Engaging Networks REST API

A setup guide for clients working with agencies

REST API Private Keys & Tokens

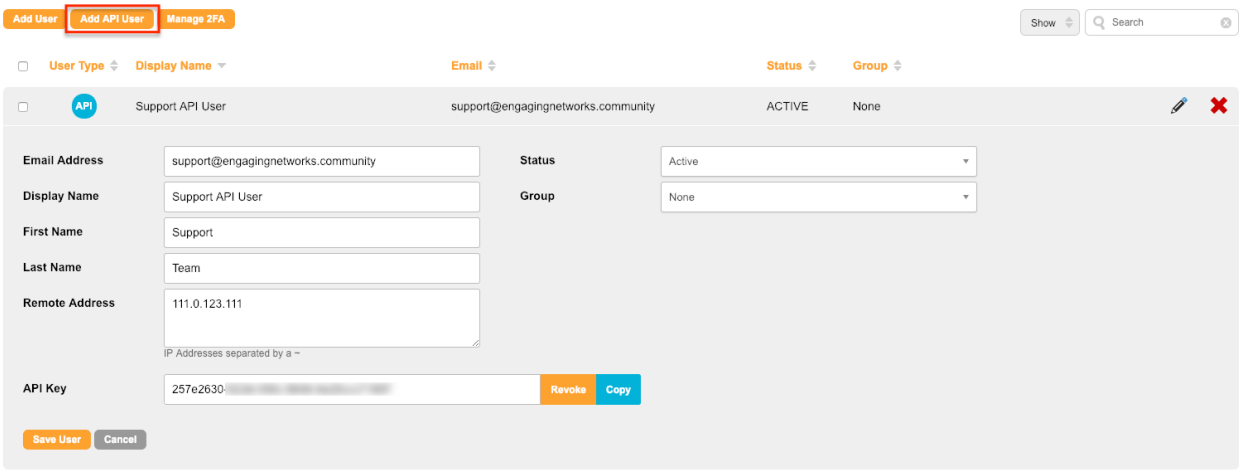
What are REST API private keys and tokens?
A REST API private key is a string of unique characters that act as a key for external applications to externally authenticate with the Engaging Networks platform. Upon authentication the application receives a private REST API token, which is valid for 1 hour.

What are Data API private tokens used for?
Private REST API tokens allow external connections into a client's Engaging Network account to perform bulk real time creation, reading, updating or deletion of database records, as well as external page submissions programmatically.

Private REST API tokens give full access to the supporter records in your account, so these tokens should always be treated with the utmost security.

How do I generate and access a REST API private key?
To generate a REST API private key you need to be logged in to your Engaging Networks account as a Super Admin, then navigate to Hello Menu > Account Settings > Users.

You will need to create a special user called an API User.



In addition to adding the email address, display, first and last names for the API User, you will also need to add the IP address of any incoming servers that will be accessing the API. Your developer or agency will be able to supply these IP addresses to you.

You can also set the API User status to Active/Non Active and assign a permission group to restrict the actions that can be taken by this user.

Need assistance? Contact Engaging Networks Support at support@engagingnetworks.community

You can revoke a REST API private key or delete an API User at any time, however if any applications are using the current key and any associated generated tokens they will stop working until a new REST API private key is updated in the application.

Delivering your private REST API key to an agency.
If you are working with an external agency they may ask you to generate a private REST API key for them so they can work on your project. When sending a key to any 3rd party you must deliver it securely so that only you and the agency employee know what the key is.

Do not send private REST API keys through plain text email or any other form of unencrypted communications.

You could for example add the key into a text file, zip up the text file with a password and email the zip file to your agency. Then use an alternative method such as SMS or WhatsApp to send your agency the password to unzip the file you sent via email.

You can also use a service such as onetimesecret.com to deliver your token.

Permission groups

Permission groups can be set to limit the actions an API User can take through the REST API. To create permission groups or adjust permission settings visit Hello>Account Settings>Permission Groups

If this API User is to only 'Process a page', then having no user group set for the API User is a valid option. However, if the API User is intended to use the 'Supporter Services' calls, a permission group with the permission 'Manage individual supporters' (under Data Management) enabled, must be assigned.