2025

SSO Walkthrough

REACH Media Network

INTRO TO LOGIN TYPES

Before we get into the nitty-gritty of SSO, there are some login types within CMS 2.0 you should all be aware of:

Basic: this is essentially the username and password users will use to log in to CMS 2.0. Every organization is assigned a basic login. It cannot be edited or deleted. New users will also be automatically added to this system.

- This is useful if the SSO of a system fails. SSO failures are usually the result of a certificate failure that breaks the SSO. When SSO breaks, we can fall back to this system.

SSO: a login method that allows users to automatically log into multiple apps or websites with just one set of login credentials.

Now that we have this basic understanding, let's dive into creating an SSO policy.

CREATING AN SSO POLICY

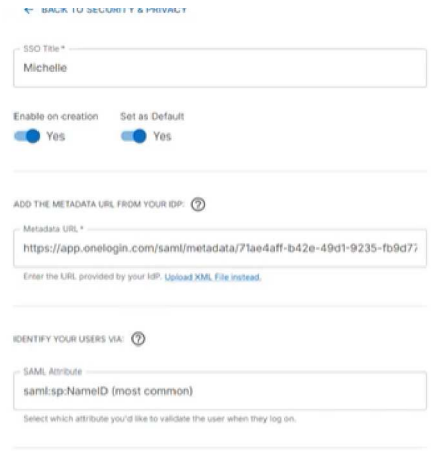
First, we will enter the IdP Information. This is essentially the information that will get the REACH system and the client's system to talk. Their IdP is their SSO provider. This can include:

- Microsoft
- OneLogin
- Okta
- And any other company providing their SSO

Now, let's dive into the steps.

1. Enter the name of the SSO. Usually, just the company name is sufficient.
2. Ensure both "Enable on Creation" and the "Set as Default" toggles are enabled. They should be on by default.
    - Enable on Creation means whenever a new user is created, they will be added to this SSO policy
    - Set as Default ensures this is the default setting users will use to sign into the CMS. You may want to disable this if clients are transitioning to a new SSO policy once that new configuration is set up.
3. Next, enter the Metadata URL route. They will have to provide this to you from their SSO provider.
    - We highly recommend using a Metadata URL route over uploading XML files. The reason is that when the SSO certificate expires, without a URL, the clients must be on top of it and know when exactly that certificate expires so they can reupload the file. A URL will automatically receive the new data.
4. Next, enter the SAML Attribute data. The SAML Attribute is basically what bridges the user, the REACH CMS, and the Metadata URL to each other so that each system can communicate.
    - This info must match up with how their SSO provider configures SSO. For instance, if they use email to configure SSO and the SAML attribute is set up for an employee ID number, the policy will not work.

5. Once complete, the information should look similar to the test example below.



ADVANCED SETTINGS

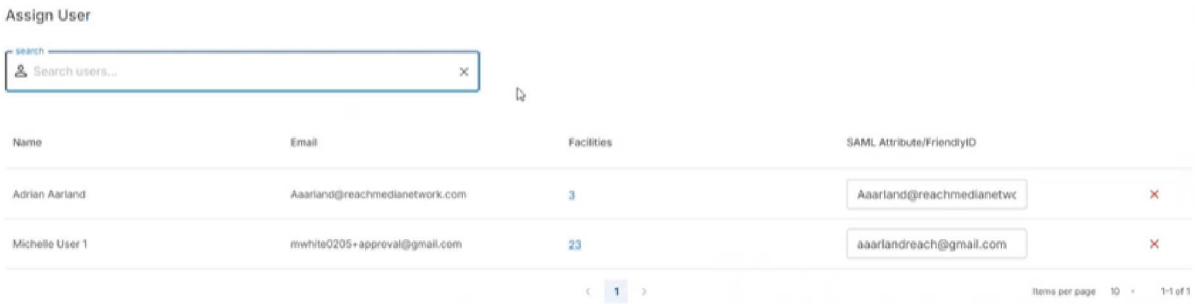
Clients typically see the log out/log in page when they log out. With Single Log Out, you can redirect clients to a specific webpage if they desire.

1. Enter the FriendlyID. This checks to see if the SAML attribute matches for client redirect.
2. Enter the Redirect URL. This will be the webpage clients are redirected to after logging out.

Note on FriendlyIDs: You must be very clear on what the configuration of the SAML Attribute is set to. If you look at our options, some of them are very unclear as to what the attribute is set to. The friendly ID does nothing to the configuration but makes it clear what you have your SAML Attribute configured as. [Example: employee emails or employee ids]

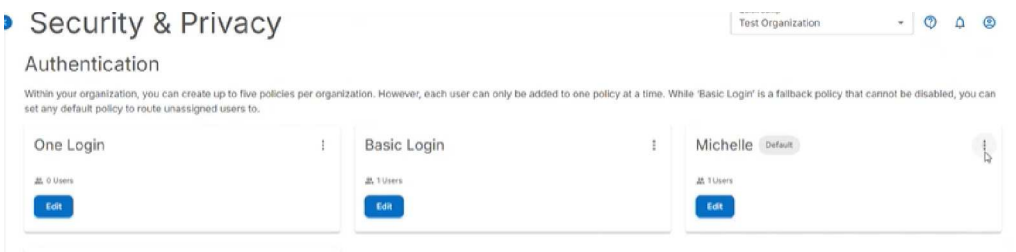
ASSINGING USERS TO SSO

After completing the IdP page and clicking "Next," you'll come to the "Assign" tab. Here, you'll be able to assign users to the SSO policy.
This page will automatically fill the assign user menu with every employee under the client's SSO policy.
From there, you simply enter the SAML attribute into the SAML Attribute/FriendlyID column. You will also have the option to remove users if the client desires.



FINALIZING THE SSO POLICY

After you assing your users, clicking "Next" will bring you to the REACH Information tab. At this point, the SSO policy has been saved. On this page, you will be able to test the SSO policy before launching. You will also see an REACH API link. The client will need to download REACH Media Network's Metadata using this link and plug that into their SSO policy provider. This is client-specific, as each one could be using a different provider.
The Vanity URL is the URL the client's IT team would use to implement the REACH CMS into their SSO policy dashboard. It is essentially the page from which their users can log into all their apps and webpages.
From there, you will see the SSO policy show up on the Security & Privacy page.



Once complete, users will be able to go in and edit the policy, as well as delete it altogether.

FINALIZING THE SSO POLICY

Once an SSO Policy is configured, when you add a new user to your organization you will be able to easily apply the SSO policy and SAML Attribute when creating that user. REACH does not force you to add the SSO policy; If you select a policy, you are forced to apply the SAML attribute.

After adding the user to your organization, the individual users will still go through our onboarding process.