment Management, click Add Equipment to add the corresponding OM/Unified communications platform (OMX) device. (If there are 8 OM devices and one Unified communications platform (OMX), you need to add 8 corresponding OM devices and one Unified communications platform (OMX) on the page.)

Add OM

Add equipment

* Select enterprise:

* Name:

Equipment type:

* Device MAC:

FSP security code:

Cache address: ☒ The IP address is 192.168.130.211:5000
☐ Outside the network terminal to register the domain name (P2P penetrate)

Enter the IP address of the OM device.

Timezone:

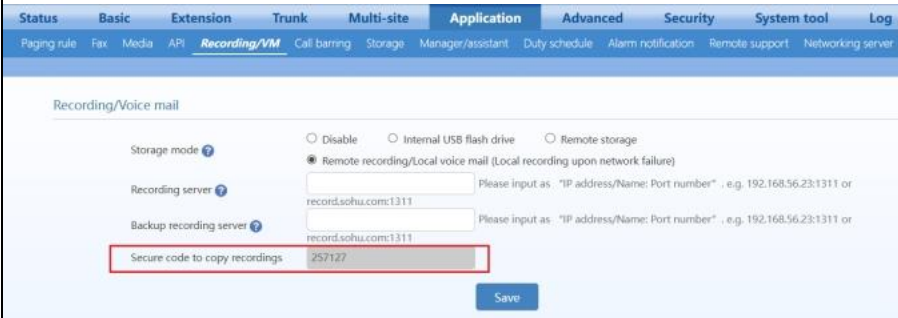
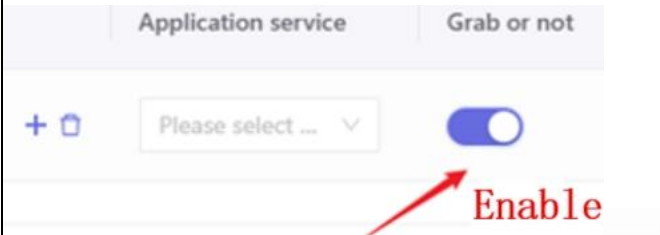
Get interval:

Application service | Grab or not

+ ☒ Open

Cancel OK

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 

Add the unified communication platform (OMX)

Add equipment
×

* Select enterprise: Please select a business

* Name: Please enter name

Equipment type: OMX

* Device MAC: Please enter MAC

Cancel
OK

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

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.

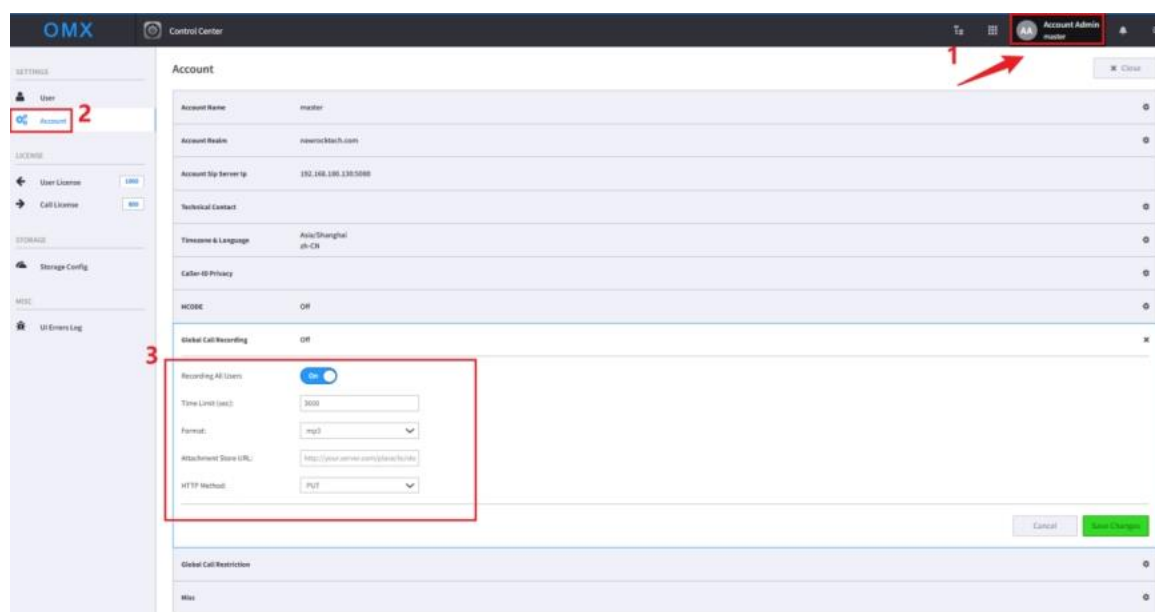
Step 1. Access the Unified Communications Platform Web interface: Use a browser to access the Unified Communications Platform Web interface. The URL is:
<http://192.168.130.71:8085> . (Modify according to the URL of the server you deployed.)

Step 2. 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 3. After logging in successfully, click the admin account in the top-right corner

Step 4. After entering the control center, click "Account" in the left-hand menu to access the tenant configuration page.



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 <code>http://192.168.131.82:8096/recording</code>
HTTP Method	Select POST

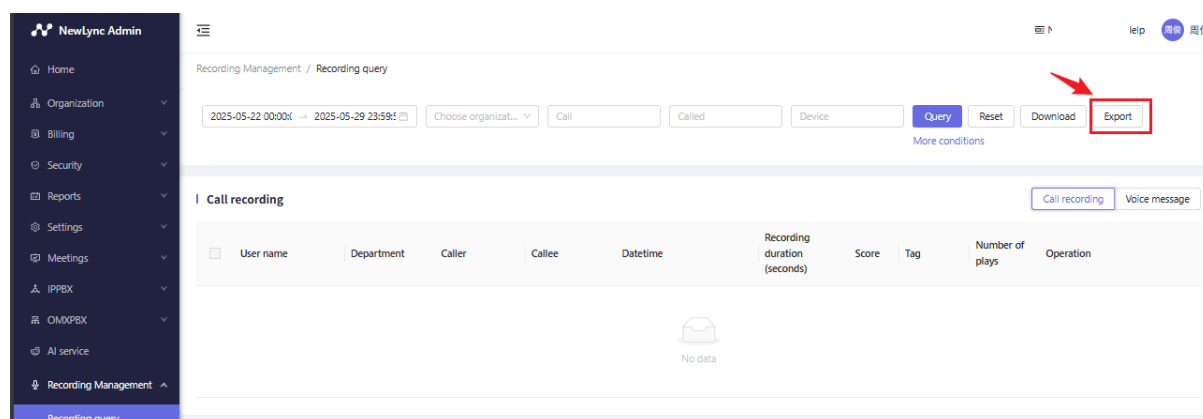
Cloud PBX Configuration Recording Upload

Step 1. To configure the team to be recorded in the NewLync Ops platform, please contact our technical staff for assistance.

Step 2. Go to the NewLync management backend and click Cloud PBX Service->Extension Management. Edit the extension and turn on recording.

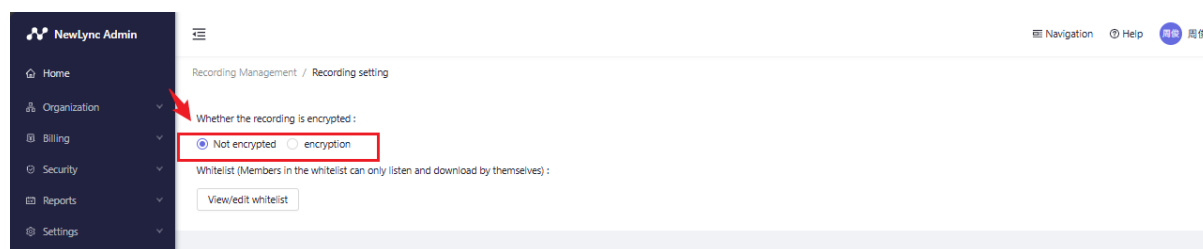
7.11.2 Sound Recording Inquiry

Go to the NewLync administration backend and click Recording Management->Recording Inquiry. Recordings can be filtered by multiple conditions, and can be played and downloaded. Click Export Data to export the recordings and generate an excel file. First select the filter conditions, then click Query, click Export, you can export the recording records of the specified conditions.

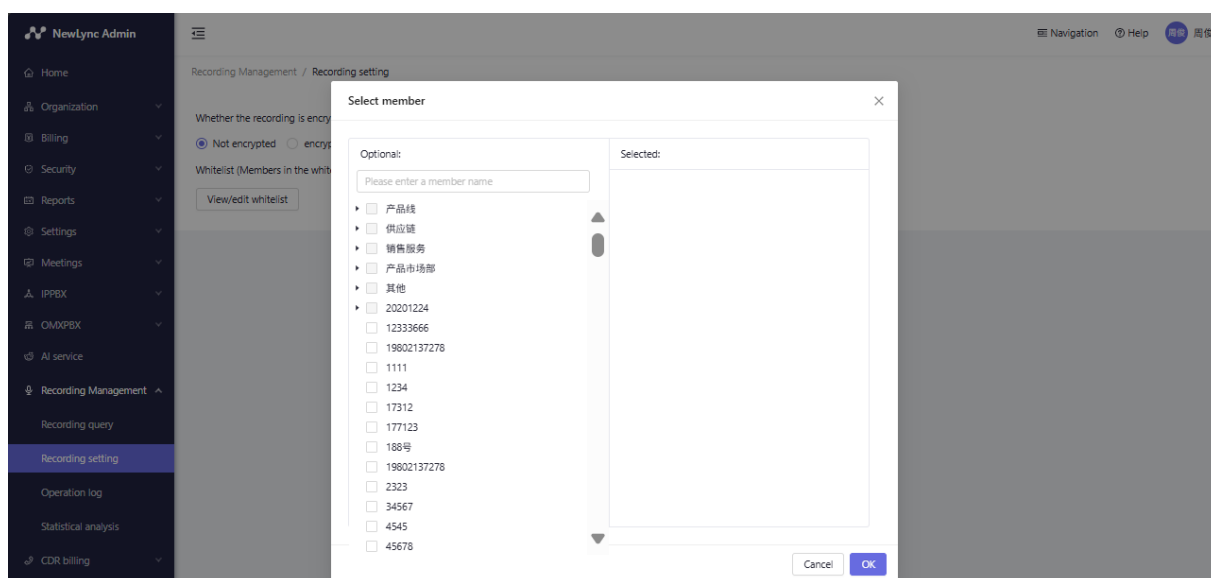


7.11.3 Recording settings

Go to the NewLync admin backend and click Recording Management->Recording Settings. The Recording Settings page allows you to configure recording encryption and whitelisting. When encryption is turned on, the recording files are encrypted and saved on the server, which is more secure and does not affect the playback and download on the admin page.

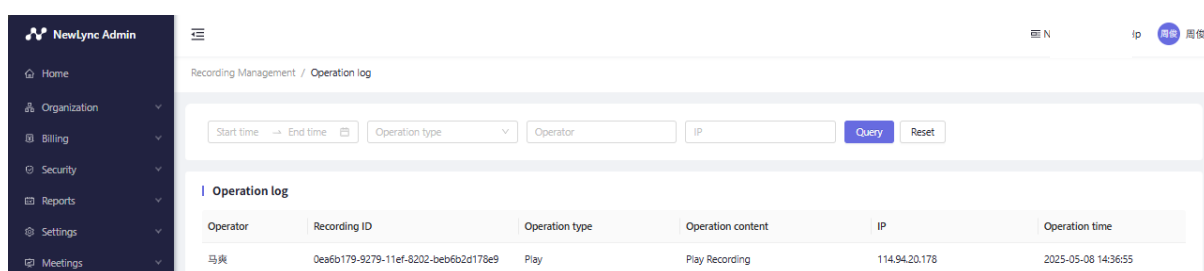


Click + View /Edit Whitelist to add members to the whitelist. After a member is added to the whitelist, only the super administrator and yourself can query and audition the member's recordings, no other administrator can. Other administrators can still audition recordings of members who are not in the whitelist.



7.11.4 Operation log

Go to the NewLync admin backend and click Recording Management->Operation Log. This page allows you to view the operation log about the recording.



7.11.5 Statistical analysis

Go to the NewLync admin backend and click Recording Management->Statistical Analysis. This page allows you to view recording statistics. Click on a report template to switch between daily, monthly, annual, sub-departmental and customized reports.



7.12 CDR Billing

7.12.1 CDR Configuration

NewLync can manage CDRs for IPPBXs and cloud PBXs. IPPBX and Cloud PBX upload CDRs to NewLync and administrators view them uniformly in the management backend.

IPPBX Configuration CDR Upload

Step 1. To configure the OM for reporting CDRs in the NewLync Ops platform, please contact our technical staff for assistance.

Step 2. Log in to OM WEB, click Application Services->API, select Customize, and enter the CDR server address. Enable status monitoring of extensions in the API function.

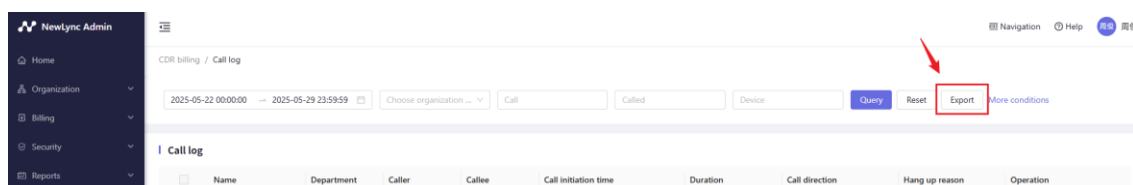
Cloud PBX Configuration CDR Upload

Step 1. To configure the cloud PBX for reporting CDRs in the NewLync Ops platform, please contact our technical staff for assistance.

7.12.2 Call record

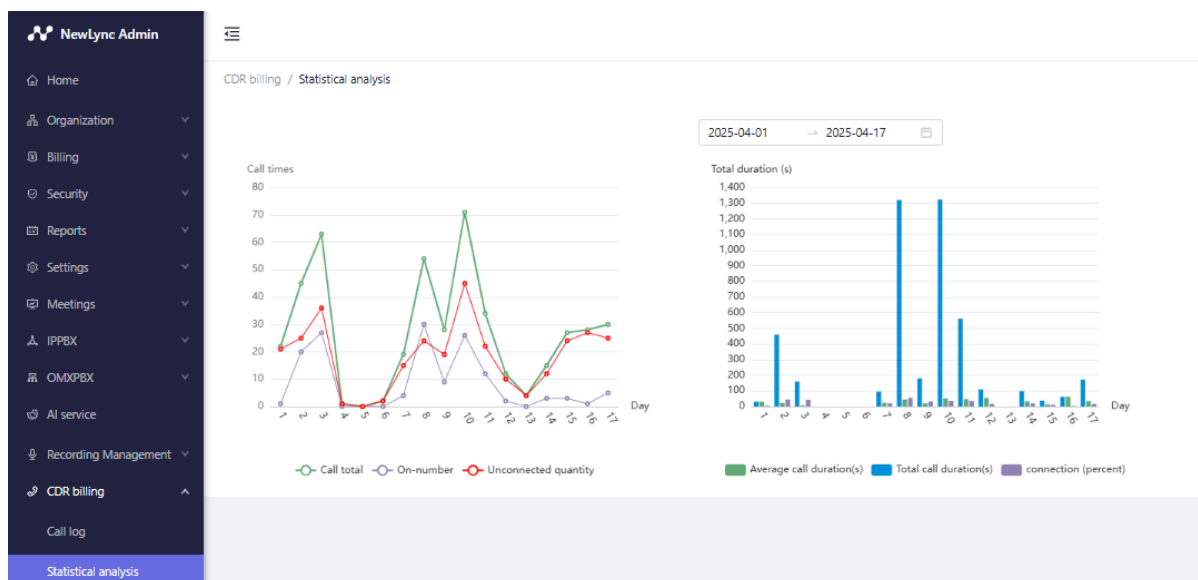
Go to the NewLync admin backend and click CDR Billing->Call Log. The call logs support multi-medium condition filtering and can be viewed in detail.

Click Export Data to export the call logs and generate an excel file. First select the filter conditions, then click Query, click Export, you can export the call records of the specified conditions.



7.12.3 Statistical analysis

The Statistical Analysis page provides a visual display of the number of calls and call duration to help administrators analyze call data. The chart on the left side shows the number of different types of calls, including "Calls" (all calls) in green, "Connections" (connected calls) in red, and "Unconnected" (unconnected calls) in blue. The timeline allows users to view the number of calls made during different time periods. The right side shows call duration statistics, including "Total call duration (sec)" in purple, "Connect duration (sec)" in blue and "Average call duration (sec)" in green. This helps administrators to assess the duration of a call, and allows them to filter the data by selecting a specific date range.



7.13 Billing center

The billing center supports outbound billing, internal calls and inbound are not billed.

7.13.1 Intend

Step 1. Go to NewLync admin backend, click Organizational Structure->Members & Departments to add members, please refer to the previous section.

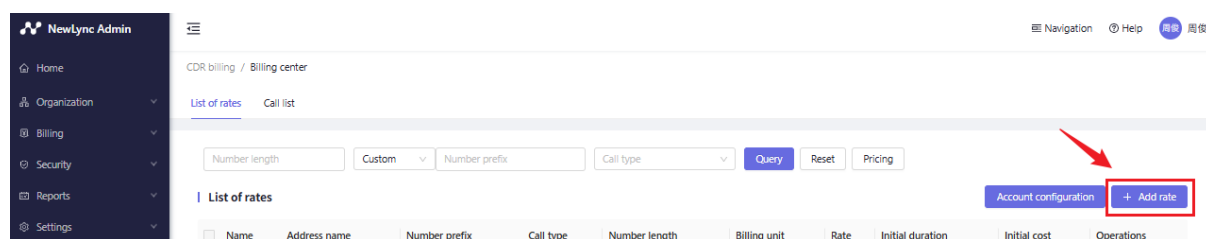
Step 2. Go to the NewLync management backend, click Cloud PBX Service->Extension Management, and add billing extensions.

Step 3. Go to the NewLync admin backend, click Organizational Structure->Members & Departments, edit the member profile, and the Extension field is configured as the billing extension number.

The screenshot shows the 'NewLync Admin' interface. On the left is a sidebar with navigation options: Home, Organization, Members and departments, Invitation, Members profile, LDAP, User group, Billing, Security, Reports, Settings, Meetings, IPPBX, OMMPBX, AI service, Recording Management, and CDR billing. The main content area is titled 'Organization / Members and departments / Member detail'. It contains a 'Member details' form with fields for Name, Cellphone, Department, Email, Hidden phone, Sequence, Rank, Lock user, and a 'Basic info' section with fields for English name, Gender, Employee ID, Seat ID, Job title, Direct manager, Workforce Type, Date of employment, Phone, Extension, and Address. The 'Extension' field is highlighted with a red box and a red arrow pointing to it.

7.13.2 Add Rate

Step 1. Go to the NewLync admin backend, click CDR Billing-> Billing Center, click + Add Rate.



Step 2. Enter the rate parameters in the pop-up window.

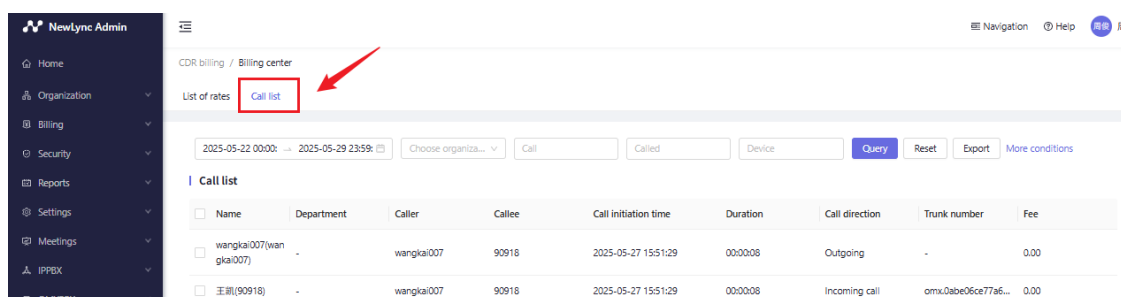
The 'Add rate' pop-up window is shown. It has a title bar with a close button (X). The form contains the following fields:

- * Name: Please enter a name
- Number prefix: Please enter the number prefix
- Number length: 7
- * Rate: Please enter rates
- * Billing unit (s): Please enter a billing unit
- * Initial duration (s): Please enter the initial duration
- * Initial cost: Please enter the initial cost

 At the bottom right, there are 'Cancel' and 'Done' buttons. The 'Done' button is highlighted in blue.

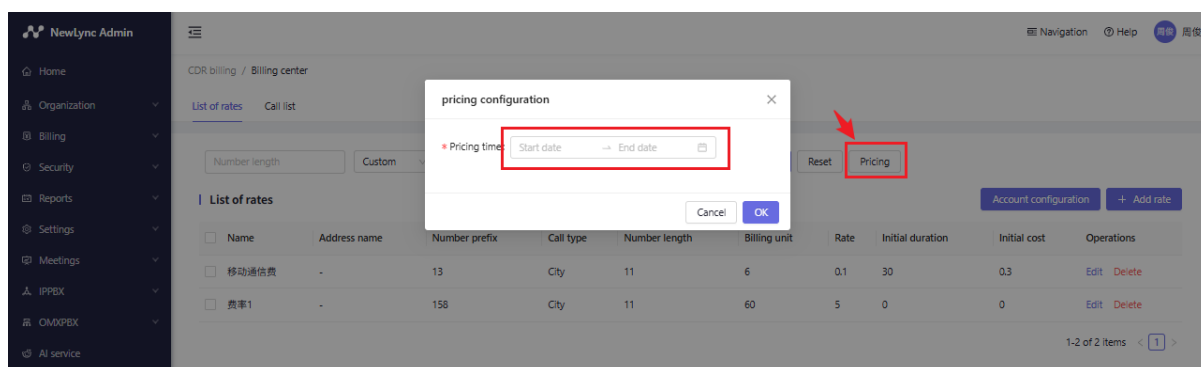
Item	Define
Item	Customizable
prefix of a number	Match the prefix of the number for outbound calls, and if it matches it will be calculated at that rate
Number Length	Matches the prefix of the outgoing number, if it matches it will be calculated at that rate, 0 matches any length
tariff	Rate for one billing unit
Billing unit (seconds)	Duration of a billing unit
Initial duration (seconds)	Costs are fixed for the initial duration, 0 means no initial duration is configured
Initial costs	Costs within the initial duration
Type of call	Multiple types can be selected for easy categorization of call charges

Step 3. Initiate an outbound call using an IP phone and view the charges in the call detail.



7.13.3 Description of rates

1. Fee Calculation Formula, Total Fee = Initial Fee + (Call Duration - Initial Duration) / Billing Unit * Rate.
2. Calls are not billed until after the rate is added, previous calls are not billed, and the call billing date can be selected using the batch rate feature.



3. After modifying the rate, the default is to make it effective only for subsequent calls; use the batch pricing feature to have previous calls re-priced.

7.14 Statement of Accounts

The Billing Statement page shows the Billing Filter component and the Monthly Bill.

The screenshot shows the NewLync Admin interface. The left sidebar contains a navigation menu with items like Home, Organization, Billing, Security, Reports, Settings, Meetings, IPPBX, OMOIPBX, AI service, Recording Management, CDR billing, Call log, Statistical analysis, Billing center, and Billing statement (selected). The main content area is titled 'CDR billing / Billing statement'. It features a filter bar with a dropdown menu set to 'New Rock', date range '2025-04-29' to '2025-05-29', a 'FeeNum' input field, and a 'Statement details' button. Below the filter is a table titled 'Monthly bill list' with two columns: 'Month' and 'Operations'. The table lists months from 2025-05 down to 2024-11. Each row has two links under the 'Operations' column: 'Departmental billing details' and 'All the departments billing details'.

Select the department and time in the filter, enter the extension number, and click Extension Query Billing to query the bill for the specified extension; if the extension is left blank, then query the bill for the extension in the specified department.

This screenshot is identical to the previous one, but with red rectangular boxes highlighting the 'New Rock' dropdown menu and the 'FeeNum' input field in the filter bar.

8 Common Problems

1. How to set the username/password expiration date for Ubuntu, Kirin, UOS Server, Ola OS?

Answer: The administrator can enter the commands in the following table to set the account and password expiration date.

Command	Definition
<code>sudo usermod -e XXXX-xx-xx username</code>	Setting the account expiration time
<code>sudo usermod -e -1 username</code>	Setting up accounts to never expire
<code>sudo usermod -U username</code>	Unlock Account
<code>sudo usermod -L username</code>	Lock your account now
<code>sudo chage -m 7 username</code>	Minimum number of days to use the password Minimum change interval
<code>sudo chage -M -1 username</code>	Set a password that never expires
<code>sudo chage -M 90 username</code>	User's password expires after 90 days
<code>sudo chage -l 30 username</code>	Account lockout 30 days after password expiration
<code>sudo chage -d 0 username</code>	Password validity set to 1970-01-01 (expires immediately)
<code>sudo chage -W 14 username</code>	Number of days warning before password expiration
<code>sudo chage -l username</code>	Check user and password expiration dates



Note With the Unicom server, the passwords for newly created users expire after 90 days if the configuration file has not been modified. A reminder is sent 7 days before the expiration date. After the password expires, there is a grace period of 1 month, during which you can only change the password, but after the grace period, the account will be locked out and you will not be able to log in.

2. How do I view and manage call logs?

Answer: You can view the call logs through the NewLync admin backend. Go to the CDR Billing menu, select Call Logs, and you can query specific call logs using a variety of filters. Call logs are exported to Excel files for subsequent analysis and archiving.

3. How do I perform a system backup and restore?

Answer: In NewLync 2.0 , you can backup your data through the Backup and Restore function in the System Settings page.

4. How do I configure and manage my internal address book?

Answer: In the Contacts Management page, you can import your organization's personnel information into the NewLync 2.0 system, and the system will automatically generate an enterprise address book. You can categorize by department, position, etc. and allow users to quickly find information about their coworkers.

5. How do I configure user permissions and roles?

Answer: In NewLync 2.0 , you can configure user rights and roles through the User Management page. First, create a new user or edit the information of an existing user, and then select the appropriate role in Permission Management.

9 Glossary

Letter	Nomenclature	Definition
A	Active-Standby (two-machine hot standby architecture)	High availability is achieved by configuring a primary and backup server. When the primary server fails, the backup server automatically takes over to ensure uninterrupted system service.
A	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.
C	CDR (Call Detail Record)	A system that records detailed information (e.g., call length, start and end times, participant numbers) about each call activity for analyzing call data and calculating charges.
C	Cloud PBX	With a private telephone exchange system based on cloud services, enterprises realize internal and external voice communication through cloud PBX, avoiding the complex management and high cost of hardware equipment.
C	Cloud PBX (Cloud PBX)	A cloud-based telephone switching system where users access and manage telephone services over the Internet.
D	Data Synchronization	Synchronize data across multiple servers or devices to ensure data consistency and real-time performance.
D	DNS (Domain Name System)	Used to convert a domain name into an IP address, allowing users to access a website through the domain name.
D	DOD (Direct Outside Dialing)	A telephone system feature that allows users to make direct external calls without going through a switch.
I	IMS (IP Multimedia Subsystem)	An architecture for multimedia communications that supports multiple types of communications such as voice, video, and data.
L	LDAP (Lightweight Directory Access Protocol)	Helps computers find and manage people or device information on the network, such as e-mail addresses or printers, and is commonly used for user and resource management within an organization.

Letter	Nomenclature	Definition
P	Provisioning	The process of automating the configuration and management of devices in a system, including the configuration of users, devices, outside trunks, and so on.
R	RTP (Real Time Transport Protocol)	A network protocol used to transmit real-time data such as audio and video over the Internet.
S	SIP (Session Initiation Protocol)	A communication protocol for creating, modifying, and terminating voice and video calls in an IP network.
S	SIP Trunk (SIP Trunking)	A technology that connects the NewLync 2.0 system to external telecommunication networks (e.g., telephone networks, VoIP service providers, etc.) via the SIP protocol for external call origination and access.
T	TCP (Transmission Control Protocol)	A network protocol that ensures the accurate and error-free transmission of data packets through an acknowledgement and retransmission mechanism for applications that require high reliability, such as e-mail and file transfers.
U	UDP (User Datagram Protocol)	A fast network transmission protocol that does not guarantee packet order or integrity for video streaming and online gaming, where speed is more important than transmission reliability.
V	Virtual IP	IP addresses shared between multiple servers or devices