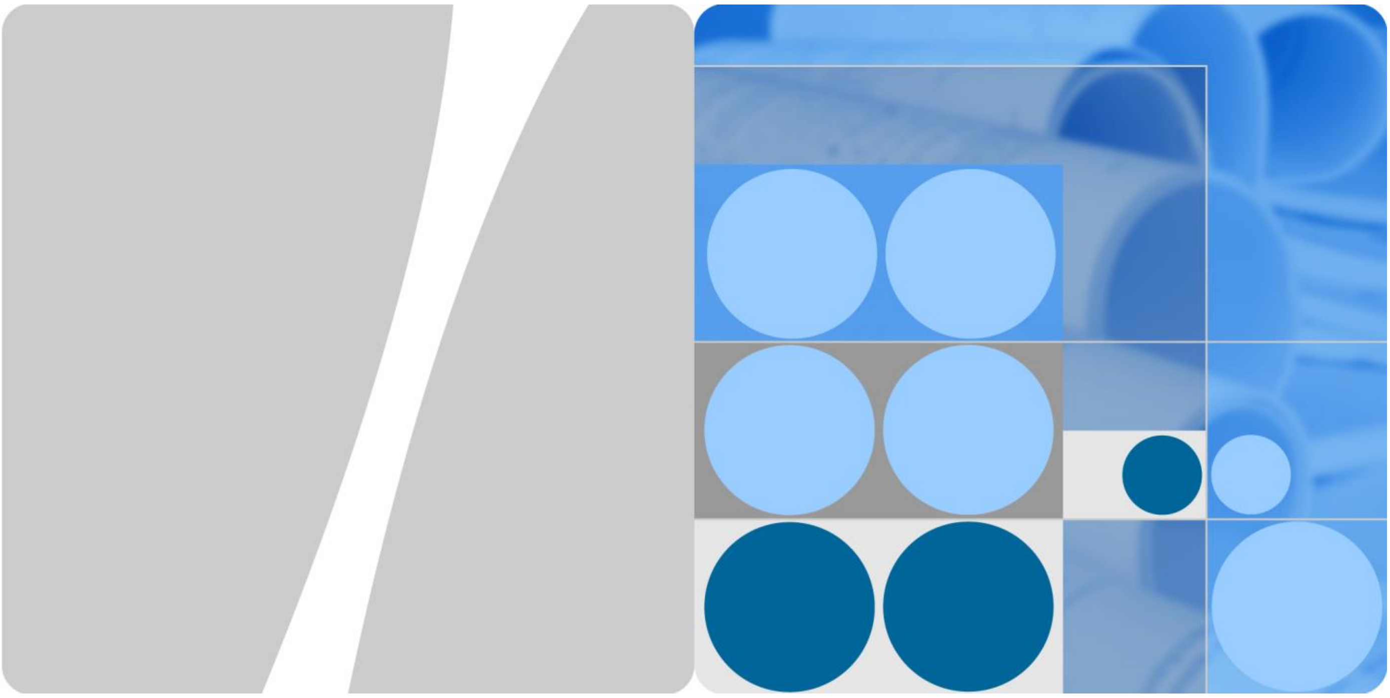


Agile Controller-Campus V100R002C10

Guest Management Technology White Paper

Issue	**01**
Date	**2016-04-15**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 Overview

1.1 Background

Advances in Information and Communication Technologies (ICT) mean that enterprise users require network access from anywhere. A large number of mobile staff and partners frequently use their own terminals (such as laptops) to access enterprise LANs, which threatens enterprise information security. When external users need to connect to the intranet or Internet temporarily, they should be authenticated and assigned with access rights that are different from those assigned to enterprise employees.

Furthermore, with the popularization of Wi-Fi networks, guests connect to networks temporarily in public places such as shopping malls. The admission control is required and guests' behavior should be audited.

Huawei offers the Agile Controller guest management solution to help enterprises manage guests efficiently and conveniently. With the solution, enterprises can customize access right control policies for different guests and implement full life-cycle guest management.

1.2 Technical Features

The guest management function developed by Huawei supports full life-cycle guest management which can be classified into four phases: guest service initialization, guest account creation and delivery, guest account authentication, guest account maintenance and audit.

The guest management function has the following features:

1. Diversified guest account types: System and guest administrators can create guest accounts, and guests can register accounts. Account attributes can be customized.
2. Various guest authentication modes: Guest accounts can be approved by an administrator, a receptionist, or an employee (through QR code scanning), or do not need to be approved.

3. Guest pages customized based on templates: Enterprises can provide self-defined pages to improve enterprise brand image.
4. Customized guest page pushing policies: Guest pages, including advertisements and information, are pushed based on access locations, SSIDs, terminal types, and access time.
5. Local languages for guests and guest administrators
6. Third-party account-based access: Guests can use third-party accounts such as Google, Facebook, Twitter, or WeChat accounts to connect to networks.
7. Guest account audit: Guest account approval records and login and logout logs can be audited.
8. 5W1H-based authorization: Access rights of guests are strictly controlled.

Guest access scenarios are classified into Wi-Fi access of visitors in enterprise campuses, Wi-Fi access of guests in public places such as shopping malls, and Wi-Fi access of guests in high-density stadiums.

2 Services and Functions of Guest Management

2.1 Guest Management

Guest accounts are created by organizations to authenticate guests. Guests usually include partner personnel and customers. In general, guest accounts are temporary accounts that are granted with low-level access rights. The guest account management function implements full life-cycle management of guest accounts, including guest account registration, approval, allocation, and deregistration.

The guest account management phases include:

1. Account application, approval, and creation

   A large number of account generation policy templates are created based on demands for various account types and built in the system to help administrators and guests (self-registration mode) create accounts easily by using associated guest account policies.

2. Account allocation

   After guest accounts are created or approved, the server notifies guests on web pages or by sending SMS messages or emails. The account policy associated with the page to be pushed determines the notification mode.

3. Account authentication

   After obtaining accounts and passwords, guests can pass the authentication and connect to networks.

4. Account audit and management

   After guest accounts are applied for successfully, administrators can audit guest account approval records. After guests connect to networks, administrators can audit login and logout logs of guests, configure account validity periods so that the system can automatically deregister and clear expired accounts.

Guest account policies are critical to guest account creation and cover the following key configuration items:

- Account creation mode: Guest accounts can be created by administrators one by one or in batches or registered by guests themselves.
- Guest account approval mode: Guest accounts can require no approval, or can be approved by an employee, an administrator, or a receptionist (through email activation or QR code scanning).
- Guest notification mode: Guests are notified by using SMS messages, emails, or web pages.
- Account generation policy: mobile phone, email address, account and passcode

Other configuration items are also provided, including account validity periods, effective time, and roles and user groups to which guest accounts belong, password policies, and password types. You can create various guest accounts based on the scenario.

2.2 Page Customization

Guest pages can be customized based on templates and enterprises can provide self-defined pages to improve enterprise brand image.

Three highlights of the page customization function are as follows:

- Abundant templates are provided for page customization.
- Visualized page customization is easy-to-use.
- Page templates can be localized.

Page customization supports the entire guest access authentication process. You can customize the user notice page, authentication page, authentication success page, registration page, and registration success page.

2.3 Page Pushing

After authentication and registration pages are customized for different users, the page pushing function developed by Huawei allows you to configure Portal page pushing rules to ensure that users can access corresponding authentication and registration pages.

Pages are pushed based on:

- Time
- Terminal IP address range
- Operating system type: Windows, iOS, Android, Linux\Unix, and MAC OS

Account type (WeChat or QR code): Page pushing rules are provided in scenarios where guests use WeChat accounts or scan public QR codes to connect to networks.

User-defined parameters (such as SSIDs and AP MAC addresses): When terminals attempt to connect to the network, access devices deliver the configured URL and parameter information. The Agile Controller pushes pages based on URL parameter information.

In addition, after the authentication succeeds, web pages requested by guests before the authentication are displayed automatically.

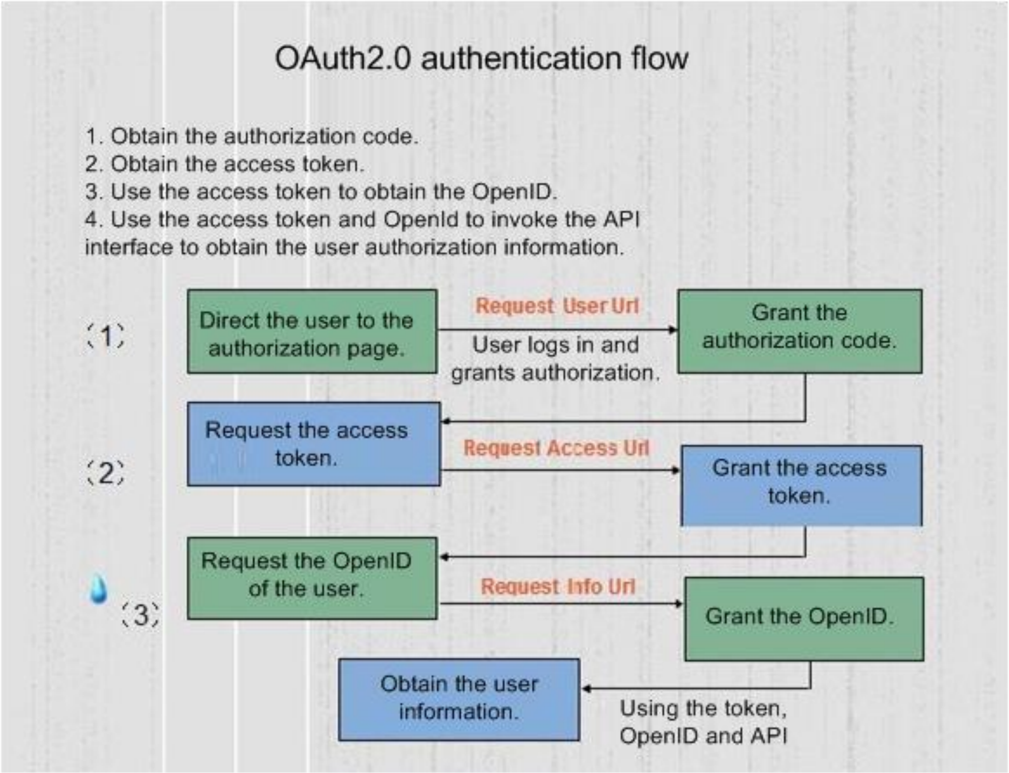
2.4 Third-Party Account-Based Guest Access

The third-party account-based access function enables the Agile Controller to interconnect with social media platforms such as Google, Facebook, Twitter and WeChat so that guests can use third-party accounts to connect to networks.

Open APIs for account authorization provided by public platforms (Google, Facebook, and Twitter) use the Open Authorization (OAuth) protocol so that third-party apps can perform authentication. Google and Facebook use the OAuth2.0 protocol and their authentication procedures are similar. Twitter uses the OAuth1.0 protocol and an authentication procedure that is slightly different from those used by Google and Facebook.

OAuth is an open standard for authorization. It allows secure API authorization in a simple and standard method from web, mobile and desktop applications. With users' authorization, third-party websites can access information stored by users in service providers while user names and passwords of users are not provided to the third-party websites.

OAuth allows access tokens to be issued to third-party websites. OAuth access tokens are used to grant access to specific resources for a specific period of time.


OAuth2.0 authentication flow
1. Obtain the authorization code.
2. Obtain the access token.
3. Use the access token to obtain the OpenID.
4. Use the access token and OpenId to invoke the API interface to obtain the user authorization information.
(1)
Direct the user to the authorization page.
Request User Url
User logs in and grants authorization.
Grant the authorization code.
(2)
Request the access token.
Request Access Url
Grant the access token.
(3)
Request the OpenID of the user.
Request Info Url
Grant the OpenID.
Obtain the user information.
Using the token, OpenID and API

The following process is the process for logging in to the Agile Controller using a third-party account:

1. On the customized authentication page, links to social networking sites are provided. You can click a link to open the corresponding login page.
2. The Portal server and social networking site use the OAuth authentication to ensure security.
3. After being authorized by the social networking site, the Agile Controller obtains user information from the social networking site and then continues the authorization with the Agile Controller server.

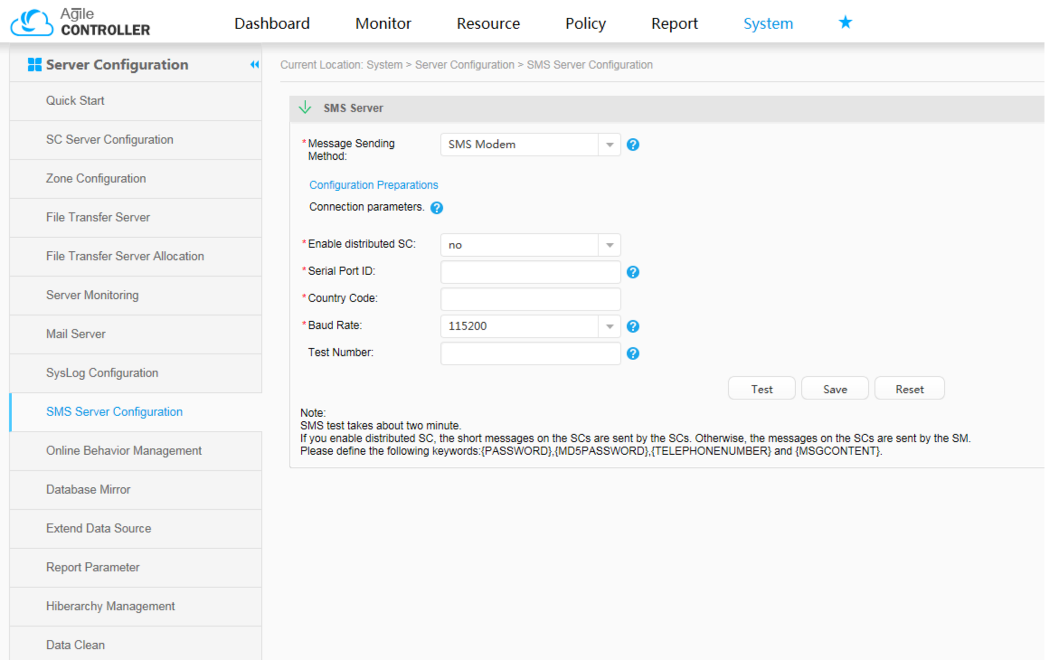
3 Typical Access Scenarios

3.1 Guest Uses a Mobile Number to Register an Account and Connect to the Network

Scenario: A shopping mall provides wireless network services to customers. The shopping mall has the following requirements: When customers try to visit web pages in the mall, authentication pages are displayed automatically. Customers can enter their mobile numbers to obtain passwords and then access the Internet. The passwords expire after 8 hours. Customers then need to obtain new passwords before they can continue using the Internet service.

Configuration Process

Step 1 The administrator configures the SMS server to send passwords to mobile phones.



Current Location: System > Server Configuration > SMS Server Configuration

SMS Server

*Message Sending Method: SMS Modem

Configuration Preparations

Connection parameters.

*Enable distributed SC: no

*Serial Port ID:

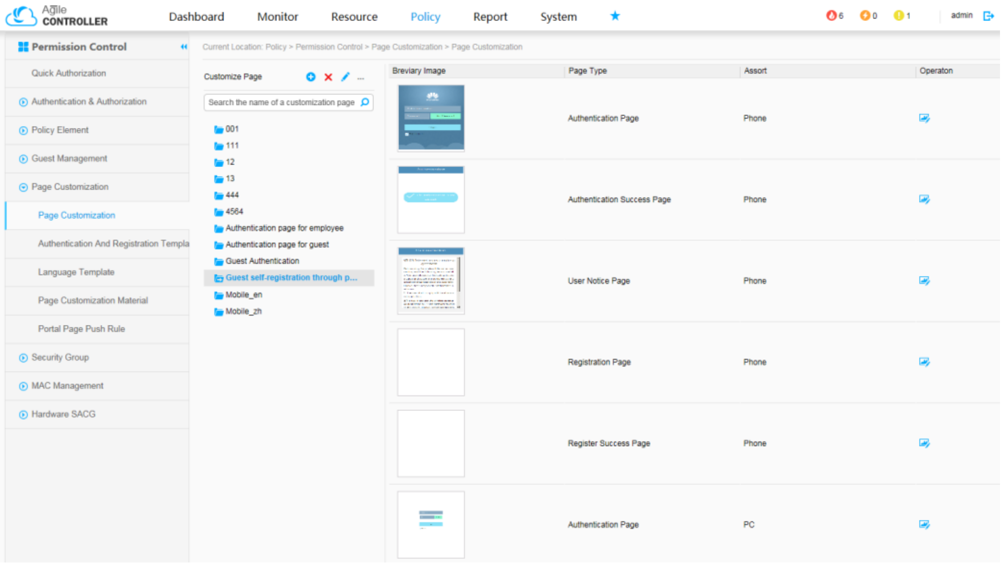
*Country Code:

*Baud Rate: 115200

Test Number:

Note:
SMS test takes about two minute.
If you enable distributed SC, the short messages on the SCs are sent by the SCs. Otherwise, the messages on the SCs are sent by the SM.
Please define the following keywords:{PASSWORD},{MD5PASSWORD},{TELEPHONENUMBER} and {MSGCONTENT}.

Step 2 The administrator customizes the authentication page according to the default mobile number-based guest account policy and mobile number-based rapid authentication template.



Current Location: Policy > Permission Control > Page Customization > Page Customization

Breviary Image	Page Type	Assort	Operaton
	Authentication Page	Phone	
	Authentication Success Page	Phone	
	User Notice Page	Phone	
	Registration Page	Phone	
	Register Success Page	Phone	
	Authentication Page	PC	

Step 3 The administrator configures the Portal page pushing rule for mobile number-based rapid authentication.

After the configuration is complete, guests can use mobile phones and other mobile terminals to apply for passwords on the rapid authentication page. After receiving passwords contained in SMS messages, guests can enter their phone numbers and passwords to access the Internet.

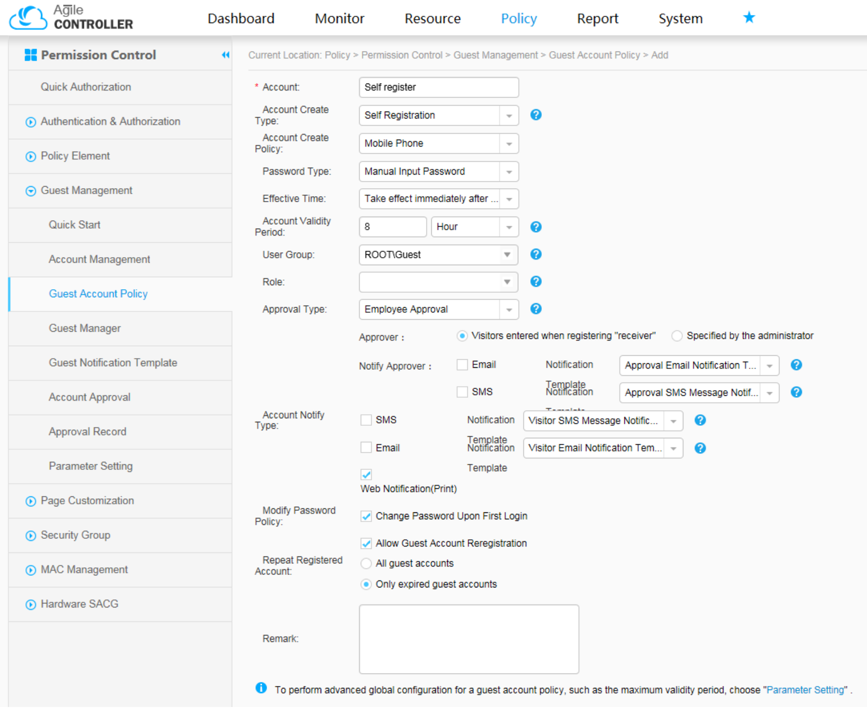
----End

3.2 Guest Applies for an Account and Connects to the Network After Being Approved by an Employee

Scenario: An enterprise's guest needs to connect to the enterprise intranet. After the guest arrives at the enterprise and applies for an account and password, and then connects to the enterprise intranet after being approved by an employee who receives the guest.

Configuration Process

Step 1 The administrator configures the guest account policy and sets the **Approval Type** to **Employee Approval**.



Current Location: Policy > Permission Control > Guest Management > Guest Account Policy > Add

* Account:	Self register
Account Create Type:	Self Registration
Account Create Policy:	Mobile Phone
Password Type:	Manual Input Password
Effective Time:	Take effect immediately after ...
Account Validity Period:	8 Hour
User Group:	ROOT\Guest
Role:	
Approval Type:	Employee Approval

Approver： ● Visitors entered when registering "receiver" ○ Specified by the administrator

Notify Approver： □ Email Notification Template: Approval Email Notification T... □ SMS Notification Template: Approval SMS Message Notif...

Account Notify Type: □ SMS Notification Template: Visitor SMS Message Notific... □ Email Notification Template: Visitor Email Notification Tem... ☑ Web Notification(Print)

Modify Password Policy: ☑ Change Password Upon First Login

☑ Allow Guest Account Reregistration

Repeat Registered Account: ○ All guest accounts ● Only expired guest accounts

Remark:

To perform advanced global configuration for a guest account policy, such as the maximum validity period, choose "Parameter Setting" .

Step 2 The administrator customizes the authentication and registration pages based on the guest account policy.

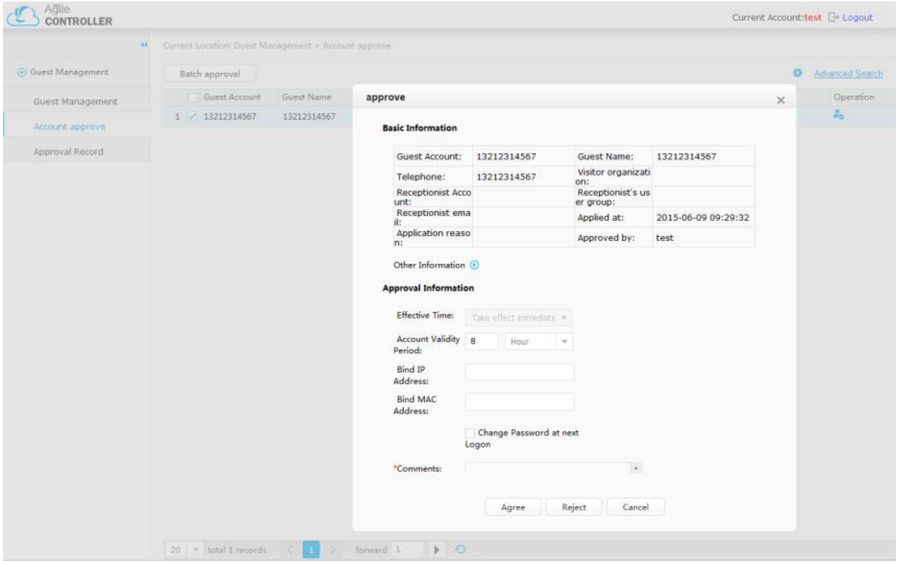
Step 3 The administrator configures the pushing rule for the customized Portal pages.

----End

Access Process

Step 1 A guest tries to connect to the network, completes registration on the pushed registration page, and waits for the receptionist's approval.

Step 2 The receptionist connects to the network and approves the guest account.



approve

Basic Information

Guest Account:	13212314567	Guest Name:	13212314567
Telephone:	13212314567	Visitor organization:	
Receptionist Account:		Receptionist's user group:	
Receptionist email:		Applied at:	2015-06-09 09:29:32
Application reason:		Approved by:	test

Other Information

Approval Information

Effective Time: Take effect immediate

Account Validity Period: 8 Hour

Bind IP Address:

Bind MAC Address:

□ Change Password at next Logon

*Comments:

Step 3 The guest enters the approved account and password on the authentication page to connect to the network.

----End

3.3 Guest Uses the Account Created by a Receptionist to Connect to the Network

Scenario: An enterprise's guest needs to connect to the enterprise intranet. To ensure that the guest can connect to the network as soon as possible, the enterprise requires that the receptionist creates guest accounts before the guests arrive at the enterprise.

Configuration Process

Step 1 The administrator creates the guest account policy that allows the receptionist to create guest accounts.

Step 2 The administrator grants the rights to the receptionist to create guest accounts.

Step 3 The administrator customizes the authentication and registration pages based on the guest account policy.

Step 4 The administrator configures the pushing rule for the customized Portal pages.

----End

Access Process

Step 1 The receptionist connects to the network, creates guest accounts in batches, and informs the guests of passwords.

Step 2 The guest enters the temporary accounts and passwords on the authentication page to connect to the network.

----End

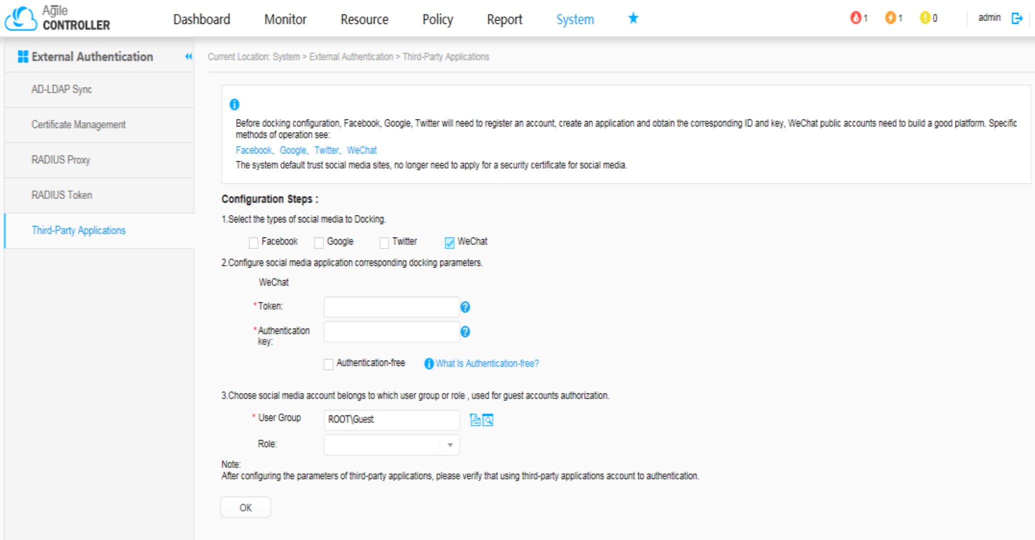
3.4 Third-party Account-based Access

3.4.1 Guests Follow a WeChat Public Account to Connect to the Network

Scenario: A shopping mall wants to provide free Wi-Fi services to customers after customers follow its WeChat public account.

Configuration Process

Step 1 The administrator configures the parameters for connecting the Agile Controller to the WeChat server.



Current Location: System > External Authentication > Third-Party Applications

Before docking configuration, Facebook, Google, Twitter will need to register an account, create an application and obtain the corresponding ID and key, WeChat public accounts need to build a good platform. Specific methods of operation see:
Facebook、Google、Twitter、WeChat
The system default trust social media sites, no longer need to apply for a security certificate for social media.

Configuration Steps :

1.Select the types of social media to Docking.

□ Facebook □ Google □ Twitter ☑ WeChat

2.Configure social media application corresponding docking parameters.

WeChat

*Token:

*Authentication key:

□ Authentication-free What Is Authentication-free?

3.Choose social media account belongs to which user group or role , used for guest accounts authorization.

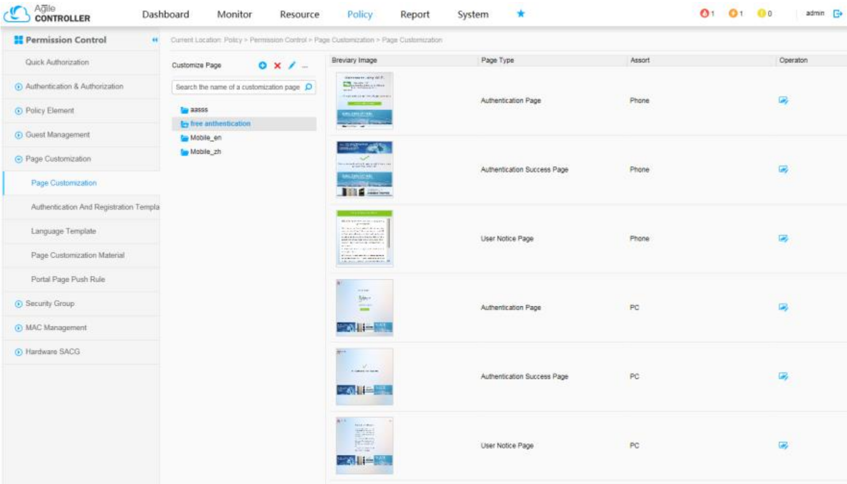
* User Group ROOT\Guest

Role:

Note:
After configuring the parameters of third-party applications, please verify that using third-party applications account to authentication.

OK

Step 2 The administrator uses the template to customize the free authentication page.



Current Location: Policy > Permission Control > Page Customization > Page Customization

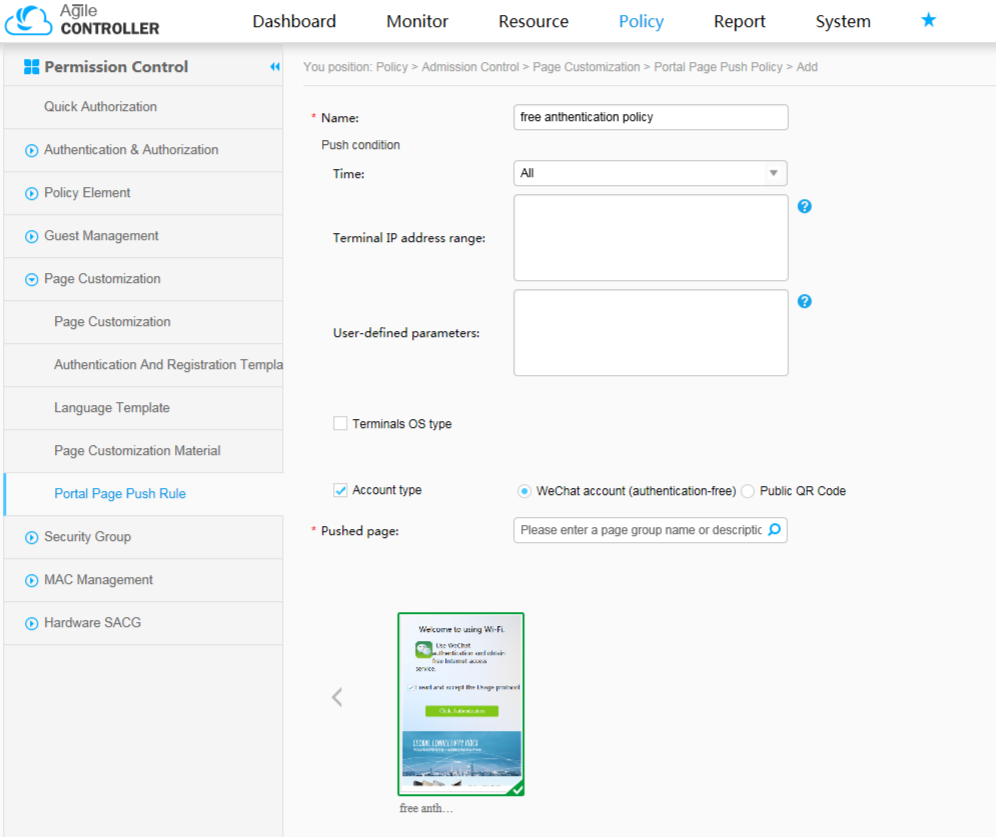
Customize Page

Search the name of a customization page

- aasss
- free anthentication
- Mobile_en
- Mobile_zh

Breviary Image	Page Type	Assort	Operation
	Authentication Page	Phone	
	Authentication Success Page	Phone	
	User Notice Page	Phone	
	Authentication Page	PC	
	Authentication Success Page	PC	
	User Notice Page	PC	

Step 3 The administrator configures the Portal page pushing rule.



You position: Policy > Admission Control > Page Customization > Portal Page Push Policy > Add

* Name: free anthentication policy

Push condition

Time: All

Terminal IP address range:

User-defined parameters:

□ Terminals OS type

☑ Account type ● WeChat account (authentication-free) ○ Public QR Code

* Pushed page: Please enter a page group name or descriptic

Welcome to using Wi-Fi.

Use WeChat authentication and obtain free Internet access service.

✓ I read and accept the Usage protocol

Click Authentication

free anth...

After the configuration is complete, guests can obtain the URL of the free authentication page by following the WeChat public account and use the URL to connect to the network.

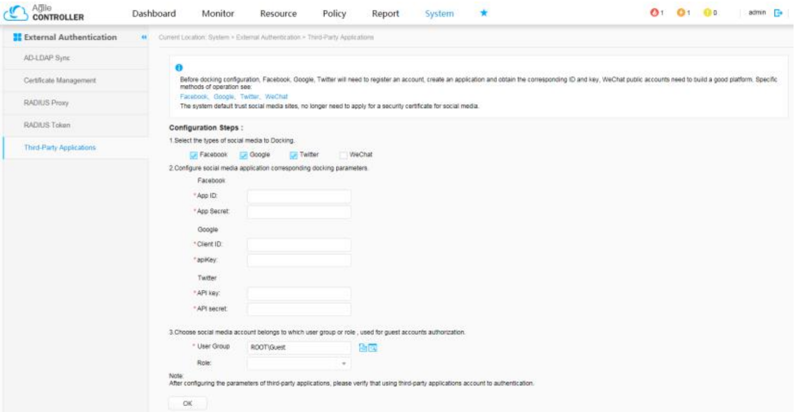
----End

3.4.2 Guests Use Social Media Accounts such as Google Accounts to Connect to the Network

Scenario: A high-density soccer stadium wants to provide free Wi-Fi services to fans during games. Because the stadium will accommodate a large number of fans, the stadium wants fans to use their social medial accounts to connect to the network.

Configuration Process

Step 1 The administrator sets third-party app parameters.



Current Location: System > External Authentication > Third-Party Applications

Before docking configuration, Facebook, Google, Twitter will need to register an account, create an application and obtain the corresponding ID and key, WeChat public accounts need to build a good platform. Specific methods of operation see:

Facebook、Google、Twitter、WeChat

The system default trust social media sites, no longer need to apply for a security certificate for social media.

Configuration Steps :

1.Select the types of social media to Docking.

☑ Facebook ☑ Google ☑ Twitter □ WeChat

2.Configure social media application corresponding docking parameters.

Facebook

* App ID:

* App Secret:

Google

* Client ID:

* apiKey:

Twitter

* API key:

* API secret:

3.Choose social media account belongs to which user group or role , used for guest accounts authorization.

* User Group: ROOT\Guest

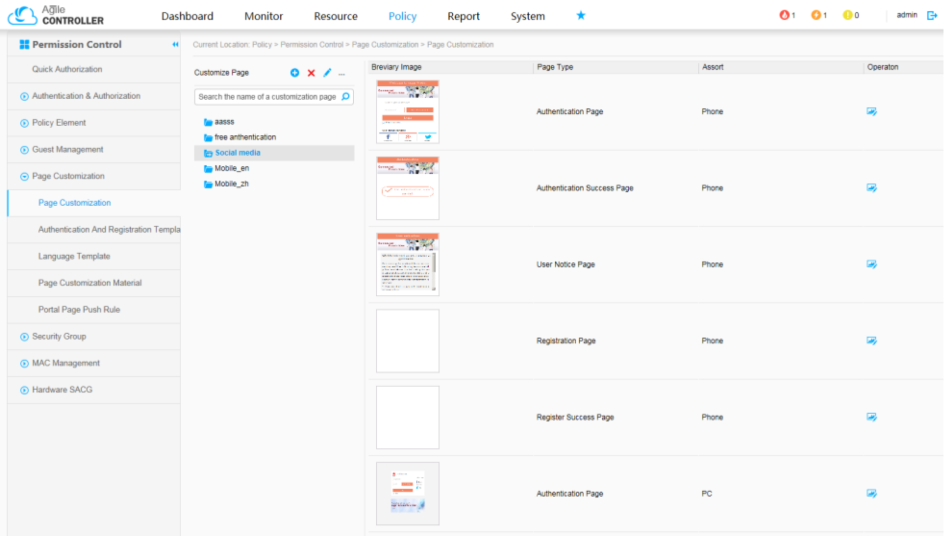
Role:

Note:

After configuring the parameters of third-party applications, please verify that using third-party applications account to authentication.

OK

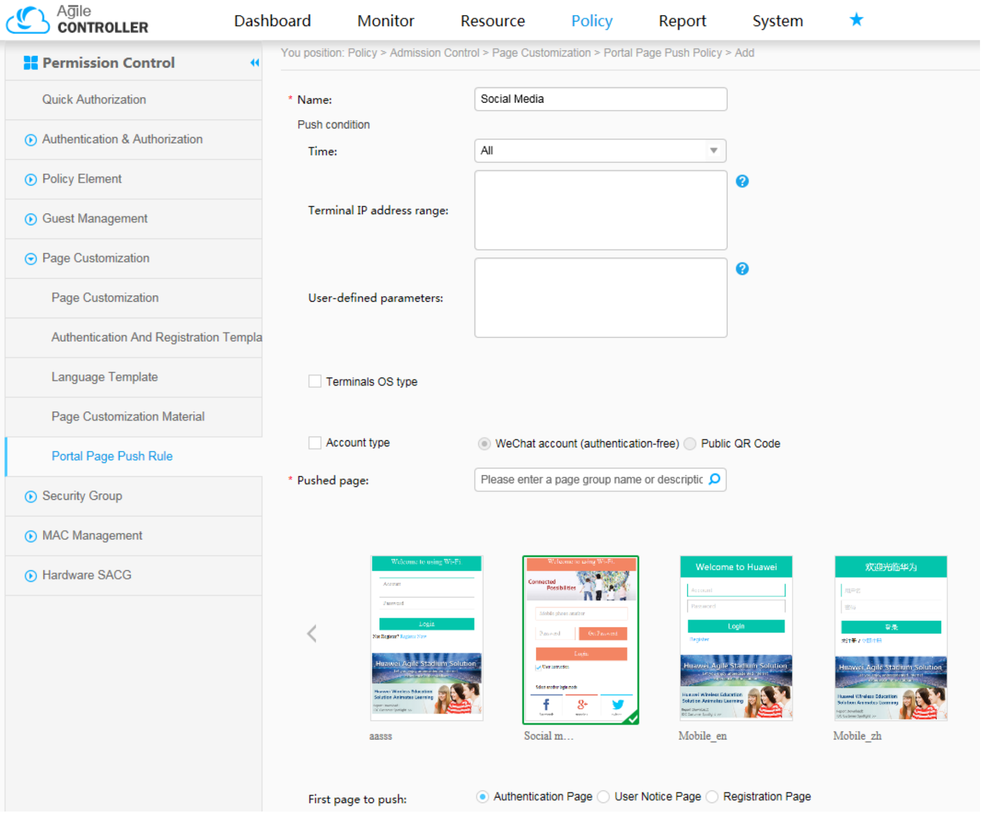
Step 2 The administrator uses the template to customize the third-party account-based authentication page.



Current Location: Policy > Permission Control > Page Customization > Page Customization

Breviary Image	Page Type	Assort	Operaton
	Authentication Page	Phone	
	Authentication Success Page	Phone	
	User Notice Page	Phone	
	Registration Page	Phone	
	Register Success Page	Phone	
	Authentication Page	PC	

Step 3 The administrator configures the Portal page pushing rule.



You position: Policy > Admission Control > Page Customization > Portal Page Push Policy > Add

* Name: Social Media

Push condition

Time: All

Terminal IP address range:

User-defined parameters:

□ Terminals OS type

□ Account type ● WeChat account (authentication-free) ○ Public QR Code

* Pushed page: Please enter a page group name or descriptic

First page to push: ● Authentication Page ○ User Notice Page ○ Registration Page

After the configuration is complete, guests use mobile terminals such mobile phones to associate with the Wi-Fi network. On the third-party app authentication page, guests touch the login icon and enter passwords to request authentication and connect to the network.

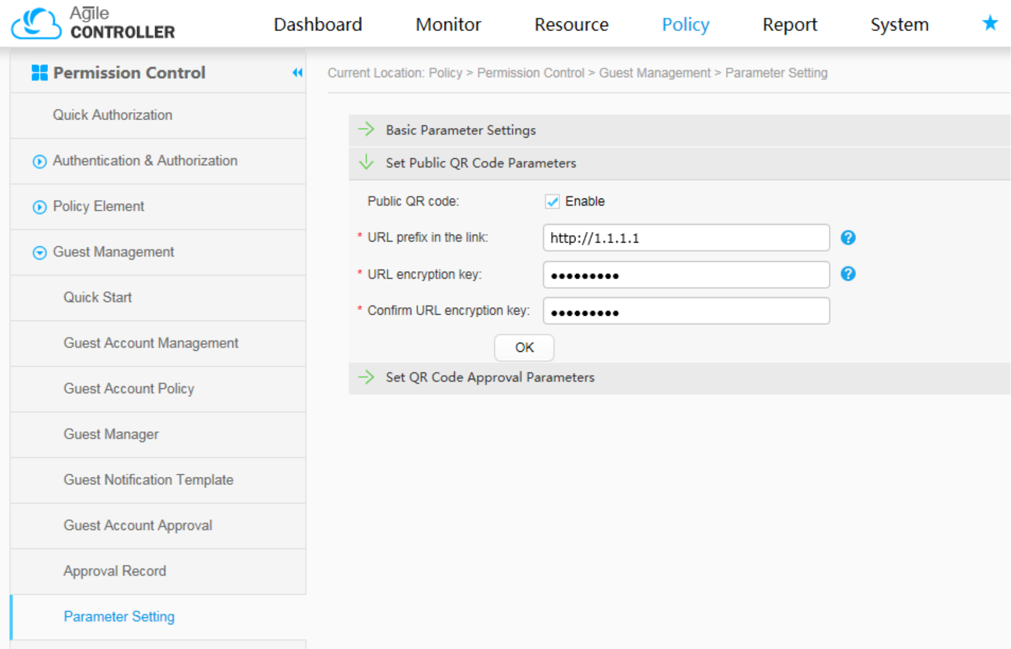
----End

3.5 Guests Scan QR Codes to Connect to the Network

Scenario: An enterprise organizes a promotion activity. Public quick response codes (QR codes) are pasted in the reception site or printed on promotion materials to inform users that they can access the Internet by scanning the QR codes.

Configuration Process

Step 1 The administrator sets public QR code parameters.



Current Location: Policy > Permission Control > Guest Management > Parameter Setting

Set Public QR Code Parameters

Public QR code: ☑ Enable

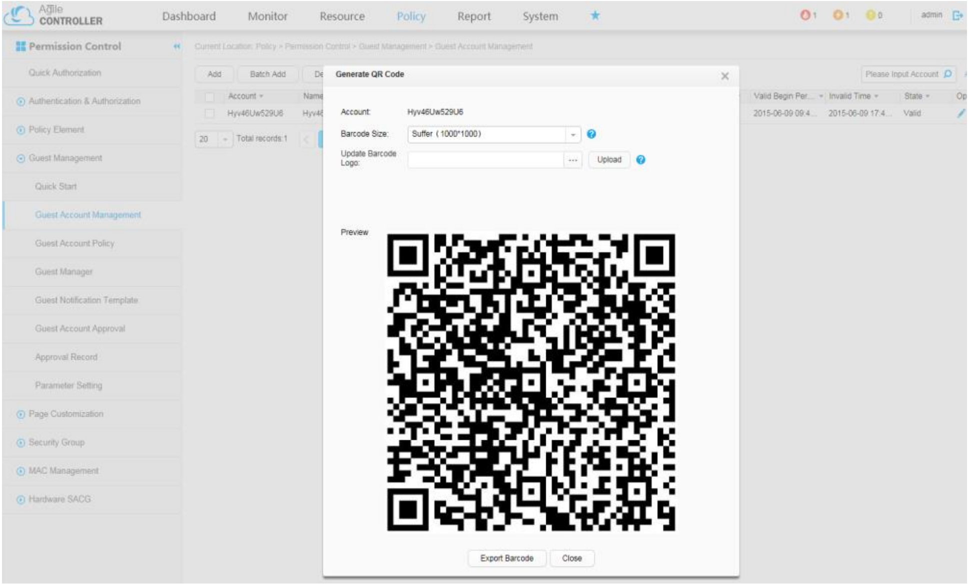
* URL prefix in the link: http://1.1.1.1

* URL encryption key: •••••••••

* Confirm URL encryption key: •••••••••

Step 2 The administrator creates the QR code-based guest account policy.

Step 3 The administrator creates a QR code account.



Current Location: Policy > Permission Control > Guest Management > Guest Account Management

Account	Name	Valid Begin Per...	Invalid Time	State
Hyv46Uw529U6	Hyv4	2015-06-09 09:4...	2015-06-09 17:4...	Valid

20 Total records:1

Generate QR Code

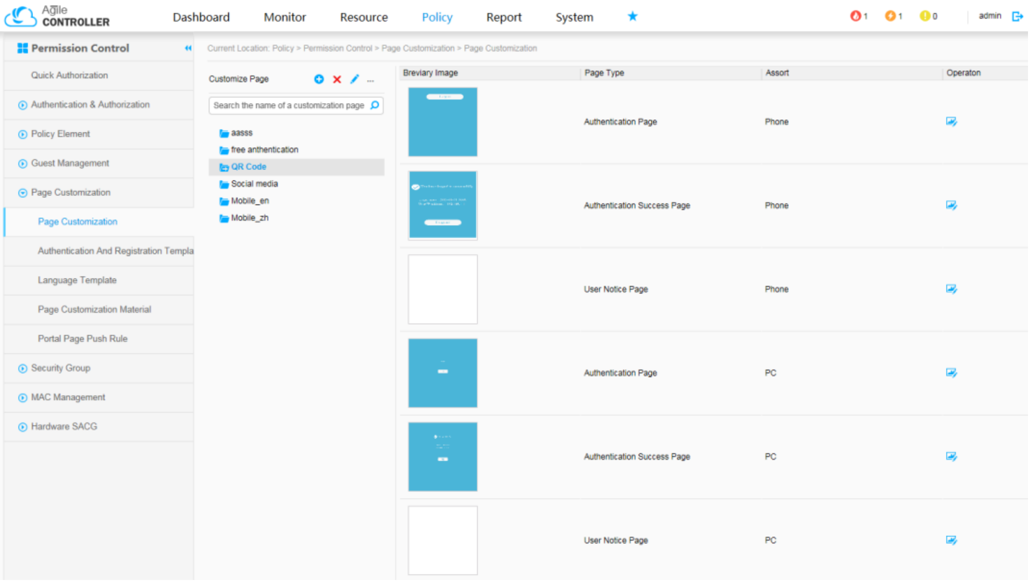
Account: Hyv46Uw529U6

Barcode Size: Suffer（1000*1000）

Update Barcode Logo:

Preview

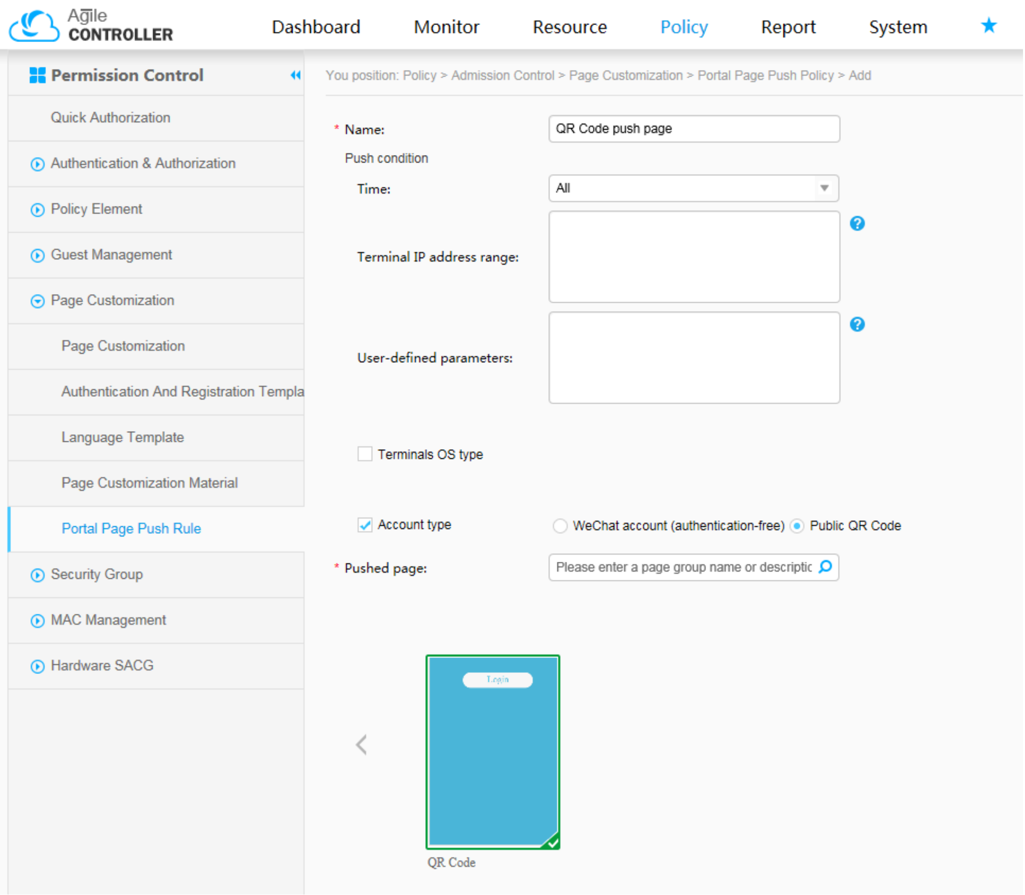
Step 4 The administrator customizes QR code pages.



Current Location: Policy > Permission Control > Page Customization > Page Customization

Breviary Image	Page Type	Assort	Operaton
	Authentication Page	Phone	
	Authentication Success Page	Phone	
	User Notice Page	Phone	
	Authentication Page	PC	
	Authentication Success Page	PC	
	User Notice Page	PC	

Step 5 The administrator configures the Portal page pushing rule.



You position: Policy > Admission Control > Page Customization > Portal Page Push Policy > Add

* Name: QR Code push page

Push condition

Time: All

Terminal IP address range:

User-defined parameters:

□ Terminals OS type

☑ Account type ○ WeChat account (authentication-free) ● Public QR Code

* Pushed page: Please enter a page group name or descriptic

After the configuration is complete, guests can use mobile terminals such as mobile phones to scan QR codes to connect to the network.

----End