SANGFOR

IAM

User self-registration & self-management

Configuration Guide

Version 12.0.25

Change Log

Date	Change Description
June 5, 2019	Document release.

CONTENT

Chapter 1 Overview 1

Chapter 2 Instructions 1

2.1 Requirements 1

2.2 Configurations 1

2.3 Account Registration 1

2.3.1 Scenario 1

2.3.2 Which Authentication Methods Support Account Registration 1

2.3.3 Configurations 1

2.4 Endpoint Registration 7

2.4.1 Scenario 7

2.4.2 Which Authentication Methods Support Account Registration 7

2.4.3 Configurations 7

2.5 User Information Self-Management 10

2.5.1 Scenario 10

2.5.2 How To Access 10

2.5.3 My Profile 11

2.6 Self Registration Approval Options 12

Chapter 3 Precautions 14

Chapter 1 Overview

Authentication is an interactive process that interacts between users and the platform.

Based on the previous interaction, the administrator expects to obtain information about the user or endpoint for some work purposes. The user information is all maintained by the IT administrator causing high workload, and the update is not timely enough, causing there is error in information.

Instead of centralized management, self-management is better, Sangfor online behavior management proposes self-registration, self-management concept, self-registration of account, and self-registration of endpoint.

Chapter 2 Instructions

2.1 Requirements

Local user and external password authentication support [account self-registration].

Open authentication support [endpoint self-registration].

Other authentication servers do not support self-registration. If you select an unsupported authentication server, the self-registration function will be grayed out.

2.2 Configurations

User authentication and management

[Authentication Policy] – [Open Authenticaiton] – [Self-registration]

[Authentication Policy] – [Password Based Authentication] – [Enable Self-Registration]

[Self-Service] – [Registration]

You can configure the self registration policy one by one when configuring the authentication policy. You can also define the self-registration related information in advance and directly reference it in the authentication policy.

In order to facilitate the explanation, the document adopts the method of “defining the self-registration related information in advance and directly reference it the authentication policy”.

2.3 Account Registration

2.3.1 Scenario

Password based authentication, it is expected to log some personal information to help management.

Previously administrators created one by one, and now users can register themselves on demand.

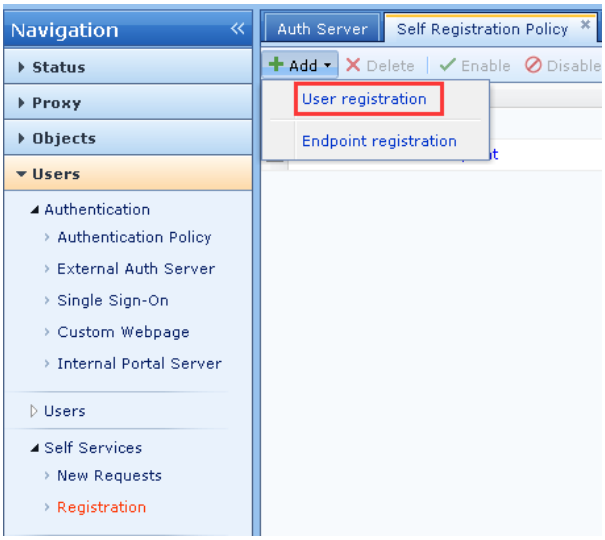
2.3.2 Which Authentication Methods Support Account Registration

Local password authentication, external authentication server password authentication (including WeChat/SMS quick login).

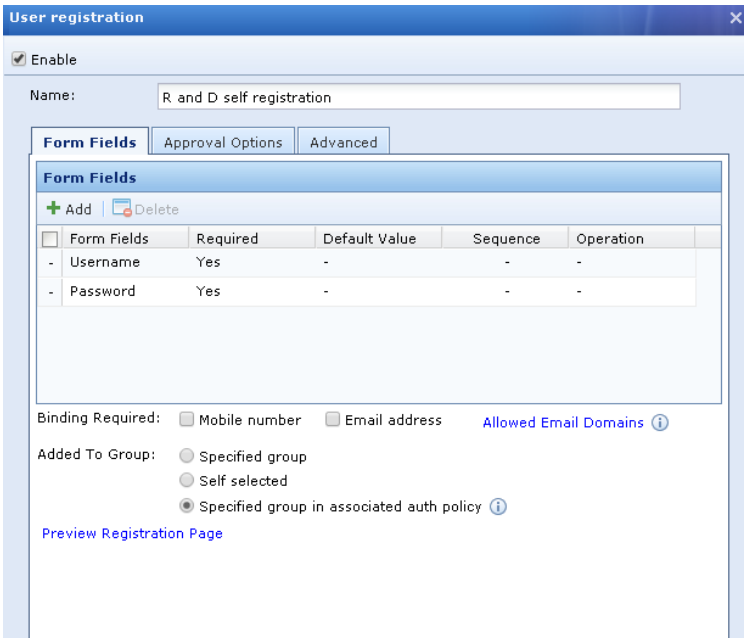
2.3.3 Configurations

2.3.3.1 Configure Self-Registration

Add new user registration.



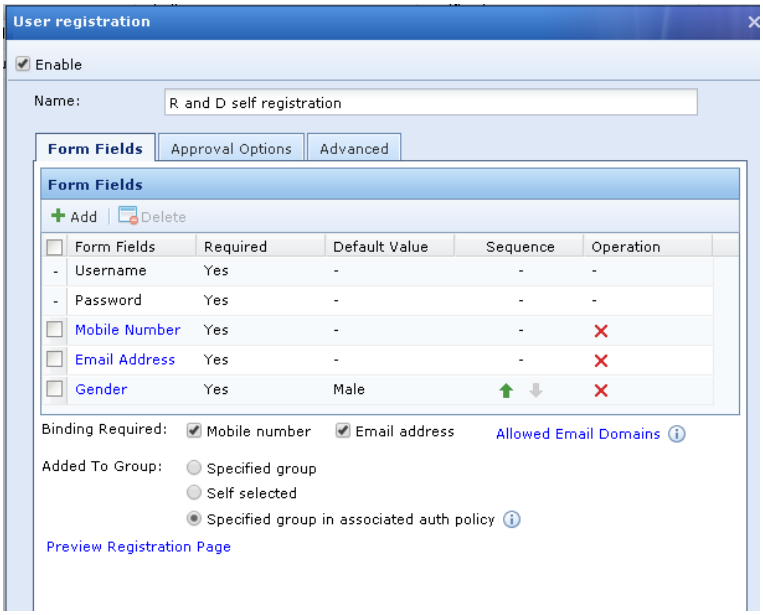
Form fields settings.



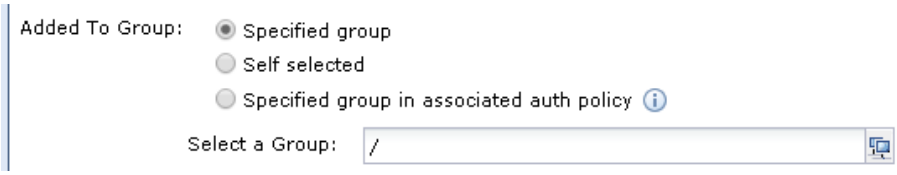
Form fields items: mobile number, email address, gender, birthday, etc. (the best analogy, the information required when registering at a forum).

Add content item, define form fields, default value (can be left blank), whether it is required.

Registration binding: support mobile phone number binding, email address binding. Can also be used to recover passwords.

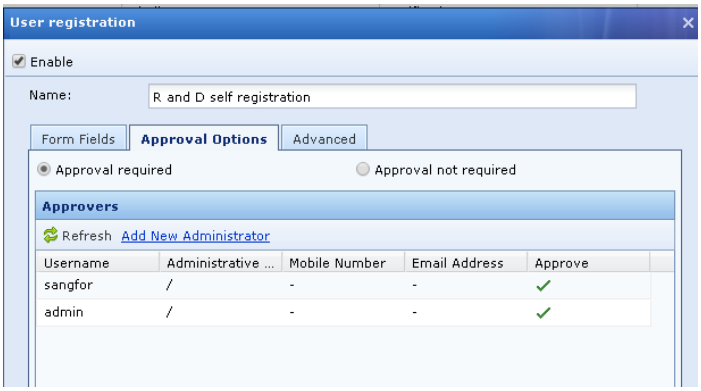


The group to which the registered user belongs: The local user can specify the specific group to which he belongs.

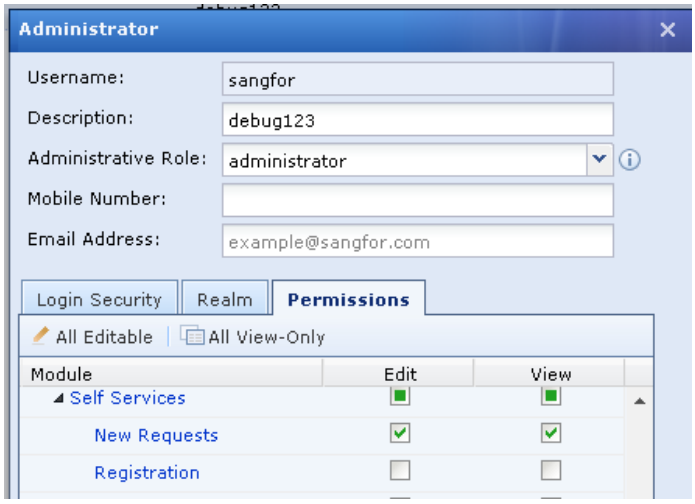


Approval Options

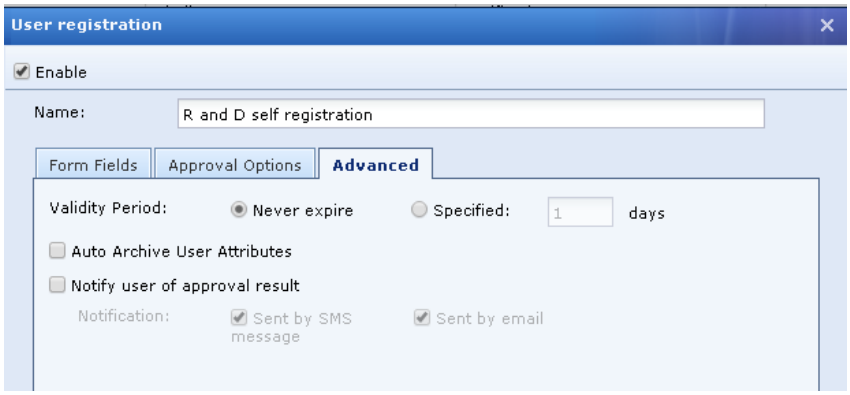
Whether the content entered by the self-registration needs approval, the administrator can decide at his own decision.



If approval is required, the new requests permission has to be given to the administrator.



Advanced



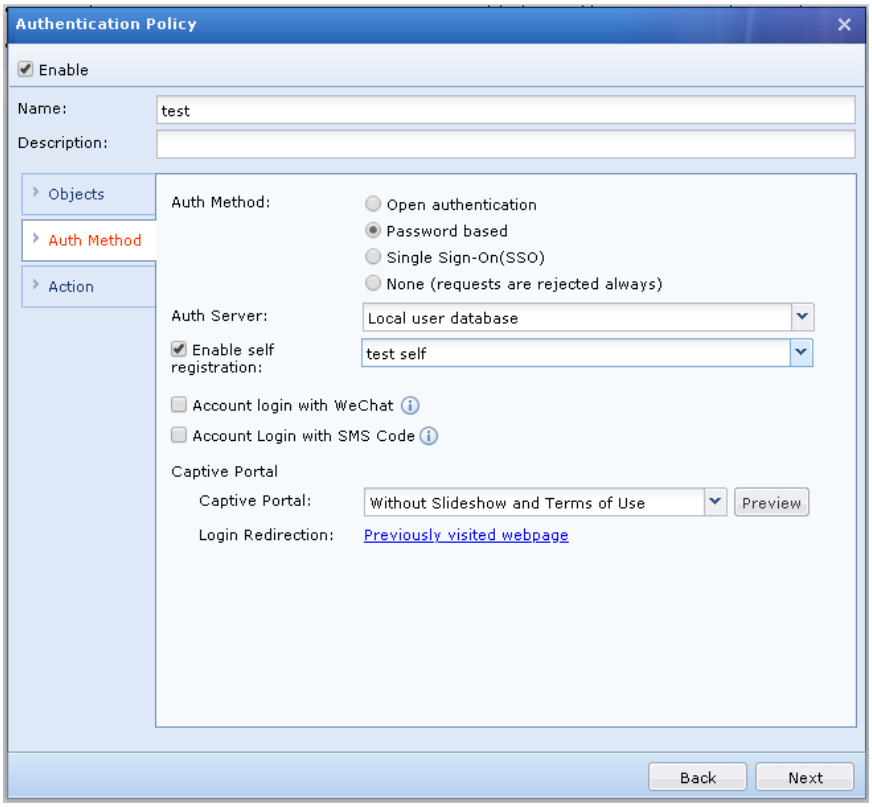
Account validlity period can be configured.

Account support to auto archive user attributes.

In the scenario where the administrator needs to approve, can select whether the approval result is notified to the user, optional (for SMS, SMS notification server needs to be available).

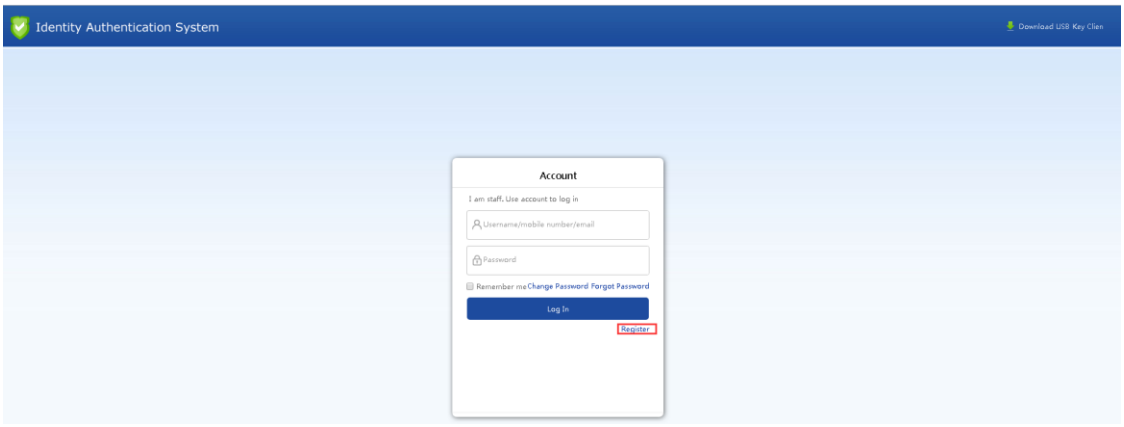
2.3.3.2 Configure Authentication Policy

Add new authentication policy-->Select password based authentication, the authentication server selects the local user authentication server, tick Enable self-registration, select the self-registration method-->Select the online group for authentication, and click Commit.

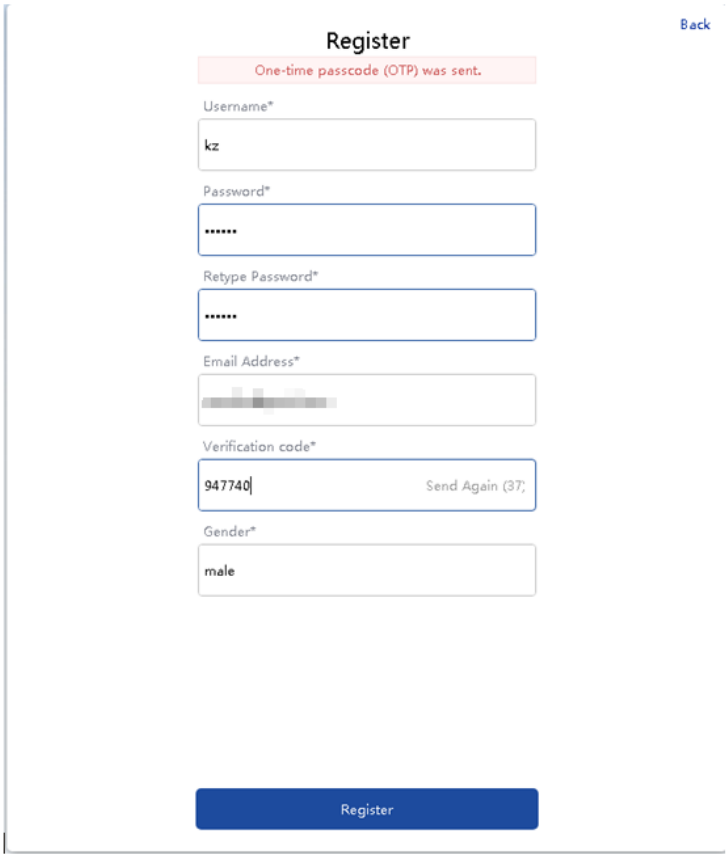


2.3.3.3 Testing Results

Visit any webpage and redirect to the authentication page. Since there is no account, click "Register" in the lower right corner.

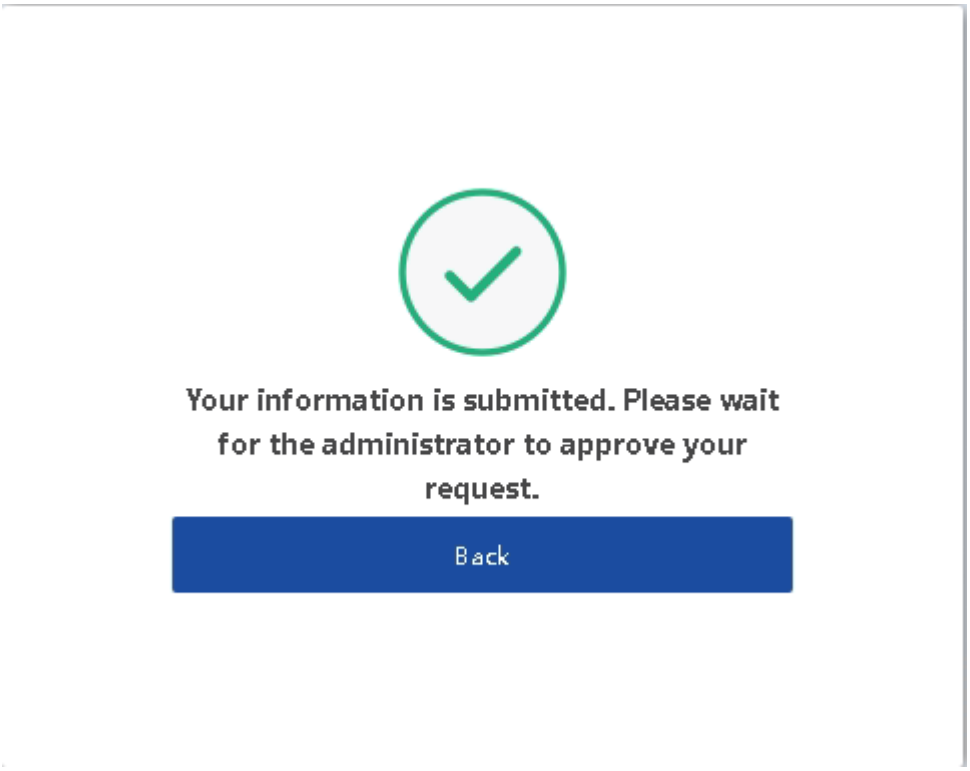


Enter the necessary information.



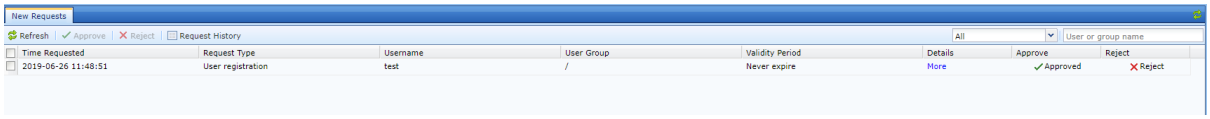
In approval not required scenario, after registration is completed, directly use the account password for authentication;

In approval required scenario, after information submission is completed, need to wait for administrator approve.



After the administrator receives the notification, log in to the device console and the request list

sees the account registration audit information:



Click Allow, user registration is completed,

Click Reject, user registration does not pass,

If the "Notify user of approval result" is configured, the registered user will be notified of an approval result.

After the registration is passed, the user can use the account password just registered to authenticate (if the account login with SMS code is configured, the login method can also be used to complete the authentication).

If the registration does not approve by admin, the user uses the registered account password to authenticate, the username and password will show invalid.

2.4 Endpoint Registration

2.4.1 Scenario

Open authentication, expect to log some personal information for management.

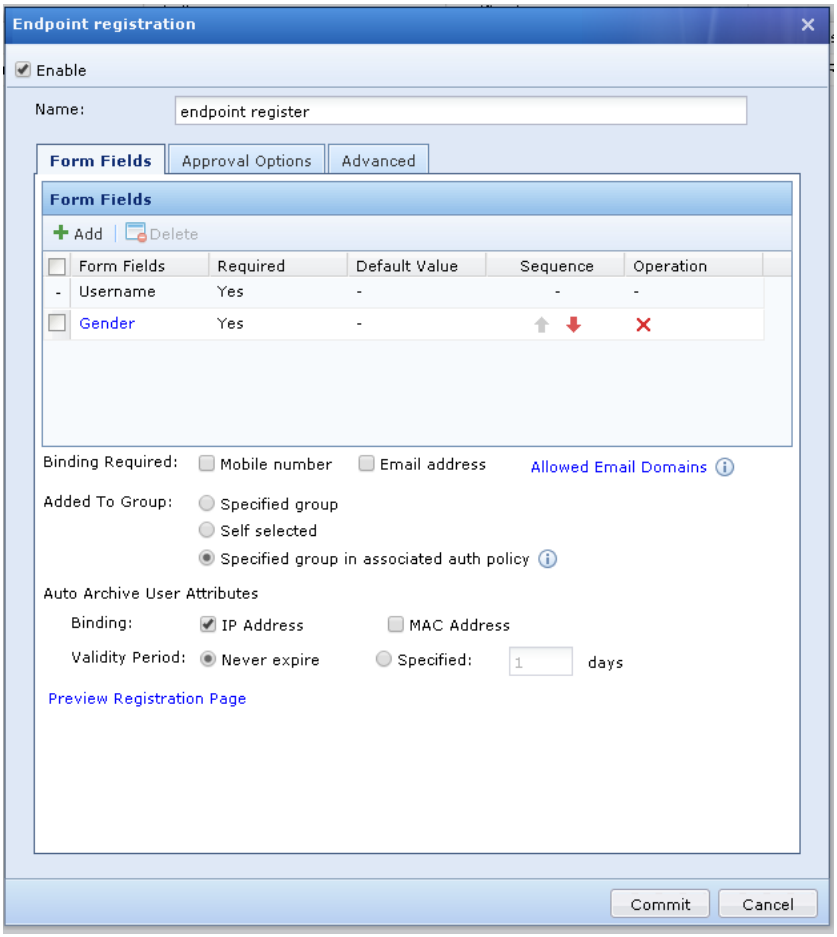
2.4.2 Which Authentication Methods Support Account Registration

Open authentication.

2.4.3 Configurations

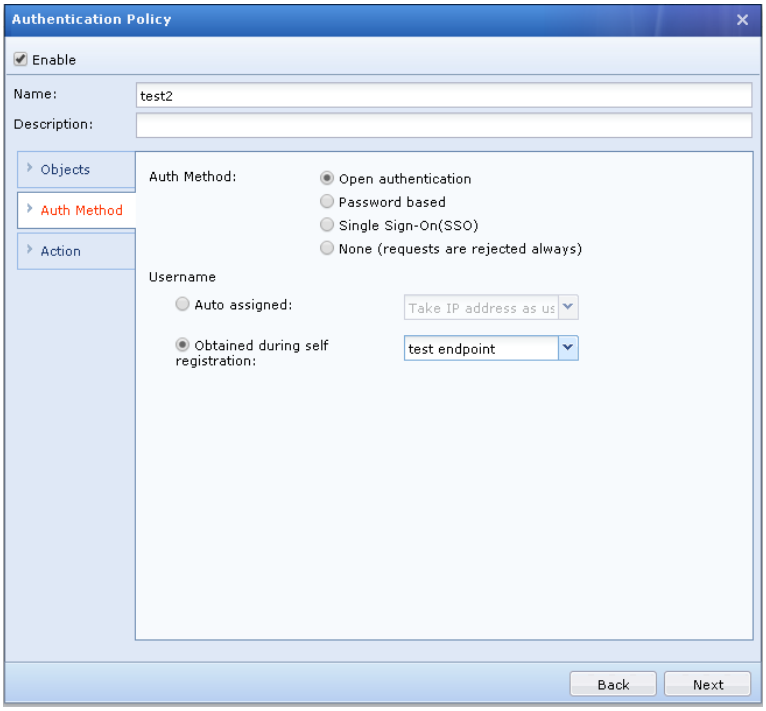
2.4.3.1 Configure Endpoint Self-Registration

Add new endpoint registration.

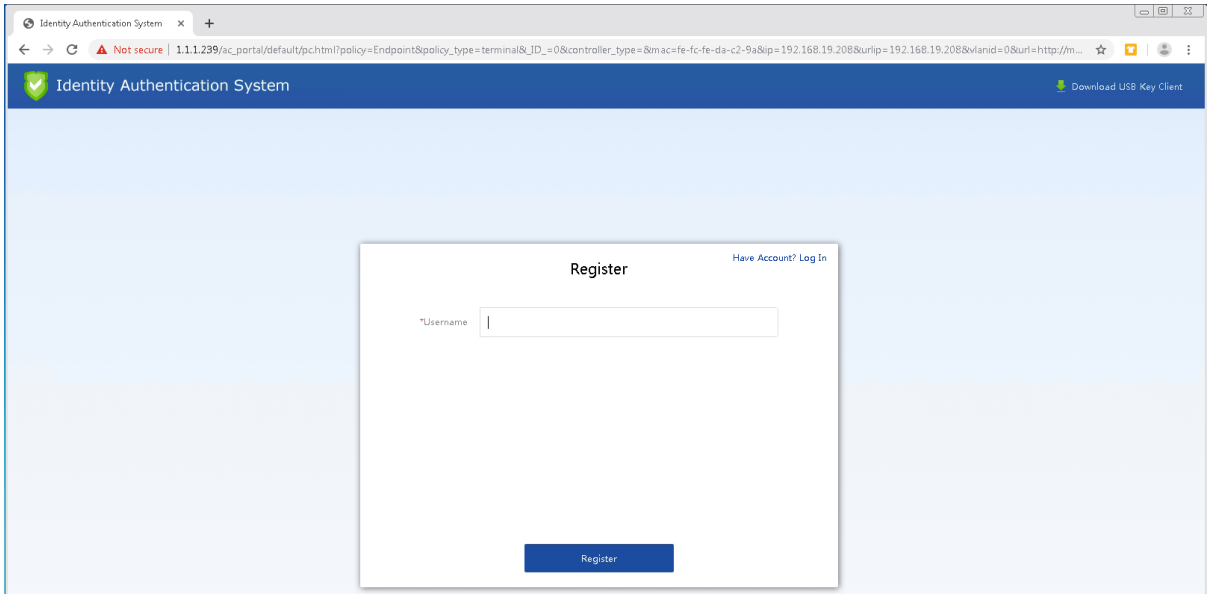


Approval options and advanced configuration methods are the same and will not be described again.

Use in authentication policy.

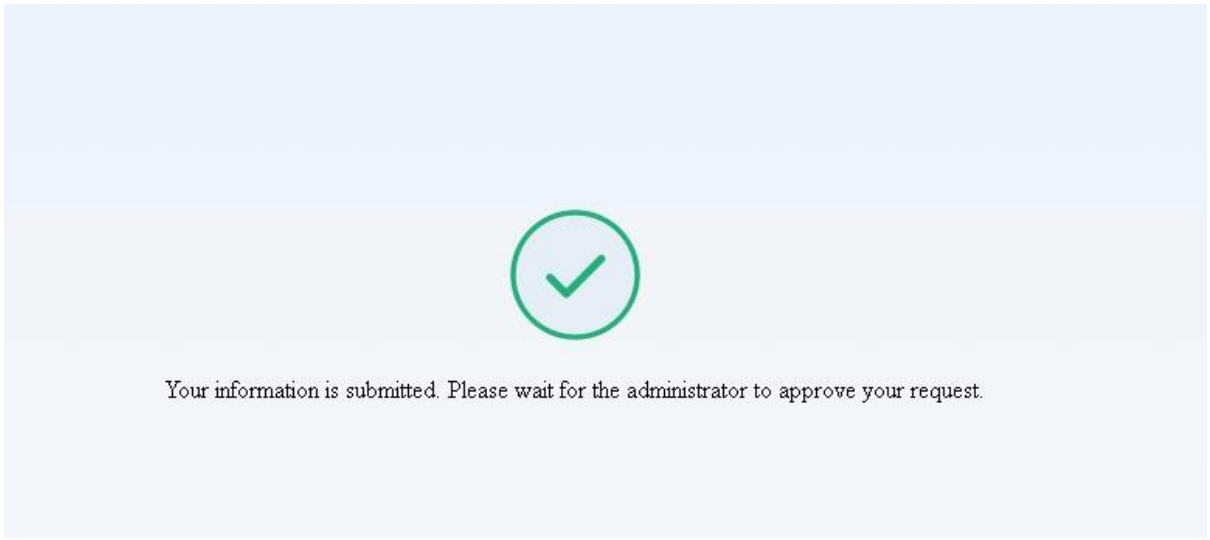


Visit any web page to pop up the registration page.

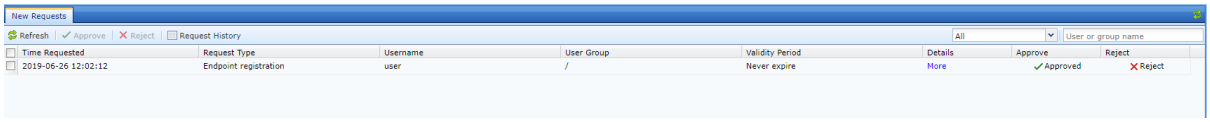


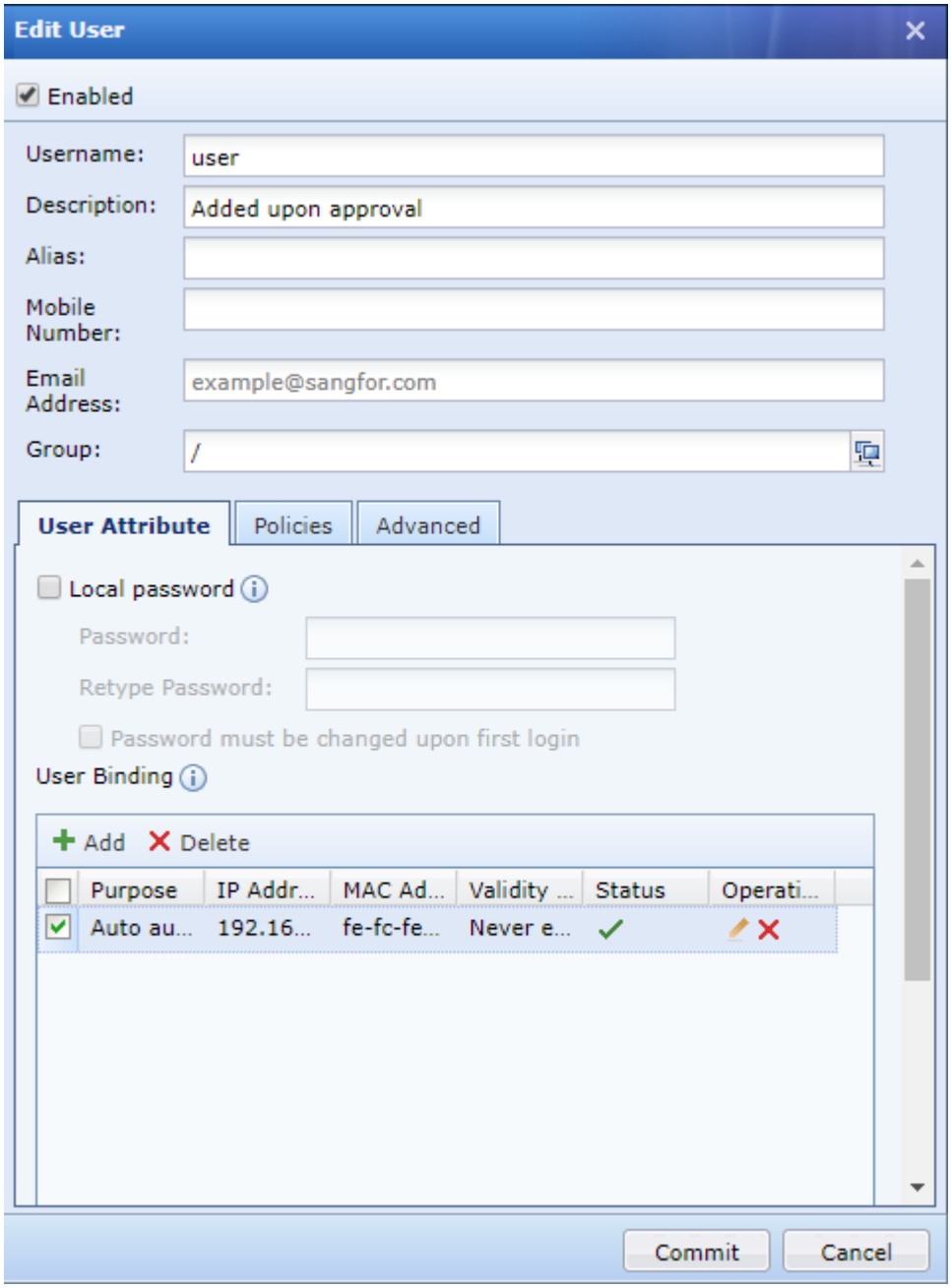
Approval not required, after input, can go online directly;

Approval required, after input, wait for the approval result.



After approval, can see the user information.





2.5 User Information Self-Management

2.5.1 Scenario

Personal information modification, etc.

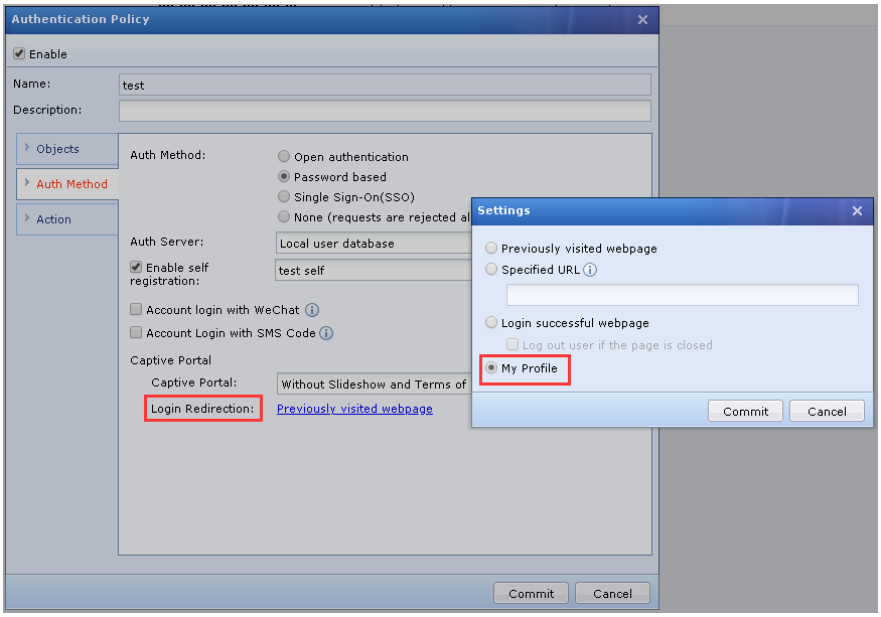
2.5.2 How To Access

Webpage is:

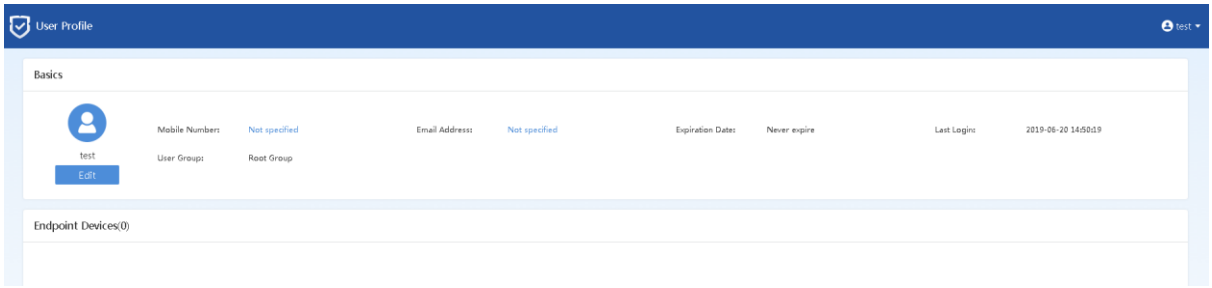
http://IAMIP/homepage/index.html?_FLAG=1

Manually access http://IAMIP (port 80) directly

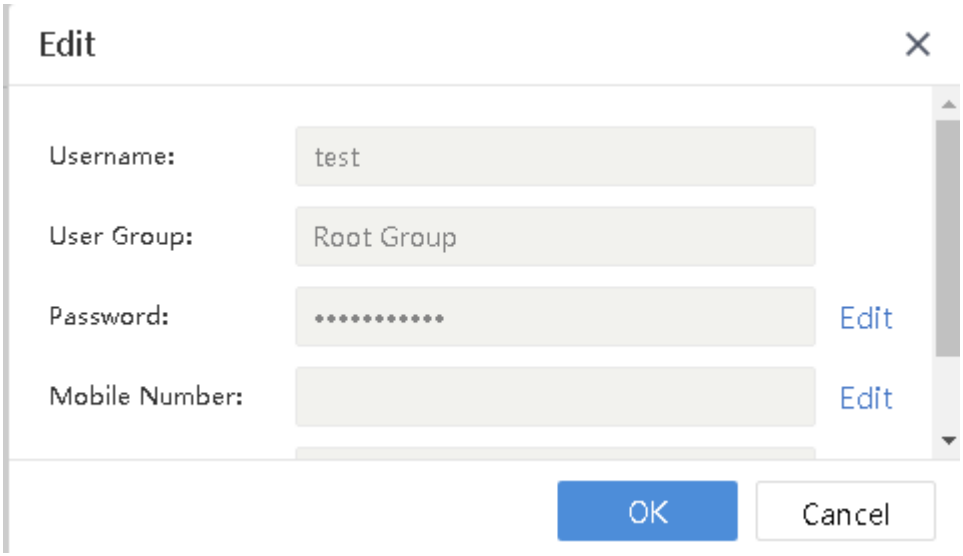
Use the login redirectionfunction to jump to the profile page.



2.5.3 My Profile

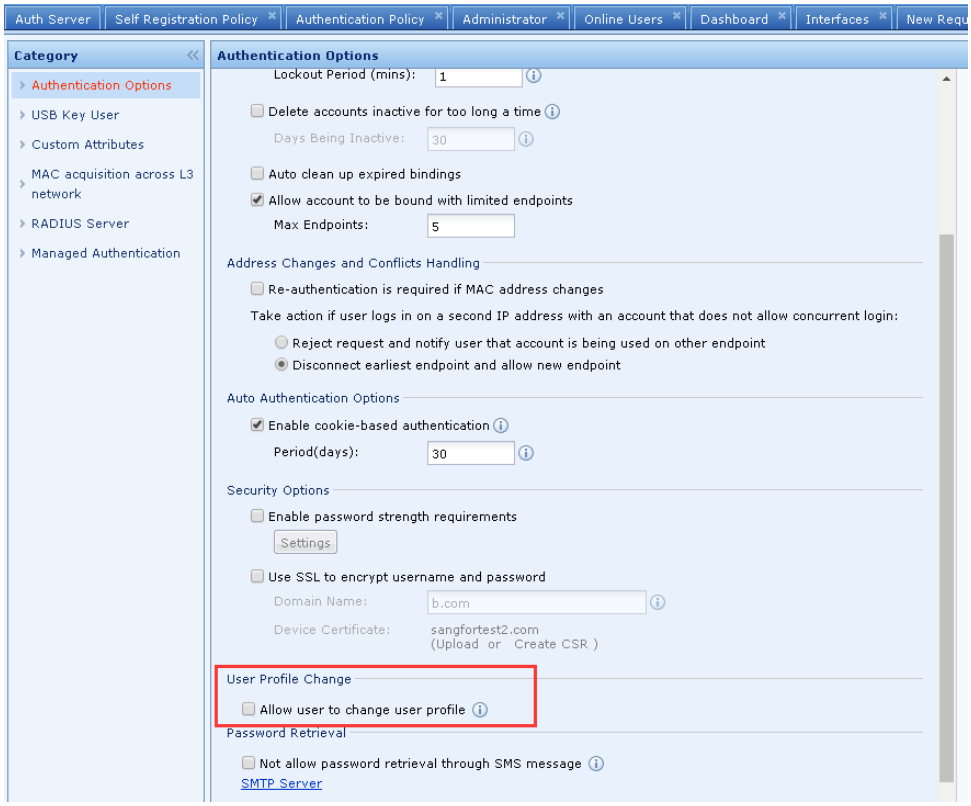


Click on edit.

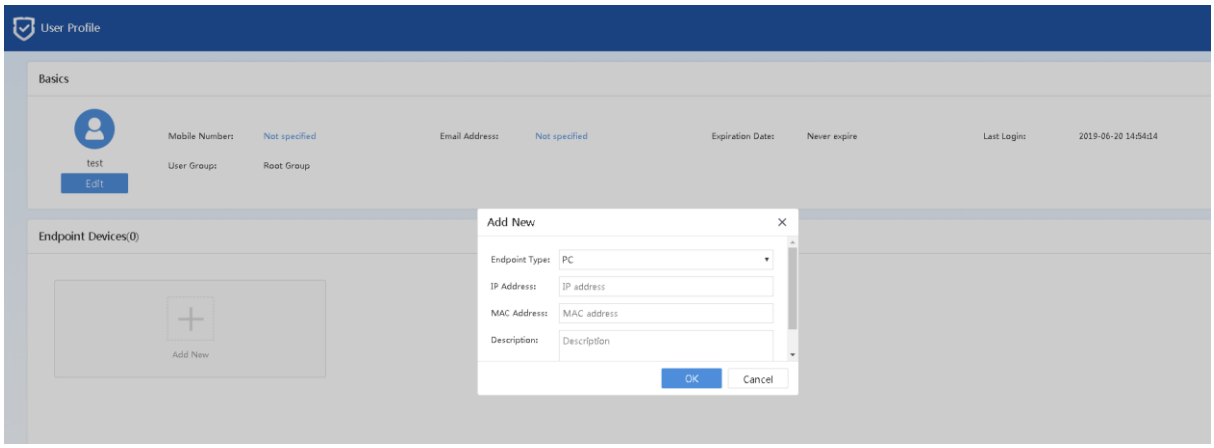


Bound endpoint can only be viewed by default.

[Users Advanced] – [User Profile Change] –Allow user to change user profile.



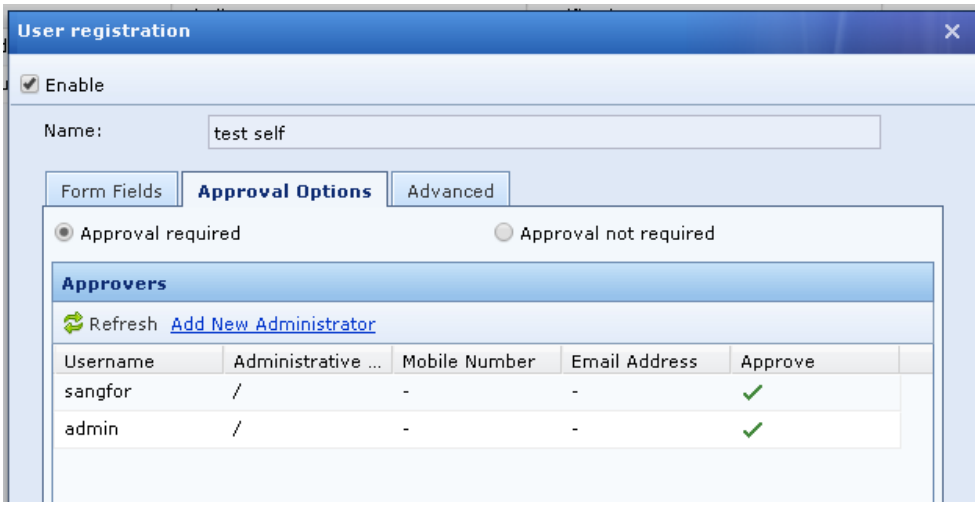
After ticked:



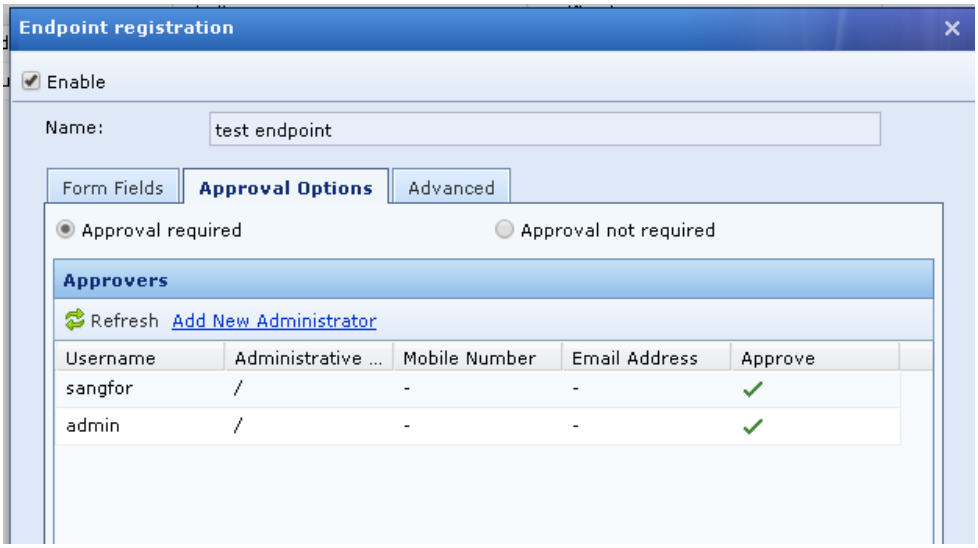
2.6 Self Registration Approval Options

Regardless of the user registration or the endpoint registration, when the user submits the registration information can be approved in two ways, one is approval not required, which means that after register success the account will become valid, and another one is approval required, indicating that the administrator who needs the corresponding group permission to approve only the account can take effect.

Self Registration Approval Options



Endpoint self-registration approval option



After the administrator logs in to the device, you can view the registration request submitted by the user in the request list. You can choose to allow or reject. If admin choose allow then the registration is valid, if reject the registration will not take effect. The user needs to resubmit the registration request.

Chapter 3 Precautions

1. Guest QR code authentication supports the logging of information items, but does not belong to self-registration, and the information filled in the QR code is only used for confirmation by the approver when reviewing.
2. Multiple approval administrators are configured. Can each administrator receive the information that needs to be approved?
3. The endpoint registration automatically binds the MAC address, acquistion across layer three network must be enabled across the layer three environment.

SANGFOR