STE-DDA Customer Service Portal

Operator Manual

TCH Confidential

Date: 1/18/2022

Version: 1.2

Authorization and Disclaimer

Document properties

Product build version	1.5.0-sp2
Classification	TCH Confidential
Status	Final
Publication date	January 2022

Table of Contents

Revision History

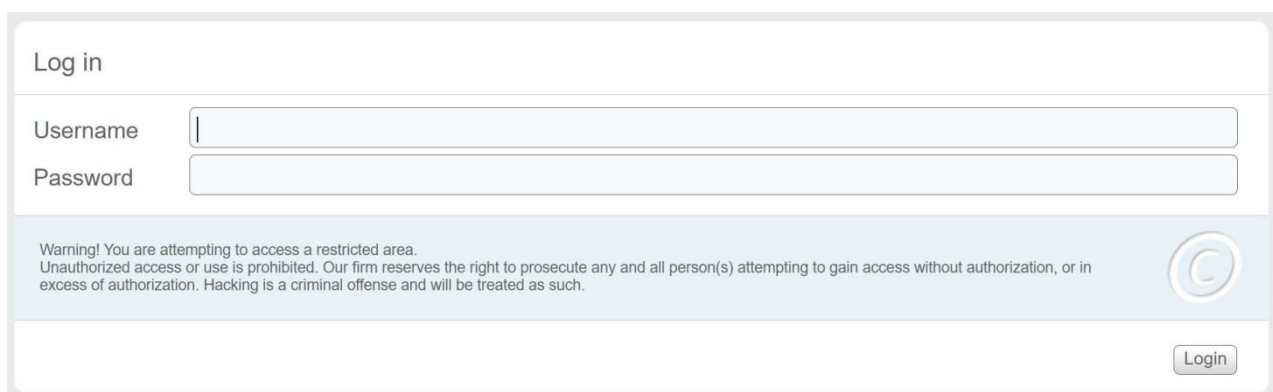| Version	Change	Comments
0.1	Initial Version	N/A
1.0	Final Version	N/A
1.1	Made updates as per 1.5.0-sp.1 release	N/A
1.2	Updated figure 5 in section 3.2	N/A

1. General

1.1. Purpose

The Customer Service Portal (CSP) is a component of the STE-DDA solution. The CSP provides an interface that enables participants in TCH payment networks to view and manage tokens that TCH has issued for their accounts.

2. User Login

2.1. Login

Once users have successfully navigated to the Customer Service Portal, the login page appears. Users must enter their correct username and password in order to access the Customer Service Portal.

Figure 1: Login screen

Enter the Username in the Username field.

Enter the Password in the Password field.

Press Enter or click **Login**.

2.2. New CSP users

New Customer Service Portal users will receive an email from TCH with an initial, one time password.

> *Note that this password is valid for a limited time and can only be used for the initial login.*

Enter the initial password for the first time log in.

Then enter a new password following the password rules (Password Help gives an overview of the password rules to follow to create a new password.)

Re-enter the new password.

Choose a security question and answer.

2.3. Changing your password

To change the current password,

from the top menu click on **User/Change Password**.

Following screen will appear.

Figure 2: Change password screen

Enter the current password

Enter the new password.

Re-enter the new password.

Click **Save**

3. Customer Service Portal Functions
3.1. Searching in Customer Service Portal

After login, the **Dashboard** page is displayed. From this page, users can perform a search to retrieve token and account information.

Navigate to **Home** if the **Dashboard** page is not displayed.

Users can search for full and exact values only. Wildcards (e.g. using '*' or '?') cannot be used in the search. The system retrieves all tokens linked to the search value.

The search takes into account which Financial Institution the user belongs to: the user can only retrieve tokens and account information for accounts that belong to that Financial Institution.

TCH Confidential

Figure 3: Customer Service Portal Dashboard with Search box.

The default search option is to search by the Real Routing + Real Account number to retrieve linked tokens. Enter the full and exact value in the search field as a combined number (Example: 9999999992343232123). Click **Search**.

Changing the default search option

The following search options are available:
- Real routing + real account number
- Token routing + token account number
- Token account creation date. (Use the dd.mm.yyyy format)

Click on the **+** *button in* the **Options** panel to expand to view all the different search options.

Select a different search option by clicking inside the radio button to select it.
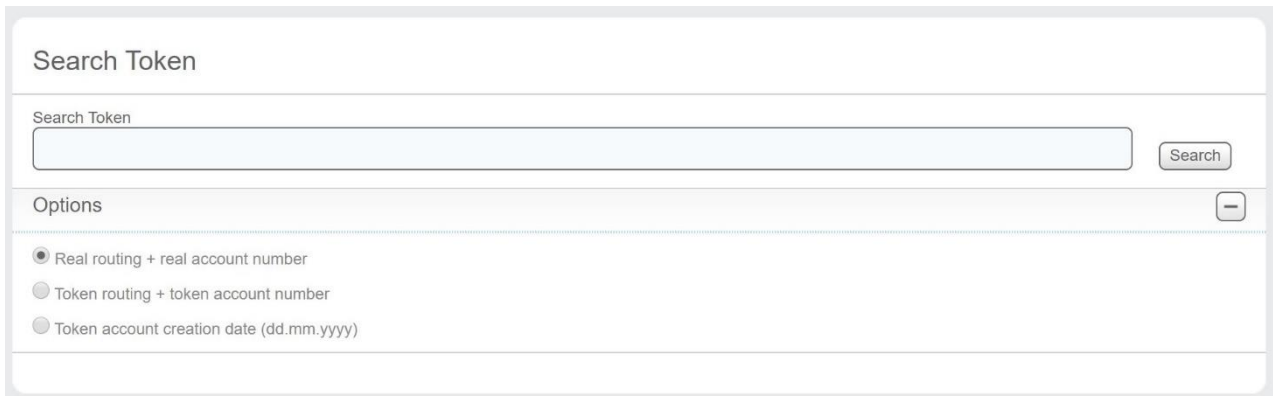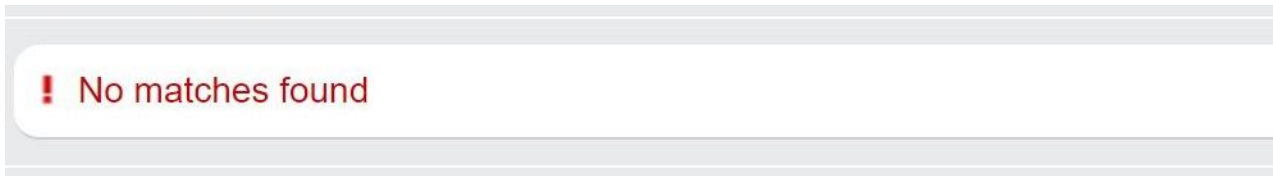

Figure 4: Search Token

If the search is successful, the **Token Overview** page is displayed with the search results. Otherwise, a message is displayed above the search box indicating that the search did not find any results. See message below:

3.2. CSP Token overview page

The CSP Tokens Overview page displays all tokens that meet the search criteria.

Figure 5: CSP Tokens Overview

The following information is displayed in the **CSP Tokens Overview** page:

Property	Description
Token Reference ID	Unique Reference ID of the Account Token
Real Routing	The routing number of the real account numbers
Real Account	The real Account Number
Token Routing	The routing number of the tokenized account numbers
Token Account	Token Account number linked to the real account
Counter Party Routing	The counter party routing number that is linked to the token

Property	Description
Counter Party Account	The counter party account number that is linked to the token. If a token is linked to a counter party account, it can only be used for payments to this account.
Expiry Date	Expiry date of the token
State	Current lifecycle state of the token
Last Event	Date/time of last action performed on the token
Financial Institution	Name of the financial institution
Token Requestor ID	Identifier of the Token Requestor that owns the account token.
Requestor	The name of the Token Requestor entity which provisioned the Account Token.
RequestedDate	Date/time of the token request (=tokenization request).
Domain	Name of the domain the token belongs to.

Figure 6: Token overview fields

3.3. Changing the state of a token

Token Lifecycle is shown below.
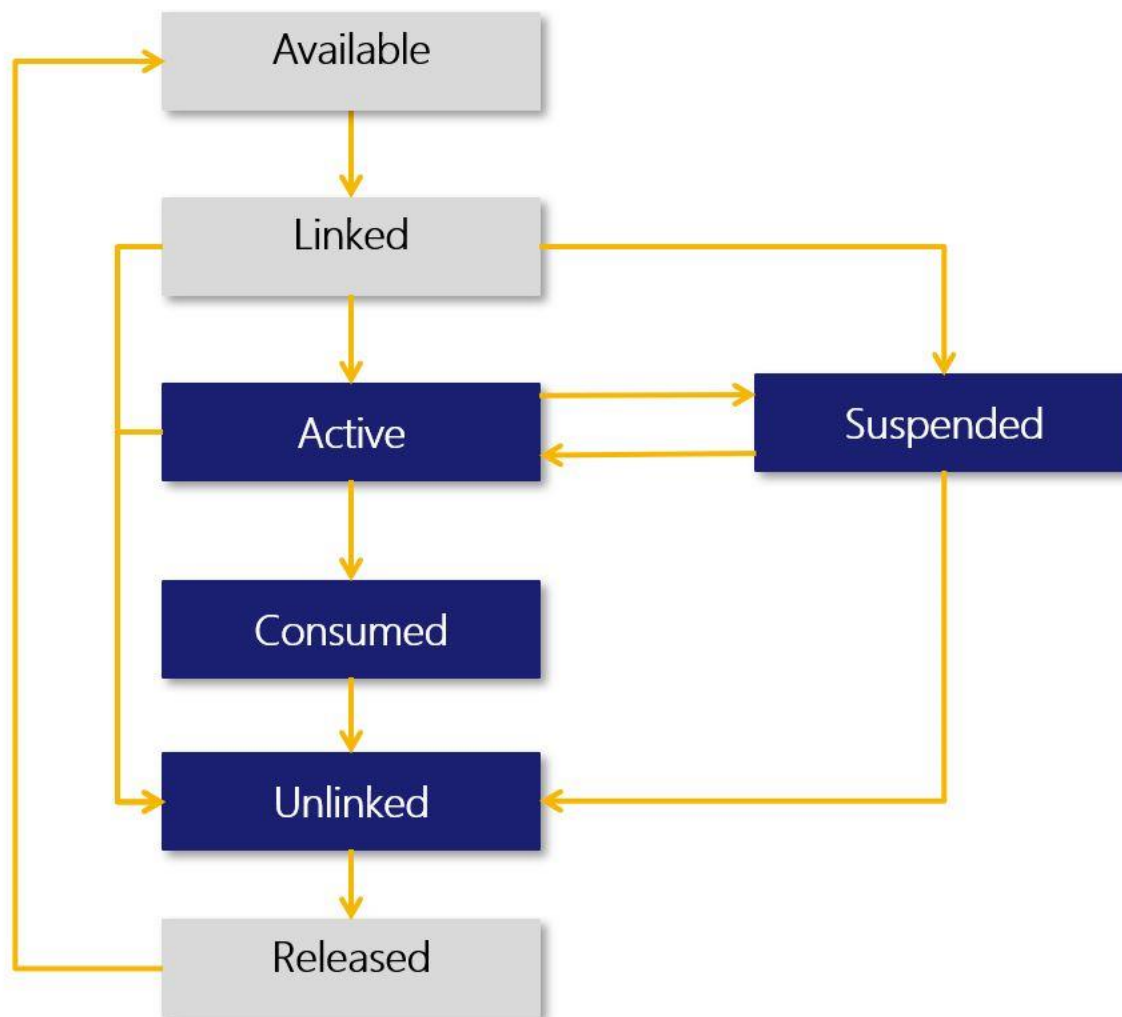
Figure 7: Lifecycle of the account token

State	Description
Available	At regular intervals, new tokens are created for each Financial Institution in the *Available* state. A scheduled job checks if the number of available tokens falls below the *low water mark* and if so, it generates tokens until it reaches *high water mark*. The low and high water marks are set when configuring a Financial Institution.
Linked	When a token request comes in for a Financial Institution's account, an available token for the Financial Institution is linked to the real account it was requested for. It is then in the *Linked* state.
Active	Upon successful provisioning, a token will be in an Active state and ready for use. A token can only be used in a transaction when it is in the *Active* state.
Suspended	A token can be suspended, meaning it can temporarily not be used. The reason can be that fraud is suspected. Tokens can be suspended by the Financial Institution or Token Requestor. A suspended token can be activated (again).
Consumed	When a token expires, it moves to the *Consumed* state. In addition, if a single-use token is used in a transaction it moves to the *Consumed* state.
Unlinked	If a token is unlinked, the link with the Account is removed.
Released	After a configured period of time, an unlinked token is released. From that moment, it can become available again for re-use.

Changing the Token State

Search for the token to be changed.

The Tokens Overview page shows the tokens that match the search criteria.

Figure 8: Tokens Overview screen

Select the token by clicking on the row in the Tokens Overview page.

Click *Change state*.

Figure 9: Change State pop up

Property	Description
Action	Select an action from the drop down list. Note that the contents of the drop down list depend on the current state of the token and shows only the possible state transitions. For instance, 'Activate' is only visible when the token is in state 'Suspended'.

Property	Description
Reason	To provide a reason for performing the state change. The value entered will be added to the Remark column in the audit trail. Usually, this field is optional, but when unlinking an active token the reason is mandatory.
Next state	Shows the next state. This state is reached after selecting the proper action and clicking *Apply now*.

Figure 10: Change State pop-up fields

Select the action.

Enter a reason for the state change (optional).

Click **Apply now**.

Note that the state change is registered in the audit trail for the token.

3.4. Unmasking Token and Account Numbers

By default, the CSP user interface masks the Real Account Numbers, Token Account Numbers and Counterparty Account Numbers.

CSP users can be authorized to unmask Real Account Numbers and/or Token Account Numbers. In that case, the Unmask Token/Account button is enabled in the Tokens Overview screen when a row is selected.

Unmasking Token and Account Numbers

Search for the token to be unmasked.

The Tokens Overview page shows the tokens that match the search criteria.

#	Real Routing	Real Account	Token Routing	Token Account	Counter Party Routing	Counter Party Account	Expiry Date	State	Last Event	Financial Institution	RequestedDate	Domain
1	023456789	000000*****1708	222456789	999999*****8405			12/21	Unlinked	Tue Jan 19 14:05:00 CET 2021	Bank TWO	Sat Jan 16 14:01:43 CET 2021	Domain for Direct API
2	023456789	000000*****1705	222456789	999999*****0252			12/21	Unlinked	Tue Jan 19 14:05:00 CET 2021	Bank TWO	Sat Jan 16 14:01:41 CET 2021	Domain for Direct API
3	023456789	000000*****2179	222456789	999999*****8622	033456789	000000*****1580	12/21	Active	Sat Jan 16 14:28:33 CET 2021	Bank TWO	Sat Jan 16 14:28:33 CET 2021	Domain for Direct API
4	023456789	000000*****2178	222456789	999999*****3573	033456789	000000*****1580	12/21	Active	Sat Jan 16 14:28:32 CET 2021	Bank TWO	Sat Jan 16 14:28:32 CET 2021	Domain for Direct API
5	023456789	000000*****2177	222456789	999999*****2300	033456789	000000*****1579	12/21	Active	Sat Jan 16 14:28:30 CET 2021	Bank TWO	Sat Jan 16 14:28:30 CET 2021	Domain for Direct API
6	023456789	000000*****2176	222456789	999999*****3411	033456789	000000*****1579	12/21	Active	Sat Jan 16 14:28:30 CET 2021	Bank TWO	Sat Jan 16 14:28:30 CET 2021	Domain for Direct API
7	023456789	000000*****2175	222456789	999999*****9297	033456789	000000*****1578	12/21	Active	Sat Jan 16 14:28:28 CET 2021	Bank TWO	Sat Jan 16 14:28:28 CET 2021	Domain for Direct API
8	023456789	000000*****2174	222456789	999999*****8751	033456789	000000*****1578	12/21	Active	Sat Jan 16 14:28:27 CET 2021	Bank TWO	Sat Jan 16 14:28:27 CET 2021	Domain for Direct API
9	023456789	000000*****2173	222456789	999999*****5094	033456789	000000*****1577	12/21	Active	Sat Jan 16 14:28:26 CET 2021	Bank TWO	Sat Jan 16 14:28:26 CET 2021	Domain for Direct API
10	023456789	000000*****2172	222456789	999999*****5309	033456789	000000*****1577	12/21	Active	Sat Jan 16 14:28:25 CET 2021	Bank TWO	Sat Jan 16 14:28:25 CET 2021	Domain for Direct API
11	023456789	000000*****2171	222456789	999999*****9540	033456789	000000*****1576	12/21	Active	Sat Jan 16 14:28:24 CET 2021	Bank TWO	Sat Jan 16 14:28:24 CET 2021	Domain for Direct API
12	023456789	000000*****2171	222456789	999999*****5803	033456789	000000*****1575	12/21	Active	Sat Jan 16 14:28:23 CET 2021	Bank TWO	Sat Jan 16 14:28:23 CET 2021	Domain for Direct API
13	023456789	000000*****2171	222456789	999999*****4226	033456789	000000*****1574	12/21	Active	Sat Jan 16 14:28:22 CET 2021	Bank TWO	Sat Jan 16 14:28:22 CET 2021	Domain for Direct API
14	023456789	000000*****2171	222456789	999999*****1767	033456789	000000*****1571	12/21	Active	Sat Jan 16 14:28:21 CET 2021	Bank TWO	Sat Jan 16 14:28:21 CET 2021	Domain for Direct API
15	023456789	000000*****2170	222456789	999999*****9646	033456789	000000*****1573	12/21	Active	Sat Jan 16 14:28:21 CET 2021	Bank TWO	Sat Jan 16 14:28:21 CET 2021	Domain for Direct API
16	023456789	000000*****2170	222456789	999999*****2901	033456789	000000*****1572	12/21	Active	Sat Jan 16 14:28:20 CET 2021	Bank TWO	Sat Jan 16 14:28:20 CET 2021	Domain for Direct API
17	023456789	000000*****2170	222456789	999999*****7772	033456789	000000*****1571	12/21	Active	Sat Jan 16 14:28:19 CET 2021	Bank TWO	Sat Jan 16 14:28:19 CET 2021	Domain for Direct API
18	023456789	000000*****2169	222456789	999999*****8961	033456789	000000*****1570	12/21	Active	Sat Jan 16 14:28:18 CET 2021	Bank TWO	Sat Jan 16 14:28:17 CET 2021	Domain for Direct API
19	023456789	000000*****2168	222456789	999999*****8383	033456789	000000*****1569	12/21	Unlinked	Sat Jan 16 14:28:16 CET 2021	Bank TWO	Sat Jan 16 14:28:15 CET 2021	Domain for Direct API
20	023456789	000000*****2167	222456789	999999*****8646	033456789	000000*****1568	12/21	Unlinked	Sat Jan 16 14:28:14 CET 2021	Bank TWO	Sat Jan 16 14:28:13 CET 2021	Domain for Direct API

Total 163   1 2 3 4 5 6 7 8 9 > >>

Unmask Token/Account Update Counter Party Data Replace Account Update Token Expiry Date Change state View Audit Trail

Figure 11: Tokens Overview screen

Select the token by clicking on the row in the Tokens Overview page.

Click **Unmask Token/Account**.

A pop-up window will appear that shows the unmasked Account Number and/or Token Number.

Depending on their authorization levels, a user can see the unmasked Token Number, Account Number or both.
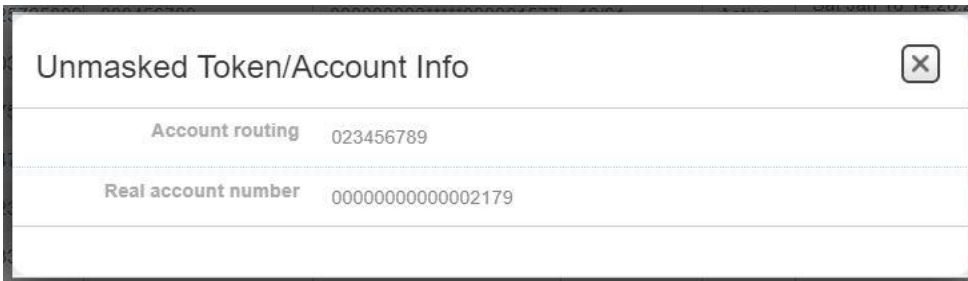
Figure 12: Unmasked Account Number

Or
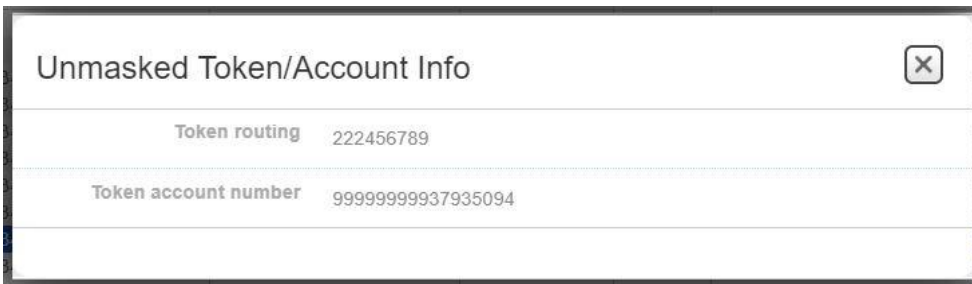
Figure 13: Unmasked Token Number

Or
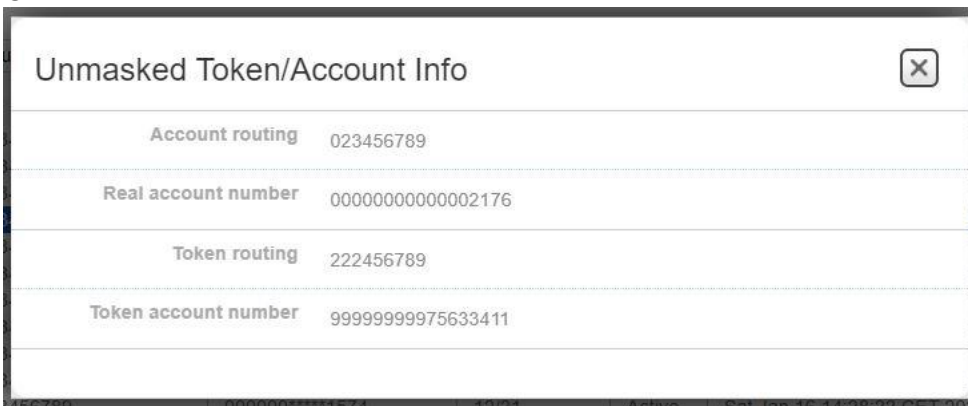
Figure 14: Unmasked Account and Token Numbers

Close the pop-up window to remove the unmasked account and/or token numbers from screen.

3.5. Update Token Expiry Date

CSP users can be authorized to update the expiry date of a token.

Updating the Token Expiry Date

Search for the token to be updated.

The Tokens Overview screen shows the tokens that match the search criteria.

Figure 15: Tokens Overview screen

Select the token by clicking on the row in the Tokens Overview page.

Click *Update Token Expiry Date.*

Figure 16: Update Token Expiry Date

Enter the new expiry date in format mmyy (e.g. 1223).

Click *Apply now,*

The account token expiry date is now updated.

> *In case the 'Update Expiry Date' button is disabled, there can be several reasons:*
>
> *- The token does not support this restriction, e.g. for RTP In-Network tokens.*

> *-The user is not authorized to perform this function.*

3.6. Update Counter Party Data

Some tokens are linked to a counter party account, which means that they can only be used for payments to this account. CSP users can be authorized to add or update a counter party account number and routing number for an active token.

Updating the Counter Party

Search for the token to be updated.

The Tokens Overview screen shows the tokens that match the search criteria.

Figure 17: Token Overview screen

Select the token by clicking on the row in the Tokens Overview page.

Click *Update Counter Party Data.*

Figure 18: Update Counter Party Data

Enter the new counter party routing number and the new counter party account number.

Click **Save**.

The new counter party data is now linked to the token.

> *In case the* 'Update Counter Party Data' *button is disabled, there can be several reasons:*
>
> *- The token does not support this restriction, e.g. for RTP In-Network tokens.*
>
> *-The user is not authorized to perform this function.*

3.7. Update Real Account number

CSP users can be authorized to link a new real account number and real routing number to an existing active or suspended token

Updating the Real Account number

Search for the token to be updated.

The Tokens Overview screen shows the tokens that match the search criteria.

Tokens Overview

#	Real Routing	Real Account	Token Routing	Token Account	Counter Party Routing	Counter Party Account	Expiry Date	State	Last Event	Financial Institution	RequestedDate	Domain
1	023456789	000000*****1708	222456789	999999*****8405			12/21	Unlinked	Tue Jan 19 14:05:00 CET 2021	Bank TWO	Sat Jan 16 14:01:43 CET 2021	Domain for Direct API
2	023456789	000000*****1705	222456789	999999*****0252			12/21	Unlinked	Tue Jan 19 14:05:00 CET 2021	Bank TWO	Sat Jan 16 14:01:41 CET 2021	Domain for Direct API
3	023456789	000000*****2179	222456789	999999*****8622	033456789	000000*****1580	12/21	Active	Sat Jan 16 14:28:33 CET 2021	Bank TWO	Sat Jan 16 14:28:33 CET 2021	Domain for Direct API
4	023456789	000000*****2178	222456789	999999*****3573	033456789	000000*****1580	12/21	Active	Sat Jan 16 14:28:32 CET 2021	Bank TWO	Sat Jan 16 14:28:32 CET 2021	Domain for Direct API
5	023456789	000000*****2177	222456789	999999*****2300	033456789	000000*****1579	12/21	Active	Sat Jan 16 14:28:30 CET 2021	Bank TWO	Sat Jan 16 14:28:30 CET 2021	Domain for Direct API
6	023456789	000000*****2176	222456789	999999*****3411	033456789	000000*****1579	12/21	Active	Sat Jan 16 14:28:30 CET 2021	Bank TWO	Sat Jan 16 14:28:30 CET 2021	Domain for Direct API
7	023456789	000000*****2175	222456789	999999*****9297	033456789	000000*****1578	12/21	Active	Sat Jan 16 14:28:28 CET 2021	Bank TWO	Sat Jan 16 14:28:28 CET 2021	Domain for Direct API
8	023456789	000000*****2174	222456789	999999*****8751	033456789	000000*****1578	12/21	Active	Sat Jan 16 14:28:27 CET 2021	Bank TWO	Sat Jan 16 14:28:27 CET 2021	Domain for Direct API
9	023456789	000000*****2173	222456789	999999*****5094	033456789	000000*****1577	12/21	Active	Sat Jan 16 14:28:26 CET 2021	Bank TWO	Sat Jan 16 14:28:26 CET 2021	Domain for Direct API
10	023456789	000000*****2172	222456789	999999*****5309	033456789	000000*****1577	12/21	Active	Sat Jan 16 14:28:25 CET 2021	Bank TWO	Sat Jan 16 14:28:25 CET 2021	Domain for Direct API
11	023456789	000000*****2171	222456789	999999*****9540	033456789	000000*****1576	12/21	Active	Sat Jan 16 14:28:24 CET 2021	Bank TWO	Sat Jan 16 14:28:24 CET 2021	Domain for Direct API
12	023456789	000000*****2171	222456789	999999*****5803	033456789	000000*****1575	12/21	Active	Sat Jan 16 14:28:23 CET 2021	Bank TWO	Sat Jan 16 14:28:23 CET 2021	Domain for Direct API
13	023456789	000000*****2171	222456789	999999*****4226	033456789	000000*****1574	12/21	Active	Sat Jan 16 14:28:22 CET 2021	Bank TWO	Sat Jan 16 14:28:22 CET 2021	Domain for Direct API
14	023456789	000000*****2171	222456789	999999*****1767	033456789	000000*****1571	12/21	Active	Sat Jan 16 14:28:21 CET 2021	Bank TWO	Sat Jan 16 14:28:21 CET 2021	Domain for Direct API
15	023456789	000000*****2170	222456789	999999*****9646	033456789	000000*****1573	12/21	Active	Sat Jan 16 14:28:21 CET 2021	Bank TWO	Sat Jan 16 14:28:21 CET 2021	Domain for Direct API
16	023456789	000000*****2170	222456789	999999*****2901	033456789	000000*****1572	12/21	Active	Sat Jan 16 14:28:20 CET 2021	Bank TWO	Sat Jan 16 14:28:20 CET 2021	Domain for Direct API
17	023456789	000000*****2170	222456789	999999*****7772	033456789	000000*****1571	12/21	Active	Sat Jan 16 14:28:19 CET 2021	Bank TWO	Sat Jan 16 14:28:19 CET 2021	Domain for Direct API
18	023456789	000000*****2169	222456789	999999*****8961	033456789	000000*****1570	12/21	Active	Sat Jan 16 14:28:18 CET 2021	Bank TWO	Sat Jan 16 14:28:17 CET 2021	Domain for Direct API
19	023456789	000000*****2168	222456789	999999*****8383	033456789	000000*****1569	12/21	Unlinked	Sat Jan 16 14:28:16 CET 2021	Bank TWO	Sat Jan 16 14:28:15 CET 2021	Domain for Direct API
20	023456789	000000*****2167	222456789	999999*****8646	033456789	000000*****1568	12/21	Unlinked	Sat Jan 16 14:28:14 CET 2021	Bank TWO	Sat Jan 16 14:28:13 CET 2021	Domain for Direct API

Total 163   1 2 3 4 5 6 7 8 9 > >>

[Unmask Token/Account] [Update Counter Party Data] [Replace Account] [Update Token Expiry Date] [Change state] [View Audit Trail]

Figure 19: Token Overview screen

Select the token by clicking on the row in the Tokens Overview page.

Click **Replace Account**

Figure 20: Replace Account

Enter the New Account Number. The Account Routing Number cannot be modified.

Enter a reason for the state change (optional).

Click **Apply now**.

The real account number is now updated.

3.8. Viewing the audit trail of a token

All state changes, tokenization and detokenization operations applied to a token are registered in the audit trail. State changes can be initiated by a CSP User, by internal processing, or by external systems, for instance the Token Requestor API or Transaction API.

To display a token's audit trail:

Search for the specific token using Token Number, Account Number or by date.

Select the token.

Click **View Audit Trail**.

Figure 21: View Audit Trail

The following information is displayed in the CSP Audit Trail page:

Property	Description
User	User name or process name that initiated the event on the token, a state change, tokenize or detokenize operation.
Timestamp	Date/time when the event on the token occurred.
Event	Type of event performed on the token.
By	User or process that initiated the event. Options are FI, TR, CSP, SYSTEM or TXN_API_BROKER.
From state	Original state before the event on the token.
To state	New state after the event on the token.

Property	Description
Reason	Reason for the event to happen. Optionally supplied by the user during the event initiation.
Request Type	The type of transaction in case of tokenization and detokenization: ▪ CREDIT_TRANSFER ▪ REQUEST_FOR_PAYMENT ▪ REQUEST_REMITTANCE_ADVICE
Currency	The currency of the transaction as per ISO-3166 currency codes specification.
Txn ID	Transaction Identifier as generated by the Participant that sent transaction.
Single Use	Identifier whether the token is single use or multiple use.
Amount	Transaction amount.

Figure 22: Audit trail fields

Click **Back** to return to Tokens Overview page

4. Administration

4.1. User Configuration Overview

During initial configuration, several groups and users are automatically created. Additional users/groups can be created and managed from the User Management menu in the CSP. The User Management menu also provides options to manage password configuration and language preferences.

4.1.1. User Rights Configuration

Initial configuration of users and groups is described below;

- A 3 digit prefix is assigned to each Financial Institution during onboarding.
- This prefix is embedded in each of the three group names and the three usernames that are automatically created.
- In this manual the prefix is referred to as <iss>

The default configuration as set up automatically during onboarding of a financial institution.

Group	Role	User	Rights
<iss> Issuers Level 1	CSP Issuer Level 1	<iss>IssuerL1	Token information can be searched and retrieved. Token state changes audit information can be retrieved.
<iss> Issuers Level 2	CSP Issuer Level 1 CSP Issuer Level 2	<iss>IssuerL2	Same as Level 1 role and they can view log information and unlink tokens.
<iss> CSP Administrators	CSP Issuer Level 1 CSP Issuer Level 2 CSP Administrators	<iss>Admin	Same as Level 1 and Level 2 roles and they can create or delete users, modify user rights, restrict user access and retrieve other data from the STE-DDA.

Figure 23: Default configuration

The configuration limits the viewing of masked Account Numbers, Token Numbers, Users, etc. to the ones belonging to the 'owner' Financial Institution.

4.1.2. Password management

Initial password

When creating a new user, a password for the new user is generated automatically. This initial password is valid for a limited time. The time limit is configurable as a system parameter and is the same for all system generated passwords.

The newly created user receives this generated password via email and will be required to change this for a real password after the first login. The user will also have to choose a security question and answer which are used during the password reset process.

Password reset

After logging in, the user clicks *Reset/change password*. The user will receive an email with a link to reset the

password. The used email address is configured in CSP Users module. Clicking the link brings the user to a page where the security question is asked.

Once the user answers the security question correctly, the user is required to set a new password and to update the security question and answer if desired. After the password is reset, the user will login with the new password to access to CSP.

Administration

There is a button in the CSP user module available to resend the invitation email (after selecting a user).

Configuration

The CSP administrator can configure the secure password reset option for their financial institution. If the option is disabled, the security question and email is not used.

4.1.3. User management

The User Management function of the CSP can be used by the financial institution admin user (<iss>Admin) to add or remove users and manage user passwords.
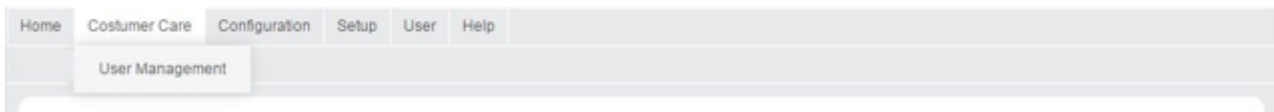

Figure 25: User Management menu

4.1.4. Users overview

In the main menu, select **Customer Care** > **User Management** to open the **Users** overview page.
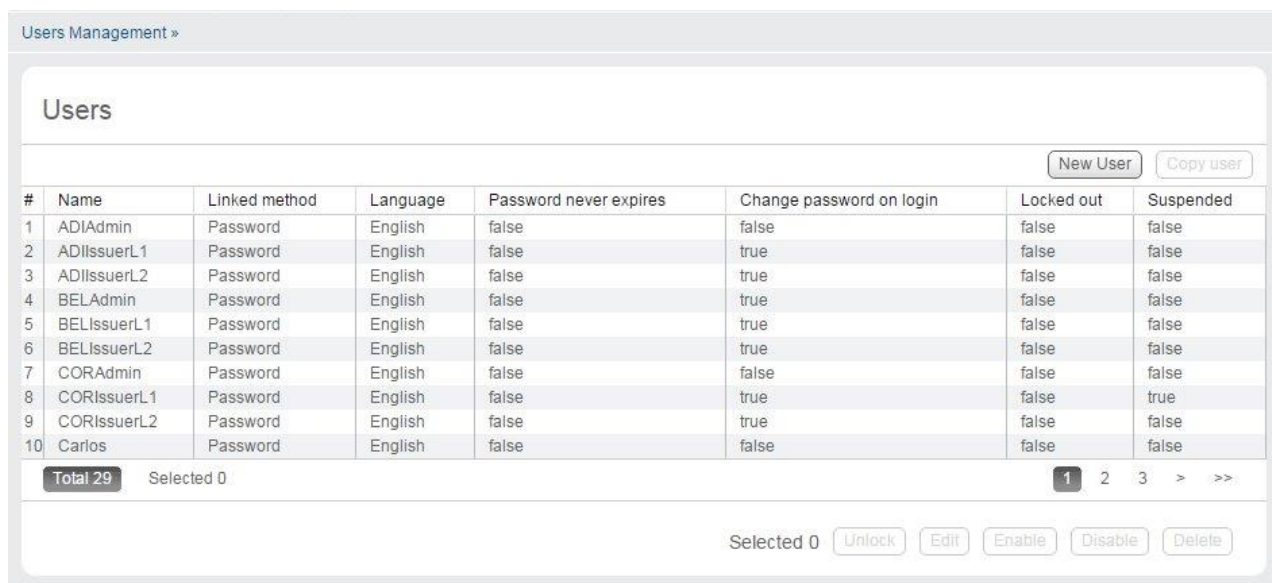

Figure 26: Users overview

The **Users** overview shows the following columns:

Property	Description
Name	User- or login name.
Linked Method	Login method; for now always 'password'.

Property	Description
Language	The language in which the user interface is displayed for this user. Default and always available is English. All other languages are only relevant if translations have been uploaded using the User Rights Module.
Password never expires	If this check box is selected, the password can remain the same and the password does not need to be updated periodically.
Change password on login	Password must be changed on next login to CSP.
Locked out	The user is locked out from login (too many faulty login tries).
Suspended	The user is temporarily suspended from login.

Figure 27: User Overview

4.1.5. Adding a Customer Service Portal user

Perform the following steps to create a user for Customer Service Portal.

In the main menu, select **Customer Care** > **User Management** to open the **Users** overview page.

The following screen appears.

Users Management »

Users

#	Name	Linked method	Language	Password never expires	Change password on login	Locked out	Suspended
1	ADIAdmin	Password	English	false	false	false	false
2	ADIIssuerL1	Password	English	false	true	false	false
3	ADIIssuerL2	Password	English	false	true	false	false
4	BELAdmin	Password	English	false	true	false	false
5	BELIssuerL1	Password	English	false	true	false	false
6	BELIssuerL2	Password	English	false	true	false	false
7	CORAdmin	Password	English	false	false	false	false
8	CORIssuerL1	Password	English	false	true	false	true
9	CORIssuerL2	Password	English	false	true	false	false
10	Carlos	Password	English	false	false	false	false

Total 29 Selected 0 **1** 2 3 > >>

Selected 0 Unlock Edit Enable Disable Delete

Figure 29: Users overview

Click **New user**.

The following screen appears.

User properties

Users Management » User settings »

Edit details

!	Login	
!	Password	••••••••••••
		••••••••••••
	First names	
	Last name	
	Language	Choose One
	Password never expires	☐
	Locked out	
	Suspended	☐
!	Authentication method	Choose One

Select groups [−]

Available groups

IS1 Administrators
IS1 Issuers

→ ← ▶▶ ◀◀

Selected groups

Cancel   Save

Figure 30: User properties

Enter the new user information.

Property	Description
Login	Name of the user. The user has to enter this name as the user name while logging in.
Password	The password the user has to use to log on to the system. If these fields are not available, the password is generated automatically.
First names	Given name(s) of the user.
Last name	Family name of the user.
Language	The language in which the user interface is displayed for this user. Default and always available is English. All other languages are only relevant if translations have been uploaded using the User Rights Module.
Password never expires	If this check box is selected, the password can remain the same and the password does not need to be updated periodically.
Locked out	Not relevant when creating a user.
Suspended	Not relevant when creating a user.
Authentication method	The method in which the user can be verified when they log on to the system.
Select groups	Link User Rights Module groups to user. Note that '<prefix> FI Level 1' and '<prefix> FI Level 2' is used for daily operators and administrators; '<prefix> FI CSP Administrators' is meant for administrators only.

Figure 31: User properties

The CSP automatically generates passwords for these users that must be changed. This can be done via **Customer Care** > **User Management** by editing these users.

4.1.6. Copy a user

In the main menu, select **Customer Care** >**User Management** to open the **Users** overview page.
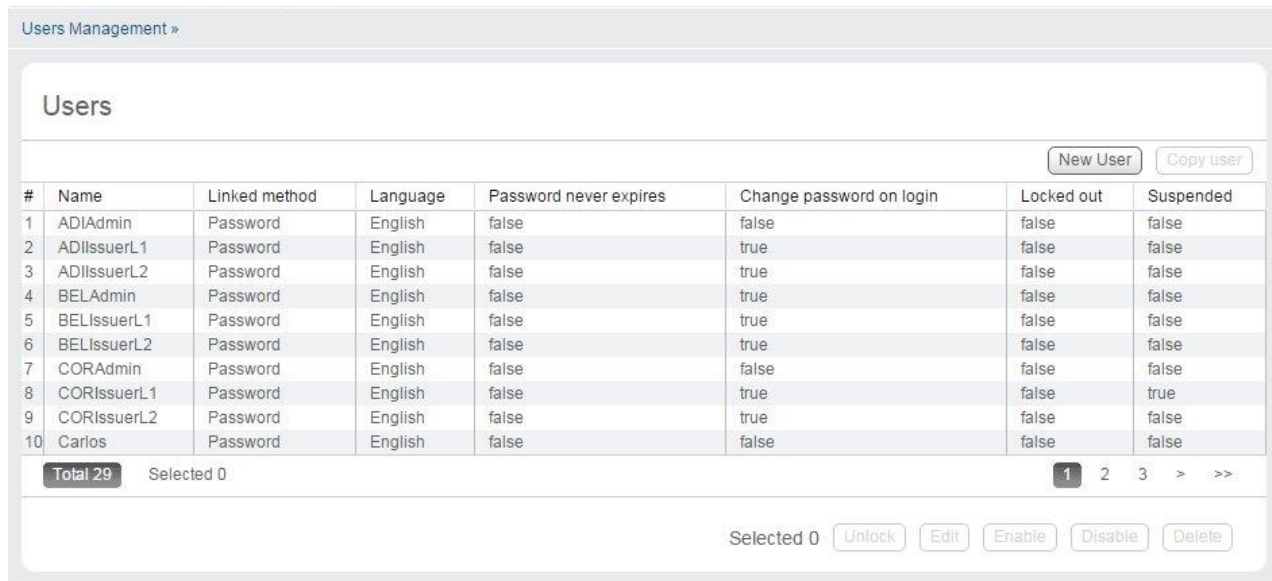

Figure 32: Users overview

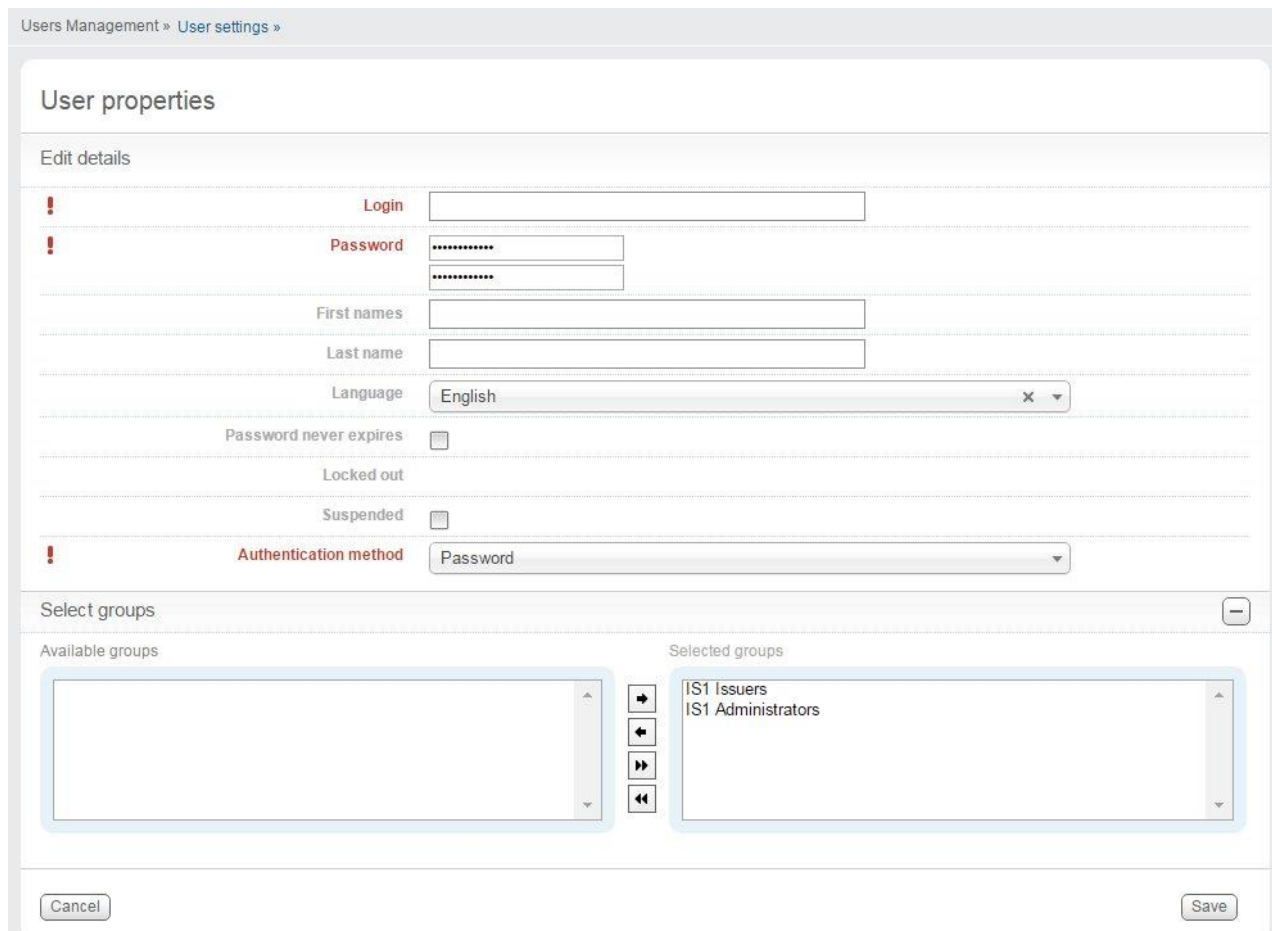Select the user record to be copied.

Click **Copy user**.

Figure 33: User properties filled in along with the "source User"

Change the properties according to the following table.

Property	Description
Login	Name of the user. The user has to enter this name as the user name while logging in.
Password	The password the user has to use to log on to the system.
First names	Given name(s) of the user.
Last name	Family name of the user.
Language	The language in which the user interface is displayed for this user. Default and always available is English. All other languages are only relevant if translations have been uploaded using the User Rights Module.
Password never expires	If this check box is selected, the password can remain the same and the password does not need to be updated periodically.
Locked out	If checked: The "source" user was locked out while the copy was made.
Suspended	If checked: The "source" user was suspended while the copy was made.
Authentication method	The method in which the user can be verified when they log on to the system.
Selected groups	Link User Rights Module groups to user. Note that <prefix> FI Level 1 and <prefix> FI Level 2 is used for daily operators and administrators; <prefix> CSP FI Administrators is meant for administrators only.

Figure 34: User properties

Click *Save*.

4.1.7. Unlock a user

A user will be locked after entering a wrong password multiple times. With this functionality, you can unlock a locked user.

Step 1:

Set a new password for this user first.

In the main menu, select **Customer Care** > **User Management** to open the **Users** overview page.

Figure 35: Users overview

Select the user to be unlocked.

Click *Edit*.

Change the password of this user.

Click *Save*.

Step 2:

From the **Users** overview page.

Select the user to be unlocked.

Click *Unlock*.

4.1.8. Edit a user

From the main menu, select **Customer Care** > **User Management** to open the **Users** overview page.

Select the user record to edit.

Click *Edit*.

Following screen is displayed:

Figure 36: Edit user

Change the properties according to the following table.

Property	Description
Login	Username or login name.
Password	The password the user has to use to log on to the system.
First names	Given name(s) of the user. Only used for recognition in this page.
Last name	Family name of the user. Only used for recognition in this page.

Property	Description
Language	The language in which the user interface is displayed for this user. Default and always available is English. All other languages are only relevant if translations have been uploaded using the User Rights Module.
Password never expires	If this check box is selected, the password can remain the same and the password does not need to be updated periodically.
Locked out	The user is locked out from login (too many faulty login tries).
Suspended	The user is temporarily suspended from login.
Authentication method	Login method. For now always 'password'.
Select groups	Link User Rights Module groups to user. Note that <prefix> FI Level 1 and <prefix> FI Level 2 is used for daily users and administrators; <prefix> CSP FI Administrators is meant for administrators only.

Figure 37: User properties

Click *Save*.

4.1.9. Disable a user

To remove access on a temporary basis without deleting, a user can be disabled. The user record remains in the system but the user cannot use the system.

In the main menu, select **Customer Care** > **Users Management** to open the **Users** overview page.

Select the user record to disable.

Click *Disable.*

Figure 38: User overview page (Disable)
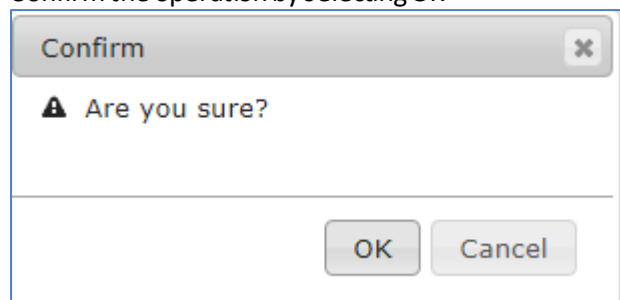
Confirm the operation by selecting OK

Figure 39: Confirm the operation to disable user

4.1.10. Enable a user

The permit access of a disabled user, a user can be enabled.

In the main menu, select **Customer Care** > **Users Management** to open the **Users** overview page.

Select the user record to enable. Note: only a user who has been previously disabled can be enabled.

Click **Enable**.

Figure 40: User overview page (Enable)

4.1.11. Delete a user

In the main menu, select **Customer Care** > **Users Management** to open the **Users** overview page.

Select the user record to delete.

Click **Delete**.

Figure 41: User overview page (Delete)

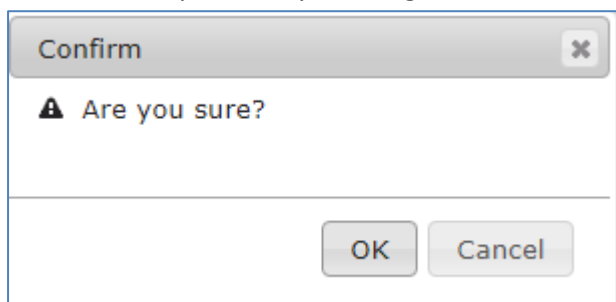Confirm the operation by selecting OK.

Figure 42: Confirm the operation to delete user

4.1.12. Resend invitation email

One-time passwords expire after a specified time period. If the one-time password has expired, the password reset invitation email can be resent with a new one-time password.

In the main menu, select **Customer Care** > **User Management** to open the **Users** overview page.

Select the user record you want to send a new password reset invitation email to.

Click **Resend invitation email**.