# Setting up Single-Sign On

In order to configure SSO for your organization, MediaValet requires the following information.

Note that you will only need to fill out one section between the SAML and OpenID Connect (OIDC + OAuth 2.0) sections, depending on which identity provider and authentication protocol your organization uses.

Once this form is complete, please forward this to [support@mediavalet.com](mailto:support@mediavalet.com)

**1. If SAML: Identity Provider Settings (REQUIRED)**

*This section does not apply if you’re using OpenID Connect SSO*

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Value** |
| Identity Provider Entity ID | Text (usually a URL) |  |
| Identity Provider Metadata Location | Text (URL to a hosted XML file, otherwise attach the file in your response to MediaValet Support)  This location varies depending on your Identity Provider’s platform. |  |
| Enable Identity Provider-initiated SSO login? | Yes/No  Enabling Identity provider-initiated SSO will allow users to access MediaValet from their IdP login hub if they’re already logged in.  If not enabled, users will only be able to login using SSO from their MediaValet library’s login page (Service-Provider initiated SSO login) |  |

**2. a. If OpenID Connect: Identity Provider Settings**  
*These sections do not apply if you’re using SAML SSO*

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Value** |
| Identity Provider Client ID | Text |  |
| Identity Provider Secret | Text |  |
| Discovery URL | Text (URL) |  |
| Response Type | Dropdown/Single choice e.g. code or code id\_token |  |
| Scopes | Text (comma separated strings)  Scopes are used by MediaValet during authentication to authorize access to the user’s details. Each scope returns a set of user attributes, which are called claims. |  |
| Authority | Text (URL) (Not required but recommended) |  |

**2. b. If OpenID Connect: Scopes**

Scopes are used by MediaValet during authentication to authorize access to the user’s details. Each scope returns a set of user attributes, which are called claims. Three scopes will be included by default and cannot be removed: openid, profile, and email.

* openid (required)
* profile (required)
* email (required)

**3. Claims Mapping Settings (REQUIRED)**

Claims are name/value pairs that contain information about a user, as well meta-information about the identity provider. Claims are typically a URL or a string.

The information provided in this section tells MediaValet’s identity service where certain information will be available from within your Identity Provider’s response.

|  |  |  |
| --- | --- | --- |
| **Field Label** | **Type** | **Value (URL or string)** |
| Email\* | Text  (Expected input: URL or label) |  |
| External User ID\* (typically the same as the username and/or email address claim) | Text |  |
| Groups\* | Text |  |
| Preferred Username\* | Text |  |
| First Name | Text |  |
| Last Name | Text |  |
| Address | Text |  |
| Department | Text |  |
| Telephone | Text |  |

**\*= Required fields to be configured and included in your Identity Provider’s response**

Note: If using the default claim value pairs for Azure AD or Okta, please let the MediaValet Support team know as we can grab these ourselves. For any other Identity Providers, please fill out the information above.

**4. Authorization Rules**

**4. a. Administrators (REQUIRED)**

Create an authorization rule to authorize one or more email addresses as Auth Rules Administrator.

**Note: These are the users that will be testing the SSO integration and will have access to modify the role-mapping page in MediaValet during testing.**

|  |
| --- |
| **Email addresses** |
|  |
|  |
|  |

**4. b. Catch-All Rule (optional)**

You can create a default authorization rule for users to automatically be assigned to. We recommend using lower-permissioned default user groups like Member or Guest.

Note: this is something that can be modified by the client once SSO is set up.

|  |
| --- |
| **Default User Group** |
| MediaValet Guest |

Once SSO is set up, additional rules can be managed on a self-serve and ongoing basis by Administrators of the library.

**5. Test Account Login Credentials (optional)**

This is optional, but recommended: if you wish, please provide us with credentials for a test user account set up in your Identity Provider’s platform, so we can validate that SSO has been set up correctly.

|  |  |
| --- | --- |
| **Field** | **Type** |
| Email | Text (email address) |
| Password | Text |