



Secure Remote Access Management (SRAM)



Third-party User Password and Token Reset Guide

February 2018

Summary

The SRAM login screen for 3rd party engineers consists of three fields:

- Username
- Password (Static and alphanumeric)
- Token (One Time passcode and numeric) ^[1]

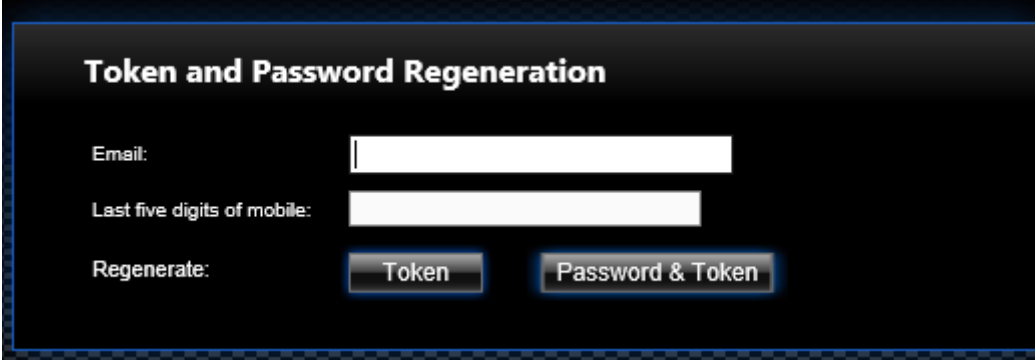
^[1] *More information about this field can be found on [Annex](#) at the end of the document.*

It has to be mentioned that their usernames are not always enabled. However, the engineers of the affiliate OTE's department are responsible for enabling access on demand using internal workflow system for a specific timeframe ^[2]. When the approval path of the workflow is completed, the username of the external engineer will be activated in the SRAM infrastructure AND an automatic SMS and Mail will be sent to him with the Token.

^[2] *The remote access is terminated as soon as this timeframe expires and the user can no longer access the system unless he requests additional time and receives OTE's approval.*

How to Reset Token/Password through SRAM

For 3rd party engineers, SRAM Reset Token and Password can be accessed through the URL:
<https://xconnect-reset.ote.gr/TokenRegen/>

The image shows a web form titled "Token and Password Regeneration" on a dark background. It contains two input fields: "Email:" and "Last five digits of mobile:". Below these fields, there are two buttons under the label "Regenerate:". The first button is labeled "Token" and the second button is labeled "Password & Token".

Token and Password Regeneration

Email:

Last five digits of mobile:

Regenerate:

Email: Type the email

Last five digits of mobile: Type the last five digits of the mobile phone number.

Token: Press this button only for token reset.

Password & Token: Press this button for password and token reset.

- After the successful regeneration of the token, a **SMS** and an **email** message will be sent to the end user containing the new token.
- After the successful reset of the password and token, a **SMS** and an **email** message will be sent to the end user with the new Fixed Password, as well as a **SMS** and an **email** message containing the token.

Annex: Token

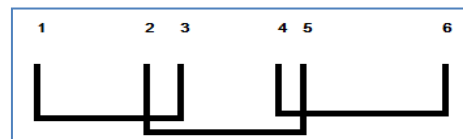
1. A Token is an OTP (One Time Password) which means that it cannot be used twice. The Token will NOT be valid for a login session, when the user has mistyped ANY of the 3 fields in the login form, OR was disconnected, OR logged off.
2. In some rare cases (exceptions approved by Information Security Division) the external engineer possesses a mobile token, in order to produce his/her own Token. If this is the case and the login fails for multiple times, the mobile token has to be resynced.

Note: Resync of a Mobile token is needed in case the username is disabled and a new “External Associate Activate Access” workflow has to be initiated.

3. In case the “External Associate Activate Access” workflows are overlapping in the time period, then the Token is not generated for each individual workflow. Only the first workflow will issue a token to the external user. In case the user needs another token, the Regenerate SMS Token application must be used.

Example: An OTE engineer has initiated the workflows described in the picture below

- | | |
|---|---------------------|
| 1 st . start time 1 o' clock | end time 3 o' clock |
| 2 nd . start time 2 o' clock | end time 5 o' clock |
| 3 rd . start time 4 o' clock | end time 6 o' clock |



The external user will receive ONLY one SMS/MAIL at 1 o'clock with a Token that is valid until 6 o'clock. For avoiding this, the start time of the next workflows and the end time of the previous workflow must have 15 minutes time difference.