

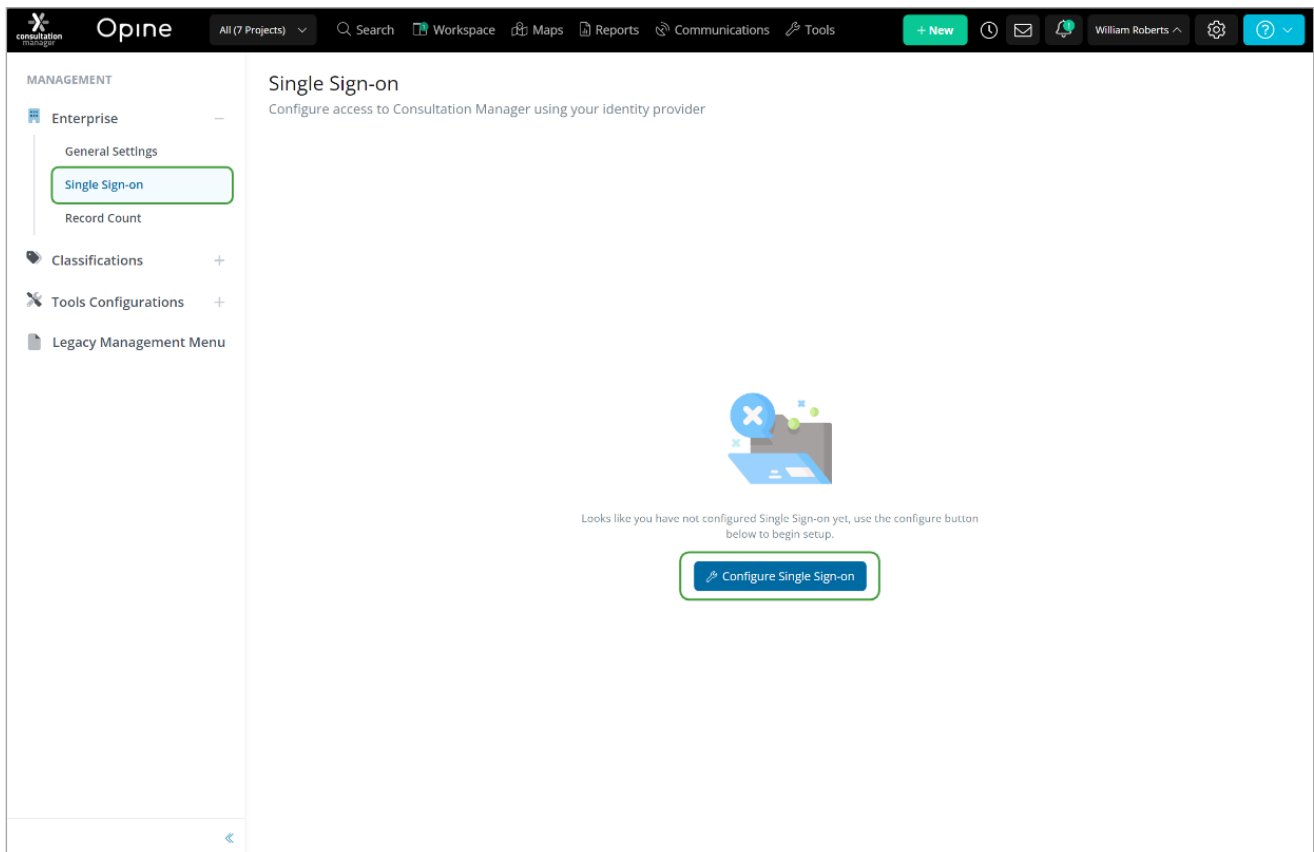


Consultation Manager

Configuring Single Sign-on in Entra

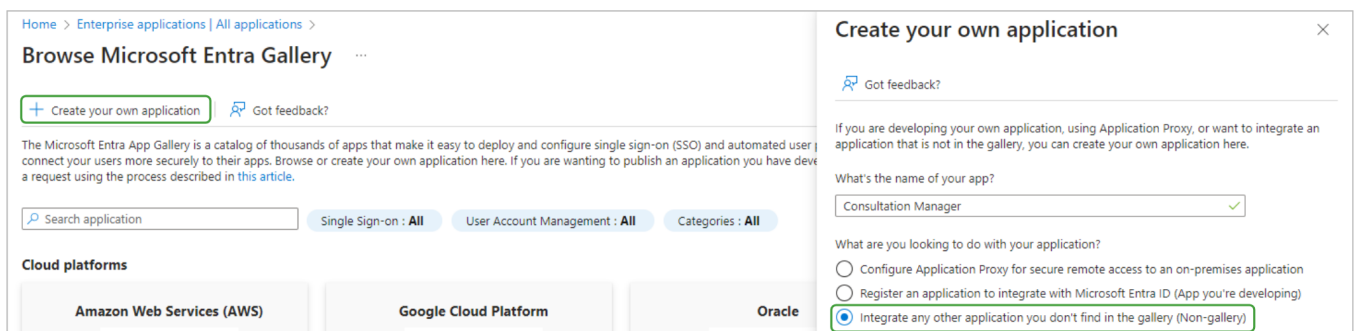
This guide will step you through how to configure a SAML based Sign-on configuration between your Consultation Manager instance and Microsoft Entra. To configure Single Sign-on in Consultation Manager you will need to be a User with Enterprise Administrator permissions.

To being setup within Consultation Manager open the **Management** area and navigate to **Enterprise > Single Sign-on** and select **Configure Single Sign-on**, this will load the Single Sign-on configuration for your instance

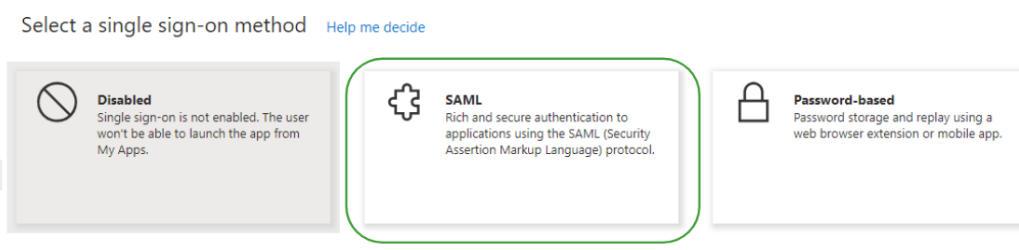


Entra Setup

Once your configuration has loaded in Consultation Manager open Microsoft Entra and navigate to **Enterprise applications** and select **+ New application**. Consultation Manager does not currently have a Gallery App and as such will need to be setup as a custom integration. To do this select **+ Create your own application** and then choose **Integrate any other application you don't find in the gallery (Non-gallery)**.



Open your new Enterprise application and select **Single Sign-on** and **SAML** as the sign-on method.

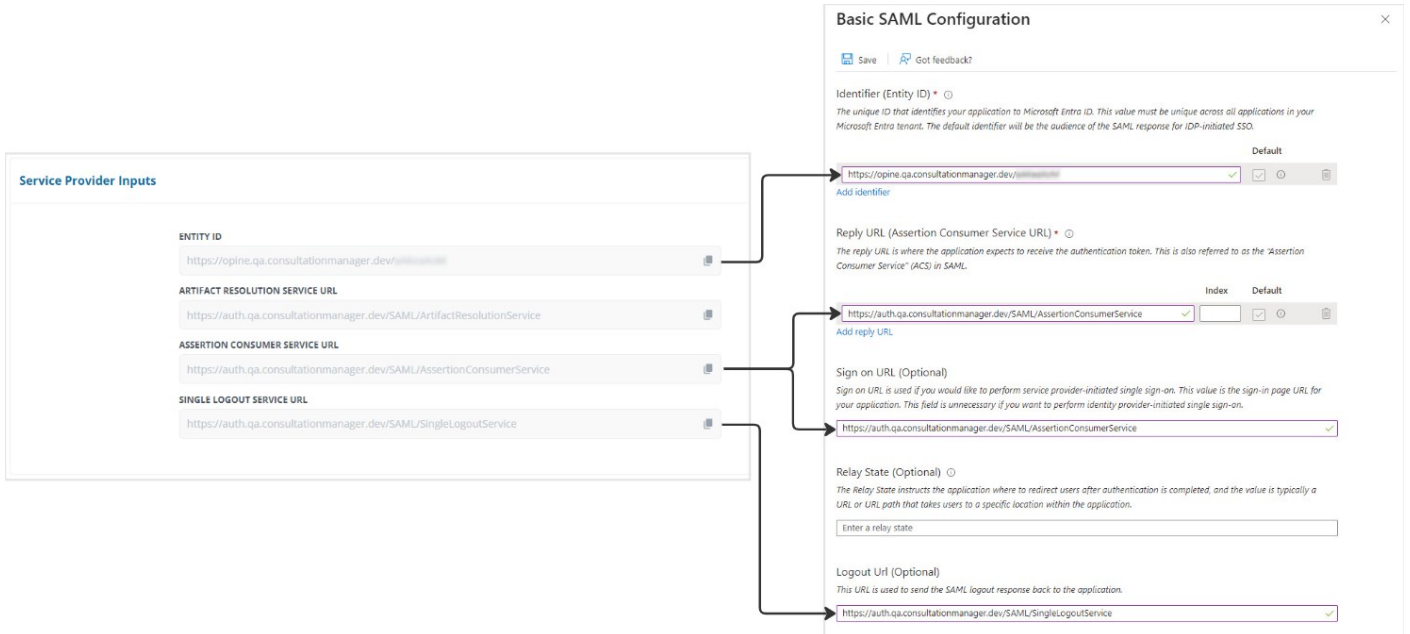


From the SAML configuration screen, select **Edit** on the **Basic SAML Configuration** panel and copy the values from the **Service Provider Inputs** in Consultation Manager to the fields detailed below:

✳ **Entity ID** > **Identifier (Entity ID)**

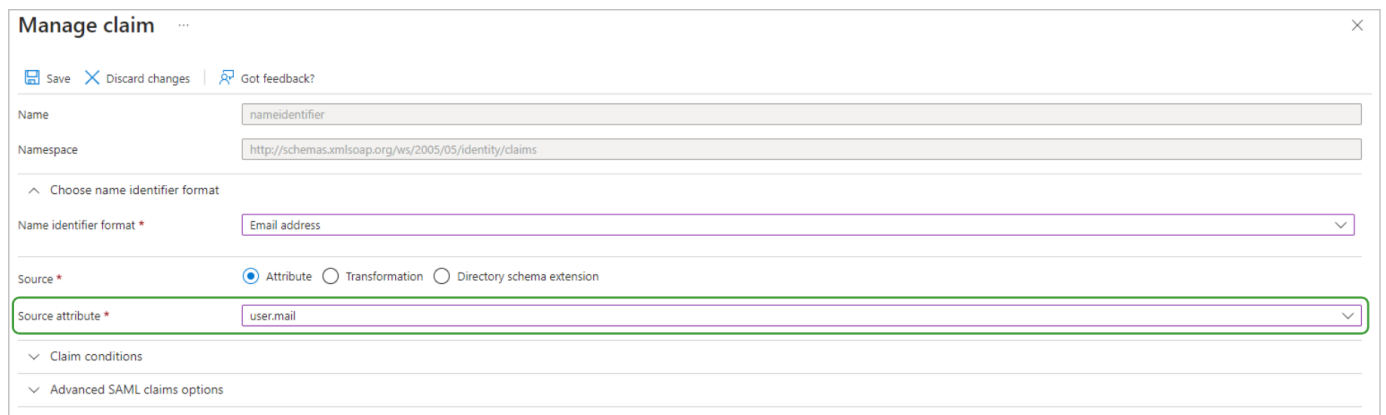
✳ **Assertion Consumer Service URL** > **Reply URL (Assertion Consumer Service URL)**

✳ **Assertion Consumer Service URL** > **Sign on URL (Optional)**

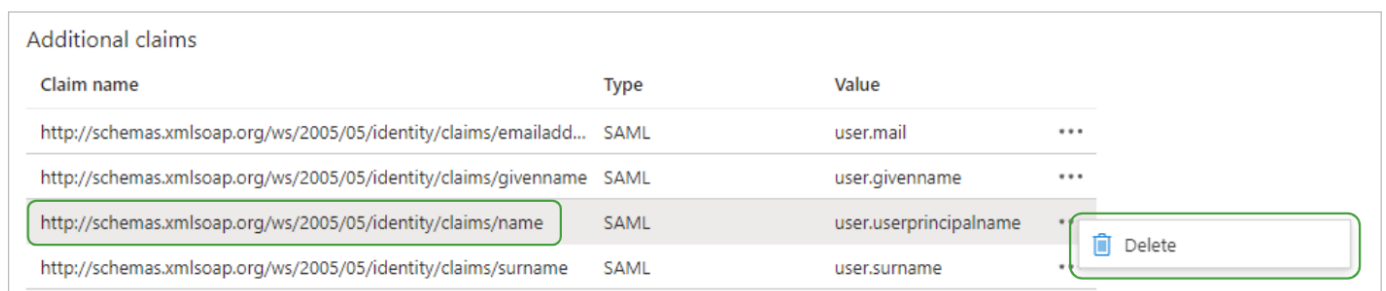


Next select **Edit** on the **Attribute & Claims** panel and modify the claims as follows:

Under **Required claim** select **Unique User Identifier (Name ID)** claim and modify the **Source attribute** to be **user.mail** from the dropdown selector and **Save** this change.



Then returning to the **Attributes & Claims** screen under **Additional claims** delete the <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> claim entry.



With the above changes applied your **Attributes & Claims** screen should match the below:

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.mail [nameid-format:emailAddress]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Lastly, ensure you add all Users required to access Consultation Manager through Single Sign-on either as an individual User or via a control group to your Enterprise application in Entra through the **User and groups** menu.

Consultation Manager - Opine - QA | Users and groups

Enterprise Application

+ Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
<input type="checkbox"/> LR Liam Robertson	User	User

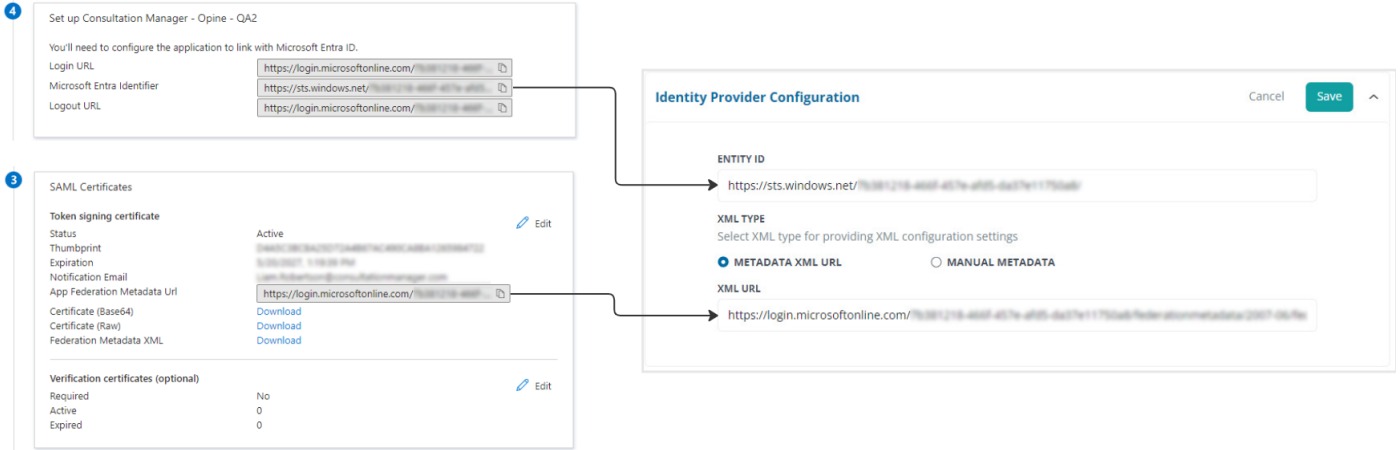
- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups**
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- > Security
- > Activity
- > Troubleshooting + Support

Consultation Manager Setup

Following all steps in Entra configuration being complete return to your Consultation Manager Single Sign-on setup area and populate the **Identity Provide Configuration** section with the following details from your Entra SAML setup menu:

◆ **App Federation Metadata URL** >  **XML URL**

◆ **Microsoft Entra Identifier** >  **Entity ID**



4 Set up Consultation Manager - Opine - QA2

You'll need to configure the application to link with Microsoft Entra ID.

Login URL <https://login.microsoftonline.com/>

Microsoft Entra Identifier <https://sts.windows.net/>

Logout URL <https://login.microsoftonline.com/>

3 SAML Certificates

Token signing certificate	Status	Actions
Token signing certificate	Active	Edit
Thumbprint	00000000-00000000-00000000-00000000	
Expiration	2023-09-01 12:00:00	
Notification Email	admin@consultationmanager.com	
App Federation Metadata Url	https://login.microsoftonline.com/	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional)

Required	Active	Expired	Actions
No	0	0	Edit

Identity Provider Configuration

ENTITY ID <https://sts.windows.net/>

XML TYPE
Select XML type for providing XML configuration settings

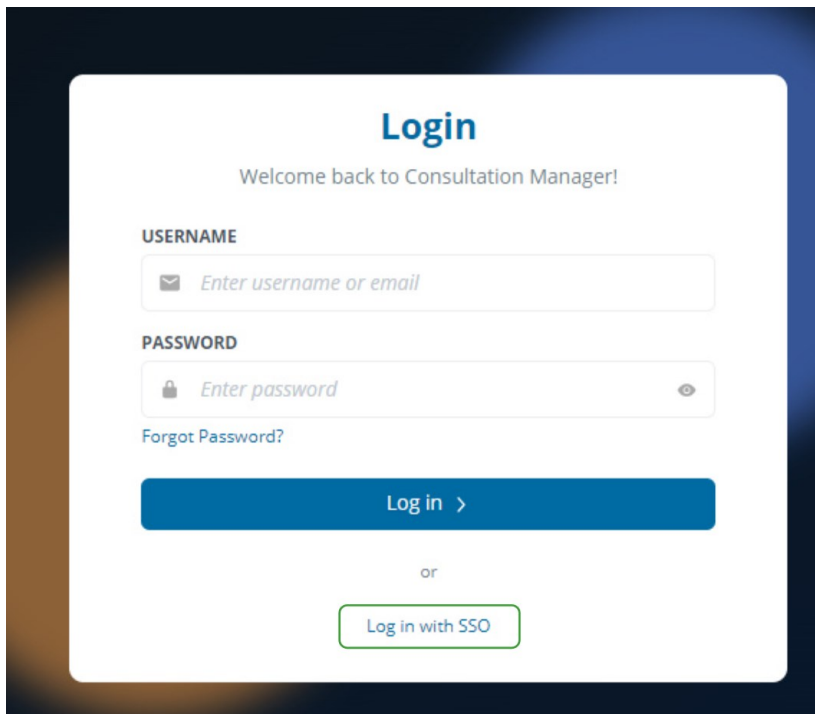
METADATA XML URL MANUAL METADATA

XML URL <https://login.microsoftonline.com/>

Once the values are copied in select **Save** to apply them to your configuration. Single Sign-on configuration is now complete for your Consultation Manager instance.

Testing

Consultation Manager does not currently support an IDP initiated flow nor can Users be provisioned into Consultation Manager through Single Sign-on, as a result to test the connection please ensure you have a User created in Consultation Manager with appropriate access to test with. Once configuration above has been complete a new **Log in with SSO** option will be available on your login portal, it is recommended you validate authentication is working correctly before enforcing Single Sign-on:



Login

Welcome back to Consultation Manager!

USERNAME

PASSWORD

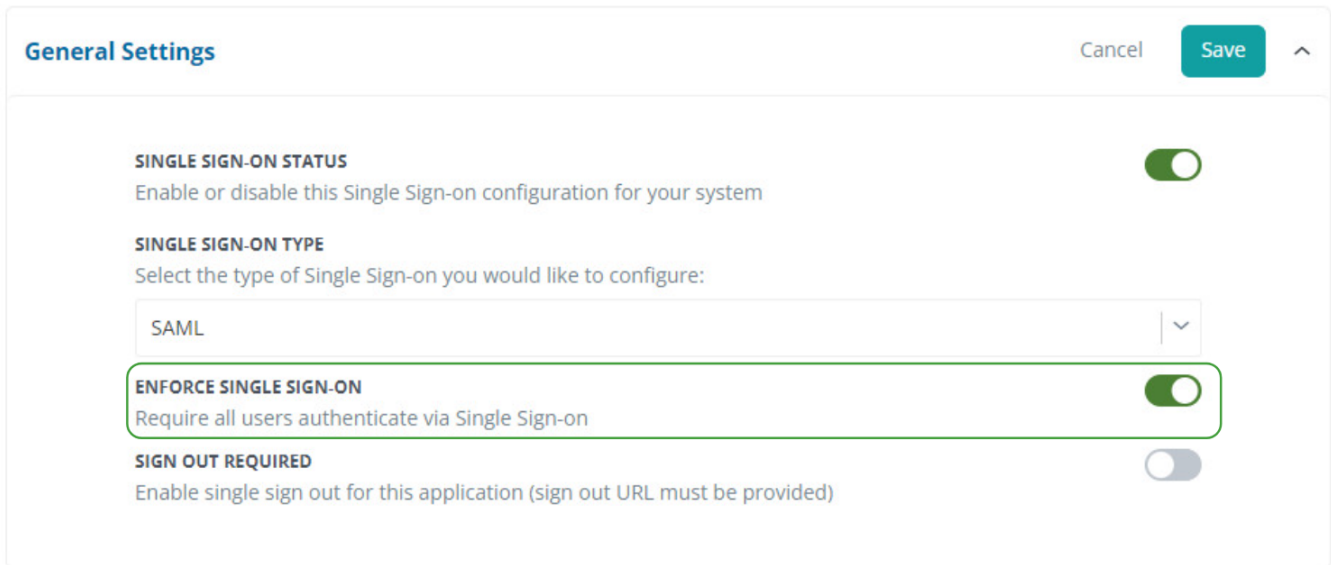
[Forgot Password?](#)

[Log in >](#)

or

[Log in with SSO](#)

When you are ready to enforce Single Sign-on, return to your Single Sign-on configuration menu in **Management** and enable the **Enforce Single Sign-on** toggle, ensure you click **Save** to apply the change. Once enabled, Users will only be able to login via your Microsoft 365 Portal.

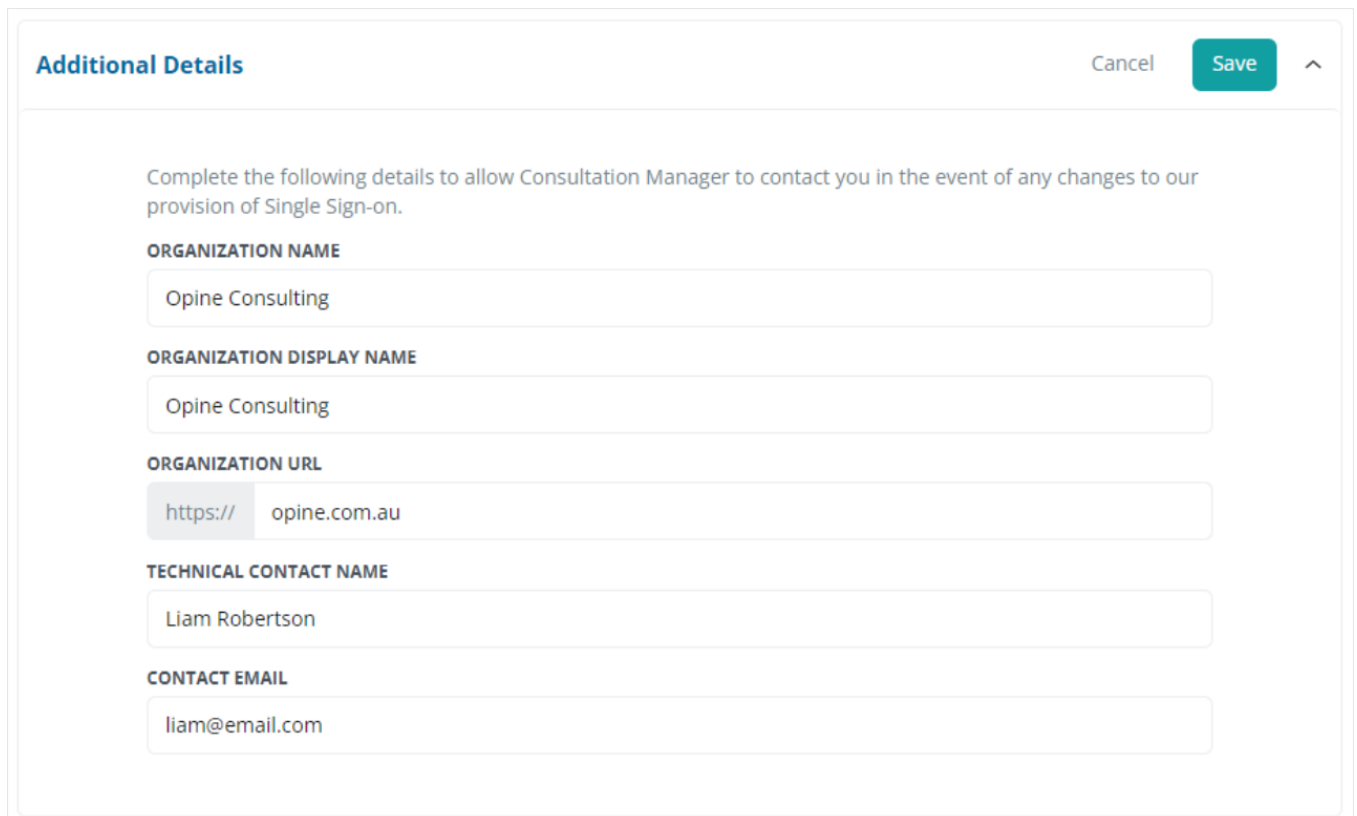


The screenshot shows the 'General Settings' configuration page. At the top right, there are 'Cancel' and 'Save' buttons. The main content area includes several settings:

- SINGLE SIGN-ON STATUS:** A toggle switch is turned on (green).
- SINGLE SIGN-ON TYPE:** A dropdown menu is set to 'SAML'.
- ENFORCE SINGLE SIGN-ON:** A toggle switch is turned on (green) and is highlighted with a green border.
- SIGN OUT REQUIRED:** A toggle switch is turned off (grey).

Troubleshooting & Support

Should you encounter any issues during the configuration process please contact us at (support@consultationmanager.com). If a technical contact can be provided in the **Additional Details** section of the Single Sign-on configuration menu please provide as a reference point should any future issues arise with the connection.



The screenshot shows the 'Additional Details' configuration page. At the top right, there are 'Cancel' and 'Save' buttons. The main content area includes a heading and several input fields:

Complete the following details to allow Consultation Manager to contact you in the event of any changes to our provision of Single Sign-on.

- ORGANIZATION NAME:** Input field containing 'Opine Consulting'.
- ORGANIZATION DISPLAY NAME:** Input field containing 'Opine Consulting'.
- ORGANIZATION URL:** Input field containing 'https:// opine.com.au'.
- TECHNICAL CONTACT NAME:** Input field containing 'Liam Robertson'.
- CONTACT EMAIL:** Input field containing 'liam@email.com'.

Additional FAQs

- **Does the application support integration via SAML 2.0 protocol?**
Yes, SAML 2.0 is the supported method.
- **Can we use Active Directory/Entra ID for IDP (Identity Provider) service?**
Yes.
- **Is the application available as a gallery application in Active Directory/Entra or will it require registration as a custom application?**
You will need to register and setup Consultation Manager as a custom application.
- **Does the application require role groups as part of authentication?** Yes, appropriate User/User Group allocations will need to be made in Active Directory/Entra on the configured Enterprise Application.
- **What anchor attribute (NameID) is to be used? (e.g.: accountname, userPrincipalName or emailaddress)?**
The NameID attribute will be emailaddress (user.mail).
- **How are the identities created in the application?**
Manually via entry in application or bulk .csv import. All Users authenticating via SSO will require an existing Consultation Manager profile to match to, we do not currently support auto-provisioning through SSO.
- **Are roles and permissions controlled through the application or via the integrated IDP?**
All application permissions are controlled through the application.
- **How are users created and off boarded in the Application?**
By other Users with either Team Leader/Enterprise Administrator system roles.
- **Do a SCIM need to be configured?**
No.
- **Is email the unique Identifier (NameID) required to match users in the SAML payload?**
Yes.
- **Other than standard SAML attributes such as first name, last name and email, are there any special attributes required?**
No additional attributes are required.
- **Is the application case sensitive to upper case or lower case in SAML claim specially for the NameID?**
No, the name ID (emailaddress) value is not case sensitive.
- **Will there be any special claims required in the authentication token?**
No.
- **Will you allow Azure administrators to have an admin account on the application side to assist with configuration on both sides?**
Application access is at the client-side application owners' discretion.
- **Is there a specific system role required to configure Single Sign-on within the application?**
Yes, the User configuring Single Sign-on will need to be setup as an Enterprise Administrator within Consultation Manager.