Ruijie OCE Identity Manager

User Guide

Document Version: V1.1
Date: July 02, 2025

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- The official website of Ruijie Reyee: https://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijie.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijie.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Note

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Instruction

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

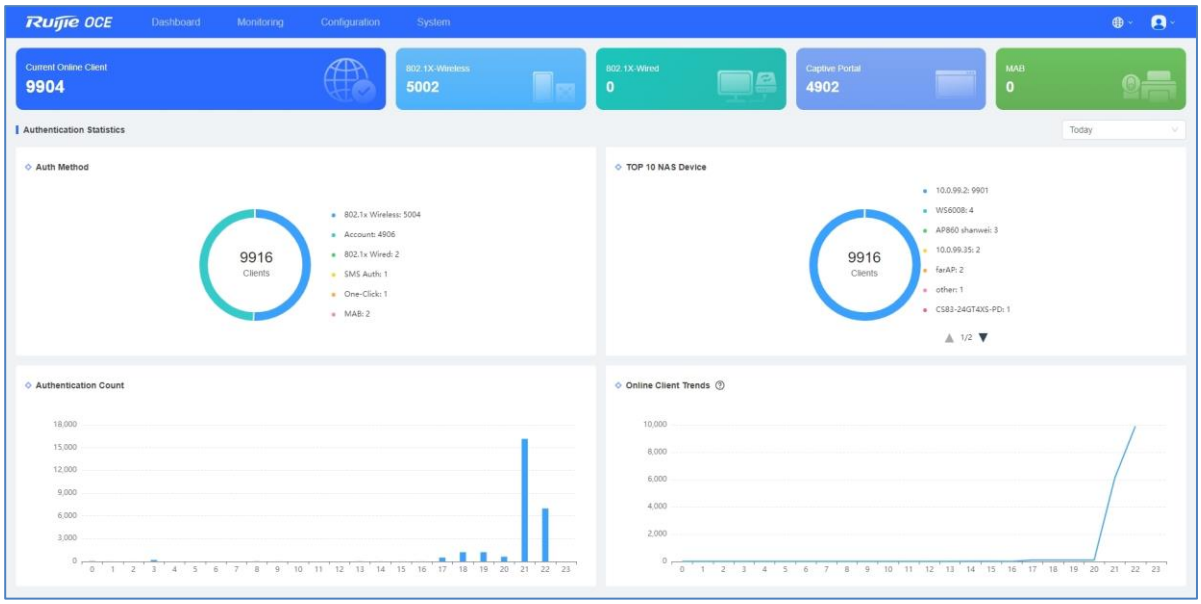
- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocol.

1 Product Introduction

1.1 Ruijie OCE Identity Manager Overview

The Ruijie Omni-Control Engine (OCE) is an on-premises platform of Ruijie public cloud. It consists of two components: the OCE Identity Manager for identity authentication, known as Network Access Control (NAC) or Authentication, Authorization, Accounting (AAA) built with a RADIUS server, and the OCE Network Manager for network device management, known as NMS server. The Ruijie OCE can be easily installed on physical servers or ESXI VM instances.

The Ruijie OCE Identity Manager features an innovative UI and simple configuration steps. It supports both wireless and wired 802.1X authentication, as well as captive portal authentication. It also provides easy access control with MAB authentication for IoT devices. It supports multiple authentication and authorization sources (local account/AD/LDAP), and can easily integrate with existing data sources. Besides, it offers rich authorization policies, including dynamic VLAN assignment, QoS, concurrent users, traffic usage, and time period control, along with flexible portal authentication methods.



1.2 Key Features

- On-Premises Deployment
  - Software installed on a local server
  - High-security data protection
  - Supports deployment on the VMware ESXi and physical deployment
  - Supports Ruijie, Reyee and third-party devices
- User-friendly UI
  - Simple configuration of authentication policies for network devices in three steps

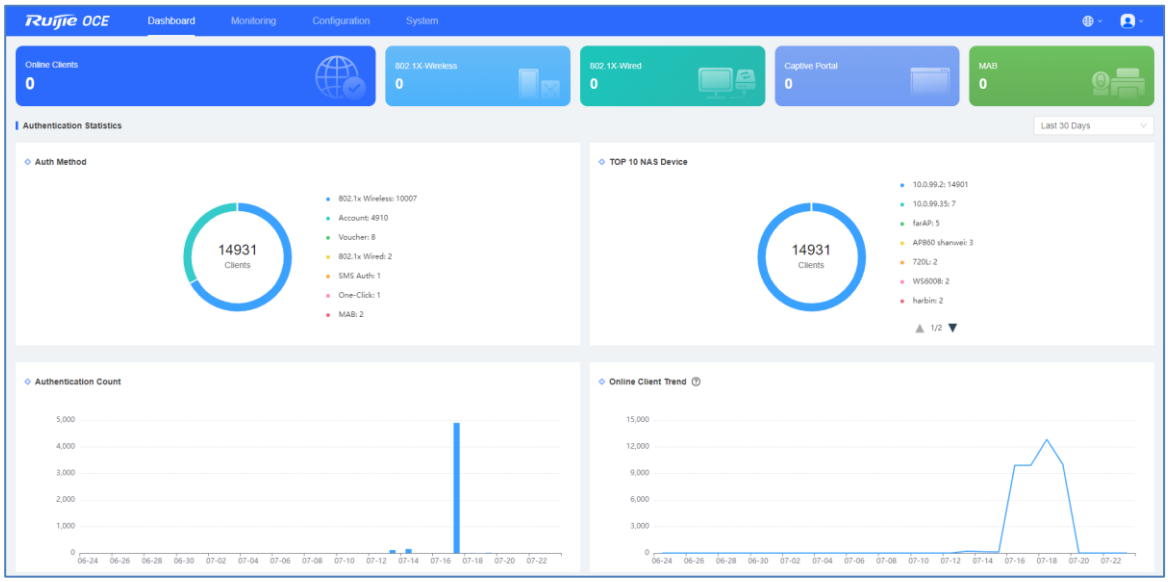
- Intuitive dashboard and real-time status monitoring
- Easily locate authentication exceptions and visibility on 802.1x requests

- Flexible Authentication Methods
  - Wireless and wired 802.1X, and captive portal authentication
  - 802.1X with dynamic VLAN assignment
  - MAB authentication for IoT devices
  - Supports multiple authentication and authorization sources (local account/AD/LDAP)
- Rich Authorization Control Policies
  - Control of concurrent online clients
  - Valid time period control
  - Valid traffic quota control
  - Dynamic QoS
  - Dynamic VLAN assignment
- Marketing Campaign & Captive Portal
  - Integrated captive portal module, supporting One-Click, Voucher, SMS Code, Account login and Email registration methods
  - Supports rich customization options for the captive portal page, such as background image, logo, welcome text, advertisement images or video, and button styles
  - Supports 10+ languages for the portal page, and flexible customization of the page language

2 Dashboard

The Ruijie OCE Identity Manager Dashboard provides a clear view of the current number of authenticated clients and the distribution of authentication methods, including the trends in authenticated clients and the peak and off-peak periods.

The Ruijie OCE homepage displays the total number of online clients, as well as the number of clients accessed through wireless 802.1X authentication, wired 802.1X authentication, captive portal, and MAB.



Authentication statistics are displayed on the Ruijie OCE homepage, including authentication modes, authentication devices, and trend analysis. You can filter data by time, and the options include **Today**, **Yesterday**, **Last 7 Days**, and **Last 30 Days**.

- **Auth Method**: indicates the authentication modes within the specified time range.
- **TOP 10 NAS Device**: displays the top 10 NAS devices by the number of authenticated clients within the specified time range.
- **Authentication Count**: shows the authentication request count trend within the specified time range, facilitating the location of the peak authentication time point.
- **Online Client Trend**: displays the online user trends based on statistics within the specified time range. It allows users to quickly view peak authentication times and the number of clients.

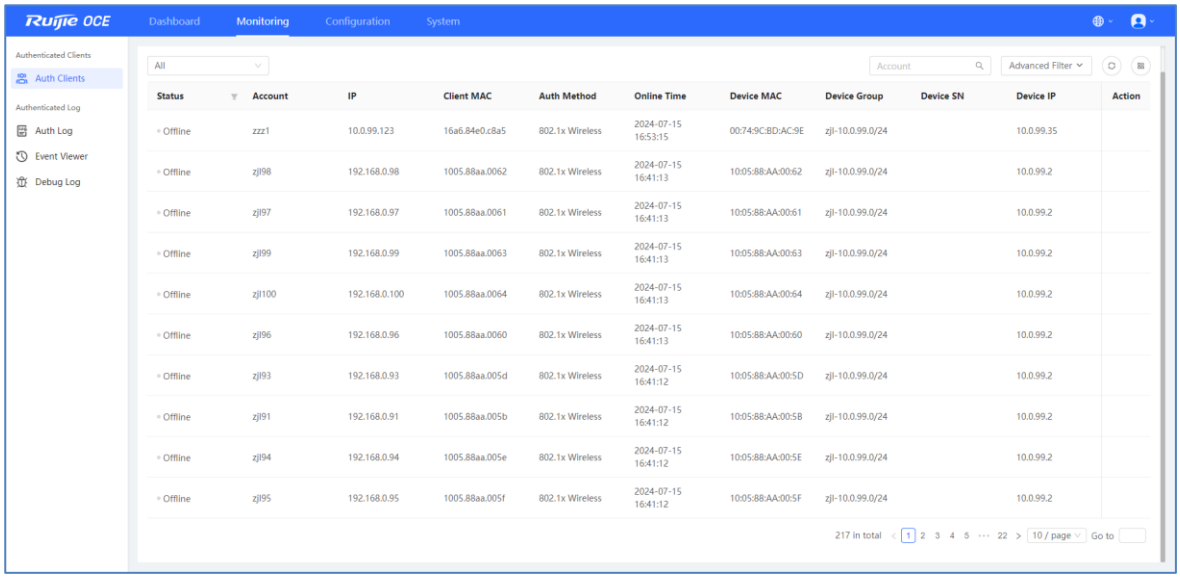
3 Monitoring

3.1 Authenticated Clients

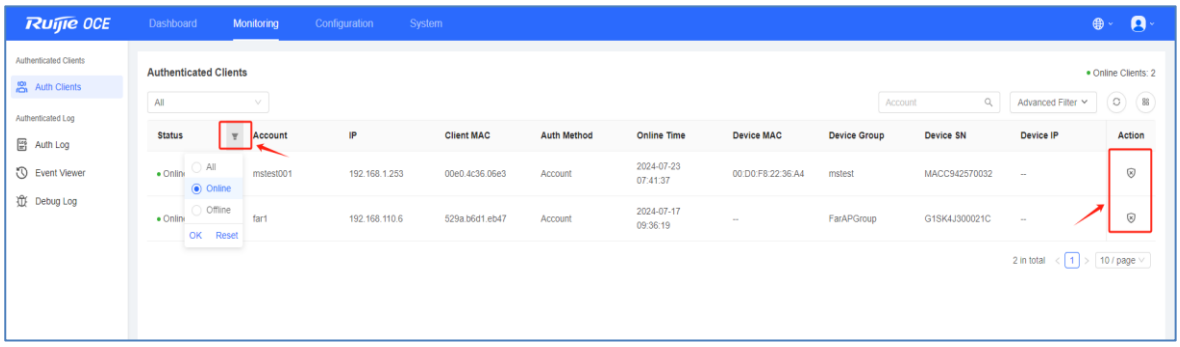
3.1.1 Authenticated Clients

Choose **Monitoring** > **Auth Clients**.

The online and offline statuses of authenticated clients can be viewed. A record is kept for the MAC address of each client.



You can filter online or offline clients. You can also click the icon in the **Action** column to disconnect an online client.



Notes about client disconnection:

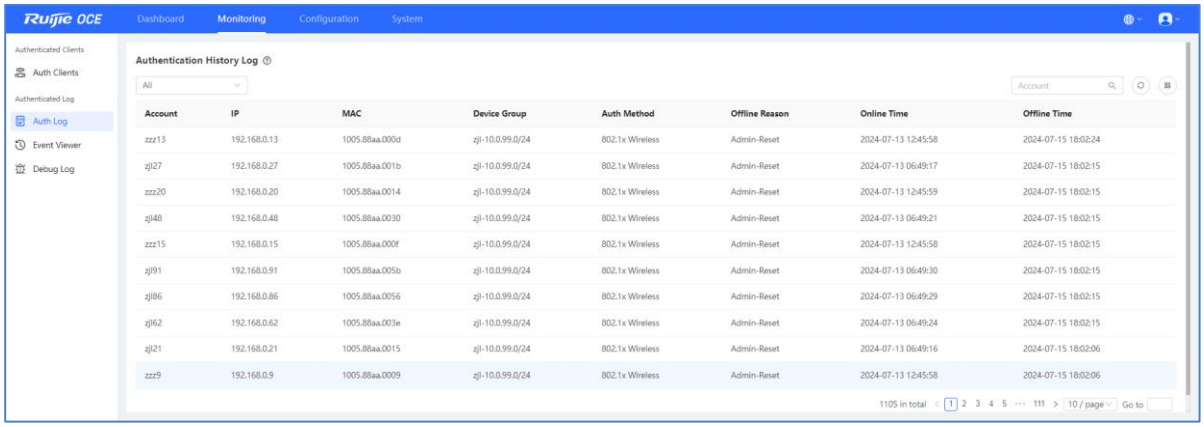
- For clients using portal authentication, the disconnected client will go offline in 1 minute. The client will be disconnected from the network only when the server receives the next heartbeat signal from the client.
- For clients using 802.1X authentication, ensure that the IP addresses of the authentication server and the network device are reachable to each other. The client authentication session on the network device is terminated and the client is disconnected only when the disconnection request sent by the RADIUS server through CoA or DM packets successfully reaches the network device.

3.2 Authentication Logs

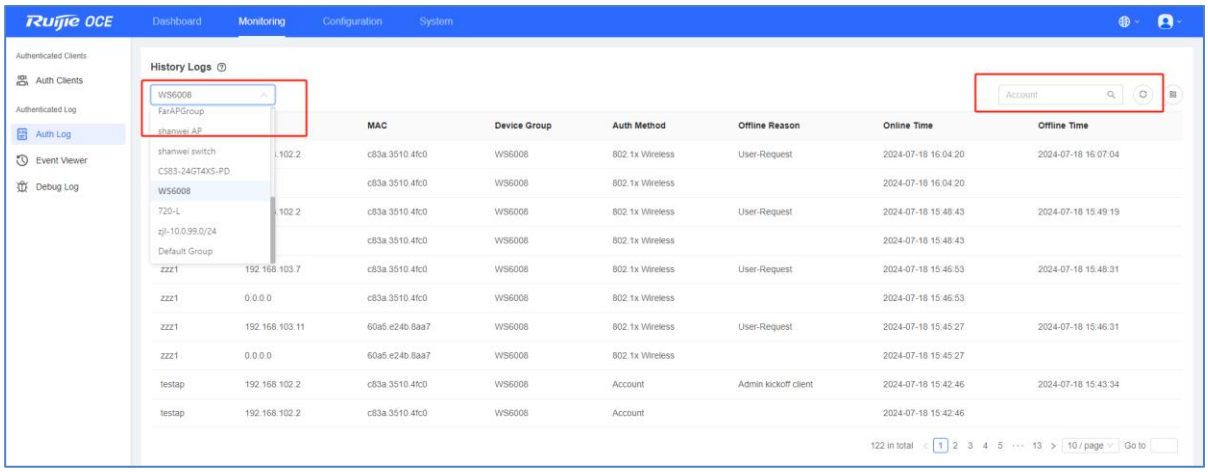
3.2.1 Authentication Log

Choose **Monitoring > Auth Log.**

You can view the online and offline records of clients using the 802.1X and Portal authentication methods in the past three months.



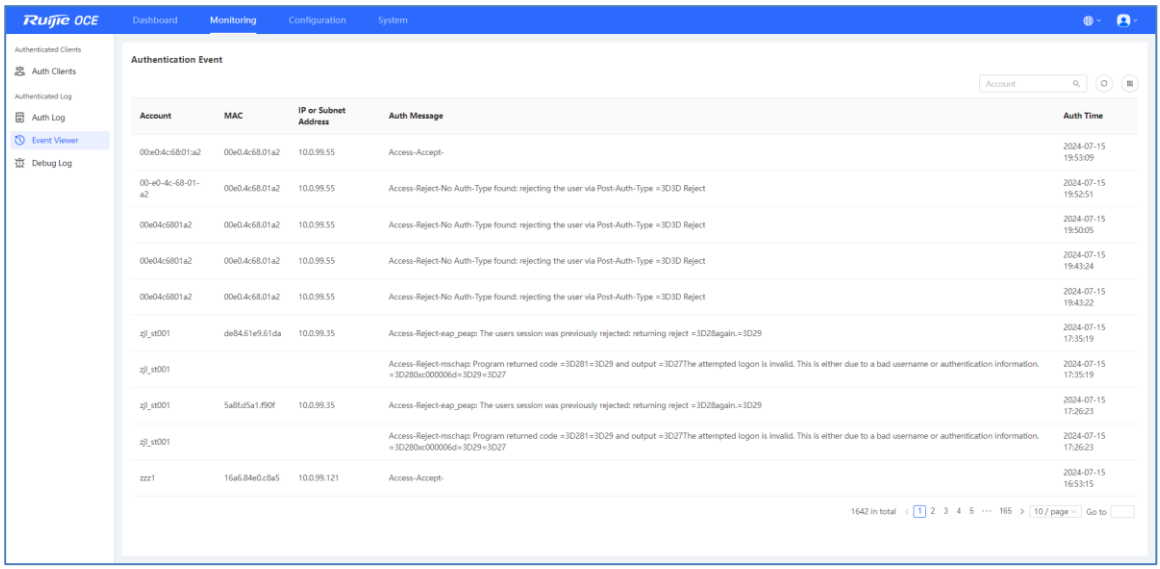
Select a device group from the drop-down list box in the upper left corner to filter authentication logs by device group. Enter a keyword in the search box in the upper right corner to search logs by account.



3.2.2 Event Viewer

Choose **Monitoring > Event Viewer.**

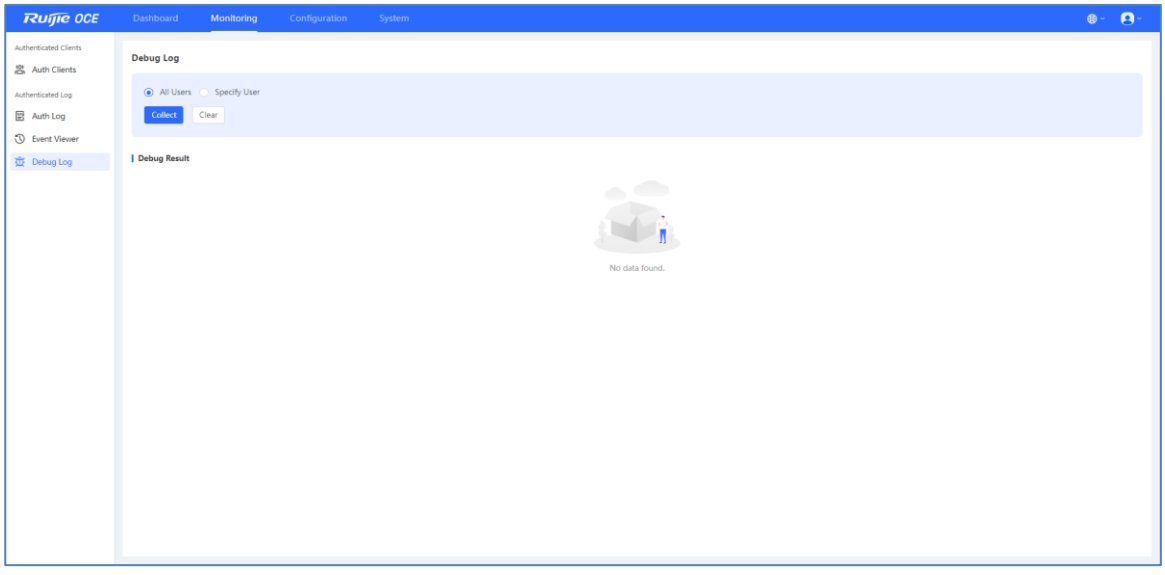
You can query exception events during authentication, such as incorrect usernames or passwords. When authentication fails for a client, details of the failure are logged and stored in this log for up to three months.



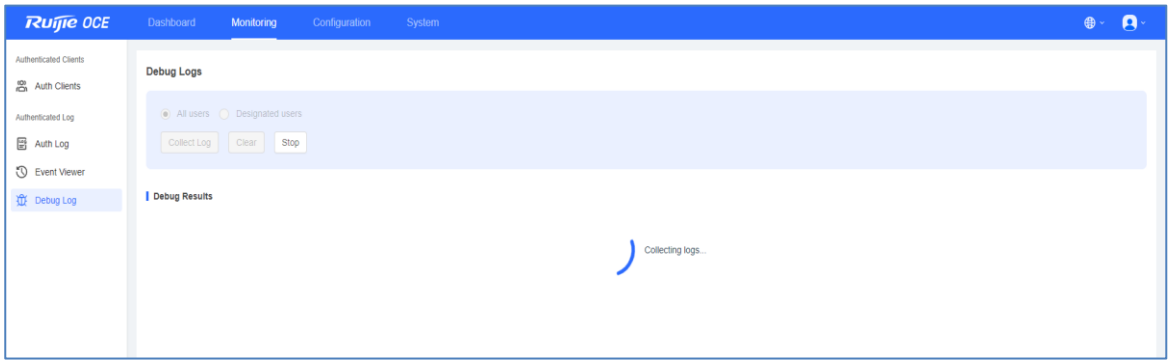
3.2.3 Debug Logs

Choose **Monitoring > Debug Log.**

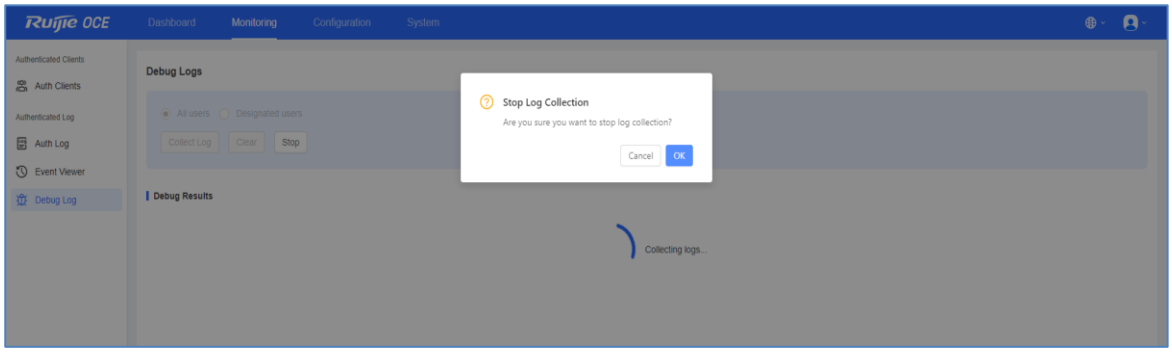
You can view the 802.1X authentication debug logs. Authentication process logs for all clients or specified clients can be collected, and the log collection duration can be customized, which facilitates fault analysis during authentication. You are advised to send this log to the after-sales support team and R&D team for analysis.



Click **Collect** to start collecting logs. Connect a mobile phone to the authentication SSID to collect authentication logs.



Click **Stop** to complete log collection.



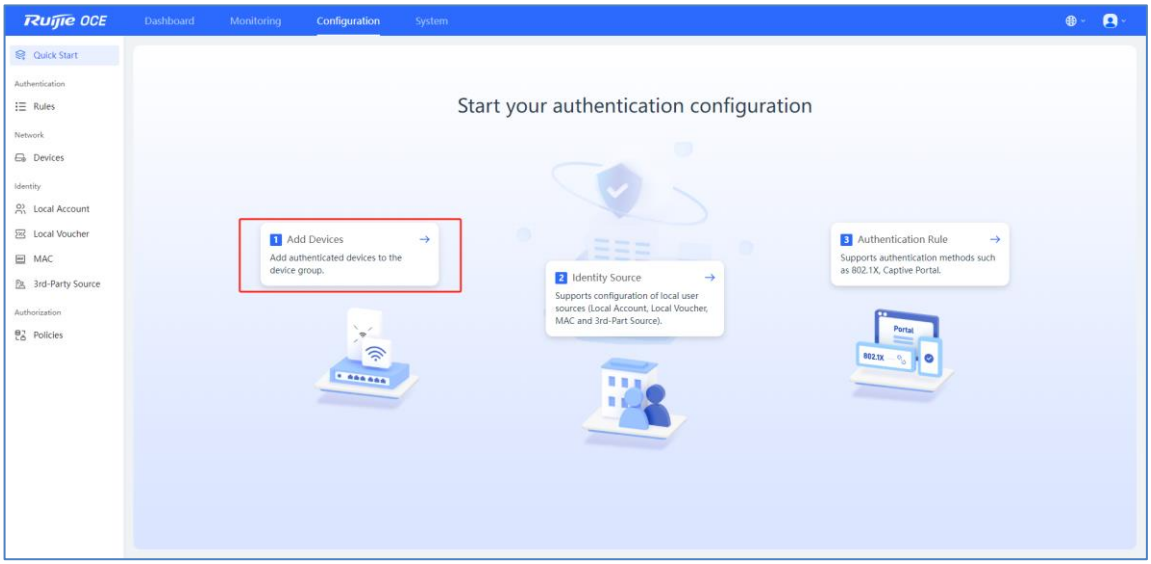
4 Configuration

4.1 Adding Network Devices

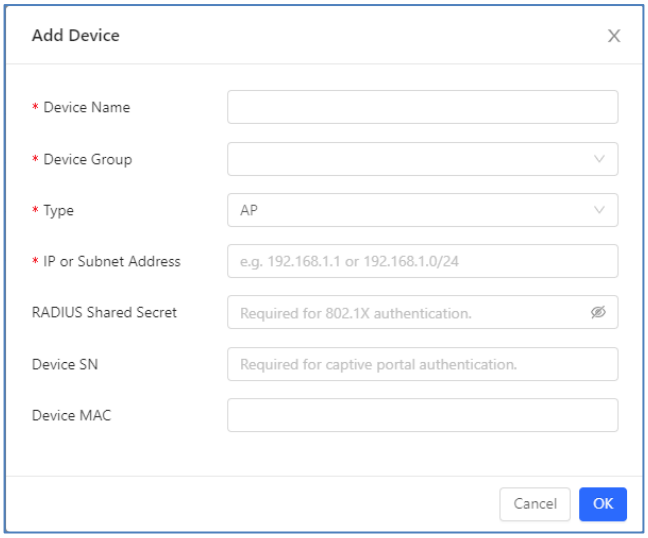
When a device is added to a device group, the authentication configurations of the device group will take effect on the device.

Procedure

(1) Choose **Configuration** > **Quick Start** > **Add Devices**.

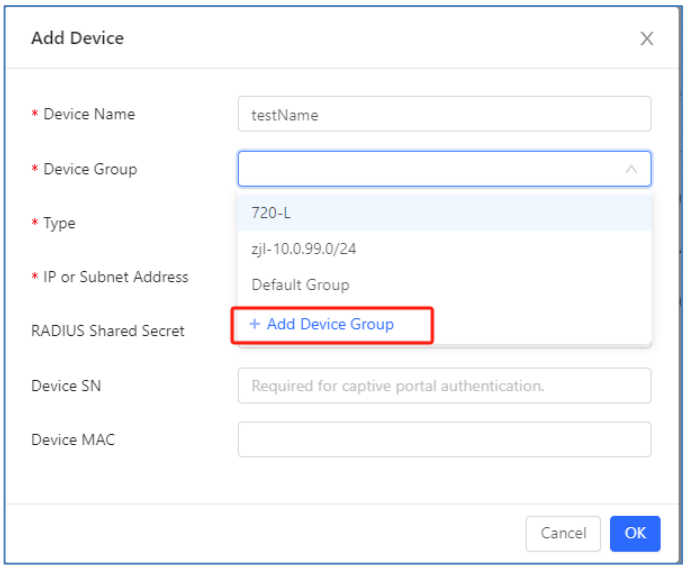


(2) Set basic parameters of the device. Then click **Next**.

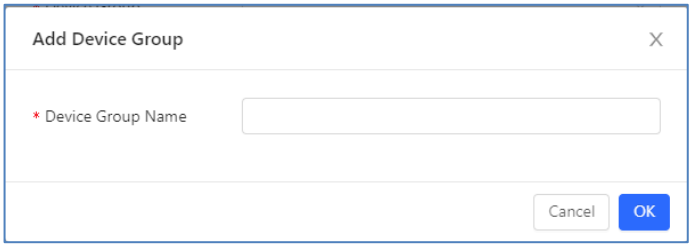


Device Name: indicates the device name. The value is a string of up to 32 characters.

Device Group: indicates a device group. Select the device group from the drop-down list box, or click **Add Device Group** to add a new device group.



The value of **Device Group Name** is a string up to 32 characters.



Type: indicates the device type, which can be AP, Switch, or Gateway.

IP or Subnet Address: indicates the IP address of the device to be added.

RADIUS Shared Secret: indicates the RADIUS key.

Device SN: indicates the device serial number. This parameter is mandatory when the captive portal authentication method is used.

Device MAC: indicates the MAC address of the device.

4.2 Configuring an Identity Source

Local user sources (Local Account, Local Voucher, MAC and 3rd-Part Source) are supported.

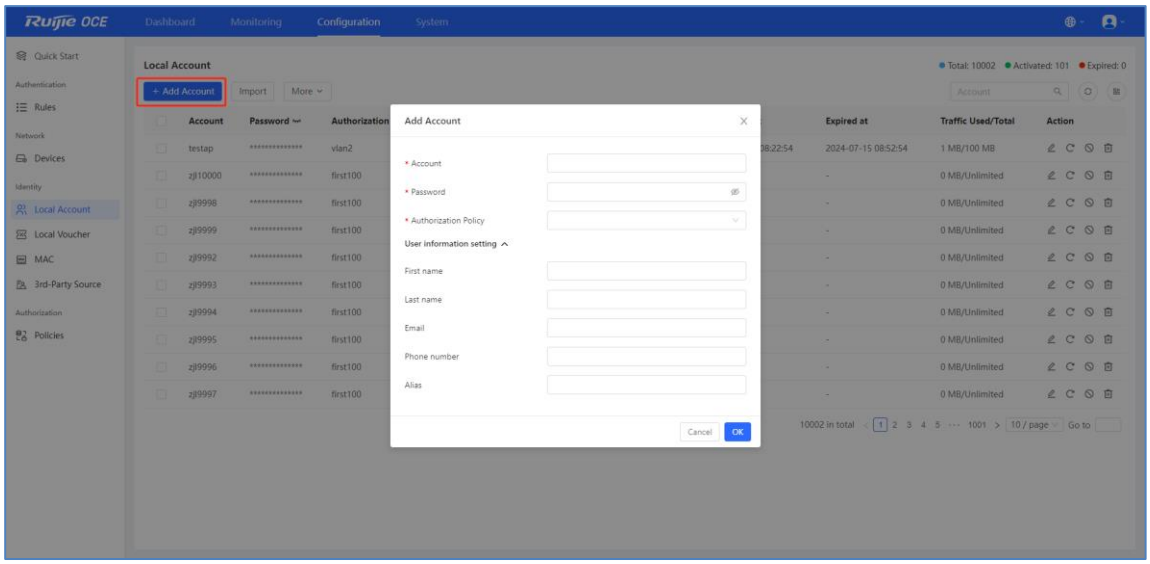
4.2.1 Local Account

A local account supports both Portal authentication and 802.1X authentication. After entering the account and password, aclient can have Internet access. Local accounts are suitable for clients who use the authentication network for a long time.

Add an Account

Choose **Configuration** > **Local Account**.

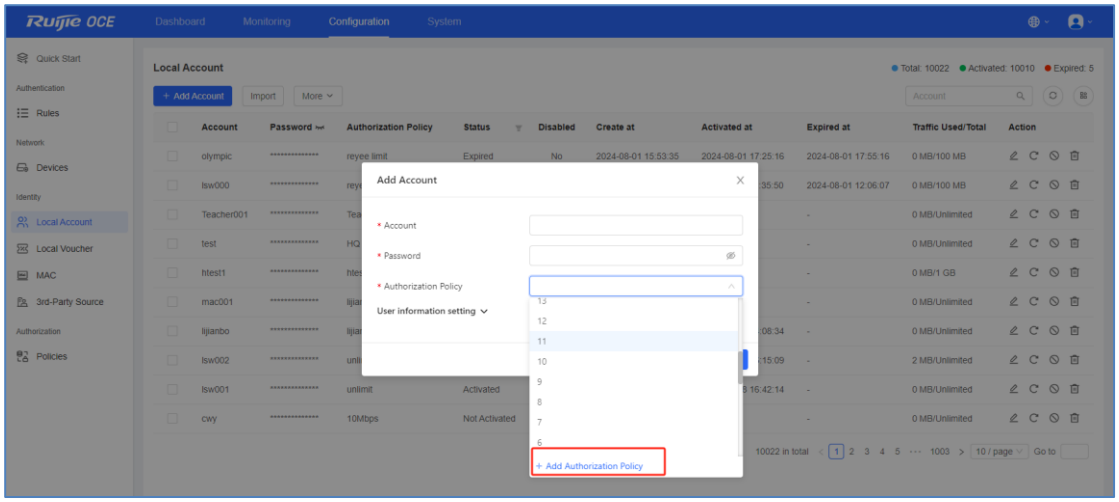
Click **Add Account** to add a local account. You can also perform batch operations such as importing, deleting, and resetting local accounts. Additionally, you can reset, disable, or delete individual local accounts.



Account: indicates the account.

Password: indicates the password.

Authorization Policy: indicates an authorization policy (Internet access policy based on user roles) from the drop-down list box. If no appropriate authorization policy is available, create a policy.



(Optional) User profile

First name: indicates the first name of the user.

Last name: indicates the last name of the user.

Email: Indicates the email address of the user.

Phone number: indicates phone number of the user.

Alias: indicates nickname of the user.

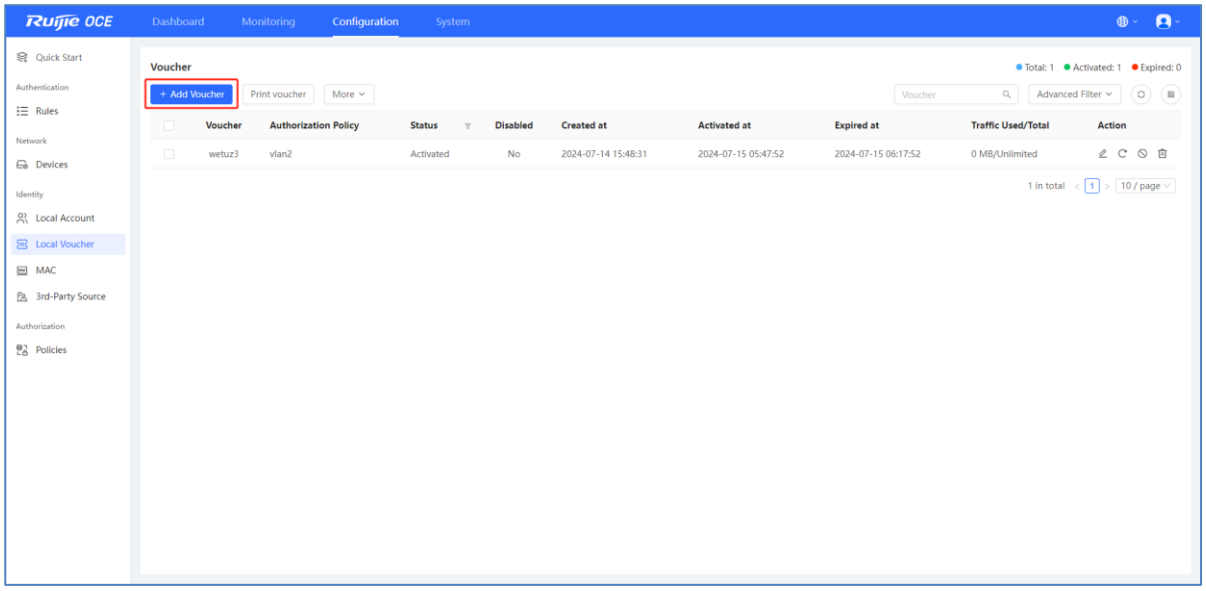
4.2.2 Local Voucher

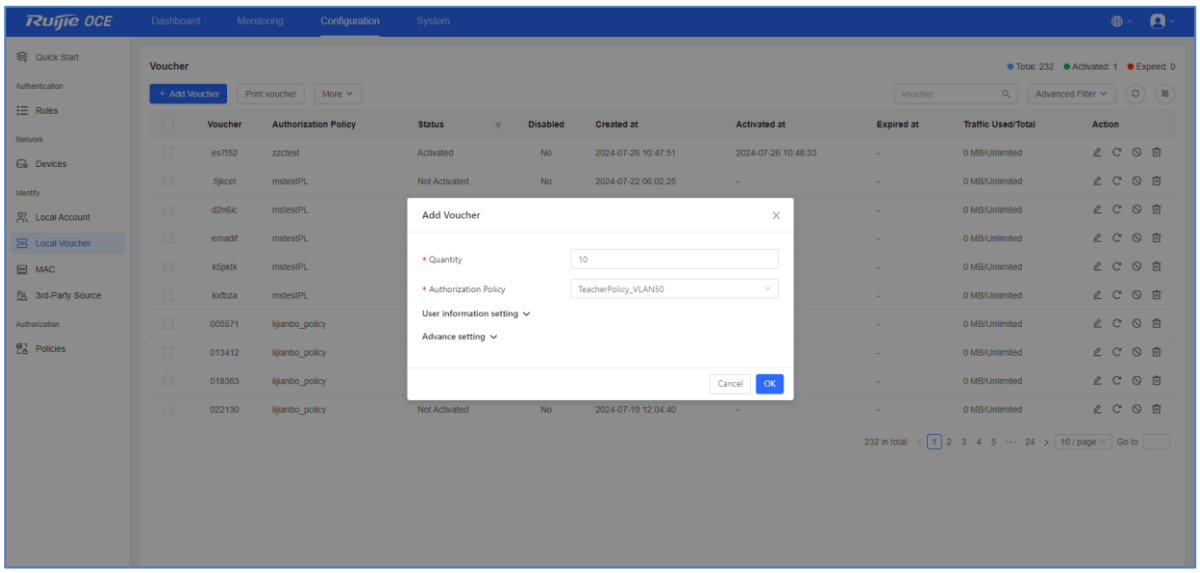
Local vouchers support Portal authentication. Clients only need a voucher to enjoy Internet access. Local vouchers are suitable for clients who need to access the Internet for a short period.

1. Adding a Voucher:

Choose **Configuration** > **Local Voucher**.

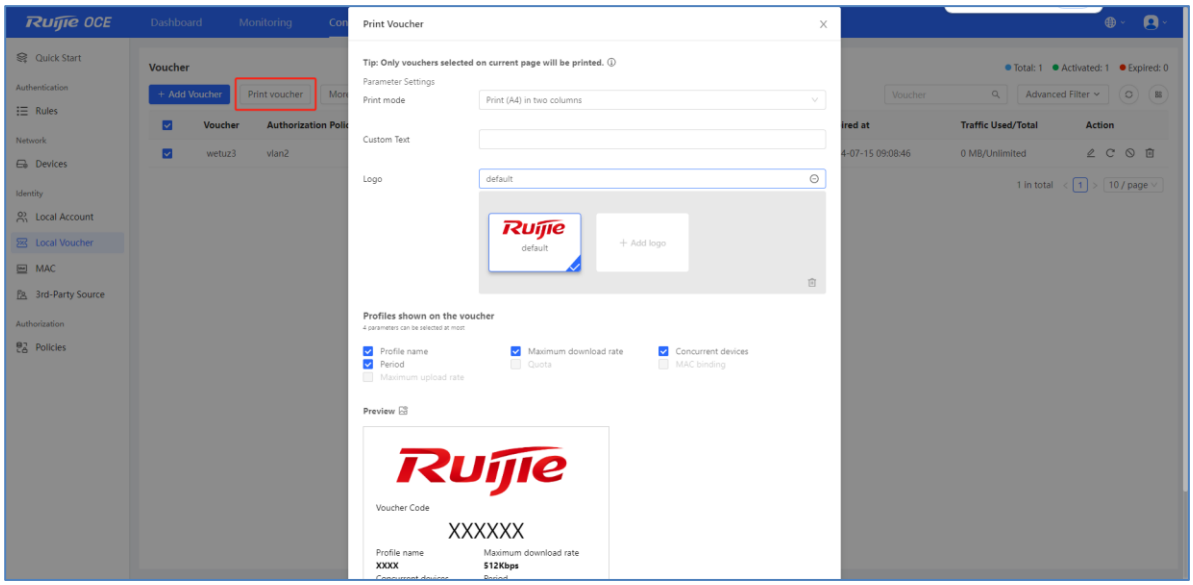
Click **Add Voucher**.





2. Printing a Voucher

The voucher format and explicit fields can be configured, and the logo can be customized. You can batch delete or reset vouchers, or reset, disable, or delete a voucher.

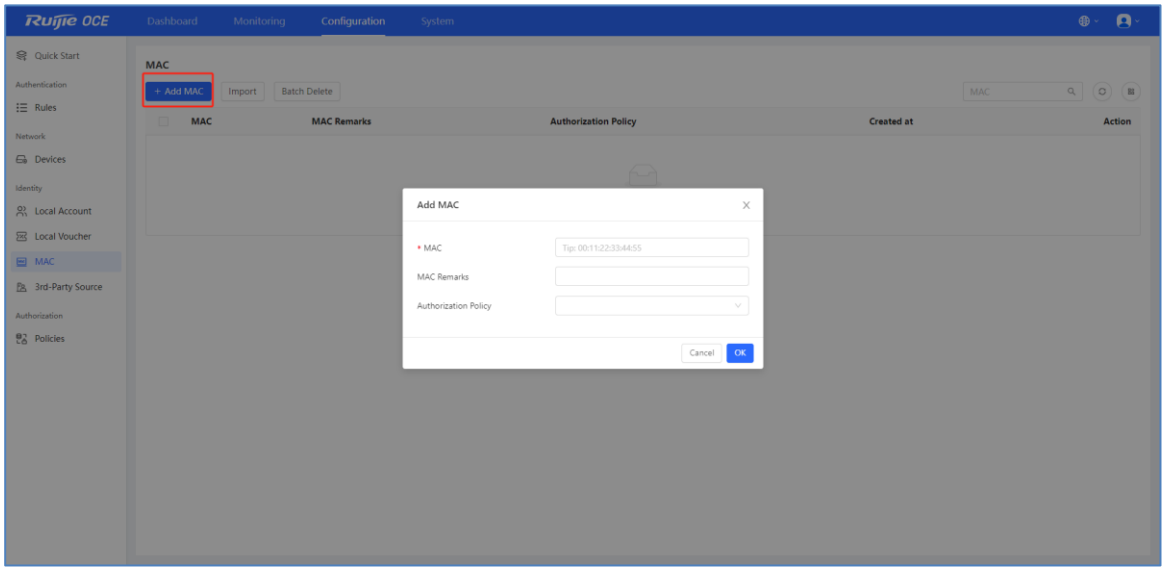


4.2.3 MAC Addresses

MAC addresses are used for MAB. Clients use MAC addresses as usernames and passwords for authentication. MAB is applicable to both wired and wireless clients, including Internet of Things (IoT) devices such as network printers and cameras.

Choose **Configuration** > **MAC**.

Click **Add MAC**.



You can batch import or delete MAC addresses.

4.2.4 Third-Party Sources

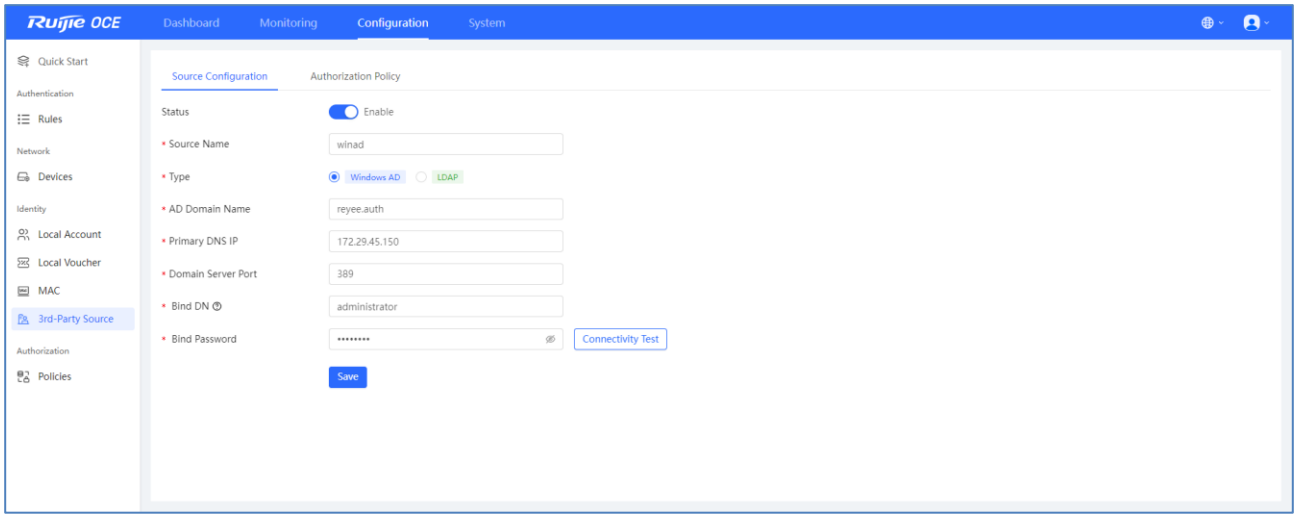
Choose **Configuration** > **3rd-Party Source.**

Windows AD and LDAP can be configured and 802.1X authentication can be performed. You can define roles and accounts of third-party sources to realize 802.1X authentication management. Ruijie OCE provides connectivity detection to check whether server information is correctly entered.

1. Configuring the AD Source

Choose **Configuration** > **3rd-Party Source** > **Source Configuration.**

Set **Type** to **Windows AD**.



Source Name: specifies the custom source name.

AD Domain Name: specifies the domain name.

Primary DNS IP: specifies the IP address of the AD domain.

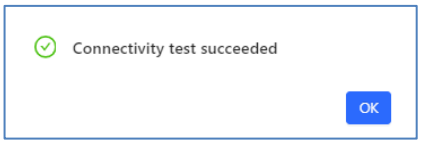
Domain Server Port: specifies the port of the AD domain.

Bind DN: specifies the administrator account of the AD domain.

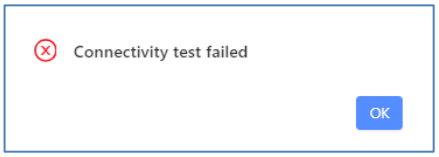
Bind Password: specifies the administrator password of the AD domain.

Click **Connectivity Test** to test the connectivity.

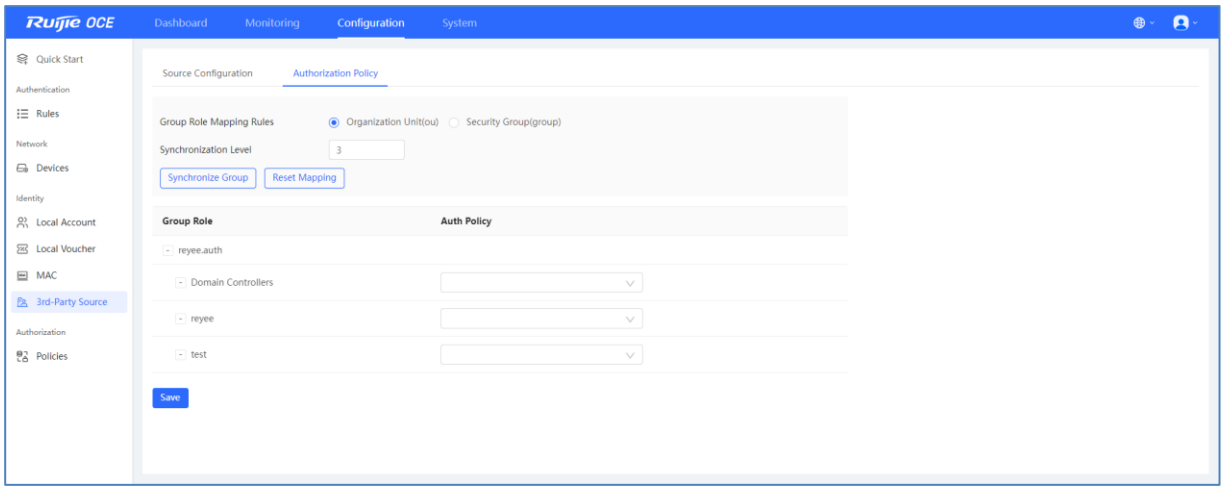
- Success



- Failure



Choose **Configuration** > **3rd-Party Source** > **Authorization Policy** to associate a group authorization policy to the identity source.



Group Role Mapping Rules: **Organization Unit(ou)** or **Security Group(group)**

Synchronization Level: specifies the synchronization group levels (1–3).

Click **Synchronize Group** to synchronize group roles based on the group type and level.

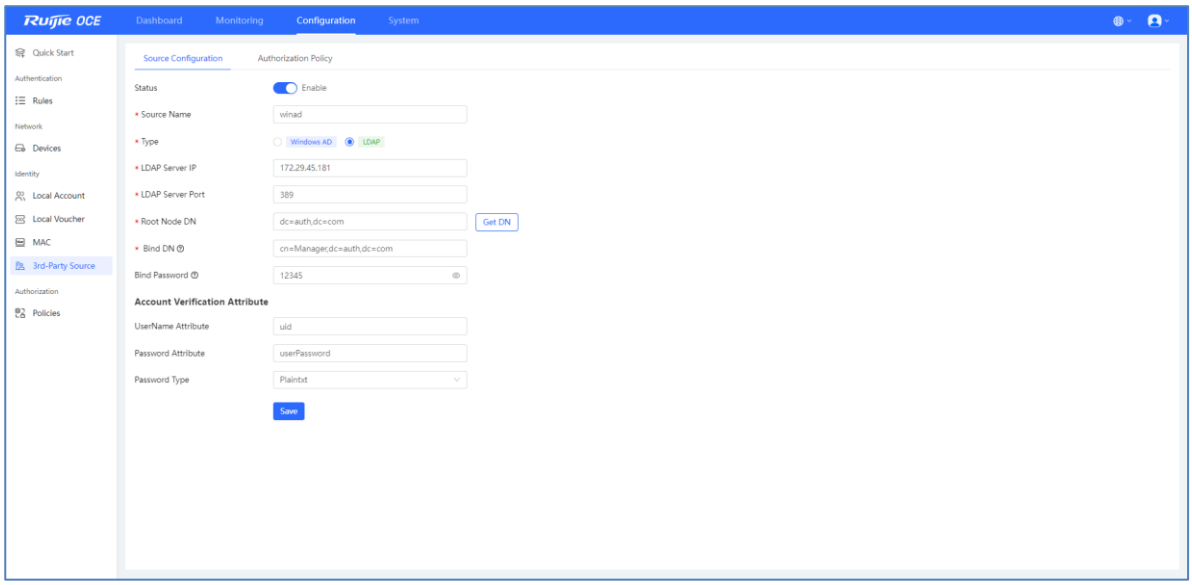
You can select an authentication policy based on the groups synchronized.

Click **Reset Mapping** to reset the selected authentication policy.

2. Configuring the LDAP Source

Choose **Configuration** > **3rd-Party Source** > **Source Configuration.**

Set **Type** to **LDAP**.



LDAP Server IP: specifies the IP address of the LDAP server.

LDAP Server Port: specifies the port number of the LDAP server. The default port number is 389.

Root DN: specifies the root node name. The root distinguished name, or root DN, is the first, or top-most, entry in an LDAP directory tree.

Bind DN: specifies the LDAP administrator username. The Bind DN is the username that will be used to do the searching and request the authentication.

Bind Password: specifies the LDAP administrator password.

UserName Attribute: specifies the authentication user name.

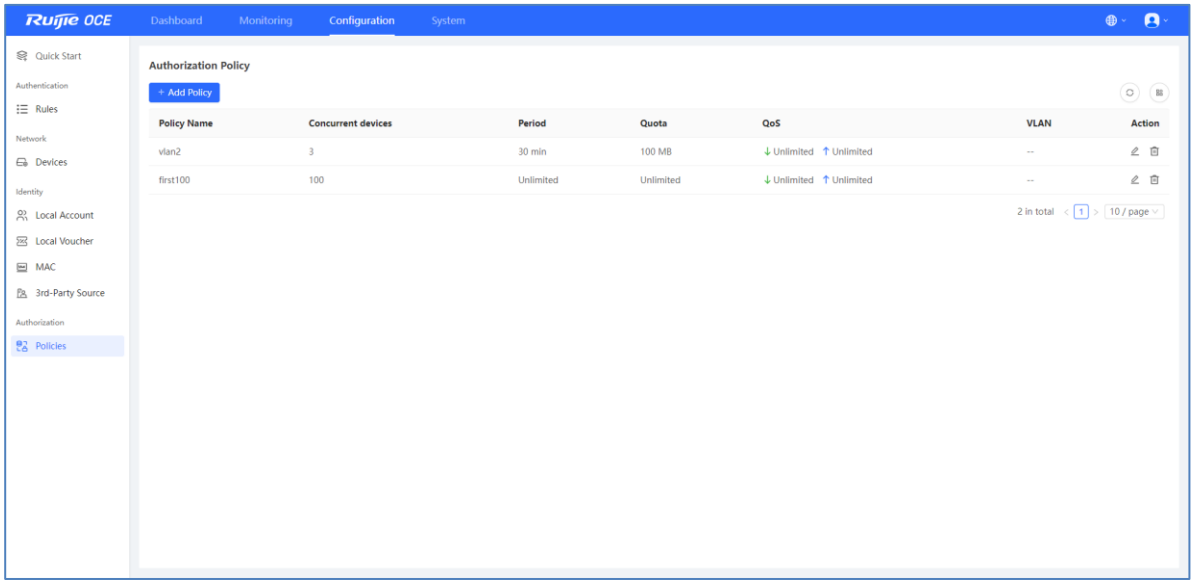
Password Attribute: specifies the authentication password.

Password Type: specifies the password type.

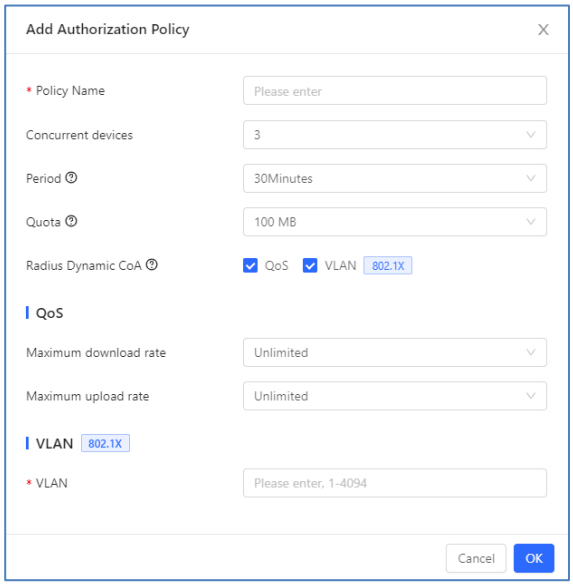
4.3 Configuring an Authorization Policy

Choose **Configuration** > **Policies**.

You can bind authorization policies of different roles with authentication accounts to control the number of concurrent online clients, available duration, traffic, uplink and downlink rates, and dynamic VLANs (used in 802.1X authentication scenarios).



Click **Add Policy** to add an authorization policy.



Policy Name: specifies the policy name.

Concurrent devices: configures the maximum number of concurrent clients supported by an account. The number of 802.1X authentication clients and Portal authentication clients are counted separately.

Period: configures the online duration of accounts. (The timer starts upon the first login of an account. It only supports Captive Portal authentication.)

Quota: configures the available traffic quota for an account. (Quota control is only supported in Ruijie AP, Reyee EG/NBR. It only supports Captive Portal authentication. Currently, traffic is detected at a 1-minute interval, which may lead to some inaccuracies in quota control.)

QoS: specifies the maximum uplink and downlink rates.

VLAN: specifies the dynamic VLAN ID in 802.1X authentication. The value range is from 1 to 4094.

4.4 Configuring Authentication Rules

You can configure 802.1X authentication and captive portal authentication rules. You only need to enter the authentication rule name, select the authentication identity source, and select the device group to which the authentication rule applies to create an authentication rule. A device group can be bound to both 802.1X authentication and Captive Portal authentication rules.

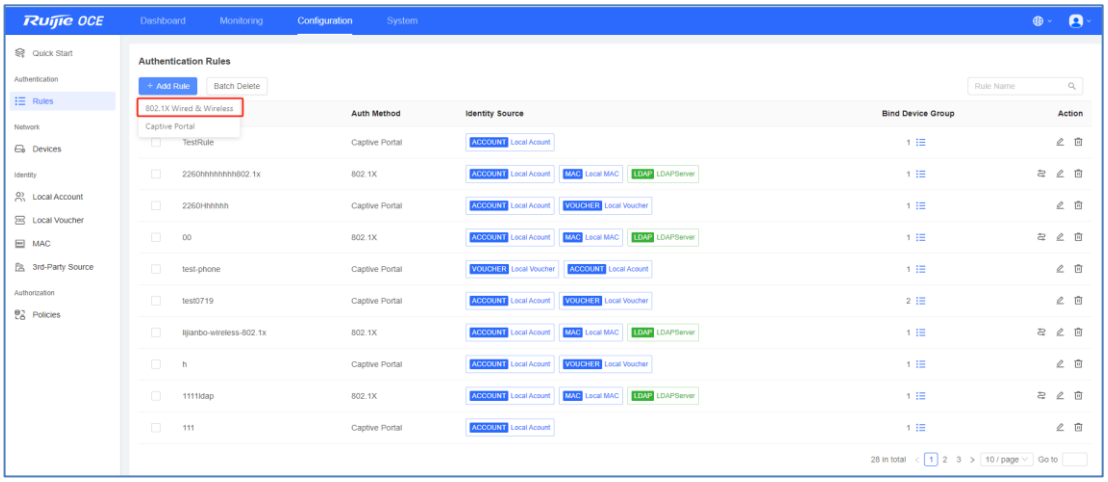
4.4.1 802.1X Authentication Rules

Choose **Configuration** > **Rules.**

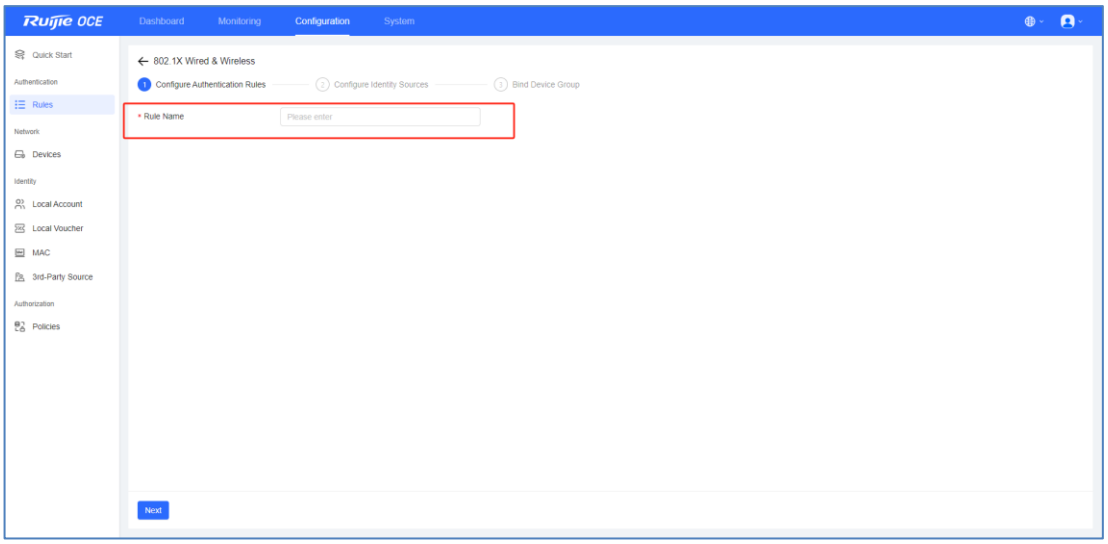
802.1X authentication supports wireless and wired connection modes. An 802.1X authentication rule can be applied to multiple device groups, but a device group can be bound to only one 802.1X authentication rule. 802.1X authentication supports three account sources: Account, Voucher, and 3rd-Party Source. The device group bound to an 802.1X authentication rule needs to be configured with correct IP address, RADIUS Shared Secret, and Device MAC. Otherwise, 802.1X authentication may fail.

1. Creating an 802.1X Authentication Rule

(1) Click **Add Rule** and select **802.1x Wired & Wireless**.



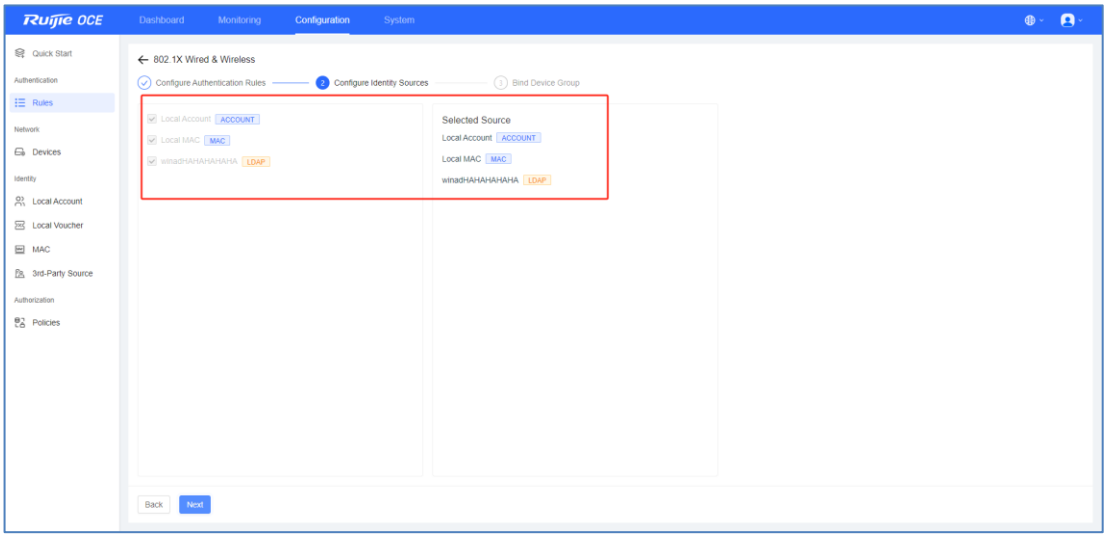
(2) Enter the rule name and click **Next**.



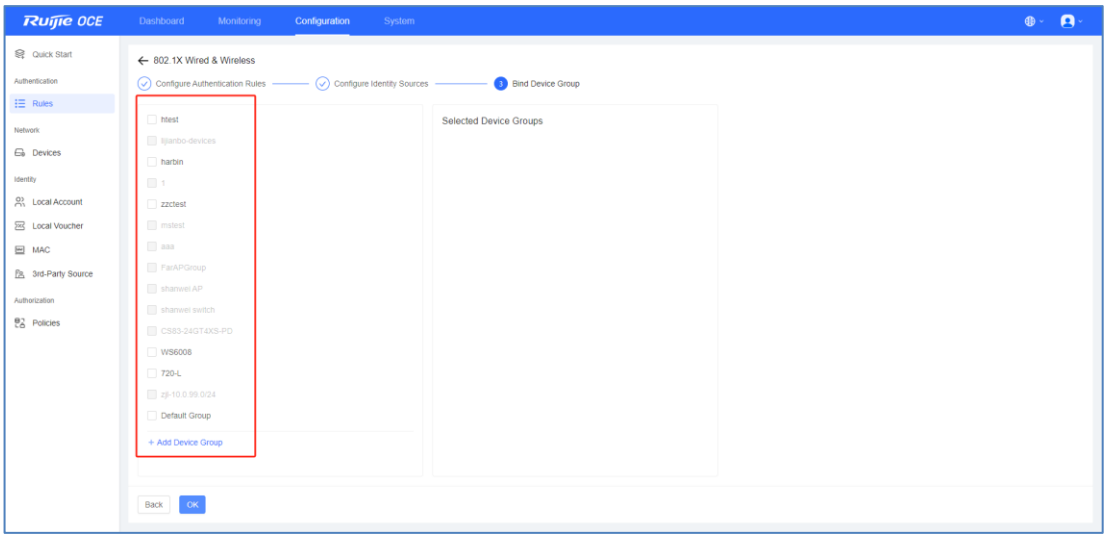
(3) Keep the default settings, and click **Next**.

Note

The 802.11 rule automatically selects all available data sources. If there are duplicate user names between a local account and a 3rd-party source, the local account prevails.



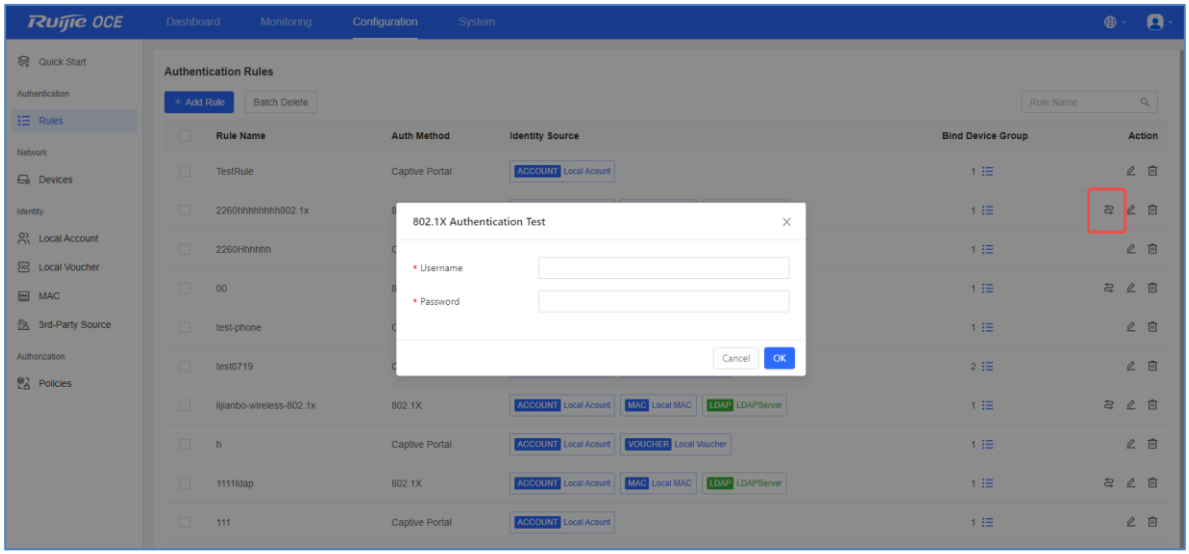
(4) Select the device group to which the authentication rule applies and click **OK**. Note that a device group bound to the 802.1X authentication rule cannot be bound to another rule.



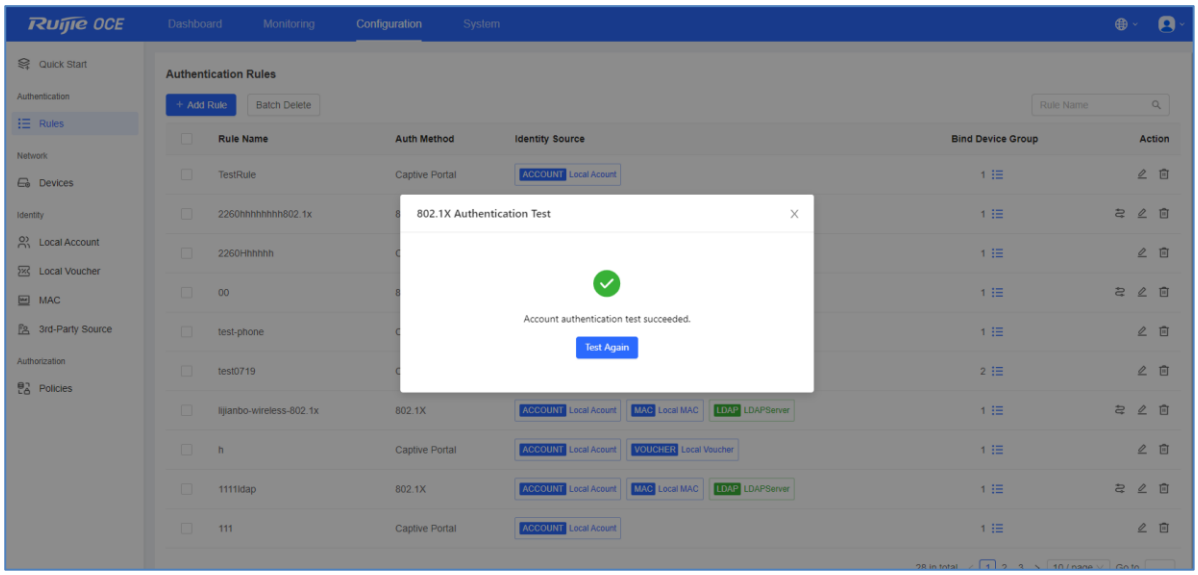
2. Performing an 802.1X Authentication Test

After 802.1X authentication rules are added, click ⇄ in the **Action** column to simulate MSCHAP authentication packets.

A local account or a third-party AD/LDAP account can be used. You can verify whether the 802.1X RADIUS response of the authentication server is normal in advance to facilitate troubleshooting and quickly determine whether the server or the device network is faulty.



Enter a username and password for a simulation test. If the system displays a test success message, 802.1X authentication on the account is successful. Otherwise, check whether the account and server configuration are correct.



4.4.2 Captive Portal Rules

The Ruijie OCE Identity Manager supports flexible portal authentication policies and integrates with Ruijie/Reyee APs and gateways. It allows for customizable pages and offers multiple authentication methods, including one-key login, vouchers, accounts, registration, and SMS.

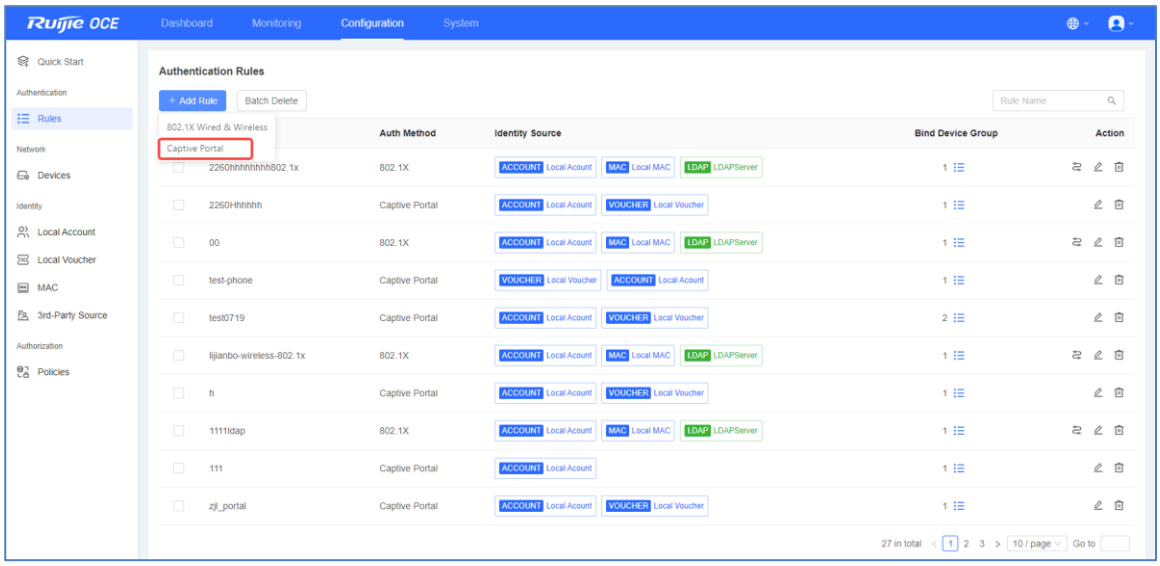
The portal supports multiple languages and advertising functions. You can easily add multiple advertising pictures or video for marketing.

Note

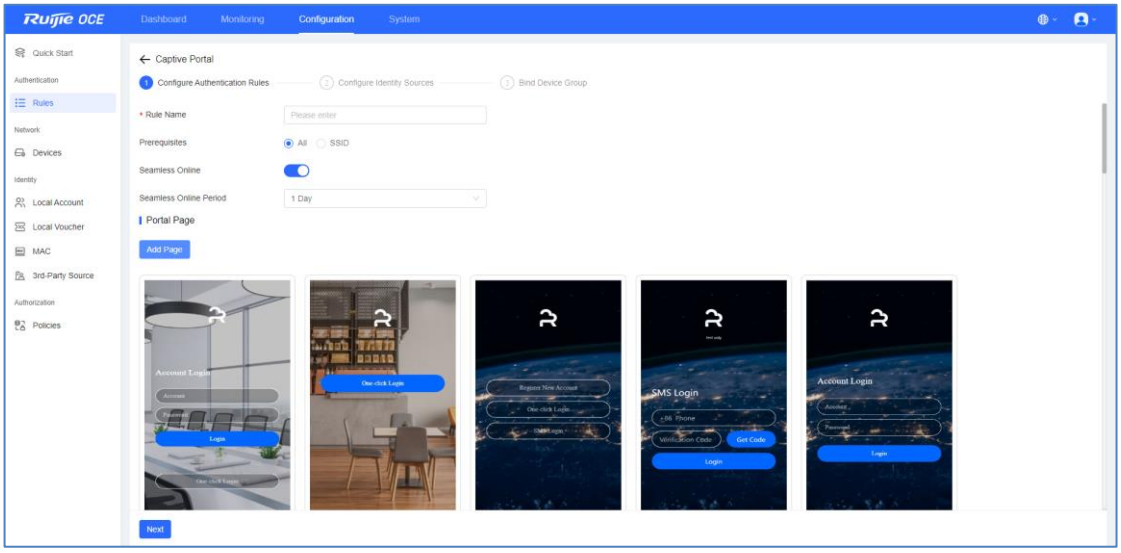
- Ruijie OCE only supports interconnection with WiFiDog Portal.
- A Captive Portal authentication rule can be applied to multiple device groups.
- A Captive Portal rule can be applied globally (multiple networks or SSIDs use the same rule) or based on SSID. One device group can be bound to only one global rule.
- Multiple SSID-based authentication rules can be set for a device group. Different SSIDs use different authentication modes and portal pages.
- If a device group is bound to a global Captive Portal rule and an SSID-based Captive Portal rule, the SSID-based Captive Portal rule prevails.

Choose **Configuration > Rules**.

Click **Add Rule** and select **Captive Portal**.

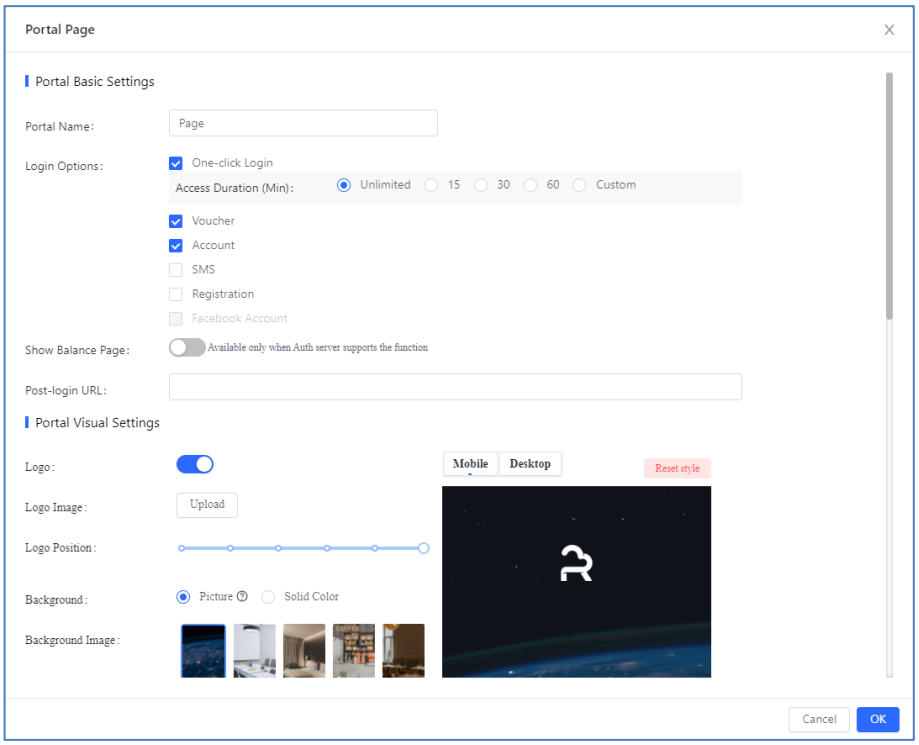


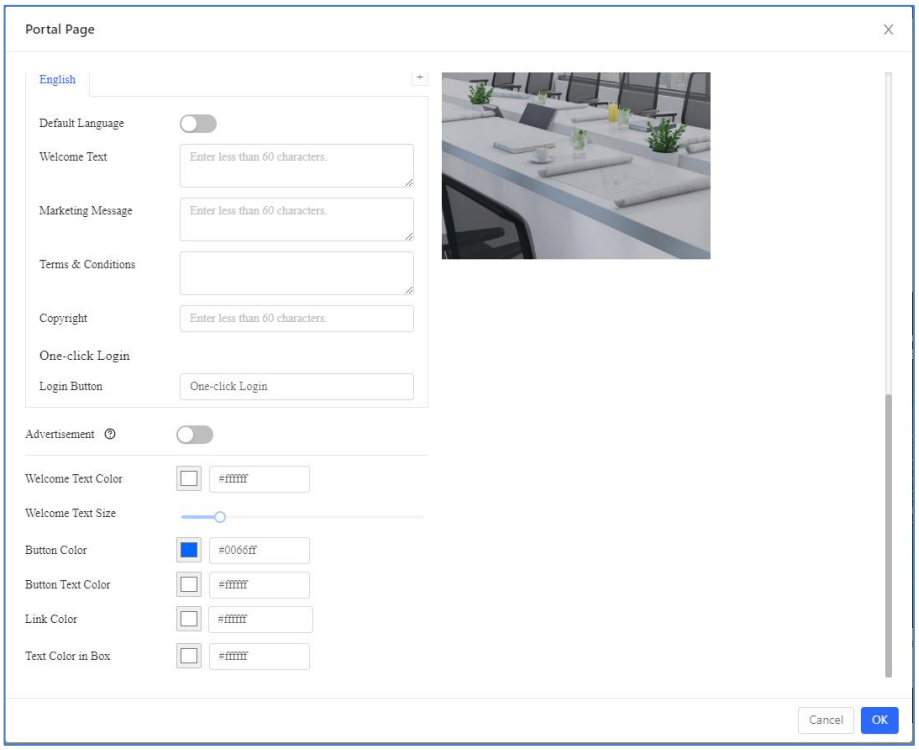
(1) Enter the rule name, enable the seamless online function, and configure the seamless online duration.



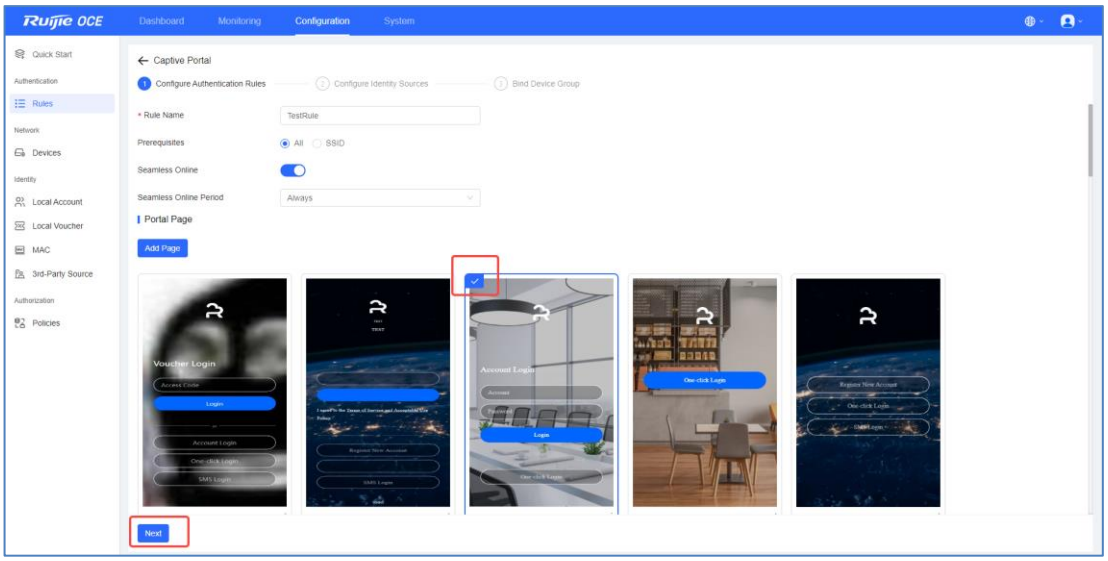
- **Seamless Online**: After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
- **Seamless Online Period**: Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.

(2) (Optional) Click **Add Page** to create a custom page and configure the Internet access authentication mode (including One-Click, Account, Voucher, SMS, and Email Registration), logo, background image, T&C Internet access disclaimer, welcome text, button text, and button color.

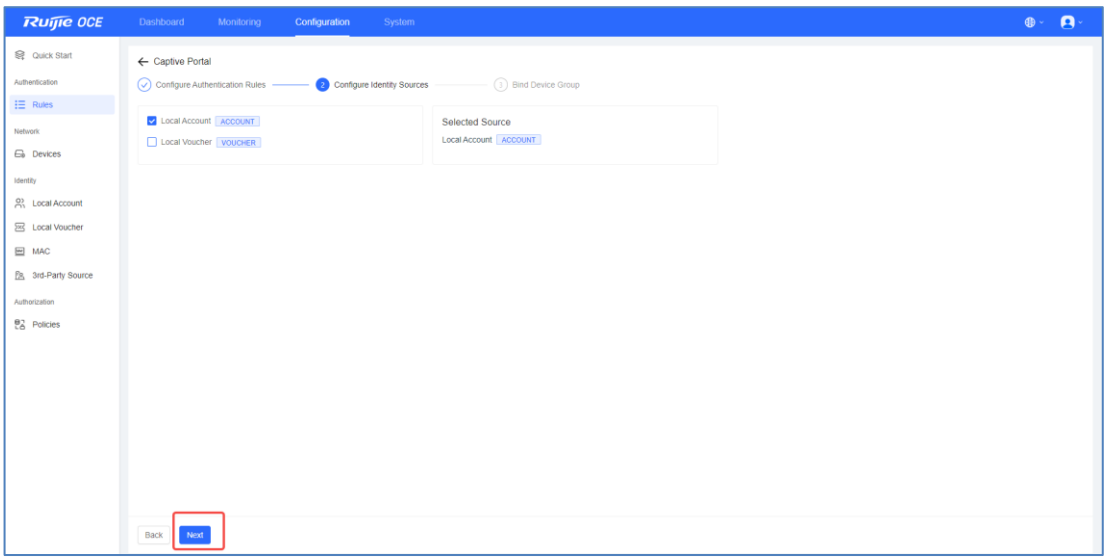




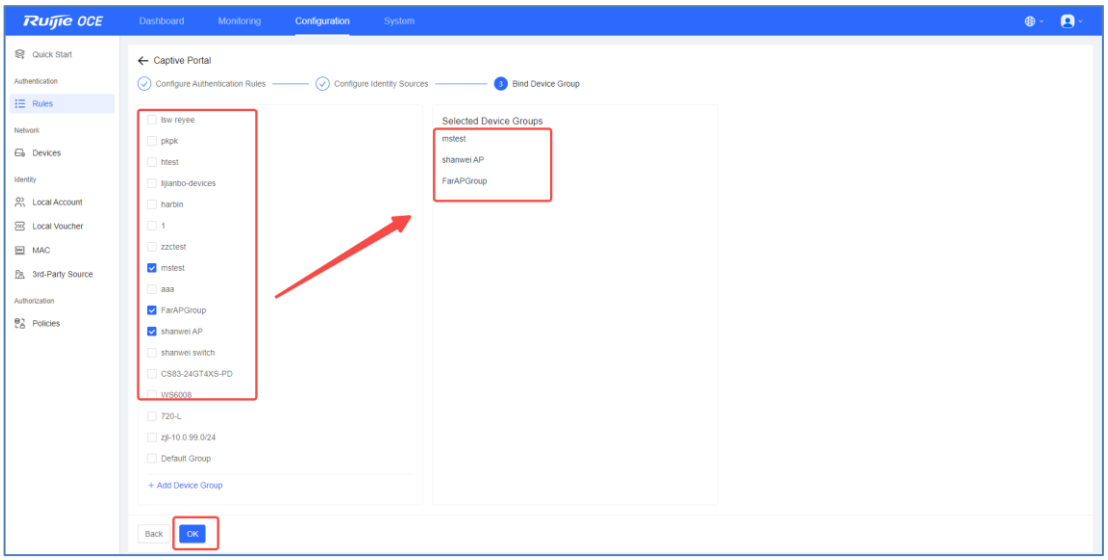
(3) Select an authentication page and click **Next**.

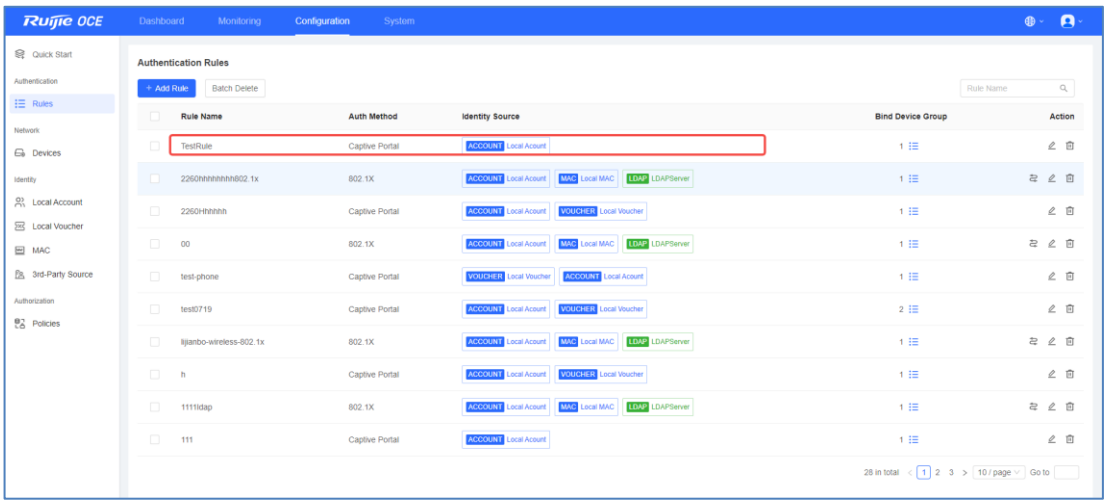


(4) Select an account identity source to be used for portal authentication. Currently, Portal authentication supports the local account and voucher (AD and LDAP identity sources will be supported in V1.1). Click **Next**.

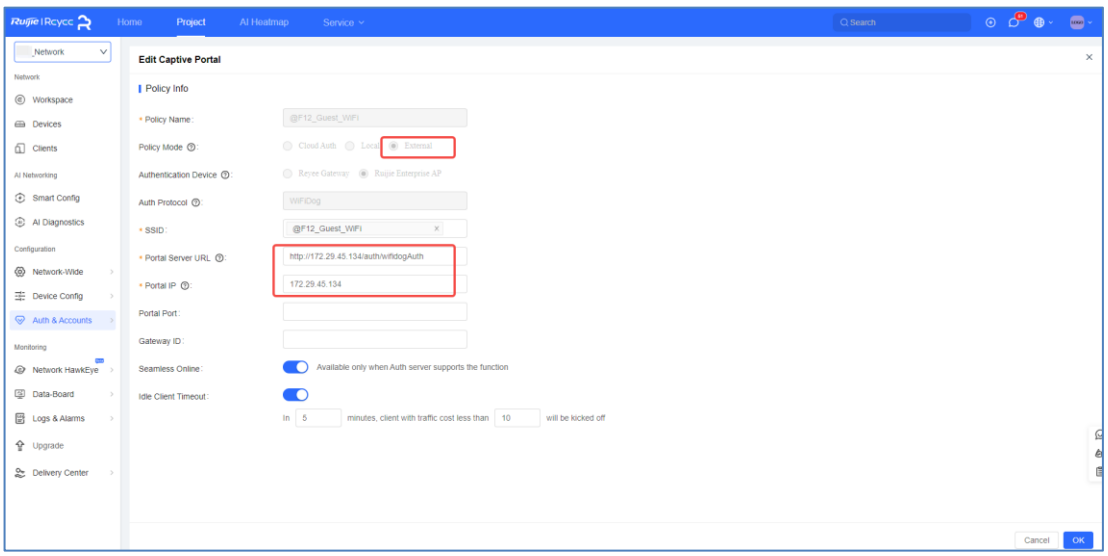


(5) Select a device group to which the Portal rule is to be applied and click **OK**. The newly created authentication rule is displayed in the rule list.





(6) To perform Portal authentication on the device interconnected with Ruijie OCE, enable WiFiDog on the device and enter the OCE server address and IP address. On Ruijie Cloud, configure external portal interconnection with the OCE software. Example: change 172.29.45.134 (IP address of the OCE) in the following figure to the IP address of a local server.

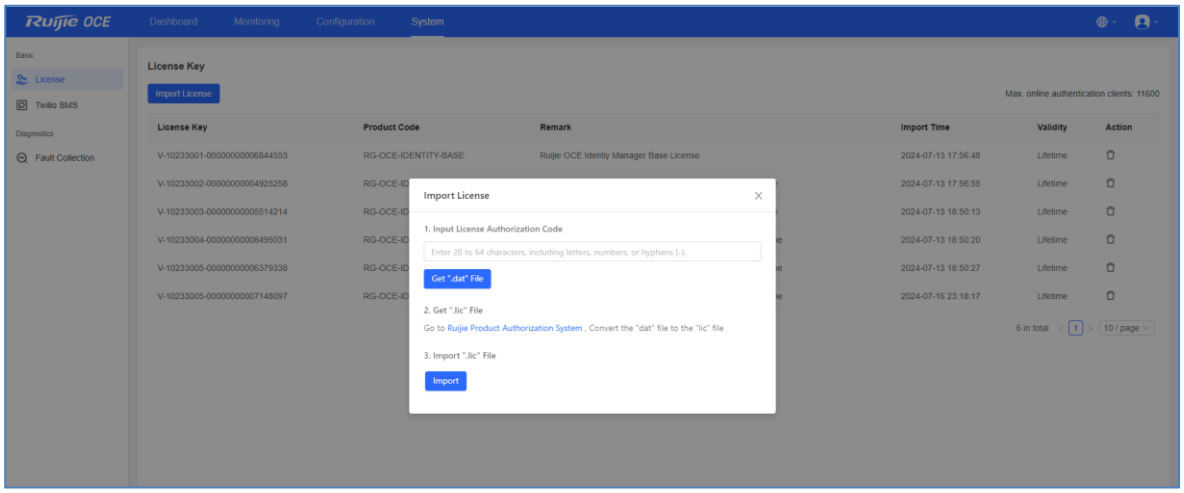


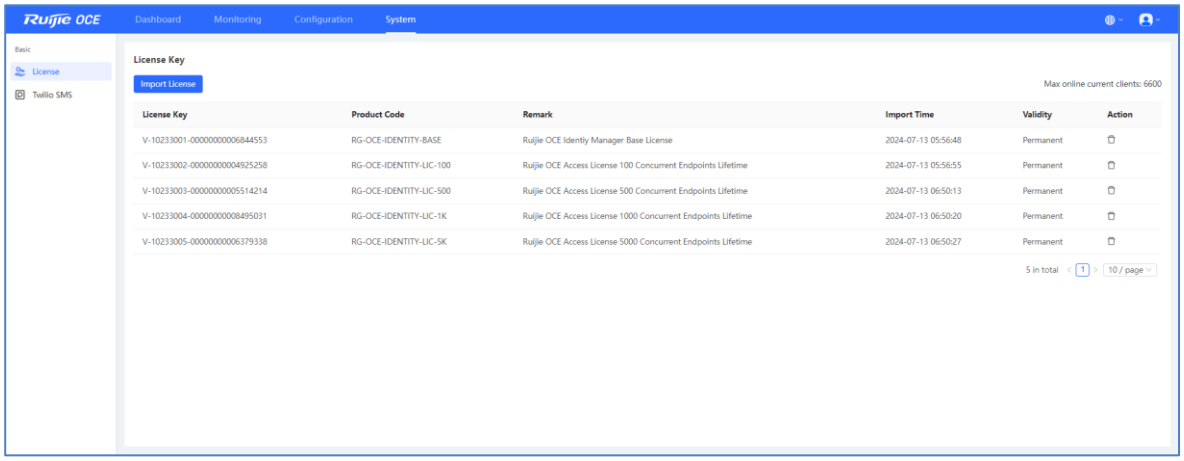
5 System

5.1 Basic

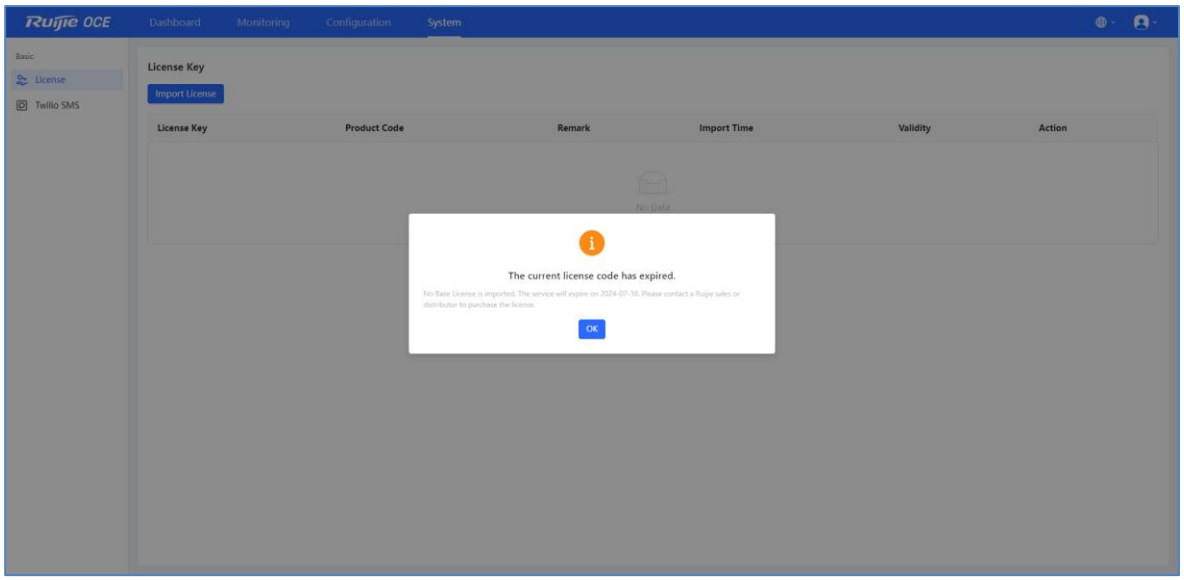
5.1.1 License

The administrator enters the purchased Ruijie OCE license authorization code to generate and download the .dat file, logs in to the Ruijie PA system to obtain the .lic file, and clicks **Import** to import the file to the OCE system.



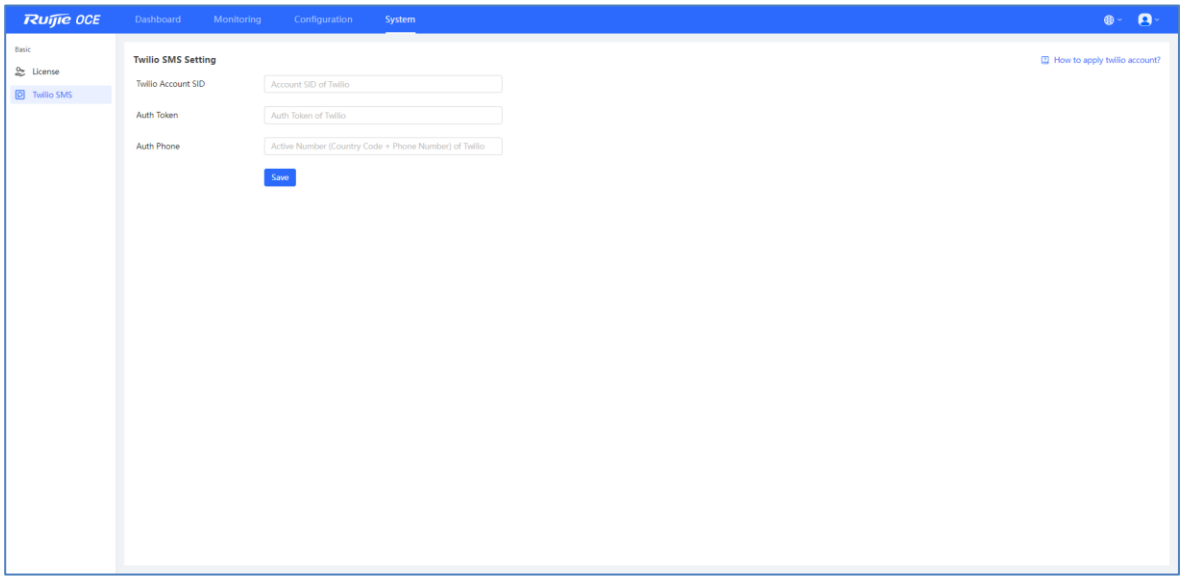


After Ruijie OCE is installed, a demo license is automatically obtained by default. The demo license supports 20 concurrent online clients and will expire in 30 days. Upon expiry, the system will become unavailable and only system license import operation can be performed.

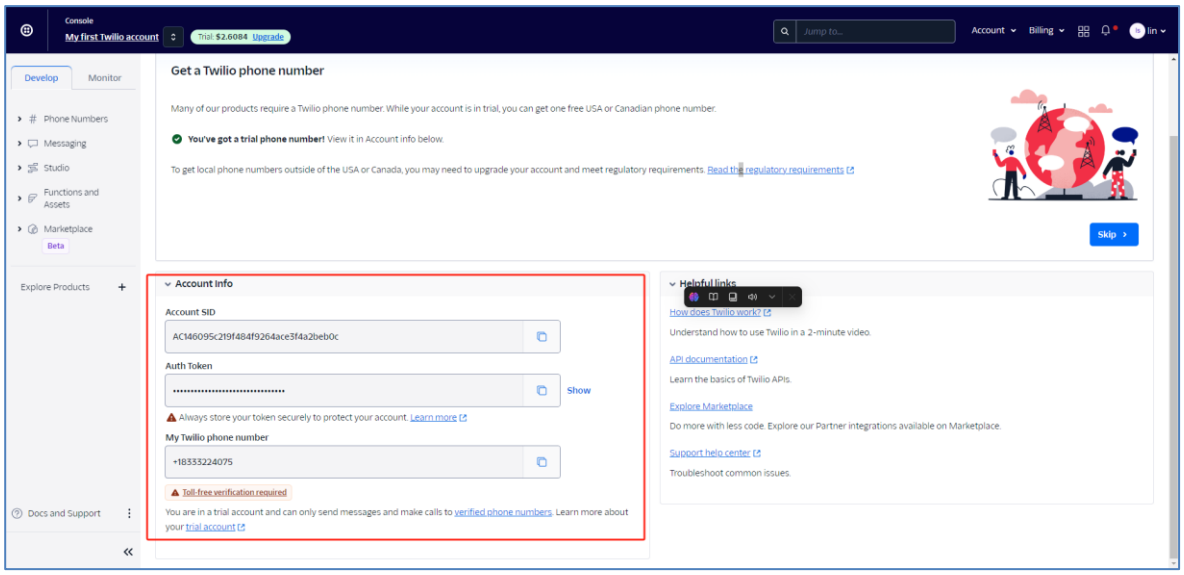


5.1.2 Twilio SMS

When Portal SMS authentication is configured, the OCE interconnects with the Twilio SMS gateway for authentication, and a Twilio SMS package needs to be subscribed.

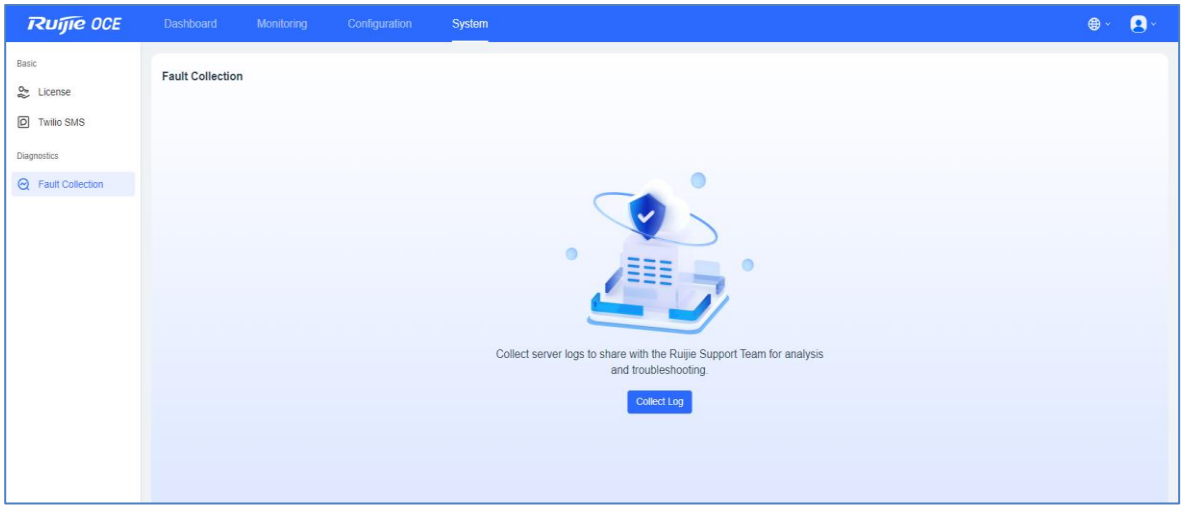


Log in https://www.twilio.com to register an account and enter the SMS gateway information shown in the figure on the SMS gateway platform.



5.2 Diagnostics

When server authentication encounters an exception or other unknown issues, you can collect system logs in one click and send them to our technical support and R&D engineers for analysis.



6 Linking Between RG-OCE NM and IM Platforms

6.1 Background

Linking the RG-OCE Network Manager (NM) platform with the RG-OCE Identity Manager (IM) platform allows users to access both platforms through single sign-on (SSO).

6.2 Procedure

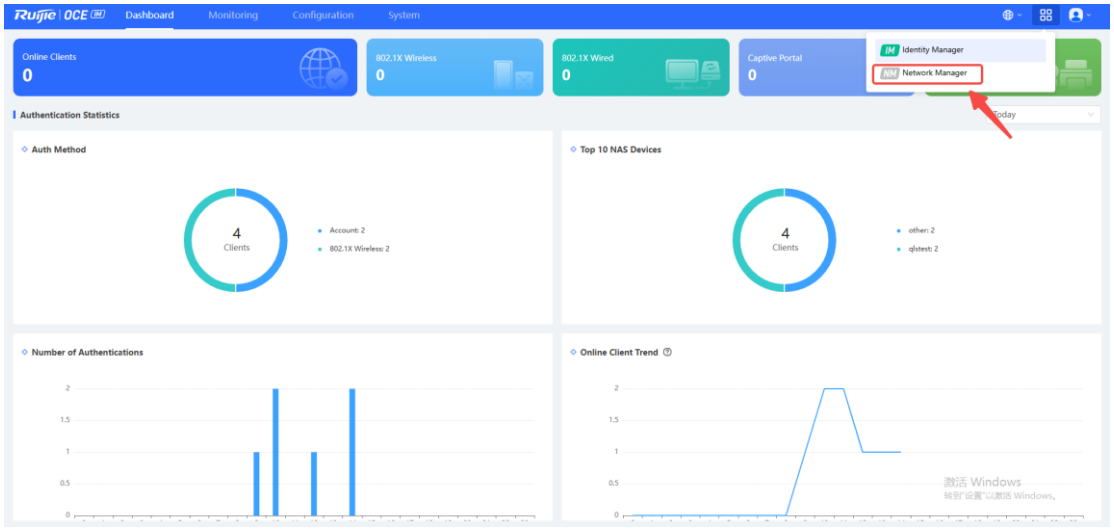
(1) Log in to the IM platform to obtain the account linking code as instructed.

(2) Then, log in to the NM platform and paste the code to complete the linking process.

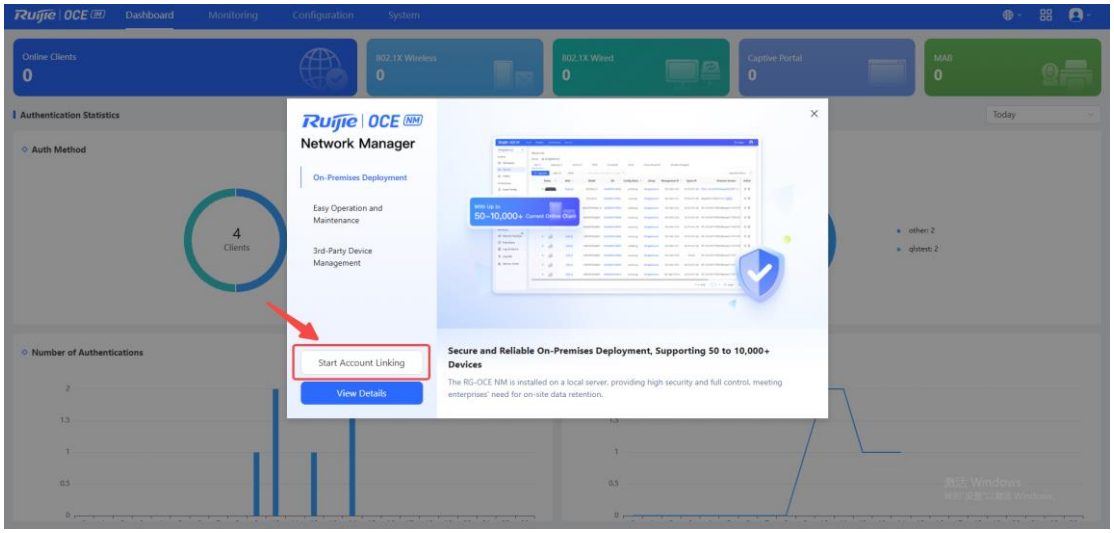
6.3 Configuration Steps

6.3.1 Operations on the IM Platform

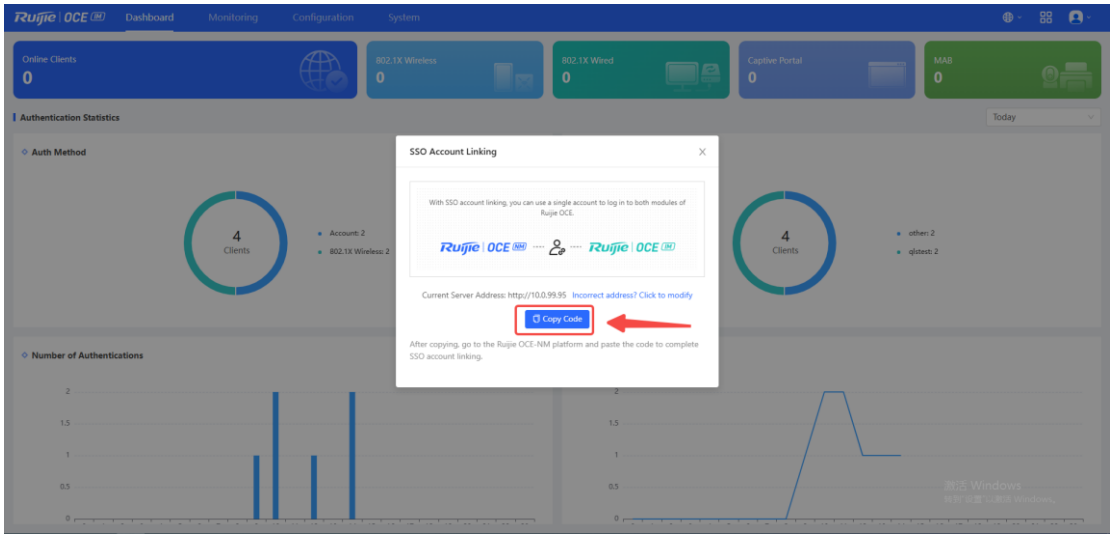
1. **Click the Switch Platform icon in the upper right corner of the IM platform and select Network Manager from the drop-down list.**



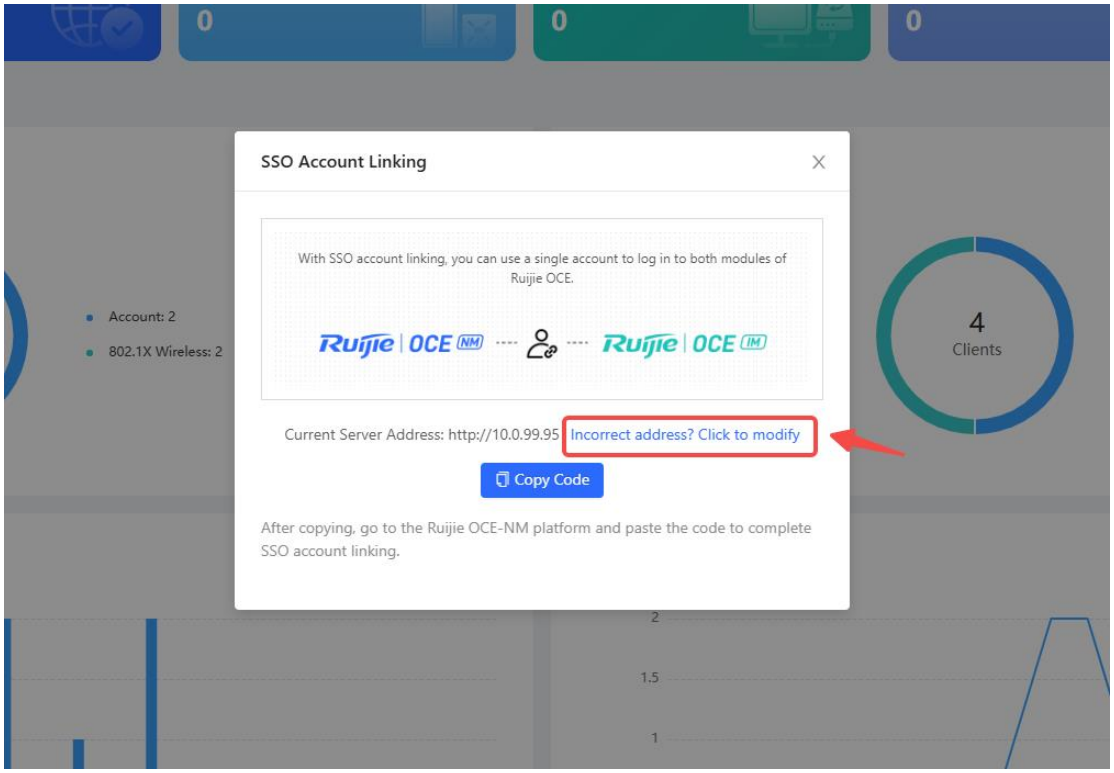
2. **On the displayed window, click Start Account Linking to start the linking process.**



3. **On the displayed SSO Account Linking window, click Copy Code to obtain the code. The system automatically copies the code to the clipboard.**

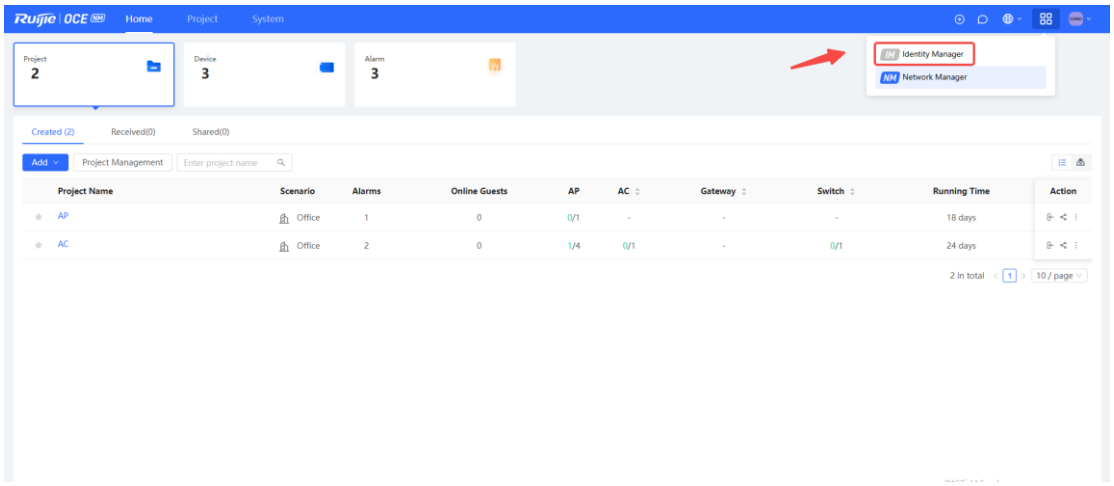


4. **If the value of Current Server Address is incorrect, click Incorrect address? Click to modify to modify the server address, as shown in the following figure. After changing the server address, click Copy Code again to obtain the latest code.**

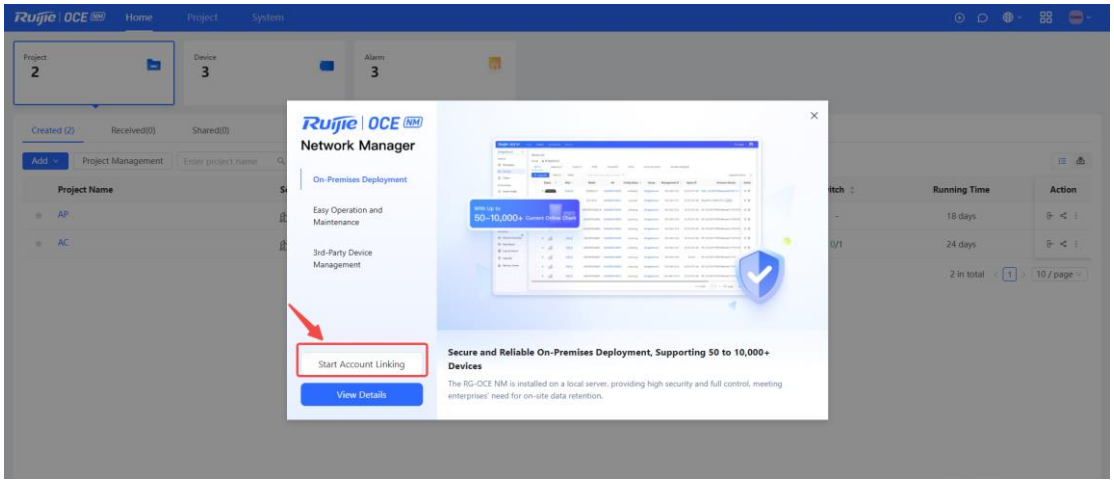


6.3.2 Operations on the NM Platform

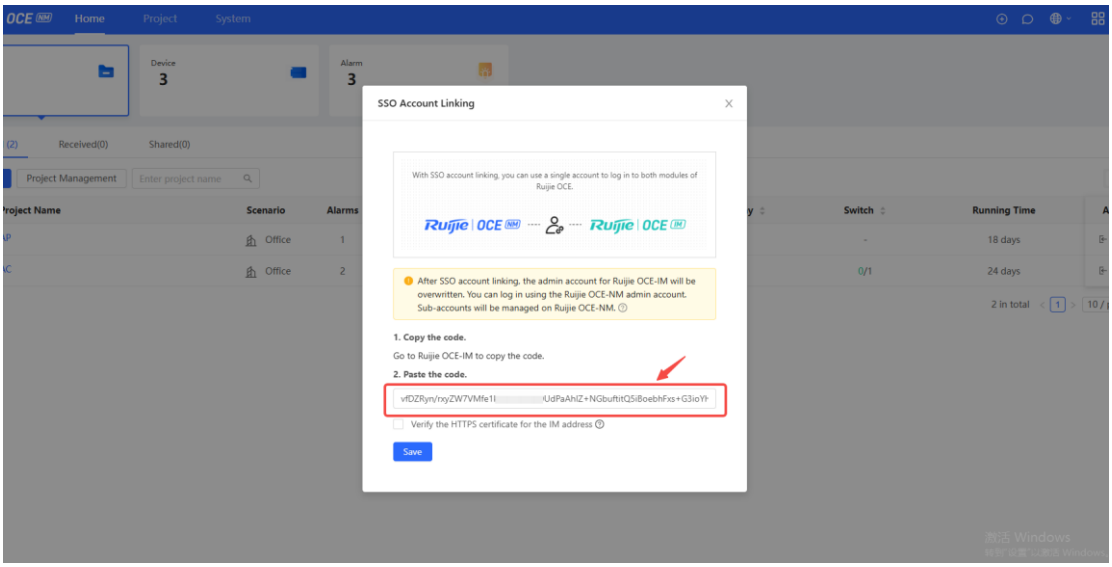
1. **Click the Switch Platform icon in the upper right corner of the NM platform and select Identity Manager from the drop-down list.**



2. **On the displayed window, click Start Account Linking to start the linking process.**



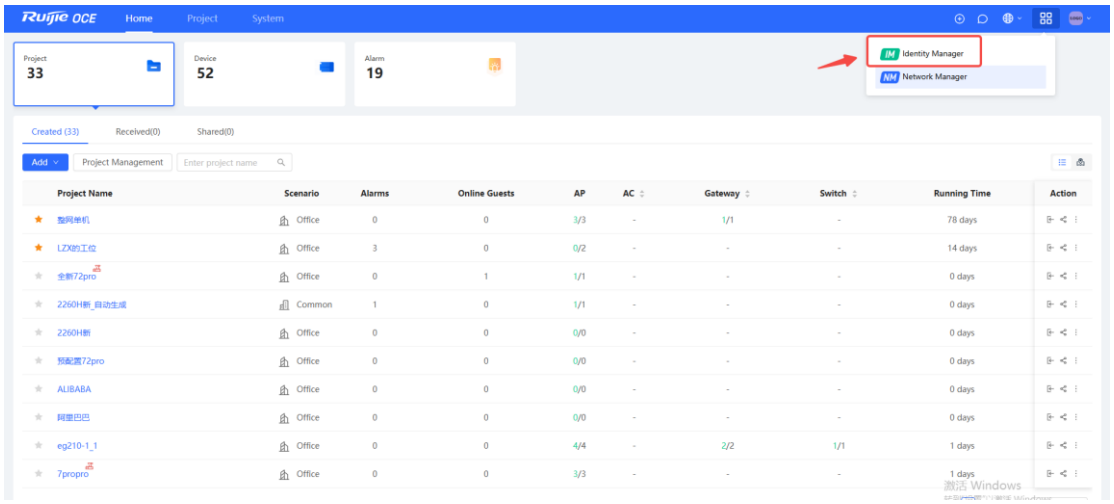
3. **On the displayed SSO Account Linking window, paste the code obtained from the IM platform to the specified input box, and click Save.**



If the IM address is a domain name bound to a formal CA certificate, you can check the "Verify the HTTPS certificate for the IM address" option.

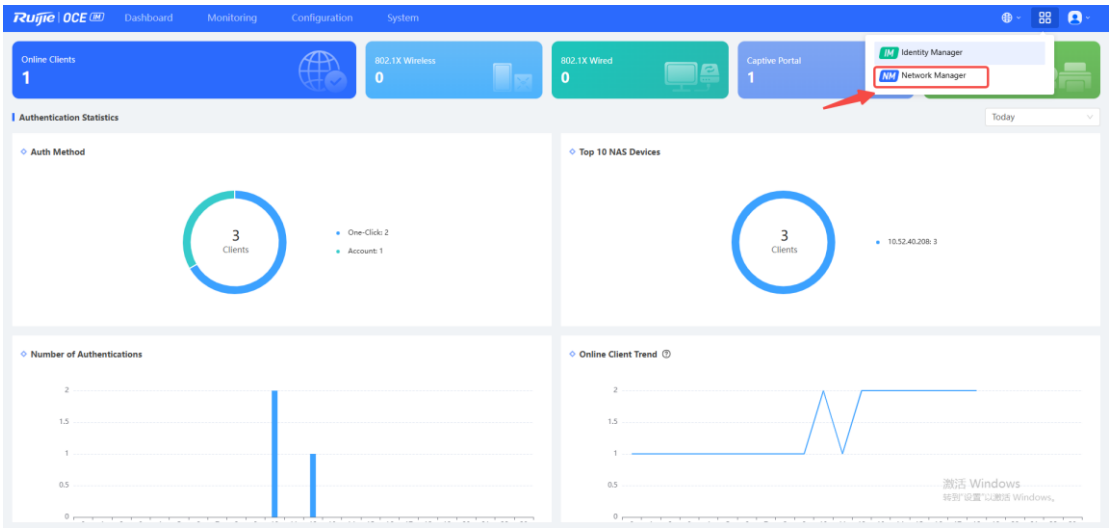
4. **Once the binding is successful, log in to the NM platform again.**

After successful login, you can click the **Switch Platform** icon in the upper right corner and select **Identity Manager** from the drop-down list to switch to the **Identity Manager** platform.



6.3.3 Switch Platform

On the IM platform, you can click the **Switch Platform** icon in the upper right corner and select **Network Manager** from the drop-down list to switch to the **Network Manager** platform.


Ruijie | OCE
Dashboard
Monitoring
Configuration
System
Online Clients
1
802.1X Wireless
0
802.1X Wired
0
Captive Portal
1
Identity Manager
Network Manager
Authentication Statistics
Today
Auth Method
3
Clients
One-Click: 2
Account: 1
Top 10 NAS Devices
3
Clients
10.52.40.208: 3
Number of Authentications
Online Client Trend