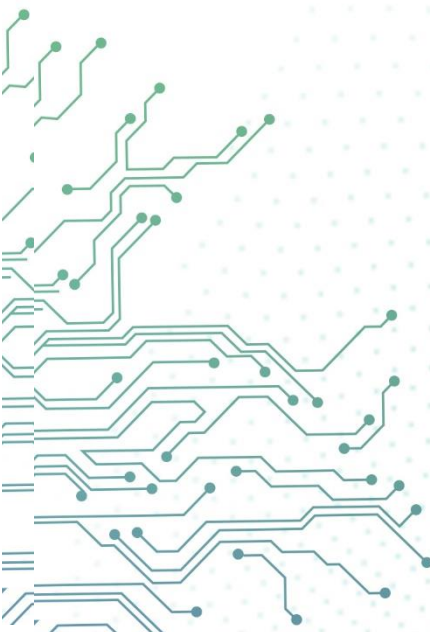




aCloud

Google OTP Configuration Guides

Version 5.8.8R1



Change Log

Date	Change Description
Sept 25, 2019	Version 5.8.8R1 document release.

CONTENT

Chapter 1 Background	1
Chapter 2 Configuration guidelines.....	1
2.1 Enable Google OTP services	1
2.2 First time verification	3

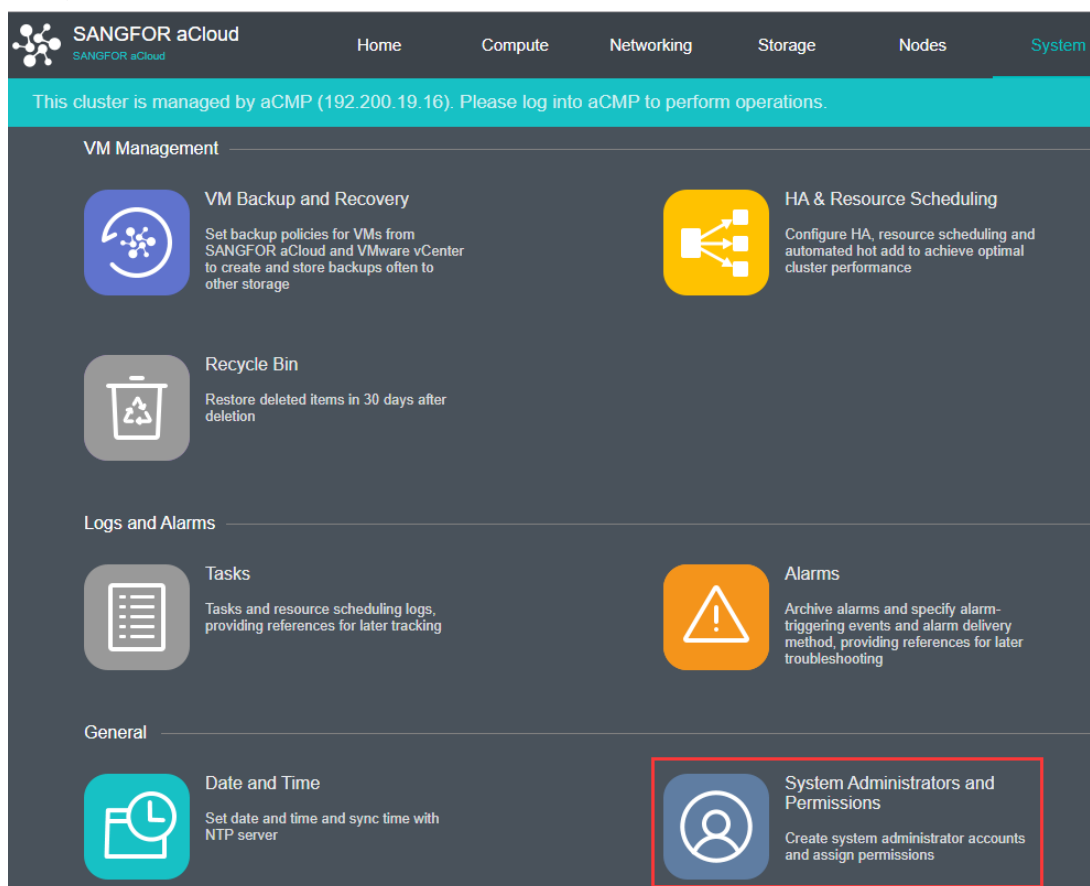
Chapter 1 Background

Sangfor aCloud 5.8.8R1 introduces 2 factors authentication method via Google OTP. Google Authenticator is a software-based authenticator that implements two-step verification services using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm, for authenticating users of mobile applications by Google.

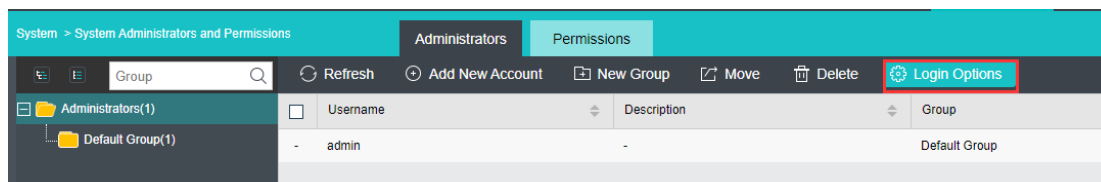
Chapter 2 Configuration guidelines

2.1 Enable Google OTP services

1. Navigate to [System] – [System Administrators and Permissions]



2. Click on the Login Options



3. Enable Google Authenticator OTP.

Login Options

Concurrent Login: ☐ Enabled ☒ Disabled
Choose whether an account can be used to log in on more than one IP addresses.

Login Restrictions:

- Max Attempts : 5
- Login Interval : 1 sec
- Session Timeout : 24 hours

Google Authenticator OTP: ☒ Enabled ☐ Disabled

To send verification code by email, configure [SMTP Server](#)

OK Cancel

4. Configure Google SMTP Server

Note: Sangfor aCloud have restriction on SMTP server address, which require IP address instead of domain name. Try **ping smtp.gmail.com** to obtains the IP address and configure server address.

```

C:\Windows\system32>ping smtp.gmail.com

Pinging gmail-smtp-msa.1.google.com [74.125.24.108] with 32 bytes of data:
Reply from 74.125.24.108: bytes=32 time=28ms TTL=48
Reply from 74.125.24.108: bytes=32 time=28ms TTL=48
Reply from 74.125.24.108: bytes=32 time=28ms TTL=48
Reply from 74.125.24.108: bytes=32 time=28ms TTL=48

Ping statistics for 74.125.24.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 28ms, Average = 28ms
    
```

SMTP Server

Sender Address: [redacted]@gmail.com

Server Address: 74.125.130.108

Port: 465

☒ SSL encryption required

☒ Authentication required

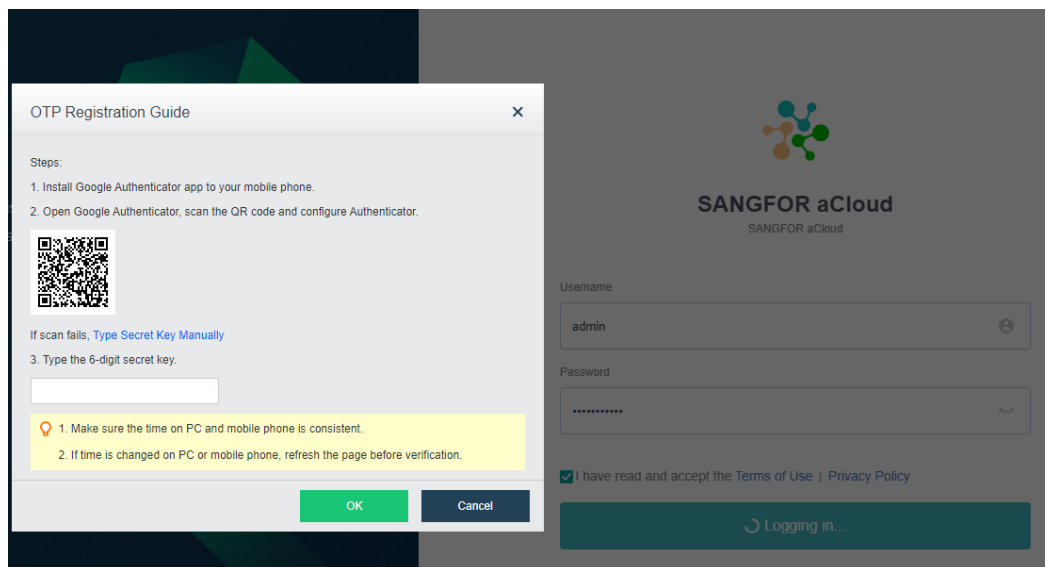
Username: [redacted]

Password: [redacted]

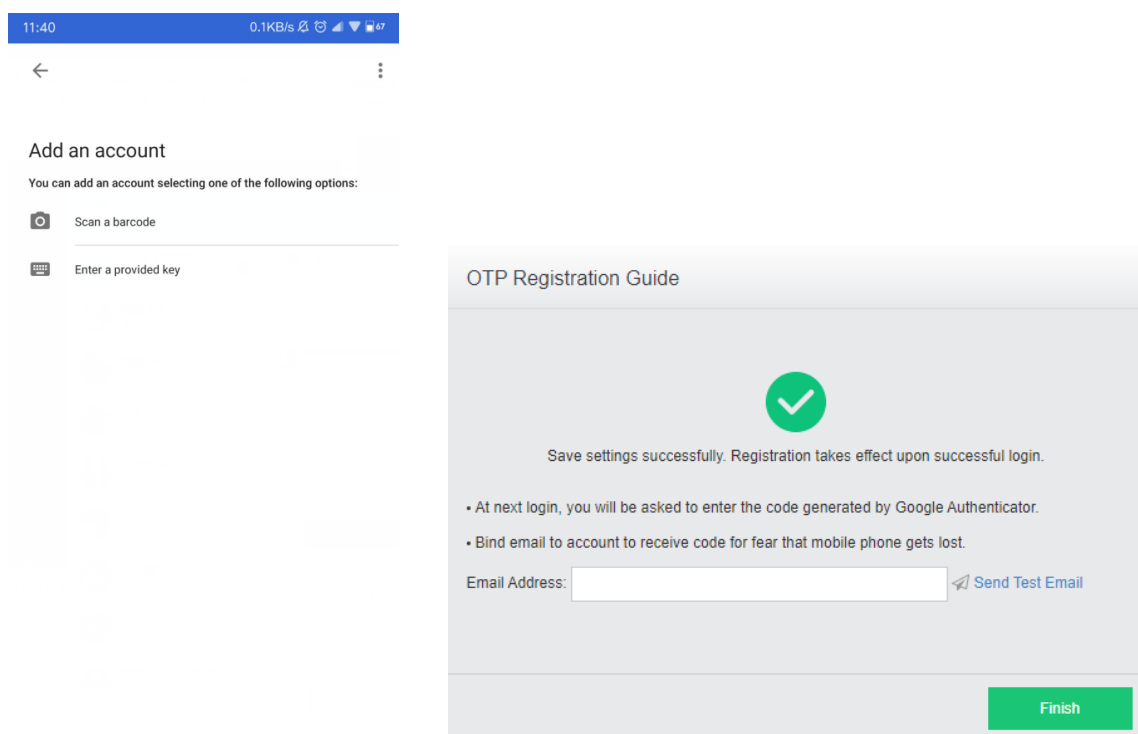
OK Cancel

2.2 First time verification

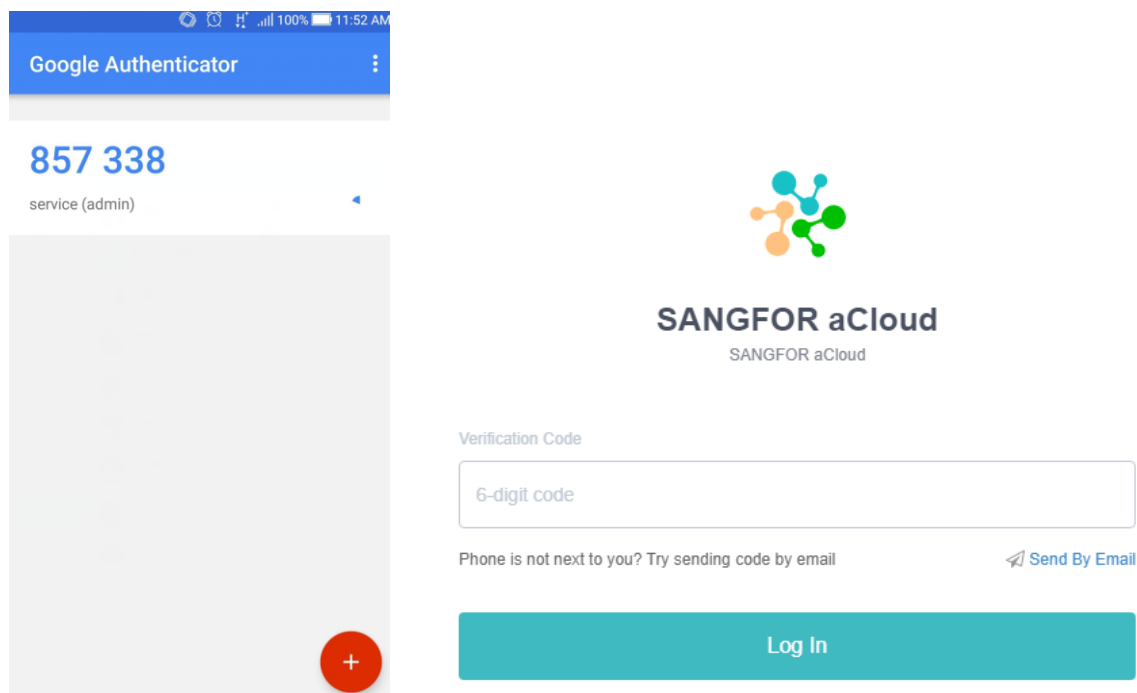
1. After Enable Google OTP, Sangfor aCloud will automatically logout. When login again, it will prompt QR code for verification.



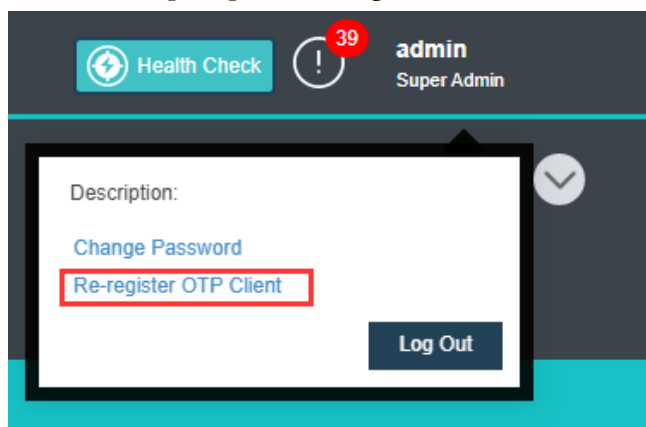
2. Download Google OTP Authenticator (Android/IOS)
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en>
3. Click on "Scan a barcode" and scan the barcode generated by Sangfor aCloud. After, type the secret key generated by Google Authenticator into Sangfor aCloud and click ok to proceed.



Note: Sangfor aCloud will bind with android Google account after first time login. Each login will be required verification code generated by the Google Authenticator apps.



4. To reset the ownership of Google OTP account, click on logged account and select “Re-register OTP client”. It will prompt new dialog with barcode for first time verification.





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

