



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.

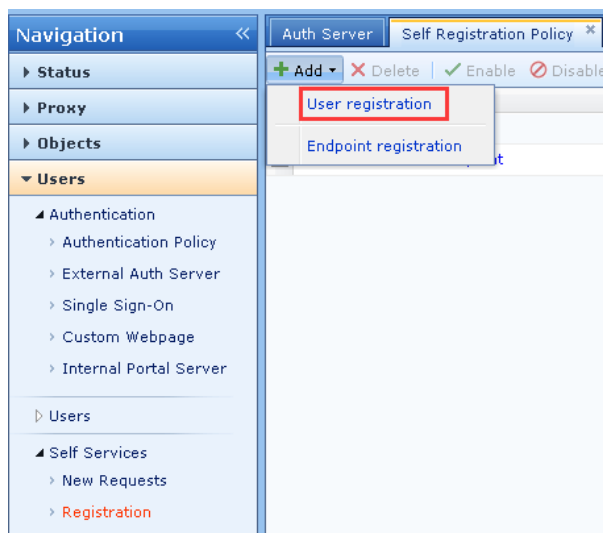
2.3.2 Which Authentication Methods Support Account Registration

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.

The 'User registration' configuration window is shown with the 'Form Fields' tab selected. The 'Name' field is set to 'R and D self registration'. Below the tabs, there is a table of form fields:

Form Fields	Required	Default Value	Sequence	Operation
- Username	Yes	-	-	-
- Password	Yes	-	-	-

Below the table, there are options for 'Binding Required' (Mobile number, Email address), 'Added To Group' (Specified group, Self selected, Specified group in associated auth policy), and a link to 'Preview Registration Page'.

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.

The 'Add New Field' dialog box is shown. It has three main sections: 'Form Fields' with a dropdown menu set to 'Gender', 'Default Value' with a text field set to 'Male', and 'Required' with radio buttons for 'Yes' and 'No'. At the bottom are 'Commit' and 'Cancel' buttons.

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

User registration

☒ Enable

Name:

Form Fields | Approval Options | Advanced

Form Fields

+ Add | Delete

Form Fields	Required	Default Value	Sequence	Operation
- Username	Yes	-	-	-
- Password	Yes	-	-	-
<input type="checkbox"/> Mobile Number	Yes	-	-	✗
<input type="checkbox"/> Email Address	Yes	-	-	✗
<input type="checkbox"/> Gender	Yes	Male	↑ ↓	✗

Binding Required: ☒ Mobile number ☒ Email address [Allowed Email Domains](#) ⓘ

Added To Group: ☐ Specified group ☐ Self selected ☐ Specified group in associated auth policy ⓘ

[Preview Registration Page](#)

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

Added To Group: ☒ Specified group ☐ Self selected ☐ Specified group in associated auth policy ⓘ

Select a Group:

Approval Options

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

User registration

☒ Enable

Name:

Form Fields | **Approval Options** | Advanced

☒ Approval required ☐ Approval not required

Approvers

Refresh [Add New Administrator](#)

Username	Administrative ...	Mobile Number	Email Address	Approve
sangfor	/	-	-	✓
admin	/	-	-	✓

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

Administrator

Username: sangfor
 Description: debug123
 Administrative Role: administrator
 Mobile Number:
 Email Address: example@sangfor.com

Login Security | Realm | **Permissions**

All Editable | All View-Only

Module	Edit	View
Self Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
New Requests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Registration	<input type="checkbox"/>	<input type="checkbox"/>

Advanced

User registration

☒ Enable

Name: R and D self registration

Form Fields | Approval Options | **Advanced**

Validity Period: ☒ Never expire ☐ Specified: 1 days

☐ Auto Archive User Attributes

☐ Notify user of approval result

Notification: ☒ Sent by SMS message ☒ Sent by email

Account validity 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.

Authentication Policy

☒ Enable

Name: test

Description:

> Objects
 > **Auth Method**
 > Action

Auth Method:

- ☐ Open authentication
- ☒ Password based
- ☐ Single Sign-On(SSO)
- ☐ None (requests are rejected always)

Auth Server: Local user database

☒ Enable self registration: test self

☐ Account login with WeChat ⓘ

☐ Account Login with SMS Code ⓘ

Captive Portal

Captive Portal: Without Slideshow and Terms of Use Preview

Login Redirection: [Previously visited webpage](#)

Back Next

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.

Identity Authentication System Download USB Key Client

Account

I am staff, Use account to log in

Username/mobile number/email

Password

☐ Remember me Change Password Forgot Password

Log In Register

Enter the necessary information.

Back

Register

One-time passcode (OTP) was sent.

Username*

kz

Password*

Retype Password*

Email Address*

Verification code*

947740

Send Again (37s)


Gender*

male

Register

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.



Your information is submitted. Please wait for the administrator to approve your request.

Back

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

W.: www.sangfor.com | W.: community.sangfor.com | E.: tech.support@sangfor.com

sees the account registration audit information:

Time Requested	Request Type	Username	User Group	Validity Period	Details	Approve	Reject
2019-06-26 11:48:51	User registration	test	/	Never expire	More	✓ Approved	✗ Reject

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.



Endpoint registration

☒ Enable

Name:

Form Fields | Approval Options | Advanced

Form Fields

+ Add | Delete

Form Fields	Required	Default Value	Sequence	Operation
- Username	Yes	-	-	-
- Gender	Yes	-	↑ ↓	✖

Binding Required: ☐ Mobile number ☐ Email address [Allowed Email Domains](#) ⓘ

Added To Group: ☐ Specified group
☐ Self selected
☒ Specified group in associated auth policy ⓘ

Auto Archive User Attributes

Binding: ☒ IP Address ☐ MAC Address

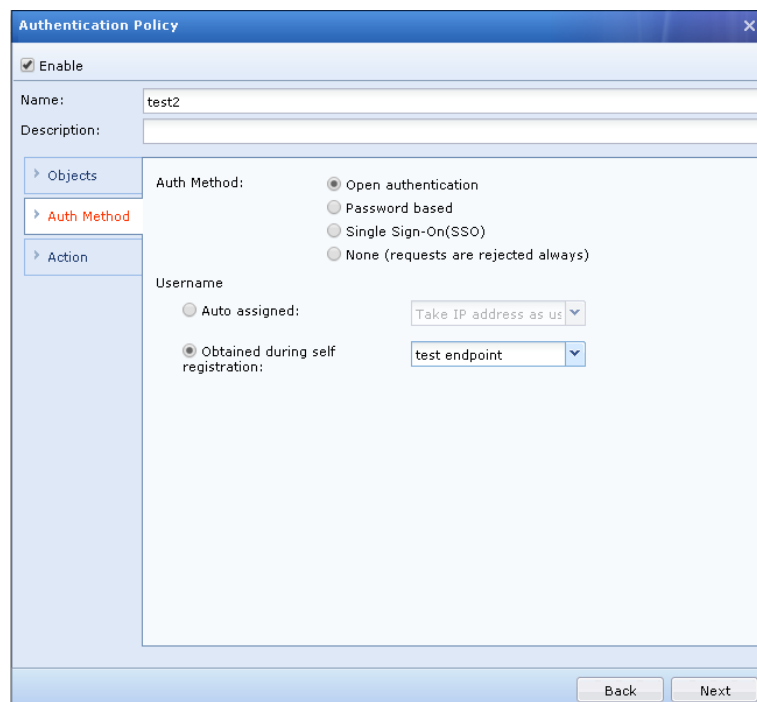
Validity Period: ☒ Never expire ☐ Specified: days

[Preview Registration Page](#)

Commit Cancel

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

Use in authentication policy.



Authentication Policy

☒ Enable

Name:

Description:

Objects | **Auth Method** | Action

Auth Method: ☒ Open authentication
☐ Password based
☐ Single Sign-On(SSO)
☐ None (requests are rejected always)

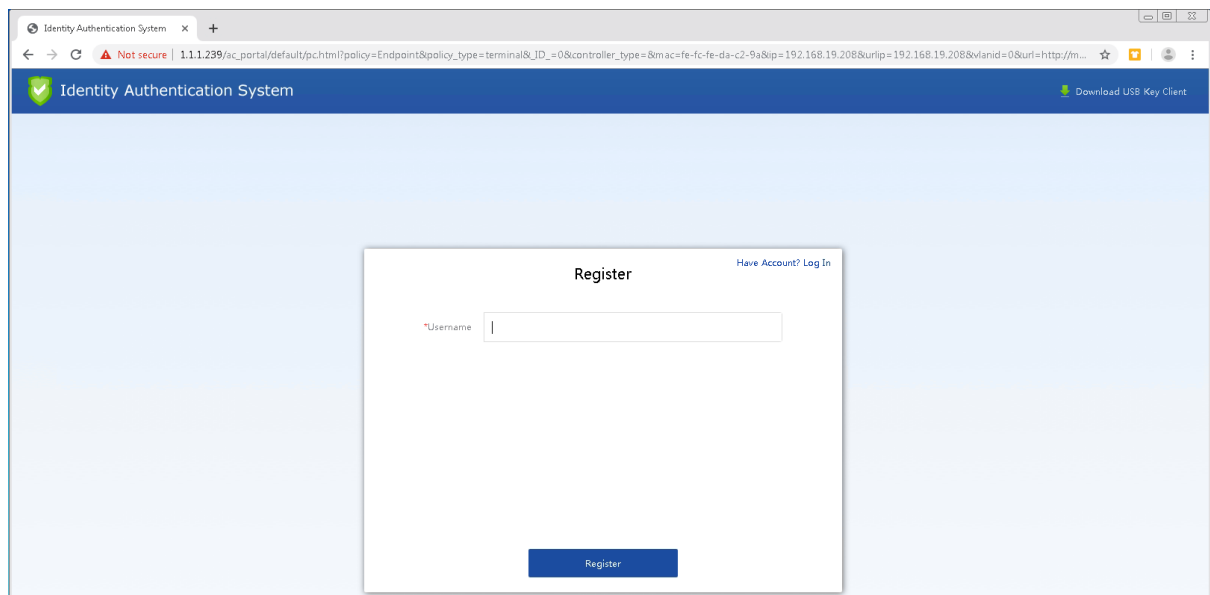
Username

☐ Auto assigned:

☒ Obtained during self registration:

Back Next

Visit any web page to pop up the registration page.



Identity Authentication System

Download USB Key Client

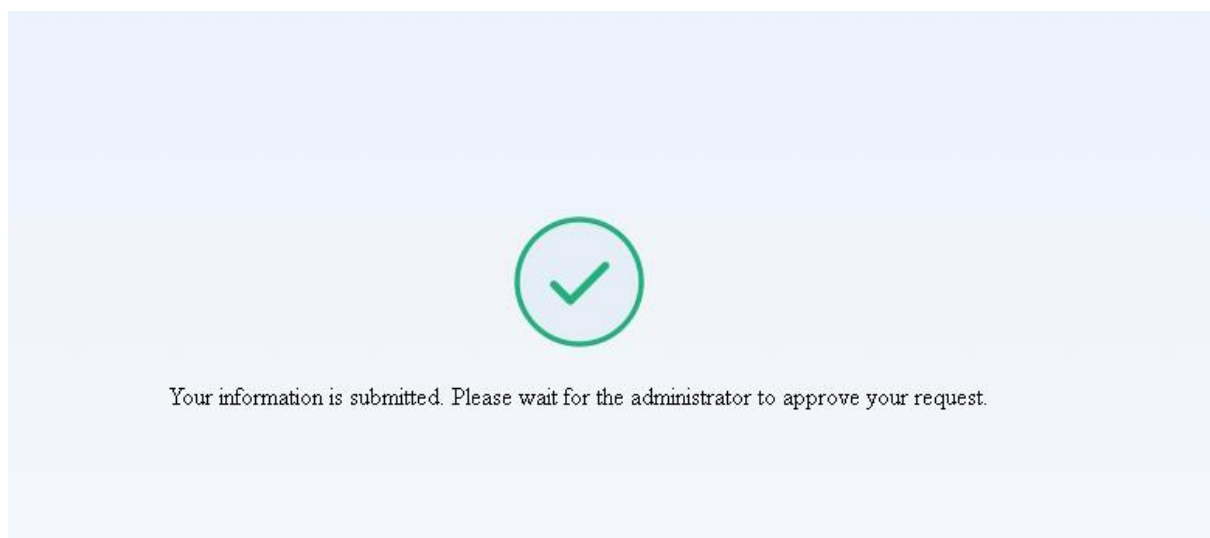
Register

Have Account? Log In

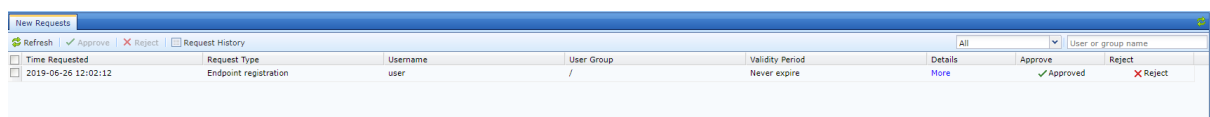
Username

Register

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.



New Requests						
Refresh Approve Reject Request History						
Time Requested	Request Type	Username	User Group	Validity Period	Details	Approve Reject
2019-06-26 12:02:12	Endpoint registration	user	/	Never expire	More	✓ Approved ✗ Reject

Edit User

☒ Enabled

Username:

Description:

Alias:

Mobile Number:

Email Address:

Group:

User Attribute | Policies | Advanced

☐ Local password ⓘ

Password:

Retype Password:

☐ Password must be changed upon first login

User Binding ⓘ

+ Add - Delete

	Purpose	IP Addr...	MAC Ad...	Validity ...	Status	Operati...
<input checked="" type="checkbox"/>	Auto au...	192.16...	fe-fc-fe...	Never e...	✓	✎ ✕

Commit Cancel

2.5 User Information Self-Management

2.5.1 Scenario

Personal information modification, etc.

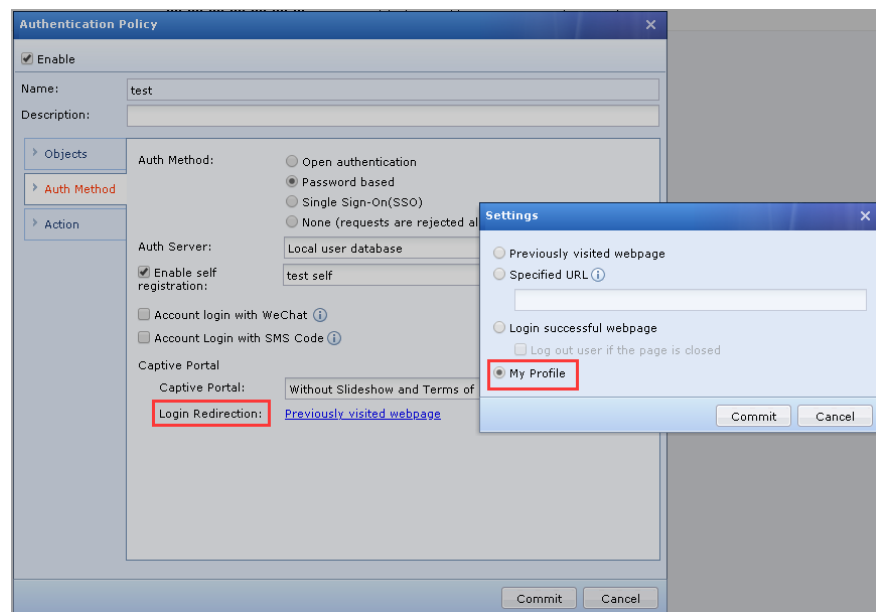
2.5.2 How To Access

Webpage is:

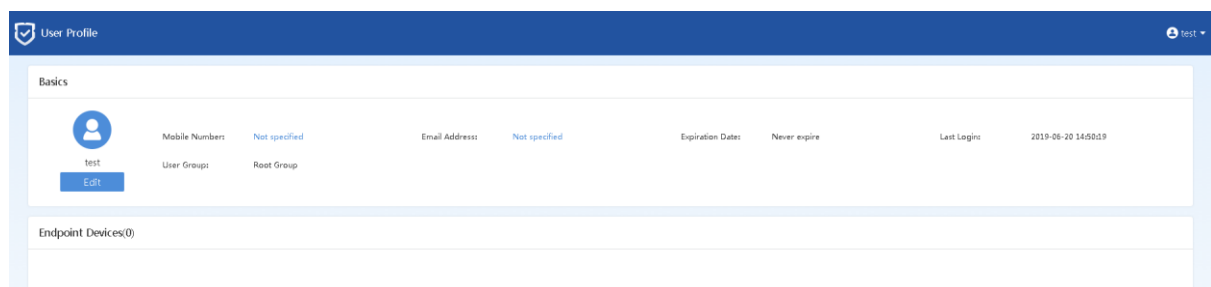
http://IAMIP/homepage/index.html?_FLAG=1

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.

The 'Edit' dialog box contains the following fields and controls:

- Username:** test
- User Group:** Root Group
- Password:** [masked] [Edit](#)
- Mobile Number:** [empty] [Edit](#)
- Buttons:** OK, Cancel

Bound endpoint can only be viewed by default.

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

The screenshot shows the 'Authentication Options' configuration page. The left sidebar lists categories: Authentication Options, USB Key User, Custom Attributes, MAC acquisition across L3 network, RADIUS Server, and Managed Authentication. The main content area is titled 'Authentication Options' and contains several sections:

- Lockout Period (mins):** 1
- ☐ Delete accounts inactive for too long a time
- Days Being Inactive:** 30
- ☐ Auto clean up expired bindings
- ☒ Allow account to be bound with limited endpoints
- Max Endpoints:** 5
- Address Changes and Conflicts Handling**
 - ☐ Re-authentication is required if MAC address changes
 - Take action if user logs in on a second IP address with an account that does not allow concurrent login:
 - ☐ Reject request and notify user that account is being used on other endpoint
 - ☒ Disconnect earliest endpoint and allow new endpoint
- Auto Authentication Options**
 - ☒ Enable cookie-based authentication
 - Period(days):** 30
- Security Options**
 - ☐ Enable password strength requirements (Settings)
 - ☐ Use SSL to encrypt username and password
 - Domain Name:** b.com
 - Device Certificate:** sangfortest2.com (Upload or Create CSR)
- User Profile Change** (highlighted with a red box)
 - ☐ Allow user to change user profile
- Password Retrieval**
 - ☐ Not allow password retrieval through SMS message

After ticked:

The screenshot shows the 'User Profile' configuration page for a user named 'test'. The 'Basics' tab is active, showing fields for Mobile Number, Email Address, Expiration Date, and Last Login. Below this, there is a section for 'Endpoint Devices(0)' with an 'Add New' button. An 'Add New' dialog box is open, showing fields for Endpoint Type, IP Address, MAC Address, and Description. The dialog box has 'OK' and 'Cancel' buttons.

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

User registration

☒ Enable

Name:

Form Fields **Approval Options** Advanced

☒ Approval required ☐ Approval not required

Approvers

[Refresh](#) [Add New Administrator](#)

Username	Administrative ...	Mobile Number	Email Address	Approve
sangfor	/	-	-	✓
admin	/	-	-	✓

Endpoint self-registration approval option

Endpoint registration

☒ Enable

Name:

Form Fields **Approval Options** Advanced

☒ Approval required ☐ Approval not required

Approvers

[Refresh](#) [Add New Administrator](#)

Username	Administrative ...	Mobile Number	Email Address	Approve
sangfor	/	-	-	✓
admin	/	-	-	✓

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.

SANGFOR | SG12.0.25 | 发帖求助 | 在线咨询 | 社区提问、资料搜索 | admin | [行为感知系统 HOT]

导航菜单: 实时状态, 对象定义, 用户认证与管理, 用户管理, 用户自助服务, 认证高级选项

自注册设置 | 认证高级选项 | 认证策略 | **审批列表**

刷新 ☒ 批量通过 ☒ 批量拒绝 | 历史审批记录 | 所有 | 请输入用户名或用户组进行:

申请时间	申请类型	用户名	用户组	账号有效天数	详细信息	通过操作	拒绝操作
2019-05-12 23:42:27	终端注册	test	/	永不过期	更多信息	✓通过	✗拒绝

注册策略: test1
 邮箱: 123456@qq.com
 性别: 男
 IP地址: 200.200.64.39
 MAC地址: 00-00-00-00-00-00
 绑定目的: 免认证
 绑定MAC: 是
 绑定IP: 是
 绑定过期天数: 永不过期

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, acquisition across layer three network must be enabled across the layer three environment.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

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. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc