SANGFOR

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

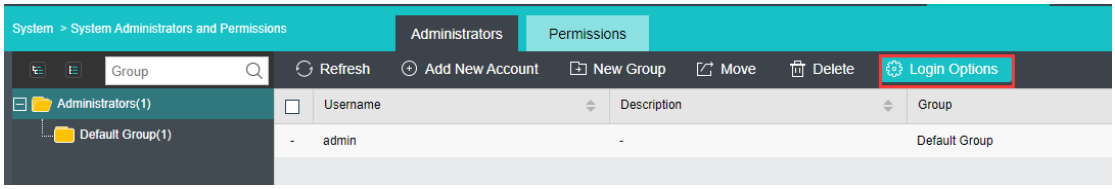
Sangfor aCloud 5.8.8R1 introduce 2 factors authentication method via Google OTP. Google Authenticator is a software-based authenticator that implements two-step verification services using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm, for authenticating users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

Chapter 2 Configuration guidelines

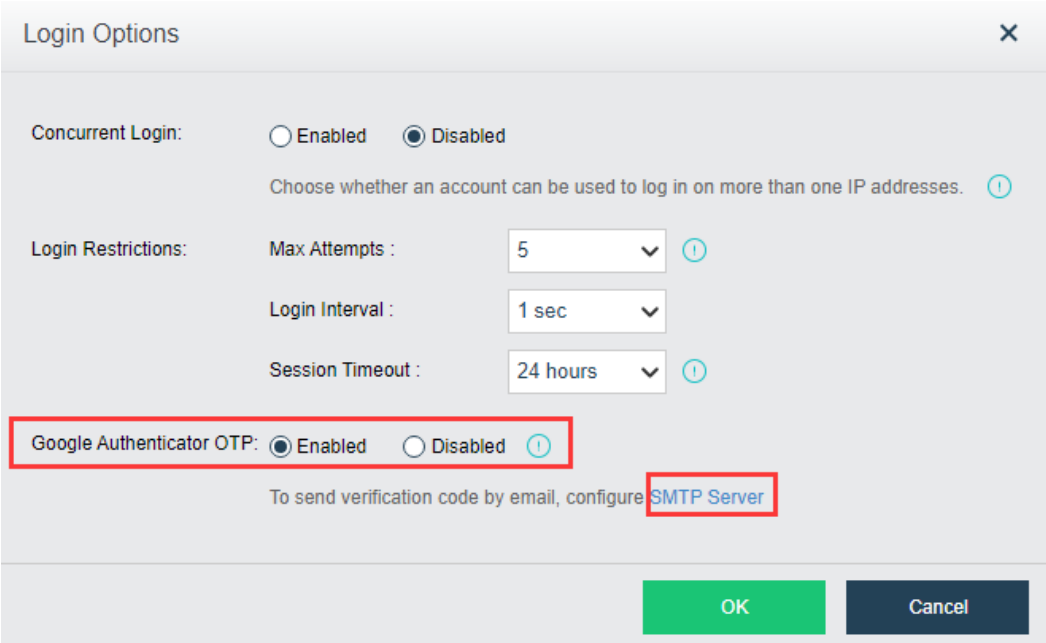
2.1 Enable Google OTP services

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

2. Click on the Login Options

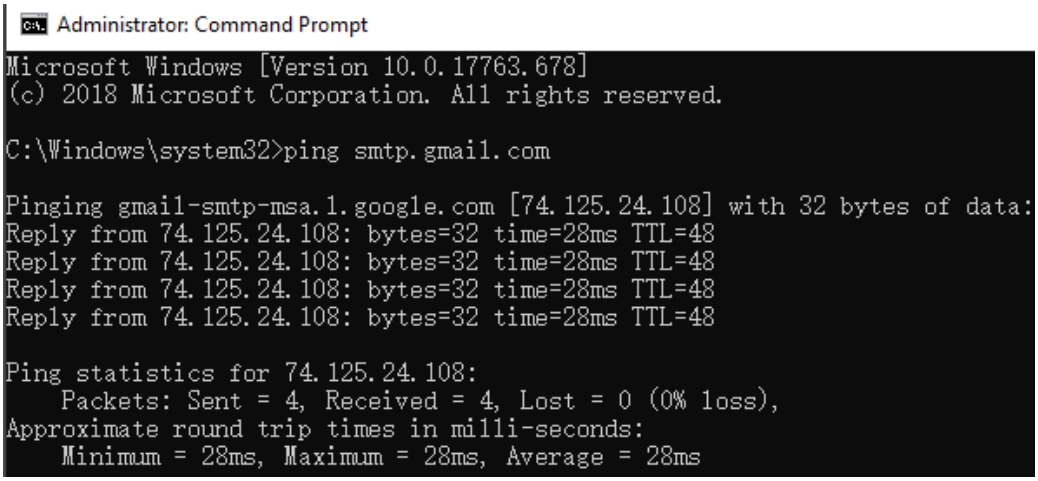


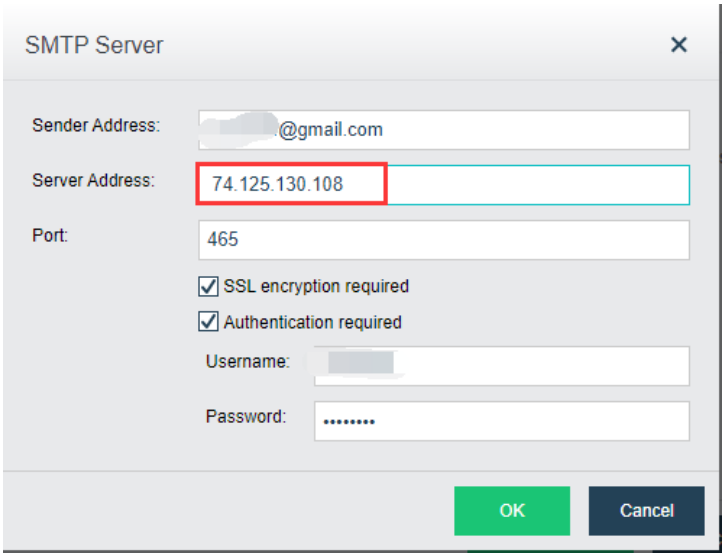
3. Enable Google Authenticator OTP.



4. Configure Google SMTP Server

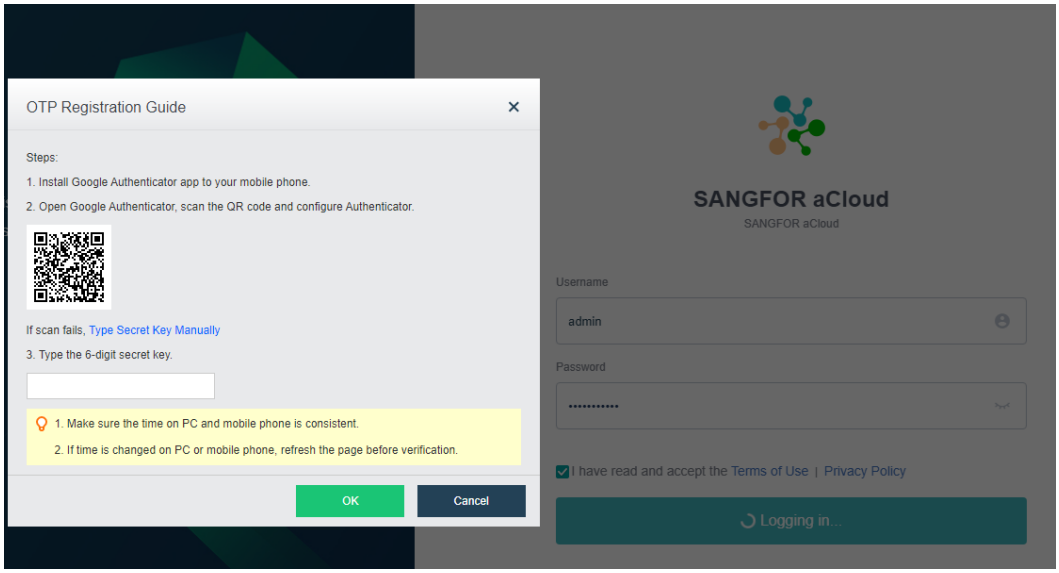
Note: Sangfor aCloud have restriction on SMTP server address, which require IP address instead of domain name. Try **ping smtp.gmail.com** to obtains the IP address and configure server address.





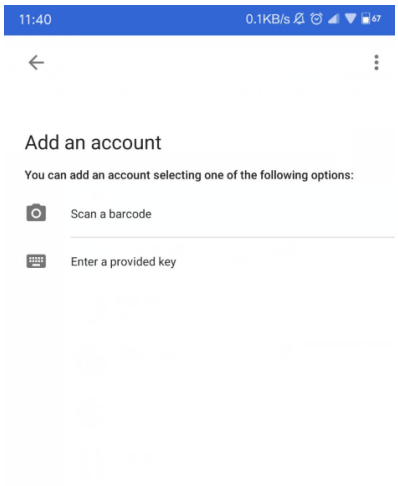
2.2 First time verification

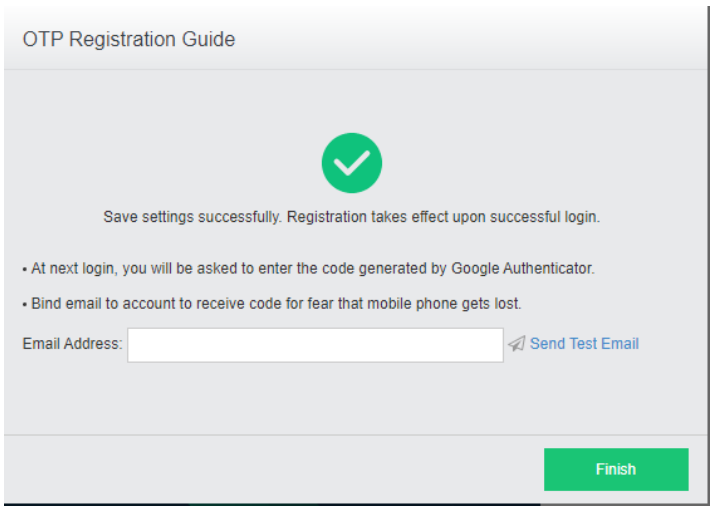
1. After Enable Google OTP, Sangfor aCloud will automatically logout. When login again, it will prompt QR code for verification.



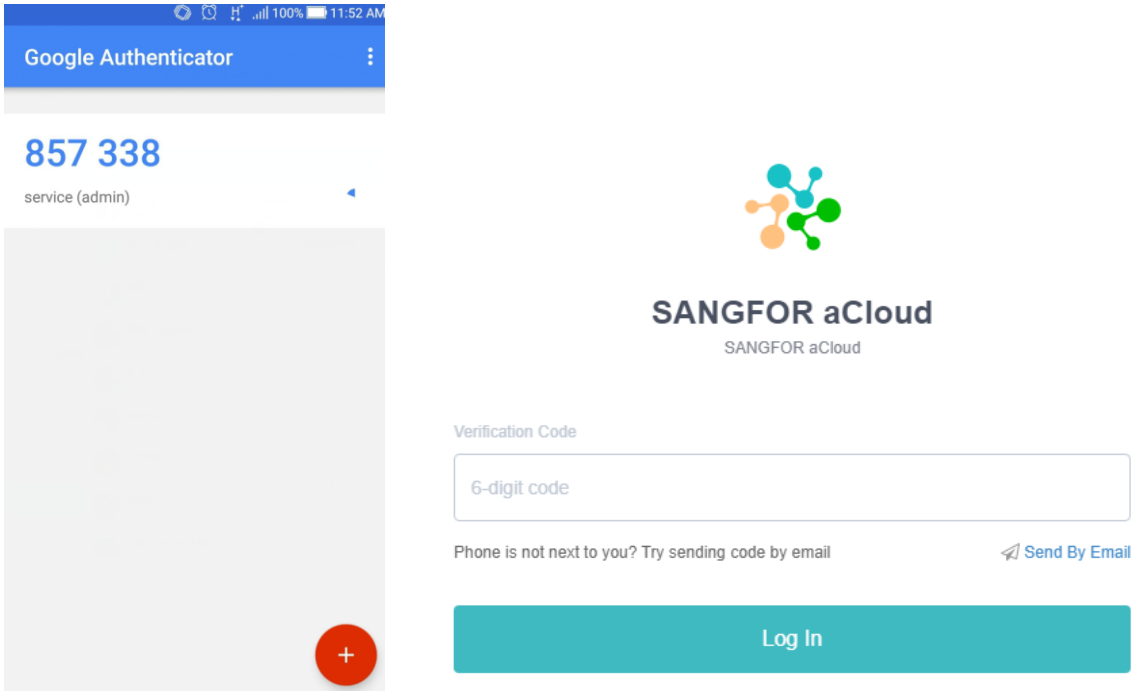
2. Download Google OTP Authenticator (Android/IOS) https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en

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.