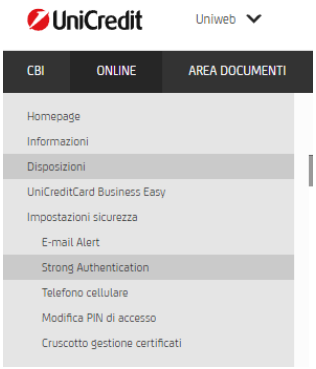
Quick Reference Guide
UniCredit Business Pass/M-Pass - Strong Authentication

Characteristics

The solution introduces an additional security control, for selected transactions, for the Customer who must insert a dynamic single-use password (One Time Password or "OTP") before the signature of the payment transactions, authorizations, and documents/contracts. The OTP is generated by a "physical" OTP generator device called "*UniCredit Business Pass*" (former-*UniWeb Pass*) or by an application for smartphones called "*UniWeb Mobile Pass*" (in UniWeb the Mobile Digital Certificate is called *UniCredit Business M-Pass*) which displays the code to be inserted in UniWeb and other services of the Corporate Portal.

It is possible to activate both the solutions but the Mobile one is activable only after the physical one.



The security functionalities are shown in the UniWeb menu called "Security Settings" in ONLINE section, which also includes the e-mail Alert management functionality which remains unchanged.

From this menu the Signatory User can see and manage the settings related to his/her profile, while from ADMINISTRATION section the UniWeb Administrator can see the status of the security settings of the administered Signatory users, but without being able to modify the data.

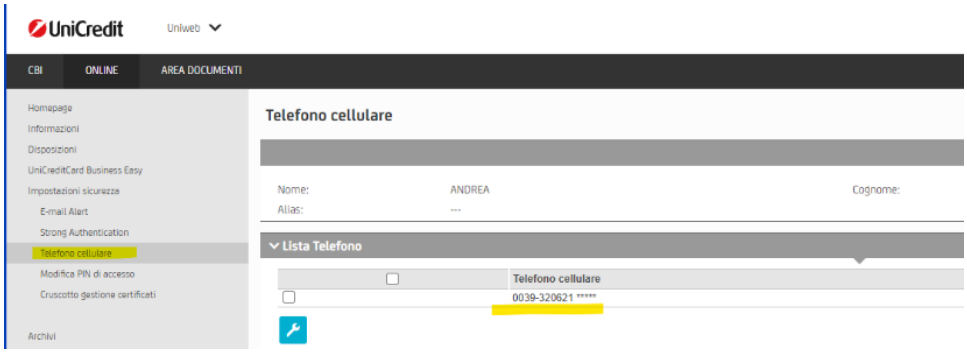
Mobile Phone Management

The contact mobile phone number, required to activate the smartphone application called *UniWeb Mobile Pass* (which manages the UniCredit Business M-Pass Certificate), can be managed from this section: *Online>Security settings>Mobile phone.*

In order to access the Corporate Portal and therefore UniWeb and other Corporate services, Signatory customers must have validated their mobile phone number in the General Registry with the Branch. With this premise, the bank representative can register the Digital Certificate of the Signatory by assigning the physical token and sending the temporary first access PIN to the aforementioned number.

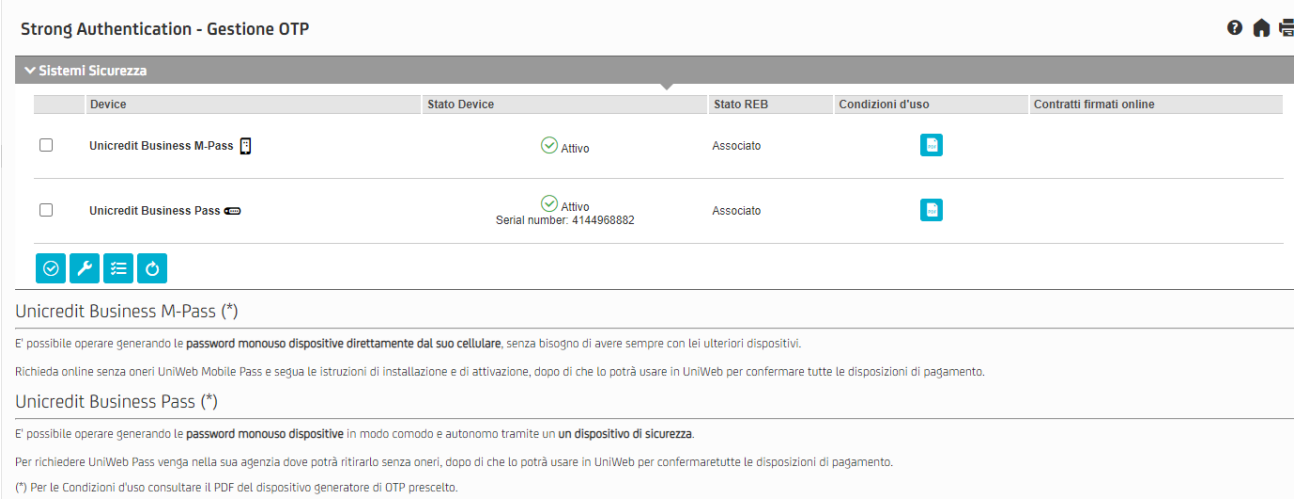
Once in possession of the OTP generator and temporary PIN, Signatories on first access to the Corporate Portal can confirm or change the mobile phone number validated with the Branch. Later, it's possible to change the number from the *Online > Security Settings > Mobile Phone section.*

In both cases, validation by entering the OTP is required.



Strong Authentication Management OTP

In this section the Signatory User can see the current situation and manage the devices *UniCredit Business Pass* e *UniCredit Business M-Pass*, moreover it will be allowed to download the terms and conditions.



The available functionalities are the following ones:

- Request/Activate – to activate the Mobile OTP generator
- Substitute – to ask for substitution of an OTP generator (it works only for M-Token)
- Associate – to associate an activated OTP generator to current REB (both physical and mobile)
- Change mPIN – to modify mPIN (only *UniWeb Mobile Pass)*

Each operation completed by the Customer selecting the device, pressing the desired button, and following the related guided process described in the next chapters, will be notified to his/her contacts (via e-mail for e-mail Alert and SMS to mobile phone number) to guarantee the security.

Request/Activation and Substitution of *UniWeb Pass*

The request for *UniWeb Pass* can be done contacting a Branch. Upon delivery of the device, the Customer is required to sign the loan agreement indicating the serial number of the device.

On first access to UniWeb, the token must be activated with the appropriate button and associated with the REB(s) of interest; the REB status becomes “Activated”.

When the UniCredit Business Pass battery drops below 10% of the charge, the display indicates the residual charge with the wording "batt0N" where "0N" indicates the percentage of battery remaining (each percentage point allows operation for about two weeks) . In the example the battery is charged to 4% (about 8 weeks of remaining operation).

Request/Activation and Substitution of *UniCredit Business M-Pass*

The request of an OTP generator *UniCredit Business M-Pass* can be completed only online in UniWeb, and it pass through the acceptance of the Terms&Conditions of the service and through the view of the contact information for the current REB.

Afterwards the Customer must choose and insert the numeric mPIN code to be used to generate the OTPs with the smartphone APP, confirming the operation with the digital signature

Then UniWeb sends to the Customer an e-mail containing the information to configure the APP (the Customer can choose to use an alphanumeric code or a QRCode).

Once received the e-mail the Customer must download from the official virtual store of the operating system of his/her mobile phone the APP *UniWeb Mobile Pass* and proceed with its configuration and activation with the following steps to be done on the smartphone:

Select the activation type

To frame the activation QRCode, or

To insert the activation alpha-numeric code and confirm it

To insert the mPIN chosen before in UniWeb and confirm it

The status of the device becomes “Activated”, but the Customer must associate it to a REB to use it.

The Customer can ask online in UniWeb the substitution of *UniCredit Business M-Pass* when he/she needs to change the mobile device (mobile phone number changes does not require actions on the APP, but only the mobile phone number change process already described)

The Customer will be asked to insert online the mPIN to confirm the operation and the status of the device becomes “To be substituted”. Afterwards the process is identical to the request process, starting from the e-mail delivered with the information for the configuration of the APP.

The new device keeps the configurations of the previous one (example: REB association) and substitutes it only when it is activated, moment when the previous one becomes unusable.
In order to complete the installation/configuration and substitution of *UniCredit Business M-Pass* it is needed that the mobile phone is connected to a mobile or Wi-Fi network, enabled to mobile data exchange.

It is possible to ask a Branch to reset the mPIN if it has been forgotten; a new automatically generated mPIN will be sent via SMS. It is possible to change the mPIN online in UniWeb too. These actions do not modify the association with the REB.

Association to REB of *UniCredit Business Pass* e *UniCredit Business M-Pass*

Activated OTP generator devices must be associated by the Customer to every REB he/she is enabled to work; once that a Customer has activated an OTP generator, then he/she must use it to sign every payment transaction on all his/her REB.

The association with the current REB is done automatically during online activation of *UniCredit Business Pass* and it must be done explicitly for *UniCredit Business M-Pass* or to include other REBs, by means of an online action in UniWeb with the insertion of an OTP and digital signature. The device status remains "Activated", while the REB status becomes "Associated".

In case of substitution or block/deactivation of a device, the associations with the REBs set by the Signatory User are kept and in case of substitution they are migrated on the new device.

Use of *UniCredit Business Pass* e *UniCredit Business M-Pass* to generate OTP

To generate an OTP when UniWeb asks for it is sufficient:

- press the button on *UniCredit Business Pass* and read the generated OTP on the display
- launch the APP *UniWeb Mobile Pass*, insert the mPIN on "scrambled" keyboard (i.e. with the keys to enter digits sorted in random order) and read the generated OTP on the display. mPIN is blocked after the fifth consecutive error

mPIN insertion

Generated OTP

The generated OTP has limited time validity and once used, it cannot be reused any more. Up to three consecutive OTP errors in UniWeb are allowed before the user is blocked. The app *UniWeb Mobile Pass* can generate up to 100 passwords in offline mode; once they run out it is needed to connect the mobile phone to a Wi-Fi or mobile network (close to the running out of the OTP "stocks" a message warns the Customer).