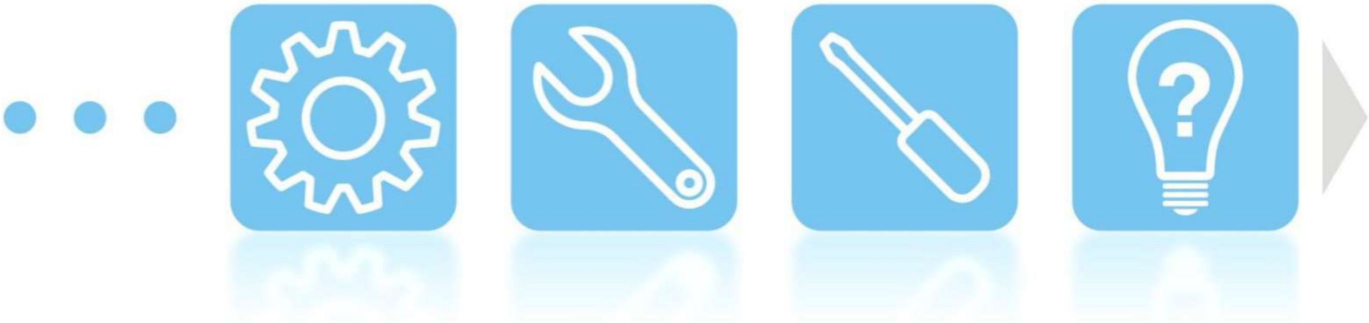


Maipu AAS Enterprise-Edition

User Manual

V5.0.1

迈普通信技术股份有限公司
www.maipu.com

Copyright

Copyright ©2017, Maipu Communication Technology Co., Ltd. All Rights Reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Maipu Communication Technology Co., Ltd.

MAIPU and 迈普 are trademarks of Maipu Communication Technology Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

The information in this document is subject to change without notice. In no event shall Maipu be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this manual or the related content on the website, even if advised of the possibility of such damage.

Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Preface

Manual Introduction

The manual mainly describes how to use Maipu AAS (enterprise edition), including three parts:

Part 1: Overview, mainly describing the basic information of the product;

Part 2: Configuration wizard, describing how to set up and complete the basic configuration of the system via one typical networking mode. You can refer to the networking mode to set up your system fast;

Part 3: Functions, you can get to know our special functions and apply to your business better.

Product Version

The product version of the manual is as follows

Product Name	Software Version
Maipu AAS(V4)	AAS-V3R2C03

Audience

This documentation is intended for:

- Commissioning engineers
- Field maintenance engineers
- System maintenance engineers

Conventions

Symbol conventions:

Format	Description
Note	An alert that contains additional or supplementary information.
Caution	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.

Format	Description
⊗**Warning**	An alert that calls attention to important information that if not understood or followed can result in personal injury or router damage.

Command conventions:

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
Italic	Italic text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

Obtaining Documentation

You can access the most up-to-date Maipu product documentation on the World Wide Web at www.maipu.cn.

Technical Support

- Technical supporting hotline: 400-886-8669
- Fax: (+8628)85148948

Documentation Feedback

You can feed back your opinions and suggestions by:

- Email: techsupport@maipu.com
- Technical hotline: 400-886-8669

Contents

PREFACE ······ 3

PART 1 OVERVIEW ······ 9

1USAGE ······ 9

2 NAMES OF PRODUCT PARTS ······ 10

3 BASIC CONFIGURATION OF THE SERVER ······ 11

PART 2 CONFIGURATION WIZARD ······ 12

4 STEP 1: INSTALLATION DEPLOYMENT ······ 13

5 STEP 2: BASIC CONFIGURATION ······ 13

5.1FAST CONFIGURATION OF AUTHENTICATION DEVICE ······ 13

5.2 FAST CONFIGURATION OF AUTHENTICATION PLATFORM ······ 16

6 STEP 3: SITE DECORATION ······ 22

6.1 HOME PAGE ······ 22

6.2DECORATE LOGIN PAGE ······ 25

6.3 DECORATE NO-PERCEPTION LOGIN PAGE ······ 26

6.4 DECORATE AD PAGE ······ 27

6.5 RELEASE THE SITE ······ 28

7 STEP 4: ADVERTISING ······ 29

8 STEP 5: INTERNET EXPERIENCE ······ 32

8.1 WIN7 CONFIGURATION AND AUTHENTICATION ······ 32

8.2 MAC SYSTEM CONFIGURATION AND AUTHENTICATION ······ 38

8.3 PORTAL AUTHENTICATION ······ 42

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

PART 3: FUNCTIONS ········ **47**

9 BASIC PLATFORM FUNCTIONS ········ **47**

9.1ORGANIZATION MANAGEMENT ········ **47**

9.2USER & AUTHORITY ········ **50**

9.3 LOG MANAGEMENT ········ **54**

9.4 SYSTEM CONFIGURATION ········ **55**

9.4.1 LICENSE ········ 56

9.4.2 PASSWORD POLICY CONFIGURATION ········ 57

9.5 SERVICE MANAGEMENT ········ **58**

9.6 HA CONFIGURATION AND MANAGEMENT ········ **59**

9.7 BACKUP, RECOVER AND DUMP ········ **59**

10 AUTHENTICATION PLATFORM FUNCTIONS ········ **64**

10.1ONLINE USER ········ **64**

10.2 BASIC CONFIGURATION ········ **64**

10.2.1USER AND USER GROUP ········ 65

10.2.1.1 User management ········ 65

10.2.1.2 User group management ········ 69

10.2.2EXTERNAL AUTHENTICATION SOURCE ········ 69

10.2.3DEVICE MANAGEMENT ········ 80

10.2.4CERTIFICATE MANAGEMENT ········ 84

10.2.5SMS POLICY ········ 85

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

10.2.6SYSTEM CONFIGURATION 90

10.2.7 ERROR CODE QUERY 92

10.3 PUSH POLICY 93

10.4 AUTHENTICATION CONFIGURATION 95

10.4.1 AUTHENTICATION POLICY 96

10.4.2 INTELLIGENT BINDING 98

10.4.3 BLACK/WHITE LIST 101

10.5 AUTHORIZATION POLICY 103

10.5.1 DURATION POLICY 103

10.5.2 AUTHORIZATION POLICY 107

10.6 LOGS 112

10.6.1 USER LOGS 112

10.6.2 GUEST QR CODE AUTHENTICATION AUDIT 114

11 WIFI MARKETING SYSTEM 115

11.1 SITE DECORATION 115

11.2 AUTHENTICATION CONFIGURATION 126

11.2.1 SMS AUTHENTICATION 126

11.2.2 INBUILT ACCOUNT AUTHENTICATION 129

11.2.3 NO-PERCEPTION AUTHENTICATION 130

11.2.4 AUTHENTICATION-FREE MODE 131

11.2.5 SECURITY AUTHENTICATION 132

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

11.2.6 AUTHORIZATION QR CODE AUTHENTICATION 134

11.3 ADVERTISING 135

11.3.1 ADVERTISEMENT LIST 135

11.3.1.1 Add an Advertisement 136

11.3.1.2 Query the Advertisement 140

11.3.1.3 Get the Advertisement Offline 141

11.3.1.4 Edit the Advertisement 141

11.3.1.5 Get the Advertisement Online 142

11.3.1.6 View the Advertisement 143

11.3.1.7 Delete the Advertisement 144

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

Part 1 Overview

1Usage

The enterprise-version software of Maipu network access system provides the user ID authentication, user access authorization, WiFi online marketing, service data analysis and other functions, applicable to 3G/4G, WLAN, wired network, and other user access scenarios. Combined with Maipu AC, AP, ISG, and other products, it provides the integrated solution of the user authentication and WiFi marketing for the enterprise.

The enterprise-version software of Maipu network access system supports the current mainstream authentication technologies, including PPP authentication, 802.1X authentication, web authentication, and so on, and supports the IMSI information binding of the SIM card in the 3G/4G access, SSID binding in the WLAN scenario, IP address delivering, and other specifical authentication binding functions.

The enterprise-version software of Maipu network access system provides the rich industry templates, helping the enterprise create the micro portal fast, and rapidly promoting the enterprise brand image. The platform provides the self-service marketing function for the user, allowing customers to quickly promote hot products and preferential information.

The enterprise-version software of Maipu network access system provides SMS, authentication-free, and other authentication modes, solving the problem of fast accessing Internet for the user, so that more users can access Internet conveniently. At the same time, accumulate more users for enterprises, and expand the subsequent marketing value.

The enterprise-version software of Maipu network access system provides an integrated solution of user identity authentication and WiFi online marketing, which can meet the requirements of the user for different application scenarios.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

2 Names of Product Parts

System	**Description**
Basic platform	The basic platform provides the functions of organization management, user&authority, log and license management for the user.
Marketing platform	Provide site generating, advertising, and site display service.
Authentication platform	Provide user access control authentication, authorization, and so on.

copyright©2016 迈普通信技术股份有限公司，保留所有权利

3 Basic Configuration of the Server

Server CPU	Intel Xeon(R) 3.1GHz 4 core above
Server memory	>=16G
Hard disk space of the server	>=500G
Server network card	Gigabit dial network cards
Operation system	SLES-11-SP3(x86_64)

copyright©2016 迈普通信技术股份有限公司，保留所有权利

Part 2 Configuration Wizard

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

4 Step 1: Installation Deployment

Refer to *Maipu Network Access Authentication System Installation Manual V5.0.1*.

5 Step 2: Basic Configuration

5.1Fast Configuration of Authentication Device

This chapter mainly describes the basic configuration of the authentication on S3320. For the other configurations of S3320, refer to the configuration manual of S3320.

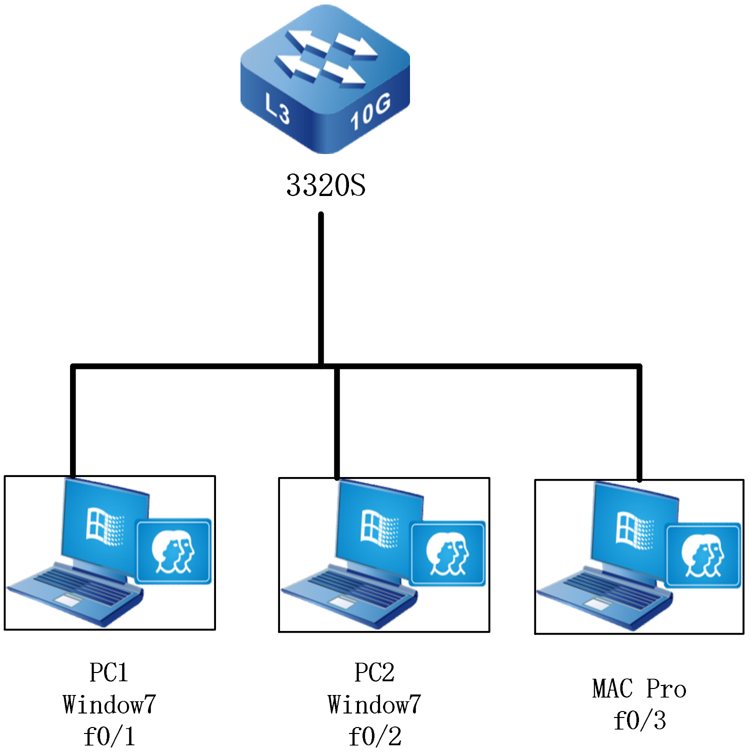
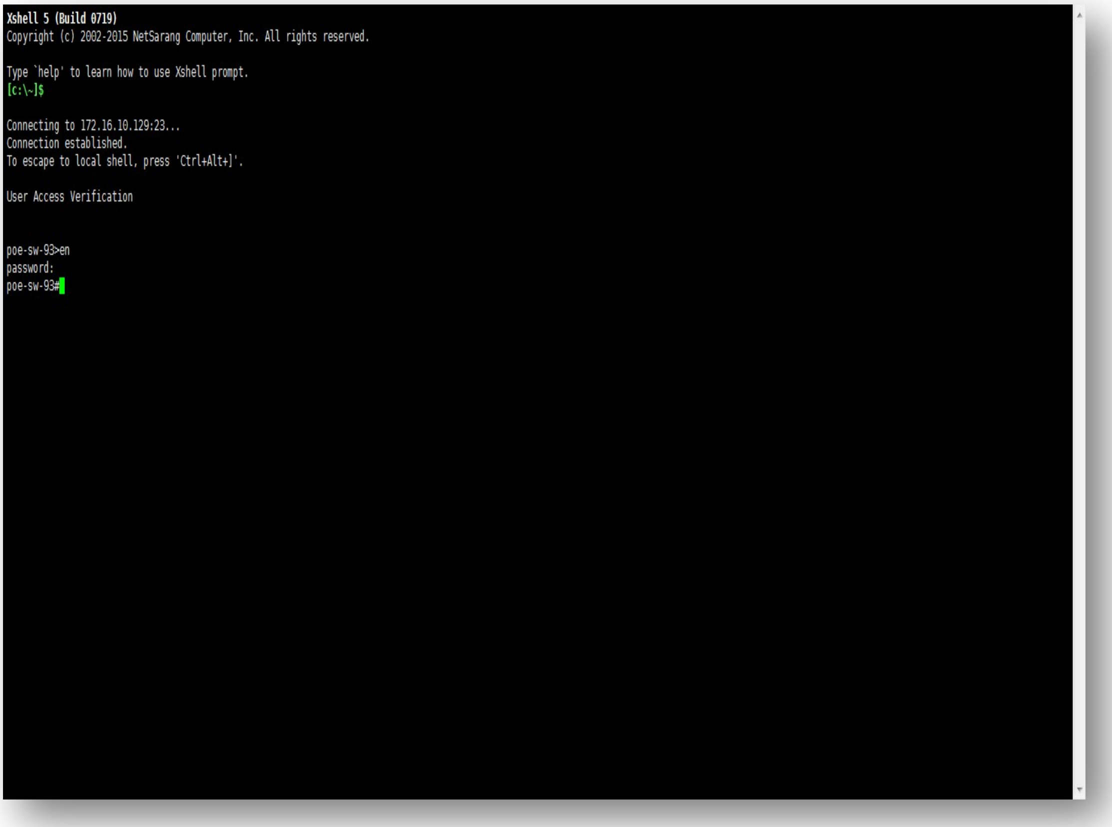


Figure 5-1-1

Step 1: Log into S3320 via the serial port, as shown in Figure 5-1-2.

All Rights Reserved



```
Xshell 5 (Build 0719)
Copyright (c) 2002-2015 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.
[c:\~]$

Connecting to 172.16.10.129:23...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

User Access Verification


poe-sw-93>en
password:
poe-sw-93#
```

Figure 5-1-2 Enter S3320 management interface

Step 2: Configure the authentication server for S3320, as follows:

```
poe-sw-93#conf t
```

```
poe-sw-93(config)#radius-server host 172.16.10.115 auth-port 1812 acct-port 1813 priority 0 key 0 admin
```

"172.16.10.115" is the IP address of the AAS server. If it is the HA deployment mode, it is necessary to configure the virtual IP address. "admin" is the authentication key. By default, fill in admin for both.

Enable the AAA authentication, as follows:

```
aaa new-model

aaa authentication login wen none

aaa authentication connection default radius

aaa accounting update periodic 1

aaa accounting connection default start-stop radius
```

If the uplink port of S3320 is configured with dhcp server, it is necessary to add the corresponding DHCP configuration, as follows:

1. Global configuration

```
dhcp-snooping
```

2. Enable the dhcp configuration on the uplink port of S3320

```
dhcp-snooping trust
```

3. Enable the access port of the terminal

```
dot1x authorization ip-auth-mode dhcp-server
```

If the PC is configured with IP address, do not need to enable the DHCP configuration.

Step 3: As shown in Figure 5-1-1, the access terminal is PC1 (Win7 system), and it is necessary to enter port 1 of S3320 to configure the following command:

```
poe-sw-93#conf t

poe-sw-93(config)#interface gigabitethernet 0/1

poe-sw-93(config-if-gigabitethernet0/1)#dot1x port-control enable

poe-sw-93(config-if-gigabitethernet0/1)#dot1x timeout quiet-period 1

poe-sw-93(config-if-gigabitethernet0/1)#dot1x eap-relay enable
```

By default, PC1 is configured with IP address.

Step 4: As shown in Figure 5-1-1, the access terminal is MAC Pro (Apple system), and it is necessary to enter port 3 of S3320 to configure the following commands:

```
poe-sw-93#conf t

poe-sw-93(config)#dhcp-snooping

poe-sw-93(config)#interface gigabitethernet 0/2

poe-sw-93(config-if-gigabitethernet0/2)#dot1x authorization ip-auth-mode dhcp-
server

poe-sw-93(config-if-gigabitethernet0/2)#dsot1x port-control enable

poe-sw-93(config-if-gigabitethernet0/2)#dot1x timeout quiet-period 1

poe-sw-93(config-if-gigabitethernet0/2)#dot1x eap-relay enable
```

By default, Apply MAC is the auto got IP address, so configure dot1x authorization ip-auth-mode dhcp-server on the access port, and enable dhcp-snooping globally. Here, the uplink port of S3320 is port 24. The configuration is as follows:

```
interface gigabitethernet0/24
```

```
dhcp-snooping trust

exit
```

5.2 Fast Configuration of Authentication Platform

This chapter mainly describes the basic authentication configuration of the authentication platform, including modify the administrator password, add an organization, add a user, add a policy, and other related authentication service modules.

Step 1: Input the address in the browser, and jump to the login interface.

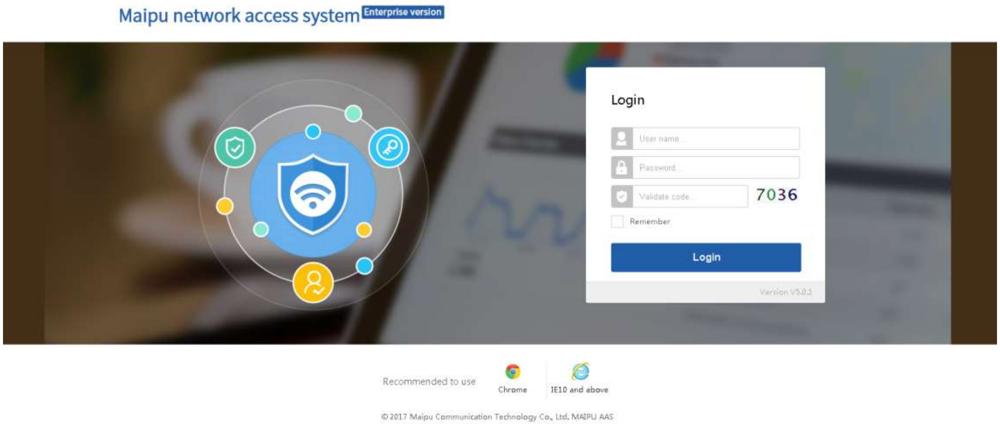
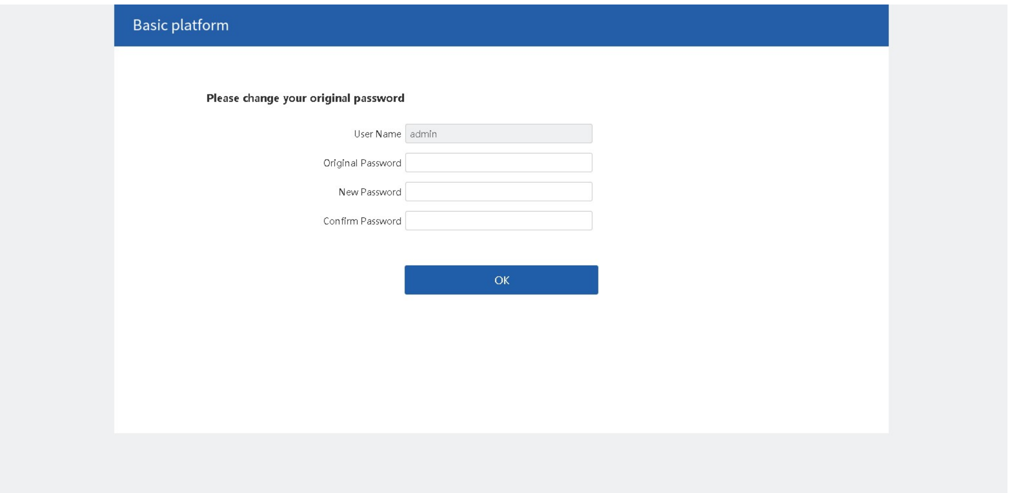


Figure 5-2-1 Maipu network access system

Step 2: Modify administrator password

When logging into the system for the first time, the system requires modifying the default administrator password. After modifying the password successfully, the system will re-jump to the login interface, input the user name and new password, and you can log into the system. The interface for modifying the password is ashown in Figure 5-2-2.

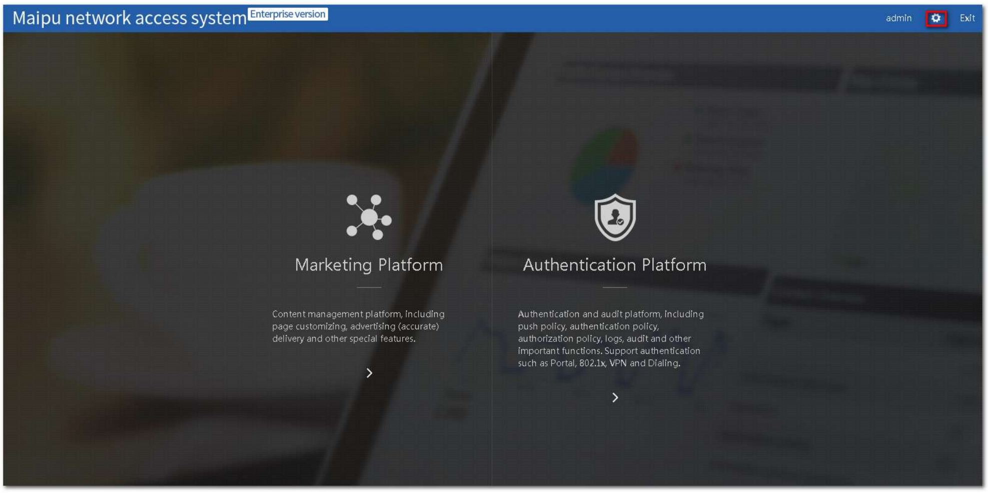


Please change your original password

User Name: admin
Original Password:
New Password:
Confirm Password:

Figure 5-2-2 Modify the administrator password

Step 3: Enter the home page of the system platform, and click the Setting icon at the top right corner to enter the platform interface (Figure 5-2-3).



Content management platform, including page customizing, advertising (accurate) delivery and other special features.

Authentication and audit platform, including push policy, authentication policy, authorization policy, logs, audit and other important functions. Support authentication such as Portal, 802.1x, VPN and Dialing.

Figure 5-2-3 The home page of the system platform

Step 4: Enter the organization management interface to add an organization

Click **Add**. The organization is mainly used to distinguish different sites. For example, when the customer needs the authentication of office building A and office building B, it is necessary to add two organizations of office building A and office building B, so as to distinguish the subsequent site device, authentication policy, and authorization policy. If the customer has only one application place, you just need to add one organization or do not add the organization, but directly adopt the default organization.

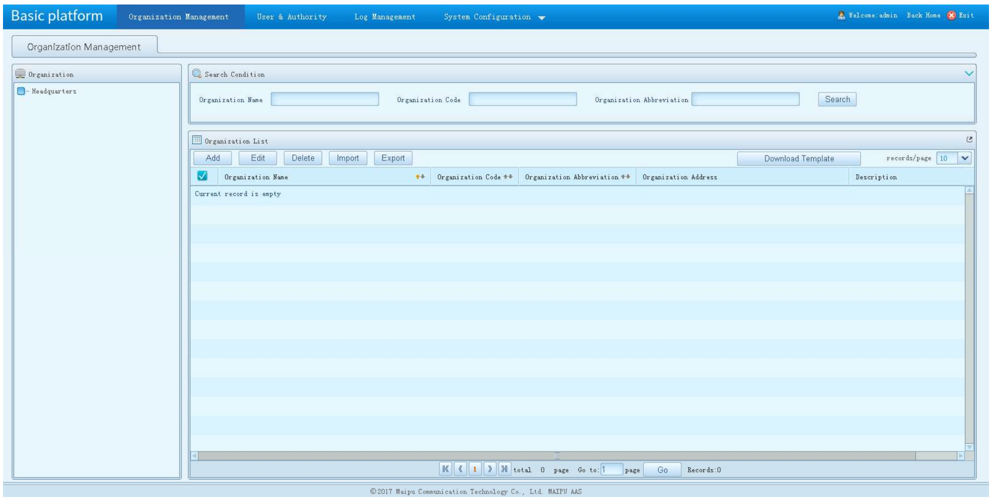
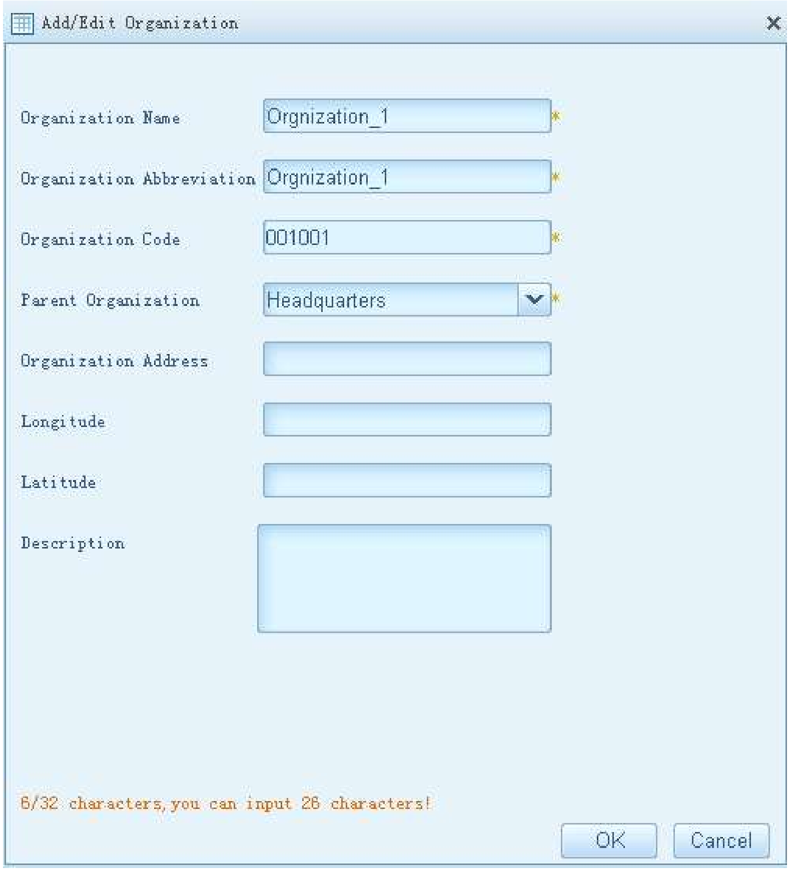


Figure 5-2-4 Organization management interface

Import the organization or add an organization. To convenient for the subsequent introduction, add the organization “Orgnizaion_1”, and the organization code is “001001”. When there are many organizations, it is suggested to add by importing. Here, you just need to fill in the mandatory fields.

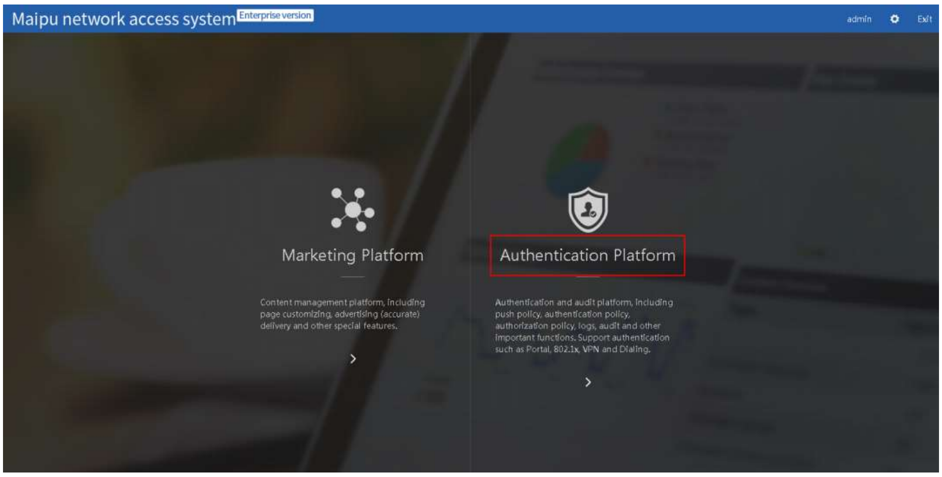


Organization Name: Orgnization_1 *
Organization Abbreviation: Orgnization_1 *
Organization Code: 001001 *
Parent Organization: Headquarters *
Organization Address:
Longitude:
Latitude:
Description:

6/32 characters, you can input 26 characters!

Figure 5-2-5 Add an organization

Step 5: Click “Back Home” to return to the home page of the platform and enter “Authentication Platform”



Content management platform, including page customizing, advertising (accurate) delivery and other special features.

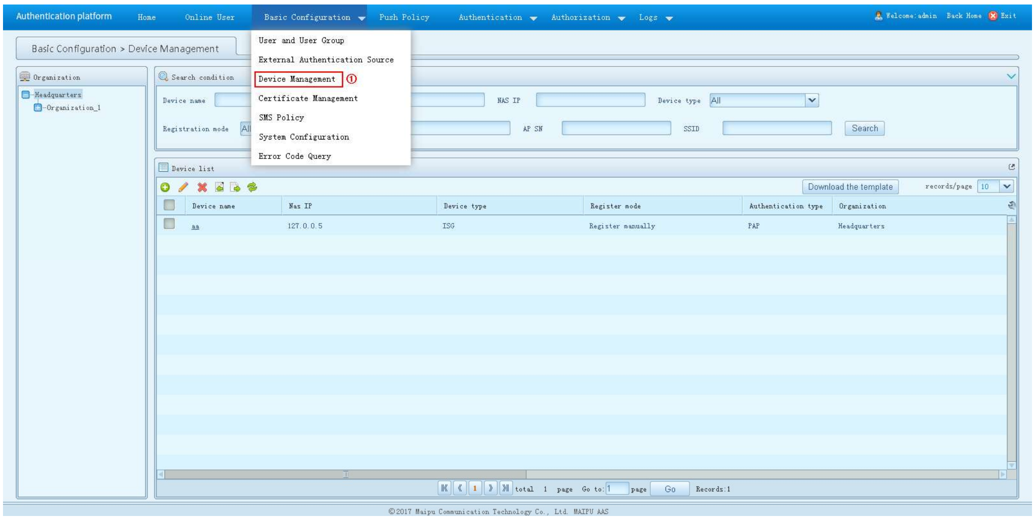
Authentication and audit platform, including push policy, authentication policy, authorization policy, logs, audit and other important functions. Support authentication such as Portal, 802.1x, VPN and Dialing.

All Rights Reserved

Figure 5-2-6 The home page of the system platform

Step 6: Enter the “Device Management” interface to add a device

Select **Basic Configuration** > **Device Management** to enter the device management interface, as shown in Figure 5-2-7.



Device type: All

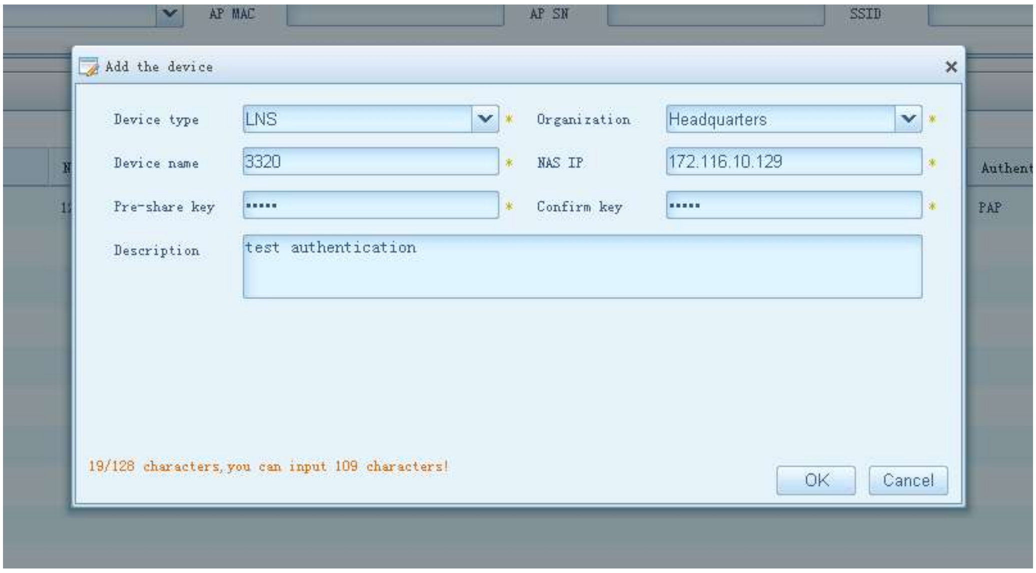
Registration mode: All

records/page: 10

☐	Device name	Nas IP	Device type	Register mode	Authentication type	Organization
☐	aa	127.0.0.5	ISG	Register manually	PAP	Headquarters

Figure 5-2-7 Device management interface

During 802.1X authentication, VPN dialing and other authentications, select LNS for “Device type” and Organizion_1 for organization, “Device name” can be customized. Fill in the configured key on the device for “Pre-share key”. Refer to step 2 of section 5.1. The default value is admin.



Device type: LNS *

Organization: Headquarters *

Device name: 3320 *

NAS IP: 172.116.10.129 *

Pre-share key: ••••• *

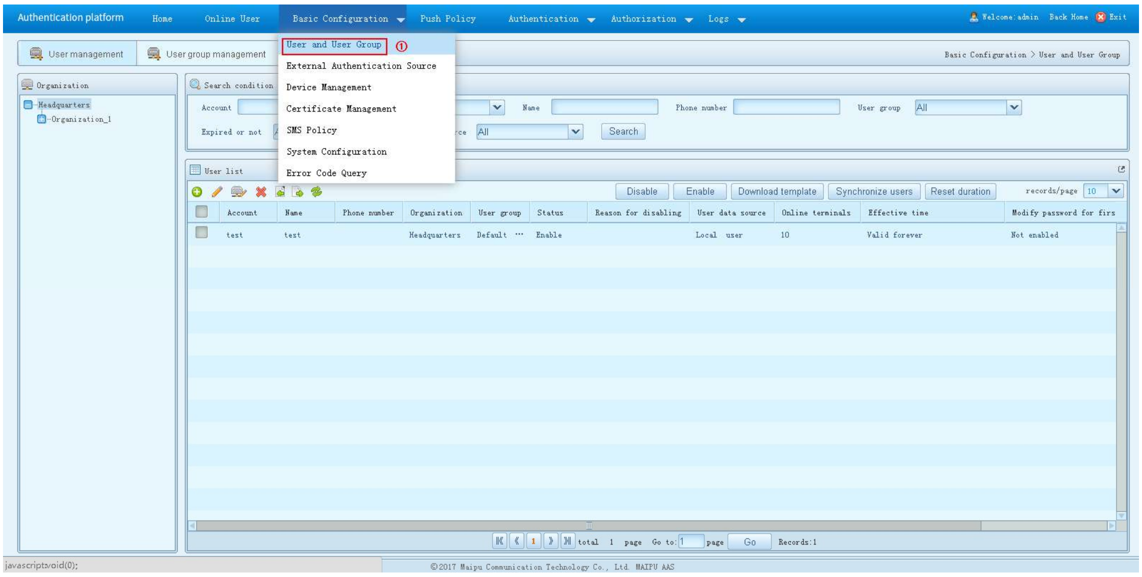
Confirm key: ••••• *

Description: test authentication

19/128 characters, you can input 109 characters!

Figure5-2-8 Add a device

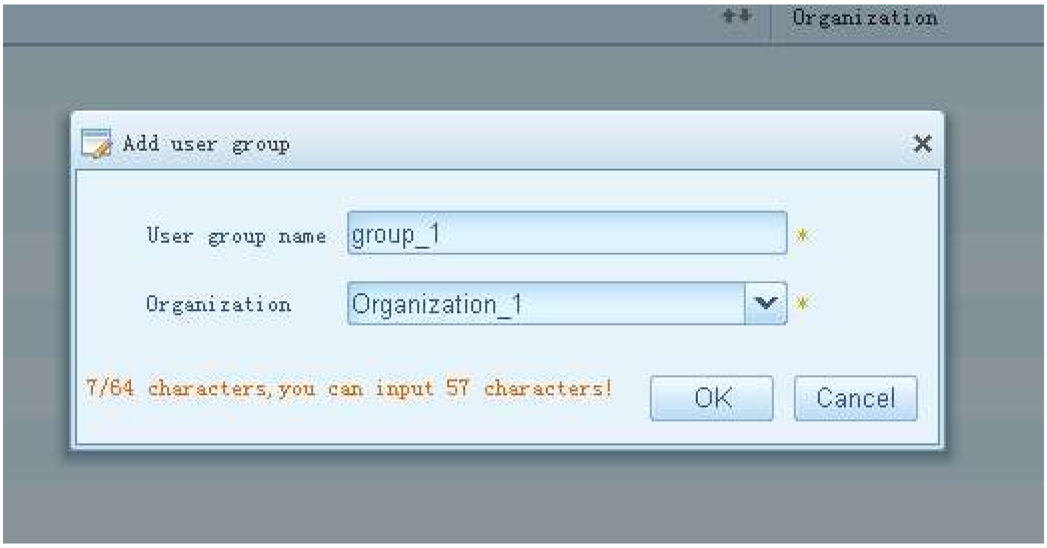
Step 7: Enter “User and User group” to add a user group and a user.



☐	Account	Name	Phone number	Organization	User group	Status	Reason for disabling	User data source	Online terminals	Effective time	Modify password for firs
☐	test	test		Headquarters	Default ···	Enable		Local user	10	Valid forever	Not enabled

Figure 5-2-9 User management

Add a user group. The user group name is “group_1”. For Organization, select the created “Organiztion_1”, indicating that the user group “group_1” belongs to the organization “Organiaztion_1”. If it is not necessary to authorize by user group or implement different authentication policies by user group, you can ignore the step, as follows:



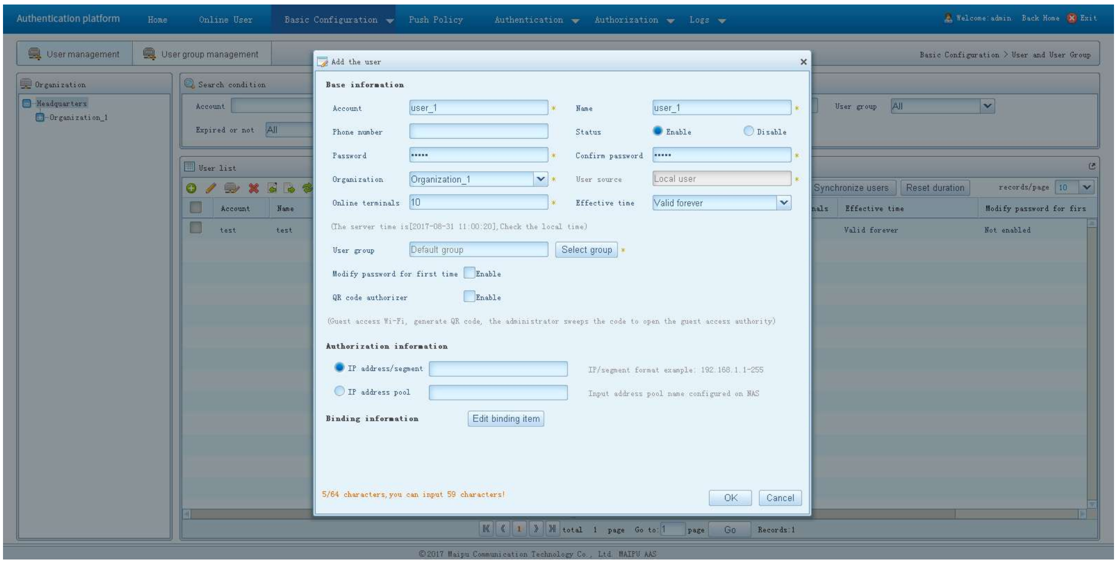
User group name: group_1 *

Organization: Organization_1 *

7/64 characters,you can input 57 characters!

Figure 5-2-10 User group management interface

After adding a user group, add one user and add the user to the group “group_1”. If the function is not needed, you can directly adopt the default setting and do not need to modify. Here, add one user “user_1”, as follows:



Add the user

Base information

Account: user_1 *
Name: user_1 *
Phone number:
Status: ● Enable ○ Disable
Password: ••••• *
Confirm password: ••••• *
Organization: Organization_1 *
User source: Local user *
Online terminals: 10 *
Effective time: Valid forever

(The server time is[2017-08-31 11:00:20],Check the local time)

User group: Default group [Select group] *
Modify password for first time ☐ Enable
QR code authorizer ☐ Enable

(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)

Authorization information

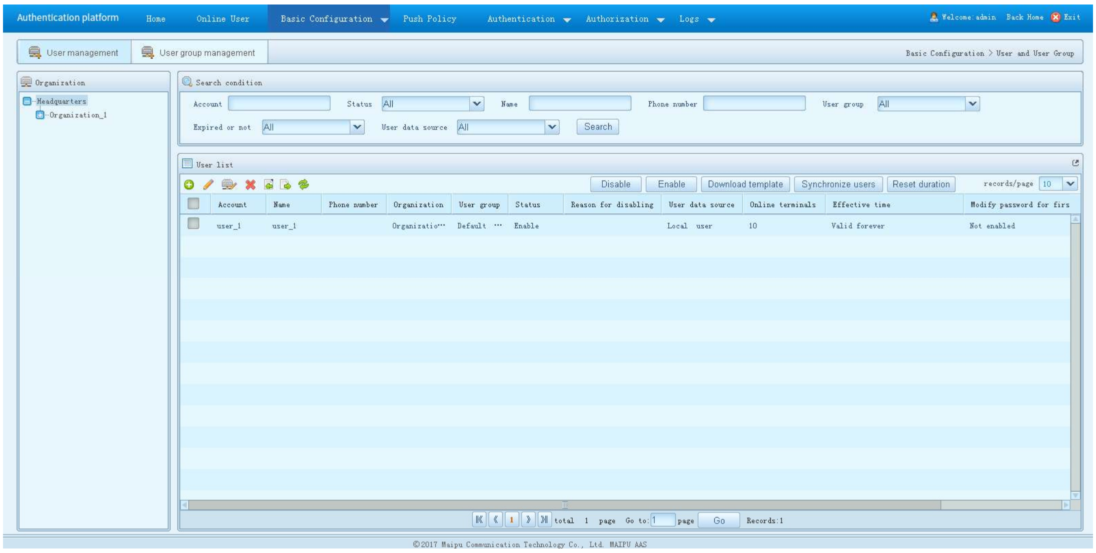
● IP address/segment — IP/segment format example: 192.168.1.1-255
○ IP address pool — Input address pool name configured on NAS

Binding information [Edit binding item]

5/64 characters, you can input 59 characters!

[OK] [Cancel]

Figure 5-2-11 Add a user



Account: Status: All Name: Phone number: User group: All
Expired or not: All User data source: All

☐	Account	Name	Phone number	Organization	User group	Status	Reason for disabling	User data source	Online terminals	Effective time	Modify password for firs
☐	user_1	user_1		Organizatio···	Default ···	Enable		Local user	10	Valid forever	Not enabled

total 1 page Go to: 1 page Records: 1

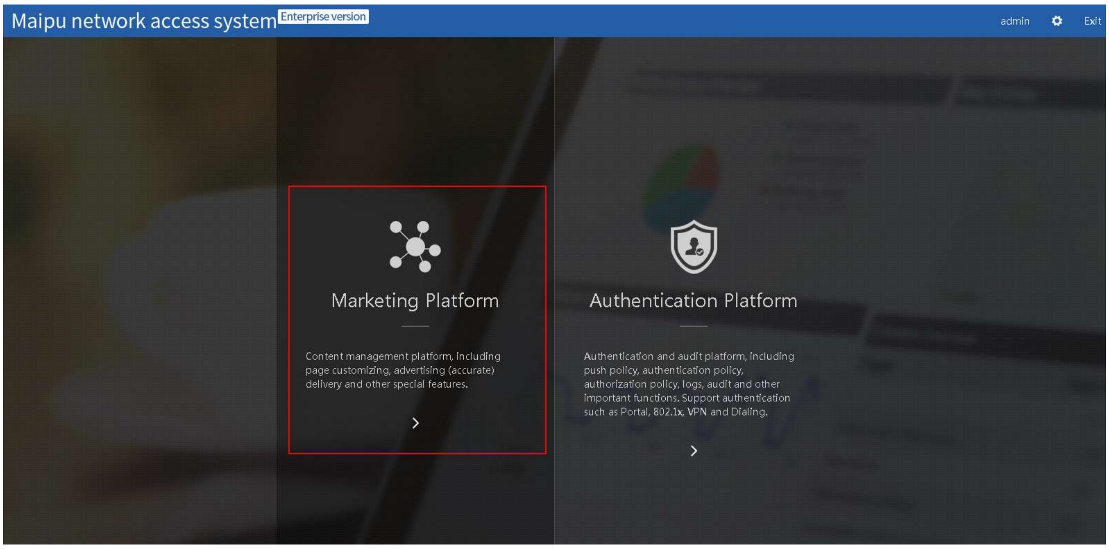
Figure 5-2-12 Add a user successfully

6 Step 3: Site Decoration

Super administrator, system administrator, and marketing system administrator can decorate the site. In the example, take the marketing system administrator as an example to describe the method of decorating the site.

6.1 Home Page

Enter the home page of the system platform, and click **Marketing Platform** to enter the marketing platform.



Content management platform, including page customizing, advertising (accurate) delivery and other special features.

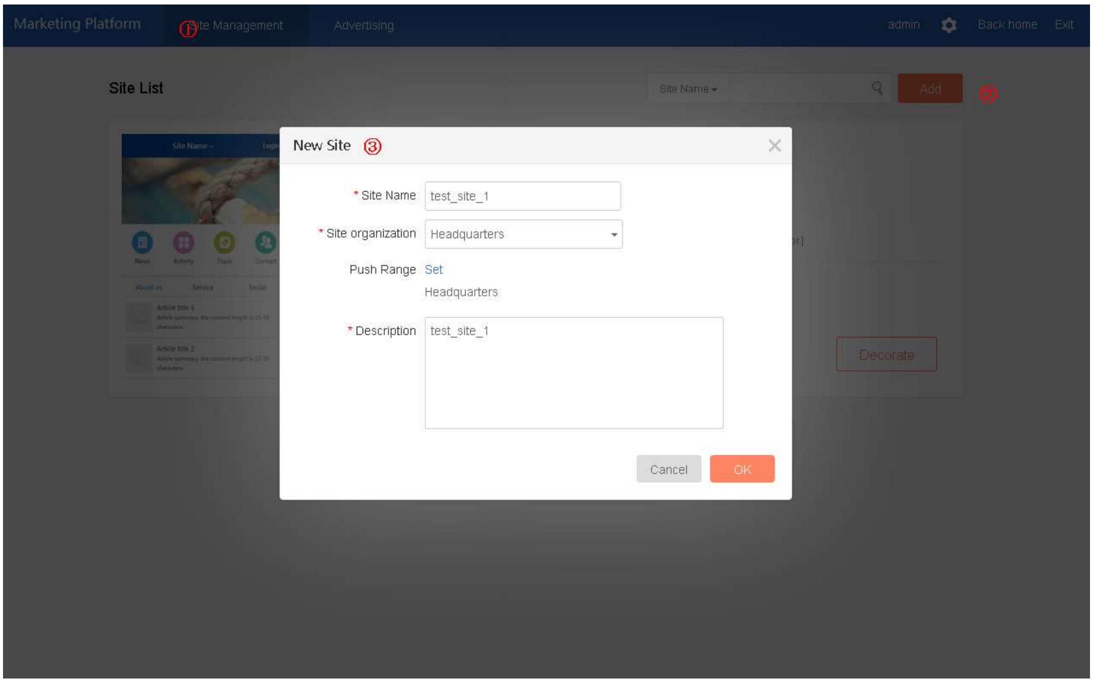
Authentication and audit platform, including push policy, authentication policy, authorization policy, logs, audit and other important functions. Support authentication such as Portal, 802.1x, VPN and Dialing.

Figure 6-1-1The home page of the system platform

Click **Site Management** to enter the site management interface and add one site, as follows:

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved



New Site ③

* Site Name: test_site_1

* Site organization: Headquarters

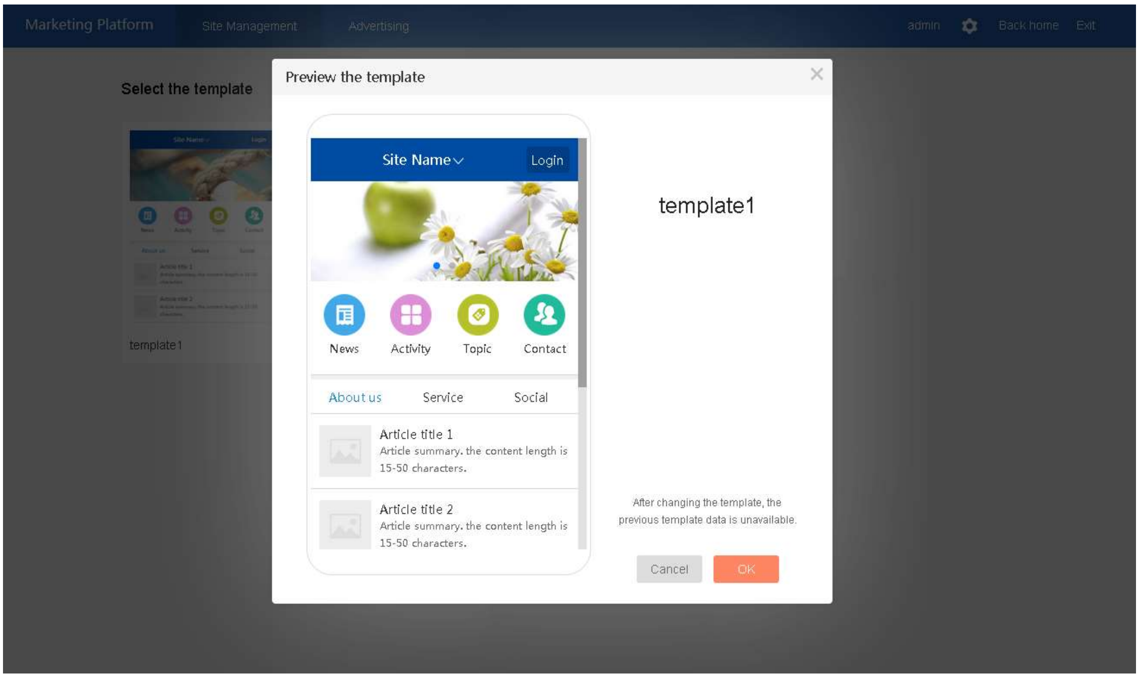
Push Range: Set

Headquarters

* Description: test_site_1

Figure 6-1-2 Create one site

After creating one site, enter the interface of selecting the template, click the desired template, and you can preview the template in the displayed dialog box:



Article title 1
Article summary. the content length is 15-50 characters.

Article title 2
Article summary. the content length is 15-50 characters.

template1

After changing the template, the previous template data is unavailable.

Figure 6-1-3 Preview the site template

After clicking OK in the displayed box of the interface for selecting the template, enter the interface of decorating the site home page.

In the red box ①, select the desired configuration interface.

In the red box ②, select the desired components.

In the red box ③, display the preview effect after configuring the components.

After enabling the button of the red box ④, the corresponding components can be displayed on the site interface.

The red box ⑤ is used to configure the selected components at the left.

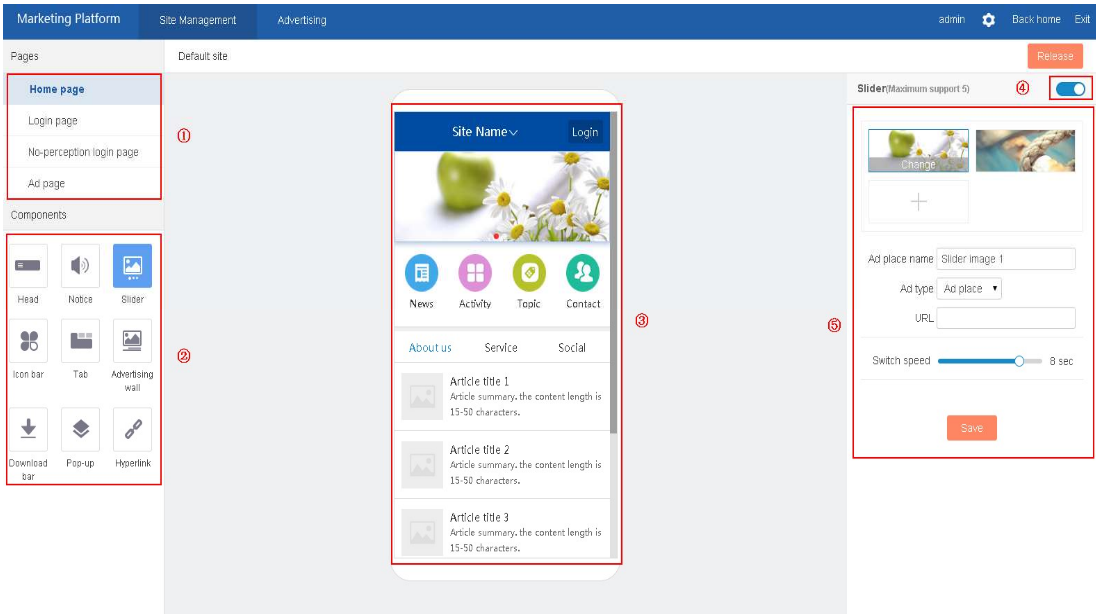


Figure 6-1-4 The home page of decorating the site

Figure 6-1-4 is the configuration interface of the site home page. The mobile phone model at the middle of the interface can preview the interface effect after decoration. The left of the mobile phone model can select the components to configure according to the interface. The right of the mobile phone model is the content configuration area of the left components.

When decorating the site home page, the marketing system administrator can select the desired phone preview box interface according to the components, and also can click the interface part of the mobile phone preview box to jump to different components. After selecting the desired components, perform the corresponding configuration at the right of the mobile phone preview box, save, and then, you can see the effect after configuration in the mobile phone preview box.

Caution

- After decorating each component at the home page, you need to click Save so that the decoration can take effect.

- When decorating the site, some components can be used normally only after enabling the switch at the top right corner of the interface, as shown in Figure 6-1-4.

6.2Decorate Login Page

After decorating the site home page, you can continue to decorate the login page, as shown in the following figure:

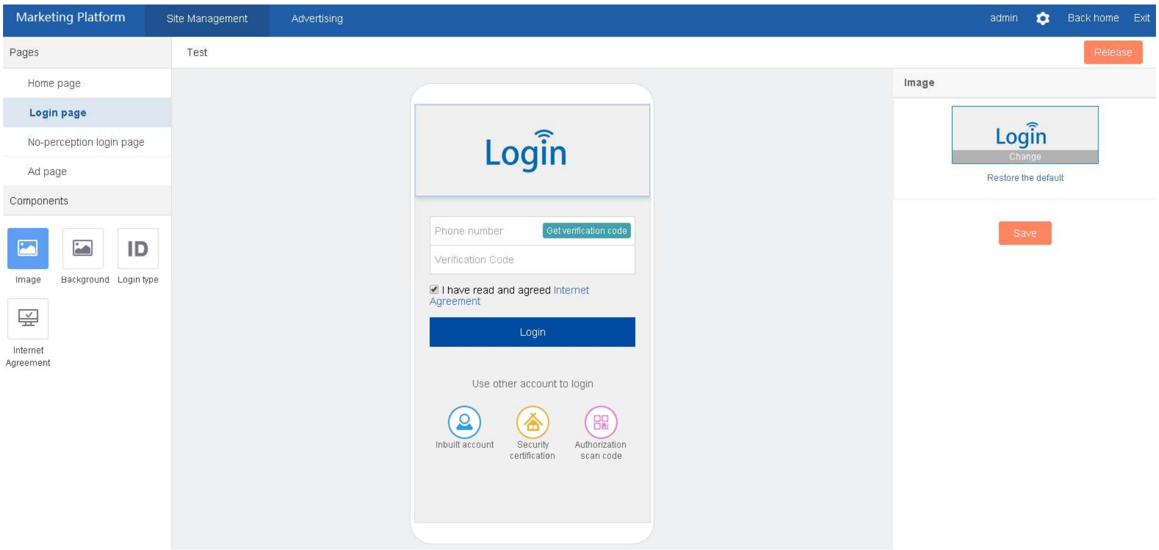
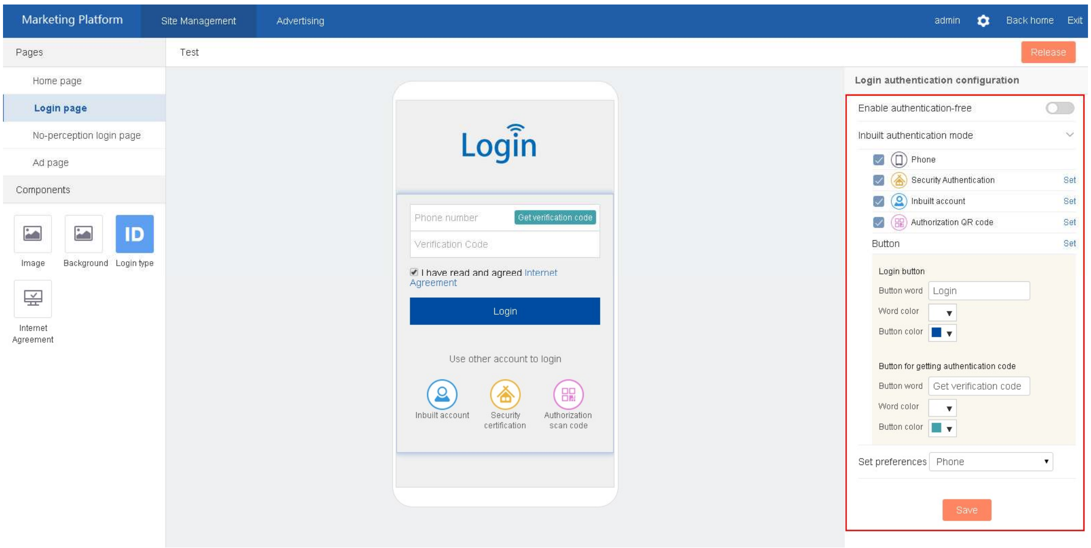


Figure 6-2-1 Login page

The image and background figure of the site login page support customized uploading. The Internet agreement can use the default words of the system, and also can be modified (The Internet agreement mainly describes some disclaimer and legal information about your WiFi service, and it is suggested to modify according to the requirements of your enterprise).

The system supports accessing Internet by various authentication modes, which can be configured in the login mode, as shown in the following figure:



Button word: Login
Button word: Get verification code
Set preferences: Phone

Figure 6-2-2 Set login mode

The authentication mode can be changed according to the service needs. By default, the system enables all authentication modes except for authentication-free. In the inbuilt authentication modes of the system, all other authentication modes except for mobile phone also can perform the personalized configuration for the page by clicking **Set**.

Caution

- After decorating each component of the login page, you need to click **Save** so that the decoration can take effect.

6.3 Decorate No-perception Login Page

The no-perception login indicates that when logging in again after being forced to get offline, the visitor does not need to input the account information to log in via the login interface, but directly clicks **Login** (no perception intervention) to get online without inputting the account information or directly logs in and gets online without any perception (no perception and no intervention). For details, refer to section 11.2.3.

The no-perception login page is the no-perception intervention page. With the page, the visitor can log in and access Internet quickly without inputting the user name and password, as shown in the following figure:

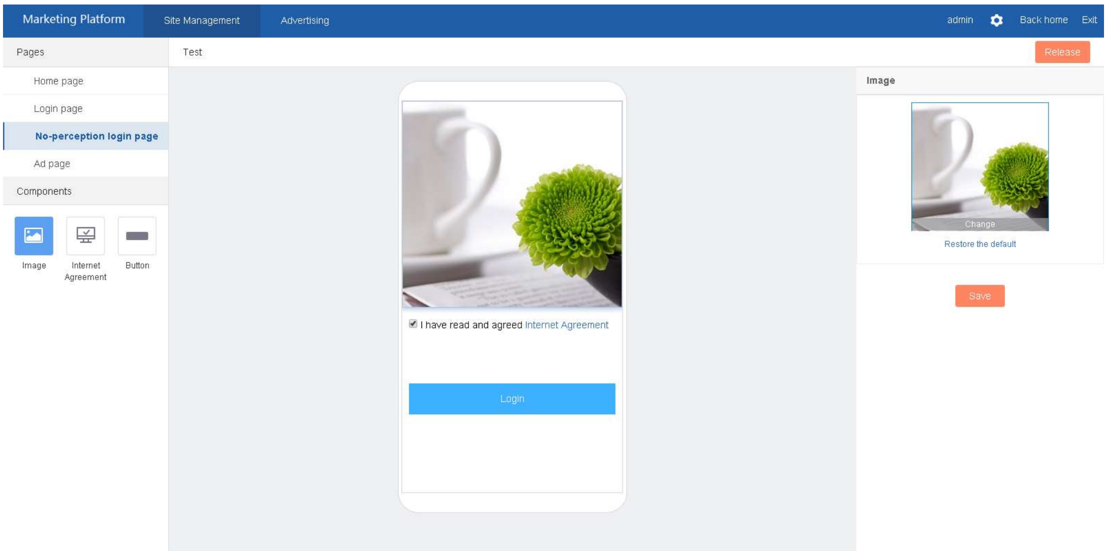


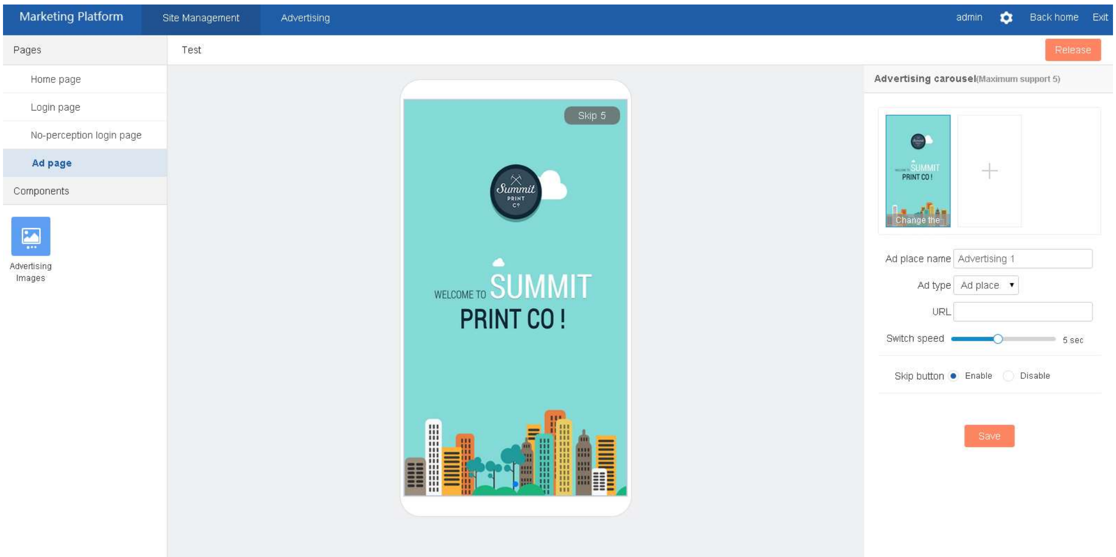
Figure 6-3-1 No-perception login page

Caution

- After decorating the no-perception login page, you need to click **Save** so that the decoration can take effect.

6.4 Decorate Ad Page

After authentication, the visitor jumps to the advertising page, used to display the business advertising, as shown in the following figure:



Ad place name Advertising 1

Ad type Ad place

URL

Switch speed 5 sec

Skip button ● Enable ○ Disable

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

Figure 6-4-1Decorate the advertising page

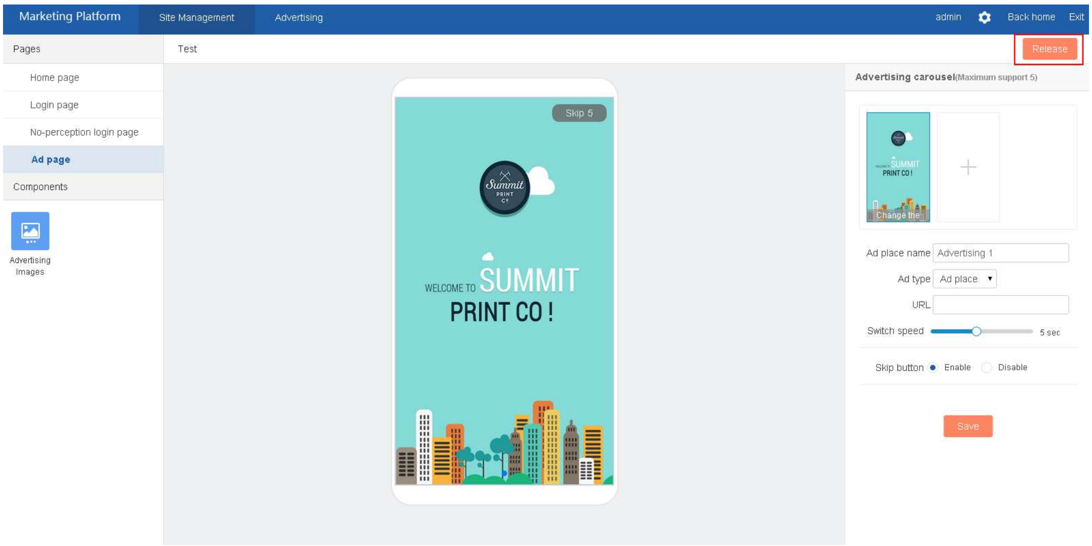
When decorating the advertising page, you can set the time of displaying the advertising page (that is the switch speed) and whether to skip. The advertising page can be added with five carousel figures at the same time. For the advertising of each carousel figure, you can select the advertising type. If setting it to the fixed advertising place, you can configure the advertising of the internal or external link.

Caution

- After decorating the advertising page, you need to click Save so that the decoration can take effect.
- The proxy server used by the traffic-save mode of Opera browser is not stable, and as a result, the countdown advertising page will stop at 0s for a long time before jumping. It is suggested to close the traffic-save mode of Opera browser.

6.5 Release the Site

After completing all decorations of above chapters, you need to click **Release** at the right top corner of the following figure so that the decorations can take effect at the visitor terminal.



Ad place name Advertising 1

Ad type Ad place ▾

URL

Switch speed 5 sec

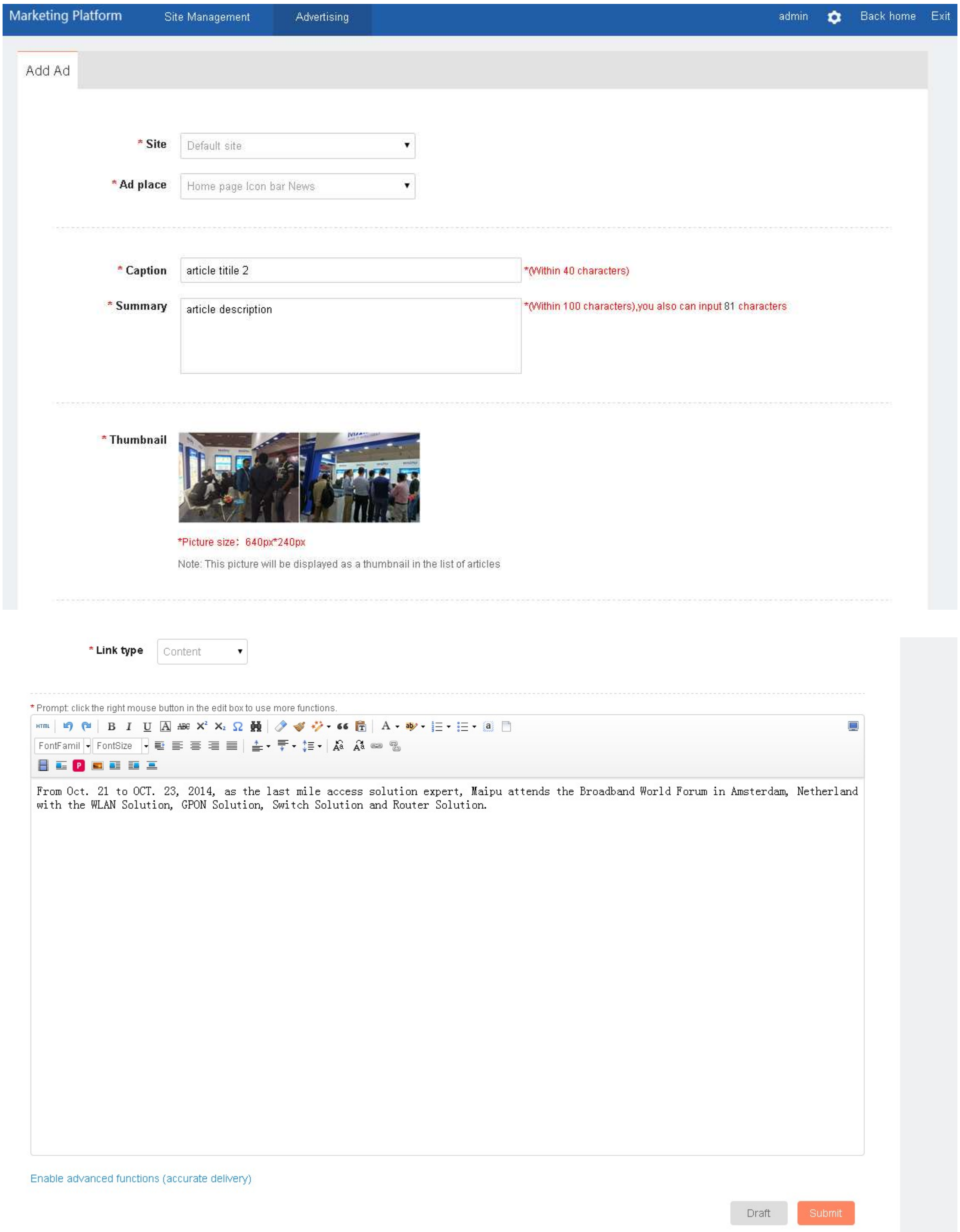
Skip button ● Enable ○ Disable

Figure 6-5-1 Release the site

7 Step 4: Advertising

Super administrator, system administrator, marketing system administrator, and content administrator can advertise. In the example, first create one marketing system administrator to describe how to advertise.

The marketing system administrator enters **Advertising** to add one advertisement, as shown in the following figure:



* Site: Default site

* Ad place: Home page Icon bar News

* Caption: article titile 2 *(Within 40 characters)

* Summary: article description *(Within 100 characters),you also can input 81 characters

* Thumbnail

*Picture size：640px*240px

Note: This picture will be displayed as a thumbnail in the list of articles

* Link type: Content

* Prompt: click the right mouse button in the edit box to use more functions.

From Oct. 21 to OCT. 23, 2014, as the last mile access solution expert, Maipu attends the Broadband World Forum in Amsterdam, Netherland with the WLAN Solution, GPON Solution, Switch Solution and Router Solution.

Enable advanced functions (accurate delivery)

Figure 7-1-1 Advertising

When adding one advertisement, you can enable the accurate delivery of the advertisement. After enabling, you can set the start time and end time of the advertising (the start time and end time of the advertising indicates the effective time of the advertising. If the start time and end time are set, the advertisement is delivered only within the time period), priority, and pushing range of the advertisement.

Priority: If the advertising time overlaps, you can set the priority. The larger the number, the higher the priority.

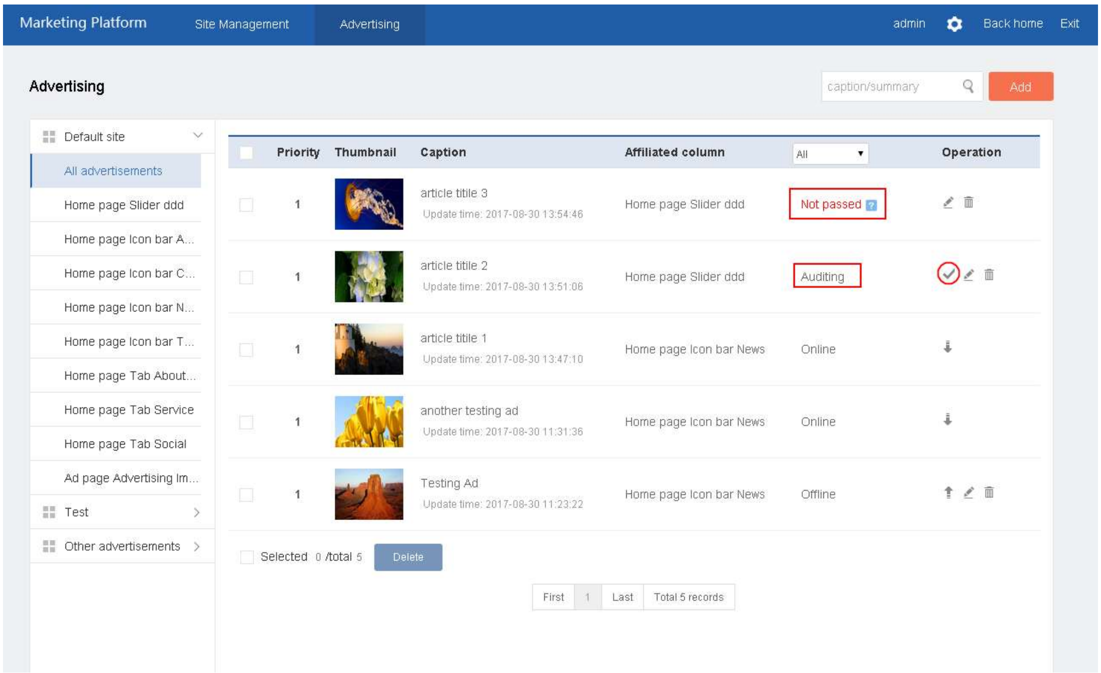
Pushing range: If the pushing range is set, the advertisement is only pushed to the selected pushing range, and the other organizations do not display the advertisement.

After adding the advertisement information, the user can select **Draft** or **Submit**.

If selecting **Draft**, the advertisement has the “draft” suffix in the advertisement list. You can re-edit draft advertisement, and then, click **Submit** to deliver. The draft advertisement cannot be delivered, and the terminal does not display the draft advertisement.

If selecting **Submit**, the advertisement will be submitted to the same level or superior administrator with the audit authority for auditing.

For the auditing advertisement, you need to click the check mark in the following figure to audit, and then, the advertisement can be delivered. If the advertisement does not pass the auditing, you can click the question mark in the following figure to view the reason. The advertisement that does not pass auditing is not delivered, and the terminal does not display it.



☐	Priority	Thumbnail	Caption	Affiliated column	All ▾	Operation
☐	1		article titile 3 Update time: 2017-08-30 13:54:46	Home page Slider ddd	Not passed ?	
☐	1		article titile 2 Update time: 2017-08-30 13:51:06	Home page Slider ddd	Auditing	✓
☐	1		article titile 1 Update time: 2017-08-30 13:47:10	Home page Icon bar News	Online	↓
☐	1		another testing ad Update time: 2017-08-30 11:31:36	Home page Icon bar News	Online	↓
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	↑

☐ Selected 0 /total 5 Delete

First 1 Last Total 5 records

Figure 7-1-2 Audit advertising

Caution

- The advertisement delivered by the super administrator passes auditing automatically after being submitted.

---

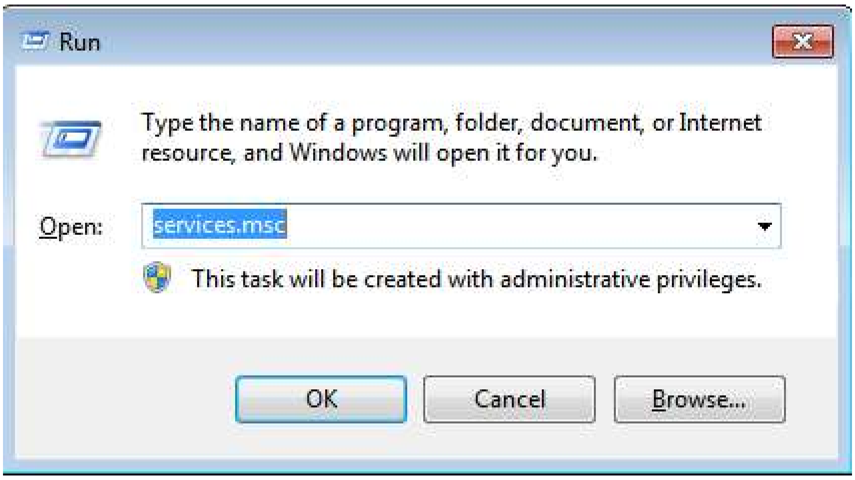
copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

8 Step 5: Internet Experience

8.1 win7 Configuration and Authentication

Step 1: By default, win7 does not enable the 802.1x wired authentication, and you need to perform the following operations to open the windows server management, as shown in Figure 8-1-1.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

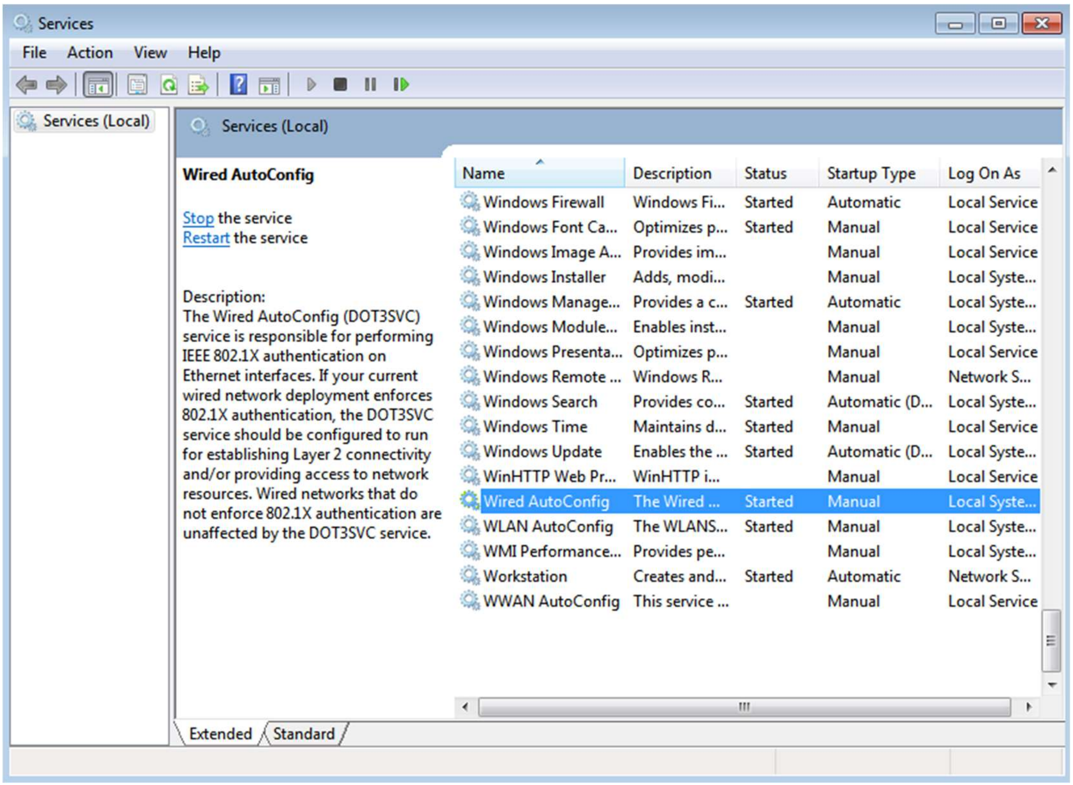
Open: services.msc

This task will be created with administrative privileges.

Figure 8-1-1 Open windows service management

Step 2: Find the Wired AutoConfig server, and enable the server, as shown in Figure 8-1-2. If the server is enabled successfully, Figure 8-1-3 is displayed.

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved



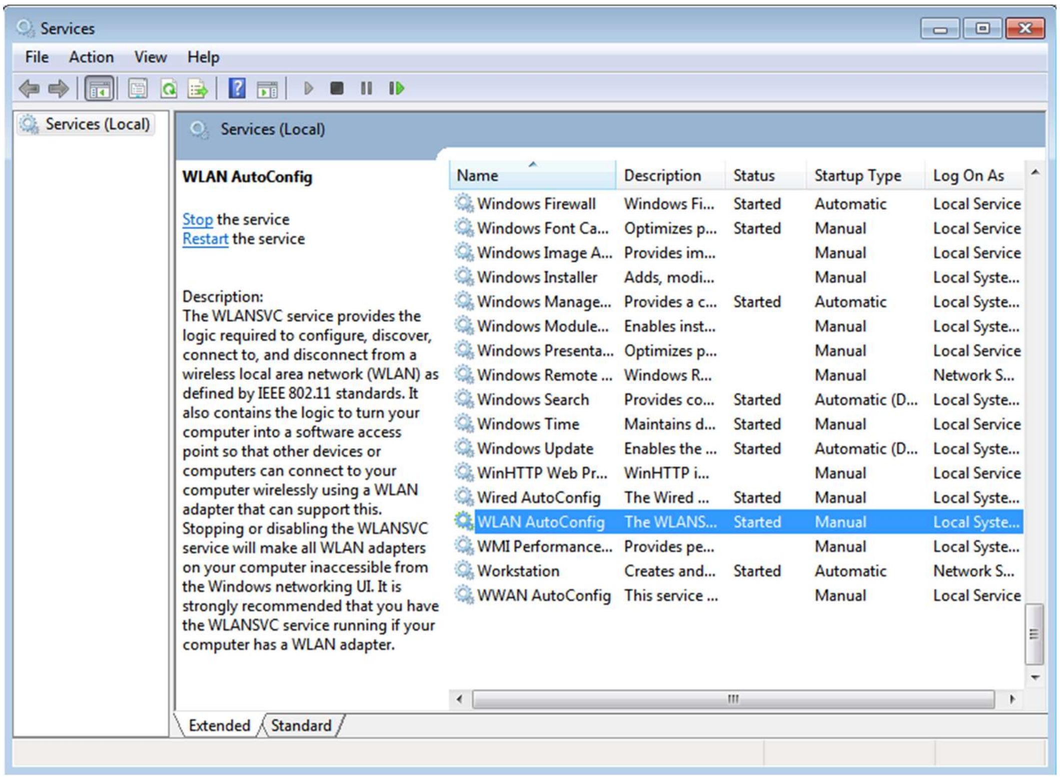
Wired AutoConfig

Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status	Startup Type	Log On As
Windows Firewall	Windows Fi...	Started	Automatic	Local Service
Windows Font Ca...	Optimizes p...	Started	Manual	Local Service
Windows Image A...	Provides im...		Manual	Local Service
Windows Installer	Adds, modi...		Manual	Local Syste...
Windows Manage...	Provides a c...	Started	Automatic	Local Syste...
Windows Module...	Enables inst...		Manual	Local Syste...
Windows Presenta...	Optimizes p...		Manual	Local Service
Windows Remote ...	Windows R...		Manual	Network S...
Windows Search	Provides co...	Started	Automatic (D...	Local Syste...
Windows Time	Maintains d...	Started	Manual	Local Service
Windows Update	Enables the ...	Started	Automatic (D...	Local Syste...
WinHTTP Web Pr...	WinHTTP i...		Manual	Local Service
Wired AutoConfig	The Wired ...	Started	Manual	Local Syste...
WLAN AutoConfig	The WLANS...	Started	Manual	Local Syste...
WMI Performance...	Provides pe...		Manual	Local Syste...
Workstation	Creates and...	Started	Automatic	Network S...
WWAN AutoConfig	This service ...		Manual	Local Service

Figure 8-1-2 Enable the Wired AutoConfig service



WLAN AutoConfig

Stop the service
Restart the service

Description:
The WLANSVC service provides the logic required to configure, discover, connect to, and disconnect from a wireless local area network (WLAN) as defined by IEEE 802.11 standards. It also contains the logic to turn your computer into a software access point so that other devices or computers can connect to your computer wirelessly using a WLAN adapter that can support this. Stopping or disabling the WLANSVC service will make all WLAN adapters on your computer inaccessible from the Windows networking UI. It is strongly recommended that you have the WLANSVC service running if your computer has a WLAN adapter.

Name	Description	Status	Startup Type	Log On As
Windows Firewall	Windows Fi...	Started	Automatic	Local Service
Windows Font Ca...	Optimizes p...	Started	Manual	Local Service
Windows Image A...	Provides im...		Manual	Local Service
Windows Installer	Adds, modi...		Manual	Local Syste...
Windows Manage...	Provides a c...	Started	Automatic	Local Syste...
Windows Module...	Enables inst...		Manual	Local Syste...
Windows Presenta...	Optimizes p...		Manual	Local Service
Windows Remote ...	Windows R...		Manual	Network S...
Windows Search	Provides co...	Started	Automatic (D...	Local Syste...
Windows Time	Maintains d...	Started	Manual	Local Service
Windows Update	Enables the ...	Started	Automatic (D...	Local Syste...
WinHTTP Web Pr...	WinHTTP i...		Manual	Local Service
Wired AutoConfig	The Wired ...	Started	Manual	Local Syste...
WLAN AutoConfig	The WLANS...	Started	Manual	Local Syste...
WMI Performance...	Provides pe...		Manual	Local Syste...
Workstation	Creates and...	Started	Automatic	Network S...
WWAN AutoConfig	This service ...		Manual	Local Service

Figure 8-1-3 Enable the Wired AutoConfig service successfully

To enable MD5 authentication, you need to download the plug-in component to install.

Copy the following attachment to the PC disk, and double-click dot1xMD5.reg to install. If the MD5 authentication is not needed, ignore the step.

dot1xMD5.reg

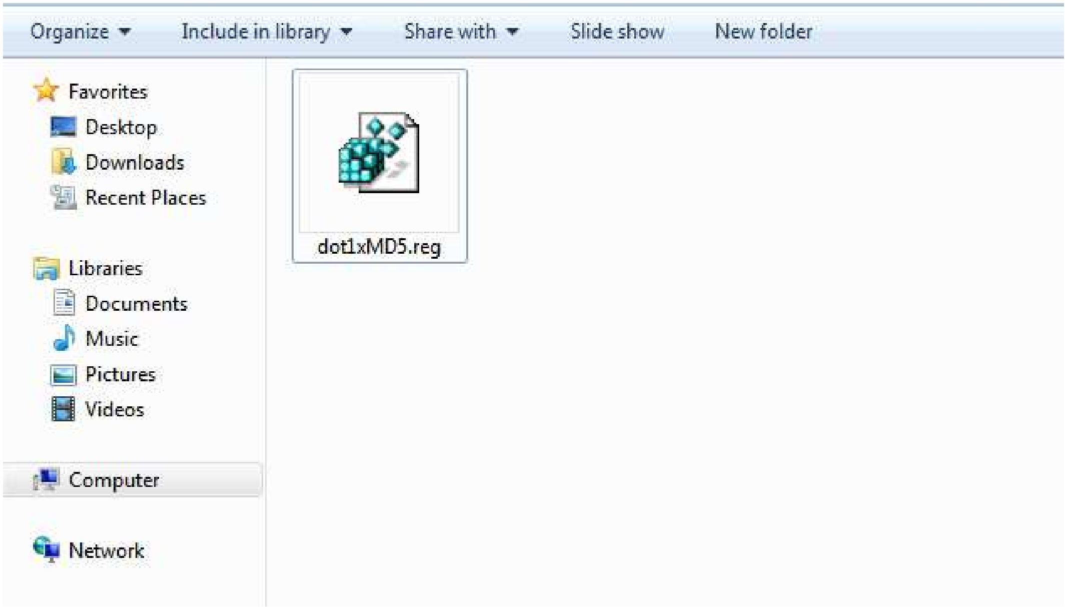


Figure 6-1-5 Enable the MD5 authentication

Step 3: In windows7, configure the network card, find the network card directly connected with port 1 of S3320, right-click and select **Properties**.

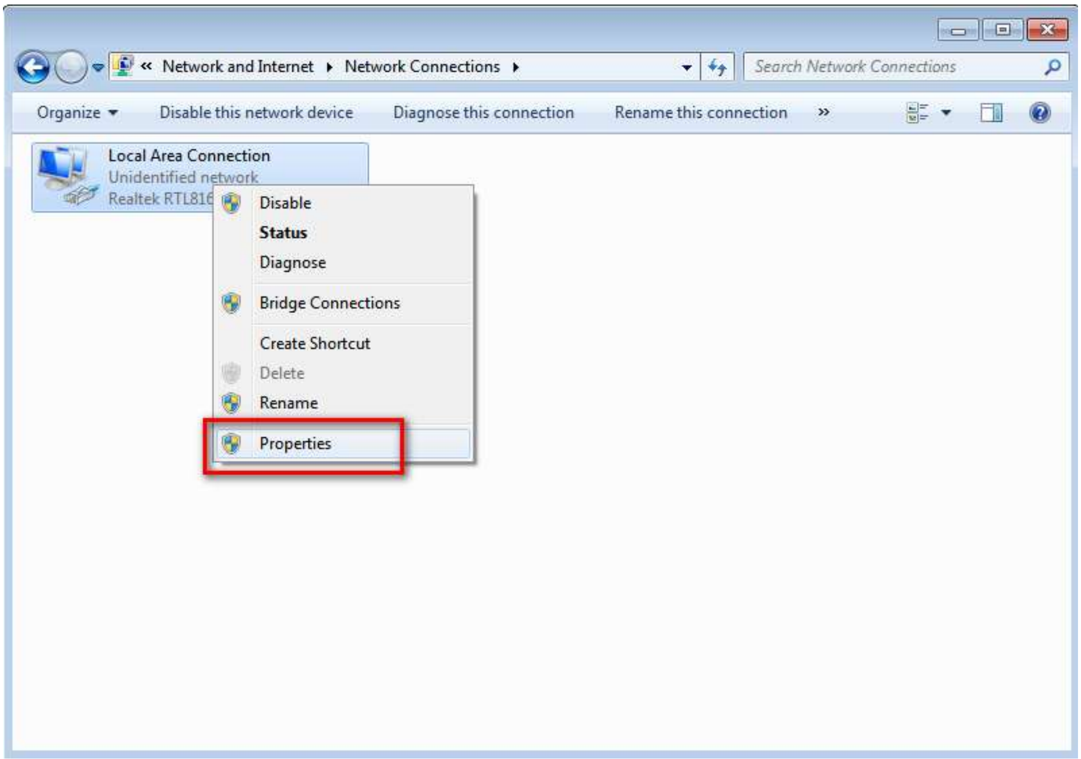
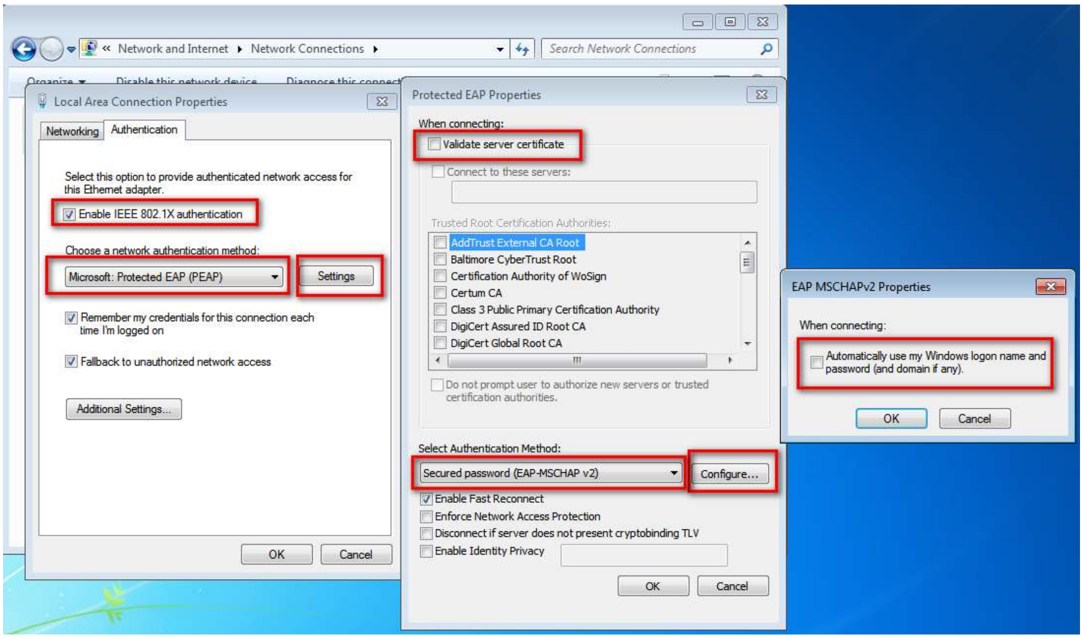


Figure 8-1-4 Network card properties

Step 4: Click **Properties** > **Authentication**:

Tick **Enable IEEE 802.1X authentication**, select **EAP (PEAP)** from the drop-down list, click **Settings**, un-tick **Validate server certificate**, and select MS-CHAPV2, as follows:



Local Area Connection Properties – Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Protected EAP Properties

When connecting:

☐ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

- ☐ AddTrust External CA Root
- ☐ Baltimore CyberTrust Root
- ☐ Certification Authority of WoSign
- ☐ Certum CA
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:
Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

EAP MSCHAPv2 Properties

When connecting:

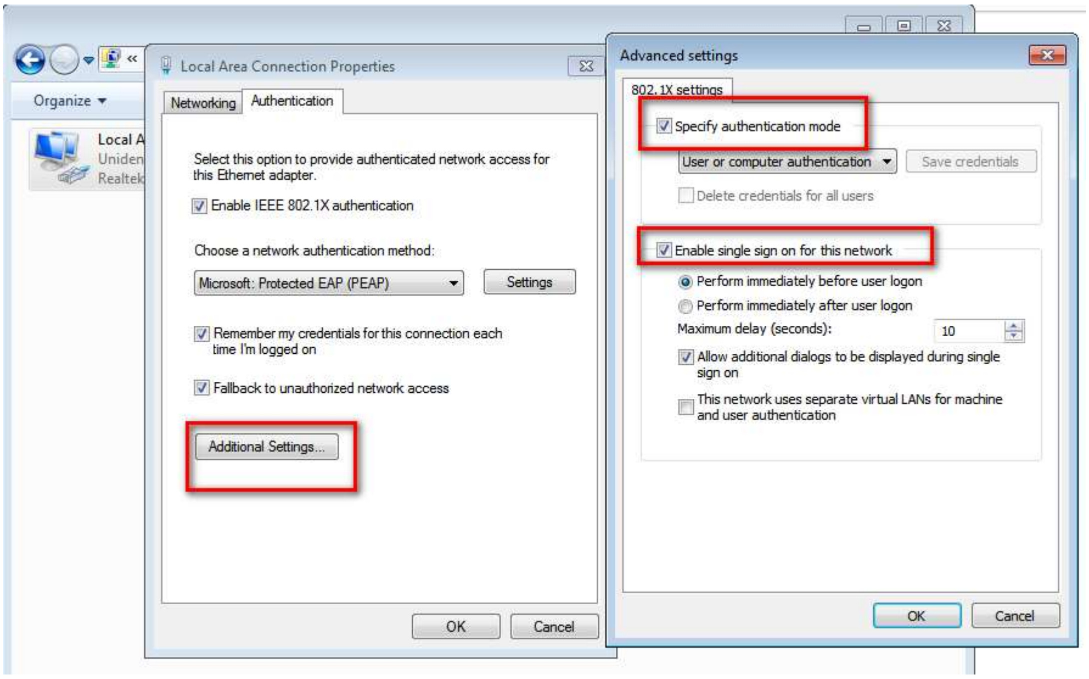
☐ Automatically use my Windows logon name and password (and domain if any).

Figure 8-1-5 Network card authentication configuration 1

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

After click **OK**, perform the following setting.



Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

☑ Specify authentication mode

User or computer authentication

☐ Delete credentials for all users

☑ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

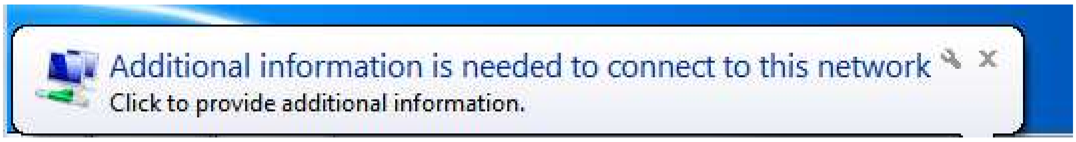
☐ This network uses separate virtual LANs for machine and user authentication

Figure 8-1-6 Network card authentication configuration 2

Step 5: At the lower right corner, display the window, click the window, and input the user name and password to authenticate.

If the window is not displayed, cancel **Enable single sign on for this network** > **OK** > **OK** in above Step 4.

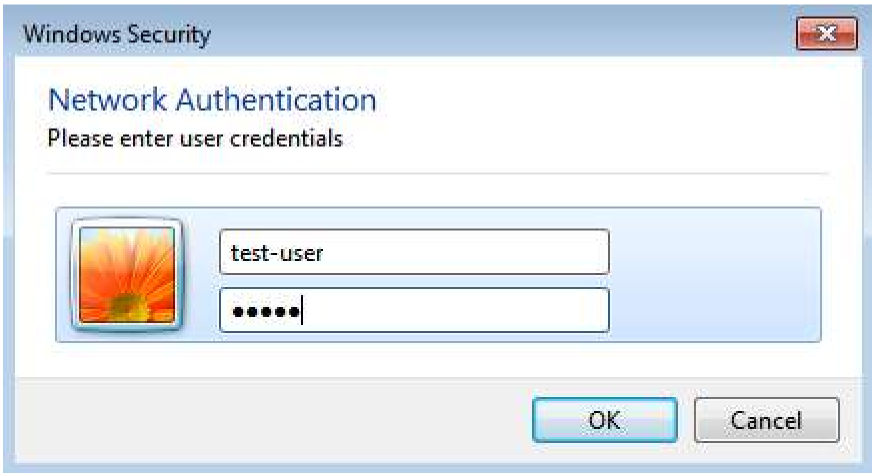
Here, the user name is the previous created test-user, and the password is the password of the user.



Additional information is needed to connect to this network

Click to provide additional information.

Figure 8-1-7 Perform authentication



Windows Security

Network Authentication

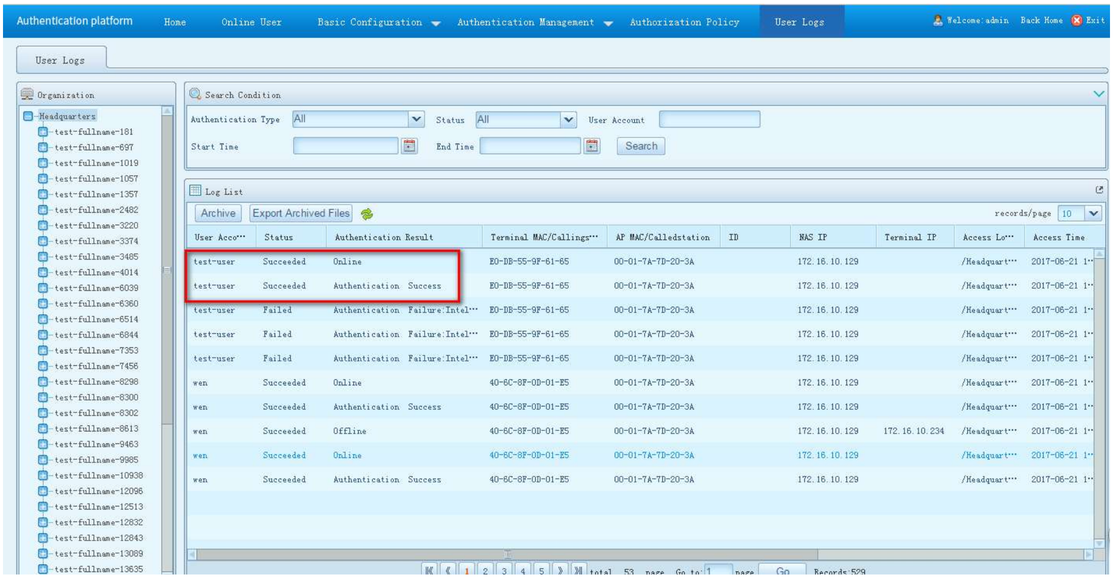
Please enter user credentials

test-user

•••••

Figure 8-1-8 Input the user name/password

Step 6: Log into the AAS, and view whether the authentication succeeds in **User Logs** and **Online User**.



Authentication Type: All

Status: All

User Account:

Start Time:

End Time:

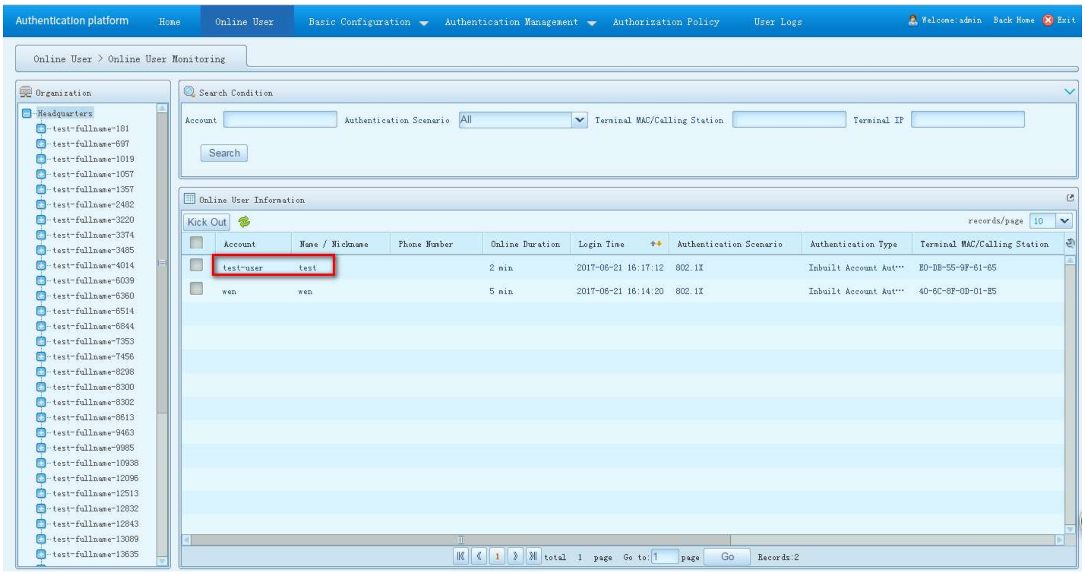
records/page: 10

User Acco···	Status	Authentication Result	Terminal MAC/Callings···	AP MAC/Calledstation	ID	NAS IP	Terminal IP	Access Lo···	Access Time
test-user	Succeeded	Online	E0-DB-55-9F-61-65	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
test-user	Succeeded	Authentication Success	E0-DB-55-9F-61-65	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
test-user	Failed	Authentication Failure:Intel···	E0-DB-55-9F-61-65	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
test-user	Failed	Authentication Failure:Intel···	E0-DB-55-9F-61-65	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
test-user	Failed	Authentication Failure:Intel···	E0-DB-55-9F-61-65	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
wen	Succeeded	Online	40-6C-8F-0D-01-E5	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
wen	Succeeded	Authentication Success	40-6C-8F-0D-01-E5	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
wen	Succeeded	Offline	40-6C-8F-0D-01-E5	00-01-7A-7D-20-3A		172.16.10.129	172.16.10.234	/Headquart···	2017-06-21 1··
wen	Succeeded	Online	40-6C-8F-0D-01-E5	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··
wen	Succeeded	Authentication Success	40-6C-8F-0D-01-E5	00-01-7A-7D-20-3A		172.16.10.129		/Headquart···	2017-06-21 1··

1 2 3 4 5 total 53 page Go to 1 page Records:529

Figure 8-1-9 View the login log

In the online list, there is the corresponding user information, as follows:



Authentication Scenario: All

records/page: 10

☐	Account	Name / Nickname	Phone Number	Online Duration	Login Time	Authentication Scenario	Authentication Type	Terminal MAC/Calling Station
☐	test-user	test		2 min	2017-06-21 16:17:12	802.1X	Inbuilt Account Aut···	E0-DB-55-9F-61-65
☐	wen	wen		5 min	2017-06-21 16:14:20	802.1X	Inbuilt Account Aut···	40-6C-8F-0D-01-E5

Figure 8-1-10 Online user information

Up to now, the user **test-user** is authenticated.

8.2 MAC System Configuration and Authentication

Step 1: Enter MAC Pro System Setting, and find **Network**.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

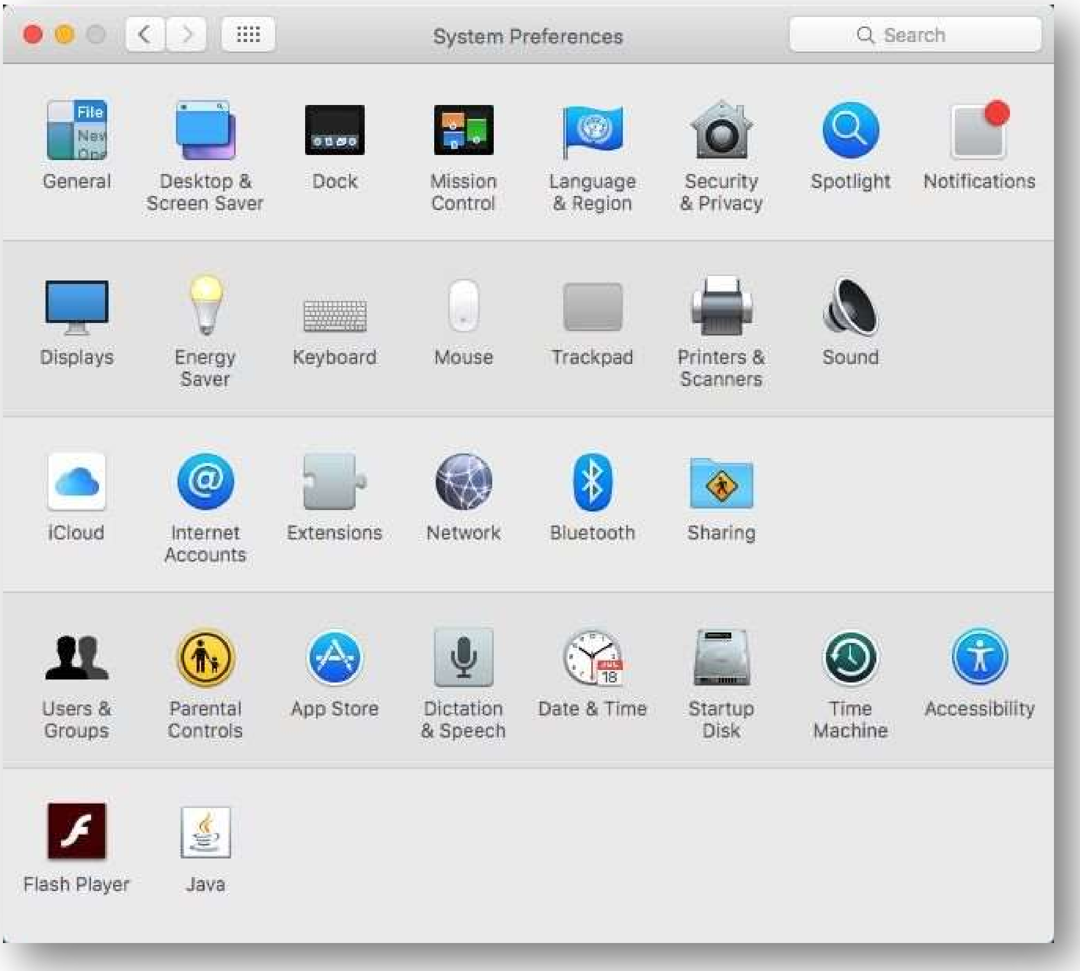
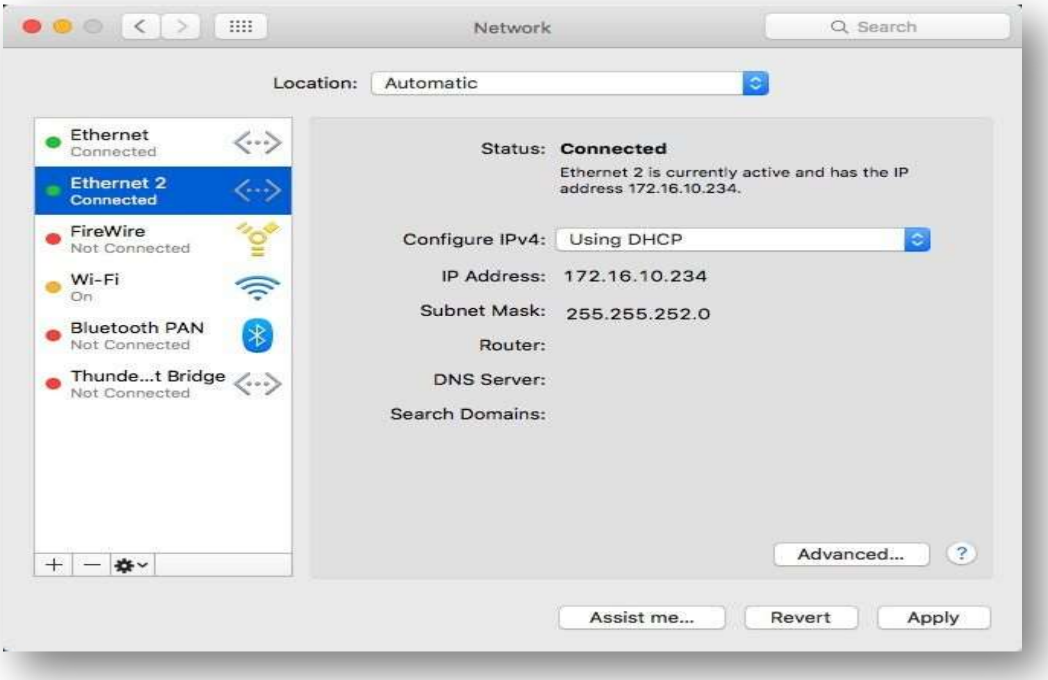


Figure 8-2-1 System setting

Step 2: Set the network card directly connected with port 3 of S3320, and set Ipv4 to get IP automatically.



Location: Automatic

Status: **Connected**

Ethernet 2 is currently active and has the IP address 172.16.10.234.

Configure IPv4: Using DHCP

IP Address: 172.16.10.234

Subnet Mask: 255.255.252.0

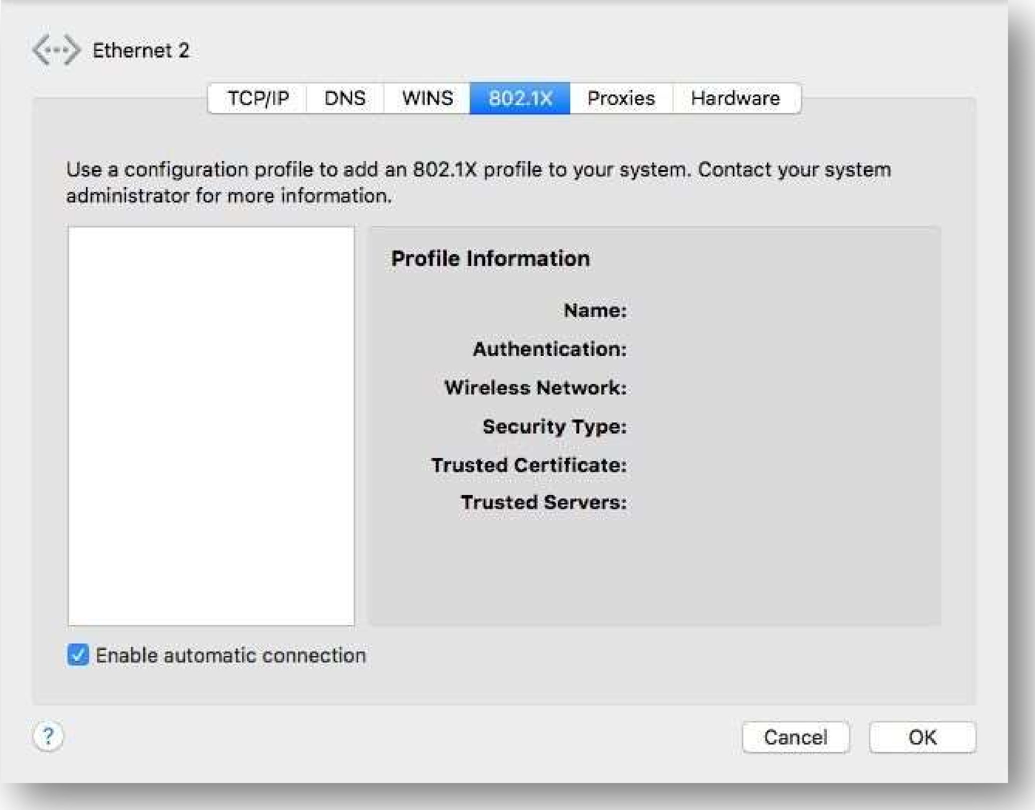
Router:

DNS Server:

Search Domains:

Figure 8-2-2 Network card configuration 1

Step 3: In the 802.1X configuration of the network card, tick **Enable automatical connection**.



Use a configuration profile to add an 802.1X profile to your system. Contact your system administrator for more information.

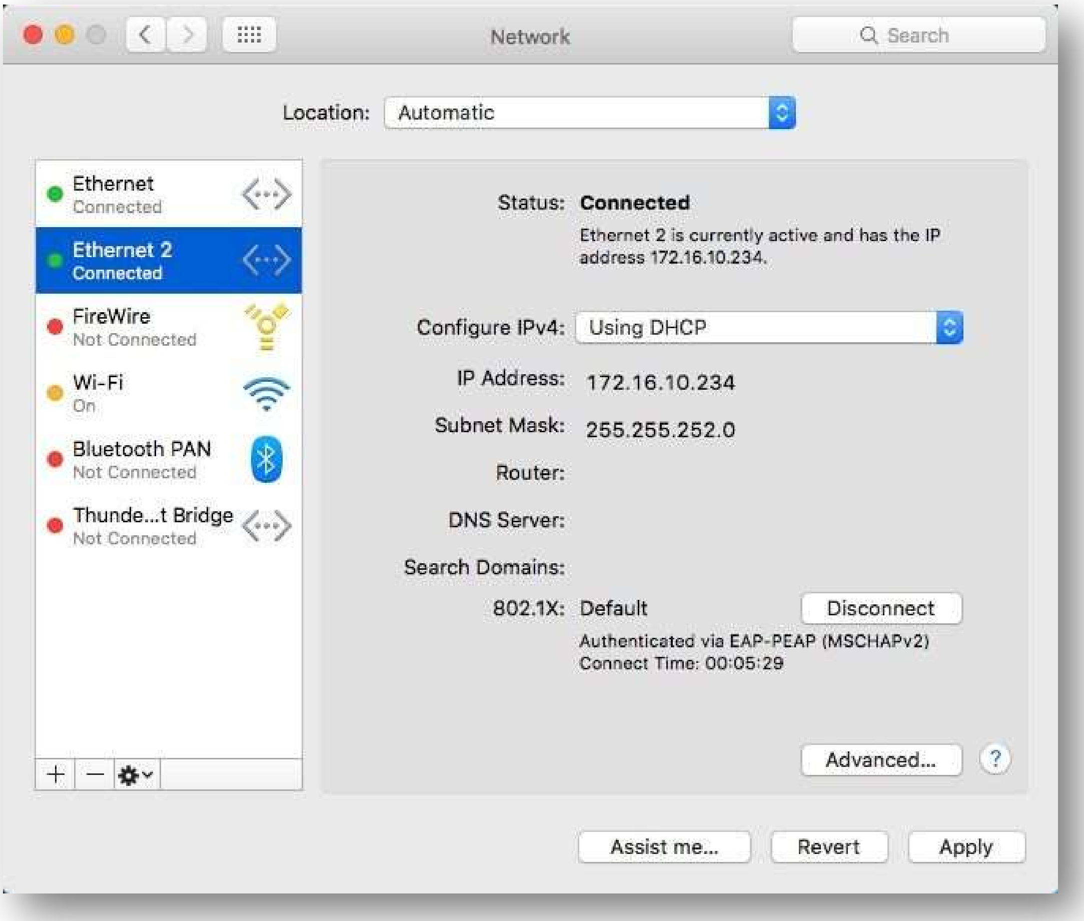
Profile Information

Name:
Authentication:
Wireless Network:
Security Type:
Trusted Certificate:
Trusted Servers:

☑ Enable automatic connection

Figure 8-2-3 Network card configuration 2

Step 4: After inputting the user name and password, MAC Pro automatically connects to the network.



Location: Automatic

Status: **Connected**

Ethernet 2 is currently active and has the IP address 172.16.10.234.

Configure IPv4: Using DHCP

IP Address: 172.16.10.234

Subnet Mask: 255.255.252.0

Router:

DNS Server:

Search Domains:

802.1X: Default

Authenticated via EAP-PEAP (MSCHAPv2)
Connect Time: 00:05:29

Figure 8-2-4 Network card connection

For the remaining check step, refer to step 6 of section 8.1.

8.3 Portal Authentication

After completing the above steps, you can start accessing Internet.

1. Use the mobile phone (or PC) terminal to connect the specified SSID. After connecting successfully, display the site home page. When the site is not displayed automatically, you need to manually open the browser to access any address (non-https website) and jump to the site home page. On the home page, you can see the home carousel figure, and tab advertisement. Click the advertisement, and you can see the specific advertisement content.

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved

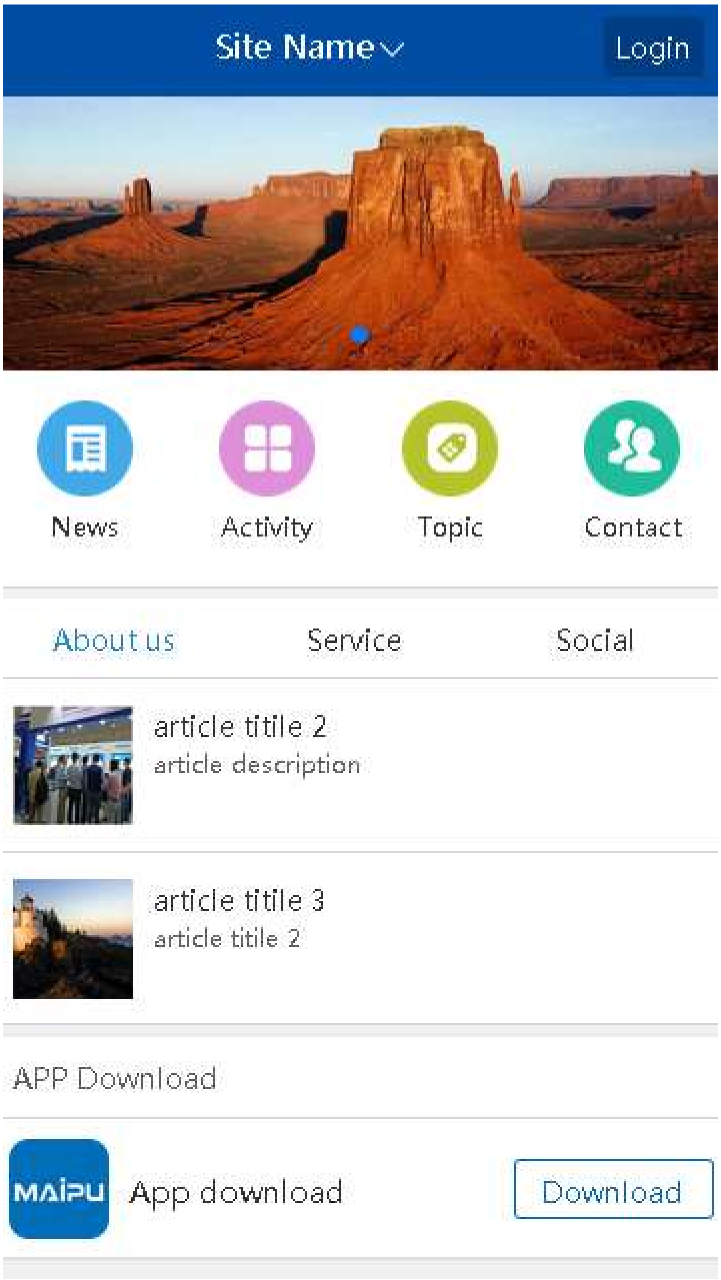
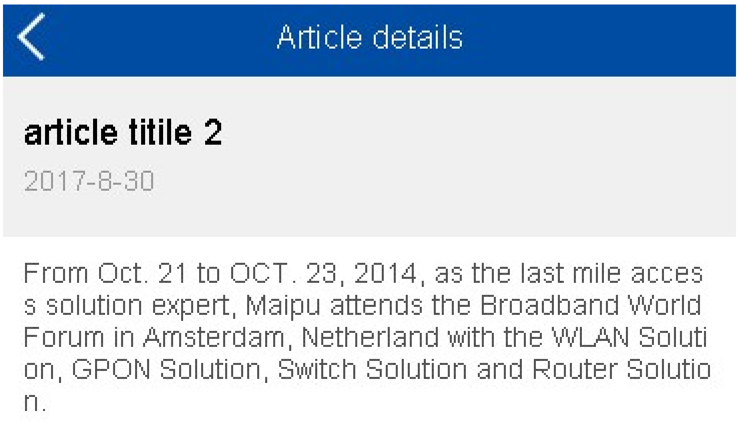


Figure 8-3-1 Site home



article titile 2

2017-8-30

From Oct. 21 to OCT. 23, 2014, as the last mile access solution expert, Maipu attends the Broadband World Forum in Amsterdam, Netherland with the WLAN Solution, GPON Solution, Switch Solution and Router Solution.

Figure 8-3-2 Advertisement details

2. On the site home page, you can click Login to enter the authentication page, as shown in the following figure, including mobile phone SMS authentication, inbuilt account authentication, and security authentication. Here, we just describe the authentication process via phone SMS.
3. Authentication by mobile phone: Open the mobile phone SMS authentication interface, input the phone number, click **Get verification code**, input the SMS verification code received by the mobile phone, tick **I have read and agreed Internet Agreement**, click **Login**, and the authentication succeeds.

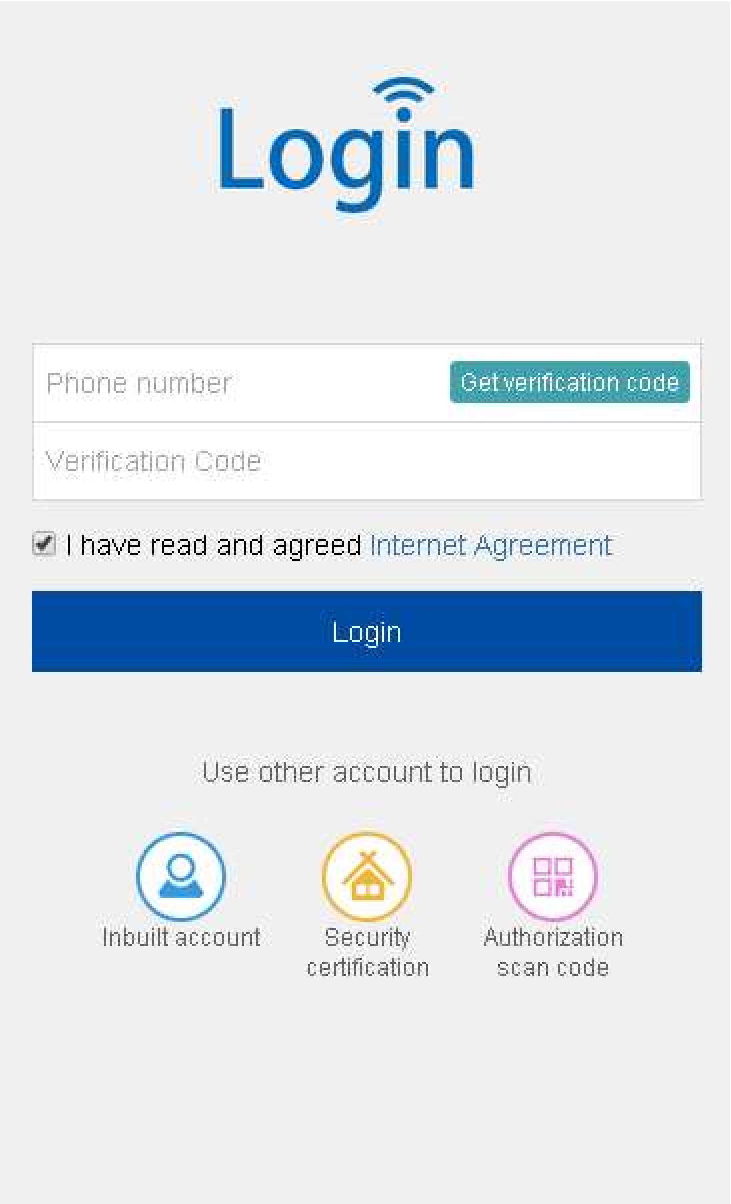


Figure 8-3-3 Authentication via mobile phone

4. After authenticating successfully, and if the advertisement countdown page is set, stop several seconds at the advertisement countdown page, and you can click the advertisement to read the advertisement content.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

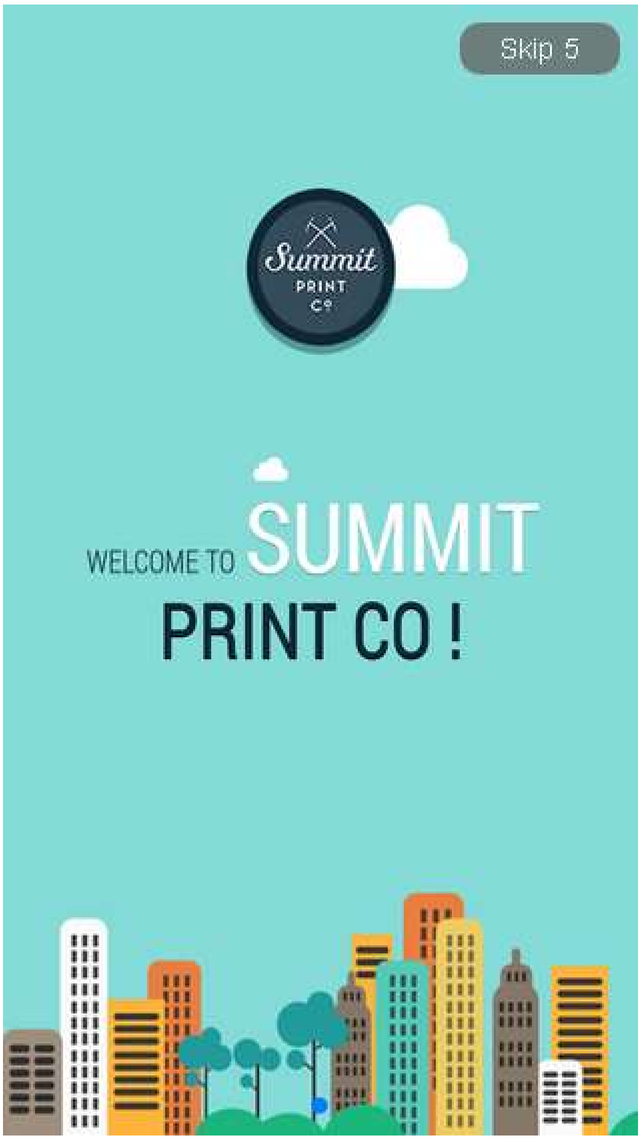


Figure 8-3-4 The page after authentication

5. The countdown of the advertisement page ends, jump to the home page. Here, the Internet authority is opened, and you can access other extranet addresses. Meanwhile, you can click **Exit** to end the Internet.

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved

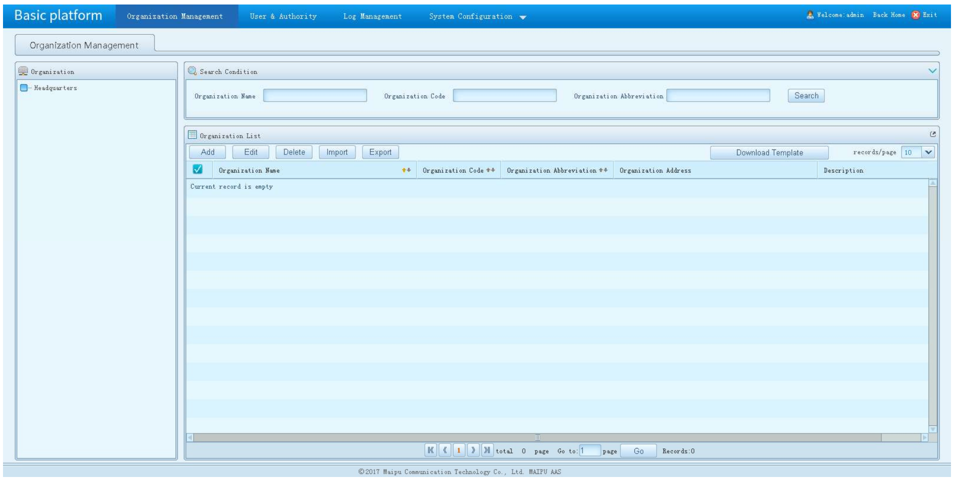
Part 3: Functions

9 Basic Platform Functions

Basic platform provides the functions of organization management, user and authority, log and system configuration for the user. The following describes the configuration of the basic platform.

9.1Organization Management

Click **Organization Management** to enter the organization management interface, providing the functions of querying, adding, modifying, deleting, importing and exporting the organization.

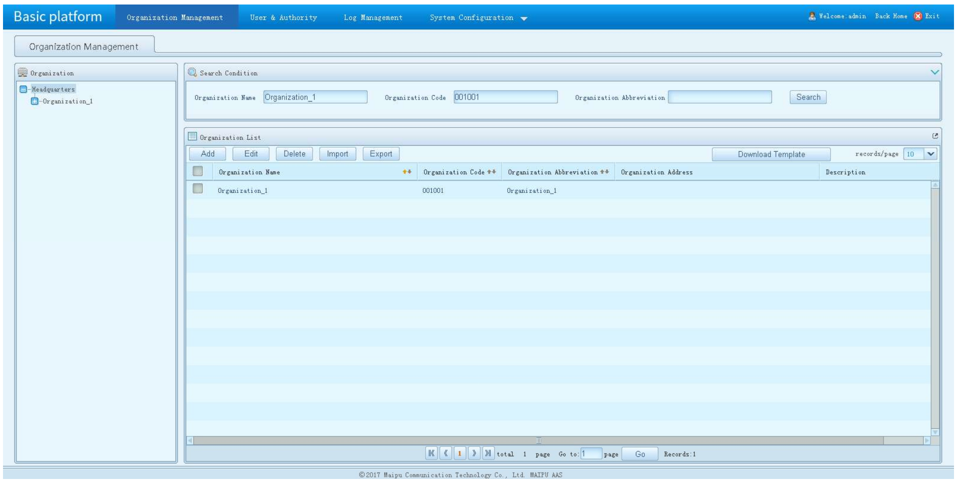


Current record is empty

Figure 9-1-1Organization management

Query the organization

You can query the organization according to the organization name, organization code and organization abbreviation, and also can only display the current organization. The queried content is displayed in the lower organization list by pages, as shown in Figure 9-1-2.



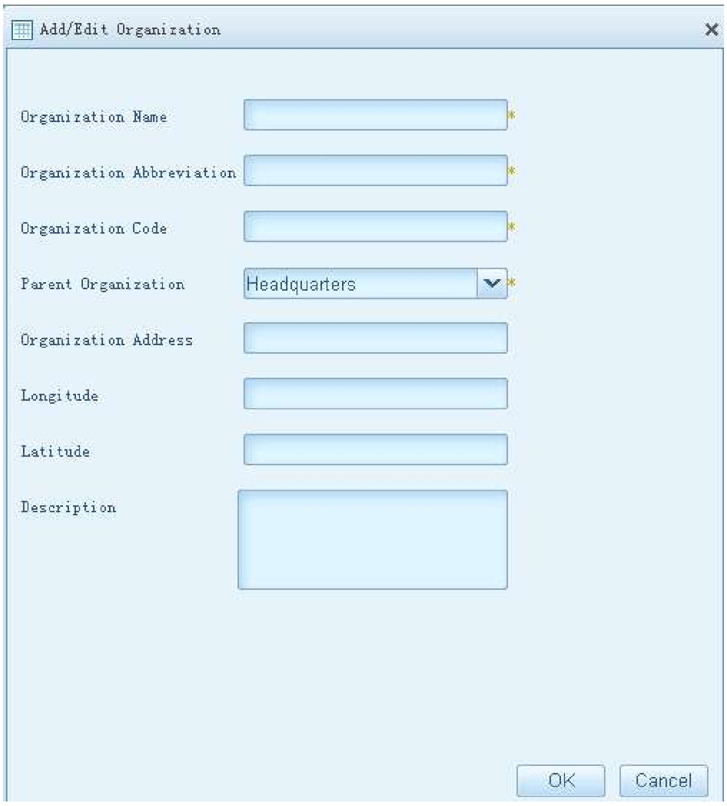
Organization Name: Organization_1
Organization Code: 001001
Organization Abbreviation:
records/page: 10

☐	Organization Name	Organization Code	Organization Abbreviation	Organization Address	Description
☐	Organization_1	001001	Organization_1		

Figure 9-1-2 Query the organization

Add an organization

Click **Add** to open the **Add/Edit Organization** dialog box. Fill in the information according to the actual demand, click **OK** and the organization is added.



Parent Organization: Headquarters

Figure 9-1-3 Add/modify the organization

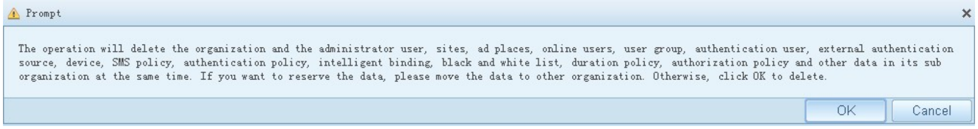
Modify an organization

All Rights Reserved

In the organization list, select one desired organization (you can only modify one organization at the same time), and click **Edit** to open the **Add/Edit Organization** dialog box (Figure 9-1-3). You can modify the organization name, organization abbreviation, organization code, parent organization, organization address, longitude, latitude, and description, and then, click **OK** to save the modified information.

Delete an organization

In the organization list, select one desired organization (you can select multiple organizations), click **Delete**, and click **OK** in the displayed dialog box (Figure 9-1-4). The system requires inputting the administrator password (Figure 9-1-5). After inputting the administrator login password correctly, you can delete the selected organization.



The operation will delete the organization and the administrator user, sites, ad places, online users, user group, authentication user, external authentication source, device, SMS policy, authentication policy, intelligent binding, black and white list, duration policy, authorization policy and other data in its sub organization at the same time. If you want to reserve the data, please move the data to other organization. Otherwise, click OK to delete.

Figure 9-1-4 Delete an organization

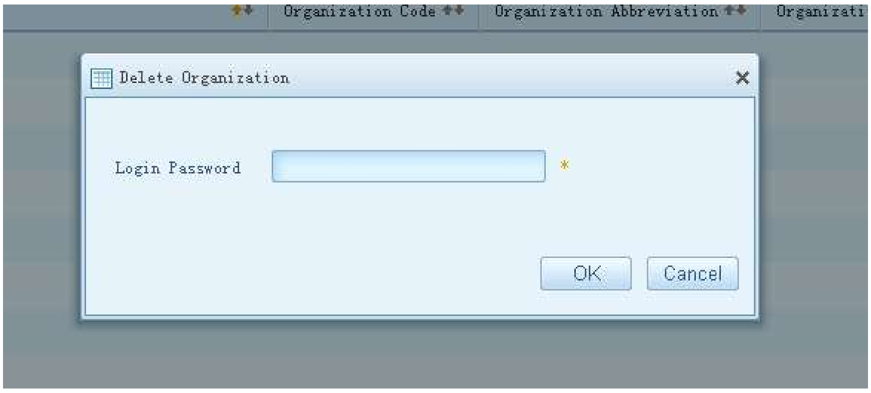


Figure 9-1-5 Input the login password when deleting an organization

Caution

- You cannot delete the default organization, that is, headquarters.
- The operation will delete the organization and the administrator user, online user, user group, authentication user, external authentication source, device, authentication policy, intelligent binding, black/white list, authorization policy and other data of its sub organization at the same time, so if you want to reserve the data, please move the data to other organization. If you do not want to reserve the data, click OK to delete.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

Import the organization

Before importing the organization, click **Download Template**, fill in according to the template content, and then, click **Import** to import the organization, as shown in Figure 9-1-5.

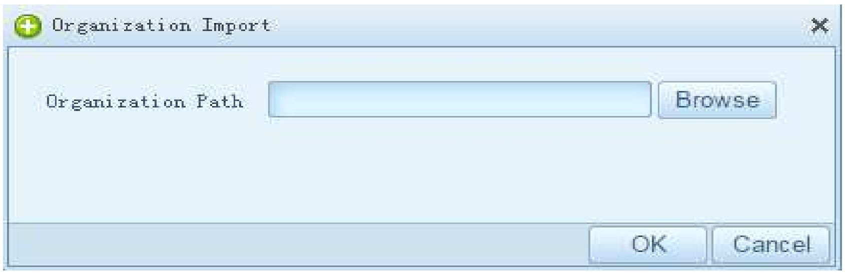


Figure 9-1-6 Import the organization

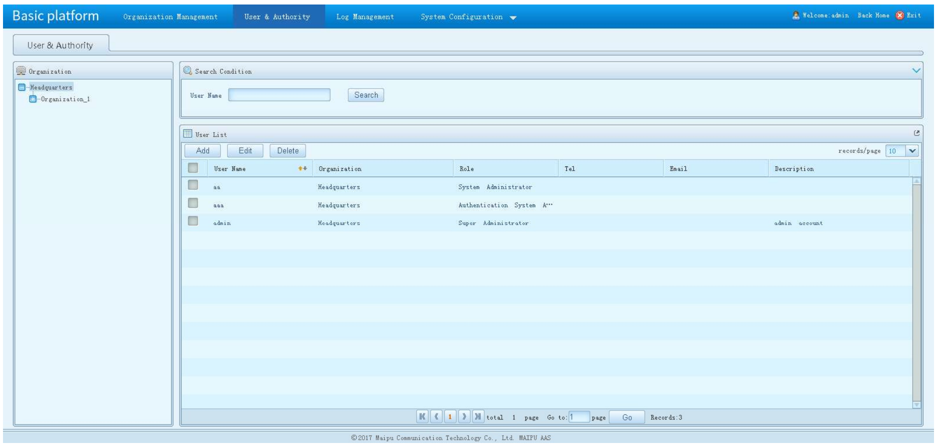
Export the organization

Click **Export** to export all available organizations of the current user.

9.2User & Authority

The basic platform adopts the matrix authority management, and the user needs to have the authority of the role authority and management area. User and authority management provides the centralized management for users and their authorities.

Click **User & Authority** to enter the user and authority management interface. The authority management interface provides the functions of querying, adding, modifying, and deleting the user.

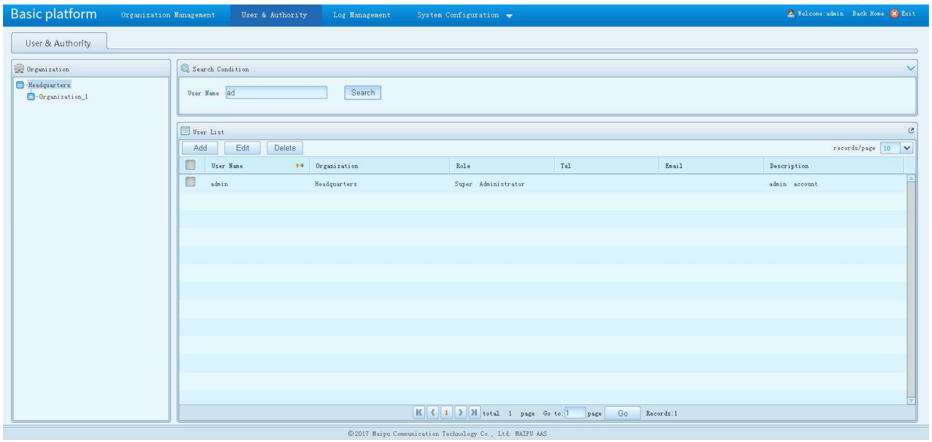


☐	User Name	Organization	Role	Tel	Email	Description
☐	aa	Headquarters	System Administrator			
☐	aaa	Headquarters	Authentication System A···			
☐	admin	Headquarters	Super Administrator			admin account

Figure 9-2-1 User and authority management

Query the user

The user query supports the fuzzy query of the user name, as shown in Figure 9-2-2.



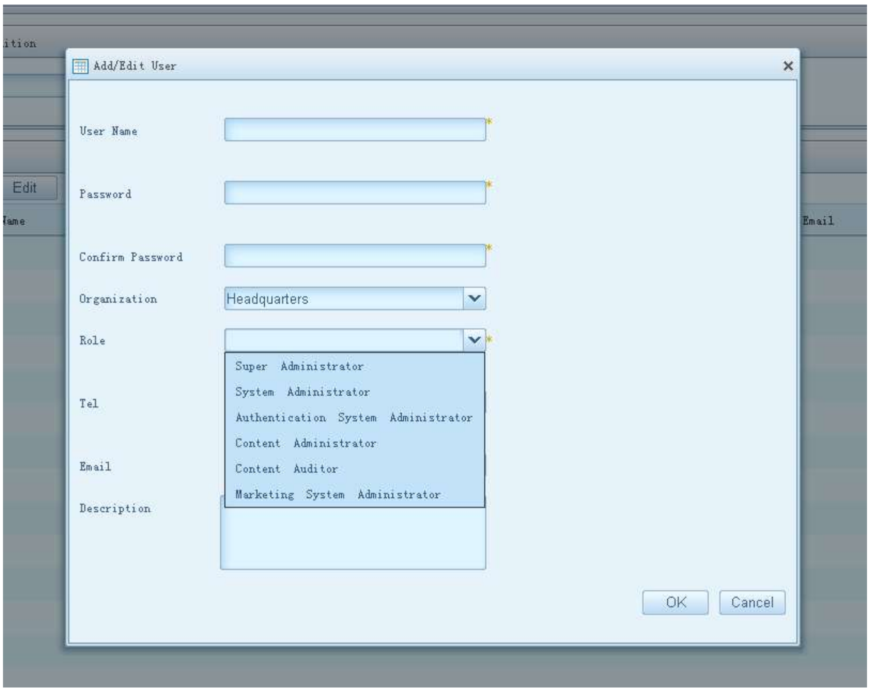
User Name: ad

User Name	Organization	Role	Tel	Email	Description
admin	Headquarters	Super Administrator			admin account

Figure 9-2-2 User query

Add a user

Click **Add** to add a new user. The user role can be super administrator, system administrator, authentication system administrator, content administrator, content auditor, and marketing system administrator. Fill in the information according to the actual demand, and click **OK**, as shown in Figure 9-2-3.



Organization: Headquarters

Figure 9-2-3 Add a user

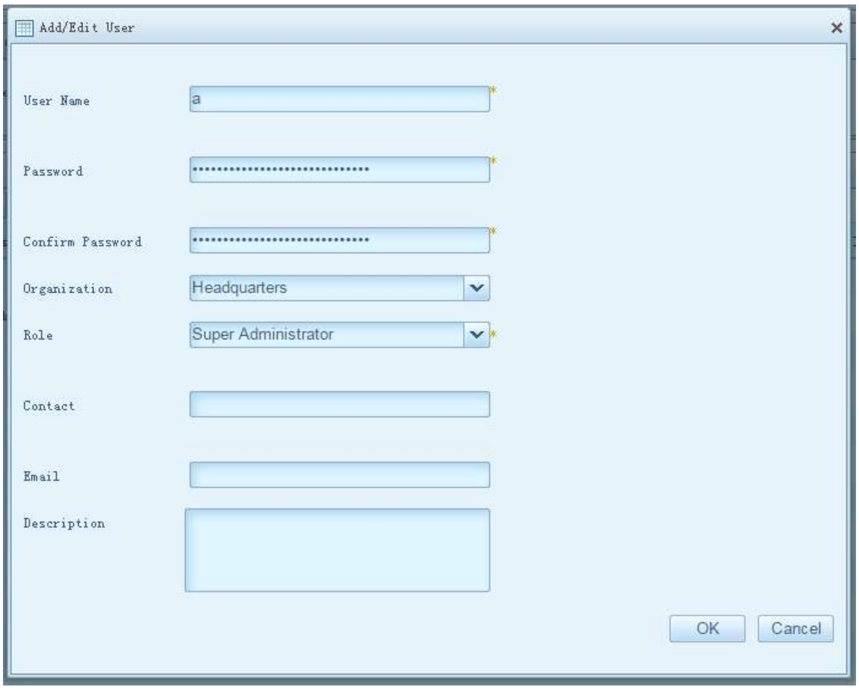
Note

- You cannot distribute the super administrator to the non-headquarter organization.
- After selecting the organization, the user can only manage the authority of the organization and its subordinate organizations.
- After selecting the organization when adding the administrator, the administrator can only have the authority of managing the organization and its subordinate organizations.
- The super administrator has the highest authority. The super administrator user can perform any operation.
- The system administrator has the system authorities of the organization and its subordinate organizations, except for import/export the organization, log management, system configuration, push policy management and external authentication source configuration,
- The authentication system administrator has all authorities of the organizations that can be managed by the authentication platform. The authentication system administrator user can only view the related interfaces of the authentication platform, and perform the operations of the related functions. The authentication system administrator user cannot access or operate the interfaces of the basic platform.
- The content administrator can advertise on the marketing platform and view and operate the online and offline services of the advertisement.
- The content auditor can audit the advertisements delivered by the organization and its subordinate organization administrators in the marketing platform.
- The marketing system administrator has all authorities of the services in the organization. The marketing system administrator can only access the marketing platform, and cannot view or operate other platforms.
- If enabling **Force modify initial password** (enable or disable on the password policy configuration interface) after creating one user, the user needs to modify the initial password when logging into the system for the first time.

Edit a user

Select one user record from the user list, and click **Edit** to edit the user information. You can modify the user name, password, organization, role, contact, email, and description.

After modifying, click **OK** to save the modified information, as shown in Figure 9-2-4.



User Name: a *
Password: ••••••••••••••••••••••••••••••• *
Confirm Password: ••••••••••••••••••••••••••••••• *
Organization: Headquarters
Role: Super Administrator *
Contact:
Email:
Description:

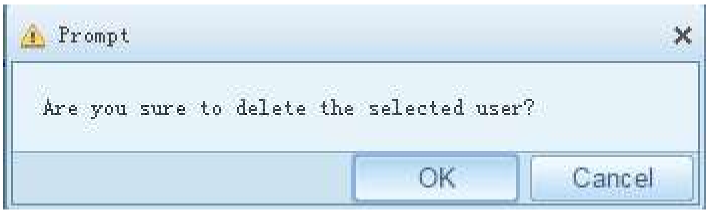
Figure 9-2-4 Modify one user

Note

- After enabling Force modify initial password (by default, it is enabled), and modifying the password of the subordinate administrator, the administrator needs to re-modify the password when logging into the system again.

Delete a user

Select one desired user from the user list, click **Delete**, and click **OK** in the displayed dialog box to delete the selected user, as shown in Figure 9-2-5:



Are you sure to delete the selected user?

Figure 9-2-5 Delete one user

copyright©2016Maipu Communication Technology Co., Ltd,

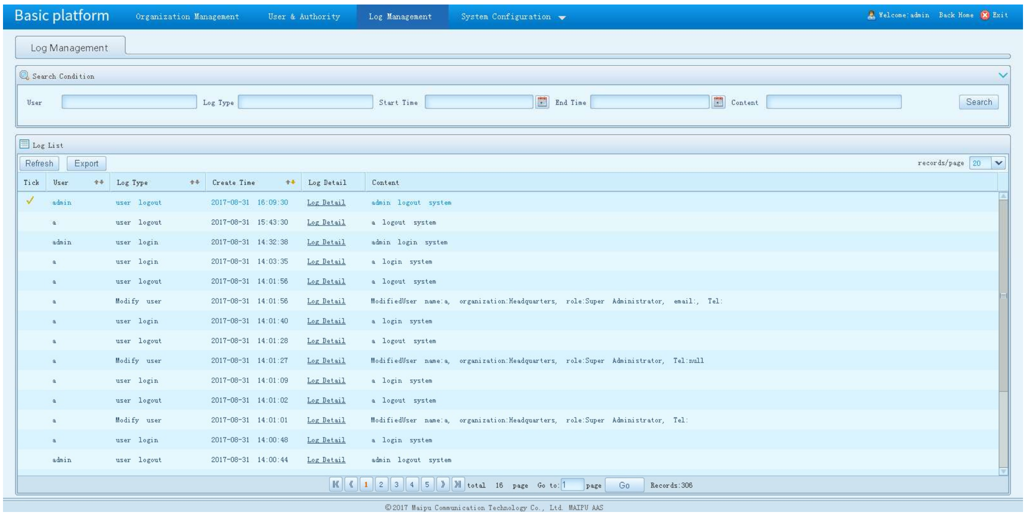
All Rights Reserved

Caution

- You cannot delete the default super administrator admin.

9.3 Log Management

Click **Log Management** to enter the log management interface, providing the functions of querying, exporting, and view the log.



Tick	User	Log Type	Create Time	Log Detail	Content
✓	admin	user logout	2017-08-31 16:09:30	Log Detail	admin logout system
	a	user logout	2017-08-31 15:43:30	Log Detail	a logout system
	admin	user login	2017-08-31 14:32:38	Log Detail	admin login system
	a	user login	2017-08-31 14:03:35	Log Detail	a login system
	a	user logout	2017-08-31 14:01:56	Log Detail	a logout system
	a	Modify user	2017-08-31 14:01:56	Log Detail	ModifiedUser name:a, organization:Headquarters, role:Super Administrator, email:, Tel:
	a	user login	2017-08-31 14:01:40	Log Detail	a login system
	a	user logout	2017-08-31 14:01:28	Log Detail	a logout system
	a	Modify user	2017-08-31 14:01:27	Log Detail	ModifiedUser name:a, organization:Headquarters, role:Super Administrator, Tel:null
	a	user login	2017-08-31 14:01:09	Log Detail	a login system
	a	user logout	2017-08-31 14:01:02	Log Detail	a logout system
	a	Modify user	2017-08-31 14:01:01	Log Detail	ModifiedUser name:a, organization:Headquarters, role:Super Administrator, Tel:
	a	user login	2017-08-31 14:00:48	Log Detail	a login system
	admin	user logout	2017-08-31 14:00:44	Log Detail	admin logout system

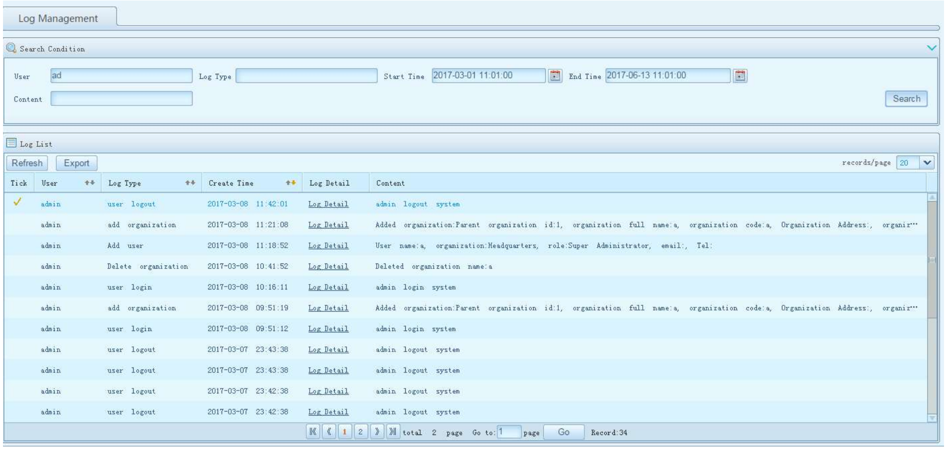
Figure 9-3-1 Log management

Log query

The log management provides the management for the log information. You can search for the desired log information by the user, start time, end time, log type and log level, advanced query. The advanced query can perform the fuzzy query for the user name, log type, level, and content at the same time.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved



User ad
Log Type
Start Time 2017-03-01 11:01:00
End Time 2017-06-13 11:01:00
Content

records/page 20

Tick	User	Log Type	Create Time	Log Detail	Content
✓	admin	user logout	2017-03-08 11:42:01	Log Detail	admin logout system
	admin	add organization	2017-03-08 11:21:08	Log Detail	Added organization:Parent organization id:1, organization full name:a, organization code:a, Organization Address:, organiz···
	admin	Add user	2017-03-08 11:18:52	Log Detail	User name:a, organization:Headquarters, role:Super Administrator, email:, Tel:
	admin	Delete organization	2017-03-08 10:41:52	Log Detail	Deleted organization name:a
	admin	user login	2017-03-08 10:16:11	Log Detail	admin login system
	admin	add organization	2017-03-08 09:51:19	Log Detail	Added organization:Parent organization id:1, organization full name:a, organization code:a, Organization Address:, organiz···
	admin	user login	2017-03-08 09:51:12	Log Detail	admin login system
	admin	user logout	2017-03-07 23:43:38	Log Detail	admin logout system
	admin	user logout	2017-03-07 23:43:38	Log Detail	admin logout system
	admin	user logout	2017-03-07 23:42:38	Log Detail	admin logout system
	admin	user logout	2017-03-07 23:42:38	Log Detail	admin logout system

1 2 total 2 page Go to: 1 page Go Record:34

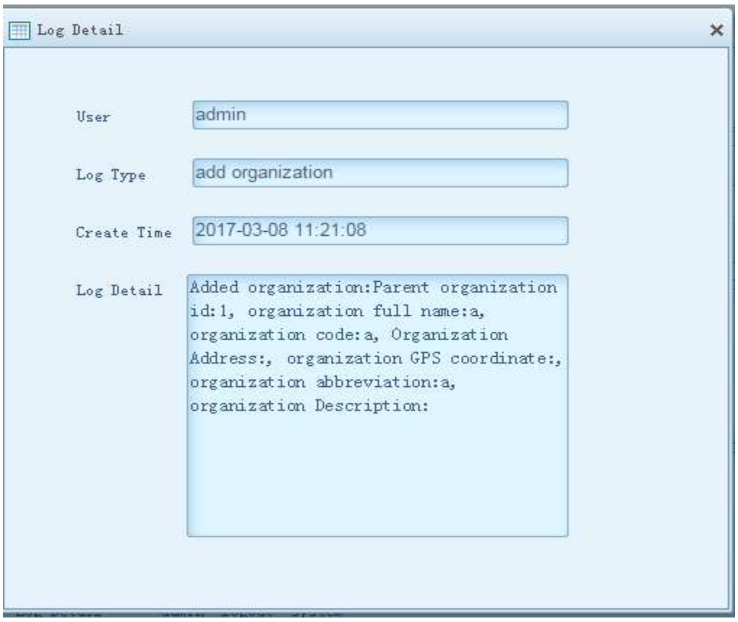
Figure 9-3-2 Log query

Export the log

Click **Export**, and you can export the log information in the list to the csv file.

Log details

The **Content** field of the log list lists the summary content of the log. To view the details of the log, you can click **Log Detail** to open the **Log Detail** dialog box, as shown in Figure 9-3-3.



User admin
Log Type add organization
Create Time 2017-03-08 11:21:08
Log Detail Added organization:Parent organization id:1, organization full name:a, organization code:a, Organization Address:, organization GPS coordinate:, organization abbreviation:a, organization Description:

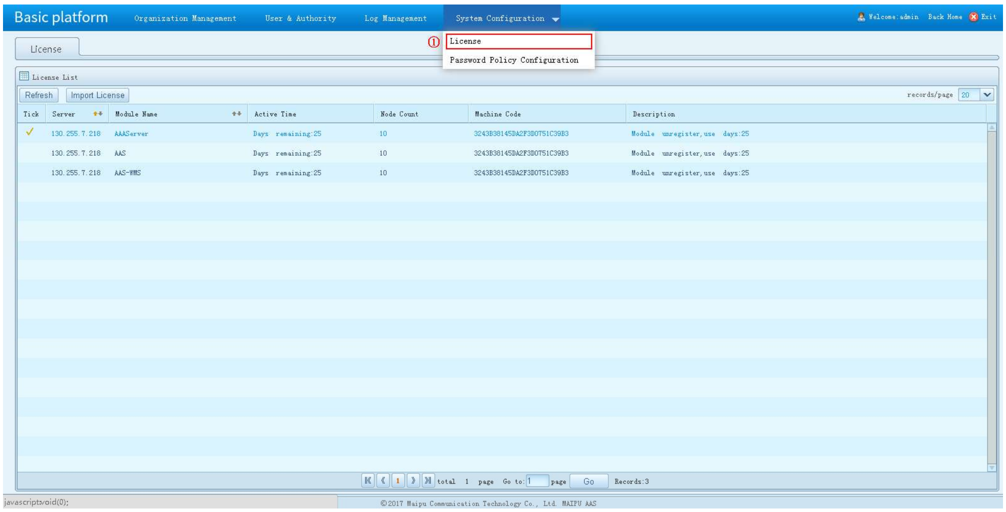
Figure 9-3-3 Log details

9.4 System Configuration

9.4.1 License

Select **System Configuration** > **License** to enter the License management interface, as shown in Figure 9-4-1.

The license management provides the functions of viewing the license and importing the component license, as shown in Figure 9-4-1.



Tick	Server	Module Name	Active Time	Node Count	Machine Code	Description
✓	130.255.7.218	AAAServer	Days remaining:25	10	3243B38145DA2F3D0751C39B3	Module unregister,use days:25
	130.255.7.218	AAS	Days remaining:25	10	3243B38145DA2F3D0751C39B3	Module unregister,use days:25
	130.255.7.218	AAS-WMS	Days remaining:25	10	3243B38145DA2F3D0751C39B3	Module unregister,use days:25

Records:3

Figure 9-4-1 License management

View the License

Click **Refresh** and you can view the latest license information (Figure 9-4-1).

Import the license

Click **Import license** to open the License Import dialog box, as shown in Figure 9-4-2.

Click **Browse**, and select the .lic file. After selecting the correct.lic file, click **Import** and you can complete the operation of importing the new license.

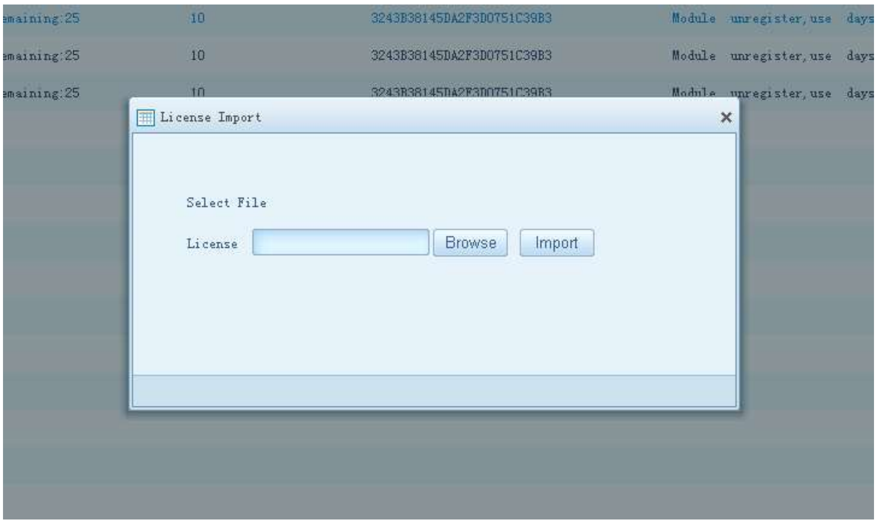
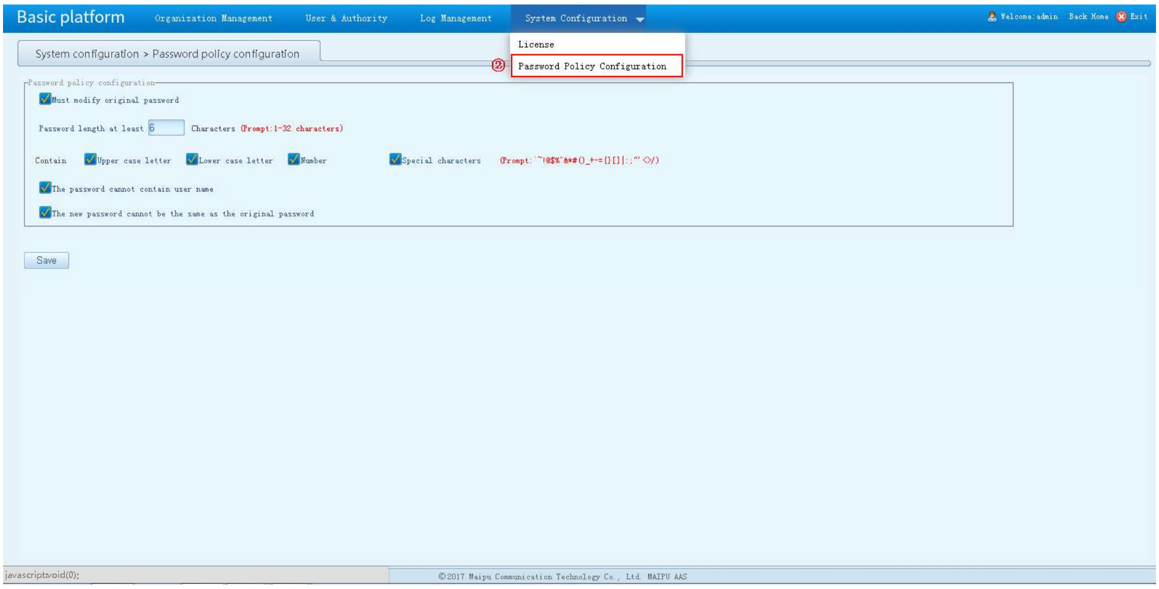

emaining:25 10 3243B38145DA2F3D0751C39B3 Module unregister,use days
emaining:25 10 3243B38145DA2F3D0751C39B3 Module unregister,use days
emaining:25 10 3243B38145DA2F3D0751C39B3 Module unregister,use days
License Import
Select File
License
Browse
Import

Figure 9-4-2Import the license

9.4.2 Password Policy Configuration

Select **System Configuration** > **Password Policy Configuration** to enter the password configuration interface, as shown in Figure 9-4-3.

The password policy configuration interface provides the function of setting the password rule and password complexity. On the interface, you can configure whether to force modify original password, minimum length of the password, whether the password contains the upper case letter, lower case letter, number, special character, or user name, and whether the new password is the same as the original password, as shown in Figure 9-4-3. After configuring the password policy, click **Save** to complete the configuration of the password policy.


Basic platform
Organization Management
User & Authority
Log Management
System Configuration
Welcome:admin
Back Home
Exit
License
②
Password Policy Configuration
System configuration > Password policy configuration
Password policy configuration
Save
javascript:void(0);
©2017 Maipu Communication Technology Co., Ltd. MAIPU AAS

☑ Must modify original password

Password length at least 6 Characters (Prompt:1-32 characters)

Contain ☑ Upper case letter ☑ Lower case letter ☑ Number ☑ Special characters (Prompt: `~!@$%^&*#()_+-={}[]|:;"' <>/)

☑ The password cannot contain user name

☑ The new password cannot be the same as the original password

Figure 9-4-3 Password policy configuration

Note

- The complicated password policy can improve the system security.
- By default, the system enables the high-level password configuration policy.

9.5 Service Management

The following commands need to enter the Linux server command line terminal to execute.

Configuration Command	Description
service srvmgt init	Initialize the local service
service srvmgt status	View the configured service operation status of the system
service srvmgt start	Enable all services of the system
service srvmgt start {srv_name}	Enable one service, such as service srvmgt start aasnode
service srvmgt stop	Stop all services of the system
service srvmgt stop {srv_name}	Stop one service, such as service srvmgt stop aasnode
service srvmgt restart	Restart all services of the system
service srvmgt restart {srv_name}	Restart one service, such as service srvmgt restart aasnode
service srvmgt list	View which services are configured
service srvmgt config srvlist	Customize the service starting list
Servicesrvmgt config db dbload-frompeer	In the HA mode, completely synchronize the data of the peer database to the local

---

Caution

- The command **service srvmgt config srvlist** is the high-risk command, and should be executed carefully.

9.6 HA Configuration and Management

HA configuration and management is used when there are the standby and active servers, and provides the commands for configuring and managing HA. The commands need to be executed in the command line of Linux server.

Configuration Command	**Description**
service mpha show	View the HA configuration
service mpha takeover	Switch the standby server to the active server
service mpha standby	Switch the active server to the standby server
service mpha start	Start HA
service mpha stop	Stop HA
service mpha status	View the HA status
service mpha shutdown	Force to stop HA

9.7 Backup, Recover and Dump

Configuration Command	**Description**
/home/mpup/mpupdefault/bin/backup.sh config	Back up the parameter configuration
/home/mpup/mpupdefault/bin/backup.sh backup	Back up the current configuration and database
/home/mpup/mpupdefault/bin/backup.sh resume {filepath}	Restore the current configuration and database from the file
/home/mpup/mpupdefault/bin/db.sh dumpconfig	Dump the parameter configuration

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved

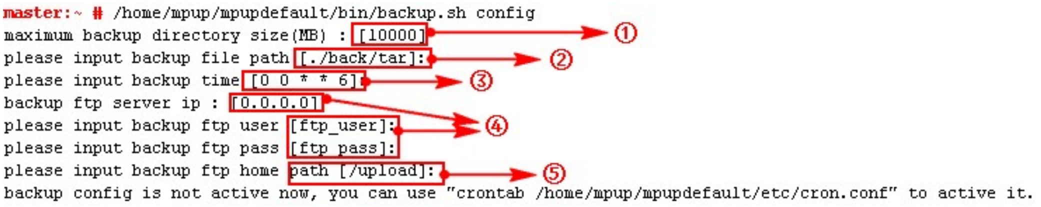
/home/mpup/mpupdefault/bin/db.sh backup	Back up the database
/home/mpup/mpupdefault/bin/db.sh resume {filepath}	Restore the current database from the file
/home/mpup/mpupdefault/bin/db.sh dump	Dump the current database

Back up configuration file and data

The system supports backing up the data and configuration file in the database manually and automatically. The auto backup of the system needs to be configured and enabled in advance.

On the server installed with the software, execute the following command to configure the timing backup function:

/home/mpup/mpupdefault/bin/backup.sh config



```
master:~ # /home/mpup/mpupdefault/bin/backup.sh config
maximum backup directory size(MB) : [10000]
please input backup file path [./back/tar]:
please input backup time [0 0 * * 6]:
backup ftp server ip : [0.0.0.0]
please input backup ftp user [ftp_user]:
please input backup ftp pass [ftp pass]:
please input backup ftp home path [/upload]:
backup config is not active now, you can use "crontab /home/mpup/mpupdefault/etc/cron.conf" to active it.
```

Figure 9-7-1 Configuration file and data backup

Note

- ① indicates the maximum directory storage space. When the backup directory size is larger than the maximum, the backup tool will automatically delete the earlier backup file in the directory, making the backup directory size smaller than the maximum and avoiding that the disk is used up. Meanwhile, reserve one backup file at least.
- ② indicates the absolute path of backing up to the local device.
- ③Crontab expression mode, indicating the period of executing backup. For the using mode, refer to the following description.
- ④indicates the address of the FTP server, user name and password.
- ⑤ indicates the absolute path of backing up to the FTP server.

please input backup time[0 0 * * 6]: indicates the time of executing the timing backup; the time format is Linux Crontab time format. The meanings of the crontab time format fields are as follows:

The first field indicates the minute, ranging 0-59;

The second field indicates the hour, ranging 0-23 (0 indicates midnight);

The third field indicates date, ranging 1-31;

The fourth field indicates month, ranging 1-12;

The fifth field indicates weekday, ranging 0-6 (0 indicates the Sunday);

For example:

15 0 * * * indicates 0:15 every night

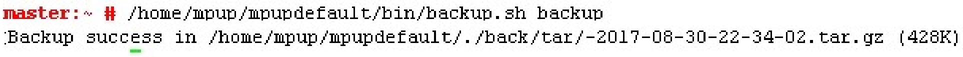
0 0 * * 0 indicates 0 a.m. of every Sunday

0 0 1,10,22 * * indicates 0 a.m. of 1st, 10th, and 22th in every month

After setting, prompt executing the command **crontab /home/mpup/mpupdefault/etc/cron.conf** to enable the timing backup function.

Execute the following command, and you can manually trigger the backup task immediately. After backup, display the path of saving the current backup file:

/home/mpup/mpupdefault/bin/backup.sh backup



```
master:~ # /home/mpup/mpupdefault/bin/backup.sh backup
Backup success in /home/mpup/mpupdefault/./back/tar/-2017-08-30-22-34-02.tar.gz (428K)
```

Figure 9-7-2 execute the backup task

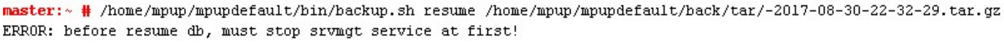
Configuration and data recovery

Use the system backup file, and you can perform the database and configuration file recovery. The recovery command should specify the relative or absolute path of the backup file:

/home/mpup/mpupdefault/bin/backup.sh resume {filepath}

{filepath} needs to be replaced as the correct backup file path. Before executing the command, you need to first stop the srvmgt service, as shown in Figure 9-7-3. Use the following command to stop the srvmgt service:

service srvmgt stop



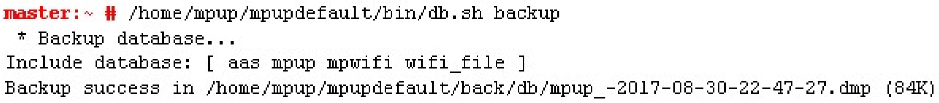
```
master:~ # /home/mpup/mpupdefault/bin/backup.sh resume /home/mpup/mpupdefault/back/tar/-2017-08-30-22-32-29.tar.gz
ERROR: before resume db, must stop srvmgt service at first!
```

Figure 9-7-3 Stop the service first before recovering the configuration file

Database backup

The system supports that the command only backs up the data in the database. The backup command is as follows:

/home/mpup/mpupdefault/bin/db.sh backup



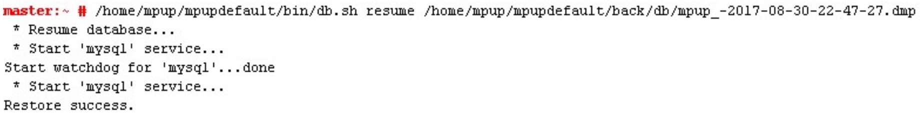
```
master:~ # /home/mpup/mpupdefault/bin/db.sh backup
 * Backup database...
Include database: [ aas mpup mpwifi wifi_file ]
Backup success in /home/mpup/mpupdefault/back/db/mpup_-2017-08-30-22-47-27.dmp (84K)
```

Figure 9-7-4Database backup

Database recovery

The system supports the command to recover the database from the backup database file:

/home/mpup/mpupdefault/bin/db.sh resume {filepath} executes recovering the data of the database from the file. {filepath} indicates the absolute path of the complete backup file:



```
master:~ # /home/mpup/mpupdefault/bin/db.sh resume /home/mpup/mpupdefault/back/db/mpup_-2017-08-30-22-47-27.dmp
 * Resume database...
 * Start 'mysql' service...
Start watchdog for 'mysql'...done
 * Start 'mysql' service...
Restore success.
```

Figure 9-7-5 Database recovery

Note

- If prompting "ERROR: before resume db, must stop srvmgt service at first!" when recovering the database, please first use the command **service srvmgt stop** to stop the srvmgt service.

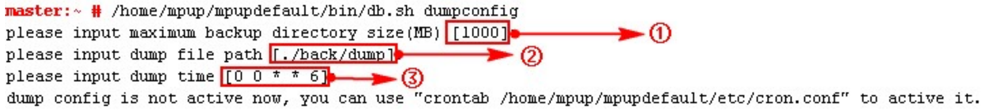
Database dump

The system supports dumping the alarm data and log data timely, supporting manual dump and auto dump. The auto dump needs to be configured and enabled in advance.

Execute the following command, and you can configure the auto dump:

/home/mpup/mpupdefault/bin/db.sh dumpconfig

After setting, you need to execute the command crontab /home/mpup/mpupdefault/etc/cron.conf to enable the timing dump function.



```
master:~ # /home/mpup/mpupdefault/bin/db.sh dumpconfig
please input maximum backup directory size(MB) [1000]
please input dump file path [./back/dump]
please input dump time [0 0 * * 6]
dump config is not active now, you can use "crontab /home/mpup/mpupdefault/etc/cron.conf" to active it.
```

Figure 9-7-6 Configure auto dump

Note

- ① indicates the threshold of the maximum dump file. When multiple dumping generate multiple files, and the total size of the dump directory exceeds the threshold, the system automatically clears the oldest file until the total size of the dump directory is smaller than the threshold.
- ② indicates the absolute path of dumping to the local device.
- ③ indicates the auto dump period, and the format complies with the Linux crontab expression mode.

After executing the dump configuration, you can execute the following command to dump immediately:

/home/mpup/mpupdefault/bin/db.sh dump

10 Authentication Platform Functions

The authentication platform provides the functions of viewing the online user, managing users, and configuring various authentication, pushing, and authorization policies for the user. The following describes the related function of the authentication platform.

10.1Online User

Online User provides the function of querying the online users of Portal, 802.1x, VPN, dialing and other authentication scenarios for the user. Meanwhile, the administrator can select one user to tick offline, as shown in the following figure:

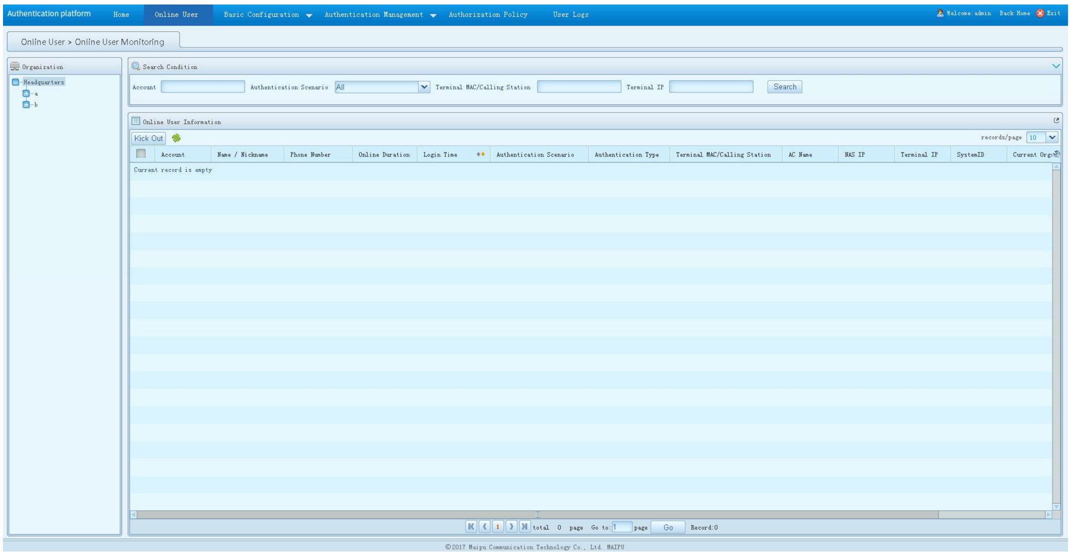


Figure 10-1 Online user

Caution

- Users who are actively kicked cannot continue to access the Internet or perform the no-perception authentication, but need to re-authenticate, and then, can access the Internet.

10.2 Basic Configuration

10.2.1User and User Group

10.2.1.1 User management

Click **Basic Configuration** > **User and User Group** to enter the User Management interface, as shown in the following figure:

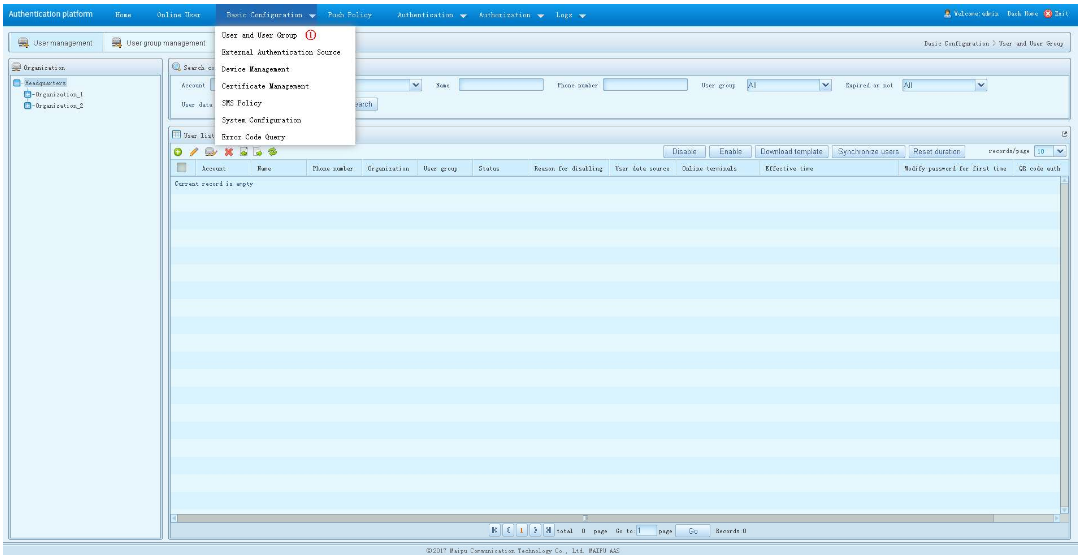


Figure 10-2-1 User Management

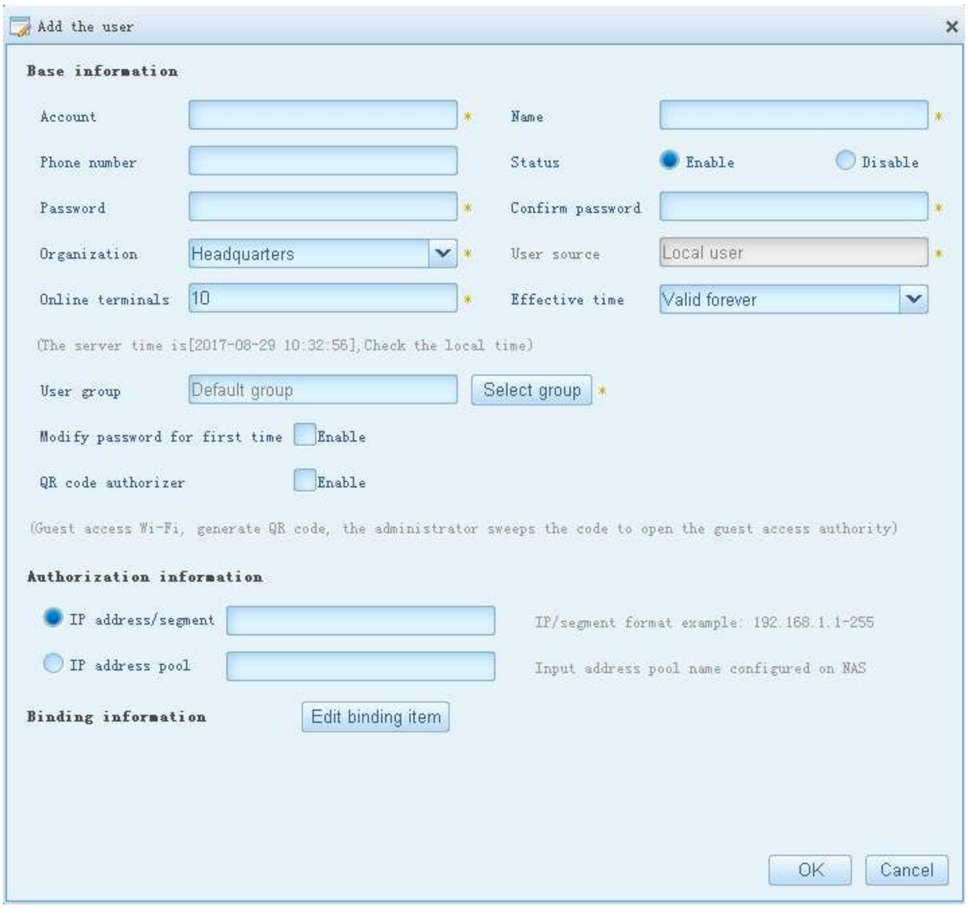
User Management provides the management of the authentication account functions, including the basic functions of querying, adding, modifying, deleting, importing and exporting the account. Meanwhile, provide the advanced functions of batch editing accounts, batch disabling/enabling accounts, and synchronizing the external authentication source account and so on.

Add a user

Click **Add** to enter the **Add the user** dialog box, which provides the basic information of the user, as shown in the following figure:

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved



Status: ● Enable ○ Disable

Organization: Headquarters *

User source: Local user *

Online terminals: 10 *

Effective time: Valid forever

(The server time is[2017-08-29 10:32:56],Check the local time)

User group: Default group *

Modify password for first time ☐ Enable

QR code authorizer ☐ Enable

(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)

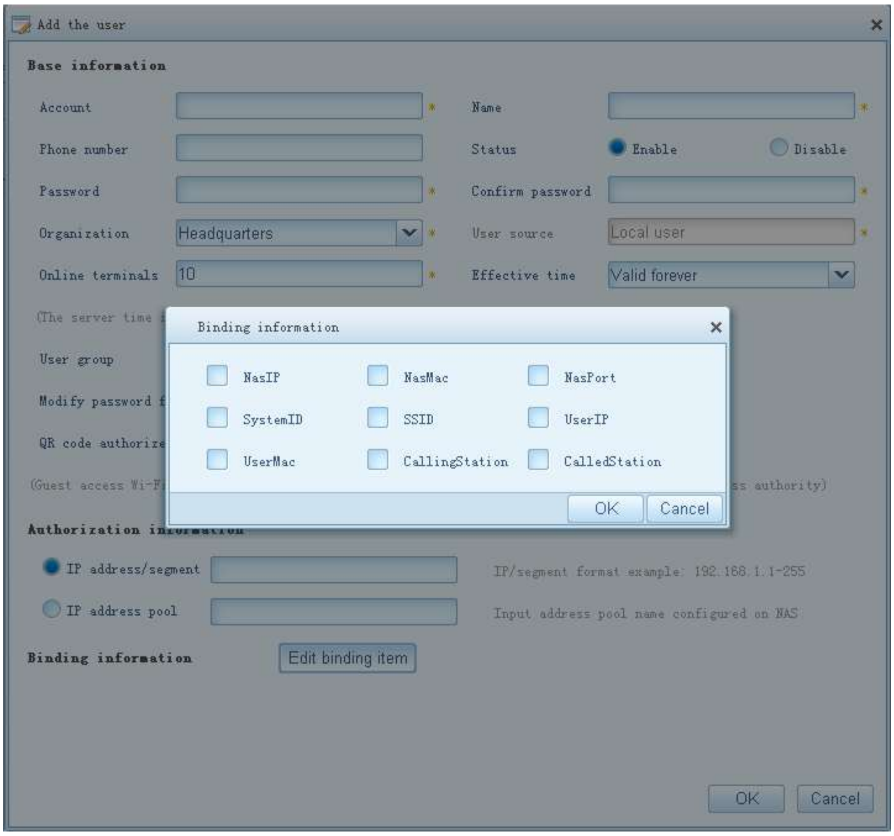
● IP address/segment — IP/segment format example: 192.168.1.1-255

○ IP address pool — Input address pool name configured on NAS

Figure 10-2-2 Add the user

1. Binding information

Click **Edit binding item** to select the desired user information. Use the semicolon to separate multiple values, such as Nas IP attribute, 192.168.0.1;192.168.0.2



Organization: Headquarters
User source: Local user
Online terminals: 10
Effective time: Valid forever

Figure 10-2-3 Binding information

2. Guest two-dimensional code authorizer

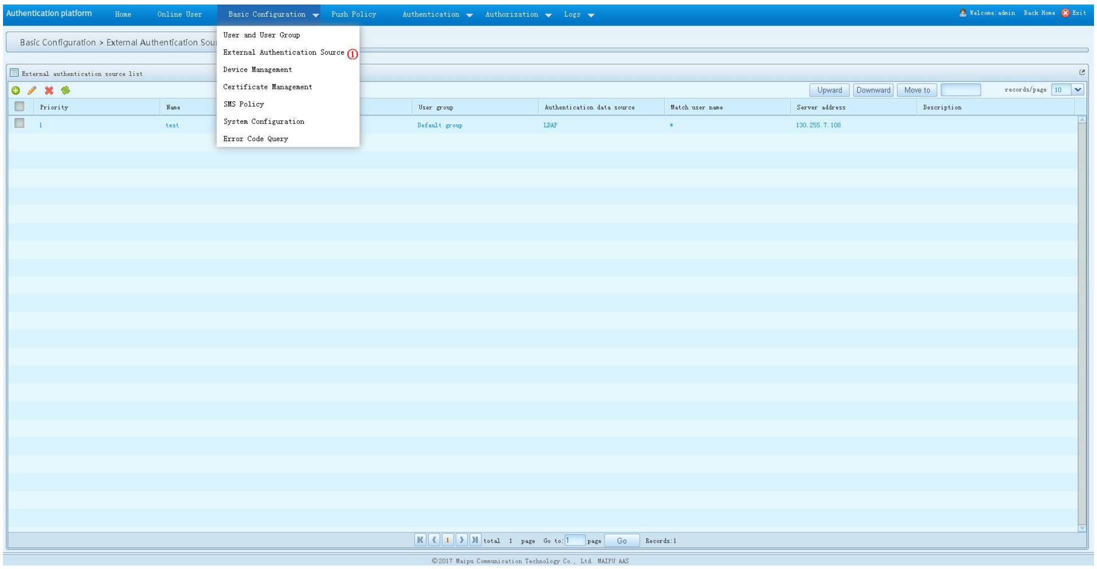
If configuring the login mode by “Authorization QR code” in the “Marketing Platform” login mode, you can select specifying one user as “QR code authorizer” in one organization when adding one user, that is, click the **QR code authorizer** button to process the network access request of the guest.

The steps of using the authorization QR code:

1. Configure the “Authorization QR code” login mode in “Marketing Platform”;
2. After the guest selects the authentication mode, fill in the basic information and generate the QR code for the authorizer to scan;
3. The authorizer scans the QR code to authorize the network access.

Synchronize the user

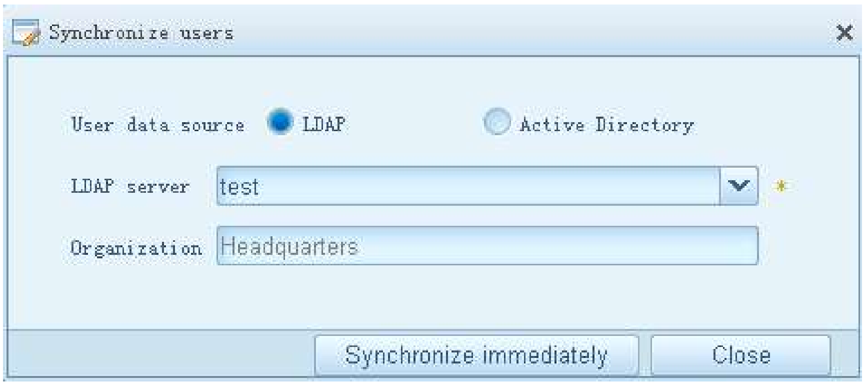
Select **Basic Configuration** > **External Authentication Source**, and add one LDAP or AD information, as shown in the following figure:



Priority	Name	User group	Authentication data source	Match user name	Server address	Description
1	test	Default group	LDAP	*	130.255.7.108	

Figure 10-2-4 External authorization source

Return to the “**User management**” interface and click **Synchronize users** to display the Synchronize users dialog box, as shown in the following figure:



User data source ● LDAP ○ Active Directory

LDAP server test *

Organization Headquarters

Figure 10-2-5 Synchronize the user

After selecting the user data source type, select the desired server (the information added in “External Authentication Source”), and click “**Synchronize immediately**”. If there is the user of the external authentication source server in the user management list, it indicates that the user is synchronized successfully.

Caution

- The organization of the synchronized user will keep consistent with the organization configured in the external authentication source.
- If configuring the “Status” of the user as “Disable”, the authentication of the

user will fail, and as a result, the user cannot access the network.

- When one user group is deleted, the related policies and instances will become invalid.

10.2.1.2 User group management

Select **Basic Configuration** > **User and User Group** to enter the **User management** interface. Click **User group management** to enter the **User group management** interface. The user group management interface mainly provides the functions of adding, deleting, and querying and so on, as shown in the following figure:

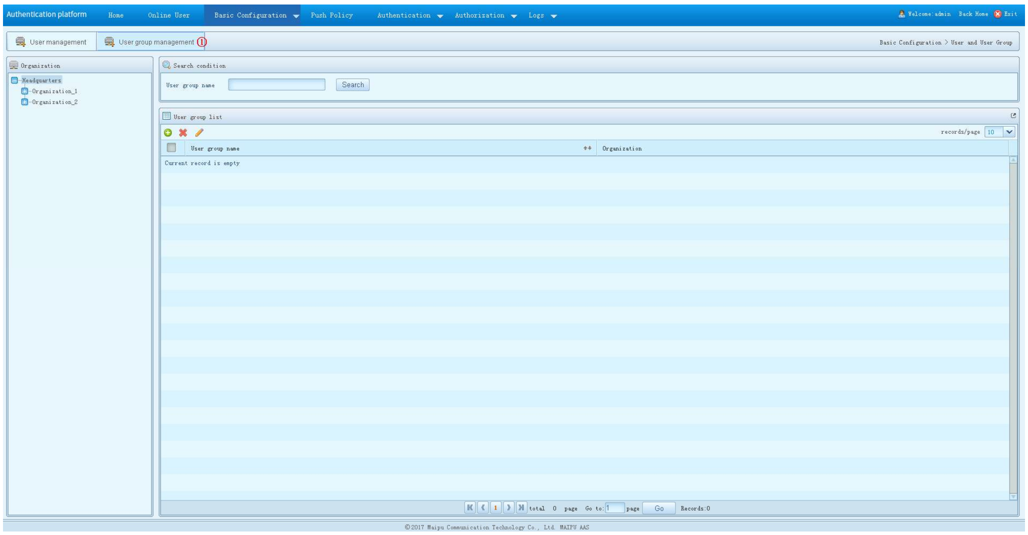


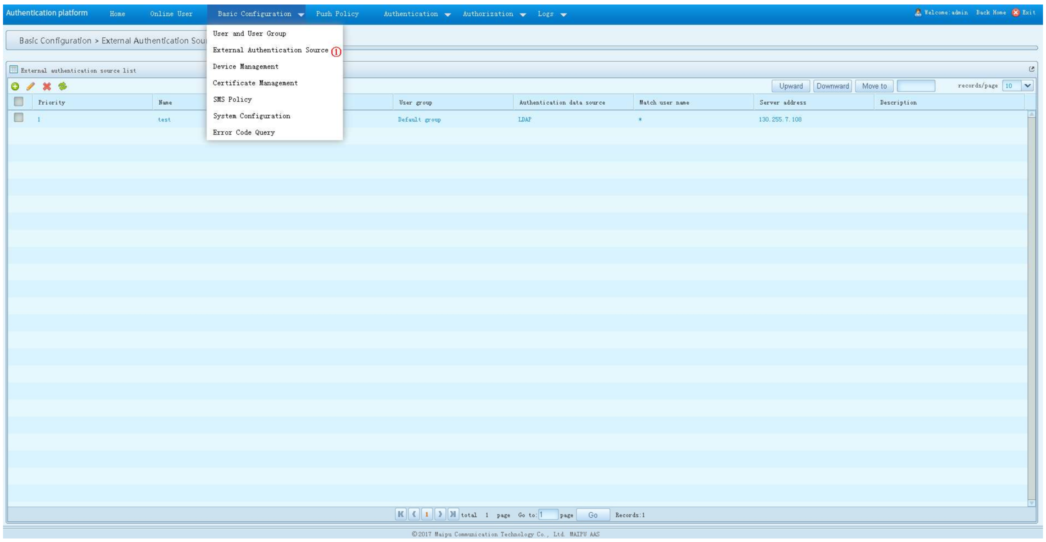
Figure 10-2-6 User group management

Caution

- When deleting one user group, the related policy and instance will become invalid.

10.2.2External Authentication Source

The user access system meets the demand of some customer that the internal staff does not need to create the account in the user access system separately, but directly uses the account on the existing AD server or LDAP server to authenticate. The external authentication in the scenario includes the AD authentication, LDAP authentication, and Radius authentication.



☐	Priority	Name	User group	Authentication data source	Match user name	Server address	Description
☐	1	test	Default group	LDAP	*	130.255.7.108	

Figure 10-2-7 External authentication source

AD authentication configuration

The user access system supports the external AD authentication. Configure the AD authentication, and you can directly use the account on the AD server for authentication. The process of configuring the AD authentication is as follows:

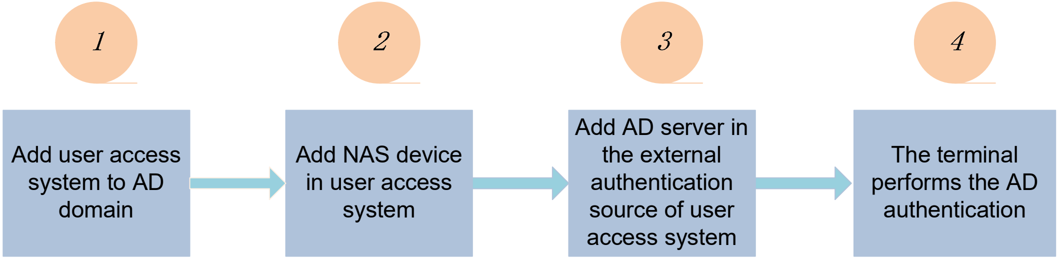
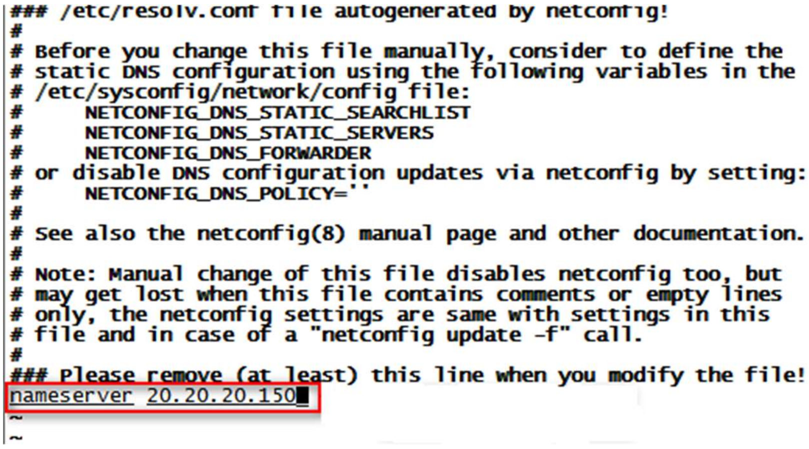

1
2
3
4
Add user access system to AD domain
Add NAS device in user access system
Add AD server in the external authentication source of user access system
The terminal performs the AD authentication

Figure 10-2-8 The process of configuring the AD authentication

Add the AD server address in the etc/resolv.conf of the user access system, as shown in the following figure:



```
### /etc/resolv.conf file autogenerated by netconfig!
#
# Before you change this file manually, consider to define the
# static DNS configuration using the following variables in the
# /etc/sysconfig/network/config file:
#     NETCONFIG_DNS_STATIC_SEARCHLIST
#     NETCONFIG_DNS_STATIC_SERVERS
#     NETCONFIG_DNS_FORWARDER
# or disable DNS configuration updates via netconfig by setting:
#     NETCONFIG_DNS_POLICY=''
#
# See also the netconfig(8) manual page and other documentation.
#
# Note: Manual change of this file disables netconfig too, but
# may get lost when this file contains comments or empty lines
# only, the netconfig settings are same with settings in this
# file and in case of a "netconfig update -f" call.
#
### Please remove (at least) this line when you modify the file!
nameserver 20.20.20.150
~
~
```

Figure 10-2-9 Add the AD server

Add the AD domain in the SUSE of the user access system, and select **User and Group Management**, as shown in Figure 11-7:

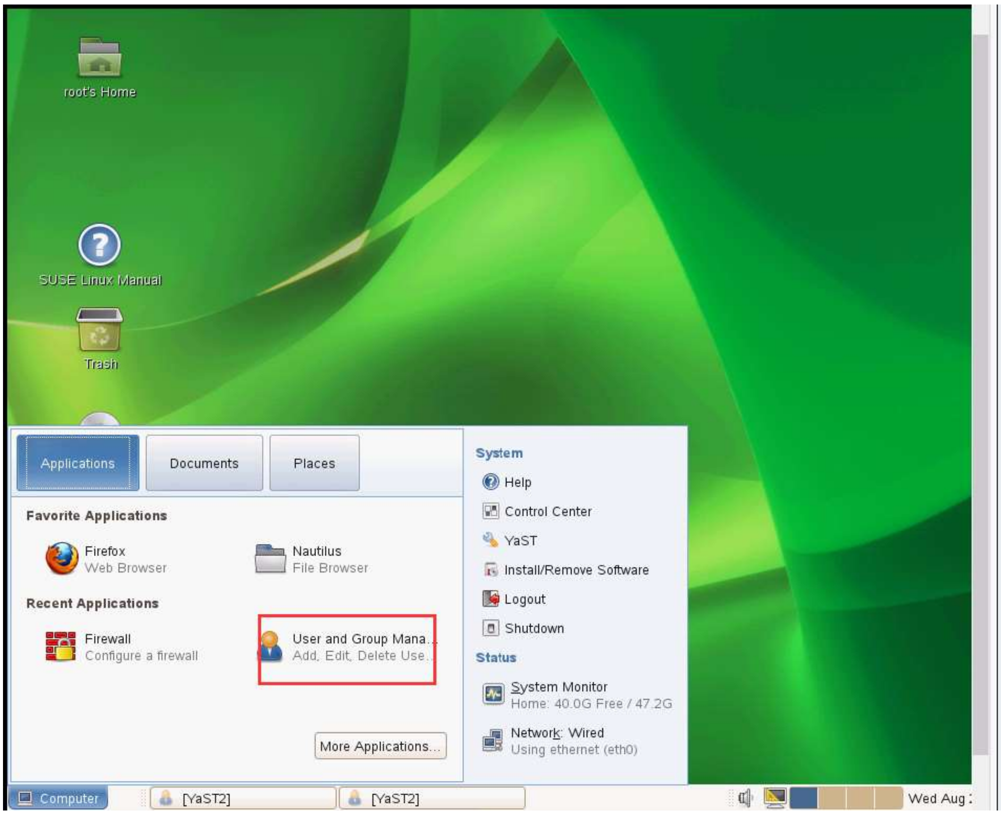
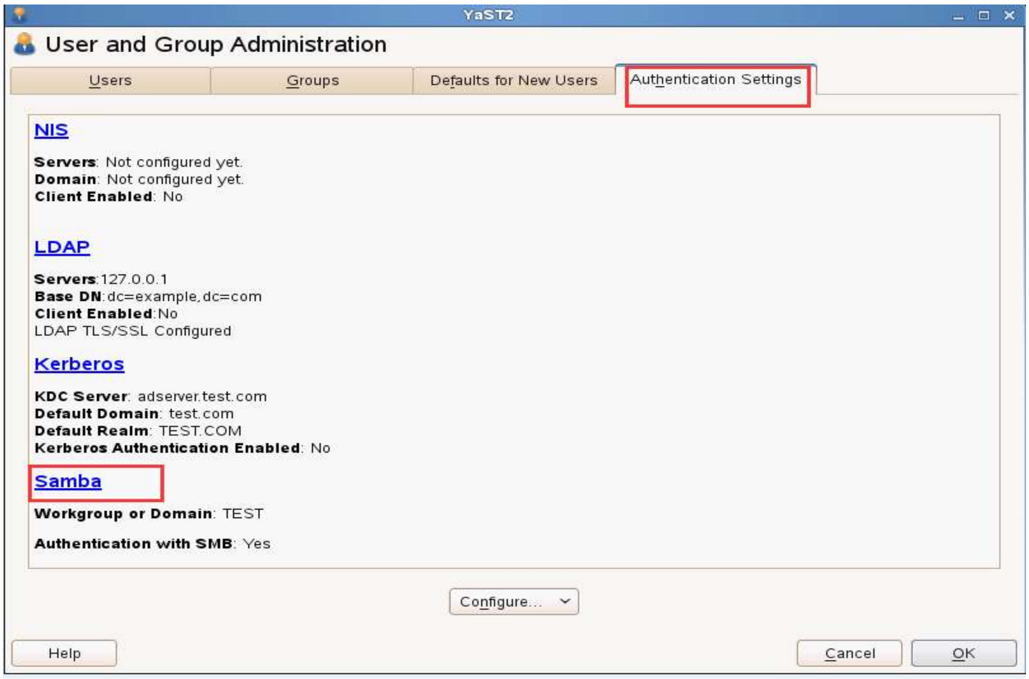


Figure 10-2-10 Add one AD domain

Select Authentication Setting->Samba



NIS

Servers: Not configured yet.
Domain: Not configured yet.
Client Enabled: No

LDAP

Servers:127.0.0.1
Base DN:dc=example,dc=com
Client Enabled:No
LDAP TLS/SSL Configured

Kerberos

KDC Server: adserver.test.com
Default Domain: test.com
Default Realm: TEST.COM
Kerberos Authentication Enabled: No

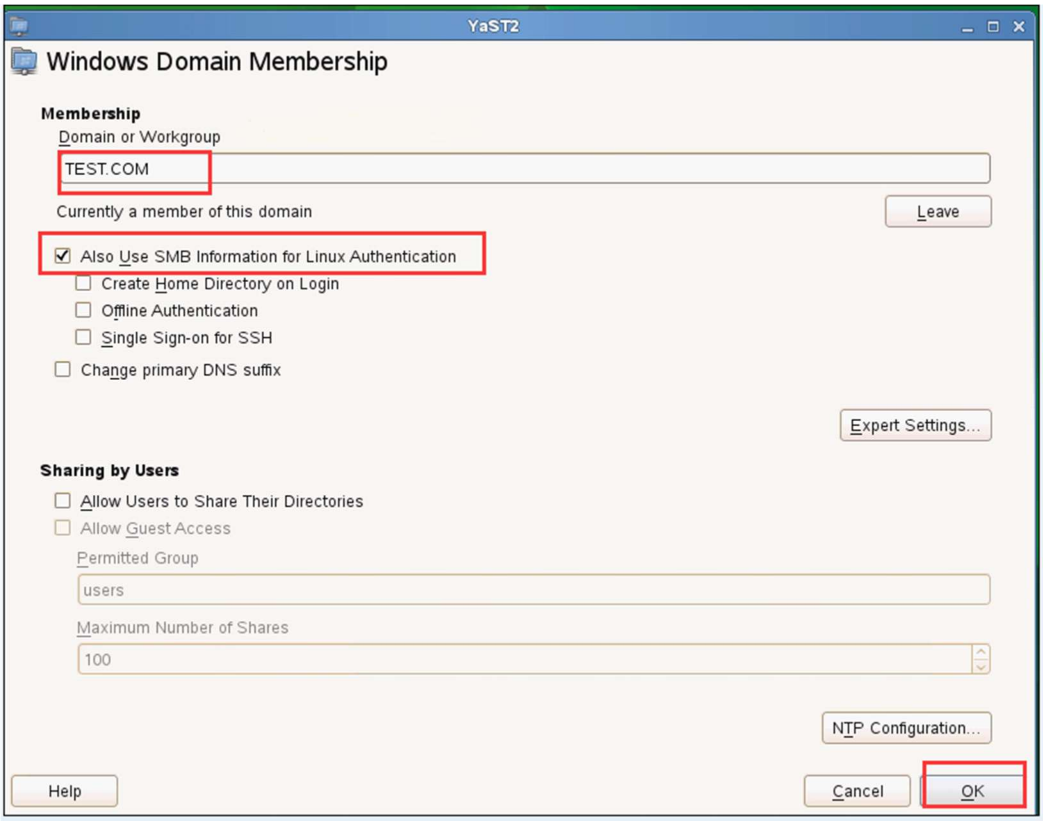
Samba

Workgroup or Domain: TEST

Authentication with SMB: Yes

Figure 10-2-11 AD selection option

In Windows Domain Membership, configure AD, and input the corresponding information, as shown in the following figure:



Membership

Domain or Workgroup: TEST.COM

Currently a member of this domain

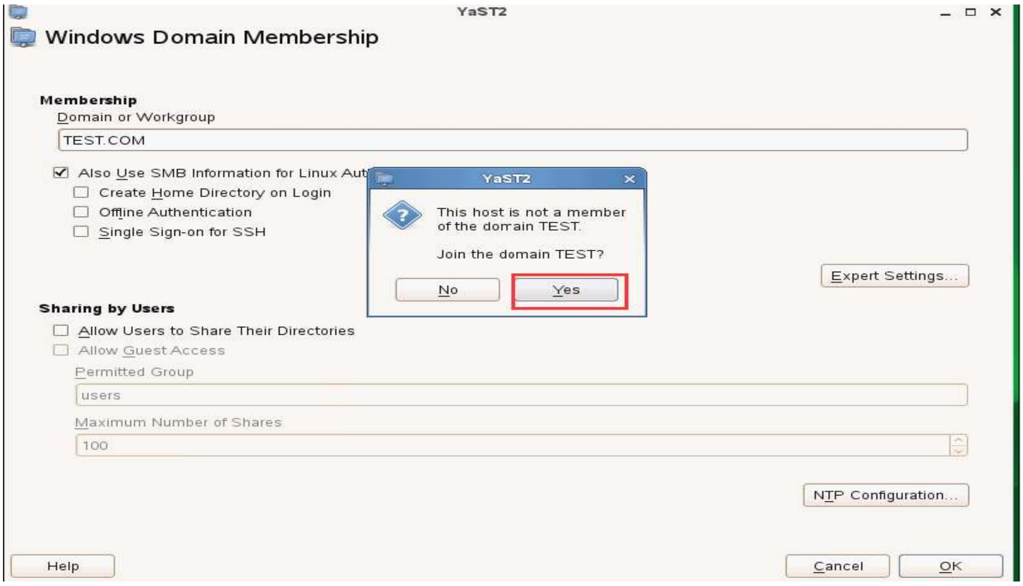
☑ Also Use SMB Information for Linux Authentication
☐ Create Home Directory on Login
☐ Offline Authentication
☐ Single Sign-on for SSH
☐ Change primary DNS suffix

Sharing by Users

☐ Allow Users to Share Their Directories
☐ Allow Guest Access
Permitted Group: users
Maximum Number of Shares: 100

Figure 10-2-12 Fill in the domain name of AD

Click **OK**.



Membership

Domain or Workgroup: TEST.COM

☑ Also Use SMB Information for Linux Aut

☐ Create Home Directory on Login

☐ Offline Authentication

☐ Single Sign-on for SSH

Sharing by Users

☐ Allow Users to Share Their Directories

☐ Allow Guest Access

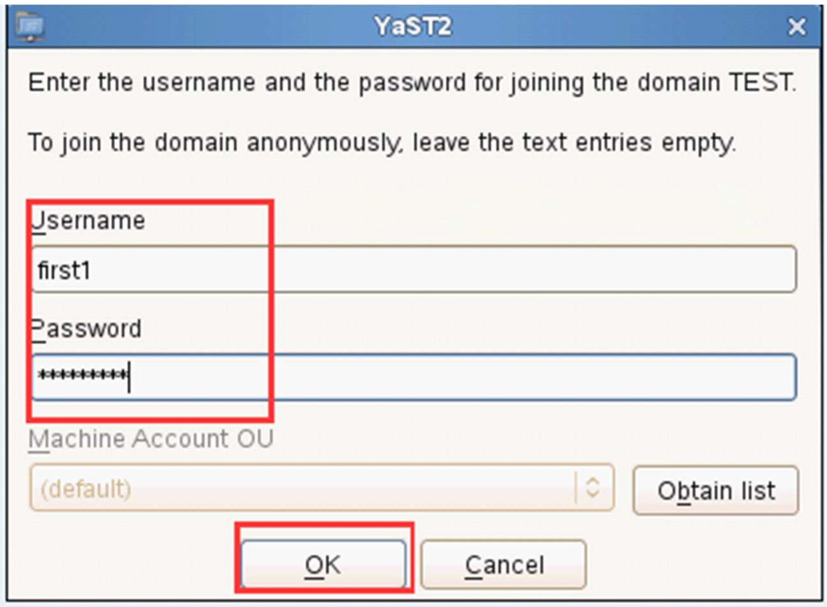
Permitted Group: users

Maximum Number of Shares: 100

This host is not a member of the domain TEST.

Join the domain TEST?

Figure 10-2-13 Finish configuring the domain name of AD



Enter the username and the password for joining the domain TEST.

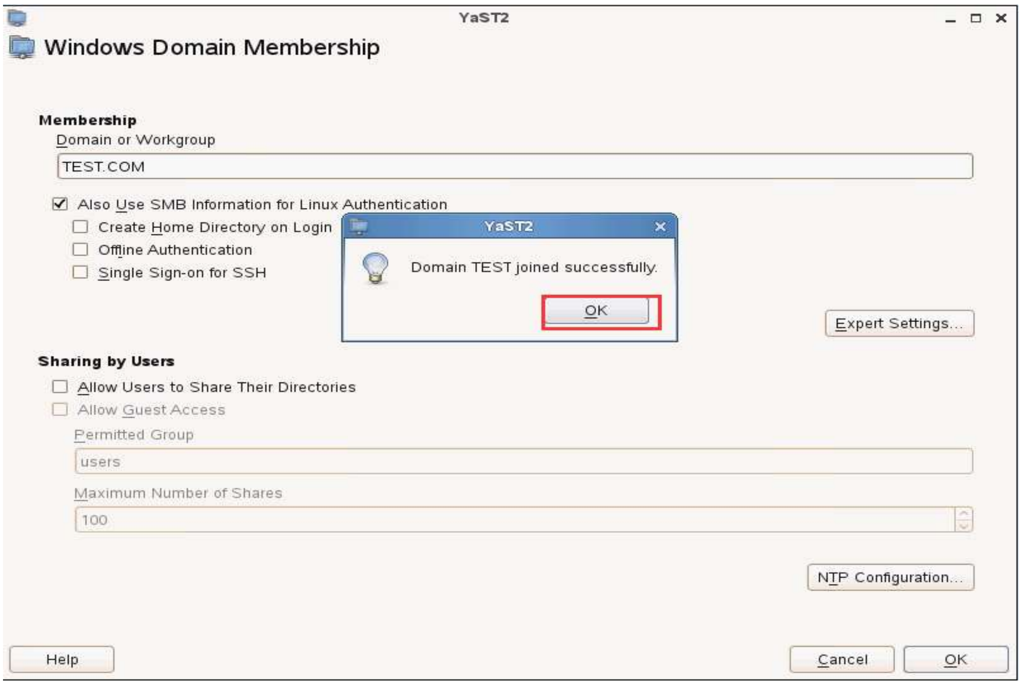
To join the domain anonymously, leave the text entries empty.

Username: first1

Password: *********

Machine Account OU: (default)

Figure 10-2-14 Input the account and password



YaST2

Windows Domain Membership

Membership

Domain or Workgroup: TEST.COM

☑ Also Use SMB Information for Linux Authentication

☐ Create Home Directory on Login

☐ Offline Authentication

☐ Single Sign-on for SSH

YaST2: Domain TEST joined successfully.

Sharing by Users

☐ Allow Users to Share Their Directories

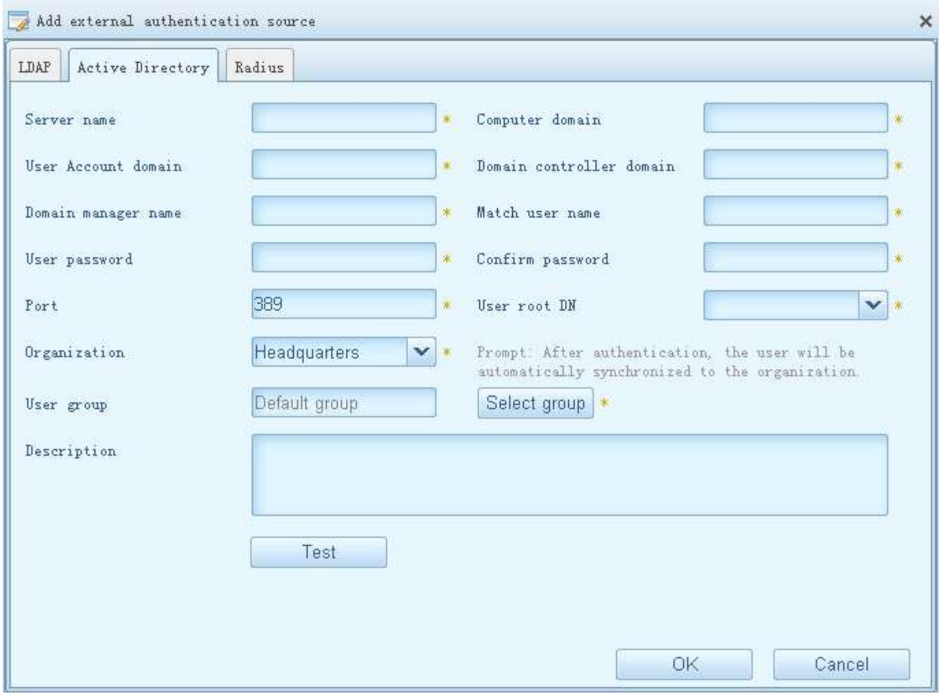
☐ Allow Guest Access

Permitted Group: users

Maximum Number of Shares: 100

Figure 10-2-15 Configuration succeeded

In the external authentication source, add the AD server.



Add external authentication source

LDAP | Active Directory | Radius

Server name *

Computer domain *

User Account domain *

Domain controller domain *

Domain manager name *

Match user name *

User password *

Confirm password *

Port: 389 *

User root DN *

Organization: Headquarters *

Prompt: After authentication, the user will be automatically synchronized to the organization.

User group: Default group

Select group *

Description

Figure 10-2-16 Add the external authentication source

The terminal performs the AD authentication. The supported AD authentication modes include PAP, PEAP-MSCHAPV2, PEAP-GTC, and TTLS-PAP.

Caution

- First build the AD domain server, create the AD account, and the AD account cannot be created in the root path of the AD domain.
- When configuring the AD authentication, you should add the AD server address in the etc/resolv.conf on the master server and node of the user access system.
- The master server and node of the user access system both need to be added to the AD domain.
- The supported AD authentication modes include PAP, PEAP-MSCHAPV2, PEAP-GTC, and TTLS-PAP.
- When synchronizing AD, you cannot synchronize the account in the root path of the AD domain.
- When authenticating and synchronizing AD, match according to the matched user name and set user root DN when adding the AD server in the user access system.
- When the AD and LDAP servers are connected and if the matched user names of the added AD server and LADAP server in the user access system have intersection, select the authentication on AD or LDAP according to the selected authentication mode plus the priority of the AD server and LDAP server in the external authentication source.

For example, the AD and LDAP servers are connected to one server. In the user access system, when the external authentication source adds the AD server and LDAP server, the filled match user names are all with * (all users). The priority of the LDAP server is 1 and the priority of the AD server is 2, so the user selects the AD authentication mode PEAP-MSCHAPV2 on the terminal. If the user is the share user of AD and LDAP, the authentication will fail, because adopt the LDAP authentication according to the authentication priority, while the LDAP authentication does not support PEAP-MSCHAPV2. Therefore, the access log will prompt that the user failed to perform the LDAP authentication. In this case, you can select PAP, PEAP-GTC, TTLS-PAP on the terminal to authenticate, or change the priority of the AD server to 1 without changing the terminal authentication mode PEAP-MSCHAPV2 so that the authentication can succeed.

- When the user access system communicates with the AD server, the used source IP address is the real address of the user access system, but not the configured virtual address of HA. If it is necessary to configure the firewall policy, you should pay special attention.

LDAP configuration

The user access system supports the external LDAP authentication. Configure the LDAP authentication, and you can directly use the account on the LDAP server for authentication. If the LDAP account has ever performed the LDAP authentication successfully, automatically synchronize the authenticated LDAP account to the user access system. Meanwhile, support synchronizing the LADP account manually. The synchronization does not need the LDAP authentication, but directly synchronize the matched LDAP account (the account matching the filled user name and user root DN when adding the LDAP server in the access system) on the LDAP server to the user access system.

The process of configuring the LDAP authentication is as follows:

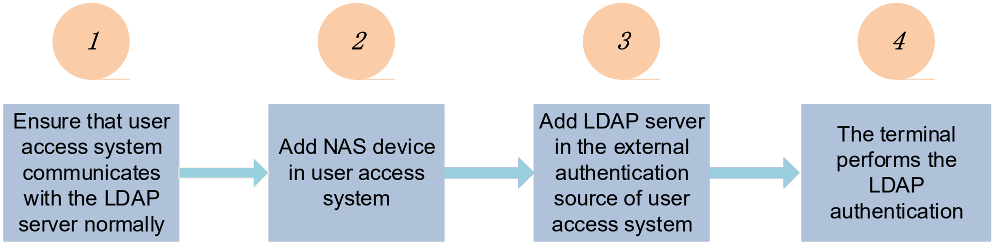
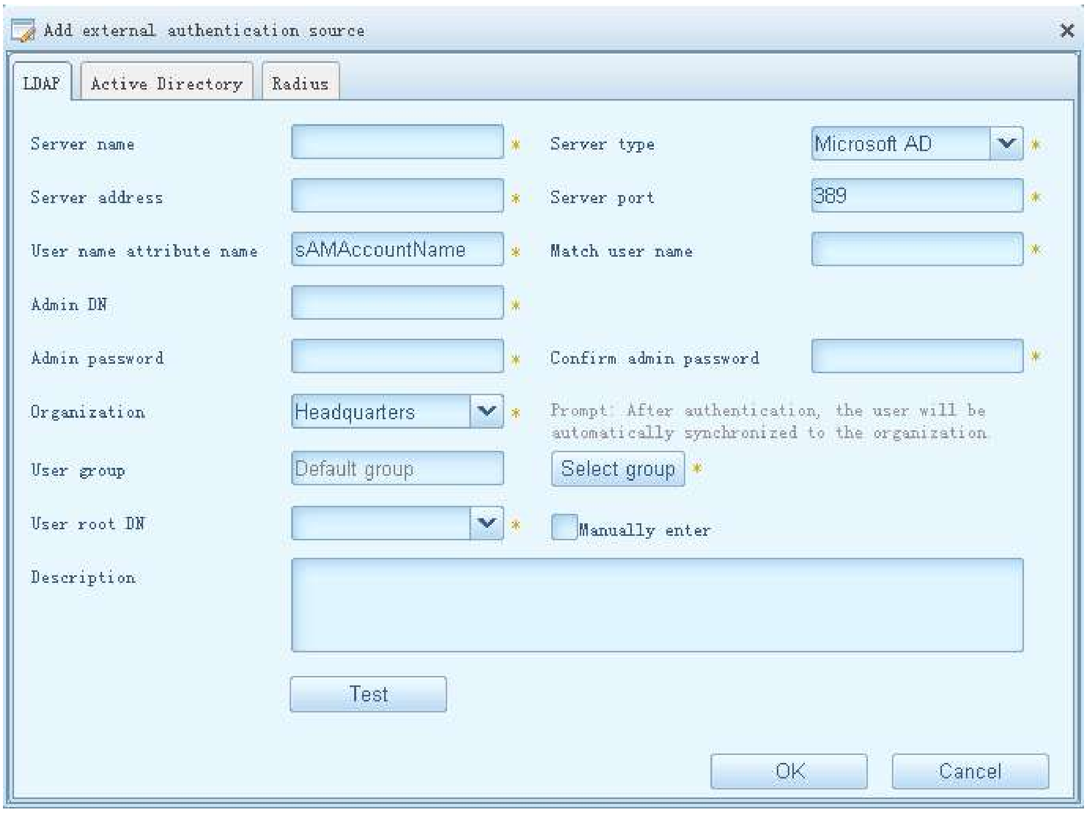

1
2
3
4
Ensure that user access system communicates with the LDAP server normally
Add NAS device in user access system
Add LDAP server in the external authentication source of user access system
The terminal performs the LDAP authentication

Figure 10-2-17 Configure LDAP

During the LDAP configuration, configuring the AD domain and adding the device are the same as the AD authentication configuration. Refer to the related configuration in the AD authentication.

Add the LDAP external authentication source, as follows:


Add external authentication source

LDAP | Active Directory | Radius

Server name: *
Server type: Microsoft AD *
Server address: *
Server port: 389 *
User name attribute name: sAMAccountName *
Match user name: *
Admin DN: *
Admin password: *
Confirm admin password: *
Organization: Headquarters *
Prompt: After authentication, the user will be automatically synchronized to the organization
User group: Default group
Select group *
User root DN: *
☐ Manually enter
Description:

Figure 10-2-18 Add the LDAP external authentication source

The terminal performs the LDAP authentication, and the supported AD authentication modes include PAP, PEAP-GTC, and TTLS-PAP.

The AD and LDAP authentication are both based on the AD domain and adopt different protocols. The setup of the AD domain can be single-node domain (single domain) and multi-node domain (

Both AD and LDAP authentication (forest domain), as follows:

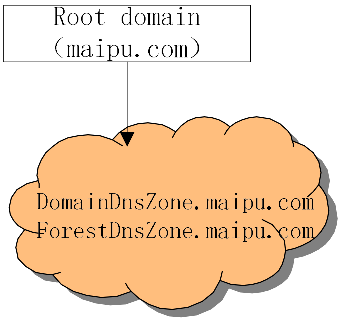


Figure 10-2-19 Single domain mode

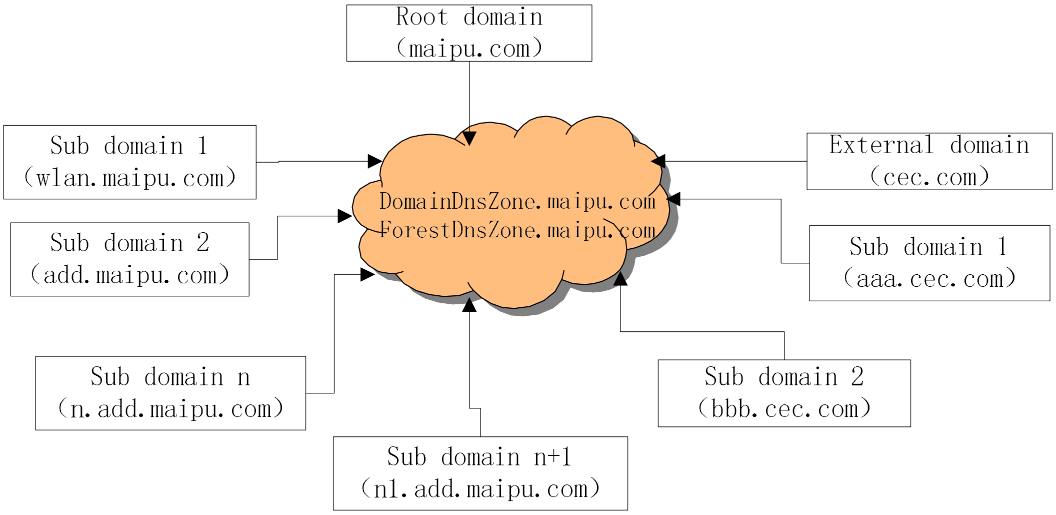


Figure 10-2-20 Forest domain mode

Single-domain mode

The mode contains one root domain node and DNS server, and the configuration of the DNS server is not mandatory. In the mode, usually configure the user root DN as one organization unit of the root domain, such as DC=aas,DC=maipu,DC=com. If configuring the root DN as the root domain, search for the sub domain and external domain in two DNS servers, that is, DomainDnsZone.maipu.com and ForestDnsZone.maipu.com, so it is necessary to ensure that the two DNS servers (DomainDnsZone.maipu.com and ForestDnsZone.maipu.com) can resolve correctly. Otherwise, there will be timeout error during authentication.

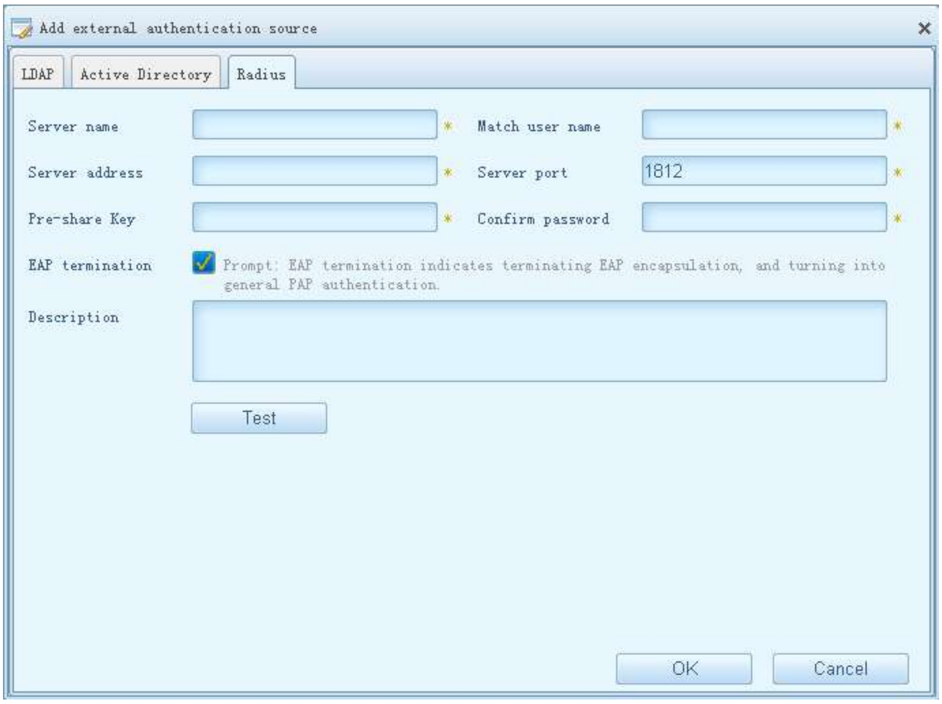
Forest domain mode

The mode contains one root domain node, multiple sub domains, or external domain nodes and DNS server, and the DNS server needs to be configured. You can correctly resolve all domain servers in the forest. In the mode, usually configure the user root DN as the root domain, such as DC=maipu,DC=com. During authentication, search for the account in the whole forest domain to authenticate. The mode is applicable to the scenario that the enterprise headquarters and the branches set up their own domain servers separately.

Radius configuration

Radius authentication mainly encapsulates the user information and sends to the third-party system for authentication, and then, returns the authentication result.

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved



Server port: 1812

EAP termination: ☑ Prompt: EAP termination indicates terminating EAP encapsulation, and turning into general PAP authentication.

Figure 10-2-21 Radius configuration

Caution

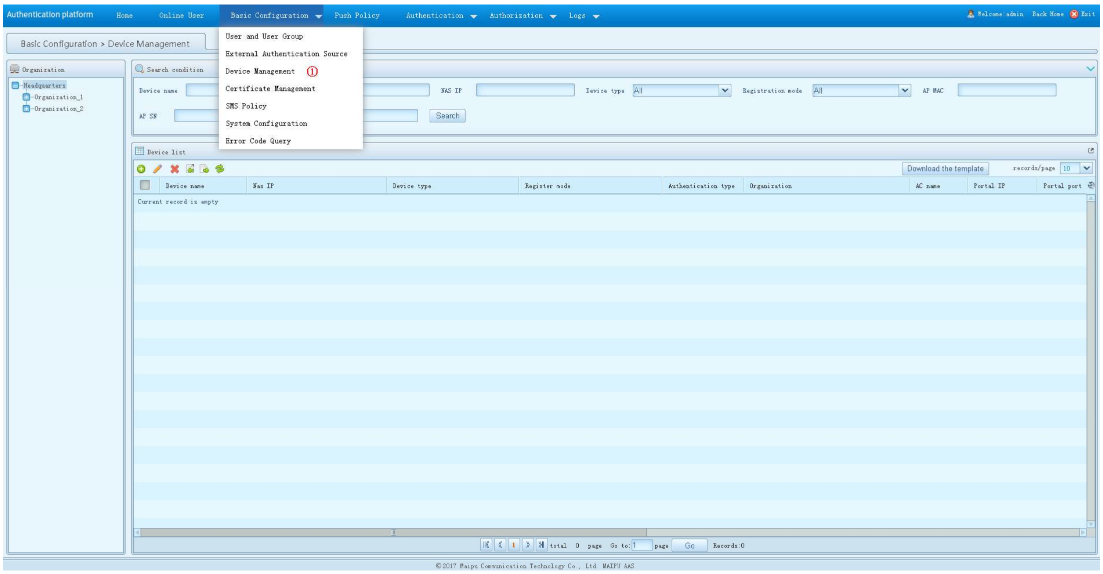
- First build the LDAP domain server, create the LDAP account, and the LDAP account cannot be created in the root path of the LDAP domain.
- When configuring the LDAP authentication, you should add the LDAP server address in the etc/resolv.conf on the master server and node of the user access system.
- The supported LDAP authentication modes include PAP, PEAP-GTC, and TTLS-PAP.
- When synchronizing LDAP, you cannot synchronize the account in the root path of the LDAP domain.
- When authenticating and synchronizing LDAP, match according to the matched user name and set user root DN when adding the LDAP server in the user access system.
- When the AD and LDAP servers are connected and if the matched user names of the added AD server and LADAP server in the user access system have intersection, select the authentication on AD or LDAP according to the selected authentication mode plus the priority of the AD server and LDAP server in the external authentication source.

For example, the AD and LDAP servers are connected to one server. In the user access system, when the external authentication source adds the AD server and LDAP server, the filled match user names are all with * (all users). The priority of the LDAP server is 1 and the priority of the AD server is 2, so the user selects the AD authentication mode PEAP-MSCHAPV2 on the terminal. If the user is the share user of AD and LDAP, the authentication will fail, because adopt the LDAP authentication according to the authentication priority, while the LDAP authentication does not support PEAP-MSCHAPV2. Therefore, the access log will prompt that the user failed to perform the LDAP authentication. In this case, you can select PAP, PEAP-GTC, TTLS-PAP on the terminal to authenticate, or change the priority of the AD server to 1 without changing the terminal authentication mode PEAP-MSCHAPV2 so that the authentication can succeed.

- When the user access system communicates with the LDAP server, the used source IP address is the real address of the user access system, but not the configured virtual address of HA. If it is necessary to configure the firewall policy, you should pay special attention.

10.2.3Device Management

Click **Basic Configuration** > **Device Management** to enter the device management interface. The module mainly provides the functions of adding, modifying, querying, deleting, importing and exporting the device and downloading the device template, as shown in the following figure:



Current record is empty

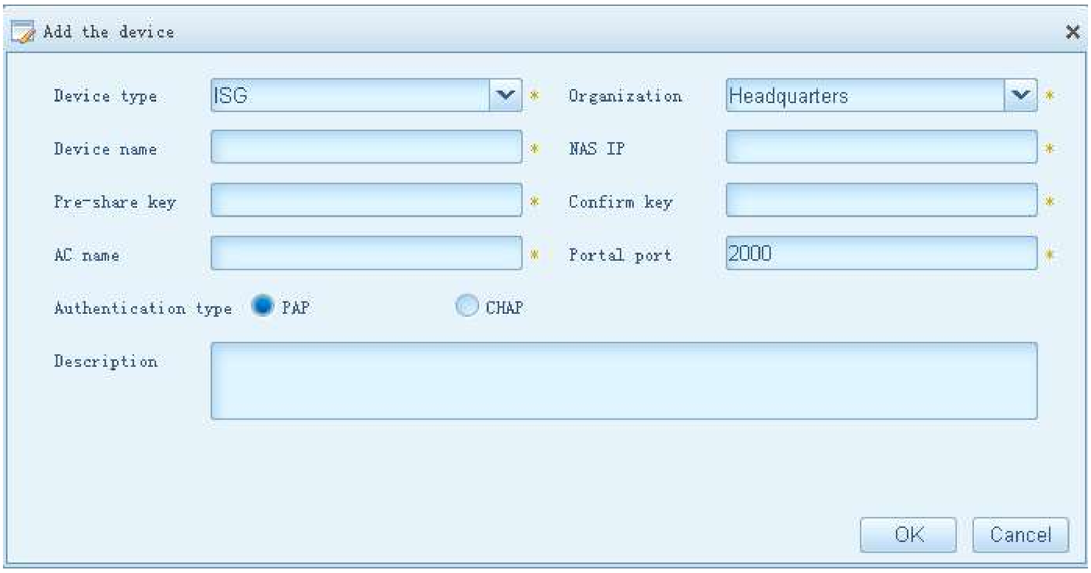
Figure 10-2-22 Device management

There are totally five devices types, that is, ISG, AC, LNS, RADIUS-IETF and virtual device group. The device information is very useful when the user terminal pushes the site. The device is bound with the organization. Query the corresponding organization according to the device information, so as to judge to which site the device information is pushed.

Creating the device is mainly used to calculate the affiliated organization, so as to judge the pushed site. The matching process of the organization is as follows:

1. Input the parameters, including AcName (*), APMAC, APSN, SSID, UserIp(*), UserMac(*) and other key parameters. Query the organization base according to the AcName as the organization code, and search for the organization. If found, return the organization. Otherwise, enter the next step.
2. Query the organization base according to the SSID as the organization code, and search for the organization. If found, return the organization. Otherwise, enter the next step.
3. Query the device base according to APMAC+AcName or APSN+AcName. If finding the corresponding device, get the organization according to the device, If found, return the organization. Otherwise, enter the next step.
4. Query the device base according to AcName+SSID. If finding the device, query the organization according to the organization of the device. If not existing, enter the next step.
5. Query the device base according to the user IP address + AcName. If finding the device, query the organization according to the organization of the device. If not existing, enter the next step.
6. Query the device base according to AcName. If the device exists, query the organization according to the organization of the device. If not existing, enter the next step.
7. Query the device base according to NasIP. If the device exists, query the organization according to the organization of the device. If not existing, enter the next step.
8. Return the root organization.

Add/modify one device



Device type: ISG

Organization: Headquarters

Portal port: 2000

Authentication type: ● PAP ○ CHAP

Figure 10-2-23 Add a device

As described in step 3 of the organization matching rules, to match the organization according to APMAC+AcName or APSN+AcName, you need to add the virtual group device. The adding and matching rules of the virtual group device are as follows:

1. Group by ap

Add the device information for the authentication platform:

Virtual device information 1: apmac: 00-1F-C6-41-D8-CD; apsn: test1; Organization: Institution1

Virtual device information 2: apmac: 00-1F-C6-41-D8-CE; apsn: test2; Organization: Institution2

Configure the push site for the marketing platform:

Site 1: Push range: Institution 1

Site 2: Push range: Institution 2

The user connects wifi to the authentication platform for authentication. Query the organization of the device according to the device information carried by the user (apmac, apsn). If matching institution 1, push site 1.

2. Group by ssid/sub interface

Add the device information for the authentication platform:

Virtual device information 1: ssid: ssid1, acname: test1; Organization: Institution1

Virtual device information 2: ssid: ssid1, acname: test2; Organization: Institution2

Configure the push site for the marketing platform:

Site 1: Push range: Institution 1

Site 2: Push range: Institution 2

The user connects wifi to the authentication platform for authentication. Query the organization of the device according to the device information carried by the user (apmac, apsn). If matching institution 1, push site 1.

3. Group by IP

Add the device information for the authentication platform:

Virtual device information 1: start ip: 1.1.1.1, end ip: 1.1.1.10, acname: test1; Organization: Institution1

Virtual device information 2: start ip: 1.1.2.1, end ip: 1.1.2.10, acname: test1; Organization: Institution2

Configure the push site for the marketing platform:

Site 1: Push range: Institution 1

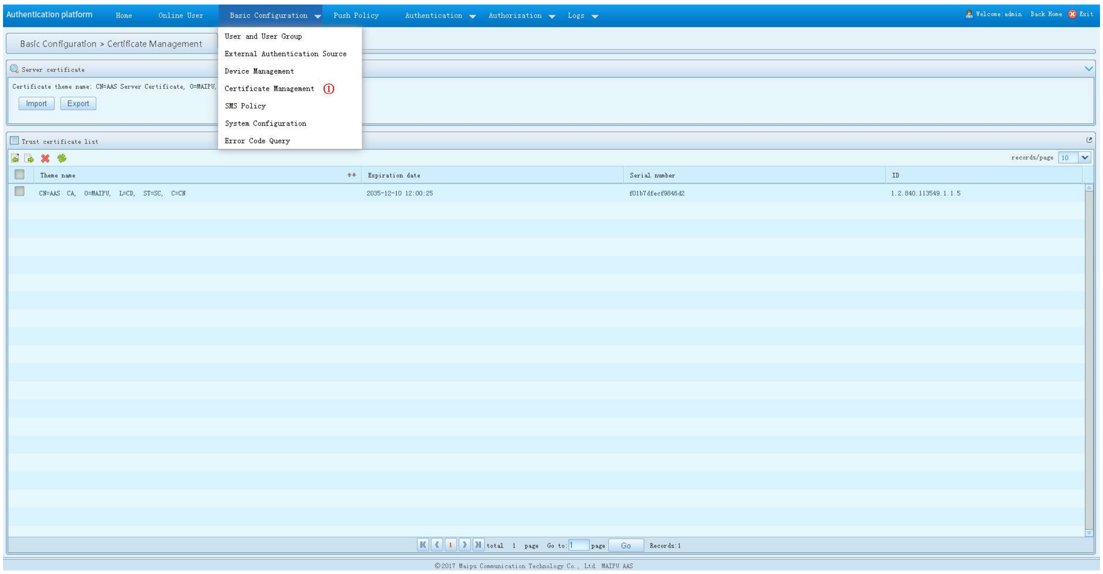
Site 2: Push range: Institution 2

The user connects wifi to the authentication platform for authentication. Query the organization of the device according to the device information carried by the user (ip, acname). If matching institution 1, push site 1.

Caution

- The pre-share key of the device should be consistent with the configured key of the device.

10.2.4Certificate Management



Certificate theme name: CN=AAS Server Certificate, O=MAIPU,

☐	Theme name	Expiration date	Serial number	ID
☐	CN=AAS CA, O=MAIPU, L=CD, ST=SC, C=CN	2035-12-10 12:00:25	f01b7dfecf9846d2	1.2.840.113549.1.1.5

total 1 page Go to: 1 page Records:1

©2017 Maipu Communication Technology Co., Ltd. MAIPU AAS

Figure 10-2-24 Certificate management

To complete the certificate authentication configuration, prepare at least three certificates, as shown in the following figure:

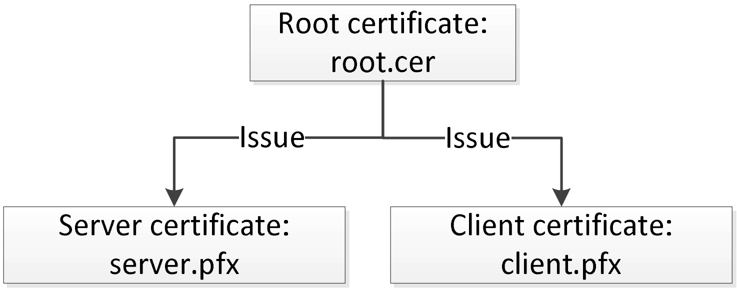
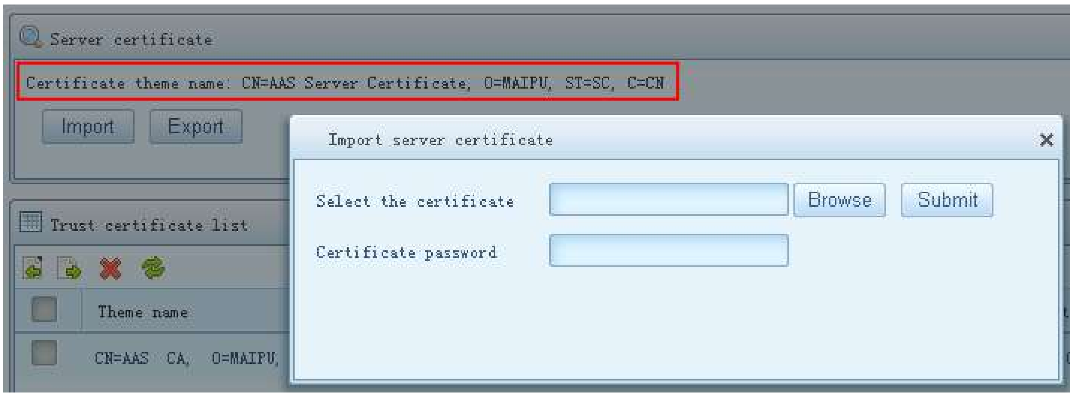


Figure 10-2-25 Certificate relation

The three certificates are root certificate (root.cer), server certificate (server.pfx), and client certificate (client.pfx). The server certificate and client certificate are issued by the root certificate.

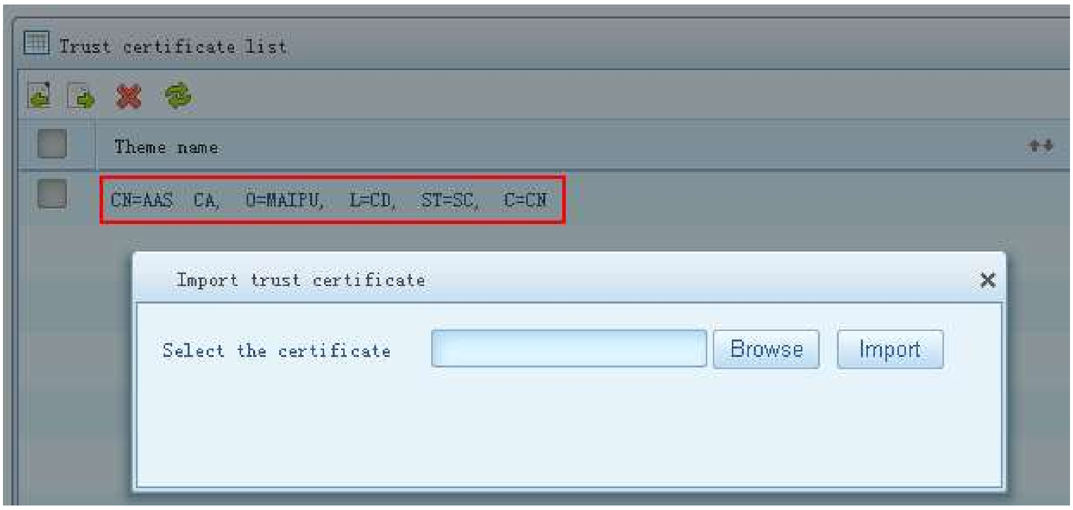
1. Import the server certificate to the server certificate management interface, as follows:



Certificate theme name: CN=AAS Server Certificate, O=MAIPU, ST=SC, C=CN

CN=AAS CA, O=MAIPU,

2. Import the root certificate to the trust certificate list, as follows:



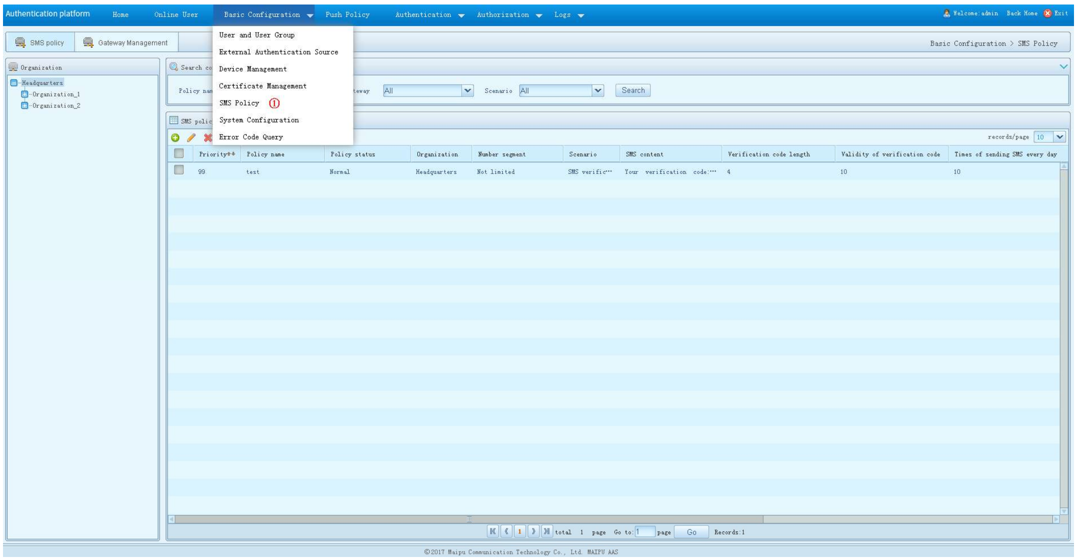
CN=AAS CA, O=MAIPU, L=CD, ST=SC, C=CN

3. Download the client certificate and import to the user authentication terminal.

After the above configuration, you can perform the certificate authentication (EAP-TTLS).

10.2.5SMS Policy

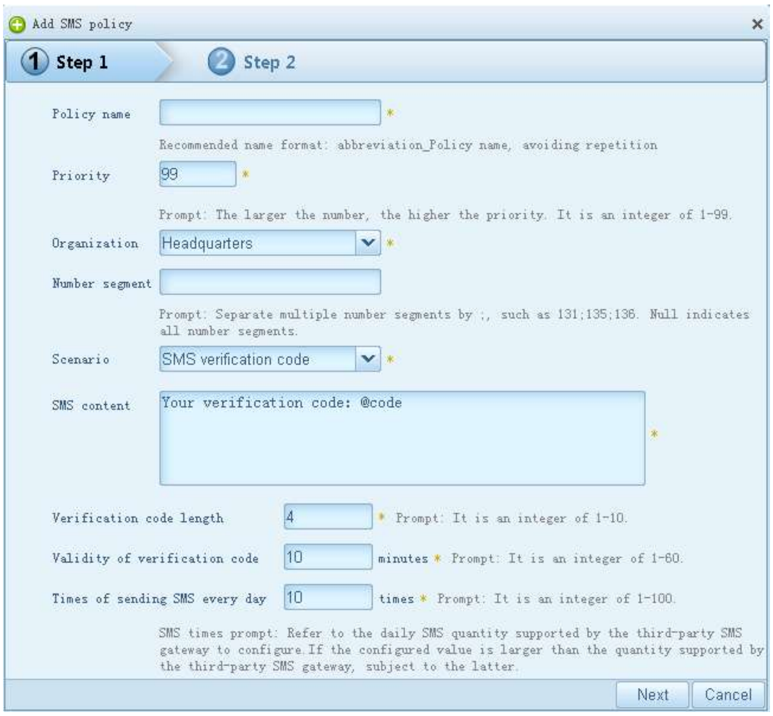
SMS policy includes two modules, that is, “SMS Policy” and “Gateway Management”. “SMS Policy” provides the functions of adding, deleting, modifying, and querying the SMS policy. “Gateway Management” mainly provides the display query for the gateways synchronized from “Marketing Platform”, as shown in the following figure:



Priority	Policy name	Policy status	Organization	Number segment	Scenario	SMS content	Verification code length	Validity of verification code	Times of sending SMS every day
99	test	Normal	Headquarters	Not limited	SMS verific···	Your verification code:···	4	10	10

Figure 10-2-26 SMS policy

Add/modify the SMS policy:



Policy name: *

Recommended name format: abbreviation_Policy name, avoiding repetition

Priority: 99 *

Prompt: The larger the number, the higher the priority. It is an integer of 1-99.

Organization: Headquarters *

Number segment:

Prompt: Separate multiple number segments by ;, such as 131;135;136. Null indicates all number segments.

Scenario: SMS verification code *

SMS content: Your verification code: @code *

Verification code length: 4 * Prompt: It is an integer of 1-10.

Validity of verification code: 10 minutes * Prompt: It is an integer of 1-60.

Times of sending SMS every day: 10 times * Prompt: It is an integer of 1-100.

SMS times prompt: Refer to the daily SMS quantity supported by the third-party SMS gateway to configure.If the configured value is larger than the quantity supported by the third-party SMS gateway, subject to the latter.

Figure 10-2-27 Add the SMS policy

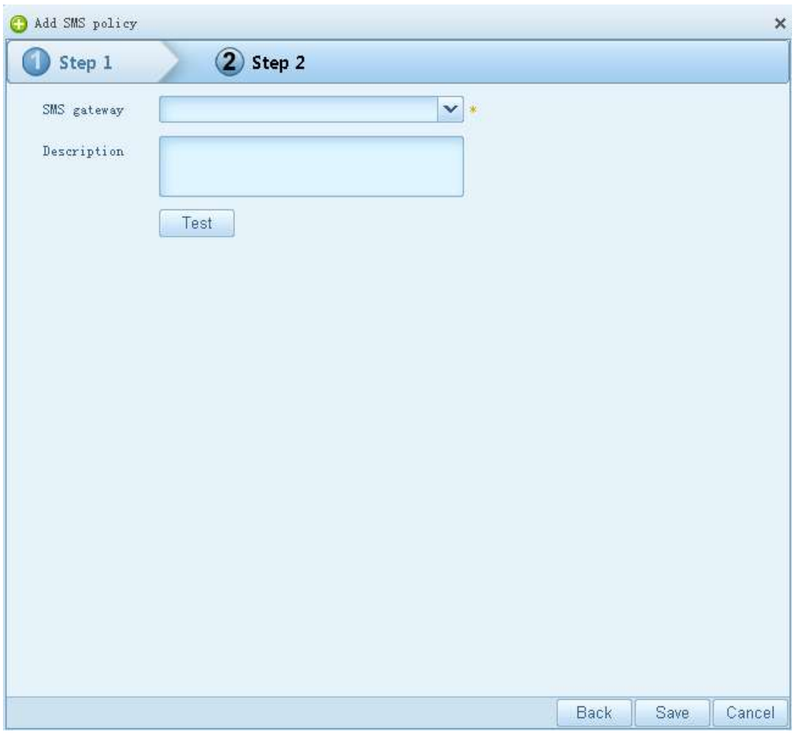
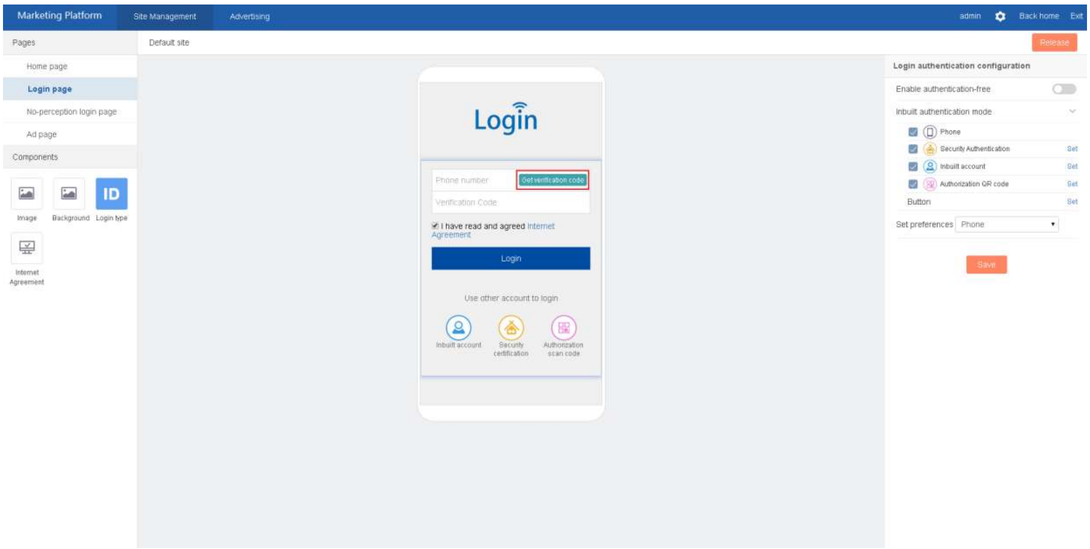


Figure 10-2-28 Add the SMS policy

Instance:

1. Authentication by mobile phone

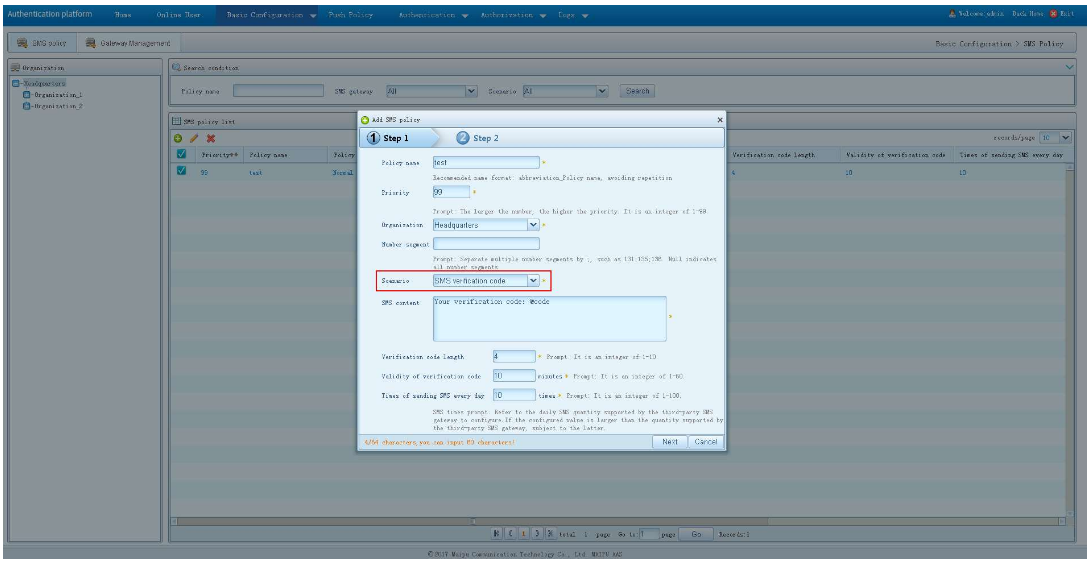
1) When selecting “Marketing Platform” as “Phone”, the part in the red box needs to configure “Scenario” as “SMS verification code” in the SMS policy of the authentication platform, as shown in the following figure:



Set preferences Phone

2) And then, you need to configure one SMS policy in “Authentication Platform”, as

shown in the following figure:



Add SMS policy

Step 1 Step 2

Policy name: test *

Recommended name format: abbreviation_Policy name, avoiding repetition

Priority: 99 *

Prompt: The larger the number, the higher the priority. It is an integer of 1-99.

Organization: Headquarters *

Number segment:

Prompt: Separate multiple number segments by ;, such as 131;135;136. Null indicates all number segments.

Scenario: SMS verification code *

SMS content: Your verification code: @code *

Verification code length: 4 * Prompt: It is an integer of 1-10.

Validity of verification code: 10 minutes * Prompt: It is an integer of 1-60.

Times of sending SMS every day: 10 times * Prompt: It is an integer of 1-100.

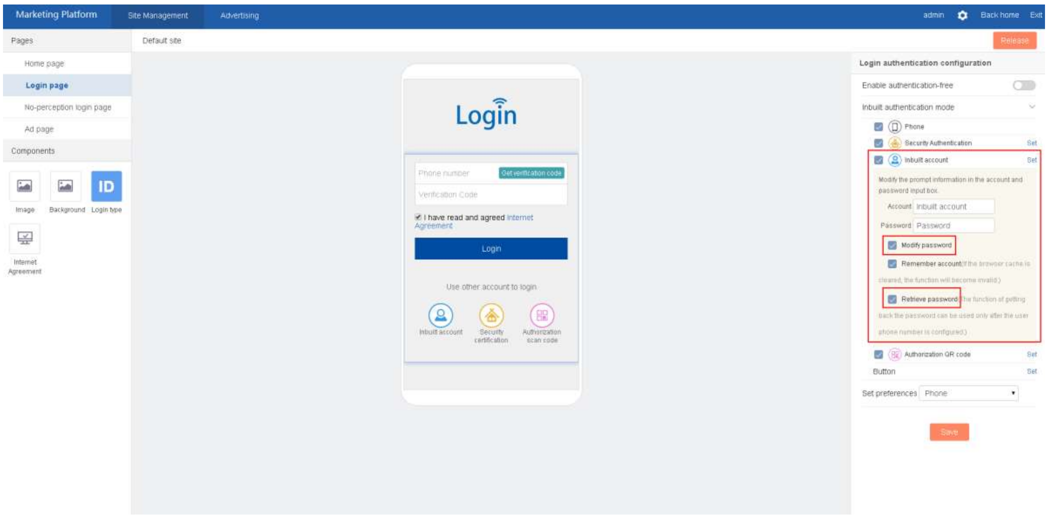
SMS times prompt: Refer to the daily SMS quantity supported by the third-party SMS gateway to configure.If the configured value is larger than the quantity supported by the third-party SMS gateway, subject to the latter.

4/64 characters,you can input 60 characters!

3) When the visitor authenticates after connecting wifi, receive the verification code via the SMS. After inputting the verification code correctly, the visitor can log in and access Internet successfully.

2. Modify the password

1) When selecting the login mode as “Inbuilt account” in “Marketing Platform”, and if the function “Modify password” is configured, as shown in the following figure:



Login authentication configuration

Enable authentication-free

Inbuilt authentication mode

☑ Phone

☑ Security Authentication

☑ Inbuilt account

Modify the prompt information in the account and password input box.

Account: Inbuilt account

Password: Password

☑ Modify password

☑ Remember account(If the browser cache is cleared, the function will become invalid.)

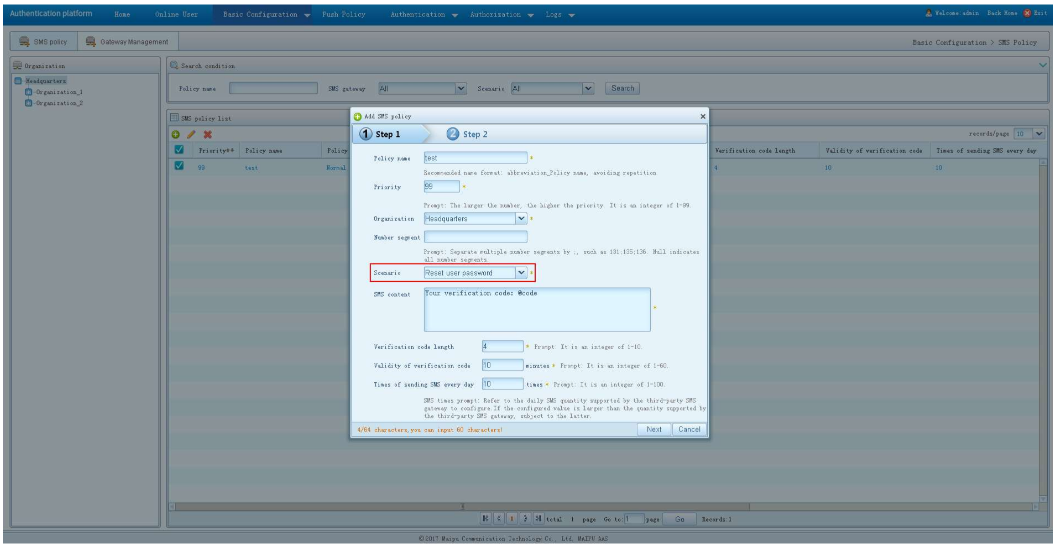
☑ Retrieve password(The function of getting back the password can be used only after the user phone number is configured.)

☑ Authorization QR code

Button

Set preferences: Phone

2) And then, you need to configure one SMS policy in “Authentication Platform”, as shown in the following figure:



Policy name: test

Recommended name format: abbreviation_Policy name, avoiding repetition

Priority: 99

Prompt: The larger the number, the higher the priority. It is an integer of 1-99.

Organization: Headquarters

Number segment:

Prompt: Separate multiple number segments by ;, such as 131;135;136. Null indicates all number segments.

Scenario: Reset user password

SMS content: Your verification code: @code

Verification code length: 4 * Prompt: It is an integer of 1-10.

Validity of verification code: 10 minutes * Prompt: It is an integer of 1-60.

Times of sending SMS every day: 10 times * Prompt: It is an integer of 1-100.

SMS times prompt: Refer to the daily SMS quantity supported by the third-party SMS gateway to configure.If the configured value is larger than the quantity supported by the third-party SMS gateway, subject to the latter.

4/64 characters,you can input 60 characters!

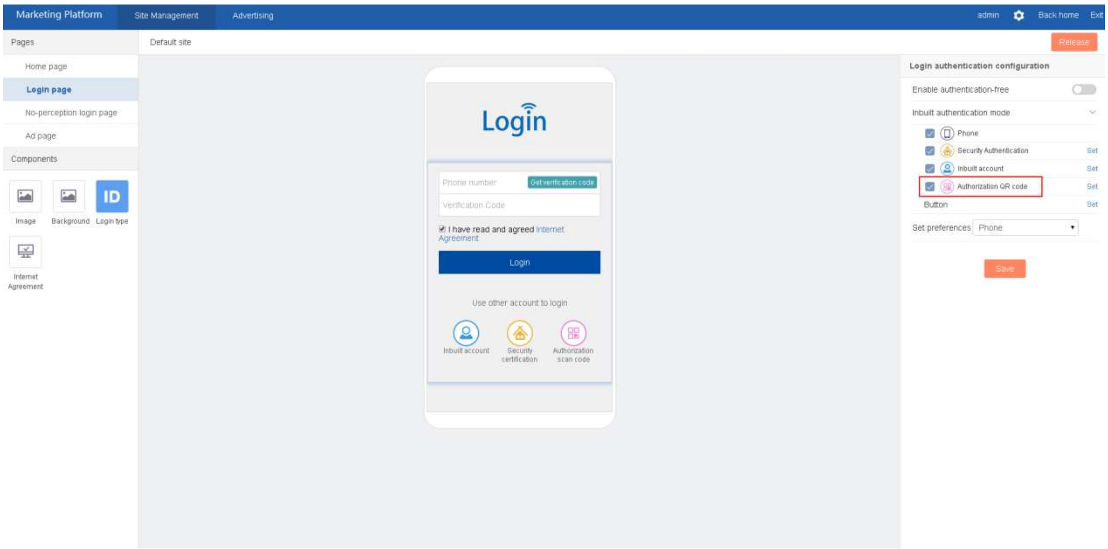
3) To modify the password when the visitor authenticates after connecting wifi, receive the verification code via SMS. After inputting the verification code correctly, the password can be modified.

3. Visitor arrival notification

Refer to the instance of section 11.5.2.3.

4. Authorization scan code for authentication

1) First enable the “Authorization QR code” authentication mode in “Marketing Platform”.



Login authentication configuration

Enable authentication-free

Inbuilt authentication mode

☑ Phone

☑ Security Authentication Set

☑ Inbuilt account Set

☑ Authorization QR code Set

Button Set

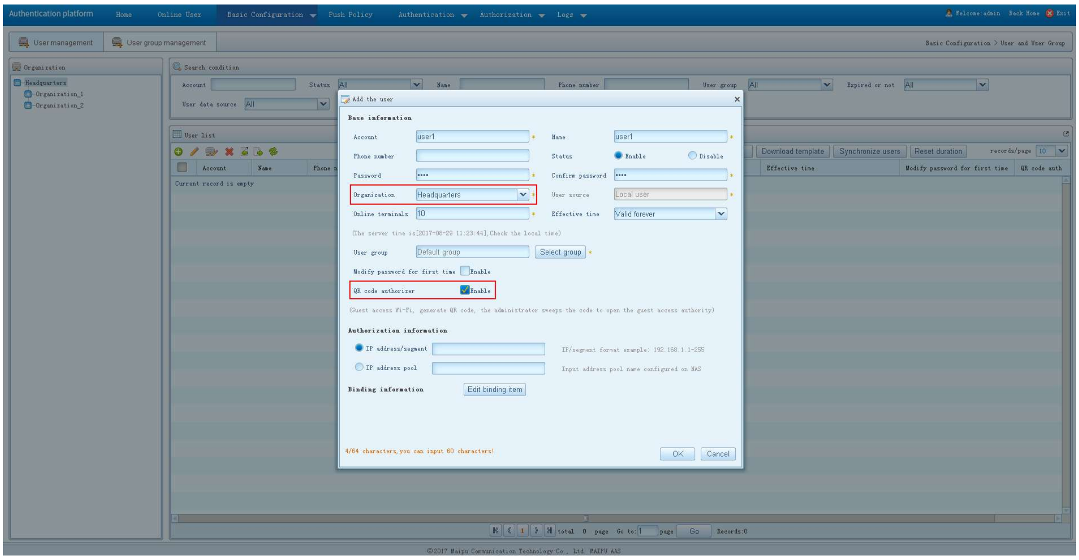
Set preferences: Phone

2) After the visitor connects wifi, select “Authorization QR code” to log in, Input the basic information, and then, generate the QR code.

3) Add one user in “User management” of “Authentication Platform”, and enable

All Rights Reserved

"QR code authorizer". Note that the organization needs to correspond to the organization of the current site.



Add the user

Base information

Account: user1 *
Name: user1 *
Phone number:
Status: ● Enable ○ Disable
Password: •••• *
Confirm password: •••• *
Organization: Headquarters *
User source: Local user *
Online terminals: 10 *
Effective time: Valid forever

(The server time is[2017-08-29 11:23:44],Check the local time)

User group: Default group *
Modify password for first time ☐ Enable
QR code authorizer ☑ Enable

(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)

Authorization information

● IP address/segment — IP/segment format example: 192.168.1.1-255
○ IP address pool — Input address pool name configured on NAS

Binding information

4/64 characters,you can input 60 characters!

4) After the authorizer of the user scans the QR code, it has the authority of deciding whether to permit the user to access Internet.

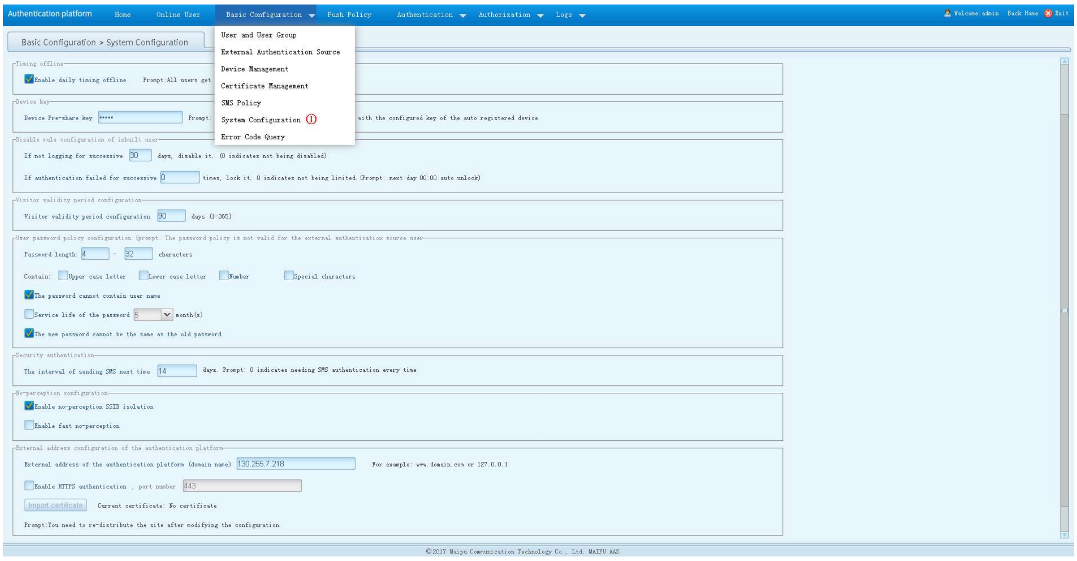
5) If permitted, the user accesses Internet successfully.

Caution

- "Using scenarios" in the SMS policy correspond to different services, and different services need to add the policies of different "Using scenarios".

10.2.6System Configuration

The module mainly provides the configurations of the timing offline, no-perception configuration and enabling portal push authentication using https protocol, as shown in the following figure:



Timing offline

☑ Enable daily timing offline Prompt:All users get

Device key

Device Pre-share key ••••• Prompt: with the configured key of the auto registered device

Disable rule configuration of inbuilt user

If not logging for successive 30 days, disable it. (0 indicates not being disabled)

If authentication failed for successive 0 times, lock it. 0 indicates not being limited. (Prompt: next day 00:00 auto unlock)

Visitor validity period configuration

Visitor validity period configuration 90 days (1-365)

User password policy configuration (prompt: The password policy is not valid for the external authentication source user

Password length: 4 - 32 characters

Contain: ☐ Upper case letter ☐ Lower case letter ☐ Number ☐ Special characters

☑ The password cannot contain user name

☐ Service life of the password 5 month(s)

☑ The new password cannot be the same as the old password

Security authentication

The interval of sending SMS next time 14 days. Prompt: 0 indicates needing SMS authentication every time

No-perception configuration

☑ Enable no-perception SSID isolation

☐ Enable fast no-perception

External address configuration of the authentication platform

External address of the authentication platform (domain name) 130.255.7.218 For example: www.domain.com or 127.0.0.1

☐ Enable HTTPS authentication , port number 443

Current certificate: No certificate

Prompt:You need to re-distribute the site after modifying the configuration.

Figure 10-2-29 System configuration

Https configuration

Enable the https function: Import the https certificate issued by the trusted organization to the system. Meanwhile, click “Enable HTTPS authentication” and specify the port. Currently, only support the “.p12” certificate.

Disable the https function: After clicking “Enable HTTPS authentication”, the click button of the check box is cancelled, that is, disable the https function. After enabling or disabling, the site needs to issue again.

No-perception configuration

No-perception login: If the user does not actively click the offline button or is not ticked offline by the administrator on the authentication platform, the user can access Internet without re-logging in after connecting ssid, that is, the current authentication mode of the user is no-perception login.

1. No-perception SSID isolation

    1) Not enable no-perception SSID isolation function

The user adopts the account test1 to access Internet via the device with ssid name ssid1, and then, the user can access Internet with no-perception login, but does not need to log in again. Meanwhile, the user also can perform the no-perception login and access Internet on the device with the ssid name ssid2, but does not need to log in again.

    2) Enable no-perception SSID isolation function

The user adopts the account test1 to access Internet via the device with the ssid ssid1, and then, the user can access Internet with no-perception login, but does not need to log in again. However, the user cannot perform the no-perception login and access Internet on the device with ssid name ssid2, but needs to log in again. After the user adopts the account test2 to log in on ssid2, the user can perform the no-perception login and access Internet on ssid2. Here, the user can perform the no-perception login and access Internet on ssid1 and ssid2 via the account test1 and test2 respectively. If the user actively gets offline or is ticked offline by the administrator on ssid1, it cannot perform the no-perception login on ssid1, but still can perform the no-perception login and access Internet on ssid2.

Fast no-perception configuration

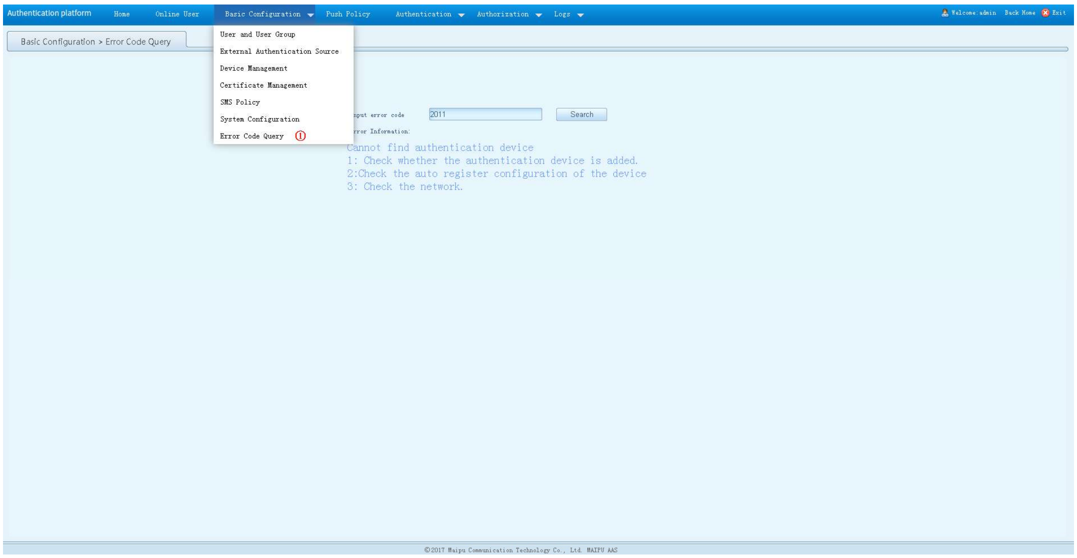
After enabling the fast no-perception, the configured “Push frequency” is “Not push” in “Authorization”->“Portal”->“Duration Policy” of the authentication platform, that is, not push the intervention interface. After the user terminal connects the device, the device will actively initiate one online packet to the authentication platform for authentication. After passing the authentication, the user can access Internet, that is, fast no-perception network access.

Caution

- The pre-share key of the device should be consistent with the configure key of the device.

10.2.7 Error Code Query

The module provides the query function for the returned error code when the user authentication fails, as shown in the following figure:



nput error code 2011

rror Information:

```
Cannot find authentication device
1: Check whether the authentication device is added.
2:Check the auto register configuration of the device
3: Check the network.
```

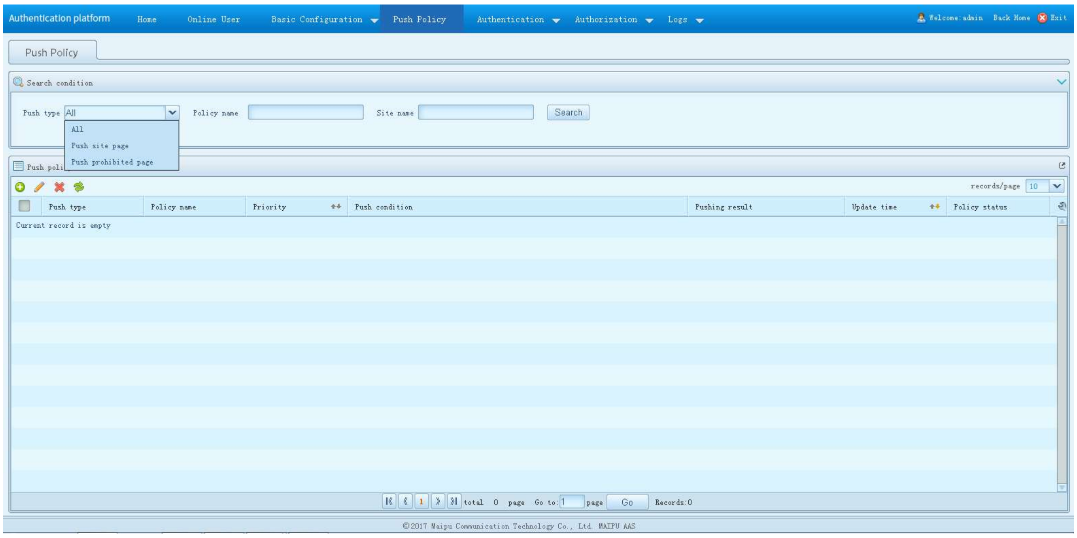
Figure 10-2-30 Error code query

10.3 Push Policy

In the push policy module functions, you can specify pushing to one site or prohibited interface by the device AP MAC, AP SN, SSID, AC_NAME, IP address segment and terminal type, and also can combine several types of information as one policy. The combination includes two cases: 1: When the conditions do not repeat, it is necessary to meet all conditions so that the policy can be executed; 2: When the conditions have repetition, it just needs to meet any repeated condition.

Push policy query

The push policy query can take the push type, policy name, and site name as the query condition to query, as shown in the following figure:



Push type: All
- All
- Push site page
- Push prohibited page

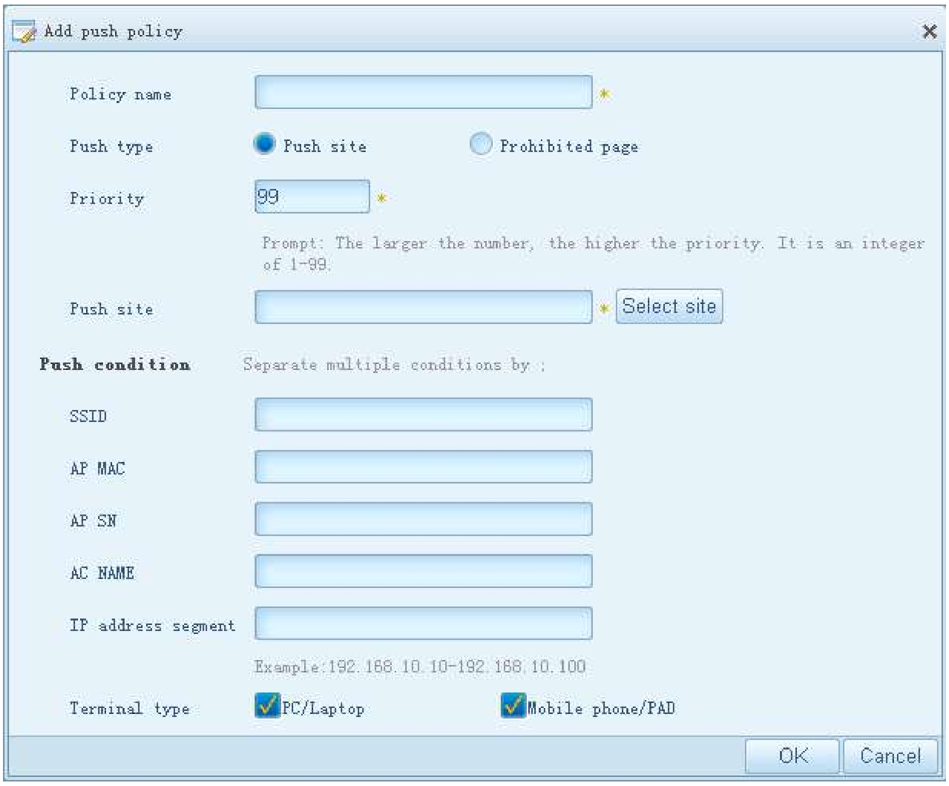
Policy name:
Site name:
records/page: 10

Current record is empty

total 0 page Go to: 1 page Records: 0

Figure 10-3-1 Query the push policy

Add/edit push policy



Policy name: *

Push type: ● Push site ○ Prohibited page

Priority: 99 *

Prompt: The larger the number, the higher the priority. It is an integer of 1-99.

Push site: *

Separate multiple conditions by ;

SSID:

AP MAC:

AP SN:

AC NAME:

IP address segment:

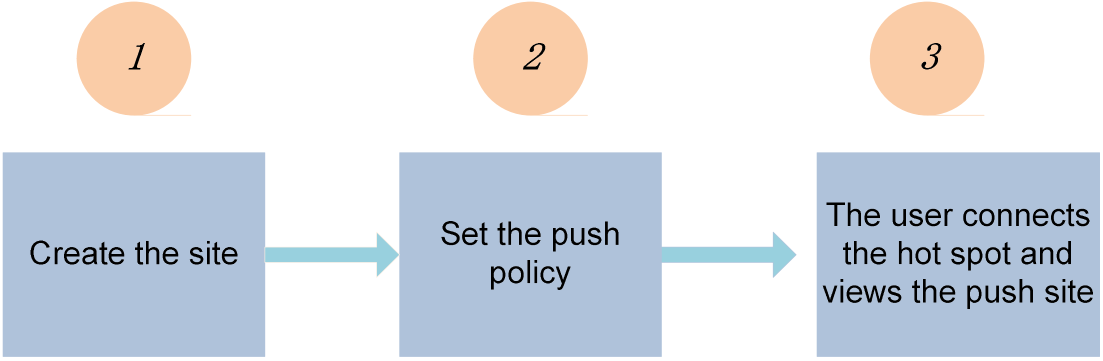
Example:192.168.10.10-192.168.10.100

Terminal type: ☑ PC/Laptop ☑ Mobile phone/PAD

Figure 10-3-2 Add/edit the push policy

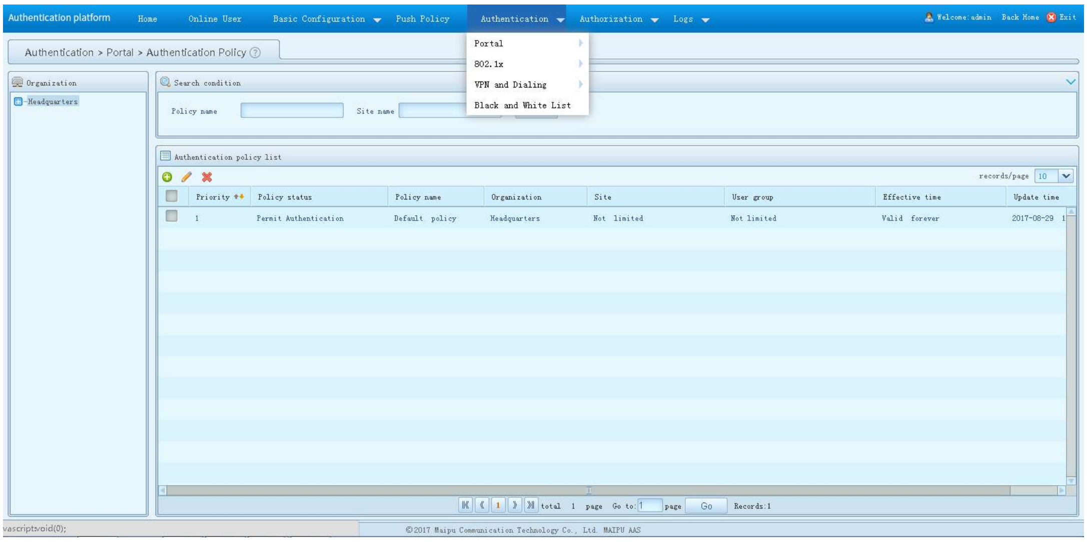
Adding the push policy of the IP address is mainly to make up for the scenario that the NAS device cannot carry the AP_MAC parameter. Pushing by the IP address segment is usually used by the combination of the IP address segment with AC_NAME and is mainly applicable to the scenario that the IP address segment is different, but the AC_NAME is the same or the IP address segment is the same, but AC_NAME is different.

The operation of the push policy realizing the push site is simple. First, add a site on the marketing platform. For details, refer to the chapter of **Site Management**.



10.4 Authentication Configuration

The authentication configuration mainly refers to the configuration of the related policies in the Portal authentication, 802.1X, VPN and dialing authentication, and also contains the configuration of the global effective black/white list. As shown in the following figure, click **Authentication**, and the following describes the functions in the authentication configuration menus.



☐	Priority	Policy status	Policy name	Organization	Site	User group	Effective time	Update time
☐	1	Permit Authentication	Default policy	Headquarters	Not limited	Not limited	Valid forever	2017-08-29 1

Figure 10-4-1 Authentication configuration

Caution

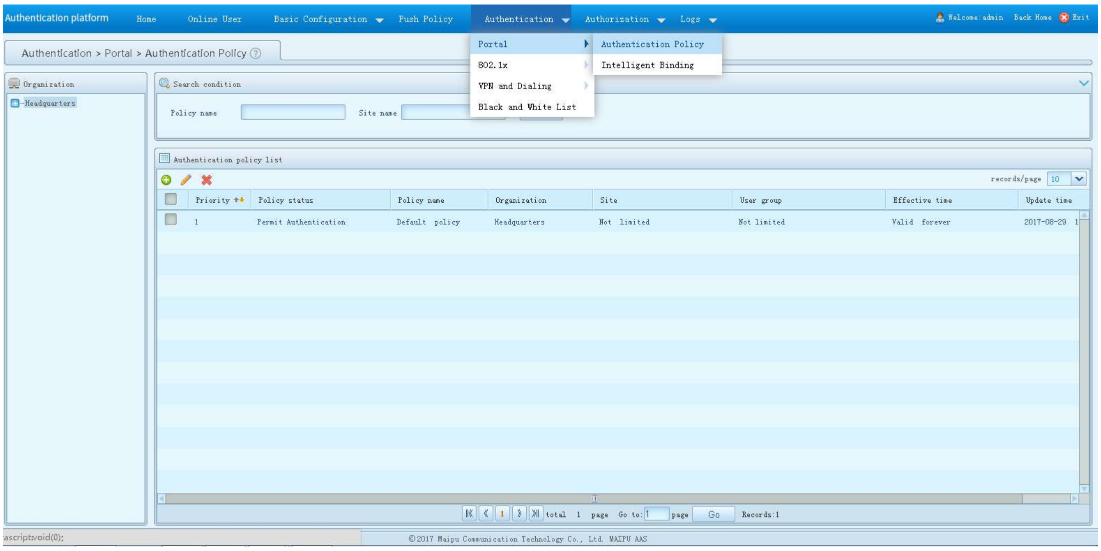
- The matching rule of the policy adopts the recursive matching to higher organization, and then, matching the policy conditions. If matching successfully, the policy is matched successfully.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

10.4.1 Authentication Policy

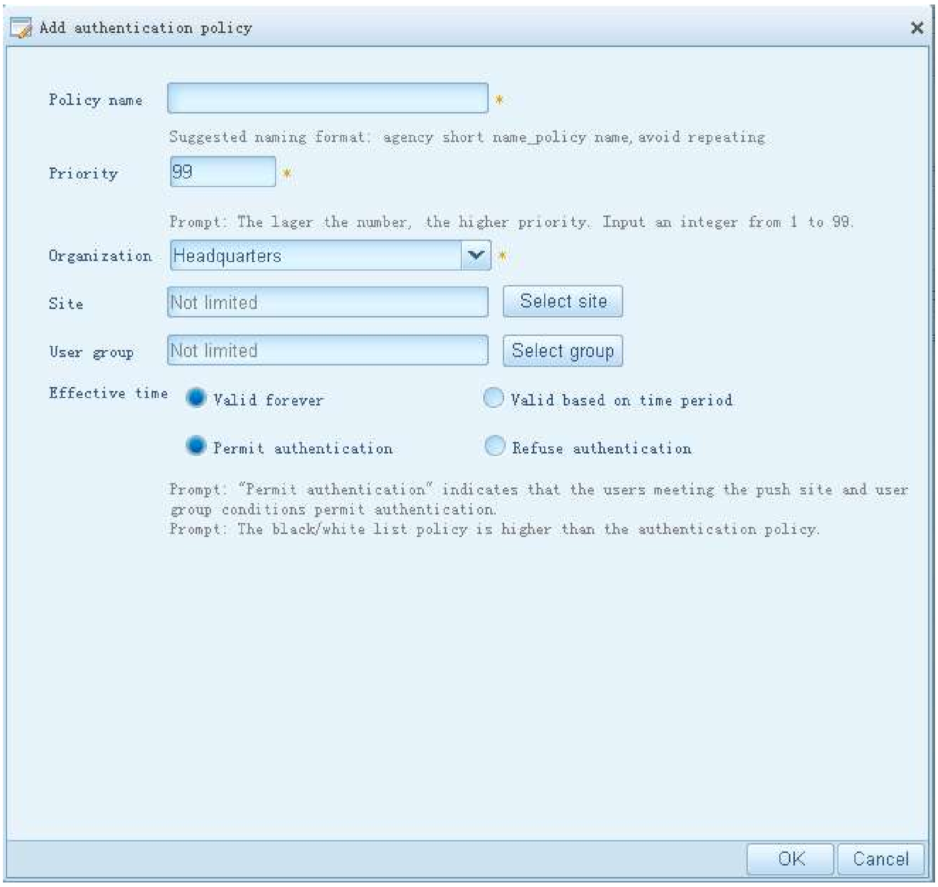
The authentication policy mainly includes Portal scenario and 802.1X scenario. The authentication policy manages the time period of the user accessing Internet according to the organization, site, user group, ssid and other combined conditions, and controls whether the user can access Internet. Take the Portal scenario as an example, and the "**Authentication policy**" interface is shown in the following figure:



☐	Priority	Policy status	Policy name	Organization	Site	User group	Effective time	Update time
☐	1	Permit Authentication	Default policy	Headquarters	Not limited	Not limited	Valid forever	2017-08-29 1

Figure 10-4-2 Authentication policy

Add/Modify the authentication policy



Add authentication policy

Policy name: *

Suggested naming format: agency short name_policy name, avoid repeating

Priority: 99 *

Prompt: The lager the number, the higher priority. Input an integer from 1 to 99.

Organization: Headquarters *

Site: Not limited

User group: Not limited

Effective time: ● Valid forever ○ Valid based on time period

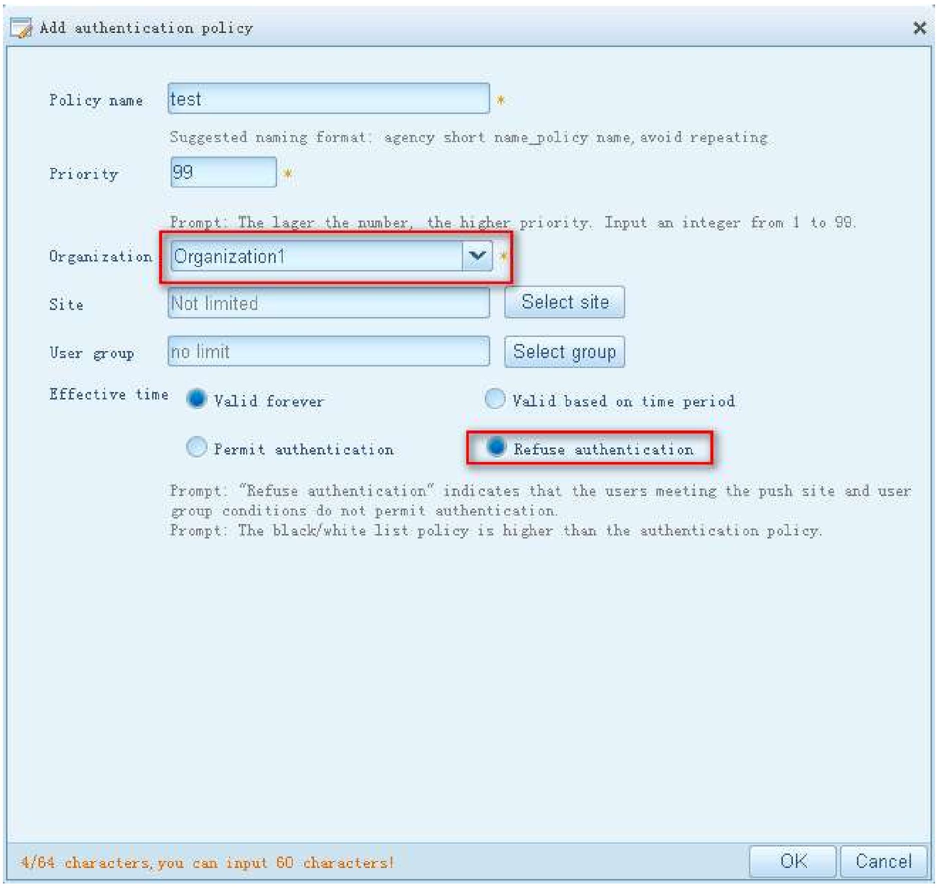
● Permit authentication ○ Refuse authentication

Prompt: "Permit authentication" indicates that the users meeting the push site and user group conditions permit authentication.
Prompt: The black/white list policy is higher than the authentication policy.

Figure 10-4-3 Authentication policy

Example:

1. Configure one authentication policy, as shown in the following figure:



Policy name: test *

Suggested naming format: agency short name_policy name, avoid repeating

Priority: 99 *

Prompt: The lager the number, the higher priority. Input an integer from 1 to 99.

Organization: Organization1 *

Site: Not limited

User group: no limit

Effective time: ● Valid forever ○ Valid based on time period

○ Permit authentication ● Refuse authentication

Prompt: "Refuse authentication" indicates that the users meeting the push site and user group conditions do not permit authentication.

Prompt: The black/white list policy is higher than the authentication policy.

4/64 characters, you can input 60 characters!

2. When the user connects wifi for accessing Internet at organization 1, the configured in the authentication policy is that all authentication modes in organization 1 are refused, so no user can pass the authentication or access Internet.

Caution

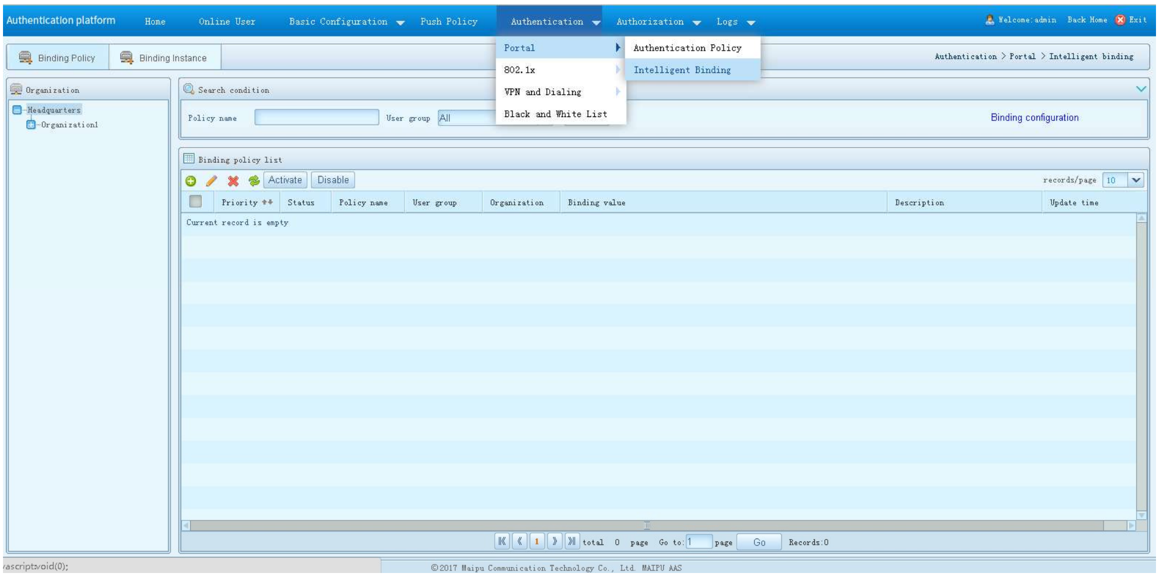
- The difference of the authentication policies in Portal scenario and 802.1X scenario is: In the Portal scenario, you can set the site; in the 802.1X scenario, when setting ssid, you cannot set the site option.

10.4.2 Intelligent Binding

The using scenario of the intelligent binding includes the Portal scenario and 802.1X scenario VPN and dialing and so on. The module contains "Binding Policy" and "Binding

Instance”. The administrator configures one intelligent binding policy. If one user meets the set conditions of the policy and matches the policy during authentication, generate one binding instance corresponding to the user according to the user information, and you can query the instance in the “Binding Instance” interface. The module mainly provides the functions of adding, deleting, modifying, activating, and disabling the binding policy, as well as activating, disabling and clearing up the binding instance. Take the Portal scenario as an example, and the “Intelligent Binding” interface is as shown in the following figure:

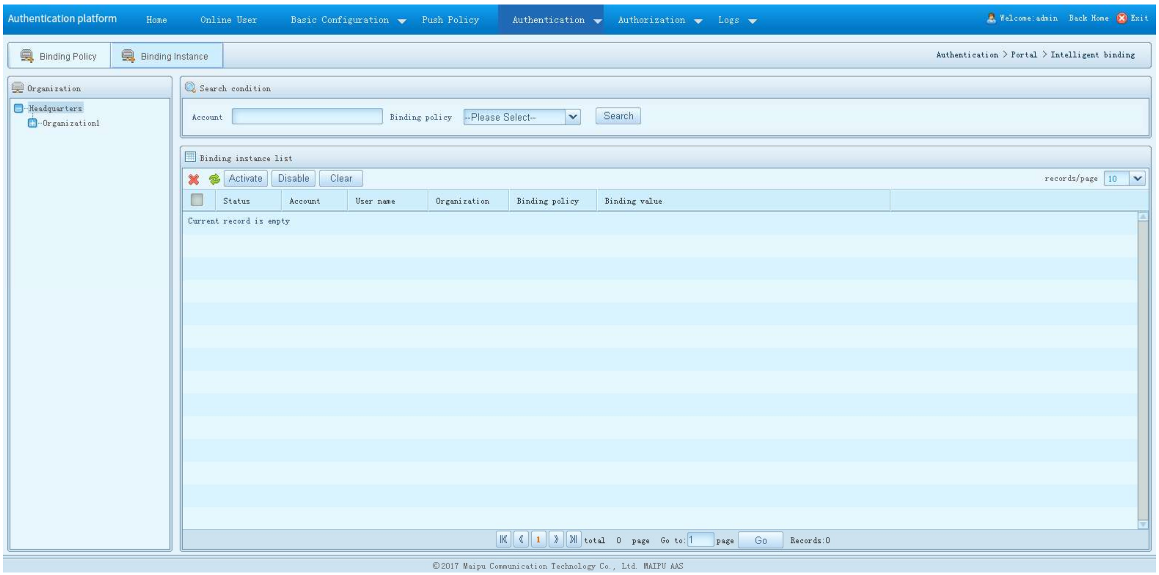
Binding policy



Current record is empty

Figure 10-4-4 Binding policy

Binding instance



Current record is empty

Figure 10-4-5 Binding instance

Binding configuration

On the “**Binding policy**” interface, click **Binding configuration**, as shown in the following figure:

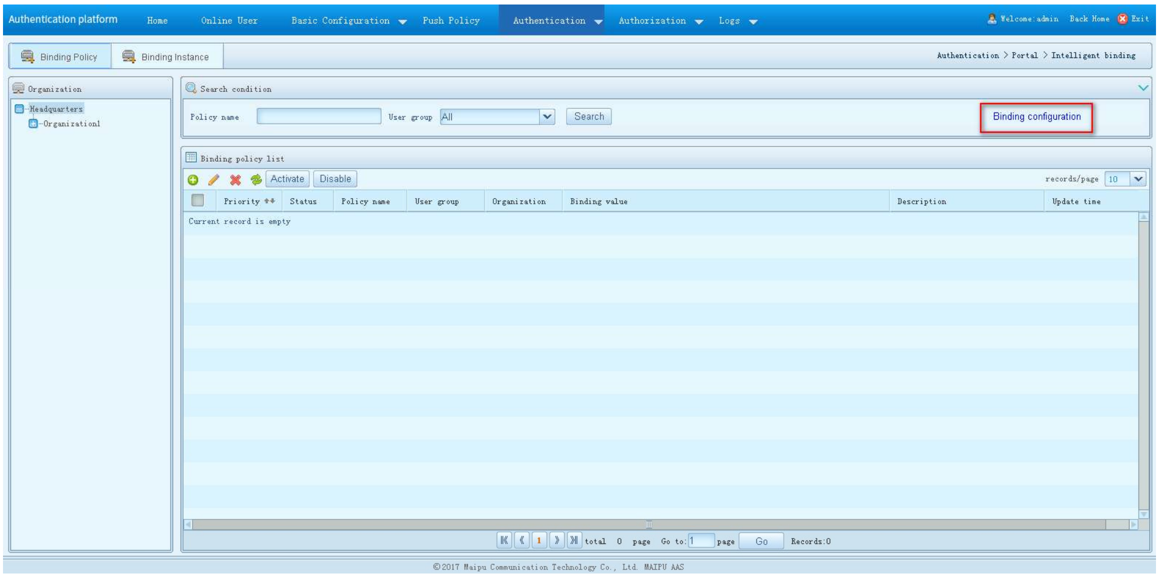
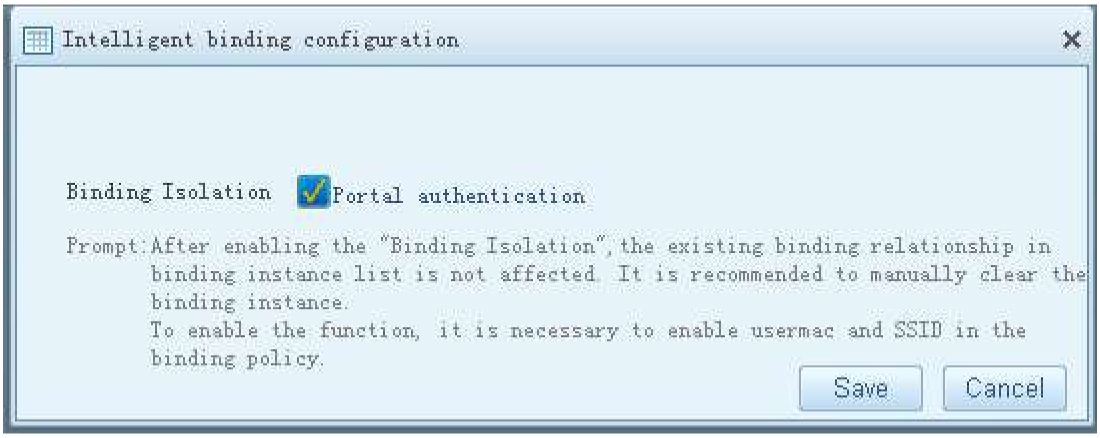


Figure 10-4-6 Binding configuration

After clicking the button, display the following dialog box:



Binding Isolation ☑ Portal authentication

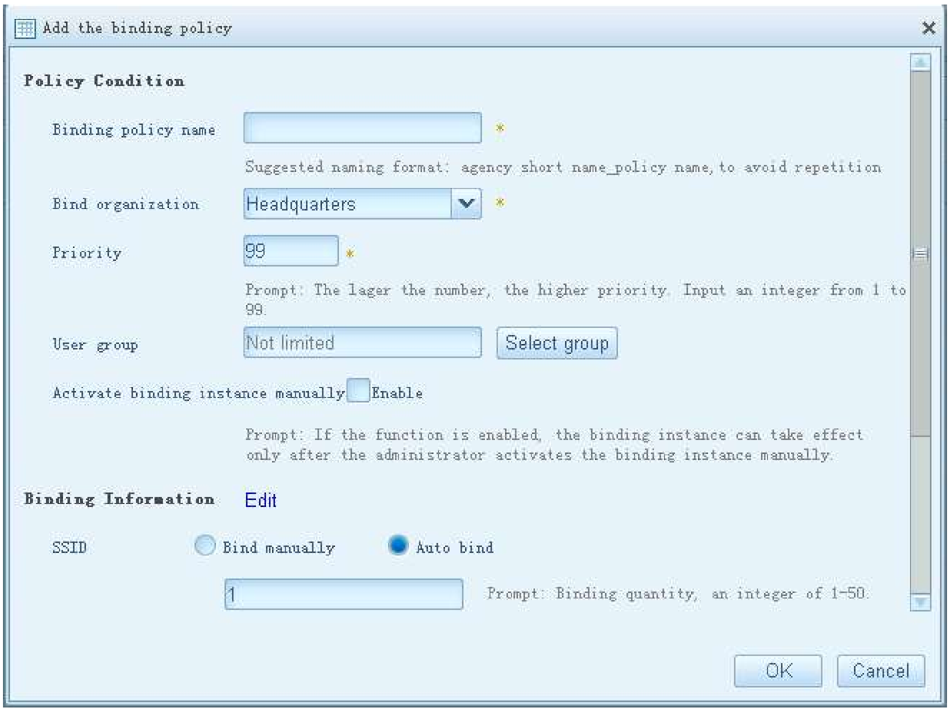
Prompt: After enabling the "Binding Isolation", the existing binding relationship in binding instance list is not affected. It is recommended to manually clear the binding instance.
To enable the function, it is necessary to enable usermac and SSID in the binding policy.

Figure 10-4-7SSID binding isolation

Enable SSID binding isolation: After the user adopts the account test1 to authenticate via the device with ssid name ssid1 successfully and access Internet and if the user authenticates via the device with ssid name ssid2 to access Internet, it will fail.

Disable SSID binding isolation: The user can access Internet after authenticating via any ssid and meeting the other policy conditions.

Add/modify the binding policy



Add the binding policy

Policy Condition

Binding policy name *

Suggested naming format: agency short name_policy name, to avoid repetition

Bind organization: Headquarters *

Priority: 99 *

Prompt: The lager the number, the higher priority. Input an integer from 1 to 99.

User group: Not limited

Activate binding instance manually ☐ Enable

Prompt: If the function is enabled, the binding instance can take effect only after the administrator activates the binding instance manually.

Binding Information

SSID ○ Bind manually ● Auto bind

1

Prompt: Binding quantity, an integer of 1-50.

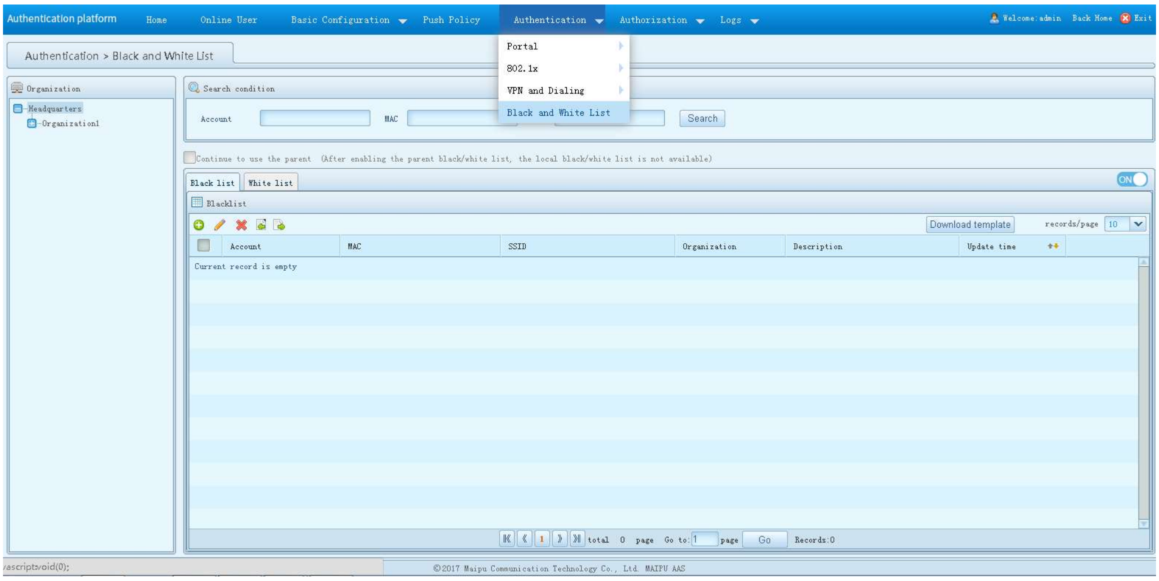
Figure 10-4-8 Add the binding policy

Caution

- When adding one “Intelligent binding policy”, the administrator needs to enter the “Bind instance” interface manually, and find the generated binding instance of the user. After activating the instance, the user can be authenticated and access the network successfully.

10.4.3 Black/White List

Click **Authentication** > **Black and White List** to enter the **Black and White List** management interface. The module mainly provides the functions of adding, modifying, querying, deleting, importing and exporting the black and white list, and downloading the template, as shown in the following figure:

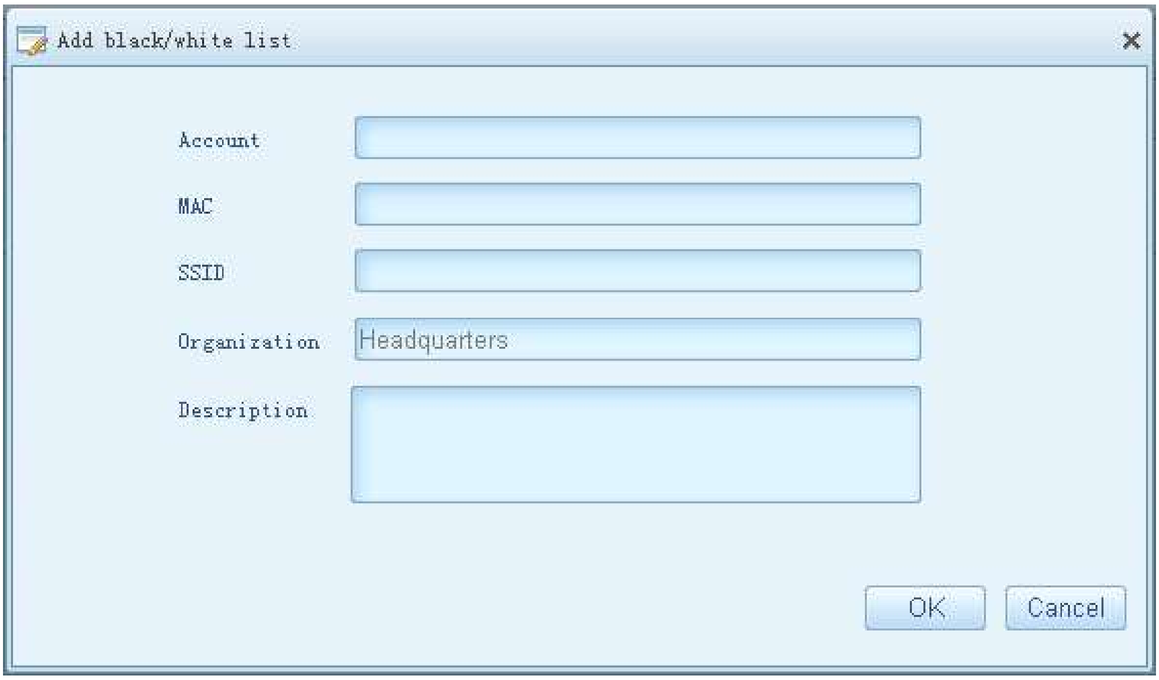


☐ Continue to use the parent (After enabling the parent black/white list, the local black/white list is not available.)

Current record is empty

Figure 10-4-9 Black and white list

Add/modify the black list or white list



Organization: Headquarters

Figure 10-4-10 Add the black and white list

Caution

- If the current organization is the root organization, it cannot continue to use the black list or white list of the parent organization. If it is not the root organization, it can continue to use the parent black/white list, and the blacklist or white list will not be available at this time, If not wanting to continue to use the parent blacklist or whitelist, first cancel the “Continue to use the parent” option above the list. Meanwhile, click the “ON” button at the right of the list. After enabling, you can configure the blacklist or whitelist of this organization.

10.5 Authorization Policy

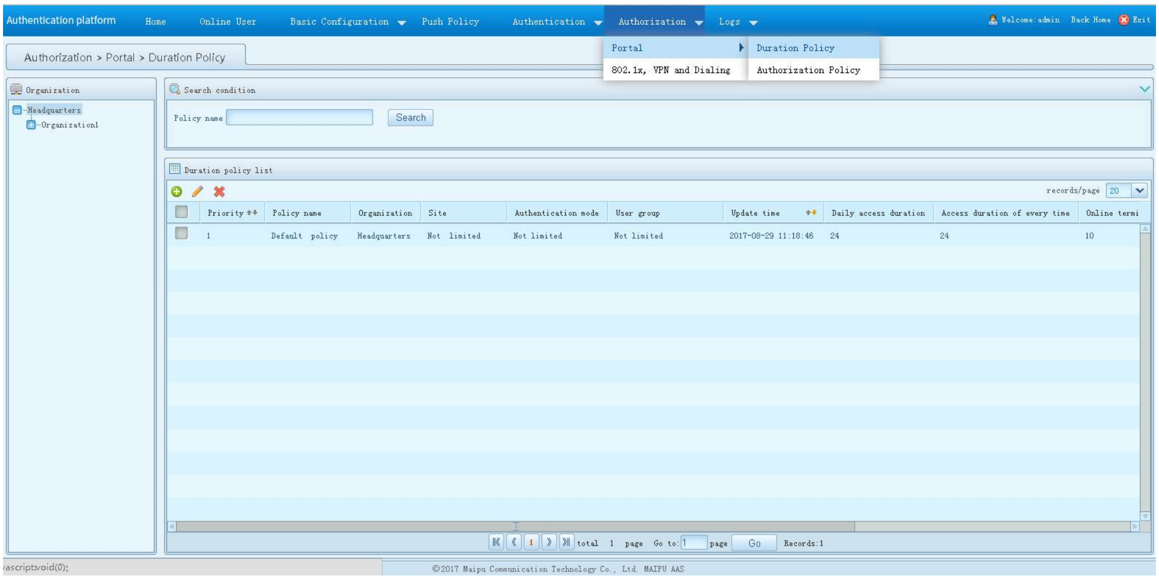
The module mainly contains the configuration of “Duration policy”, “Authorization policy” and so on.

Caution

- The matching rule of the policy adopts the recursive matching to higher organization, and then, matches the policy condition. If matching successfully, the policy matches successfully.

10.5.1 Duration Policy

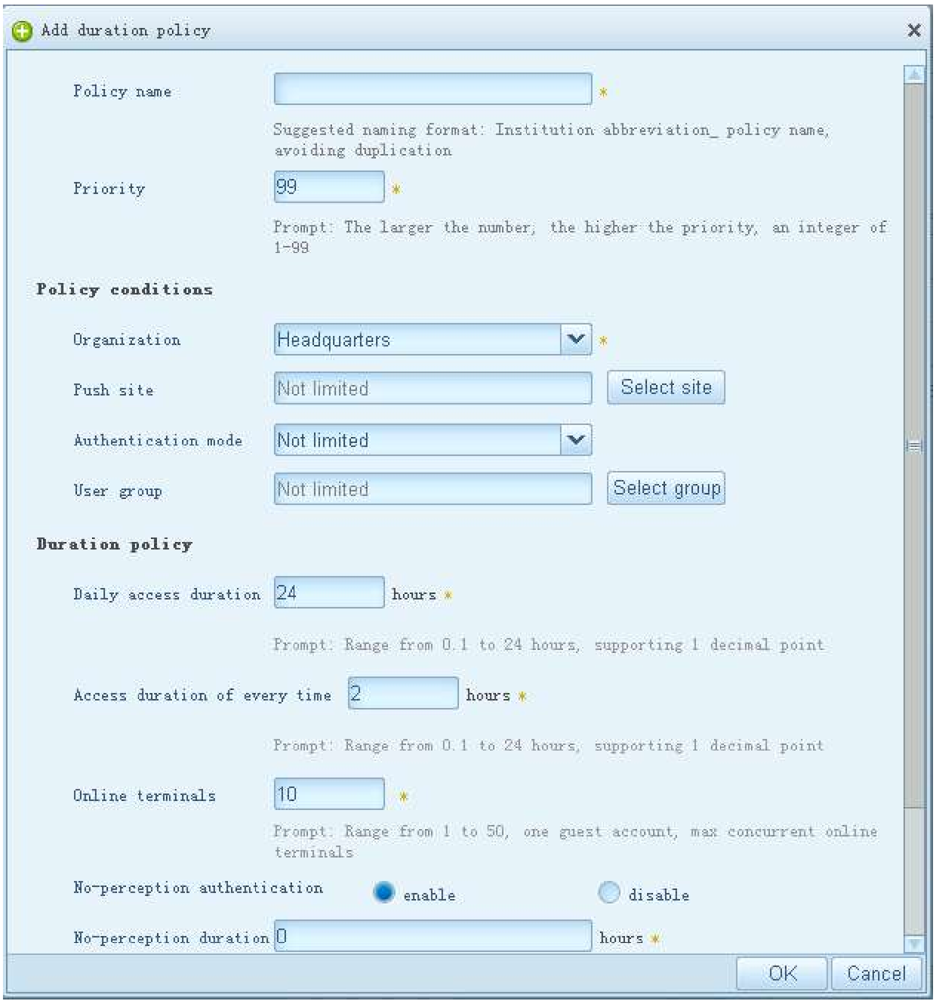
The module mainly provides the functions of adding, deleting, modifying and querying the duration policy, as shown in the following figure:



☐	Priority	Policy name	Organization	Site	Authentication mode	User group	Update time	Daily access duration	Access duration of every time	Online termi
☐	1	Default policy	Headquarters	Not limited	Not limited	Not limited	2017-08-29 11:18:46	24	24	10

Figure 10-5-1 Duration policy

Add/modify the duration policy



Add duration policy

Policy name: *

Suggested naming format: Institution abbreviation_ policy name, avoiding duplication

Priority: 99 *

Prompt: The larger the number, the higher the priority, an integer of 1-99

Policy conditions

Organization: Headquarters *

Push site: Not limited

Authentication mode: Not limited

User group: Not limited

Duration policy

Daily access duration: 24 hours *

Prompt: Range from 0.1 to 24 hours, supporting 1 decimal point

Access duration of every time: 2 hours *

Prompt: Range from 0.1 to 24 hours, supporting 1 decimal point

Online terminals: 10 *

Prompt: Range from 1 to 50, one guest account, max concurrent online terminals

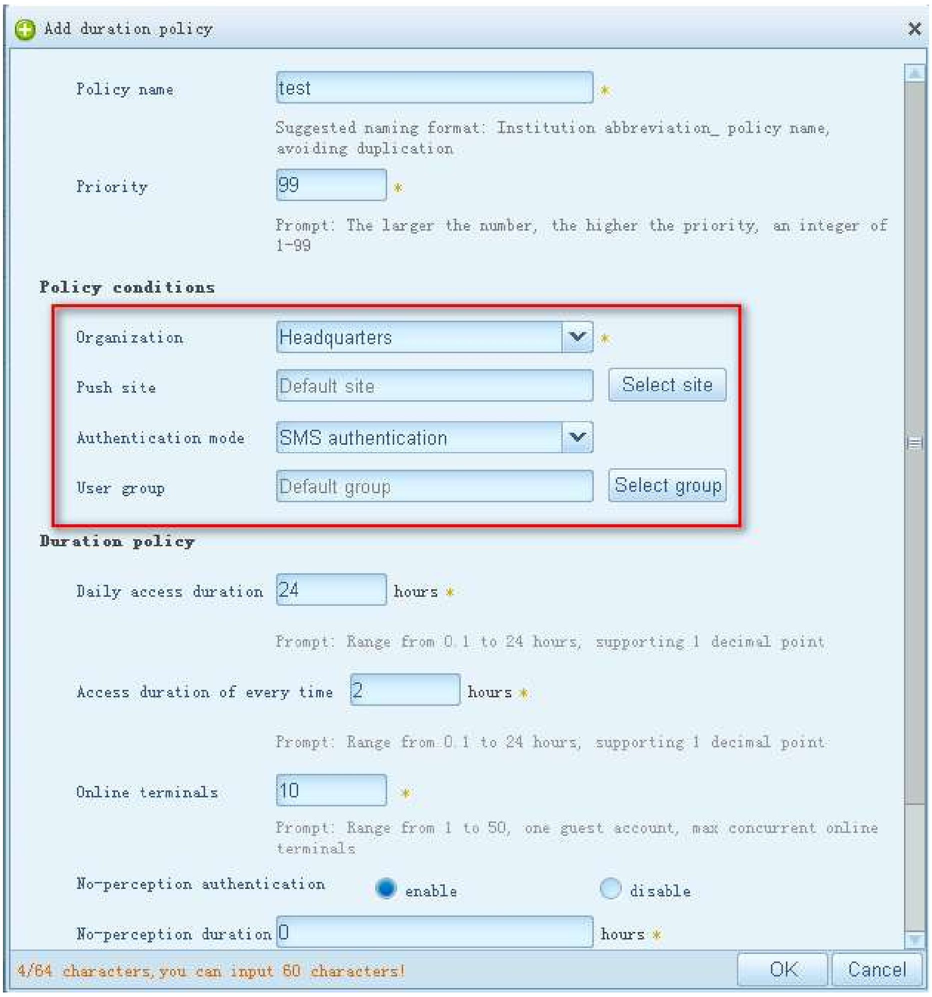
No-perception authentication: ● enable ○ disable

No-perception duration: 0 hours *

Figure 10-5-2 Add the duration policy

Instance:

1. Add one duration policy, as shown in the following figure:



Add duration policy

Policy name: test *

Suggested naming format: Institution abbreviation_ policy name, avoiding duplication

Priority: 99 *

Prompt: The larger the number, the higher the priority, an integer of 1-99

Policy conditions

Organization: Headquarters *

Push site: Default site

Authentication mode: SMS authentication

User group: Default group

Duration policy

Daily access duration: 24 hours *

Prompt: Range from 0.1 to 24 hours, supporting 1 decimal point

Access duration of every time: 2 hours *

Prompt: Range from 0.1 to 24 hours, supporting 1 decimal point

Online terminals: 10 *

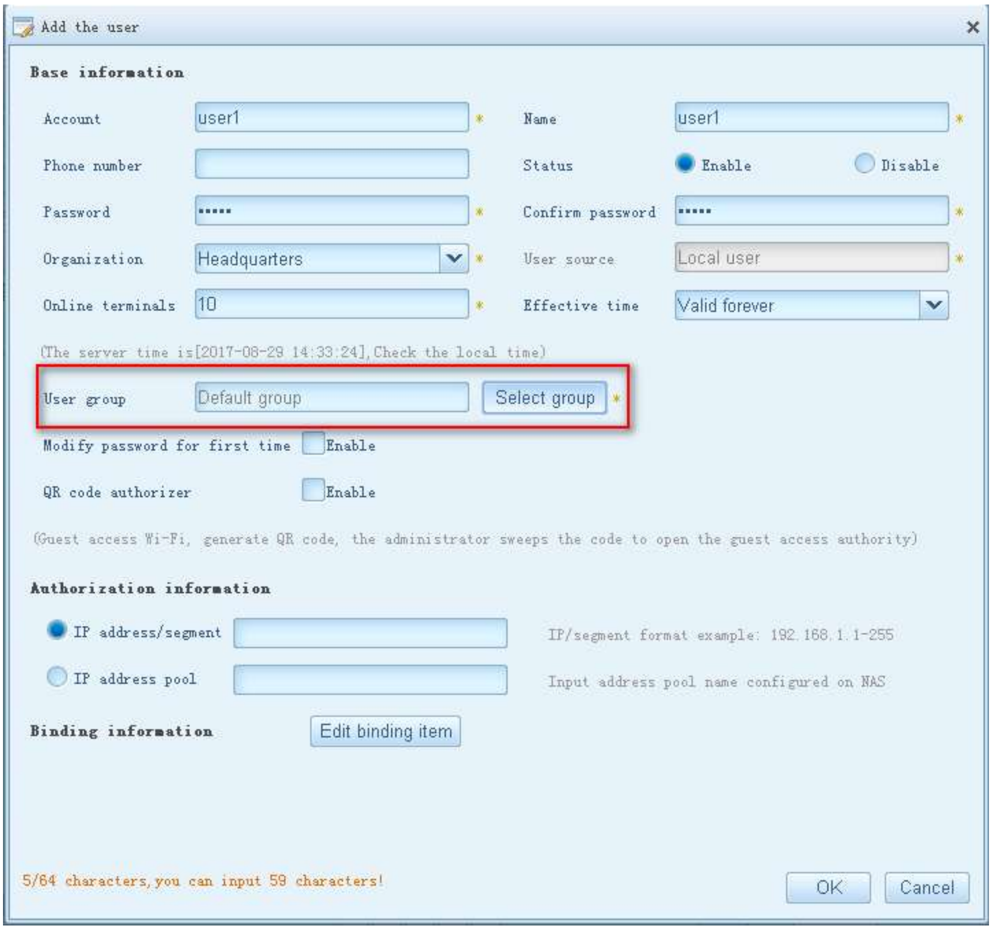
Prompt: Range from 1 to 50, one guest account, max concurrent online terminals

No-perception authentication: ● enable ○ disable

No-perception duration: 0 hours *

4/64 characters, you can input 60 characters!

2. Add a user (user 1), as shown in the following figure:



Base information

Account	user1 *	Name	user1 *
Phone number		Status	● Enable ○ Disable
Password	••••• *	Confirm password	••••• *
Organization	Headquarters *	User source	Local user *
Online terminals	10 *	Effective time	Valid forever

(The server time is[2017-08-29 14:33:24],Check the local time)

User group: Default group *

Modify password for first time ☐ Enable

QR code authorizer ☐ Enable

(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)

Authorization information

● IP address/segment — IP/segment format example: 192.168.1.1-255

○ IP address pool — Input address pool name configured on NAS

Binding information

5/64 characters,you can input 59 characters!

3. When the user adopts the account user1 to access Internet at the organization “Headquarters” and if the site pushed by the system to the user is “Default site” and the used authentication mode is “SMS authentication”, the user condition can match the push policy “test”. And then, check whether the current user matches the “Daily network access duration”, “Once network access duration” and other conditions in the policy. If meeting, the user can authenticate and access the network successfully. Otherwise, authentication fails.

Caution

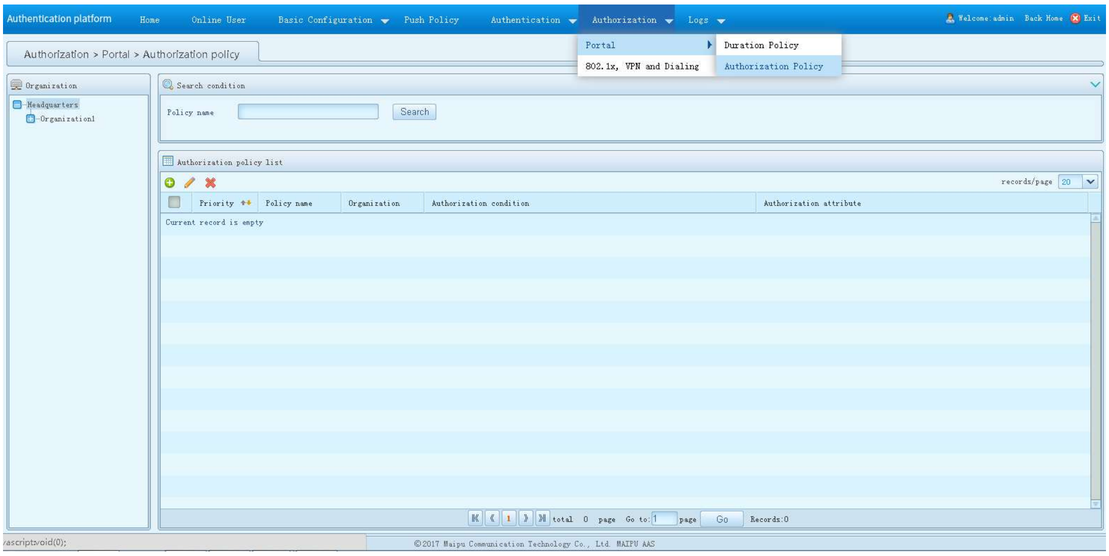
- When adding the duration policy and if “No-perception authentication” is not enabled, the user cannot perform the no-perception authentication or access Internet.
- If the “Push frequency” in the duration policy is configured as push every time when enabling “Fast no-perception” in the “System configuration”, the user cannot perform the fast no-perception authentication, but can perform the no-

perception authentication.

10.5.2 Authorization Policy

According to the connected NAS device, match the corresponding authorization policy, and deliver the attributes of the policy configuration (ACL, QoS, VLAN, authorization group, attribute set and so on).

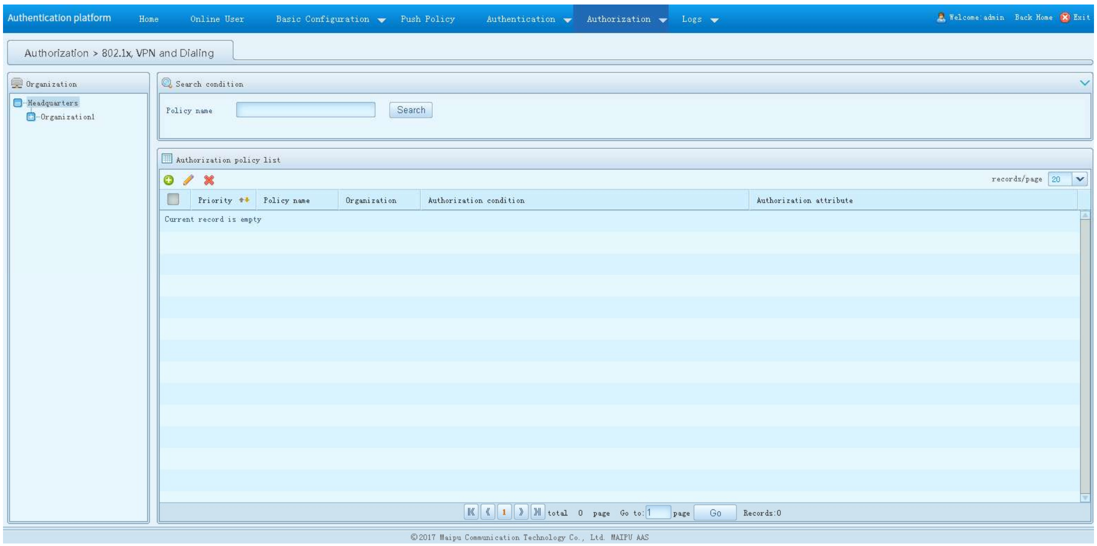
In the Portal scenario, the authorization policy is shown in the following figure.



Current record is empty

Figure 10-5-3 Authorization policy in Portal scenario

In the 802.1x, VPN and dialing scenarios, the authorization policy is shown in the following figure:

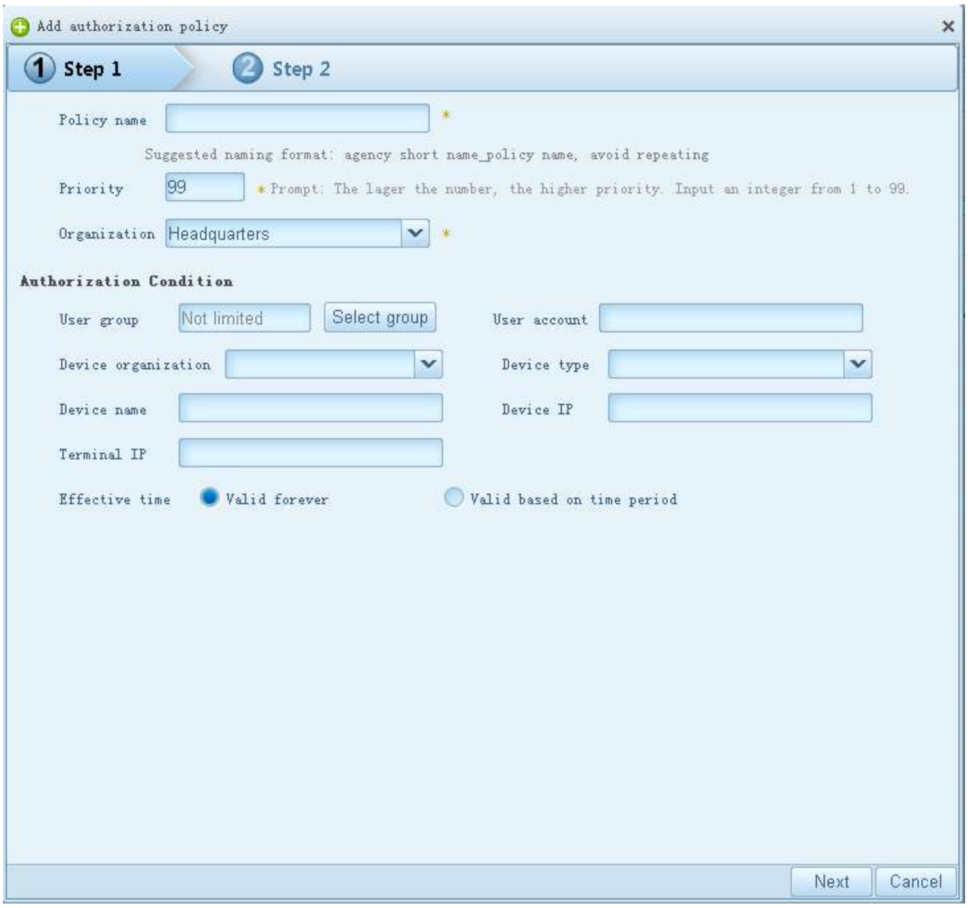


Current record is empty

Figure 10-5-4 Authorization policy in the 802.1x, VPN and dialing scenarios

Add/modify the authorization policy

Step 1:



Policy name: *

Suggested naming format: agency short name_policy name, avoid repeating

Priority: 99 * Prompt: The lager the number, the higher priority. Input an integer from 1 to 99.

Organization: Headquarters *

User group: Not limited

User account:

Device organization:

Device type:

Device name:

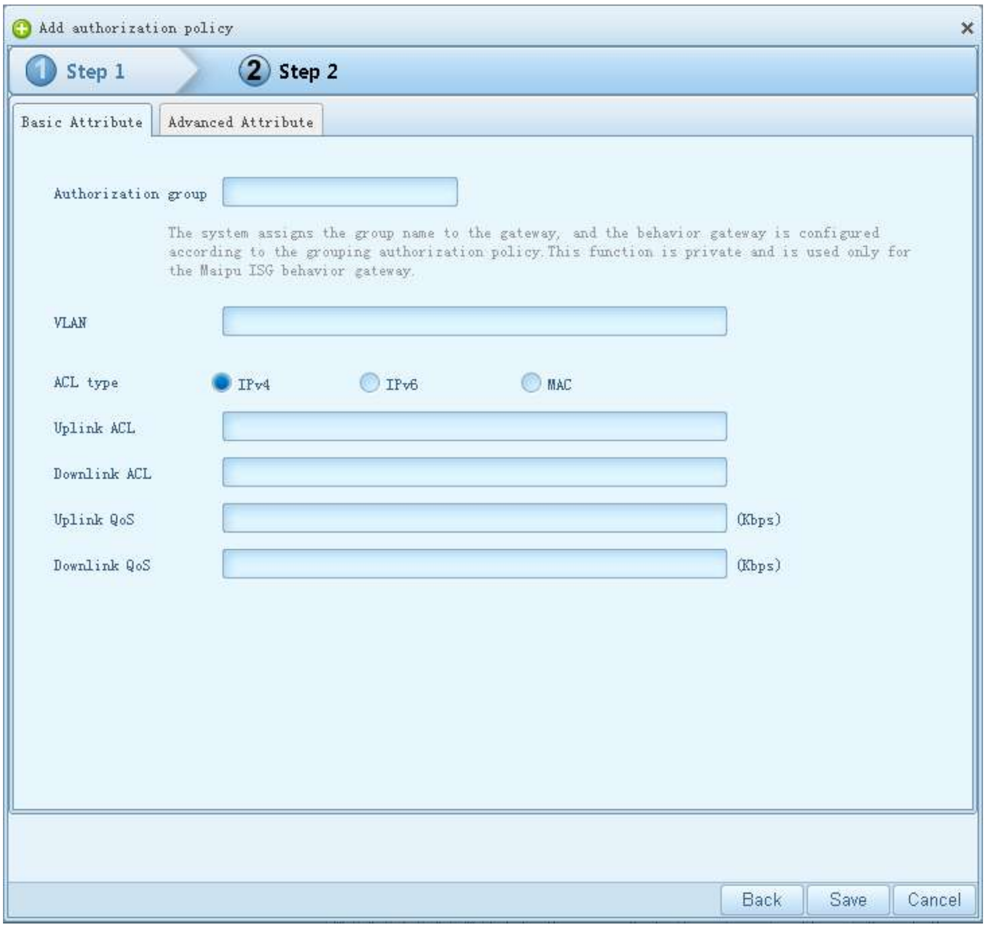
Device IP:

Terminal IP:

Effective time: ● Valid forever ○ Valid based on time period

Figure 10-5-5 Add the authorization policy

Step 2: In step 2 of adding the authorization policy, you can fill in the related attributes of the policy. Select at least one of “Basic attribute” and “Advanced attribute” at the top left corner, as shown in the following figure:



The system assigns the group name to the gateway, and the behavior gateway is configured according to the grouping authorization policy. This function is private and is used only for the Maipu ISG behavior gateway.

ACL type ● IPv4 ○ IPv6 ○ MAC

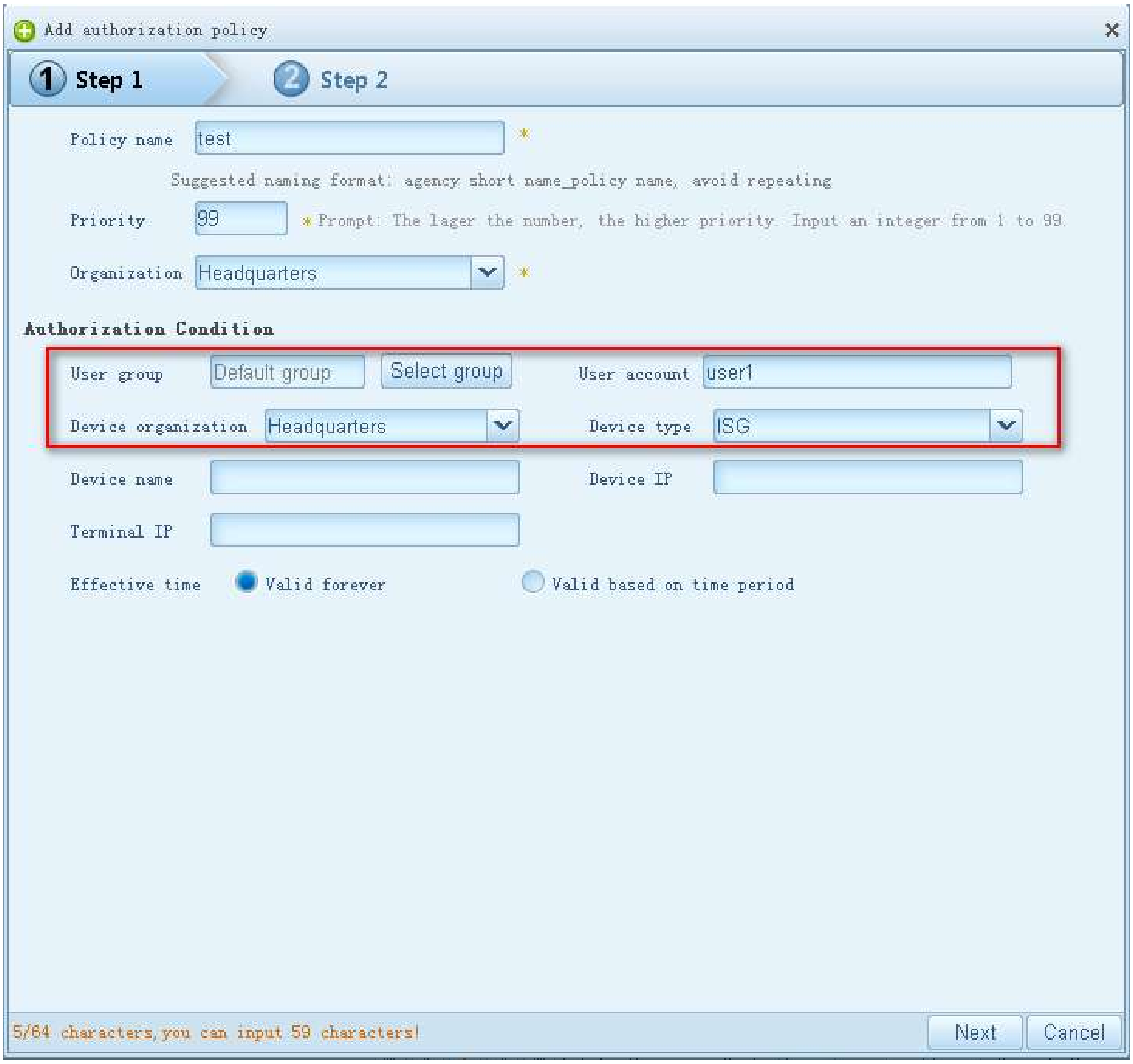
Figure 10-5-6 Add the authorization policy

When the AC device serves as Nas: Deliver the VLAN, ACL, QoS, and advanced attribute to the device.

When the ISG device serves as Nas: Deliver the authorization group to the device, and ISG does not process the other attributes.

Instance:

1. Add one authorization policy, as shown in the following figure:



Add authorization policy

Policy name: test *

Suggested naming format: agency short name_policy name, avoid repeating

Priority: 99 * Prompt: The lager the number, the higher priority. Input an integer from 1 to 99.

Organization: Headquarters *

Authorization Condition

User group: Default group

User account: user1

Device organization: Headquarters

Device type: ISG

Device name:

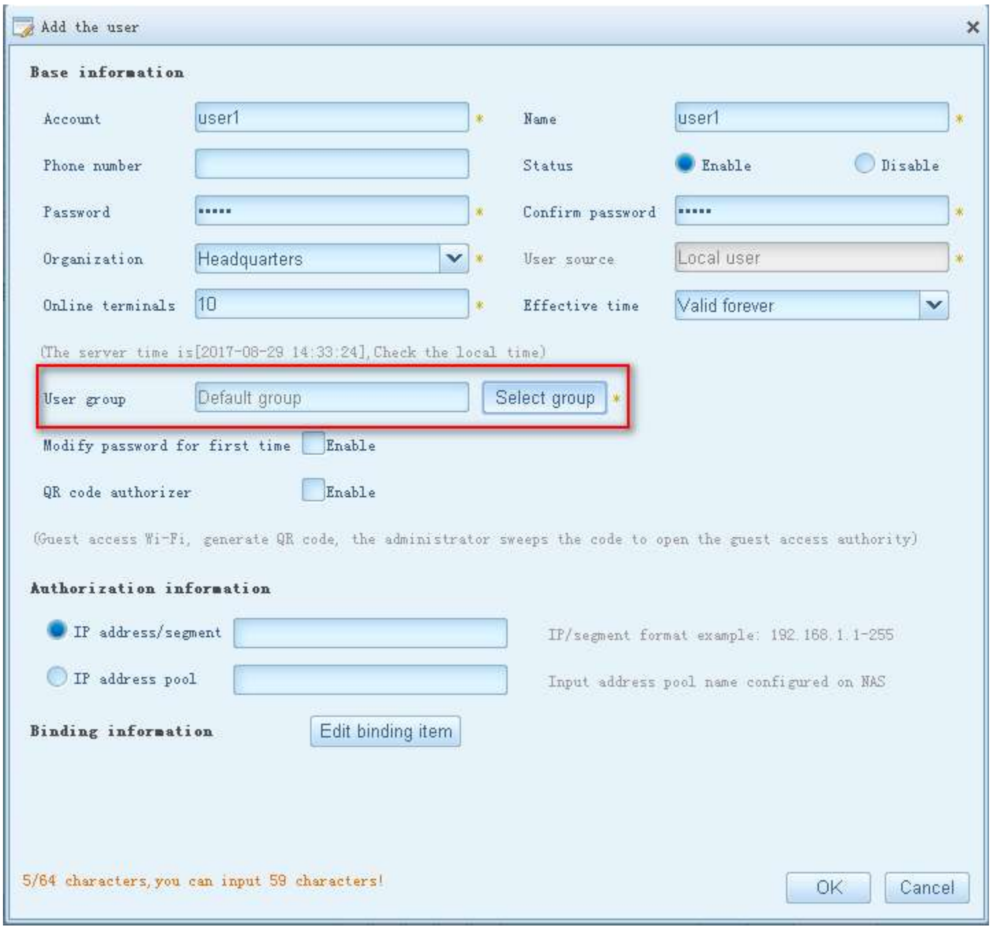
Device IP:

Terminal IP:

Effective time: ● Valid forever ○ Valid based on time period

5/64 characters,you can input 59 characters!

2. Add one user (user1), as shown in the following figure:



Add the user

Base information

Account: user1 *
Name: user1 *
Phone number:
Status: ● Enable ○ Disable
Password: ••••• *
Confirm password: ••••• *
Organization: Headquarters *
User source: Local user *
Online terminals: 10 *
Effective time: Valid forever

(The server time is[2017-08-29 14:33:24],Check the local time)

User group: Default group *
Modify password for first time ☐ Enable
QR code authorizer ☐ Enable

(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)

Authorization information

● IP address/segment — IP/segment format example: 192.168.1.1-255
○ IP address pool — Input address pool name configured on NAS

Binding information

5/64 characters,you can input 59 characters!

3. The user adopts the account user1 in the “Default group” and performs the login authentication in the “Headquarters” site. If the authentication authorization device type is ISG and the organization of the device is “Headquarters”, match the policy “test1”. After matching successfully, deliver the related attributes configured in Step 2 of the policy to the device.

Caution

- Take delivering vlan as an example. The configured VLAN in the authorization policy should be consistent with the configured vlan of the device. For example, if the configured VLAN of the authorization policy is 100, the VLAN delivered to the device should be 100.

  802.1X macbased+hybrid port+mac-vlan enable

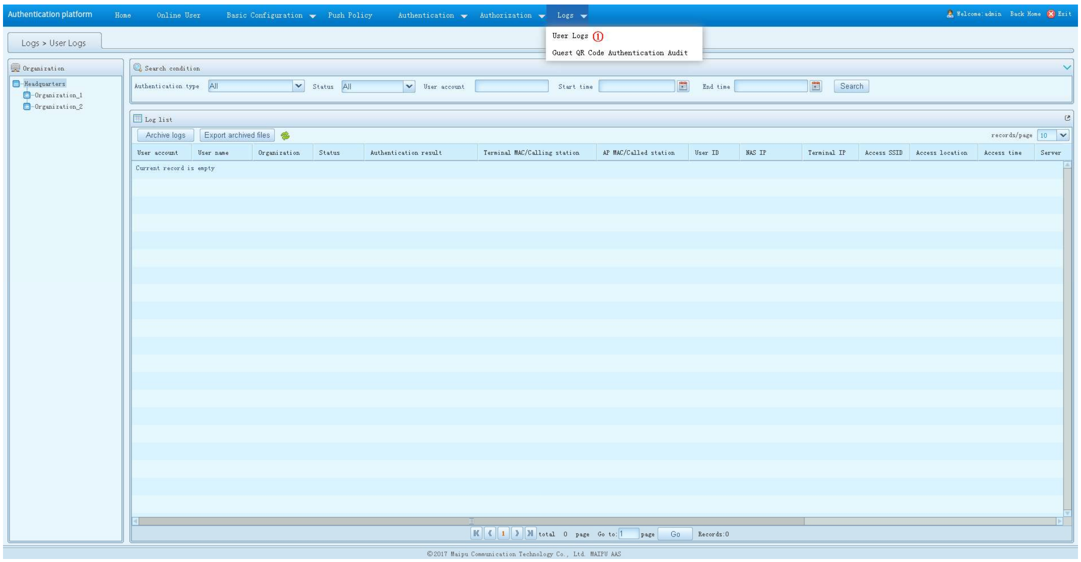
  ```
  switch(config-if-gigabitethernet0/0/8)#sho run interface gigabitethernet 0/0/8
  ```

```
Building Configuration...

interface gigabitethernet0/0/8

switchport mode hybrid

switchport hybrid untagged vlan 1,100-101

switchport hybrid pvid vlan 100

mac-vlan enable

dot1x port-control enable

exit
```

10.6 Logs

10.6.1 User logs

With the user log, you can view the login status of the user, and can archive and download the log. The main interface is shown in the following figure:



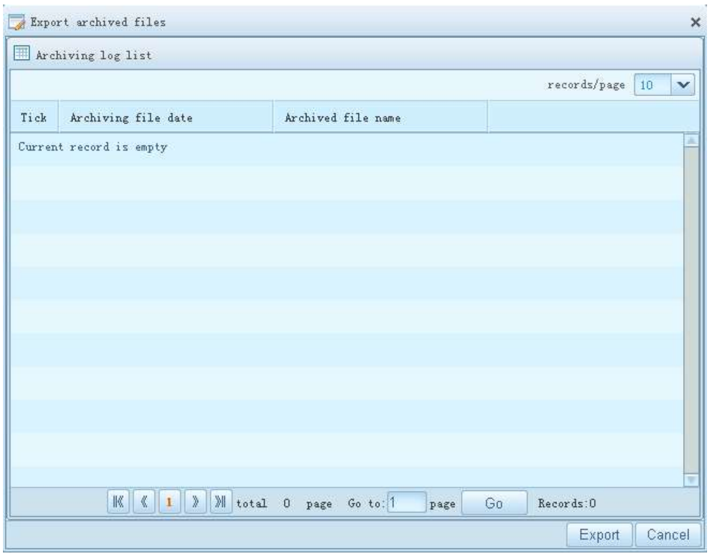
User account	User name	Organization	Status	Authentication result	Terminal MAC/Calling station	AP MAC/Called station	User ID	NAS IP	Terminal IP	Access SSID	Access location	Access time	Server
Current record is empty													

Figure 10-6-1User log list

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

Click the “Archive logs” button of the main interface, and you can archive the log. After archiving, click “Export archived files” and you can download the archived log, as shown in the following figure:



records/page 10

Tick	Archiving file date	Archived file name

Current record is empty

1 total 0 page Go to: 1 page

Records:0

Figure 10-6-2 Export the archive log

Caution

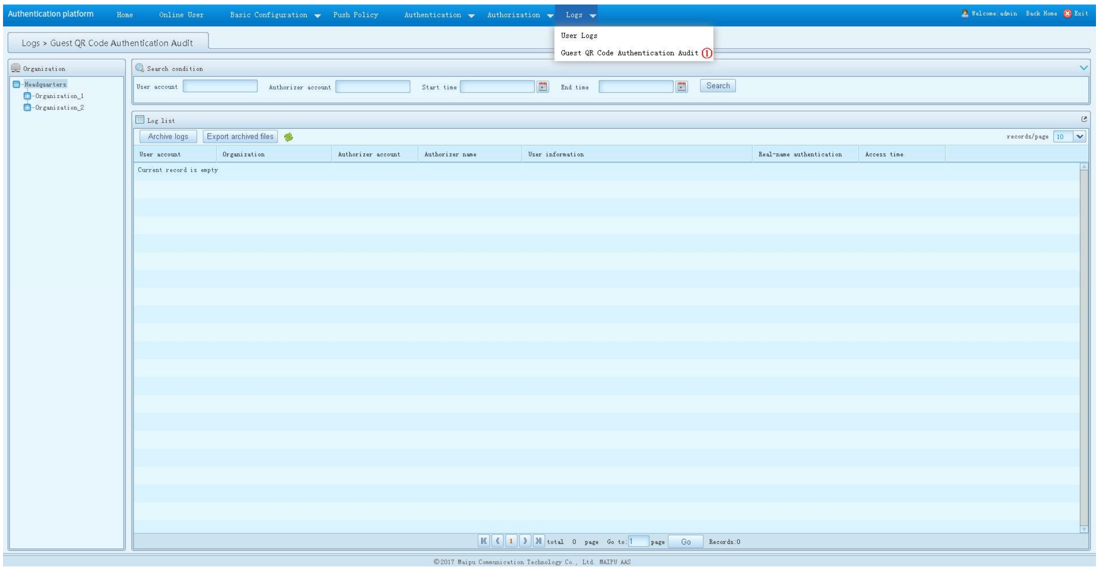
- The meaning of the error code 2051 in the user log:

  Unknown error

  1. Check whether the configured pre-share keys of the device and authentication server are consistent
  2. Check whether to perform the LDAP/AD/Radius proxy authentication, and check whether the proxy configuration is correct
  3. :Check whether to perform the certificate authentication, and check whether the server certificate/trust certificate/user certificate configuration is correct
  4. Check whether the password is correct.

10.6.2 Guest QR Code Authentication Audit

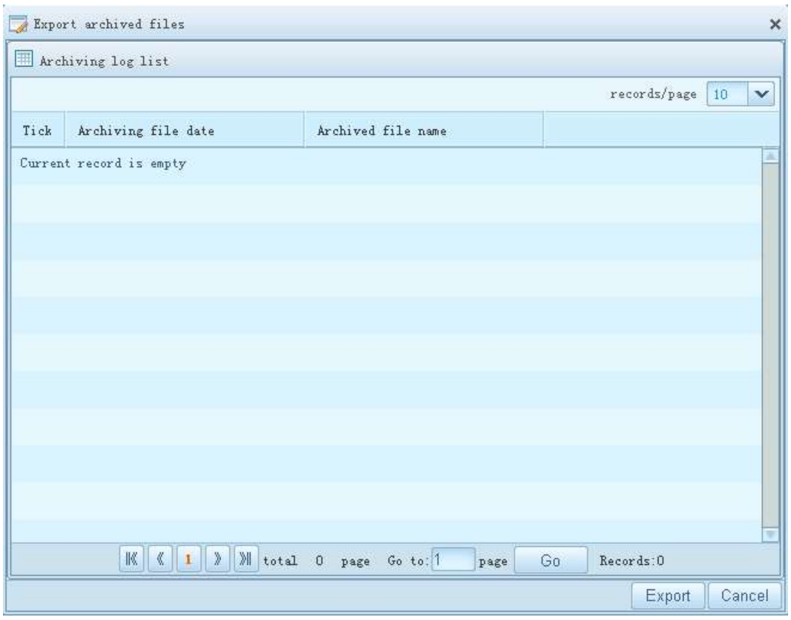
Record the log for the network access action of the guest via the “Authorization QR code” authentication mode. The module mainly provides the functions of archiving, exporting the archived files, and querying.



User account	Organization	Authorizer account	Authorizer name	User information	Real-name authentication	Access time
Current record is empty						

Figure 10-6-3 Audit the guest QR code authentication

Click the “**Archive logs**” button of the main interface, and you can archive the log. After archiving, click “**Export archived files**”, and you can download the archived logs, as shown in the following figure:



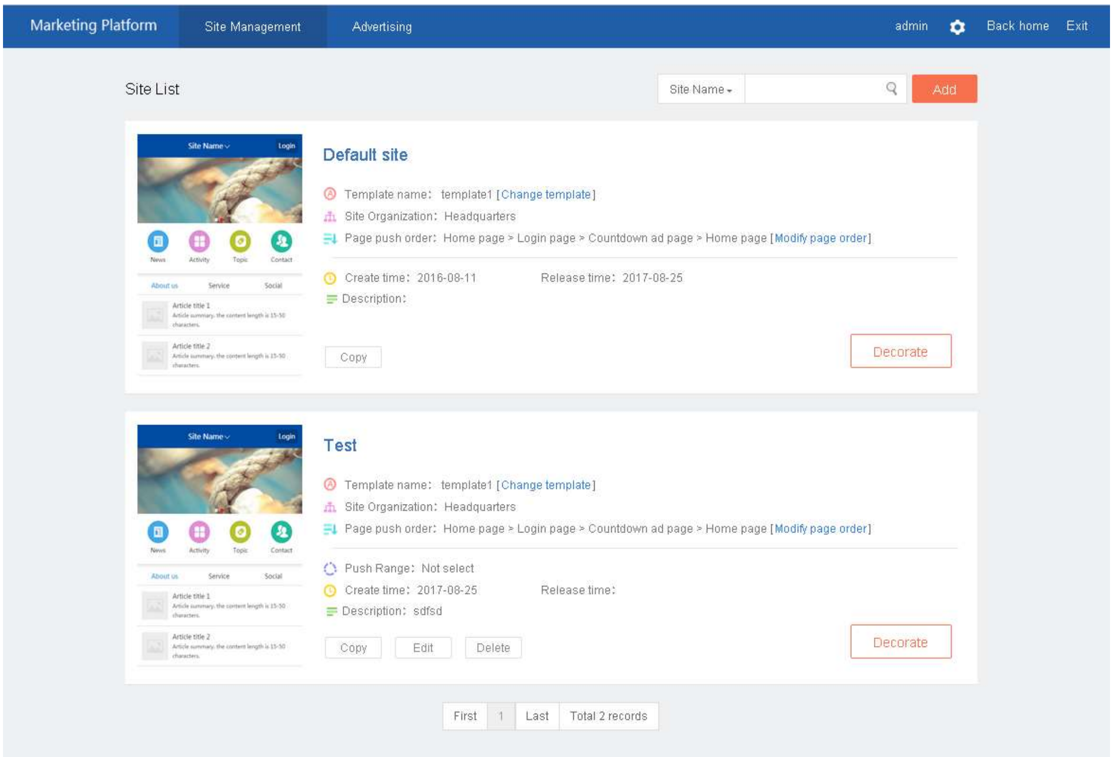
Tick	Archiving file date	Archived file name
Current record is empty		

Figure 10-6-4 Export the archived file

11 WiFi Marketing System

11.1 Site Decoration

The site decoration contains the functions of adding one site, copying the site, modifying the basic information of the site, deleting the site, querying the site, and decorating the site page. After logging into the system, click **Site Management**, and you can see the site list interface. The system has one default site, which can be modified and maintained, but cannot be deleted. Click **Add** to display the **New Site** interface, and you can input the site name and push range. For the existing site, you can copy, edit or delete.



Default site

Template name: template1 [Change template]
Site Organization: Headquarters
Page push order: Home page > Login page > Countdown ad page > Home page [Modify page order]
Create time: 2016-08-11 Release time: 2017-08-25
Description:

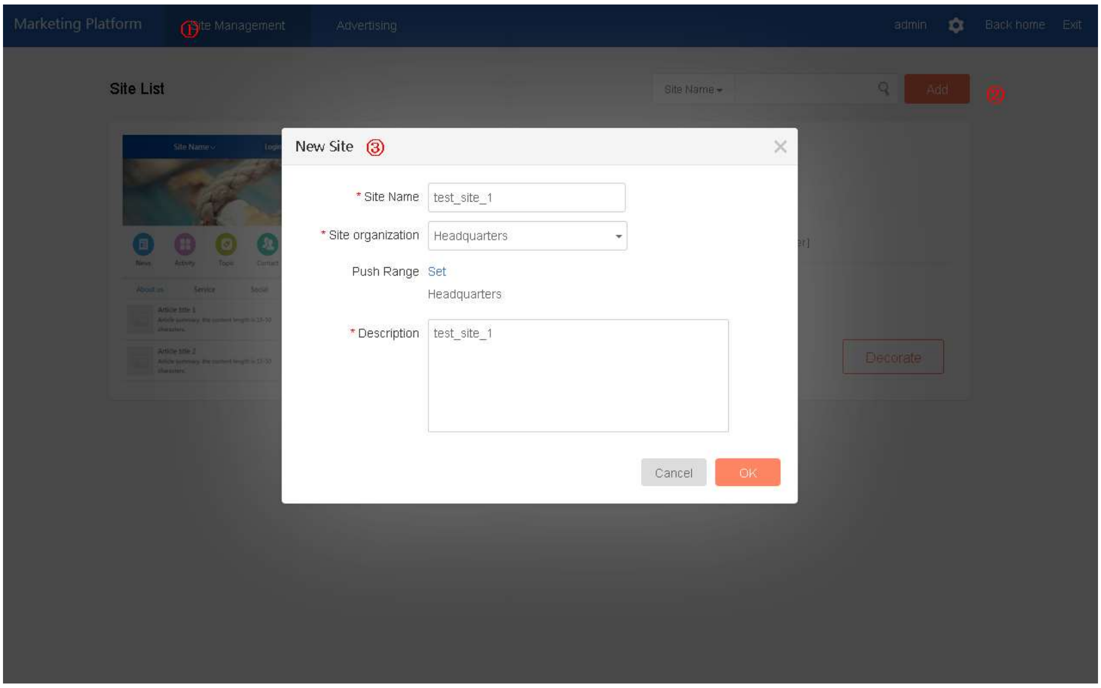
Test

Template name: template1 [Change template]
Site Organization: Headquarters
Page push order: Home page > Login page > Countdown ad page > Home page [Modify page order]
Push Range: Not select
Create time: 2017-08-25 Release time:
Description: sdfsd

Total 2 records

Figure 11-1-1Site management home

All Rights Reserved



New Site

* Site Name: test_site_1

* Site organization: Headquarters

Push Range: Set

Headquarters

* Description: test_site_1

Figure 11-1-2 Add one site

With the function of copying the site, you can copy the configuration data of the existing templates except for the advertising place to the new site.

The system supports the user to select the appropriate site template according to the service demand. The current supported templates only contain template1.

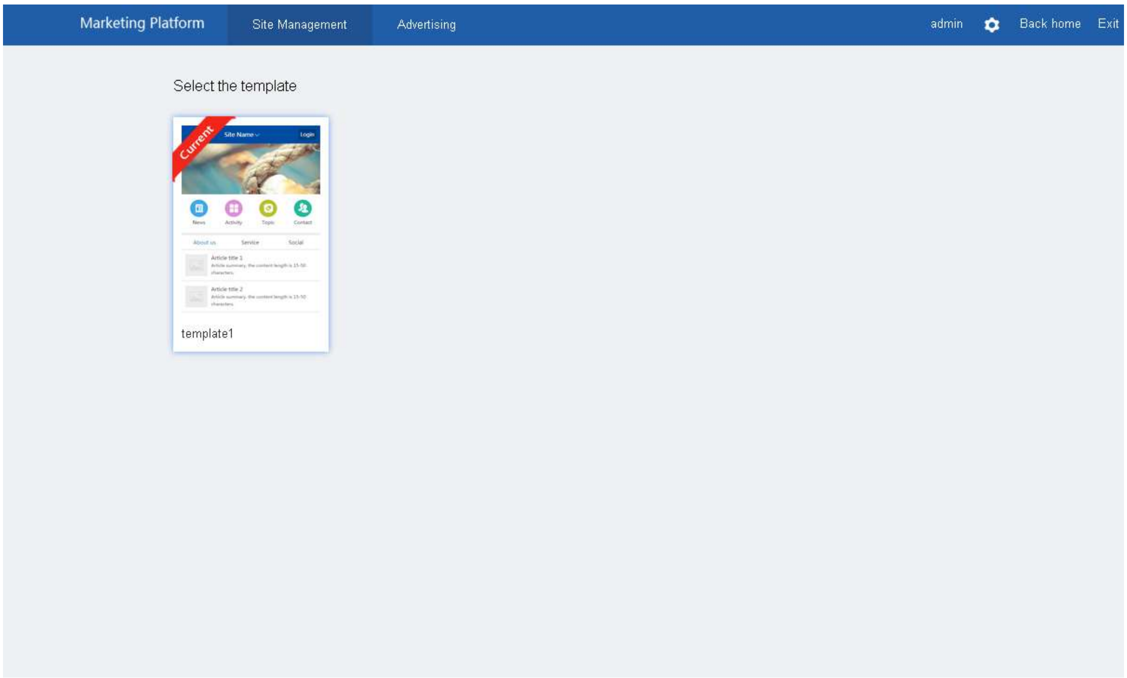


Figure 11-1-3 Select the template for the site decoration

After selecting the template, directly enter the site decoration interface. For the issued sites, you can modify the page order in the corresponding site module of the site list.

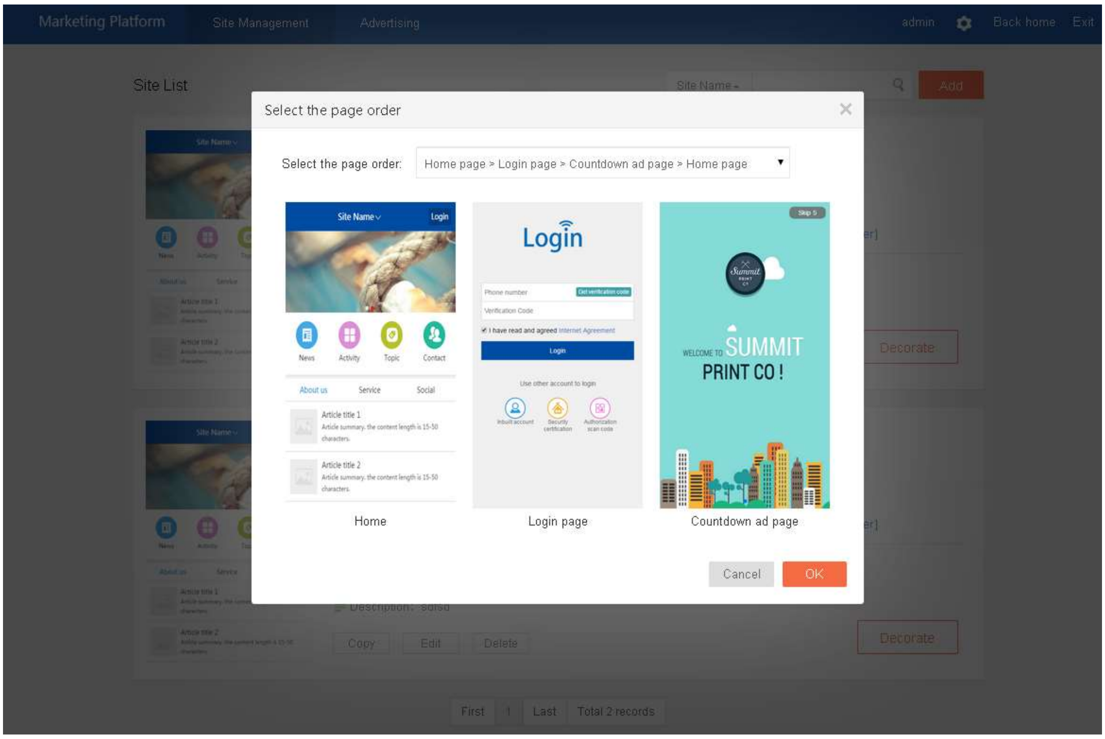

Select the page order: Home page > Login page > Countdown ad page > Home page

Figure 11-1-4 Select the order of the site decoration pages

After selecting the template, enter the site decoration page. The “Page” navigation at the left of the site decoration interface is all page directory of the current site. Under the directory, there are all components of the current page. In the middle of the page, there is a mobile phone preview box, displaying the preview effect of the current decoration page. The preview effect image is the same as the final page effect seen on the mobile phone. The right of the interface is the edit interface of the current component. Click one component in the preview image or click one component in the left directory and switch to the edit interface of the component. Click **Save** of the right component to save the data and refresh the content displayed in the phone preview box.

In red box ①, select the desired interface.

In red box ②, select the desired component.

In red box ③, display the preview effect after configuring the component.

After enabling the button in red box ④, the corresponding components can be displayed on the site interface.

Red box ⑤ is used to configure the selected component at the left.

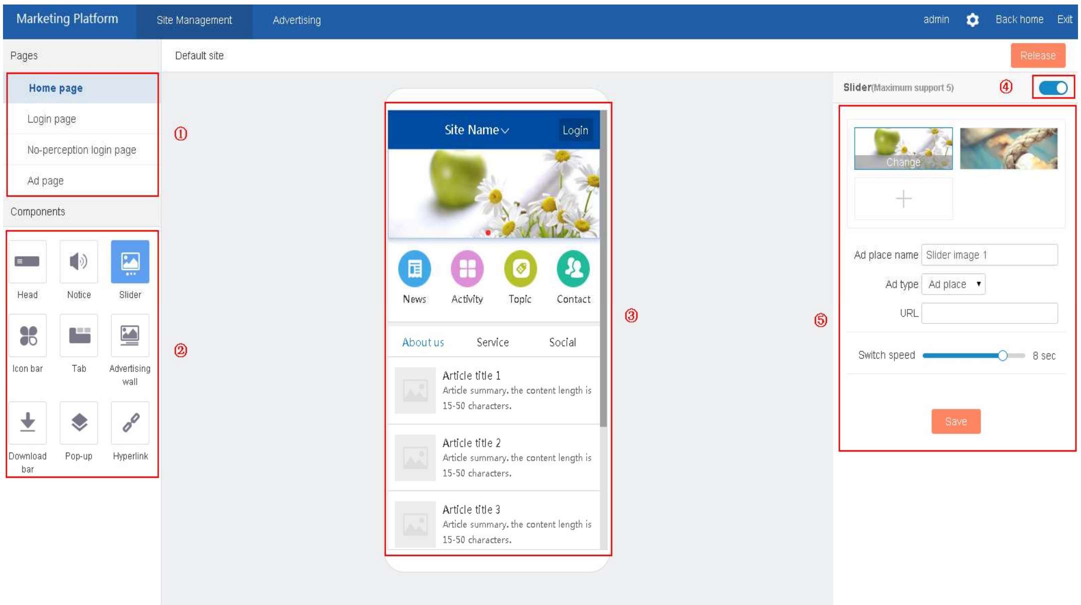
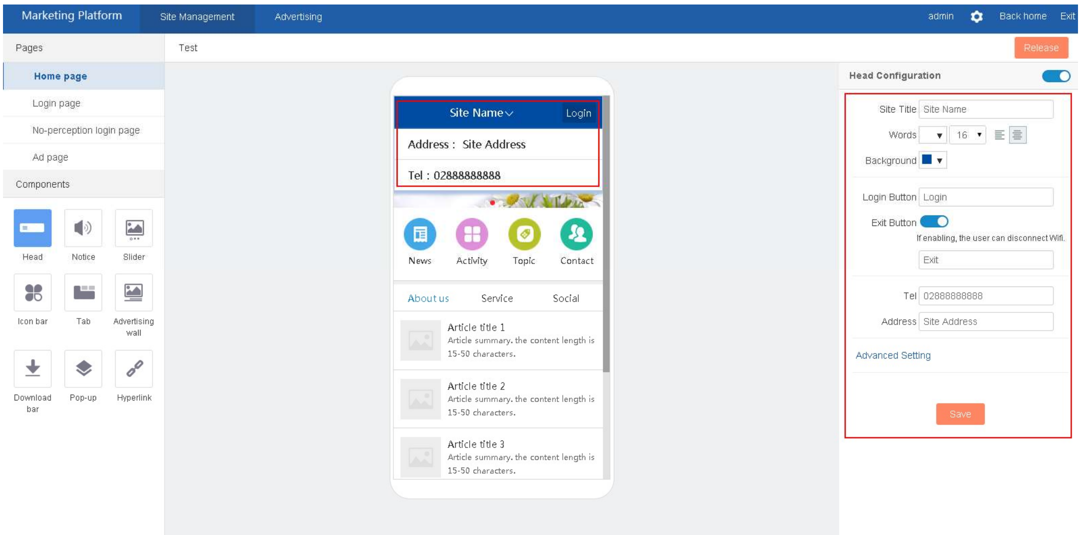


Figure 11-1-5 The deployment of the site decoration interface

The template includes the home page, authentication page, no-perception authentication page, and the advertisement page.

Click **Home** page to display the preview image of the current home page. The home page includes Head, Notice, Slider, Icon bar, Tab, Advertising wall, Downloads bar, Pop-up, and Hyperlink components. Click the component name, or click the component on the preview image, and the right panel displays the configuration interface of the current component. On the component configuration interface of the right panel, click Save to save the data configuration of the current component to the database. When entering the interface next time, display the saved configuration. After clicking **Release site**, the saved configuration information of the database takes effect on the interface pushed to the mobile phone. On the preview image, click the **Move up** or **Move down** button on the component, and you can sort the component locations. After clicking the **Move up** or **Move down** button, automatically save to the database, but do not need to click **Save** at the right panel. The following describes the configurations of the components respectively.

Head: The head component mainly displays the site name, phone number, address, and network access button. At the right configuration interface, you can configure the site name, phone number, address information, and word and button style. On the interface pushed to the phone, click the drop-down button at the right of the site title, and you can see the configured phone number, address information and so on.



Address : Site Address

Tel : 02888888888

Site Title: Site Name

Words: 16

Login Button: Login

Exit Button

If enabling, the user can disconnect Wifi.

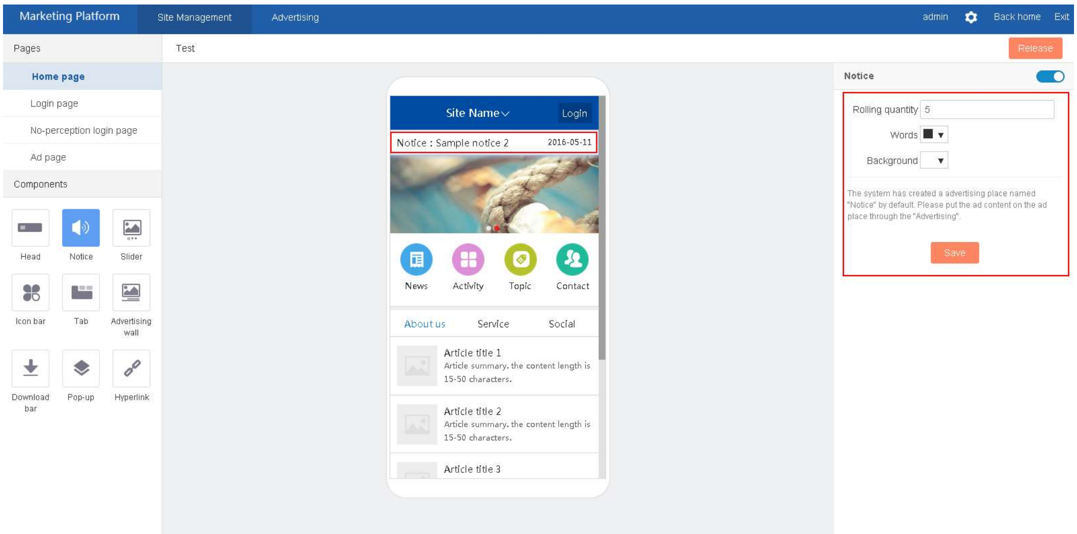
Exit

Tel: 02888888888

Address: Site Address

Figure 11-1-6 Template head decoration

Notice: By default, the Notice component is disabled. When it is necessary to use the component, you can enable the component via the button of the right configuration interface. After enabling the notice component, you can select the advertising place as notice, advertising the notice content. The notice style supports the individualized configuration. You can configure the notice word color, background color, and so on. The rolling quantity of the notice supports 1-10.



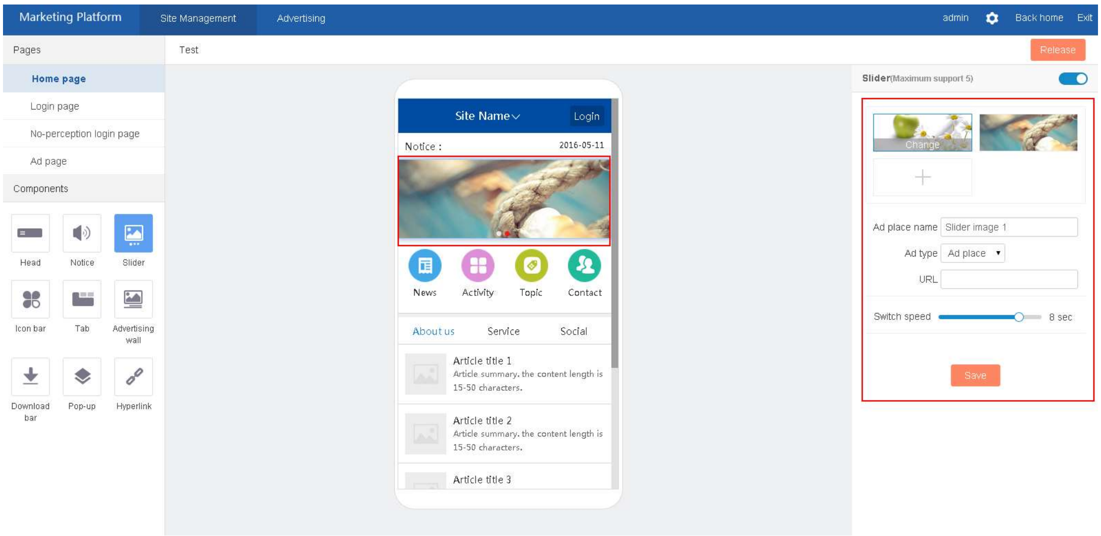
Notice : Sample notice 2 2016-05-11

Rolling quantity: 5

The system has created a advertising place named "Notice" by default. Please put the ad content on the ad place through the "Advertising".

Figure 11-1-7Template notice decoration

Slider: Slider is the image advertisement displayed by the site home slider, supporting enabling and disabling the advertisement. You can add five image advertisements at most. The advertisement type can be advertisement place or fixed advertisement. For the advertisement place, you can configure the name, used to add the advertisement in the advertising. For the fixed advertisement type, you can set the advertisement link, supporting the internal link and external link. The external link can be the customized link address. After selecting the internal link, you need to click “Select article” to display the interface of selecting the article, and then, select the desired advertisement.



Ad place name: Slider image 1

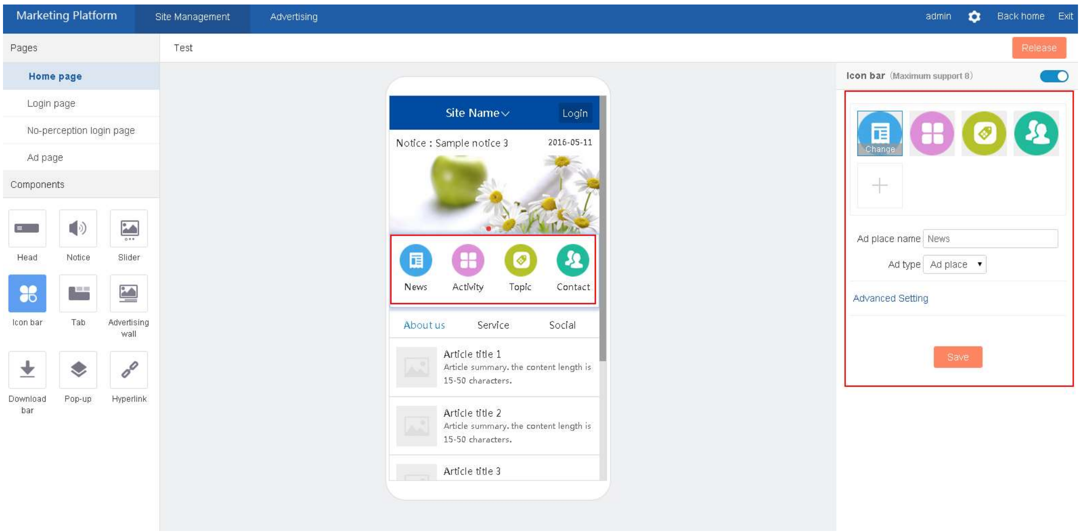
Ad type: Ad place

URL

Switch speed: 8 sec

Figure 11-1-8 Template slider decoration

Icon bar: Icon bar is also the advertising place, and it can be enabled and disabled. You can set the advertisement type and name, the same as the advertisement place in the slider.

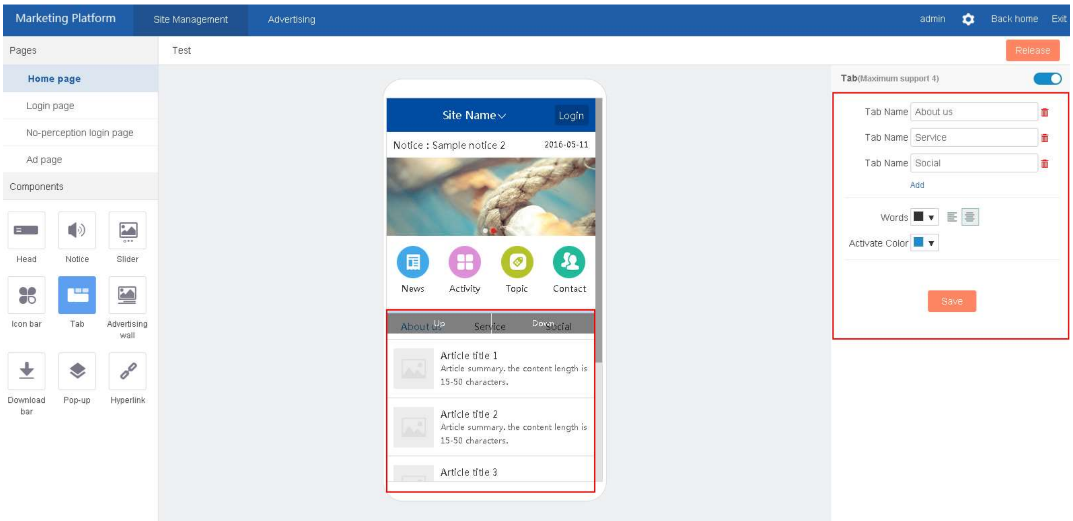


Ad place name: News

Ad type: Ad place

Figure 11-1-9 Template icon bar decoration

Tab: Tab is one switchable tab, supporting setting four tabs at most. After setting one tab, you can add the advertisement for each tab at the advertising. The component can be enabled and disabled..



Notice : Sample notice 2 2016-05-11

About us Service Social

Article title 1
Article summary. the content length is 15-50 characters.

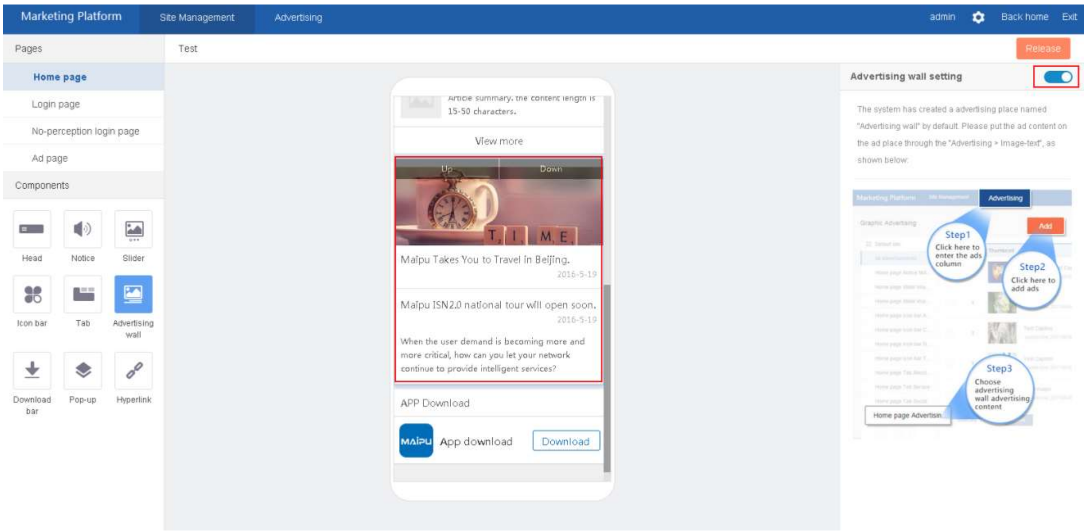
Article title 2
Article summary. the content length is 15-50 characters.

Article title 3

Tab Name: About us
Tab Name: Service
Tab Name: Social

Figure 11-1-10 Template tab decoration

Advertising wall: Advertising wall is to directly display the set advertisements, displaying the advertisement image, title and brief introduction by blocks. The component can be enabled and disabled. By default, it is disabled.



Article summary. the content length is 15-50 characters.

Maipu Takes You to Travel in Beijing. 2016-5-19

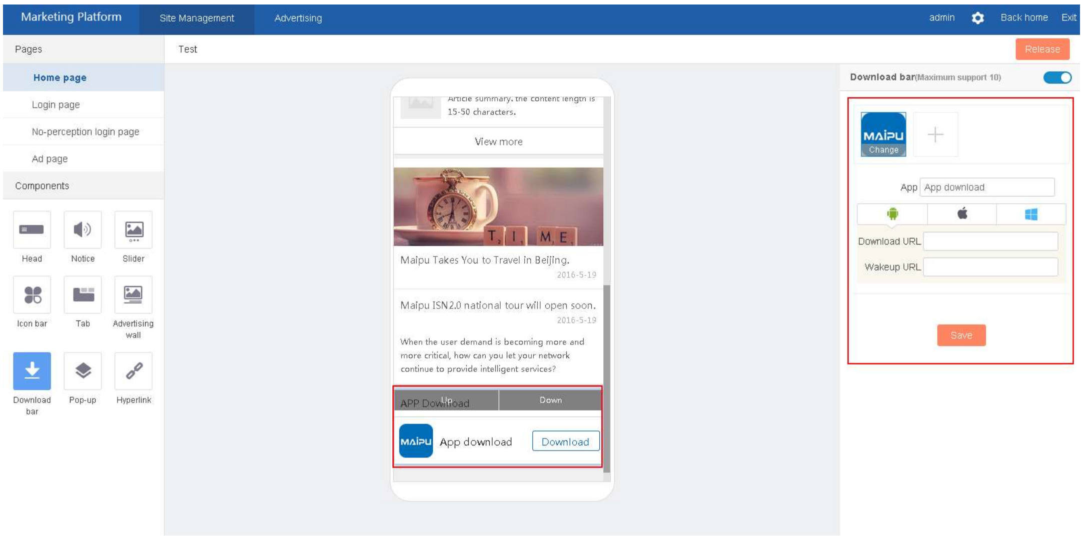
Maipu ISN2.0 national tour will open soon. 2016-5-19

When the user demand is becoming more and more critical, how can you let your network continue to provide intelligent services?

The system has created a advertising place named "Advertising wall" by default. Please put the ad content on the ad place through the "Advertising > Image-text", as shown below:

Figure 11-1-11 Template advertisement wall decoration

Downloads bar: Downloads bar provides the app download function for the site. The download bar supports downloading 10 applications at most. You can set the application name, application icon, and downloading mode for each application. The download mode supports downloading the applications of the Android system, IOS system and windows system. The component can be enabled and disabled.


Marketing Platform
Site Management
Advertising
admin
Back home
Exit
Pages
Test
Release
Home page
Login page
No-perception login page
Ad page
Components
Head
Notice
Slider
Icon bar
Tab
Advertising wall
Download bar
Pop-up
Hyperlink
Article summary, the content length is 15-50 characters.
View more
Maipu Takes You to Travel in Beijing.
2016-5-19
Maipu ISN2.0 national tour will open soon.
2016-5-19
When the user demand is becoming more and more critical, how can you let your network continue to provide intelligent services?
APP Download
Up
Down
App download
Download
Download bar(Maximum support 10)
MAIPU
Change
Save

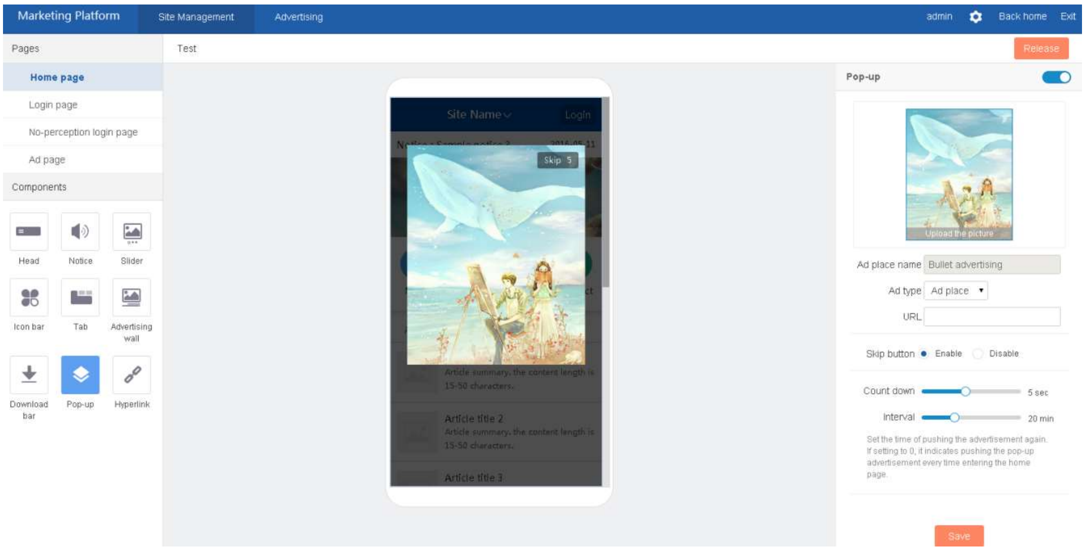
App: App download

Download URL:

Wakeup URL:

Figure 11-1-12 Template download bar decoration

Pop-up: Pop-up is one advertising place, and can be enabled and disabled. The pop-up interface can display the countdown and skip button at the same time. The “Skip” button can be disabled. The Pop-up can control the enable policy of the pop-up by configuring “Interval”.



Ad place name: Bullet advertising

Ad type: Ad place

URL:

Skip button: ● Enable ○ Disable

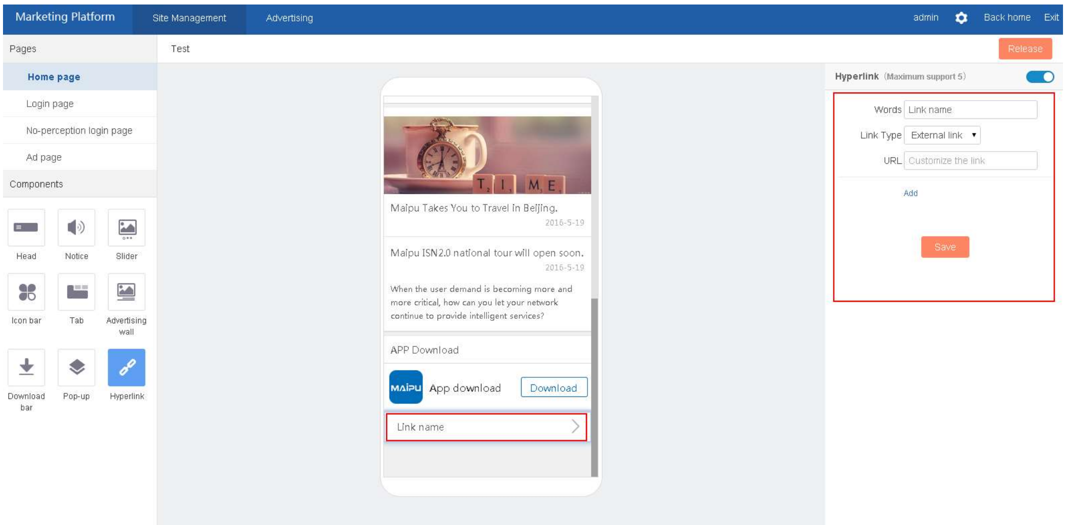
Count down: 5 sec

Interval: 20 min

Set the time of pushing the advertisement again. If setting to 0, it indicates pushing the pop-up advertisement every time entering the home page.

Figure 11-1-13 Template pop-up

Hyperlink: Hyperlink is disabled by default. After enabling the component, you can configure the Hyperlink name, link type, link address and so on at the right configuration area.



Maipu Takes You to Travel in Beijing. 2016-5-19

Maipu ISN2.0 national tour will open soon. 2016-5-19

When the user demand is becoming more and more critical, how can you let your network continue to provide intelligent services?

Words: Link name

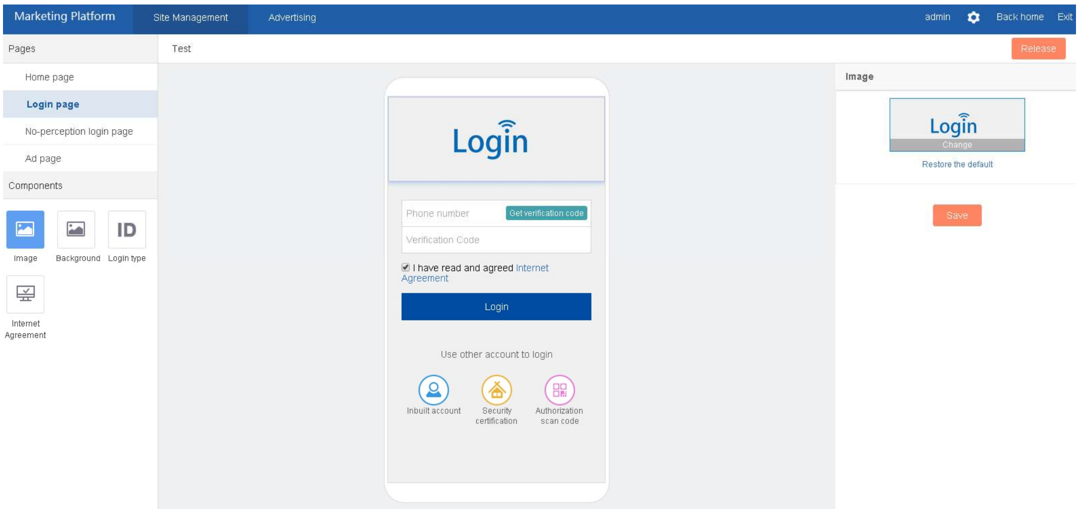
Link Type: External link

URL: Customize the link

Figure 11-1-14 Template Hyperlink

Click Login page to enter the decoration of the login page. The login page totally includes Image, Login type, Internet Agreement, and Background. The components of the login page cannot be sorted by moving up and down. The following describes the configuration of the components in the authentication page.

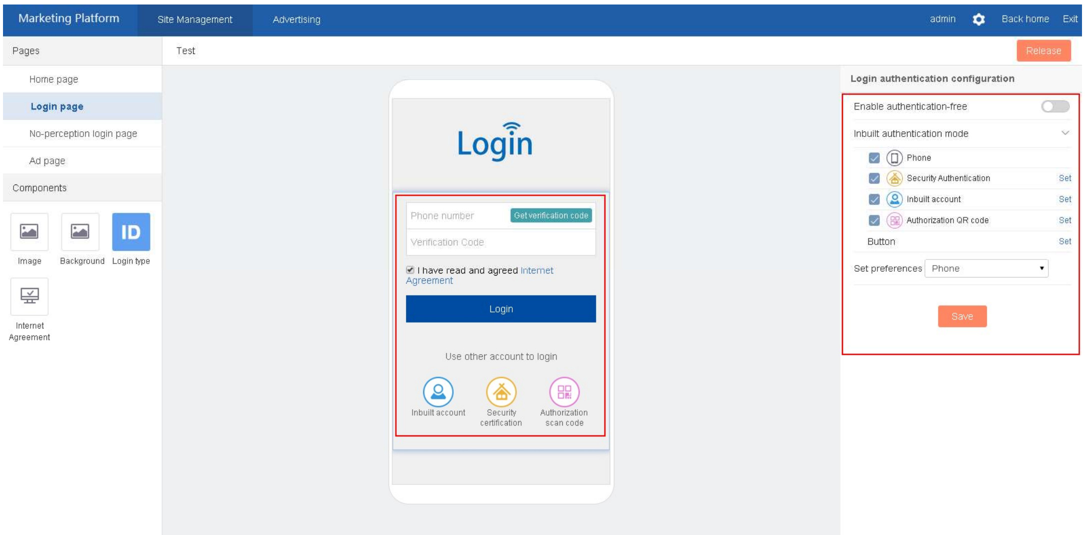
Image: Image is one image display at the head of the authentication page, supporting customizing the uploaded image.



☑ I have read and agreed Internet Agreement

Figure 11-1-15 Template image component

Login type: Login type is the most important configuration of the login page. The login authentication mode includes authentication-free, phone, inbuilt account, security login, and so on. On the login authentication page, you can set the preference, default login mode of the user, button word, color, background and so on.



Enable authentication-free ○

Inbuilt authentication mode

- ☑ Phone
- ☑ Security Authentication
- ☑ Inbuilt account
- ☑ Authorization QR code

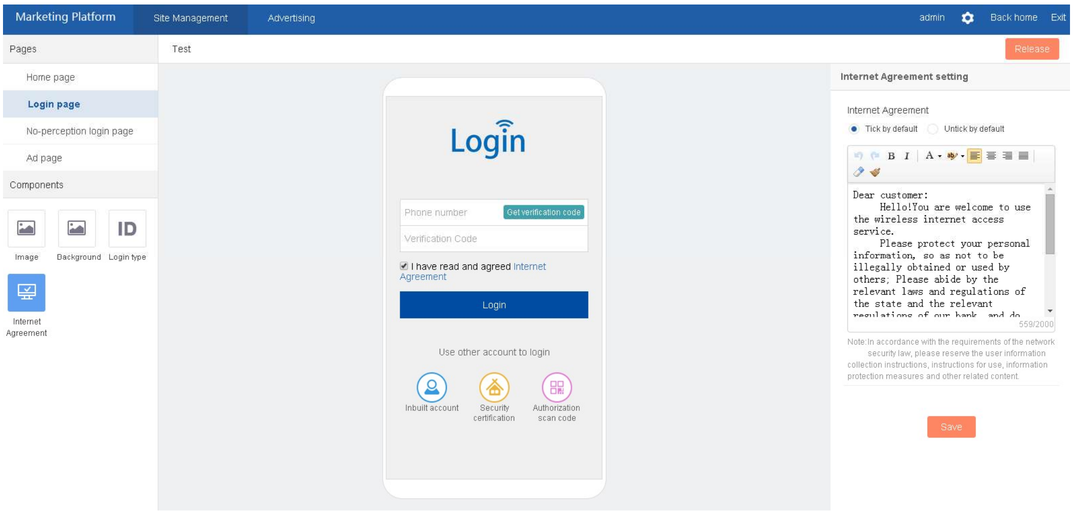
Button

Set preferences: Phone

Figure 11-1-16 Template login mode component

When enabling the authentication-free, the other authentication modes cannot be configured. After the terminal users ticks Internet agreement and clicking Authentication-free, directly pass the authentication. When not enabling authentication-free, you can tick the other authentication modes. For the phone authentication, the user inputs the phone number and click “Get verification code” to get one SMS verification code. The login authentication checks the input phone number and got verification code to authenticate. The inbuilt account authentication provides the user with the function of using the set inbuilt account and password in the portal system for authentication. The security login provides the security authentication login mode for the user. For details of the login authentication mode, refer to the section of Authentication Configuration.

Internet Agreement: Internet Agreement is to set the content displayed after the user clicks Internet Agreement. The agreement content can be edited in the text box.



Internet Agreement

● Tick by default ○ Untick by default

Dear customer:
Hello!You are welcome to use the wireless internet access service.
Please protect your personal information, so as not to be illegally obtained or used by others; Please abide by the relevant laws and regulations of the state and the relevant regulations of our bank, and do

Note:In accordance with the requirements of the network security law, please reserve the user information collection instructions, instructions for use, information protection measures and other related content.

Figure 11-1-17 Template Internet agreement

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved

Background: Set the bottom background image of the login page.

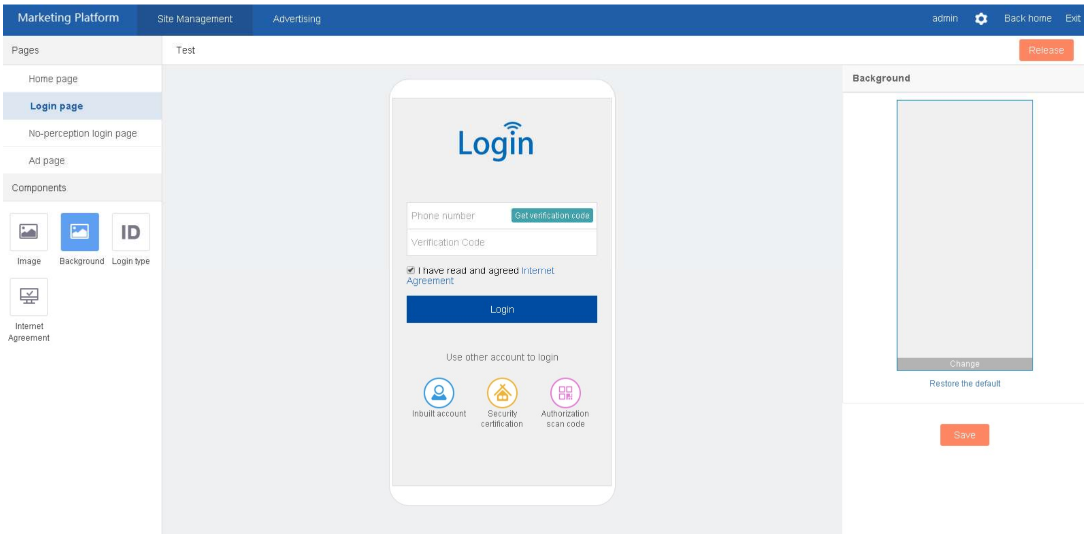


Figure 11-1-18 Template background image setting

Click No-perception login page at the left to enter the setting of the no-perception authentication page. The page has only one advertisement image and you can customize the advertisement image.

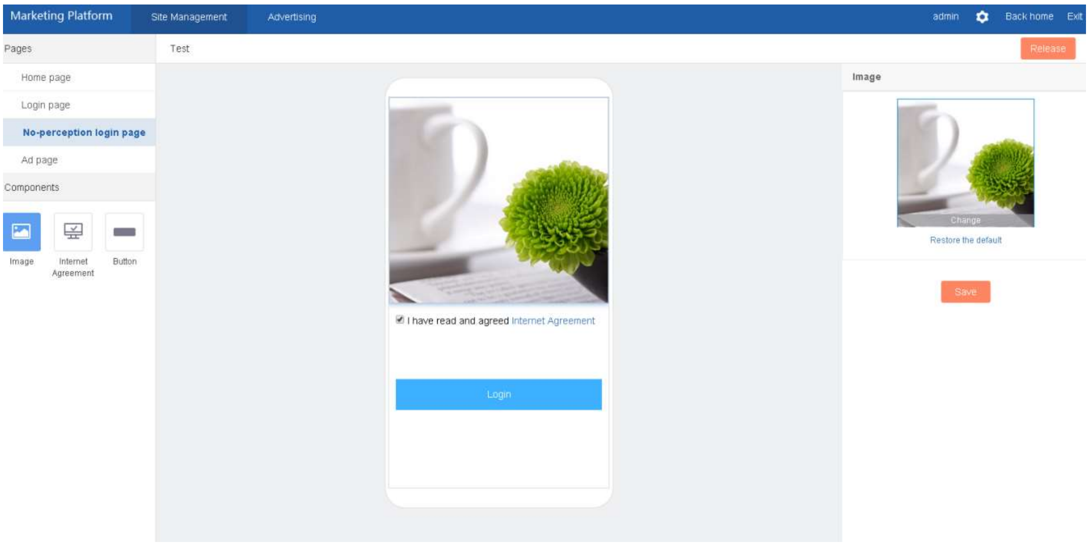
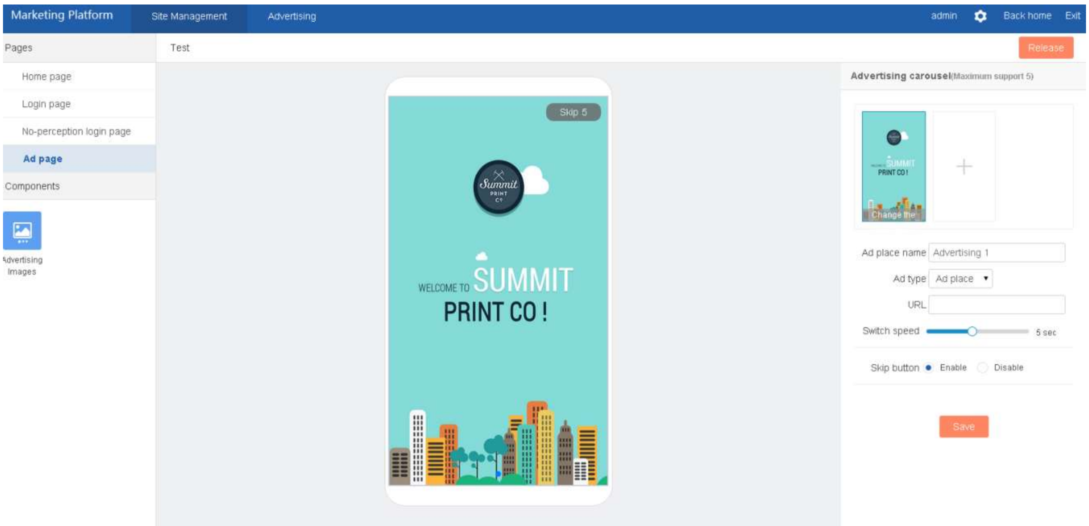


Figure 11-1-19 No-perception authentication page

Click **Ad page** at the left to enter the setting of the advertisement page. The page also have only one advertisement image component. The component can set the ad countdown time and whether to display the skip button setting. The image in the component is the image of the advertising place type, supporting five slider images at most. Each image can set the advertisement link.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved



Ad place name: Advertising 1

Ad type: Ad place

URL:

Switch speed: 5 sec

Skip button: ● Enable ○ Disable

Figure 11-1-20 Template countdown advertisement page setting

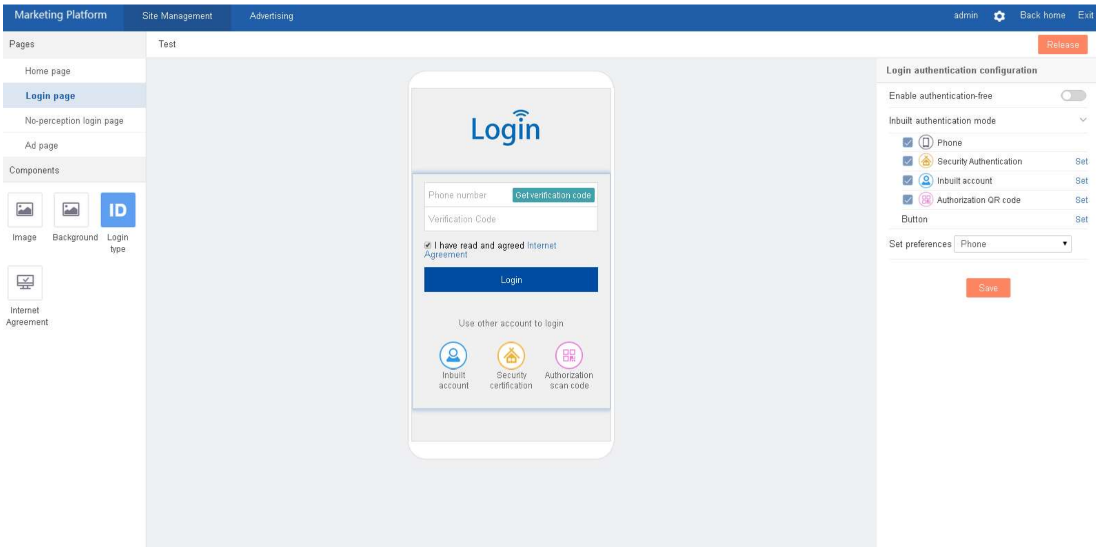
11.2 Authentication Configuration

11.2.1 SMS Authentication

SMS authentication is one common authentication mode. The basic steps are as follows:

Step 1: Configure the SMS authentication policy. For the details, refer to section 10.4.1.

Step 2: Enabling the authentication mode and setting the authentication content are both associated with the site, that is to say, you can customize different authentication modes for different sites. Enter the site decoration interface, and click Login page->Login type, as follows:



☑ Phone

☑ Security Authentication

☑ Inbuilt account

☑ Authorization QR code

Set preferences: Phone

Figure 11-2-1 Enable the SMS authentication function

To enable the SMS authentication, you just need to tick “Phone” authentication mode. After clicking **Save**, release.

After enabling the SMS authentication mode, you can set the SMS content, the length of the verification code, and the number of the sent SMS. For the setting details, refer to section 8.2.5.

Step 3: After setting the related content, connect the hotspot of the site, and click **Login** in the site page to enter the authentication page. Select the SMS authentication, input the phone number to get the verification code, and at last, input the verification code to authenticate, as follows:

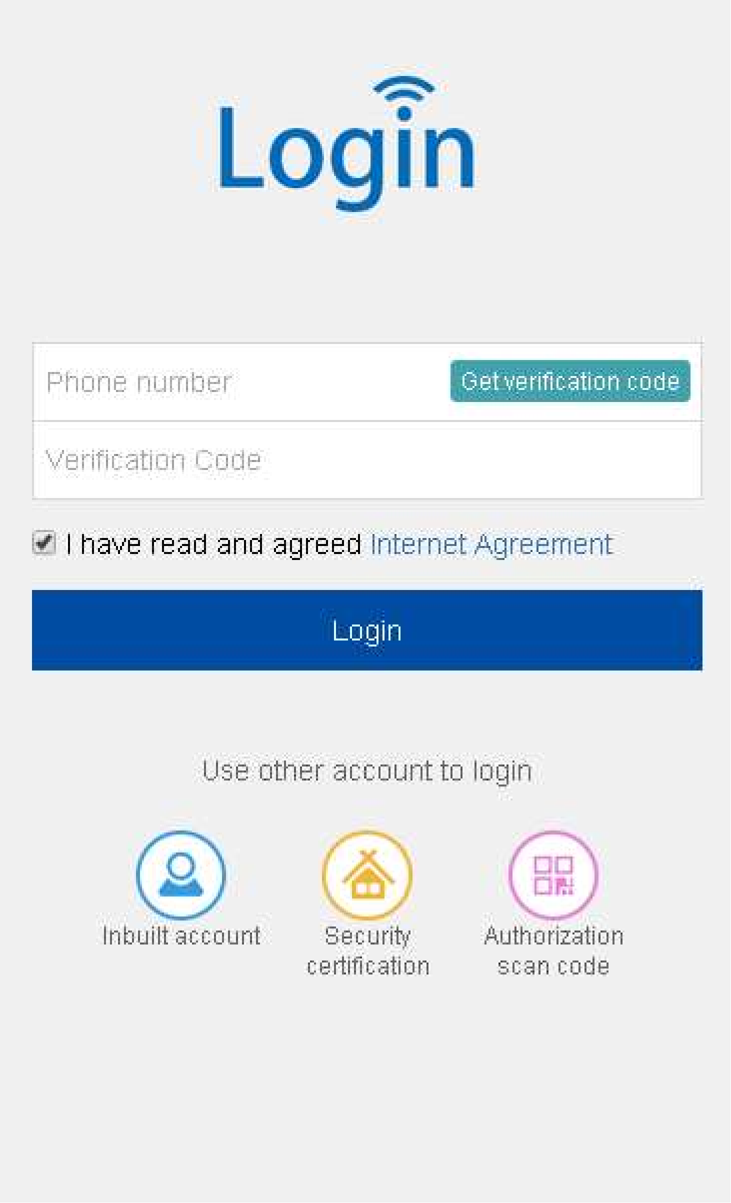


Figure 11-2-2 Main interface of the SMS authentication

On the interface, you can view the Internet agreement, and also can select other authentication mode. By default, it is the SMS authentication mode.

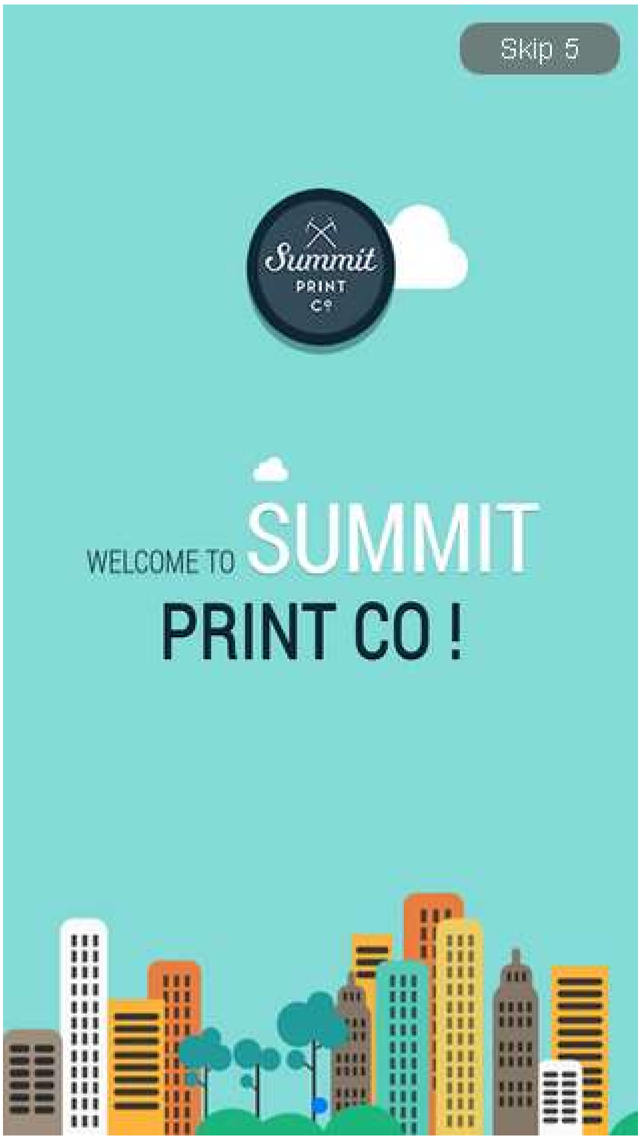


Figure 11-2-3 Enter the countdown page after authenticating successfully

The page order of the authentication process is consistent with the page order selected when creating the site. In the example, after authenticating successfully, enter the countdown page, return to the site home page after countdown ends, and the site home page displays the “Exit” button.

Step 4: After authenticating successfully, you can enter the authentication platform, and view the authentication account status, authentication result, and so on, as follows:

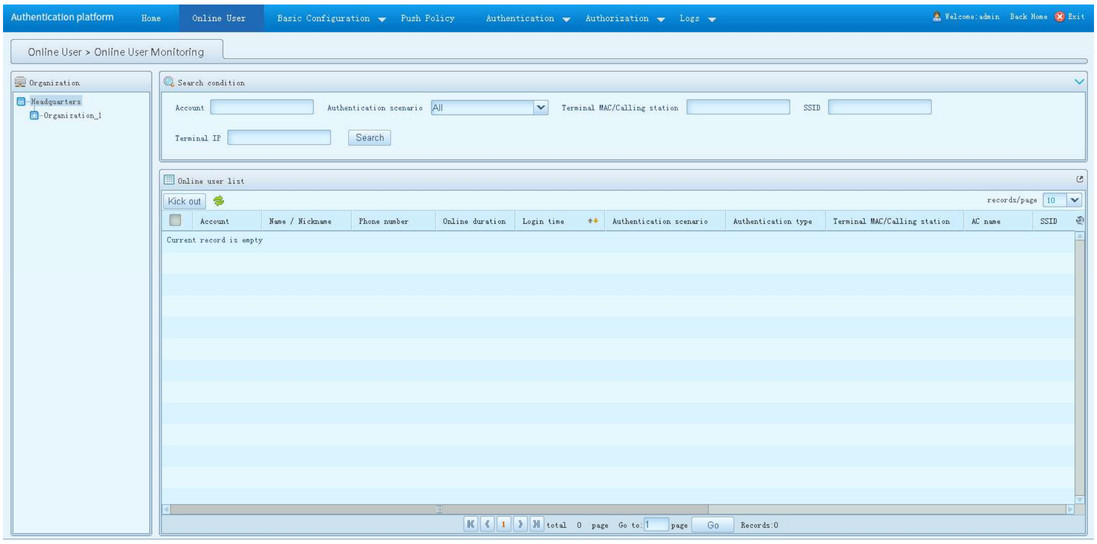


Figure 11-2-4 User logs

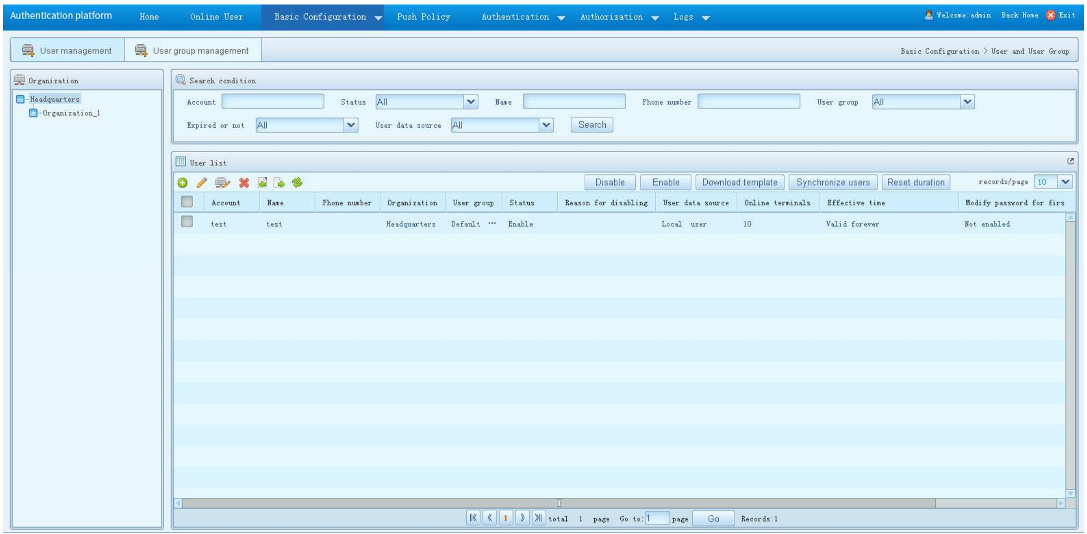
Step 5: After authenticating successfully, the terminal opens the browser to access the website, and view whether the network can be connected. The user already has the network access authority and the whole authentication process ends.

11.2.2 Inbuilt Account Authentication

The inbuilt account authentication is applicable to the internal staff of the merchant. The authentication mode is simple and the operation steps are as follows:

1. The user access system creates or imports the account and password.
2. The terminal user connects the hot spot and enters the authentication page.
3. Select the inbuilt account authentication, and input the user name and password.
4. Complete the authentication, and check the result.

Seeing from the above four steps, the biggest difference between the inbuilt account authentication and the other authentication modes is that it is necessary to create the account at the user access system before authenticating. The administrator logs into the authentication platform, and enters Basic Configuration->User and User Group, as follows:

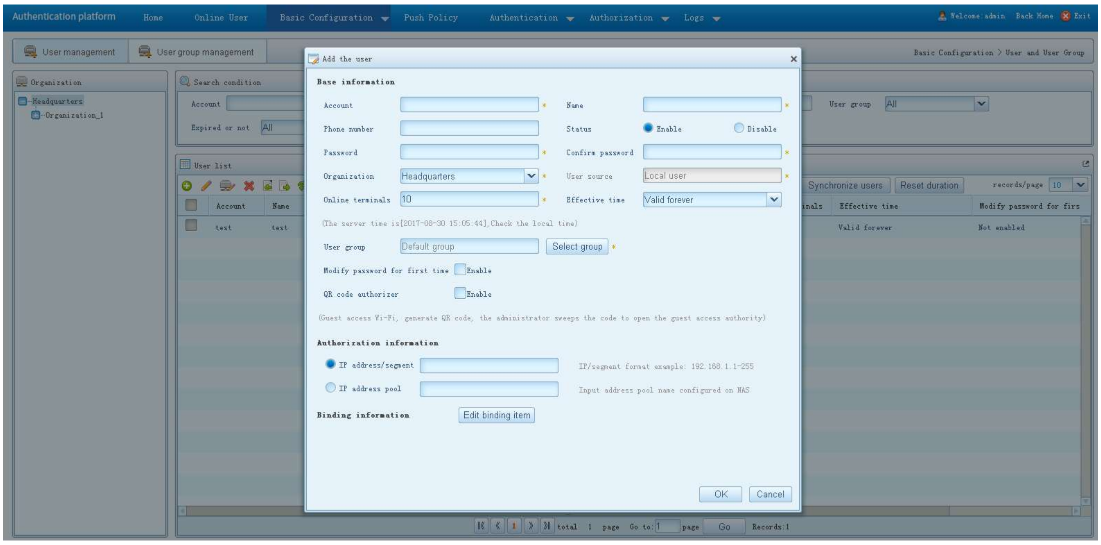


Status: All; User group: All; Expired or not: All; User data source: All; records/page: 10

☐	Account	Name	Phone number	Organization	User group	Status	Reason for disabling	User data source	Online terminals	Effective time	Modify password for firs
☐	test	test		Headquarters	Default ···	Enable		Local user	10	Valid forever	Not enabled

Figure 11-2-5 Inbuilt account list

When adding the inbuilt account, you can configure the inbuilt account as desired. Meanwhile, when adding the account, you also can list the using life of the account.



Account: *
Name: *
Phone number:
Status: ● Enable ○ Disable
Password: *
Confirm password: *
Organization: Headquarters *
User source: Local user *
Online terminals: 10 *
Effective time: Valid forever
(The server time is[2017-08-30 15:05:44],Check the local time)
User group: Default group *
Modify password for first time ☐ Enable
QR code authorizer ☐ Enable
(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)
● IP address/segment — IP/segment format example: 192.168.1.1-255
○ IP address pool — Input address pool name configured on NAS

Figure 11-2-6 Add the inbuilt account

After the inbuilt account is created successfully, input the account and password at the terminal to authenticate. The operation of viewing the log and online user information is the same as the previous authentication modes.

11.2.3 No-perception Authentication

If the network access time of the authenticated user exceeds the single network access time, it will get offline automatically. Here, the user needs to authenticate again. The re-authenticated used does not need to input the account and other information again to authenticate, but just needs to agree the Internet agreement so that it can continue to

copyright©2016Maipu Communication Technology Co., Ltd,
All Rights Reserved

access the network. The process is called no-perception authentication.

The no-perception authentication mainly depends on the configuration of the duration policy. For the configuration of the duration policy, refer to section 10.5.1.

The duration policy can configure the network access time of the terminal, mainly including daily network access duration, single network access duration, no-perception duration, and no-perception push configuration, and terminal quantity limit. Here, you can control the access duration of the SMS, authentication-free, and inbuilt account.

11.2.4 Authentication-free Mode

After enabling the authentication-free mode, all authentication modes will not be displayed in the authentication interface. The user can access the network after clicking **Agree** in the authentication interface. The operation is simple. Click **Site Management** > **Authentication Page** > **Login Mode**, and tick to enable the authentication-free.

The authentication-free mode is also bound with the site, that is to say, some sites in one system cannot enable, and some sites can enable. The site can customize whether to enable authentication-free.

The terminal user connects the hot spot. In the site homepage, click **I want to access Internet** to enter the login page.

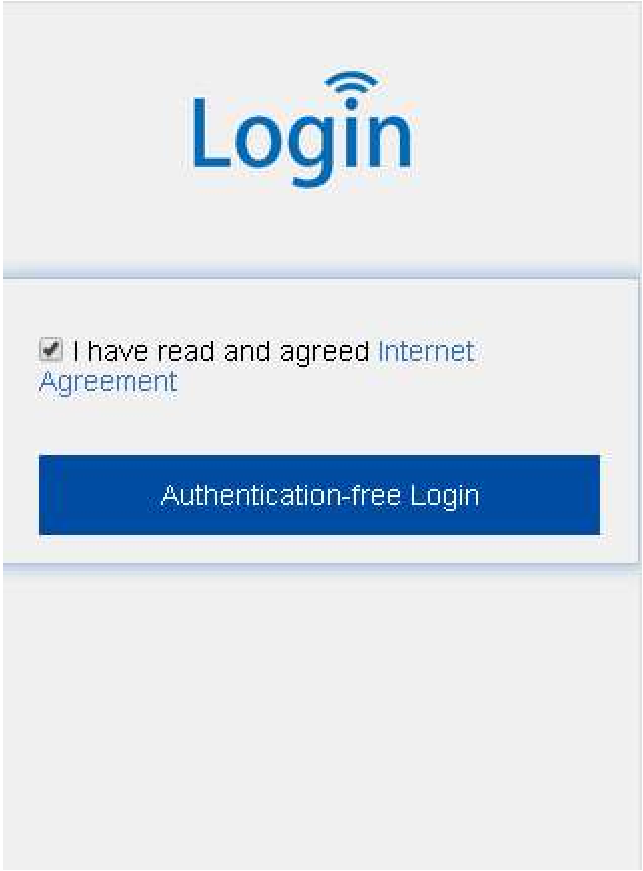

Login
☑ I have read and agreed Internet Agreement
Authentication-free Login

Figure 11-2-7 Authentication-free login page

After agreeing the Internet agreement, click **Authentication-free Login**, and you can pass the authentication to access the network.

In the authentication platform, you can view the online information of the authentication-free user, authentication log information, and so on. The query operation is the same as the user of the other authentication mode.

11.2.5 Security Authentication

The security authentication is one authentication mode of two authentications for the local user (including the LDAP user and local user), that is, if the security authentication is enabled, the user selects the security authentication mode at the login homepage pushed by the terminal, inputs the account and password of the local user, clicks **Login** to send the verification code to the preset phone number, and inputs the correct verification code so that the user can be authenticated successfully.

The steps of the security authentication:

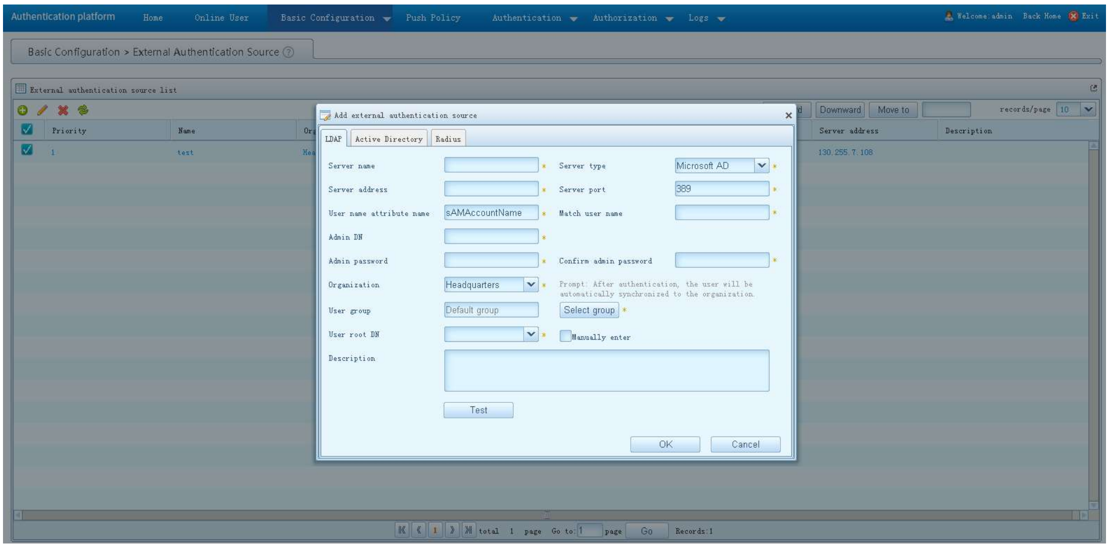
1. The user access system configures the external authentication source, and adds the local user (LDAP authentication source, inbuilt account).
2. In the site of the WIFI marketing system, open the login mode of the security authentication.
3. Connect the hot spot, enter the authentication page, select the security authentication, and input the account and password of the local user.
4. The preset phone number will receive the verification code. Input the verification code, and click **Login**.
5. Open the Internet connection to check if you can access the Internet.

Step 1: The administrator logs into the authentication platform, and adds the local user:

A: Enter **Basic Configuration**-> **External Authentication Source**, and add the LDAP external authentication source.

copyright©2016Maipu Communication Technology Co., Ltd,

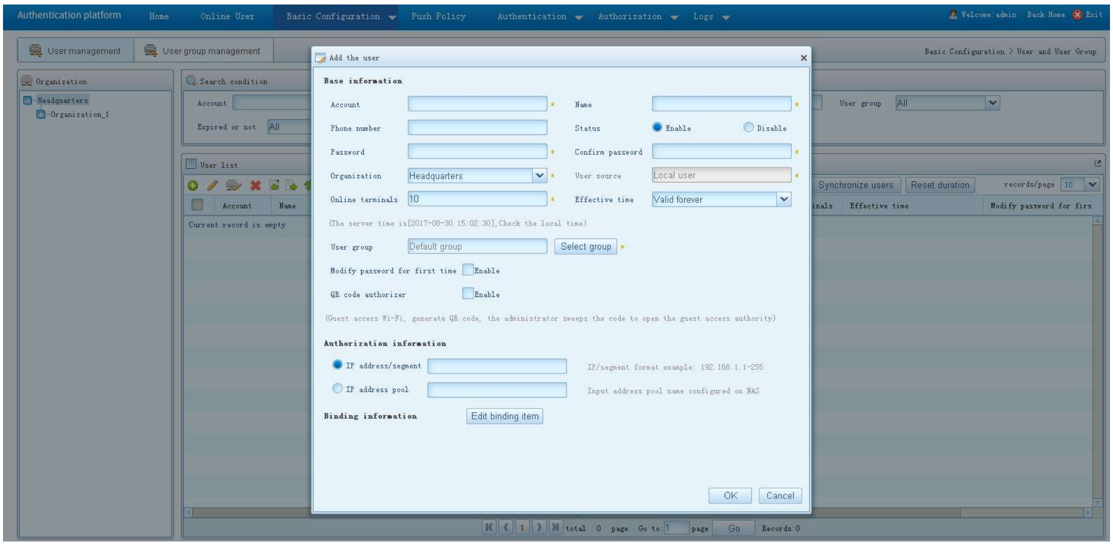
All Rights Reserved



Server name
Server type: Microsoft AD
Server address
Server port: 389
User name attribute name: sAMAccountName
Match user name
Admin DN
Admin password
Confirm admin password
Organization: Headquarters
Prompt: After authentication, the user will be automatically synchronized to the organization.
User group: Default group
User root DN
☐ Manually enter
Description

Figure 11-2-8 Add the LDAP external authentication source

B: Enter **Basic Configuration**->**User and User Group**, and add the inbuilt account.



Base information
Account
Name
Phone number
Status: ● Enable ○ Disable
Password
Confirm password
Organization: Headquarters
User source: Local user
Online terminals: 10
Effective time: Valid forever
(The server time is[2017-08-30 15:02:30],Check the local time)
User group: Default group
Modify password for first time ☐ Enable
QR code authorizer ☐ Enable
(Guest access Wi-Fi, generate QR code, the administrator sweeps the code to open the guest access authority)
Authorization information
● IP address/segment — IP/segment format example: 192.168.1.1-255
○ IP address pool — Input address pool name configured on NAS
Binding information

Figure 11-2-9 Add the inbuilt account

Step 2: If the added is LDAP authentication source, set the reserved phone number for the account that needs the security authentication.

Step 3: Enter the marketing platform, enter the site decoration page, and select **Security Authentication** in the login mode.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

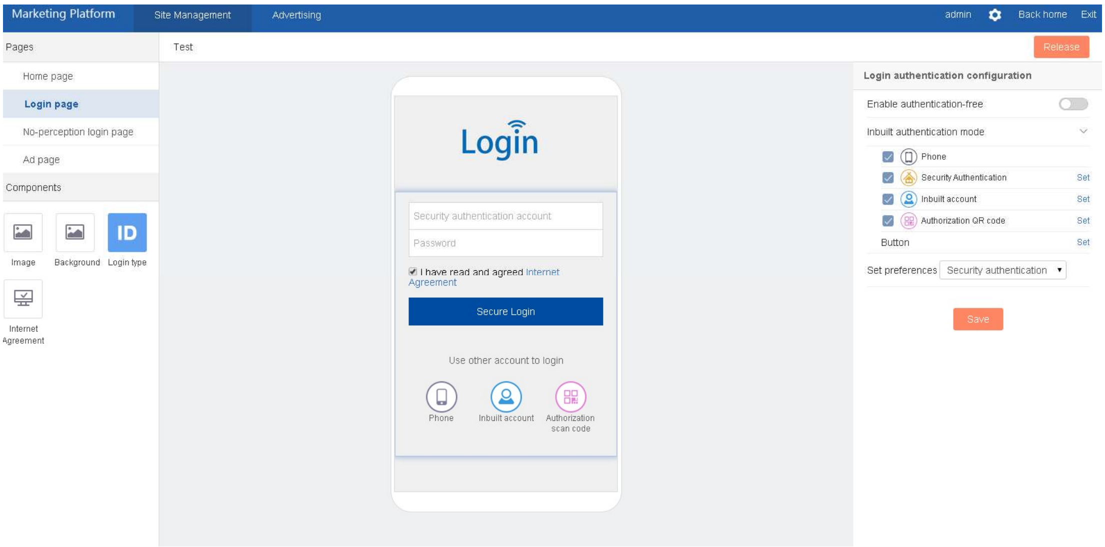


Figure 11-2-10 Security authentication configuration

Step 4: The phone connects the wifi hot spot. After pushing, select **Security certification**.

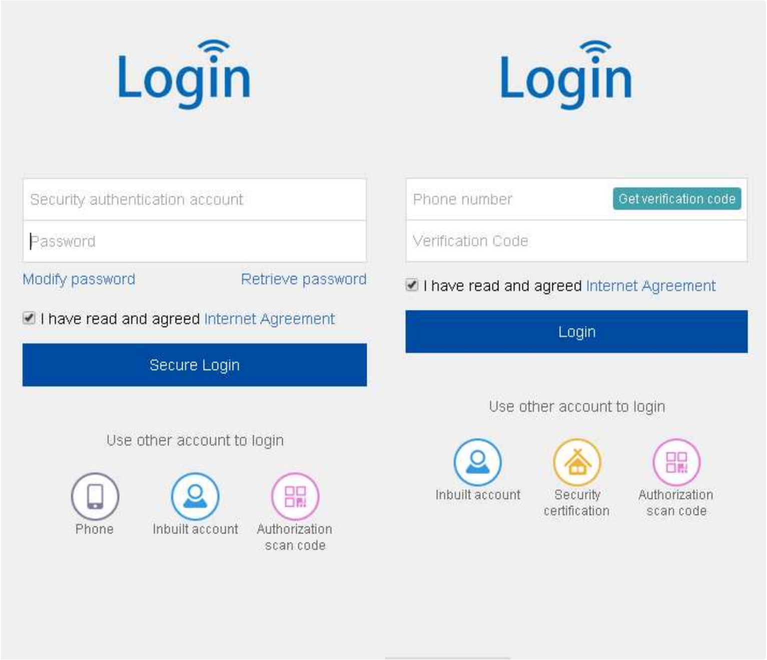


Figure 11-2-11 Security authentication

Step 5: Input the LDAP account and password, and click **Get verification code**.

After inputting the verification code, click Login, authenticate successfully, and then, jump to the advertisement page.

11.2.6 Authorization QR Code Authentication

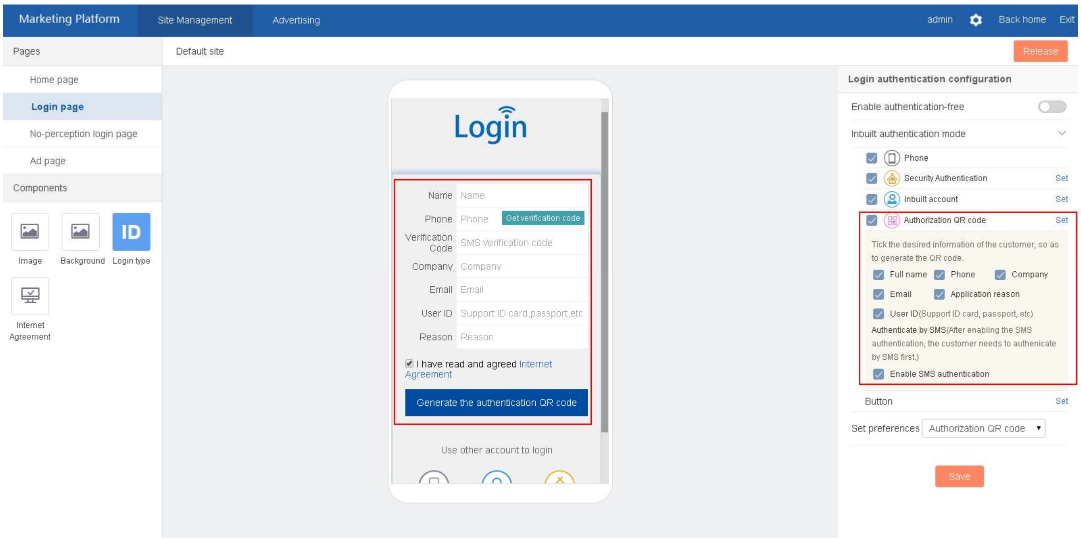
Authorization QR code authentication needs the visitor to fill in his own information, and

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

then, click to generate the QR code. At last, the authorizer scans the QR code to open the network.

On the site decoration page, you can configure the authorization QR code information. After enabling the SMS authentication, the authentication process adds the SMS authentication. After the verification code of the visitor is checked, you can get the authorization QR code. The configuration can refer to the following figure:



Enable authentication-free ○

Inbuilt authentication mode

☑ Phone

☑ Security Authentication

☑ Inbuilt account

☑ Authorization QR code

Tick the desired information of the customer, so as to generate the QR code.

☑ Full name ☑ Phone ☑ Company

☑ Email ☑ Application reason

☑ User ID(Support ID card, passport, etc)

Authenticate by SMS(After enabling the SMS authentication, the customer needs to authenicate by SMS first.)

☑ Enable SMS authentication

Set preferences: Authorization QR code

Figure 11-2-12 Authorization QR code authentication configuration

---

Caution

- Authorization QR code authentication needs to enable the guest QR code authorizer on the authentication platform.

11.3 Advertising

The advertising function mainly uses the corresponding control to realize better and more correct site advertising. For example, you can advertise the slider advertisement, tab advertisement, advertisement page, and other advertisement information. When advertising, you select according to the corresponding site. After the advertisement is delivered to the corresponding site, use the terminal device to connect the network. When pushing the site, you can view the delivered advertisements.

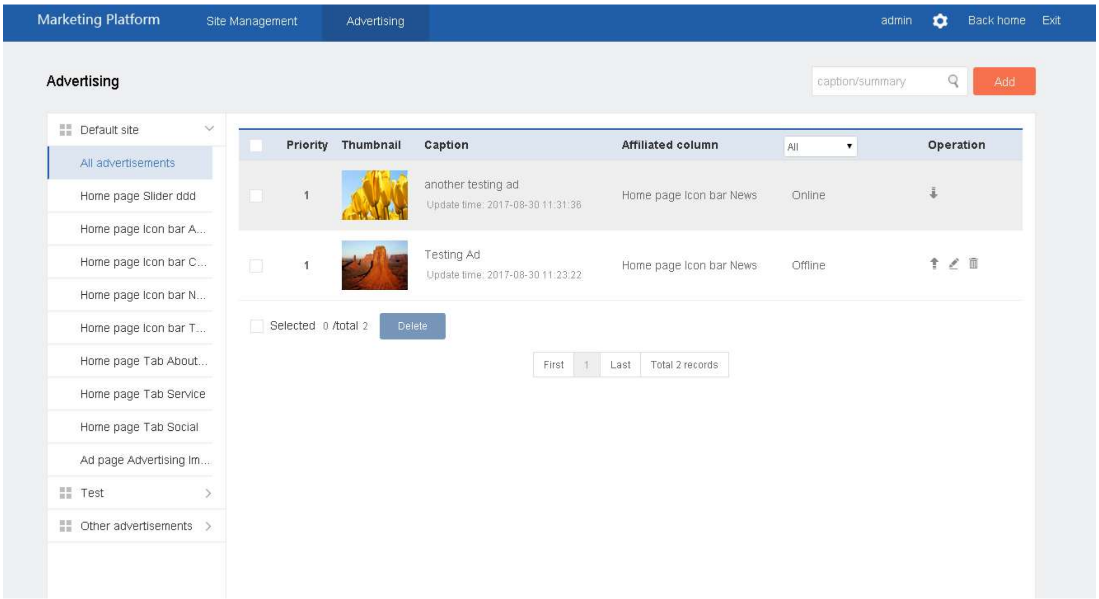
11.3.1 Advertisement List

The advertisement list is mainly used to display and manage the delivered advertisements.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

You can add, edit, get online, get offline, view, and delete the advertisement, query the advertisement by status, and query the advertisement by advertising place. First, enter the advertisement list module:



☐	Priority	Thumbnail	Caption	Affiliated column	All	Operation
☐	1		another testing ad Update time: 2017-08-30 11:31:36	Home page Icon bar News	Online	
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	

☐ Selected 0 /total 2

Total 2 records

Figure 11-3-1 Advertisement list

After logging into the platform, click **Advertising**, and you can enter the advertising module. On the advertising module page, display all delivered advertisements, and you can query the advertisements by pages.

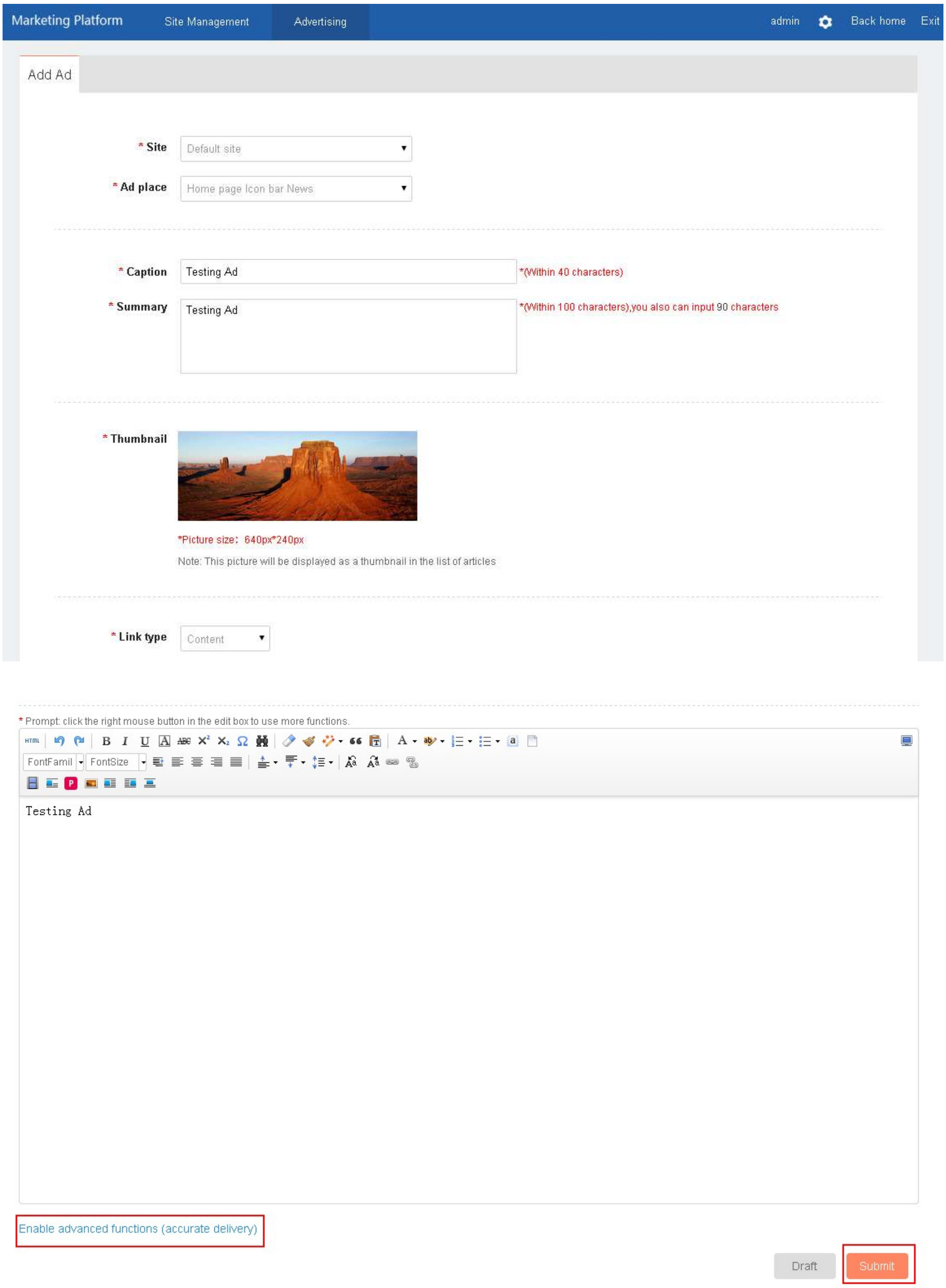
11.3.1.1 Add an Advertisement

The advertisement is delivered based on the site. Select the corresponding advertising place and you can advertise. Click the advertisement image, and you can open the material library to select the image.

Click **Enable advanced functions (accurate delivery)**, and you can enable the accurate delivery. After filling in the advertisement information, click **Submit**.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved



* Site: Default site

* Ad place: Home page Icon bar News

* Caption: Testing Ad *(Within 40 characters)

* Summary: Testing Ad *(Within 100 characters),you also can input 90 characters

* Thumbnail

*Picture size：640px*240px

Note: This picture will be displayed as a thumbnail in the list of articles

* Link type: Content

* Prompt: click the right mouse button in the edit box to use more functions.

Testing Ad

Enable advanced functions (accurate delivery)

Figure 11-3-2 Add the advertisement

1. Caption: The title content of the advertisement
2. Summary: The information displayed on the list page during advertising

Inject advertisement to the site: When injecting the advertisement, select the desired site, and the desired advertising place. When pushing the site, display the advertisement.

Inject the image and text to the advertisement: The injecting of this kind of advertisements takes effect for all sites, and the injected advertising place only has the bottom advertisement.

3. Image: The image of the injected advertisement; click the advertisement image to select the image from the material library.

Click **New group**, and you can create the material group and perform the classification management for the materials.

Click **Upload the material**, and you can upload the materials to the current group.

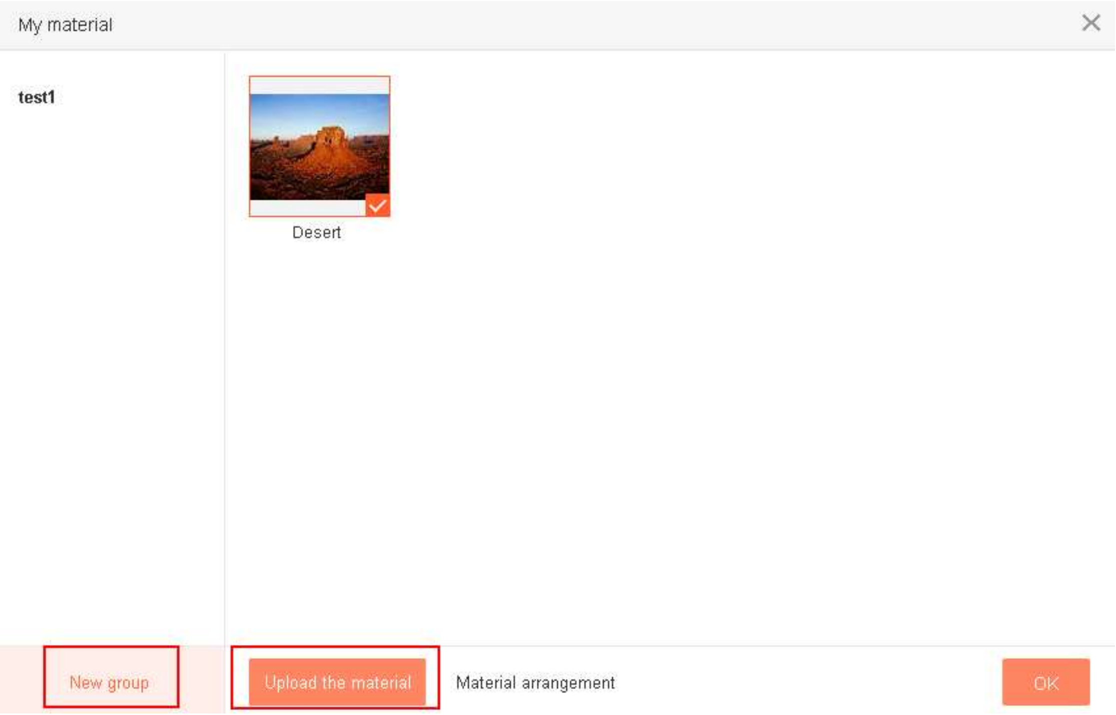


Figure 11-3-3 Image material library

1. Link type: Include **Content** and **External link**.

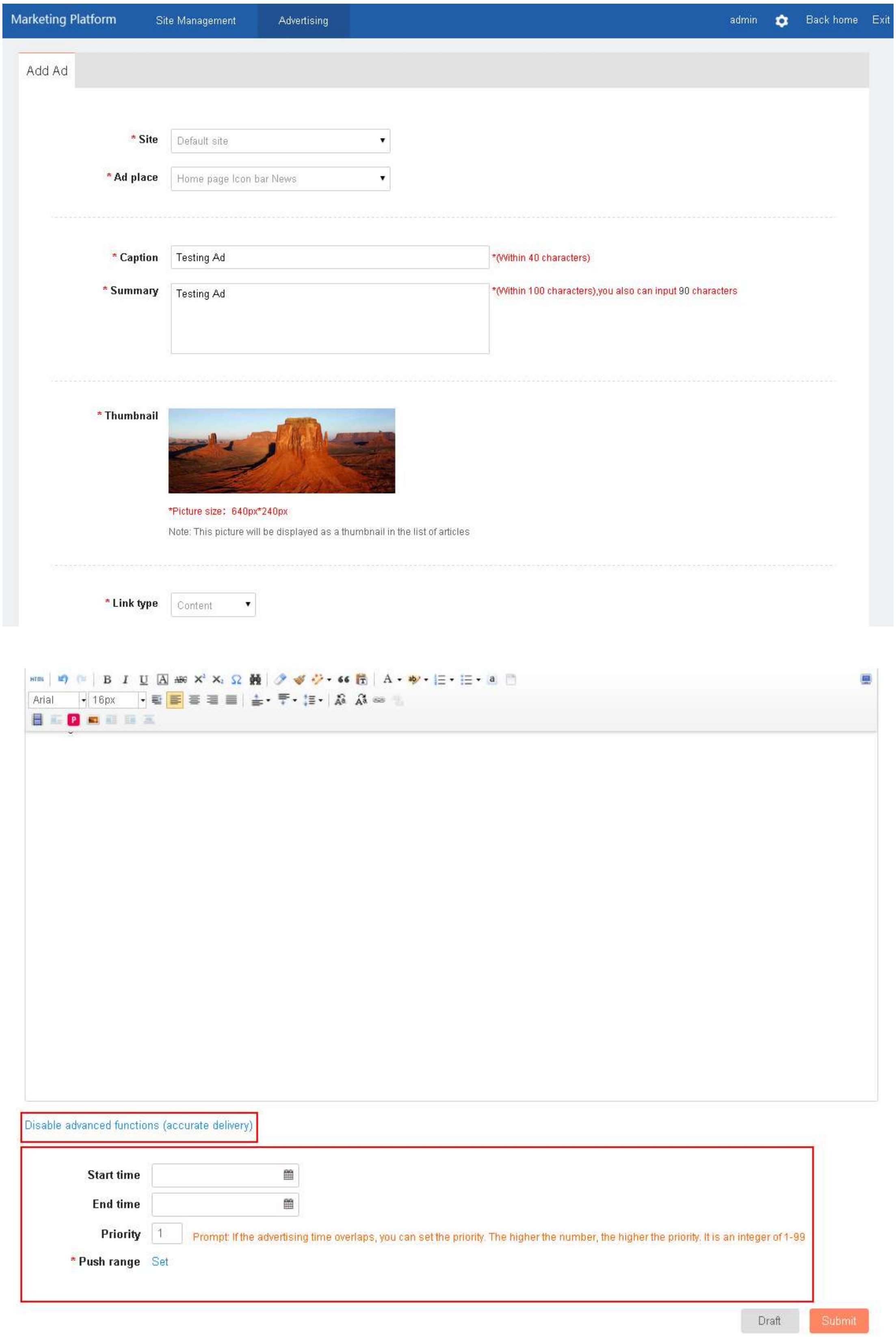
Content: The site advertisement, pushed by the administrator

External link: When it is necessary to configure the third-party advertisement link, you can select this type.

2. **Advertisement details**: When the link type is selected as **Content**, you can add additional advertising details

3. Enable advanced functions (accurate delivery)

Click **Disable advanced functions (accurate delivery)**, and you can open the advanced functions (accurate delivery).



* Site: Default site

* Ad place: Home page Icon bar News

* Caption: Testing Ad *(Within 40 characters)

* Summary: Testing Ad *(Within 100 characters),you also can input 90 characters

* Thumbnail

*Picture size：640px*240px

Note: This picture will be displayed as a thumbnail in the list of articles

* Link type: Content

Disable advanced functions (accurate delivery)

Start time

End time

Priority: 1 Prompt: If the advertising time overlaps, you can set the priority. The higher the number, the higher the priority. It is an integer of 1-99

* Push range: Set

Figure 11-3-4 Accurate delivery of the advertisement

Enable the advanced advertising, and you can set the advertising time range, priority, push range, and other conditions to perform more accurate advertisement delivery.

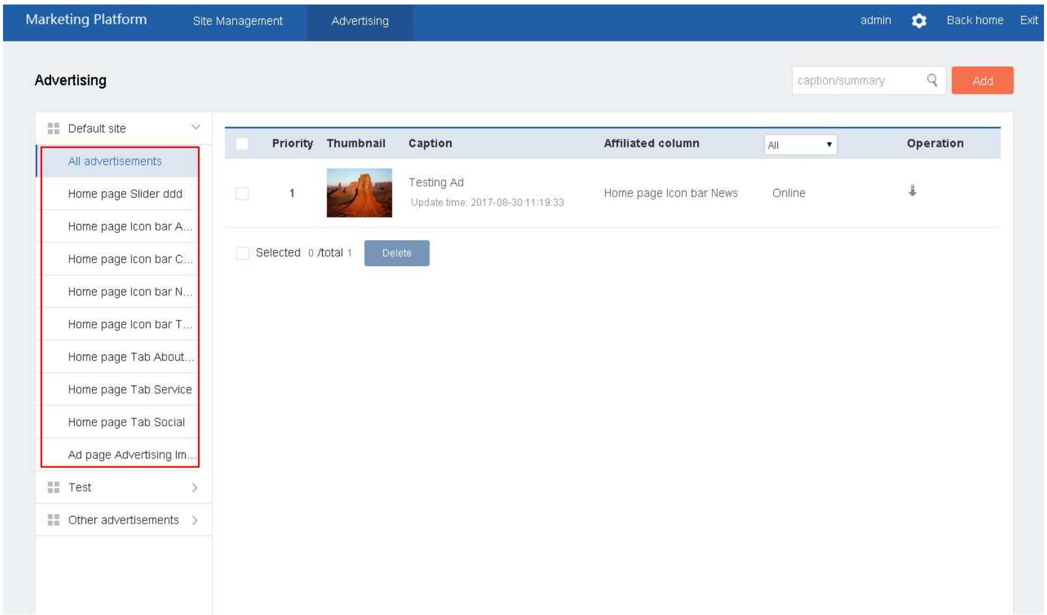
Time range: You can set the advertising time so that the advertisement can automatically get online and offline.

Push range: Push the target site accurately.

After filling in the advertisement information, you can click **Draft** to save the advertisement. In the advertisement list page, click the draft box and you can query. You also can click **Submit**. After being submitted for auditing, the advertisement is released immediately.

11.3.1.2 Query the Advertisement

Query by the advertising place: Query by the advertising place in the navigation bar.

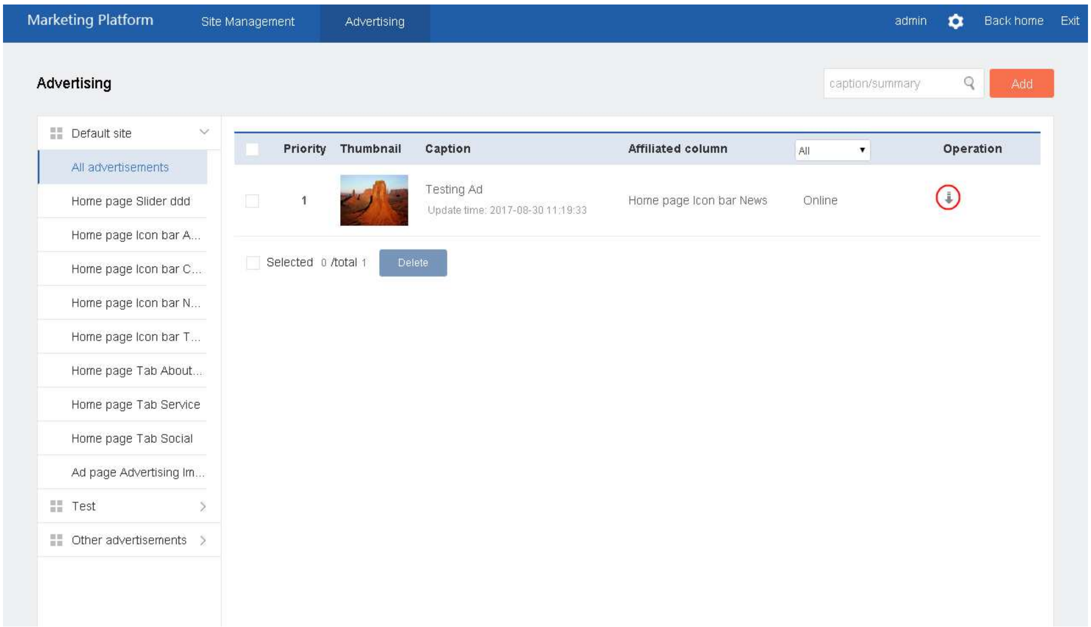


☐	Priority	Thumbnail	Caption	Affiliated column	All ▾	Operation
☐	1		Testing Ad Update time: 2017-08-30 11:19:33	Home page Icon bar News	Online	⇣

☐ Selected 0 /total 1

Figure 11-3-5 Query the advertisement by the advertising place

11.3.1.3 Get the Advertisement Offline



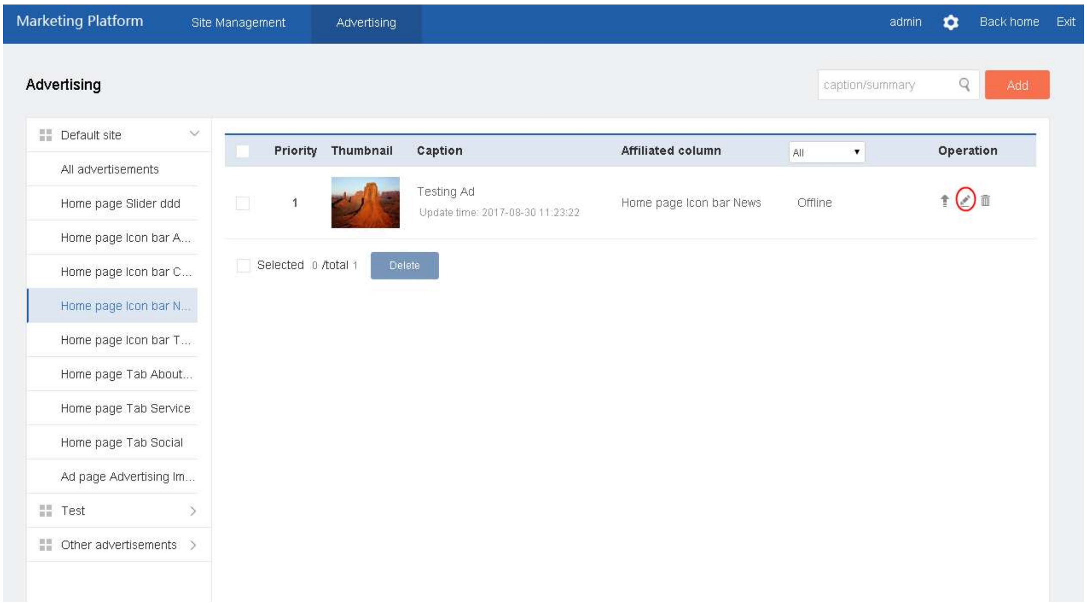
☐	Priority	Thumbnail	Caption	Affiliated column	All	Operation
☐	1		Testing Ad Update time: 2017-08-30 11:19:33	Home page Icon bar News	Online	⇩

Figure 11-3-6 Get the advertisement offline

In the advertisement list page, click the Offline button, and you can get the advertisement offline. The offline advertisement is invisible in the corresponding site.

11.3.1.4 Edit the Advertisement

Edit the content of the released advertisement.

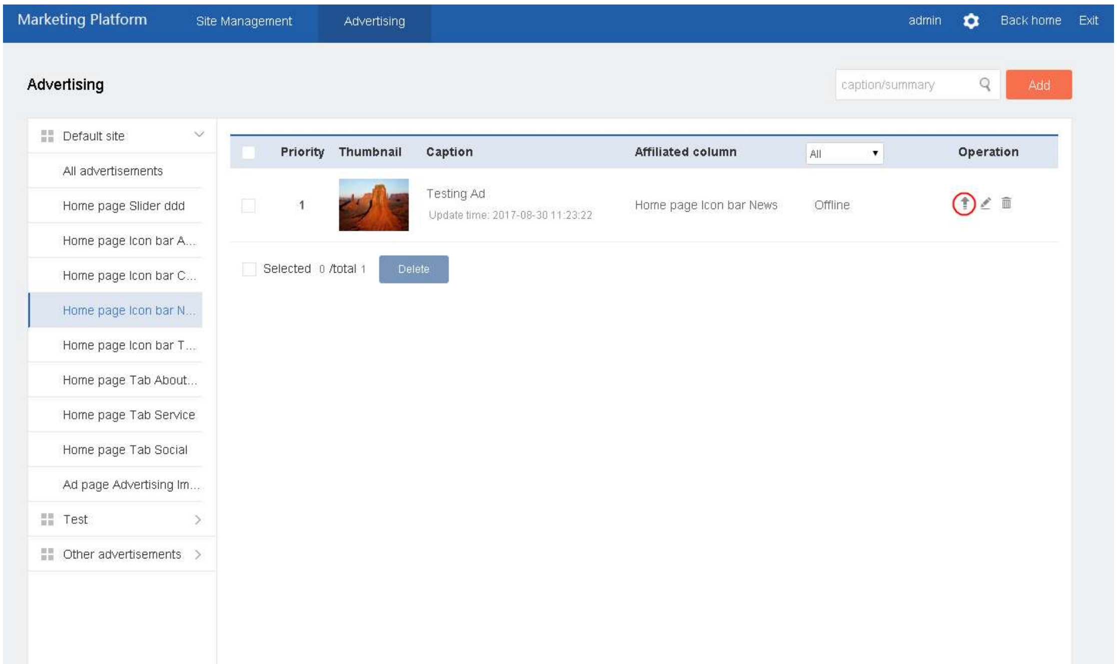


☐	Priority	Thumbnail	Caption	Affiliated column	All	Operation
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	⇧ ✎ 🗑

Figure 11-3-7 Edit the advertisement

In the advertisement list page, click the **Edit** button, and you can edit the advertisement.

11.3.1.5 Get the Advertisement Online



☐	Priority	Thumbnail	Caption	Affiliated column	All ▾	Operation
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	

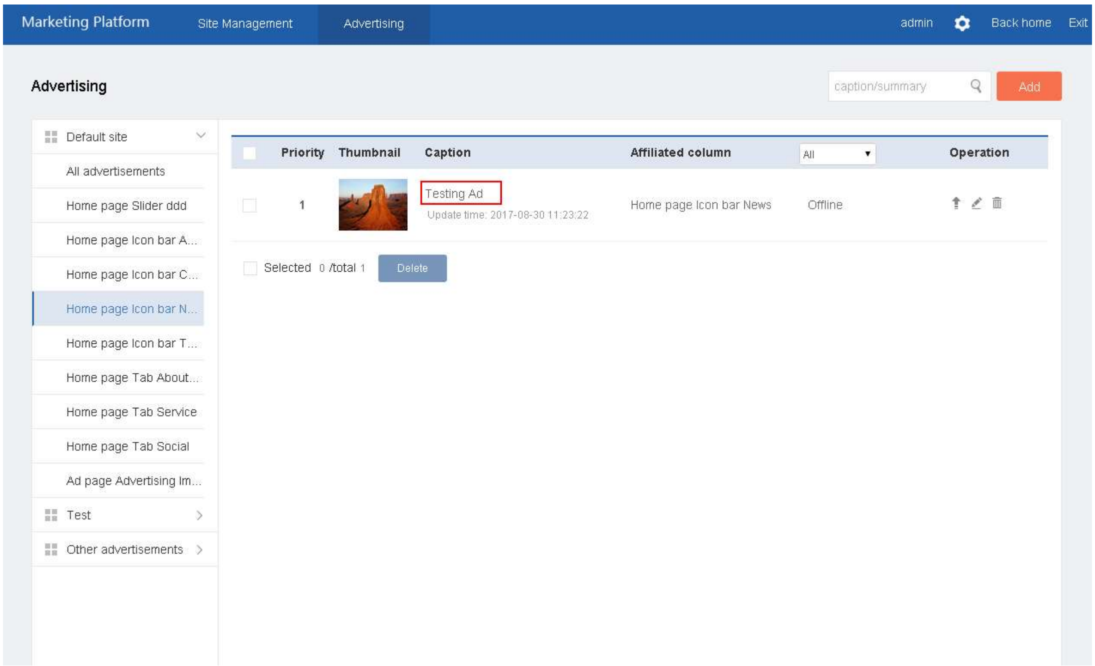
Figure 11-3-8 Get the advertisement online

In the advertisement list page, click the Online button, and you can push the advertisement to the corresponding site again.

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved

11.3.1.6 View the Advertisement

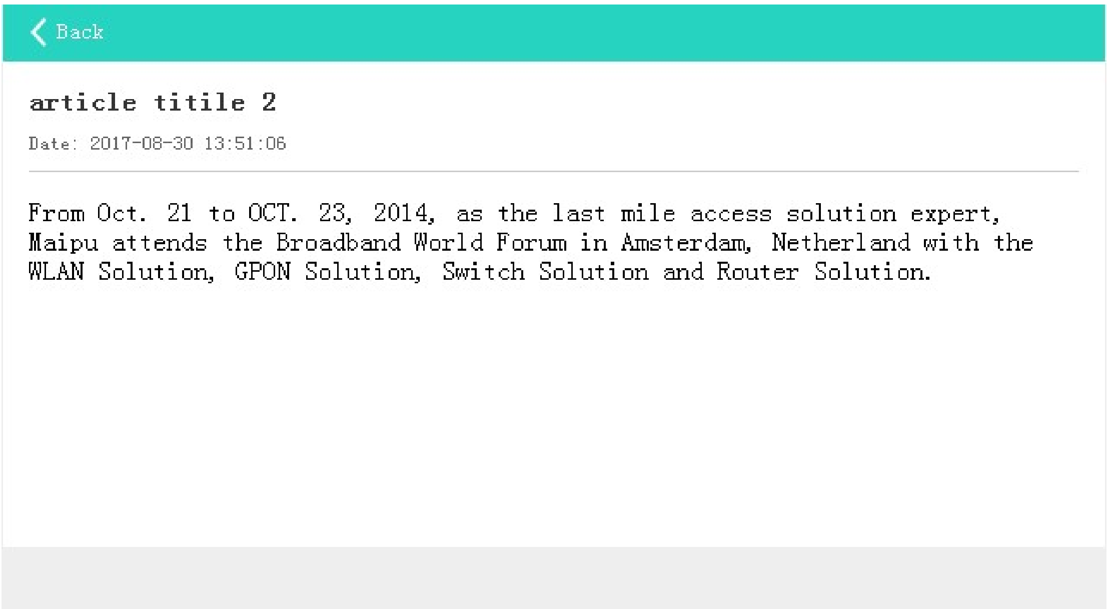


☐	Priority	Thumbnail	Caption	Affiliated column	All	Operation
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	

☐ Selected 0 /total 1

Figure 11-3-9 View the advertisement

Click the title of the advertisement in the list, and you can view the advertisement, as follows:



article titile 2

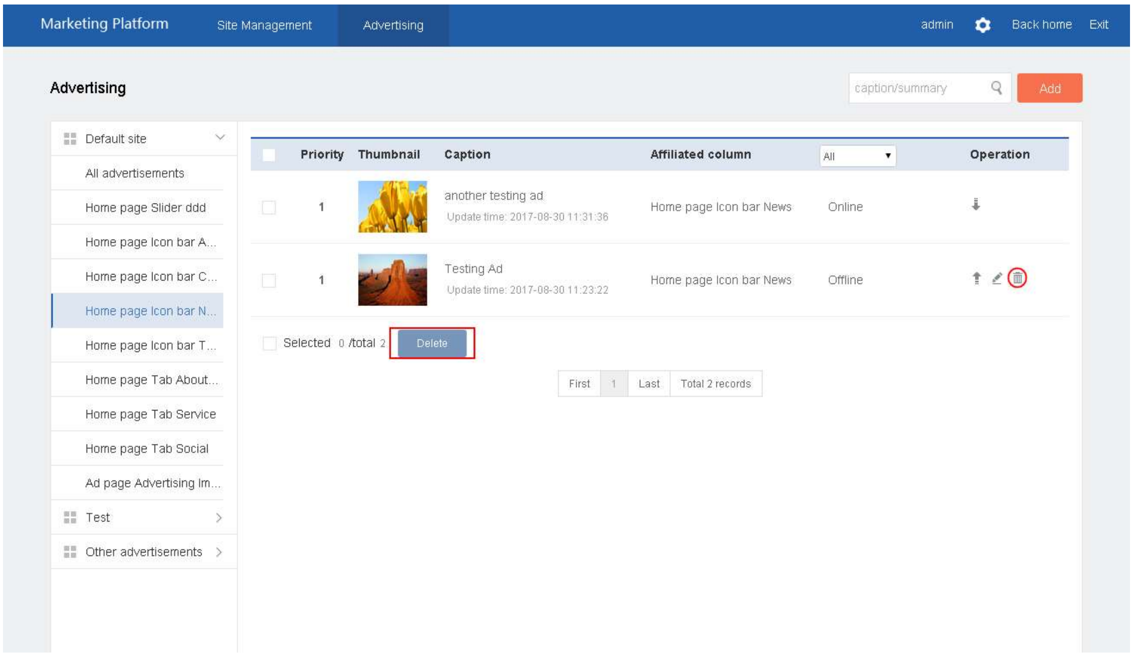
Date: 2017-08-30 13:51:06

From Oct. 21 to OCT. 23, 2014, as the last mile access solution expert, Maipu attends the Broadband World Forum in Amsterdam, Netherland with the WLAN Solution, GPON Solution, Switch Solution and Router Solution.

Figure 11-3-10 Preview the advertisement

11.3.1.7 Delete the Advertisement

You can delete one advertisement or delete the advertisements in batches. The online advertisement cannot be deleted. To delete the online advertisement, you need to get the advertisement offline first.



☐	Priority	Thumbnail	Caption	Affiliated column	All ▾	Operation
☐	1		another testing ad Update time: 2017-08-30 11:31:36	Home page Icon bar News	Online	
☐	1		Testing Ad Update time: 2017-08-30 11:23:22	Home page Icon bar News	Offline	

Figure 11-3-11 Delete the advertisement

copyright©2016Maipu Communication Technology Co., Ltd,

All Rights Reserved