

Handbook for the assignment of “UniCredit User” OTP token to UniCredit digital services Users

Summary

1. Premise: Strong Customer Authentication (SCA) and Users.....	2
2. Assignment of the UniCredit User Device to the ALREADY CENSED and ACTIVE Local User	3
3. Assignment of UniCredit User device to a NEW user.....	5

DISCLAIMER

This document was prepared by UniCredit for informational purpose only. Although the information contained in this document has been obtained from sources that UniCredit believes to be reliable, UniCredit does not guarantee its accuracy and completeness. All the information contained in this document are those held by UniCredit on the date the document is made available, and may be subject to change at any time and without notice.

Document updated to April 2019

1. Premise: Strong Customer Authentication (SCA) and Users

The so-called Local Users are individuals identified by the Customer, within the company organization, **without signatory powers** and authorized to access digital services for companies offered by UniCredit (e.g. UniWeb, Banca Multicanale Business, UC Trade Finance gate, International Payment Tracking, etc.), through **the Corporate Portal, in informative mode** and responsible only of the **preparation** of order transactions.

In order to increase the security of its services and be compliant with the new requirements introduced by the European Directive on payment services “PSD2” related to strong authentication of services users (SCA - Strong Customer Authentication), UniCredit has foreseen, during the access, the insertion of a further factor of authentication based on a One Time Password generated by a physical security device.

Based on the new security requirement, the Local Users must be equipped with a physical device for the generation of a “UniCredit User” One Time Password that UniCredit identified in a VASCO token physically similar to the one currently in use by the Signatories (UniWeb Pass or UniCredit Pass for Banca Multicanale), but to which no Digital signature Certificate is associated, therefore not enabling the user to authorize provisions,

The process of provisioning and assignment of the aforementioned Devices is divided in two main activities:

1. on **Bank** side: assignment of the “**UniCredit User**” OTP token to the company REB requested by the Customer
2. on **Company Administrator of profiles** side: assignment of the OTP Token to each User.

With regards to Step 2, the Local Users must be registered directly within the secure environment of the Corporate Portal by the Company Profiles Administrator who defines the operating profiles, assigns the temporary codes and the UniCredit User device requested for the access.

The Administrator must take care of the **acquisition** of the specific **receipt** upon **delivery of the Device** to the Local User as well as the correct keeping of a **Assignments Register** which must be kept for any possible dispute and made available to the Bank in the event of a request.

2. Assignment of the UniCredit User Device to the ALREADY CENSED and ACTIVE Local User

In case of a Local User already censed and active, it is only needed to associate the OTP token “UniCredit User”.

The Administrator of company profiles accesses to the Corporate Portal - <https://corporateportal.unicredit.it> - and, from the top left menu selects “User Administration”.

Once the list of the various users (Signatories - User managed by the Bank and Users – Local User) is displayed, activates the edit function by clicking on the pen icon on the row of the user of interest.

<input type="checkbox"/>	First name	Last name	Date of birth	User type	User status	Application status	Actions
<input type="checkbox"/>	Robert			Local user	Active	okay	
<input type="checkbox"/>	Pina	Delete	15.06.1981	Local user	Inactive	okay	
<input type="checkbox"/>	Matteo		15.06.1981	Local user	Active	okay	
<input type="checkbox"/>	NomeTest	CognomeTest		Local user	Active	okay	
<input type="checkbox"/>	Prova	Prova	15.06.1981	Local user	Active	okay	
<input type="checkbox"/>	Nicola	illo	15.06.1981	Local user	Active	okay	
<input type="checkbox"/>	Silvestri			Local user	Blocked	okay	

Selects “Add OTP token” in order to start the assignment process.

UniCredit Corporate portal

Edit user: Rossi Andrea

Internal portal ID L1003774074

Last name: ROSSI | Email: test@test.it

First name: ANDREA | Additional email: | Fiscal code: PNC

Date of birth: 07.02.1977 | Place of birth: milano | Country of birth: italia

Serial number: | **Add OTP token**

Initial password: | Repeat password: | Change password

Save | Cancel

Inserts:

- the “UniCredit User” device **Serial number** located on the back of the device including all figures and letters without blank spaces or dashes
- the **One Time Password (OTP)** generated by the device itself

UniCredit User administration

Users

Edit user: Rossi Andrea

Internal portal ID L10037740741157127

Last name ROSSI Email test@test.it

First name A Add OTP token

Date of birth 04

Place of birth mi

Country of birth ita

Serial number

Serial number

Initial password Repeat password

Change password

Save Cancel

The system returns the **confirmation message** informing that the OTP Token has been correctly assigned.

Subsequently the module has to be printed by clicking on **“Print OTP Assignment”**

UniCredit Corporate portal

Edit user: Rossi Andrea

Internal portal ID L1003774074

Last name ROSSI Email test@test.it

First name ANDREA Additional email

Date of birth 07.02.1977

Place of birth milano

Country of birth italia

Fiscal code PNC

Serial number 123456789

Print OTP Assignment

Initial password Repeat password

Change password

Save Cancel

The Administrator proceeds with the physical delivery of the OTP Token and the collection of the consent signed in the form **<Receipt of the physical device for the generation of One Time Passwords>** by the User.

The **signed and subscribed forms**, together with the **Assignment Register**, must be kept and archived by the Administrator for any possible dispute and made available to the Bank in the event of a request.

At this point the User can access the e-banking platform with his/her credentials i.e User ID + PIN + OTP (generated by UniCredit User Token).

In the period April – May 2019 the Bank will provide customers with a set of UniCredit User devices in order to be able to proceed with the assignment to the Users; the activation of the second security factor, i.e. the new method of accessing the internet banking, will take place starting from June 2019. The Administrators concerned will be notified by a message in UniWeb a few days before the actual introduction.

3. Assignment of UniCredit User device to a NEW user

The Company Profiles Administrator proceeds with the census of the Local User from the Corporate Portal “User Administration” area by selecting the “Create a new user” functionality at the top right.

The screenshot shows the UniCredit User Administration interface. At the top, there is a red header with the UniCredit logo and 'User administration'. Below this is a dark grey bar with 'Users'. The main area is titled 'Overview portal users' and contains a table of users. A red dashed box highlights the '+ Add new user' button in the top right corner of the table area.

<input type="checkbox"/>	First name	Last name	Date of birth	User type	User status	Application status	Actions
<input type="checkbox"/>		Alessandro	04.02.2019	Local user	Active	okay	
<input type="checkbox"/>		Barak		Local user	Active	okay	
<input type="checkbox"/>	pasquale		23.02.1988	Local user	Active	okay	
<input type="checkbox"/>	Matteo		15.06.1981	Local user	Active	okay	
<input type="checkbox"/>	francesco			User maintained by the bank	Active	okay	
<input type="checkbox"/>	Frank	Boss	07.05.1990	Local user	Active	okay	
<input type="checkbox"/>	Fra	Boss	02.10.2000	Local user	Inactive	Action needed	
<input type="checkbox"/>	Nicola		15.06.1981	Local user	Active	okay	
<input type="checkbox"/>	Giovanni			Local user	Active	okay	
<input type="checkbox"/>	cristina			User maintained by the bank	Partially blocked	okay	
<input type="checkbox"/>	enrico			User maintained by the bank	Active	okay	
<input type="checkbox"/>	AAAA	Cercasi		Local user	Active	okay	
<input type="checkbox"/>	BBB	Cercasi		Local user	Active	okay	
<input type="checkbox"/>	NomeTest	CognomeTest		Local user	Active	okay	
<input type="checkbox"/>	Pina	Delete	15.06.1981	Local user	Inactive	okay	

Fills in the fields with the User data and confirms by clicking on the button “Create”

The screenshot shows the UniCredit User Administration interface with the 'Add new user' form. The form is titled 'Add new user' and contains the following fields:

- Internal portal ID: L2237840209009261
- Last name:
- First name:
- Date of birth:
- Place of birth:
- Country of birth:
- Email:
- Additional email:

At the bottom right of the form, there are two buttons: 'Create' and 'Cancel'.

Once the User has been created, the Company Profiles Administrator presses the “+” button on the right. A new pop-up windows will appear and the Administrator will flag the applications to which the user will be enabled.

The screenshot shows the UniCredit user administration interface. At the top, there is a red header with the UniCredit logo and 'User administration'. Below this, the user profile for 'Rossi Andrea' is displayed with various attributes:

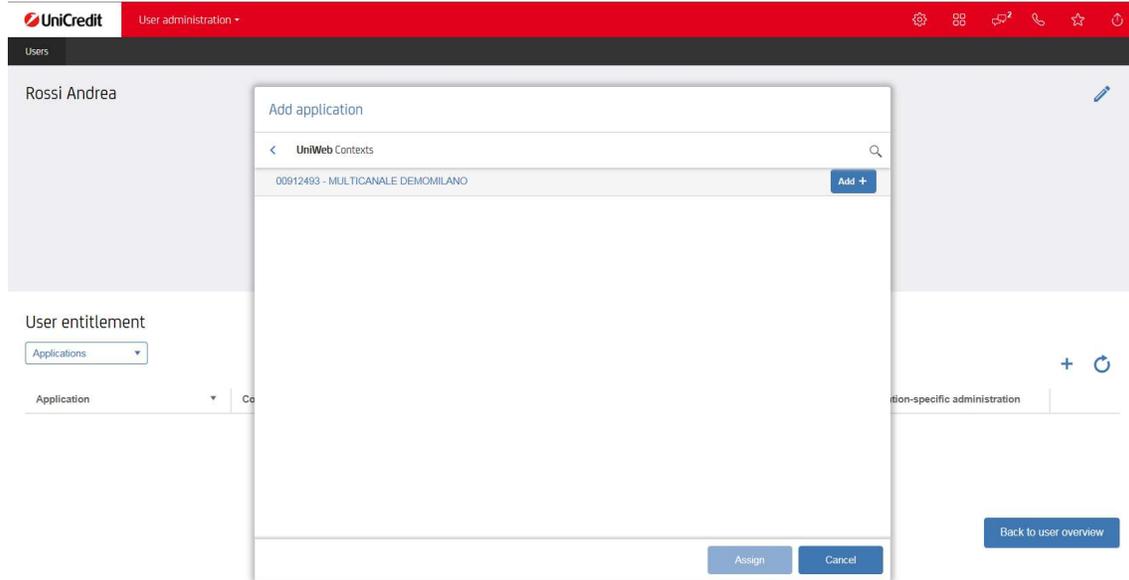
Internal portal ID	L2239010122153661	Email	andrea.rossi@fasi.it
Last name	Rossi	Additional email	--
First name	Andrea	Fiscal code	--
Date of birth	07.02.1977	User status	Inactive
Place of birth	Milano		
Country of birth	Italy		

Below the user profile, there is a 'User entitlement' section with a dropdown menu set to 'Applications'. A table with columns 'Application', 'Context', 'Application user ID', 'Status', and 'Application-specific administration' is shown, but it contains 'NO DATA AVAILABLE'. A red dashed box highlights the '+ Add new application' button in the top right corner of the table area. A 'Back to user overview' button is located at the bottom right.

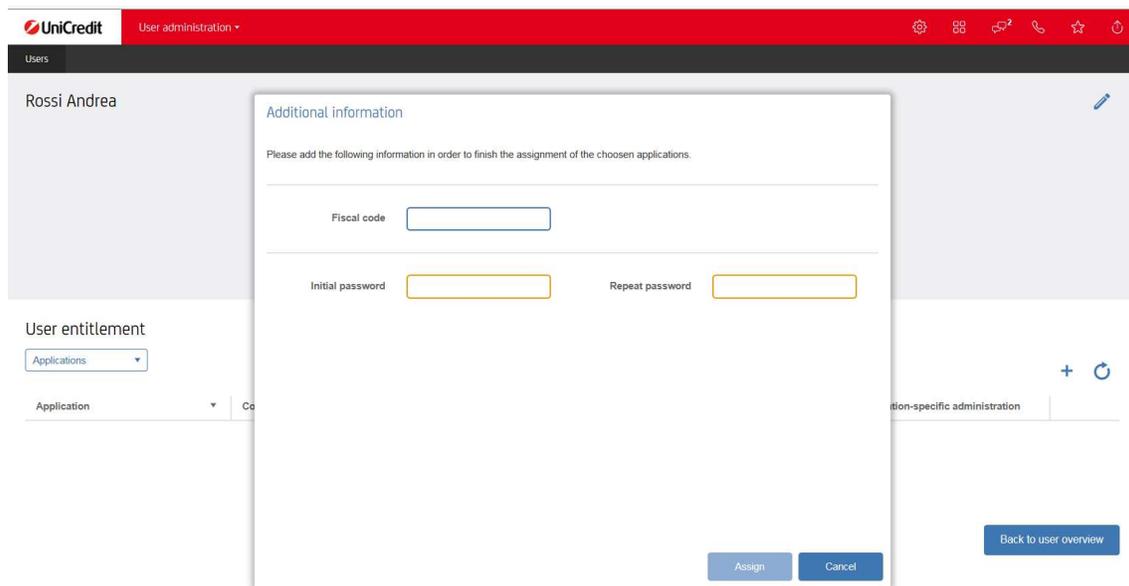
Example of UniWeb enablement: select the application **UniWeb**:

This screenshot shows the same user administration interface as above, but with the 'Add application' dialog box open. The dialog has a title 'Add application' and a section labeled 'Applications'. In this section, 'UniWeb' is selected and highlighted. At the bottom of the dialog, there are 'Assign' and 'Cancel' buttons. The background interface is dimmed, and the 'Back to user overview' button remains visible at the bottom right.

Selects the **Company REB** in UniWeb to which the new User is enabled



Indicates the User's **Fiscal code** and assigns a 5-digit **temporary PIN** (to be repeated twice in the procedure). Subsequently, at the first access, the User will be asked to modify it.



The User is still **Inactive** as shown in the following screen, as the Administrator will have to profile the specific authorizations in Uniweb by clicking on the “Activate user in UniWeb” in the lower right corner.

UniCredit User administration

Users

Rossi Andrea

Internal portal ID	L67436716	Email	test@test.it
Last name	Rossi	Additional email	--
First name	Andrea	Fiscal code	BSC
Date of birth	07.02.1977	Initial password	****
Place of birth	milano	User status	Inactive
Country of birth	italia		

User entitlement

Applications

Application	Context	Application user ID	Status	Application-specific administration
UniWeb	00912 - MULTICANALE		Inactive	Activate user in UniWeb

[Back to user overview](#)

By clicking on “Activate user in UniWeb” the system redirects to UniWeb > Administration area. In the section **Administration > Profiles and parameters Management > Users** it is displayed the summary of the Users.

UniCredit Uniweb

CBI ONLINE Financial services Administration INVOICECOMM AREA DOCUMENTI

Homepage
Profile and parameters management
Users
Privilege groups
Accounts
DocOnLine management parameters
CID Management
SEDA setup management
Local Scheduler
Security settings
Internal Approval

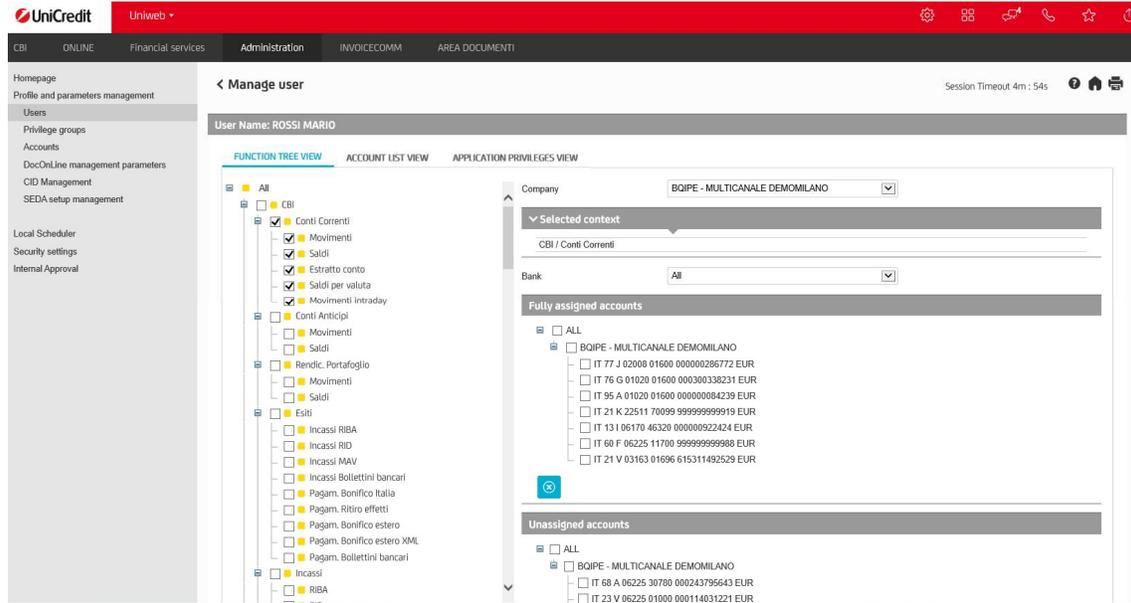
Manage User Session Timeout 2m : 57s

Filter

Users List

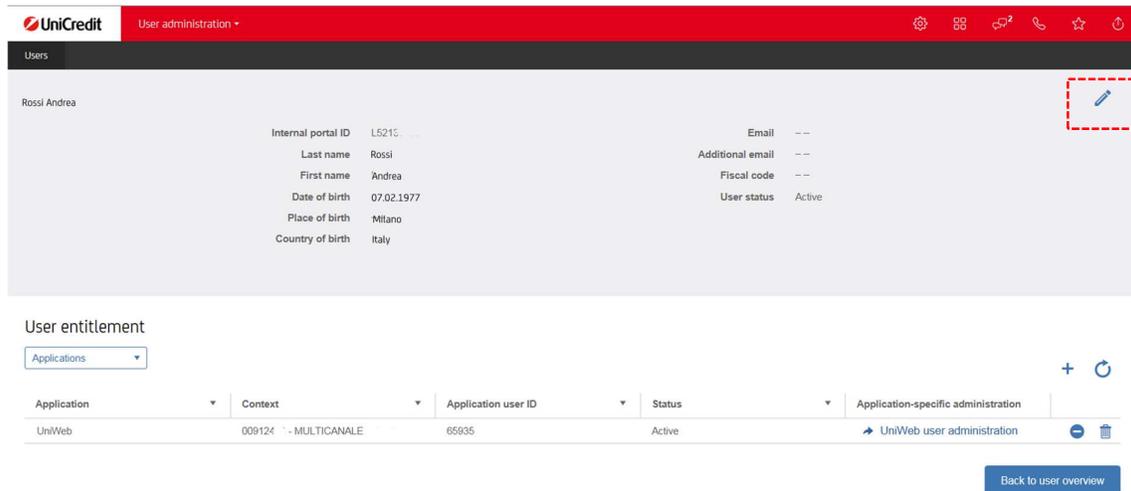
<input type="checkbox"/>	User_id	Name	Status	Functions	Account	Type	Actions
<input type="checkbox"/>	F9130498	BOSCARIELLO FRANCESCO	Active	■	■	Ucb Signatory A	
<input type="checkbox"/>	F6343740	CENTURIONI ENRICO	Active	■	■	Ucb Signatory A	
<input type="checkbox"/>	F0212456	PATUTO DANIELE	Active	■	■	Ucb Signatory A	
<input type="checkbox"/>	F4683659	FRANDINI EDMONDO	Active	■	■	Ucb Signatory	
<input type="checkbox"/>	F2570123	TABARELLI OMAR	Active	■	■	Ucb Signatory A	
<input type="checkbox"/>	F2132330	GARIGGIO MICHAELA	Active	■	■	Ucb Signatory A	
<input type="checkbox"/>	F6267060	GENSI CRISTINA	Active	■	■	Ucb Signatory	
<input type="checkbox"/>	F1474079	NICOLETTO RENZO	Active	■	■	Ucb Signatory	
<input type="checkbox"/>	62166820	ROSSI MARIO	Active	■	■	Local user	
<input type="checkbox"/>	67232865	Rossato Elena	Active	■	■	Local user	
<input type="checkbox"/>	60144559	Huber Robert	Active	■	■	Local user	
<input type="checkbox"/>	60622090	Maldonado German	Active	■	■	Local user	
<input type="checkbox"/>	60356450	Matiel Maria Ecaterina	Active	■	■	Local user	
<input type="checkbox"/>	66450180	Uni International Small Busin	Active	■	■	Local user	
<input type="checkbox"/>	65439889		Active	■	■	Local user	
<input type="checkbox"/>	69587295	prova nuovo test	Active	■	■	Local user	
<input type="checkbox"/>	61500810	Test Portale	Active	■	■	Local user	
<input type="checkbox"/>	66912291	psd2_pasquale_fx otp	Active	G	G	Local user G	
<input type="checkbox"/>	62111945	TEST1 TEST1	Active	■	■	Local user	

By clicking on the first icon on the right “edit authorizations” the relative menu will open



From here the Administrator selects UniWeb functions, company, accounts to which the user will be enabled.

At this point the Administrator returns to the “User Administration” Corporate Portal section and opens the User detail. Selects the pen at the top right “Edit”.



Selects “Add an OTP Token”

UniCredit Corporate portal

Edit user: Rossi Andrea

Internal portal ID: L1003774074

Last name: ROSSI | Email: test@test.it

First name: ANDREA | Additional email: |

Date of birth: 07.02.1977 | Fiscal code: PNC |

Place of birth: milano

Country of birth: italia

Serial number: | **Add OTP token**

Initial password: | Repeat password: | **Change password**

Save **Cancel**

Inserts:

- the **“UniCredit User” device serial number** located on the back of the device including all figures and letters without blank spaces or dashes
- the **One Time Password (OTP)** generated by the device itself

UniCredit User administration

Users

Edit user: Rossi Andrea

Internal portal ID: L10037740741157127

Last name: ROSSI | Email: test@test.it

First name: A |

Date of birth: 04 |

Place of birth: mi |

Country of birth: Ita |

Serial number: |

Initial password: | Repeat password: | **Change password**

Save **Cancel**

Add OTP token

Serial number: |

OTP: |

OK **Cancel**

The system returns the confirmation message that the OTP Token has been correctly assigned.

UniCredit Corporate portal

Editt user: Rossi Andrea

Internal portal ID L1003774074

Last name	ROSSI	Email	test@test.it
First name	ANDREA	Additional email	
Date of birth	07.02.1977	Fiscal code	PN*
Place of birth	milano		
Country of birth	italia		

Serial number 123456789

Print OTP Assignment

Initial password [masked] Repeat password [masked]

Change password

Save Cancel

The User can start operating on the Corporate Portal and UniWeb (or other services to which he/she has been enabled).

The Administrator proceeds with the physical delivery of the UniCredit User Token, of the PIN for the first access and the collection of the consent signed in the form **“Receipt of the physical device for the generation of One Time Passwords”**.

The **signed and subscribed forms**, together with the **Assignment Register**, must be kept and archived by the Administrator for any possible dispute and made available to the Bank in the event of a request.

At this point the User can access the e-banking platform with his/her credentials i.e User ID + PIN + OTP (generated by UniCredit User Token) and can change the PIN indicating one of his/her choice.

In the period April - May 2019 the new censed Users will follow the introduction of the SCA based on the migration envisaged for the Signatories. From June 2019, the new censed Users will access directly with the new mode.