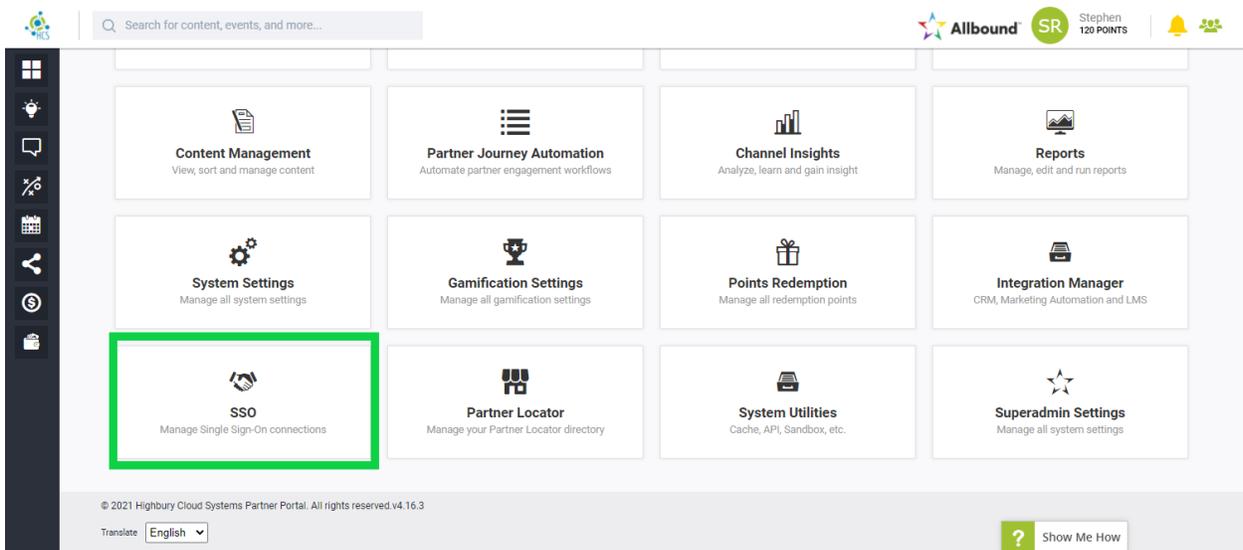
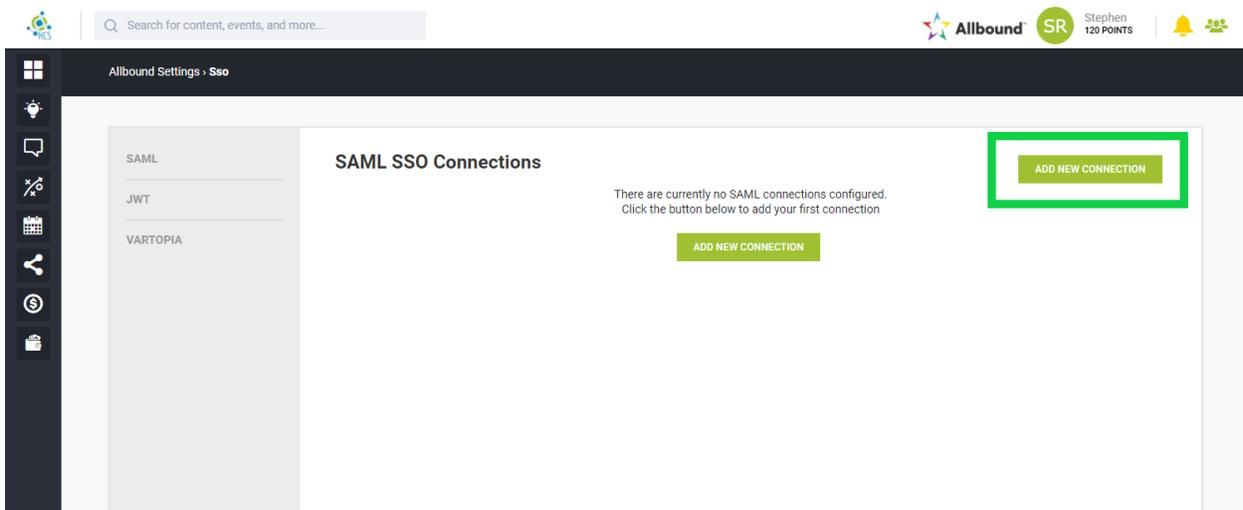


Configuring Allbound as SP

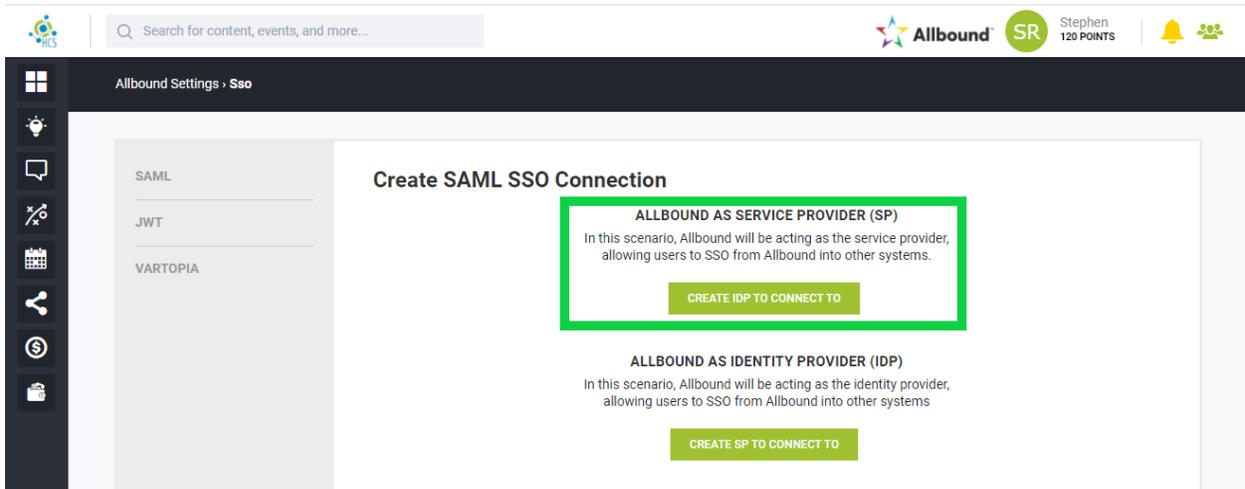
First we need to add a new SP to our settings in Allbound. In order to do so we need to navigate to our SSO settings page by going to **Allbound Settings -> SSO**.



Once there, click on “Add New Connection.”



Then click “Create IDP To Connect To” under “Allbound As Service Provider (SP).”



Once on the “IDP Edit” screen, give the IDP a Name and Description. The name will appear on the login button if activated at the bottom of the page.

The implementation will require 2 values to complete the configuration on the Allbound side, with an additional optional value.

The screenshot shows the 'Configure SAML SSO Connection' form. It includes fields for 'Name', 'Description', 'Login URL', 'Logout URL', 'Entity ID' (pre-filled with 'https://demo-master.allbound.com/'), and 'Issuer ID'. A large 'Certificate' field is highlighted with a red border. Below are 'Deep Link Request Key' and 'Deep Link Response Key' fields. A section titled 'CONFIGURE AVAILABLE ATTRIBUTES' is highlighted with a green border, containing an 'Attribute Value' dropdown (set to 'Select a user field'), an 'Attribute Key' input field, and minus/plus buttons. At the bottom, there are checkboxes for 'Enable Login Button' and 'Redirect login', an 'UPDATE SETTINGS' button, and a 'Show Me How' button.

Login/SingleSignOnService URL: This value is from Azure AD and **is required**. This value can be located in the Azure AD metadata XML file as the **SingleSignOnService** value.

Issuer ID: This value is from Azure AD and **is required**. This value can be located in the Azure AD metadata XML file as the **entityId** value, near the top of the file.

Entity ID: This value is from Allbound and **is required**. It is pre-populated with the instance URL which is the correct value.

Logout URL: This value is from Azure AD but is **optional**, and is the same as the **Login URL**.

X509 Certificate: This value is generated by Azure AD to be shared with Allbound. This value can be located in the Azure AD metadata XML file and should be in PEM format when added to the "Certificate" field. To achieve this format, simply paste the certificate between the following text.

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

The final result should appear similar to the following example:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDoDCCAoiGAWIBAgIGAWonDGNhMA0GCSqGSIb3DQEBCwUAMIGQMqswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxEtAPBgNVBAMMCGFsbGJvdW5kMRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMB4XDTE5MDQxNjE2NDcwNloXDTI5MDQxNjE2NDgwNlowgZAxChAJBgNVBAYTALVTMRMwEQYDVQQIDApDYWxpZm9ybmhmRYWYAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0wCwYDVQQKDAZPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjJERMA8GA1UEAwIYWxsYm91bmQxHDAaBgkqhkiG9w0BCQEWDLuZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQUdUq5iMQ/CB3Mj6UjGJvACh72Mv//k4U+UeL/NA/knJJ0H60Ijdybu8X4gb1YyegJEhYG9R2Zfr+0wdvDuK+77Rur0/gehbnId5d9BHBrdFYhhR5taGY6iGtHTGfgbWn6/bdQvUPSLJNPaj4jfymp3skf/likUKYKuV9NzLp7NM1C9pFJOKR7GvwNpD79dbn/0zNbQ0zua2tr8HT+B6lb0ULLZACRdM38vFvN9SbQoR6+atz/ZT8Th82l6759JtCK77QXZv0BvKxDGLkw9Hhue31q12Yj7yNLDEXkny1iRYSNn+LhV7uemzCWCbVkrw9Vnodlvh8IS53HZlmk47zLvoP4qrHmnR7sR9WhoDvDL5YDLl2hx60Je8=
```

```
-----END CERTIFICATE-----
```

Configuring Attributes: Allbound is required to configure 3 attributes to be received with specific keys.

Email => <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

First Name => <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>

Last Name => <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname>

Configuring Azure AD for a new IDP

Azure AD requires 2 values from Allbound to configure in the Azure AD SSO settings.

Entity(Issuer) ID: This value is your Allbound portal URL.

Example: **<https://myportal.allbound.com/>**

****NOTES****

- Include the forward slash ("/") at the end of the URL.
- If you have a custom domain implemented, you may use the custom domain as the Entity ID.

Assertion URL/ACS URL: This value is your Allbound portal URL /acs.

Example: **<https://myportal.allbound.com/acs>**

****NOTES****

- If you have a custom domain implemented, you may use the custom domain as the Entity ID.