AirPlus
Smarter payment. Better business.

AirPlus Virtual Cards
Secure payment with AirPlus Virtual Cards Single-use or Multi-use

AirPlus Virtual Cards Single-use can **only be used for one-time payments and are automatically closed afterwards,** so they have been officially exempted by the regulatory authority from 2FA, which applies to all conventional credit cards.

AirPlus Virtual Cards Multi-use, on the other hand, **can be used for multiple and recurring payments.** This type of virtual card is similar to a traditional plastic credit card and is therefore subject to the SCA process. We as your payment solutions provider are committed to meeting the required security standards in the financial services sector.

The following steps walk you through the 2FA process:

- Since SCA applies to AirPlus Virtual Cards Multi-use, only the card user can generate a card for himself/herself at the current time. It is not possible to generate AirPlus Virtual Cards Multi-use for coworkers or other employees.
- After you have made all the settings for your card, you will be prompted to select your 3D Secure profile that you set up when you registered for the AirPlus Portal. When you registered, you provided a security question, a phone number and email address.

- If you have not yet configured a 3D Secure profile, you will be prompted to set it up. A 3D Secure profile is necessary to authenticate yourself during the payment process.
- The one-time password we will send you by text message or email when you generate the first card during a portal session is independent of SCA.
- After successfully generating a virtual card, you can use it for payments. When you use the card for the first time, you will be required to follow the 2FA process. During the initial authorization, you will be asked to answer the security question you defined in your 3D Secure profile. In addition to answering this question, you will receive a onetime PIN (TAN) by text message or email.
- After the PIN (TAN) has been entered, the first transaction is released for authorization. The payment process is initiated by the merchant as agreed.

This process is not always mandatory for all transactions. You can **whitelist trusted merchants** to not have to authenticate them by both methods in the future.

During your initial authorization, you can indicate that you trust the merchant you are about to pay, which puts him on your whitelist. You can now authorize payments without entering a PIN (TAN).

Whitelisting is not only possible during the first authorization; you can also whitelist trusted merchants during later transactions. However, should our security checks indicate suspicious payment behavior, we reserve the right to reactivate 2FA for individual cases.

EN, 06.24, CL