

2-factor Authentication - USER MANUAL

VERSION 1.1 (2016-02-02)

What is 2-factor Authentication?

2-factor authentication (2FA) is technology and a process that requires two sets of credentials be used in authenticating the owner of an account. Ultimately, using 2FA improves the security of your account. The use of 2FA in the Control Panel requires your standard username and password first and second, a changing automatic generated code from an application on your smartphone. Since the secondary generated code is displayed through your smartphone application, physical access to your smartphone is required, making it virtually impossible to access your account without the physical phone. Please note that "2"-factor Authentication is also known as "2"-step Authentication and "2FA". More information is available at [Wikipedia](#).

How to Activate 2-factor Authentication in Control Panel?

Step 1: Install a One Time Password (OTP) Application on your Smartphone

The OTP application must be compatible with "TOTP" (Time-based One-Time Password, as specified in RFC 6238). The following mobile applications are recommended:

- FreeOTP ([Android](#) | [iOS](#))
- Google Authenticator ([Android](#) | [iOS](#))

Configure the OTP application as follows:

- Insure the application is using SHA1 - 6 digits (totp), typically this is the default
- Generated codes are only valid for 30 seconds
- Add a smartphone passcode or fingerprint for additional security

Step 2: Access and Connect the OTP Application to the Control Panel

- Navigate to Manage Account > My Account > Access Control > 2-factor Authentication for the QR code
- A randomly generated "secret key" is created and a QR code / direct output will be made available
- Connect the OTP application by scanning the created QR code / direct output on the page
- Add the 2FA profile manually by providing the generated secret key if scanning the QR code doesn't work
- The OTP mobile application is able to generate 6 digit OTP codes for your account based on the generated secret key from the Control Panel
- Since existing profiles cannot get overwritten, please delete any previous Control Panel profiles first before generating a new profile / secret key

Step 3: Use the Phone Generated Code to Activate 2FA

Using a valid generated 6 digit code and clicking on "Enable", 2FA will be activated for your account. Please note the following reasons why activation may not happen:

- The provided code may be invalid
- Codes are only valid for 30s and may have expired
- The mobile OTP application profile set up failed and thus generated wrong codes

Step 4: You are done and Optional Additional Security

Additional access control features can be turned on in the Control Panel:

- IP access limitation
 - Role users access
-

Frequently Asked Questions about 2FA

How do I Log in to the Control Panel with 2FA Active?

Login as follows:

- Click on the "2-factor Authentication" button on the Control Panel login screen
- Provide your username, your password
- Provide your 6 digits one time password auto generated by your OTP phone application

How to disable 2FA or change the Secret key?

To disable 2FA or reconfigure it (losing physical access to smartphone) please login to the Control Panel and navigate to Manage Account > My Account > Access Control and click the "Disable" button. From this screen 2FA can also be re-activate or re-setup, which will generate a completely new secret key.

How to recover your account if you lost your phone?

If you misplace your smartphone or cannot generate the 6 digit one time password for any other reason, please contact support directly. Support has a process to validate your identity and provide account access. Please note that if you lose your QR code or secret code from the Access Control page, charges may apply for additional manual verification and checking.