



IAM

**Log in using an administrator account in conjunction with
an external authentication server**

Version 12.0.23



Change Log

Date	Change Description
April 25, 2019	Version 12.0.23 document release.

CONTENT

Chapter 1 Content requirements	错误!未定义书签。
1 Document title	错误!未定义书签。
2 Product Version.....	1
3 Interface menu, option and screenshot	错误!未定义书签。
3.1 Interface menu and options	错误!未定义书签。
3.2 Interface Screenshot.....	错误!未定义书签。
4 List and Number	错误!未定义书签。
4.1 List	错误!未定义书签。
4.2 Number	错误!未定义书签。
4.3 Number	错误!未定义书签。
5 Proofing	错误!未定义书签。
6 Fonts	错误!未定义书签。
6.1 Fonts format	错误!未定义书签。
6.2 Fonts download sites:	错误!未定义书签。
6.3 Pre-created Fonts style	错误!未定义书签。
7 Highlight	错误!未定义书签。
7.1 Notes	错误!未定义书签。
7.2 Picture highlight	错误!未定义书签。
7.3 Text Highlight	错误!未定义书签。

1 Interfacing with the Tacacs+ server

1.1 Configuration example

- The IP of the tacacs+ server is 10.130.27.14
- Username tacacstest password test123456
- Port 7777

1.2 Configuration method

- Log in to the device console with the admin account and go to **System - General - Administrator**.

The screenshot shows the 'External Auth Server' configuration window. The 'General' section contains a table with the following data:

No.	Username
1	admin

The 'TACACS+ Server' section contains the following configuration:

- Server Name: [Empty]
- Authentication Options: Tacacs+
- IP Address: [Empty]
- Server Port: 49
- Timeout(sec): 15
- Shared Secret: [Empty]
- Authentication: CHAP

- Select the tacacs+ server at the external authentication server and fill in the relevant information.

External Auth Server

☒ Enable

Server Name: TACACS

Authentication Options: Tacacs+

TACACS+ Server

IP Address: 10.130.27.14

Server Port: 7777

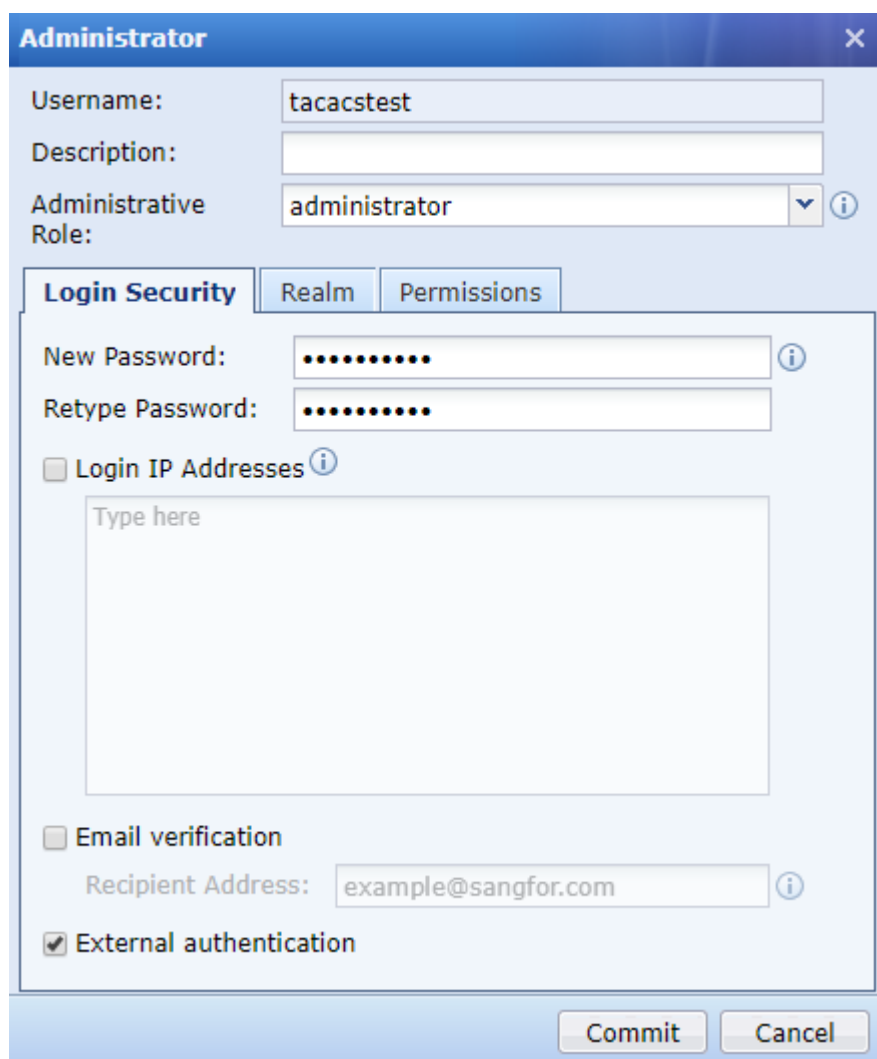
Timeout(sec): 15

Shared Secret:

Authentication: PAP

Test Validity Commit Cancel

- Add an administrator account, fill in the username on the server, and enable "**External authentication**".



Administrator

Username:

Description:

Administrative Role: ⓘ

Login Security | **Realm** | **Permissions**

New Password: ⓘ

Retype Password:

☐ Login IP Addresses ⓘ

Type here

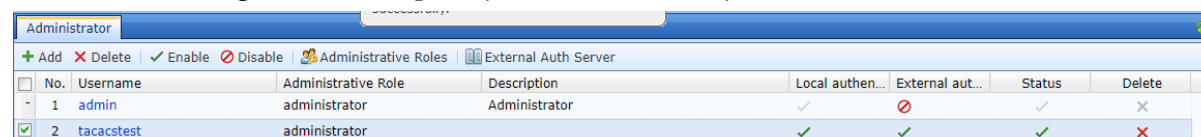
☐ Email verification

Recipient Address: ⓘ

☒ External authentication

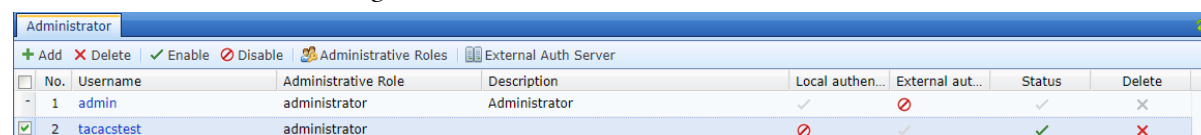
Commit **Cancel**

- After the configuration is complete, you can see the newly created user.



No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✗
2	tacacstest	administrator		✓	✓	✓	✗

- Cancel this account and log in as a local account.



No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✗
2	tacacstest	administrator		✗	✓	✓	✗

- Log in to the console with the tacacstest account.



2 Interfacing with the Radius server

2.1 Configuration example

- The IP of the radius server is **192.200.244.241**
- Username **radiustest** password **test123456**

- Port 1812

2.2 Configuration method

- Log in to the device console with the admin account and go to **System - General – Administrator**.

The screenshot shows the 'Administrator' console window. On the left, there is a table with columns 'No.' and 'Username'. The table contains one entry: '1' and 'admin'. On the right, the 'External Auth Server' configuration window is open. It has a tab labeled 'External Auth Server'. Inside the window, there is a checkbox labeled 'Enable' which is checked. Below this, there are several fields: 'Server Name:' (empty), 'Authentication Options:' (a dropdown menu showing 'Radius'), and a section titled 'RADIUS Server' containing 'IP Address:' (empty), 'Port:' (1812), 'Timeout(sec):' (15), 'Shared Secret:' (empty), and 'Protocol:' (a dropdown menu showing 'CHAP'). At the bottom of the window, there are three buttons: 'Test Validity', 'Commit', and 'Cancel'.

- Select the radius server at the external authentication server and fill in the relevant information.

External Auth Server

☒ Enable

Server Name: RADIUS

Authentication Options: Radius

RADIUS Server

IP Address: 192.200.244.241

Port: 1812

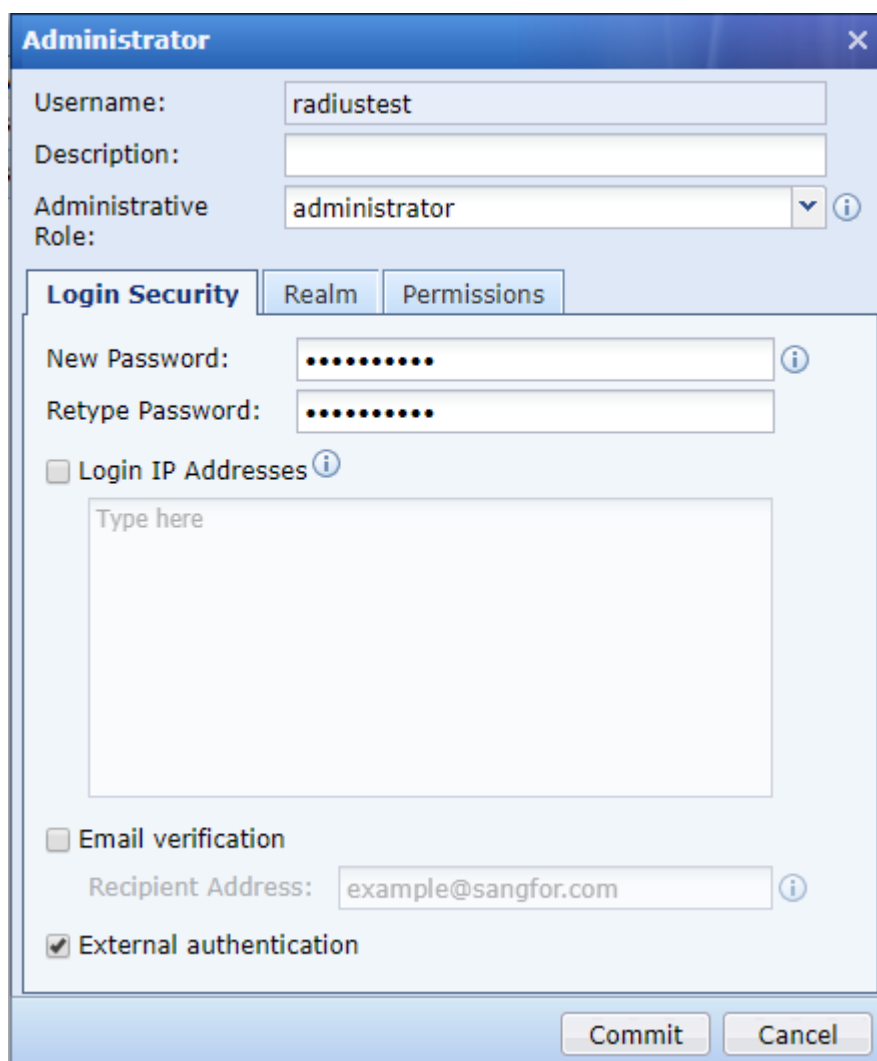
Timeout(sec): 15

Shared Secret:

Protocol: CHAP

Test Validity Commit Cancel

- Add an administrator account, fill in the username on the server, and enable "**External authentication**".



Administrator

Username: radiustest

Description:

Administrative Role: administrator

Login Security | Realm | Permissions

New Password:

Retype Password:

☐ Login IP Addresses

Type here

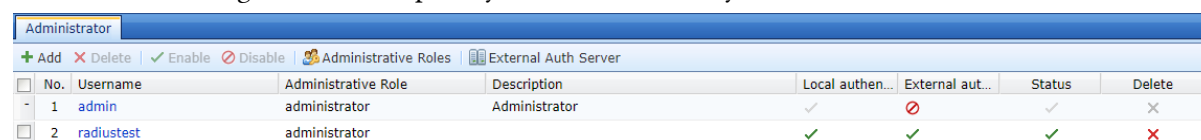
☐ Email verification

Recipient Address: example@sangfor.com

☒ External authentication

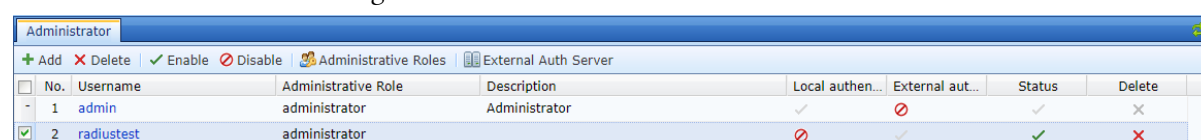
Commit Cancel

- After the configuration is complete, you can see the newly created user.



No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✕
2	radiustest	administrator		✓	✓	✓	✕

- Cancel this account and log in as a local account.



No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✕
2	radiustest	administrator		✗	✓	✓	✕

- Log in to the console with the tacacstest account.



3 Interfacing with the LDAP server

2.1 Configuration example

- The IP of the radius server is **192.168.19.89**
- Username **ldapstest** password **test123456**

- Port 389

3.2 Configuration method

- Log in to the device console with the admin account and go to **System - General – Administrator**.
- Select the ldap server at the external authentication server and fill in the relevant information.

External Auth Server

☒ Enable

Server Name: LDAP

Authentication Options: LDAP

LDAP Server

Type: MS Active Directory

IP Address: 192.168.19.89

Port: 389

User Attribute: sAMAccountName

User Filter: (!(objectClass=user)(objectClass=person))

Timeout(sec): 15

Search: ☐ Anonymous

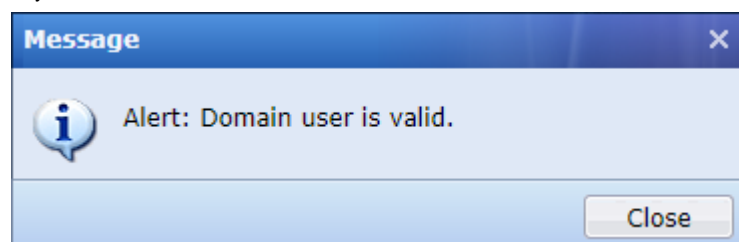
Admin DN: Admin DN or name of the server admin account

Admin Password:

BaseDN: DC=SCCORP,DC=local

Test Validity Commit Cancel

- Test account validity.



- Add an administrator account, fill in the username on the server, and enable "**External authentication**".

Administrator

Username:

Description:

Administrative Role:

Login Security | Realm | Permissions

Retype Password:

☐ Login IP Addresses

Type here

☐ Email verification

Recipient Address:

☒ External authentication

- After the configuration is complete, you can see the newly created user.

No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✗
2	ldaptest	administrator		✓	✓	✓	✗

- Cancel this account and log in as a local account.

No.	Username	Administrative Role	Description	Local authen...	External aut...	Status	Delete
1	admin	administrator	Administrator	✓	✗	✓	✗
2	ldaptest	administrator		✗	✓	✓	✗

- Log in to the console with the tacacstest account.



4 Note

- The three external authentication server options can only choose one type of use, and do not support simultaneous selection.
- The TACACS+ external authentication service does not support IPv6, and the RADIUS external authentication server and the LDAP external authentication service support IPv6.
- Local authentication and external authentication must be checked one.
- If both local and external authentication are selected, local authentication is preferred.



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