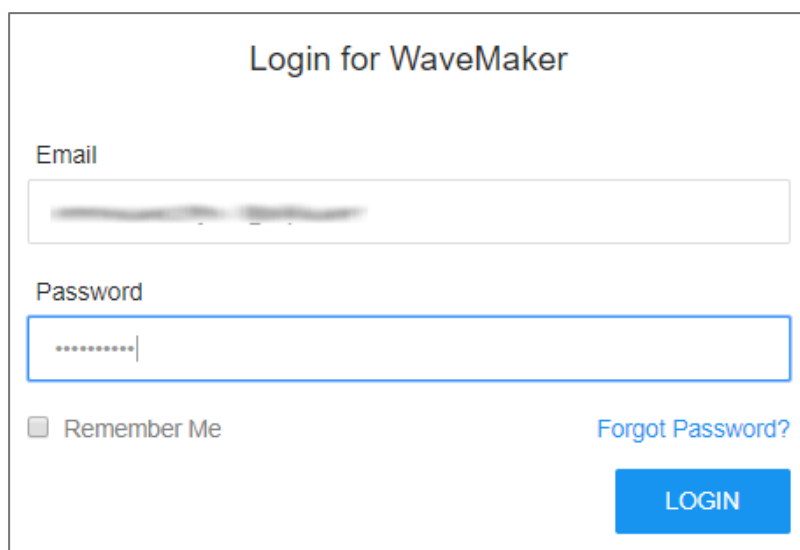


Configure WaveMaker for Single Sign-On

Configuring WaveMaker for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to WaveMaker by using the enterprise credentials.

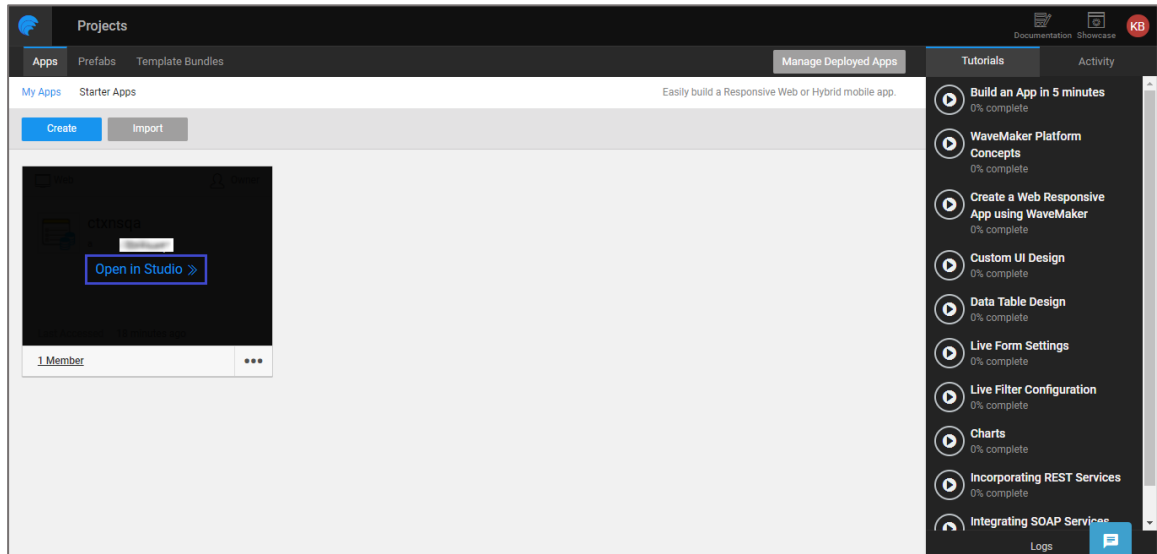
To configure WaveMaker for SSO by using SAML:

1. In a browser, type <https://www.wavemaker.com/> and press **Enter**.
2. Enter your WaveMaker admin account credentials (**Email** and **Password**) and click **LOGIN**.

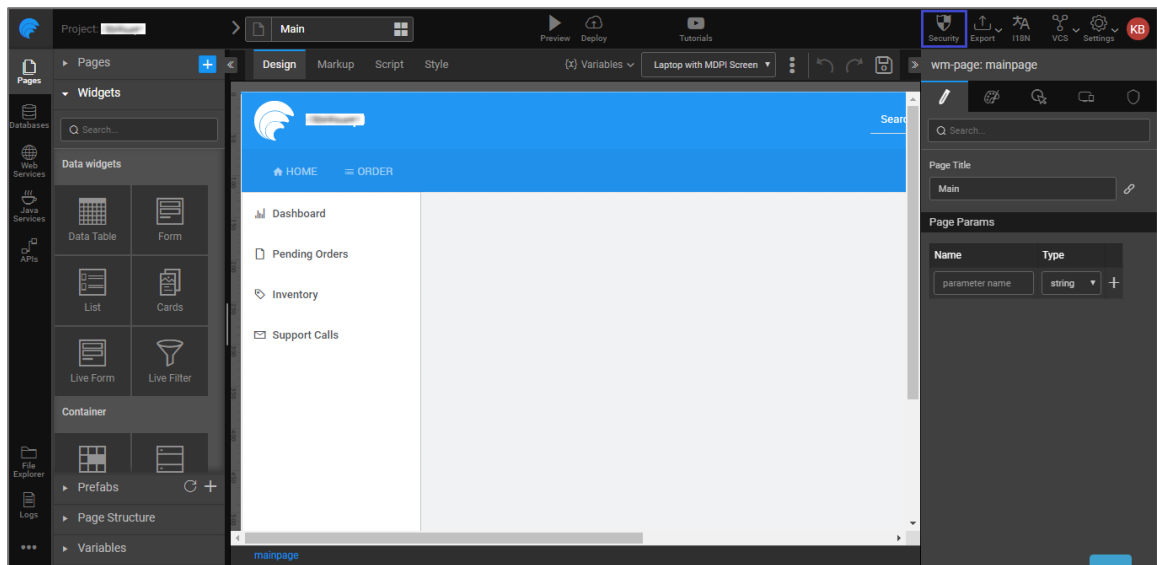


The image shows a login form titled "Login for WaveMaker". It contains two input fields: "Email" and "Password". The "Email" field has a blurred text entry. The "Password" field contains a series of dots. Below the "Email" field is a checkbox labeled "Remember Me". To the right of the "Remember Me" checkbox is a link labeled "Forgot Password?". At the bottom right of the form is a blue button labeled "LOGIN".

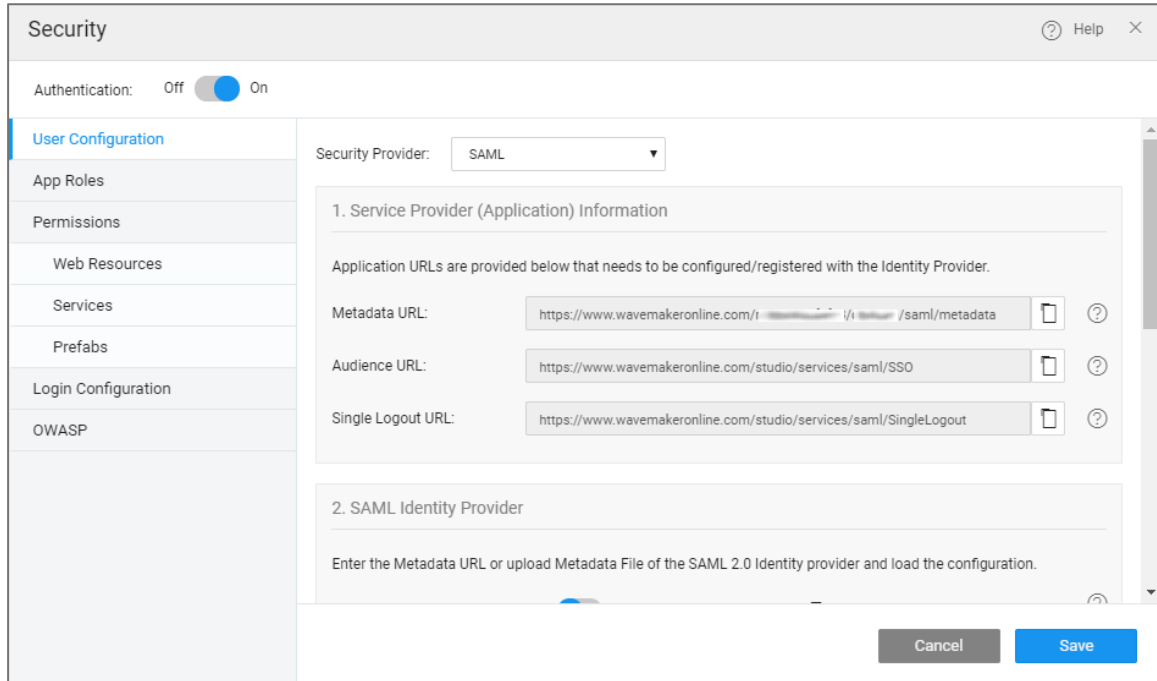
3. In the dashboard page, hover the cursor over the organization tile and click **Open in Studio** >>.



4. Click **Security** on the upper right-side of the page.



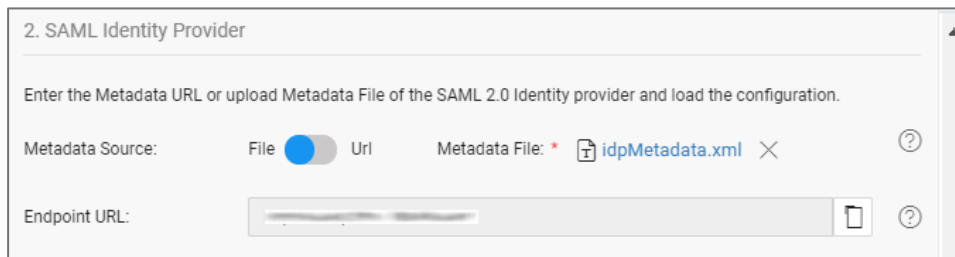
5. In the pop-up window, turn on the **Authentication** toggle switch.



6. Select **SAML** from the **Security Provider** drop-down list.

Note: Note down the **Metadata URL**, **Audience URL**, and **Single Logout URL** for IdP configuration.

7. Scroll down and choose the **Metadata Source**.



Note: Enter the metadata URL or upload the metadata file in XML format.

8. The **Service Provider Configuration** details are auto generated.

The screenshot shows a dialog box titled "3. Service Provider Configuration". It contains the following fields and controls:

- KeyStore:** A file selection field showing "key-store.jks" with a close button (X) and a help icon (?).
- Alias: ***: A text input field containing "KeyStore" and a help icon (?).
- Password: ***: A password input field with masked characters "....." and a help icon (?).
- Subject Name: ***: A text input field containing "cn=..., OU=WM, O=WM, L=LA, ST=CA, C=US" and a help icon (?).

Below these fields is a section titled "4. Role Mapping" with a "Search User Role:" toggle switch set to "Off". At the bottom right are "Cancel" and "Save" buttons.

9. Click **Save**.

10. In the pop-up window, click **OWASP** and turn off the **Protection** toggle switch under **CSRF**.

The screenshot shows a "Security" configuration window with a sidebar on the left and a main content area on the right. The sidebar includes the following items:

- Authentication: Off On
- User Configuration
- App Roles
- Permissions
- Web Resources
- Services
- Prefabs
- Login Configuration
- OWASP** (highlighted in blue)

The main content area shows the following settings:

- XSS**: Strategy: NONE (dropdown menu). Below it, the text "Application is vulnerable to XSS attacks" is displayed.
- CSRF**: Protection: Off On (toggle switch). This section is highlighted with a blue box.
- CORS**: Enable: Off On (toggle switch).

At the bottom right are "Cancel" and "Save" buttons.

