Engaging Networks Client Developer Access Checklist

This checklist is designed to help you assist giving your internal developer access to your Engaging Networks account safely and securely so they can carry out projects. It outlines some of the key things you may need to consider taking action on when working with your agency.

Adding A Developer To Your Account

When working with a developer you may need to give them access to your Engaging Networks account and you may want to limit visibility to certain pages and / or data.

For security reasons we would suggest that developers are only set up as Users on your account. You can find step by step instructions on adding a user at the following link on our support site.

Creating A New User:
http://support.engagingnetworks.net/permissions-creating-new-user

If your organization's security policies require two factor authentication to be enabled on Engaging Networks accounts you can choose to add this in the user's settings when you set them up in your account.

System Permissions

The level of access you give the developer is entirely controlled by you the client. Engaging Networks will not give account access to any party on behalf of a client, so you will need to set up the appropriate system access permissions yourself to grant access depending on what type of work they're carrying out.

You can find step by step instructions to set user permissions at the following links on our support site:

Permissions Overview:
http://support.engagingnetworks.net/permissions-overview

Creating Permission Groups:
http://support.engagingnetworks.net/permissions-creating-permission-groups

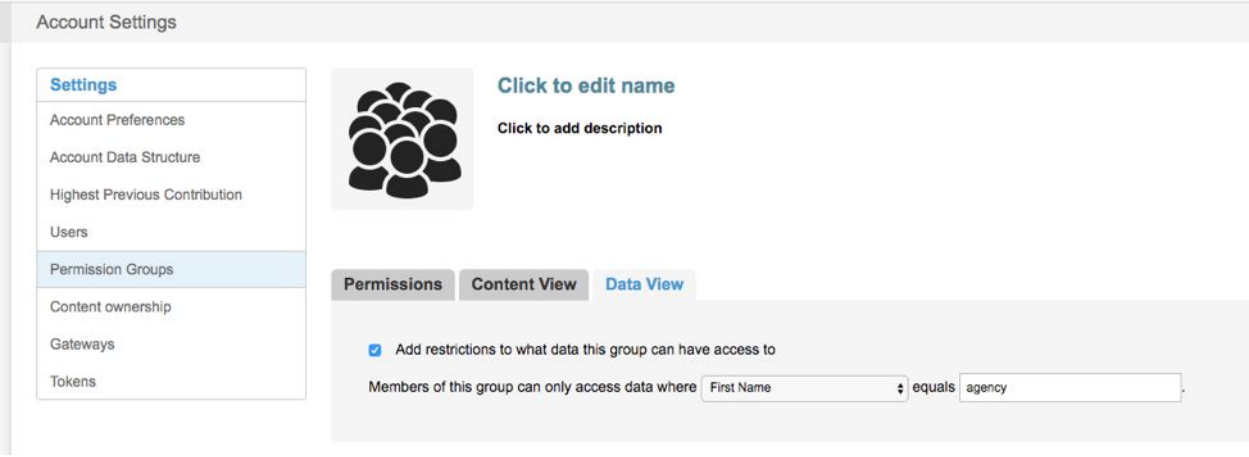
Engaging Networks Client Developer Access Checklist

Data Access

Developers may need to test that data is populating correctly into your database from pages or external integrations.

You can either give temporary data access to your agency using system permissions, or if you wish to shield your supporter database from access by the agency you can create a permission group for the agency and use the ‘data view’ function in your account to restrict access to records that contain only a specified value.

So, for example you could set up a developer permission group and set the Data View setting of the group to only display records where the first name field matches the word ‘developer’.



You can add the developer to this permission group and they could then test page submissions by filling in the first name field as ‘agency’. They would then only have access to the test records they have created in your database and not the rest of the live supporter records.

This also helps you find and delete any test records created by a developer to clean up your database after a project has been completed.

If you require further assistance with creating users or setting their permissions, please contact the Engaging Networks support desk – details are at http://support.engagingnetworks.net/

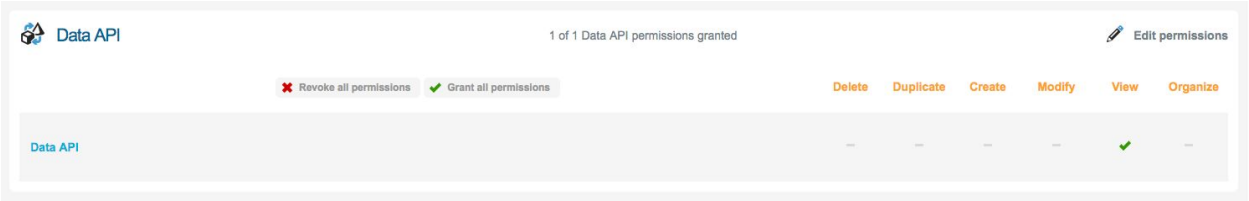
Engaging Networks Client Developer Access Checklist

API Access

If the developer requires access to the Application Programming Interface (API) or Engaging Networks Services (ENS) you may need to set them up as an API user in your account

How To Create An API User:
http://support.engagingnetworks.net/permissions-creating-api-user

In addition you'll need to grant access to API in the permission group the user is part of.



Tokens

If the developer needs access to the Engaging Networks API then they'll most likely request a public or a private token from you depending on the scope of the project.

Public Token

A public token is a key that developers can use to access limited information from your account through our API. This allows developers to create extended functionality (for example custom display widgets)

Private Token

A private token is a key that gives developers full access to your database records and may be needed for data integration.

Creating & Managing Tokens

Tokens must be created by the client, logged in to Engaging Networks as a Super Admin. Users with User or Admin access do not have access to tokens.

For full details on creating, assigning and the security of tokens please see the following link
http://support.engagingnetworks.net/public-and-private-tokens