SANGFOR

Sangfor NGAF

SSL VPN 2FA Configuration Guide

Product Version	8.0.35
Document Version	01
Released on	August 29, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

Change Log

Date	Change Description
Aug. 29, 2021	This is the first release of this document.

Contents

1 Scenario

TOTP, an abbreviation for Time-based One-Time Password, indicates a one-time password based on a timestamp algorithm.Based on the comparison between the client's dynamic password and the clock of the dynamic token authentication server, a new password is usually generated every 30 or 60 seconds.

The client and server are required to maintain the correct clock very precisely to keep the one-time password generated to be consistent on both sides.

NGAF SSLVPN can combine with dynamic tokens based on TOTP protocol to achieve two-factor authentication for account security.

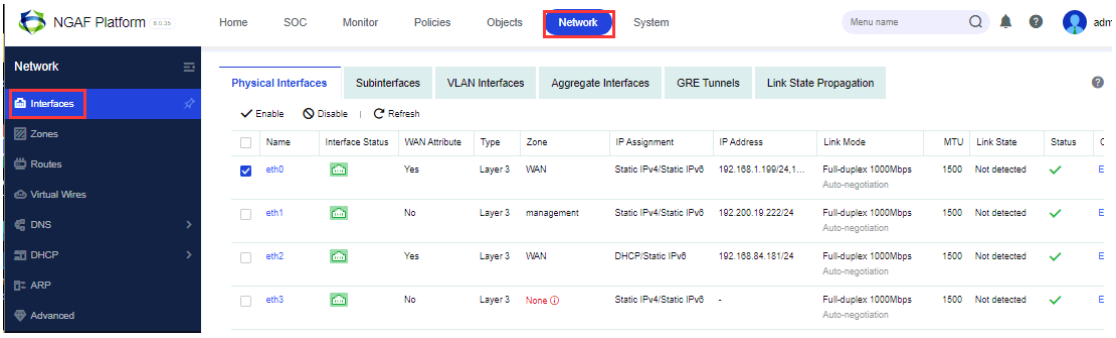
The commonly used TOTP dynamic tokens client are Google Authenticator, Microsoft Authenticator, M token, etc. This configuration guide uses Google Authenticator as an example.

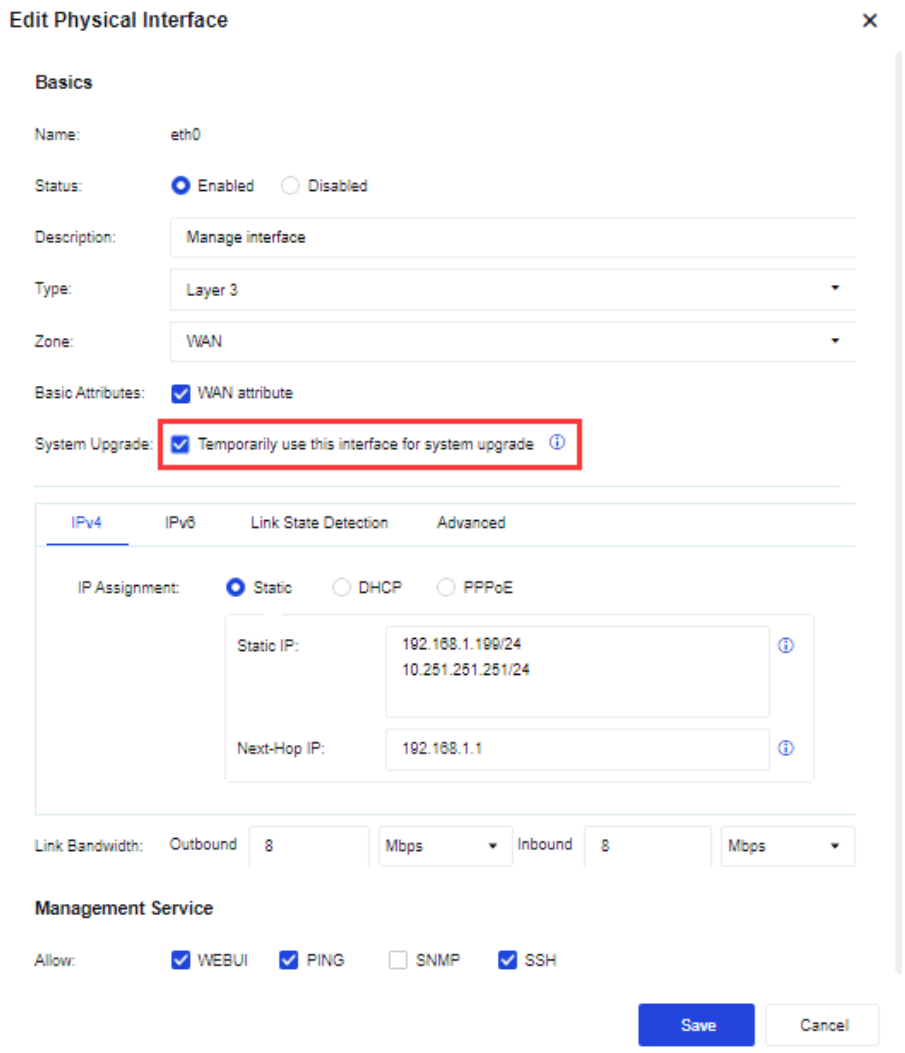
2 Configuration Steps

2.1 Install SSL VPN 2FA patch on NGAF

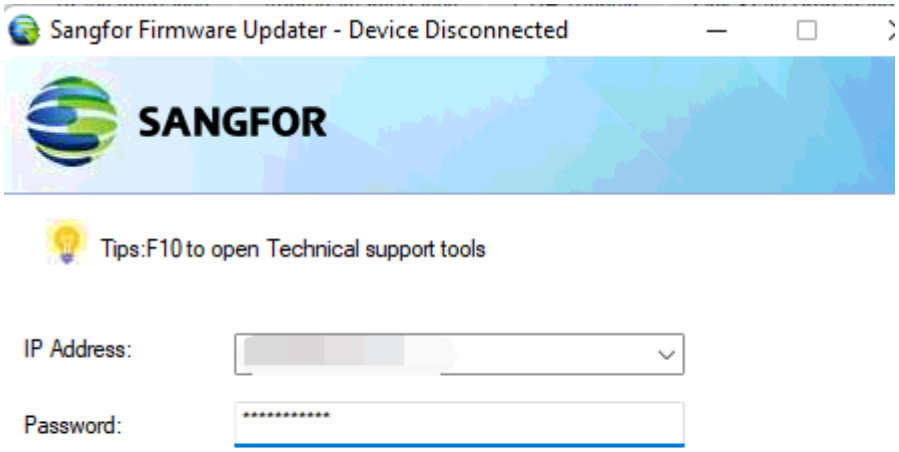
Step 1. Request SSL VPN 2FA patch from Sangfor Personnel

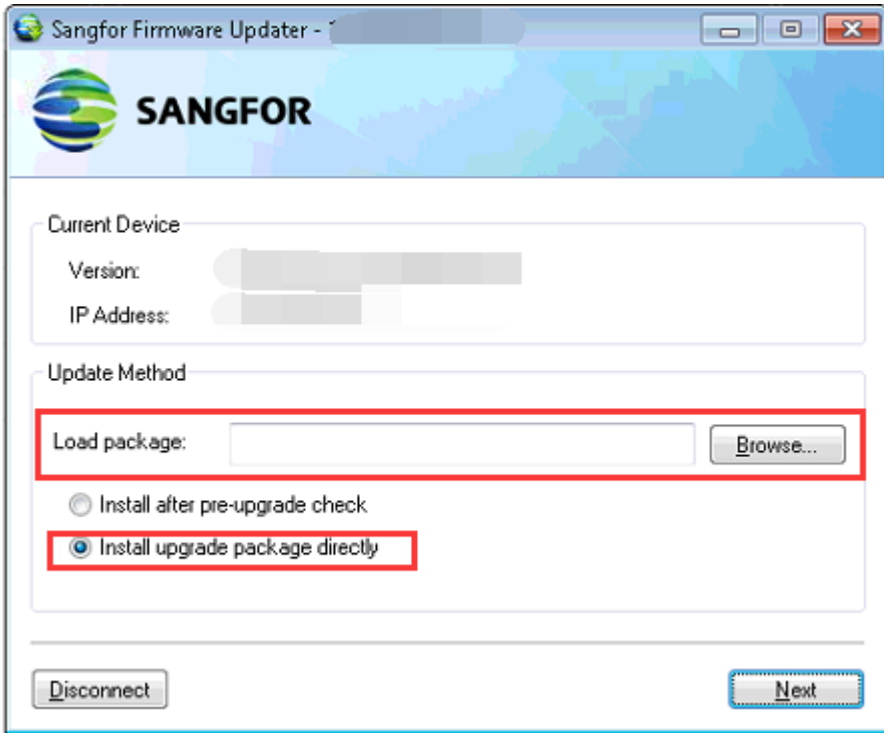
Step 2. Login to the NGAF web console and enable system upgrade setting on the interfaces that you connected. **Network > Interfaces > Physical Interface**.





Step 3. Run Sangfor Updater software and log in with the **admin** account credential. After that, click on browse and select SSL VPN 2FA patch package. Then select **Install upgrade package directly**.

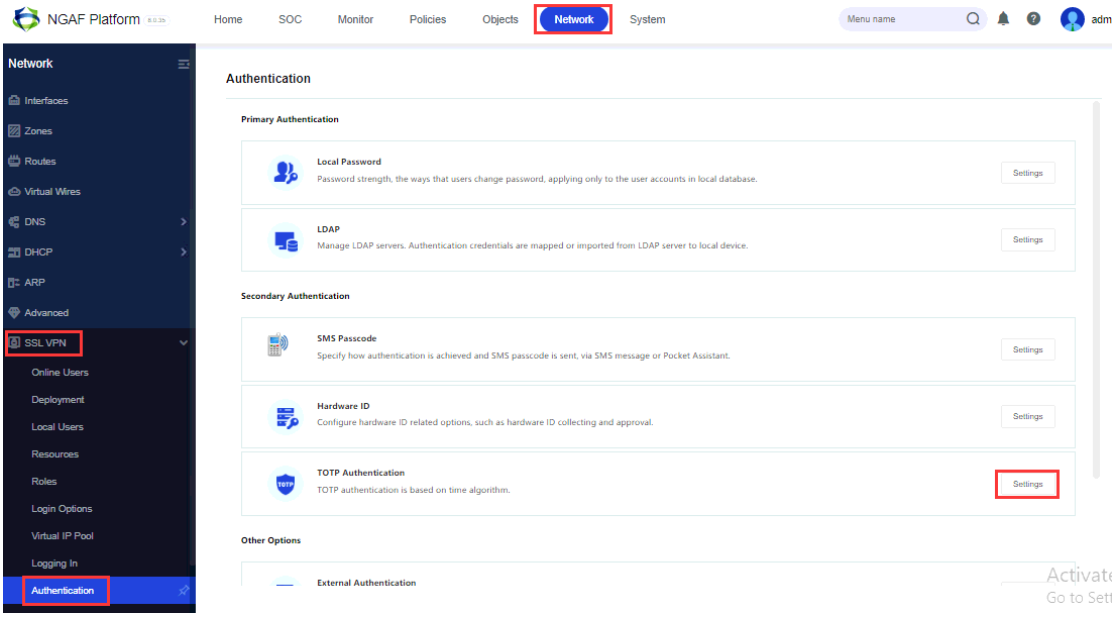


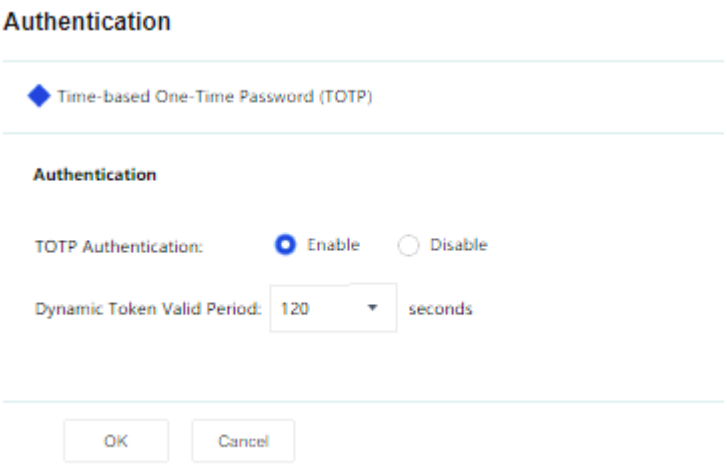


Step 4. Click **Next** to proceed to install the SSL VPN 2FA patch to NGAF.

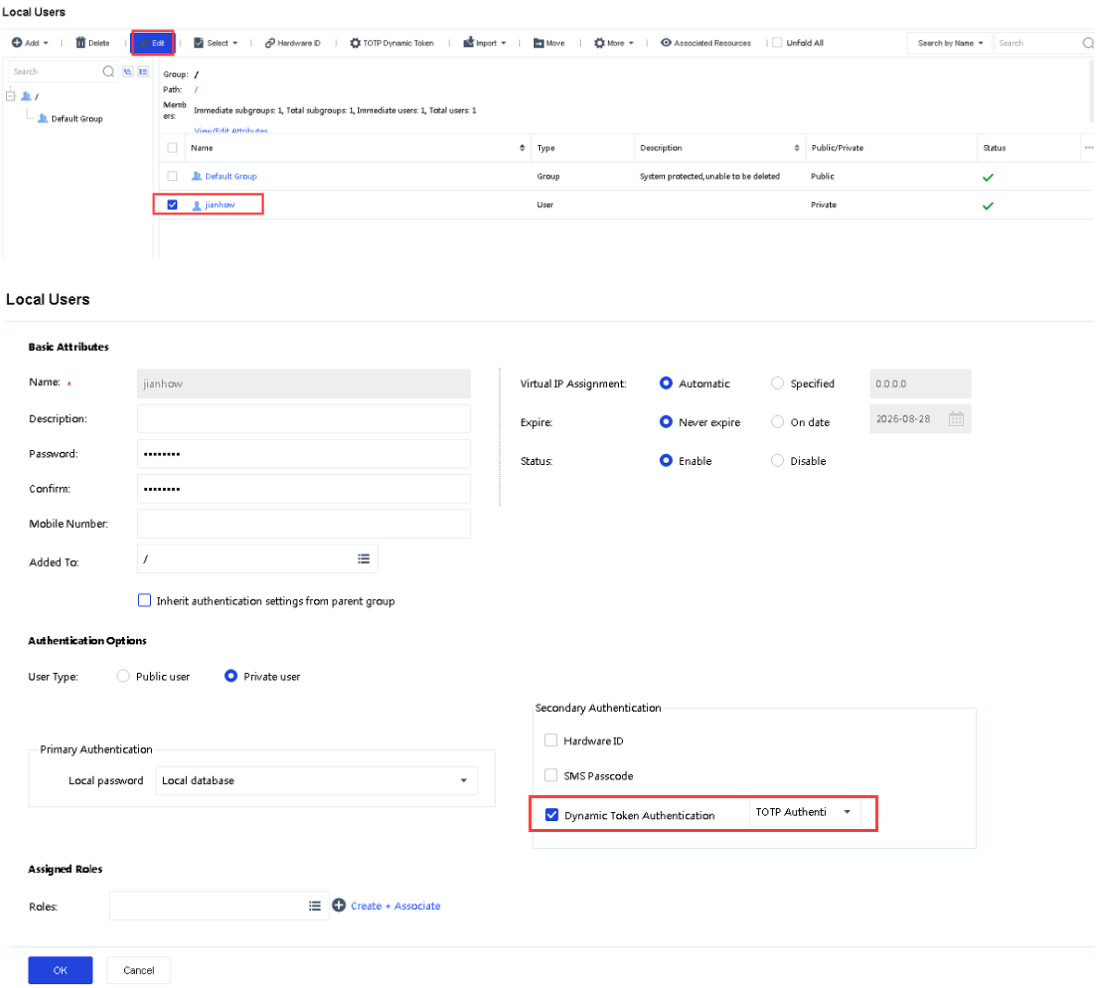
2.2 Enable TOTP authentication

Step 1. After installed SSL VPN 2FA patch on NGAF, proceed to enable TOTP authentication settings. **Network > SSLVPN > Authentication > TOTP authentication**.

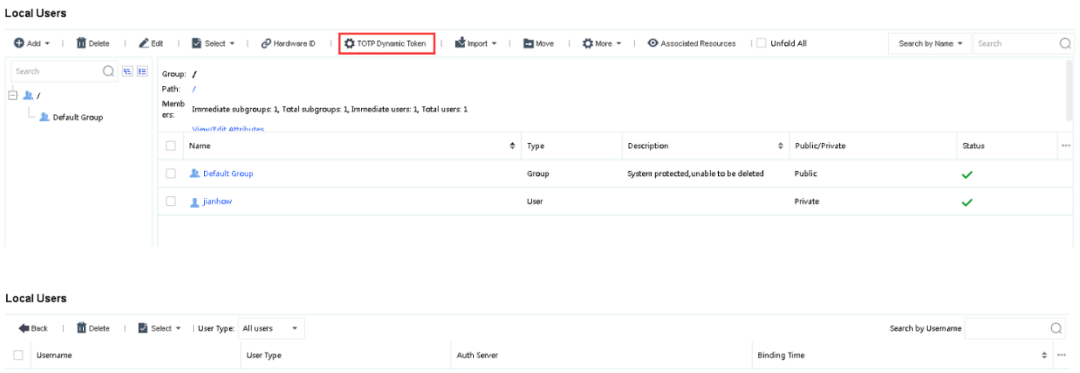




Step 2. Enable TOTP authentication on specific users. Select the user and click on edit under **Network > SSLVPN > Local User**. Next, select **Dynamic Token Authentication** > **TOTP authentication**.



Step 3. Check the TOTP authentication database to view which user is bind with TOTP authentication **SSL VPN > Local Users > TOTP Dynamic Token**. You can see the **User Type** and **Binding Time**. Administrators can delete the user from the TOTP authentication database manually if the user lost their TOTP software.

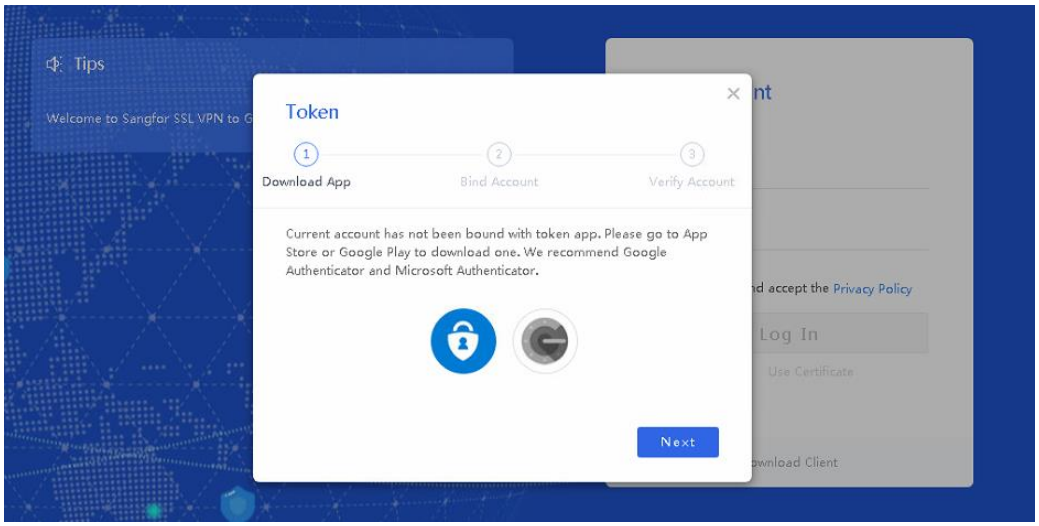


3 Test Result

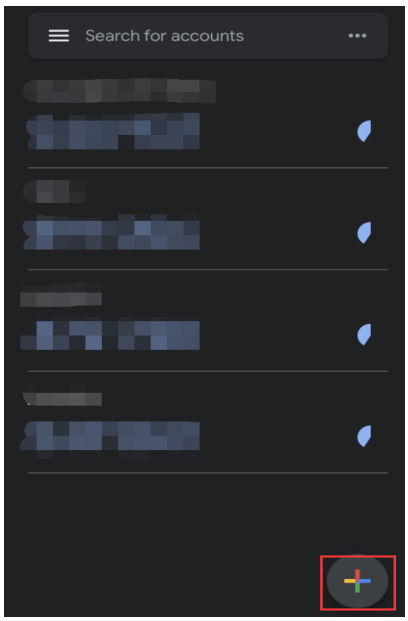
3.1 First Login to SSLVPN after enabling TOTP authentication

3.1.1 Token binding by scanning QR code

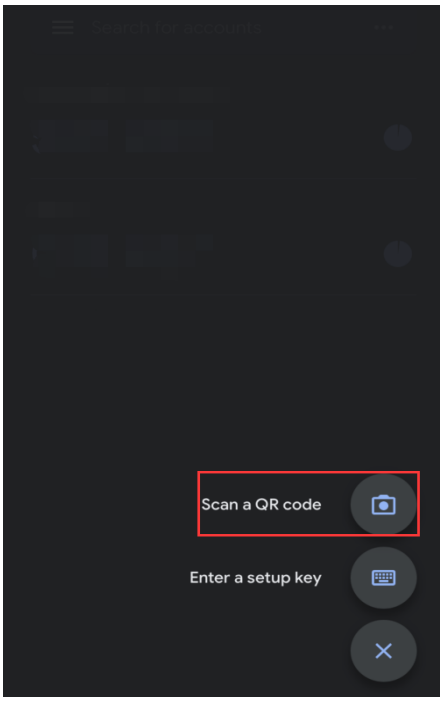
Step 1. Once enter login credentials and click **Log in**, a message that requires the user to do the token binding with authenticator apps will prompt. Download Google Authenticator on phones (Apple Apps Store or Google Play Store) and click **Next**.

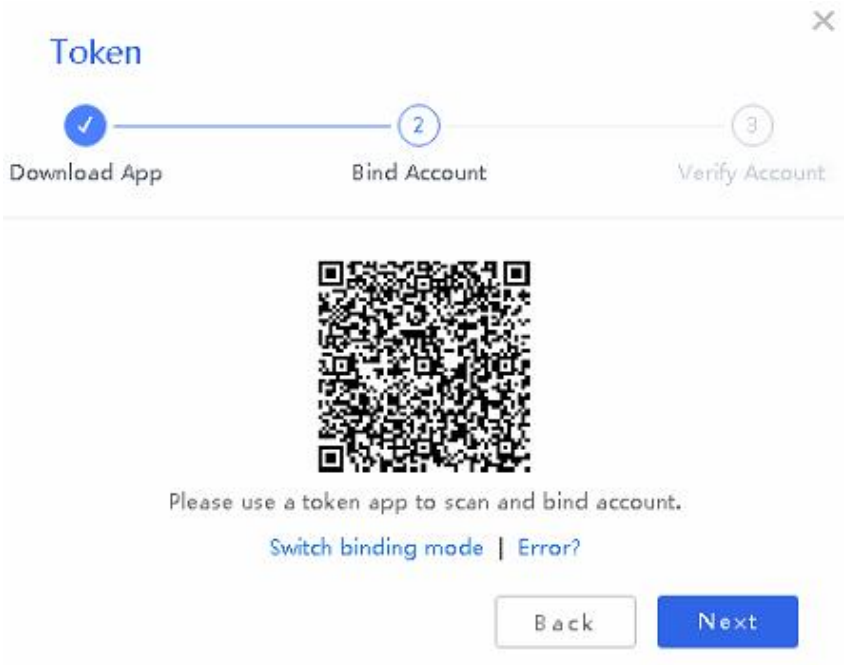


Step 2. Run the authenticator apps and click the **ADD** button at the bottom.

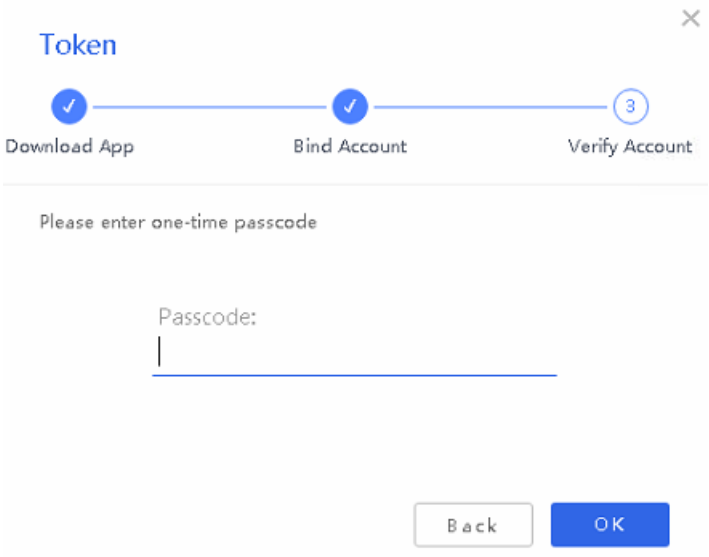


Step 3. Select **Scan a QR code** on the user's phone and scan the QR code displayed on the login page.





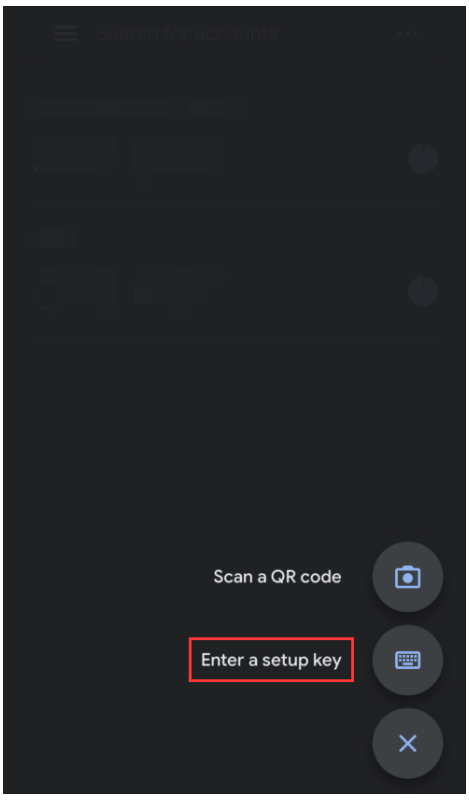
Step 4. Enter the code displayed on the authenticator on the SSLVPN login page to complete the login process.



3.1.2 Token binding manually

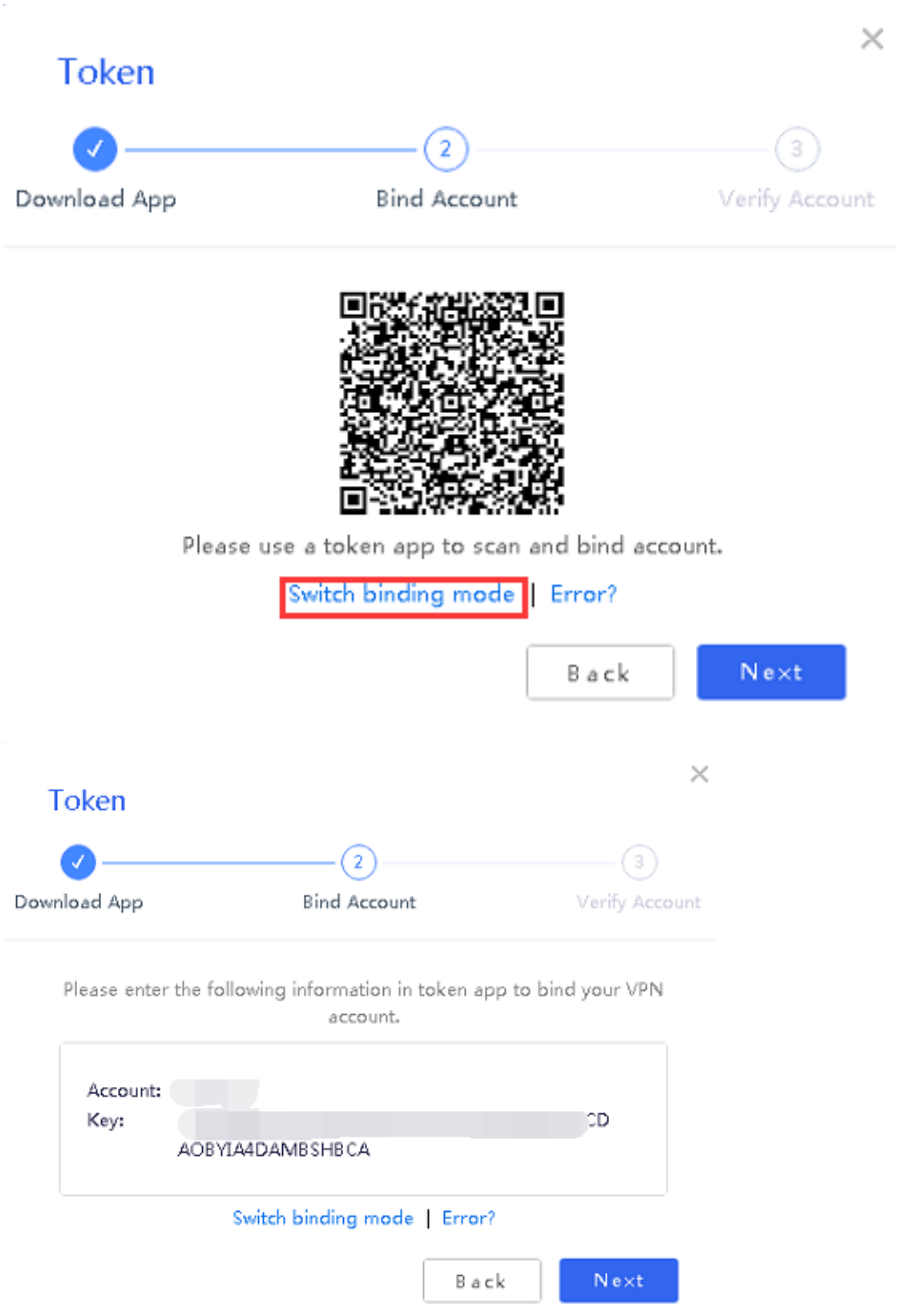
If the user is having an issue using their mobile camera to scan QR code, they may proceed to do binding manually as shown below:

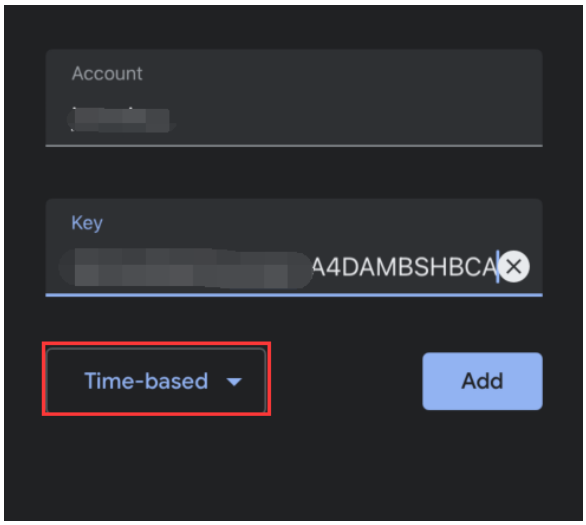
Step 1. Run Google Authenticator and click the **ADD** button. Next, select **Enter a setup key**.



Step 2. Select **Switch binding mode** on the Bind Account setting.

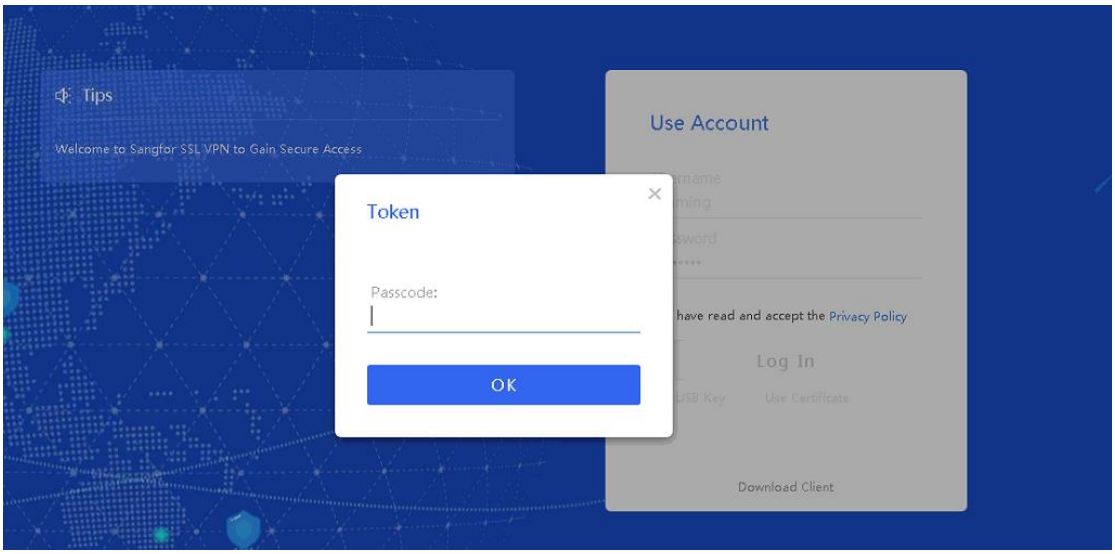
Copy and enter the key shown into Google Authenticator. Then select "**Time-based**" and click **Add**.





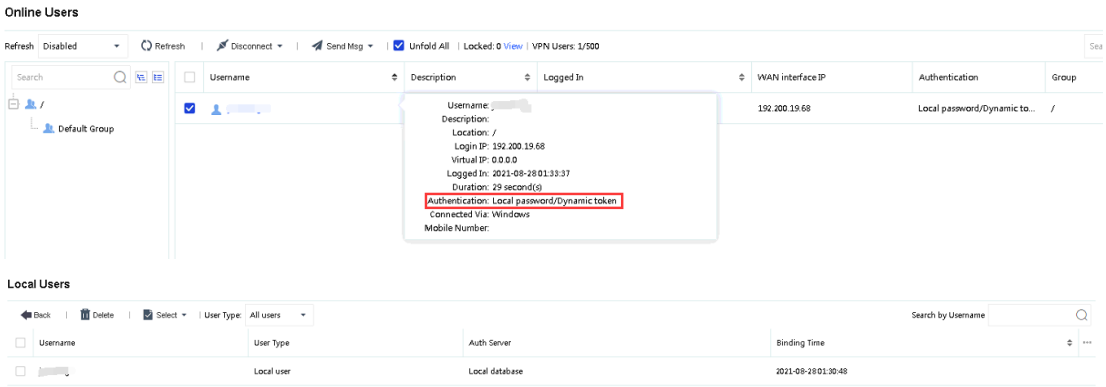
3.2 Second login after token binding

After the first login to SSLVPN and complete the token binding, the following login will not request token binding again as long as administrators didn't delete the binding relationship on the TOTP authentication database.



3.3 Verification on the binding relationship

Administrators can check on the user authentication method on the online user list **Network > SSL VPN > Online users,** and also the binding status at **Network > SSL VPN> Local users > TOTP Dynamic Token**.



SANGFOR