Two-Factor Authentication

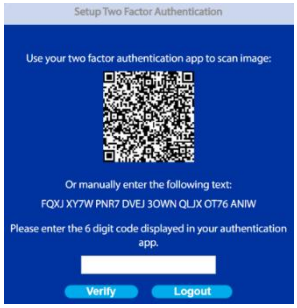
Setting Up 2FA on Copa Connect Web SPRK

Two-Factor Authentication (2FA) adds an extra layer of security to the login process. Instead of relying solely on a password, the user must provide a second factor to verify their identity. One of the most common forms of 2FA is through **TOTP (Time-Based One-Time Password)** codes.

Below are the steps to configure it:

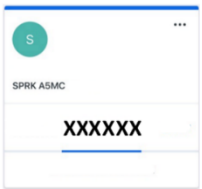
1. **Initial 2FA Setup**
   - The agent logs in as usual on Copa Connect Web (SPRK).

2. **Code Generation**
   - Once you have successfully entered the Office ID, Agent ID, and Password, a pop-up window will appear, prompting the agent to scan the QR code using an authentication app such as Google Authenticator, Authy, Microsoft Authenticator, or Duo Mobile. If you do not have any of these apps installed, you can download them from Google Play or the App Store. If the QR code does not work, you can also manually enter the provided alphanumeric code. Note: This process only needs to be completed once.

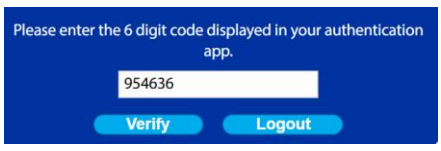


The QR code in this guide is for illustrative purposes only.

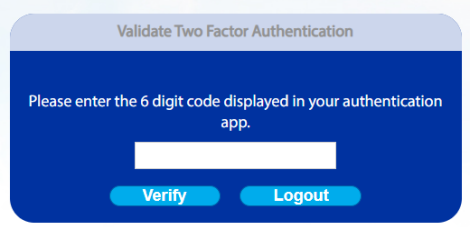
3. **Code Generation**
   - A QR code or secret key is generated and displayed on the website or app.
   - This code changes every 30 seconds, making it temporary and valid only for that period.



4. **Entering the TOTP Code**
   - When the user attempts to log into their account, after entering their password, they must enter the TOTP code generated by their authentication app.



5. **Code Verification**
    - The server verifies if the entered code matches the expected one, based on the shared secret key and the current time.
    - If the code is valid and matches the one generated by the app, the user gains access to their account.
6. **Regular Login**
    - Once the authentication app is configured, the user must open the app and enter the corresponding code when logging into SPRK.
    - This code changes every 30 seconds and is only valid for that period.



User Lockout

When logging in, a user has a maximum of 5 attempts. If this limit is exceeded, their account will be locked and must be reset by an administrator. This same mechanism applies when entering the two-factor authentication code: after 5 failed attempts, the user will be locked out and must contact the system administrator to reset their password.

Note: When a user's password needs to be reset or they request a password change (forgotten password), two-factor authentication will only be required after the user has entered the new password. SPRK will not validate two-factor authentication before sending the password reset link to the user.

Lost, Stolen, or Damaged Devices

If two-factor authentication is enabled, agency administrators will have access to profile management in SPRK, allowing them to reset the two-factor authentication code for a specific ticketing agent. When a user's password is reset, they must configure a new two-factor authentication code on their next login, without needing to delete their account to reactivate it on a new device.