How to configure Single sign-on with Microsoft Azure Active Directory to control access

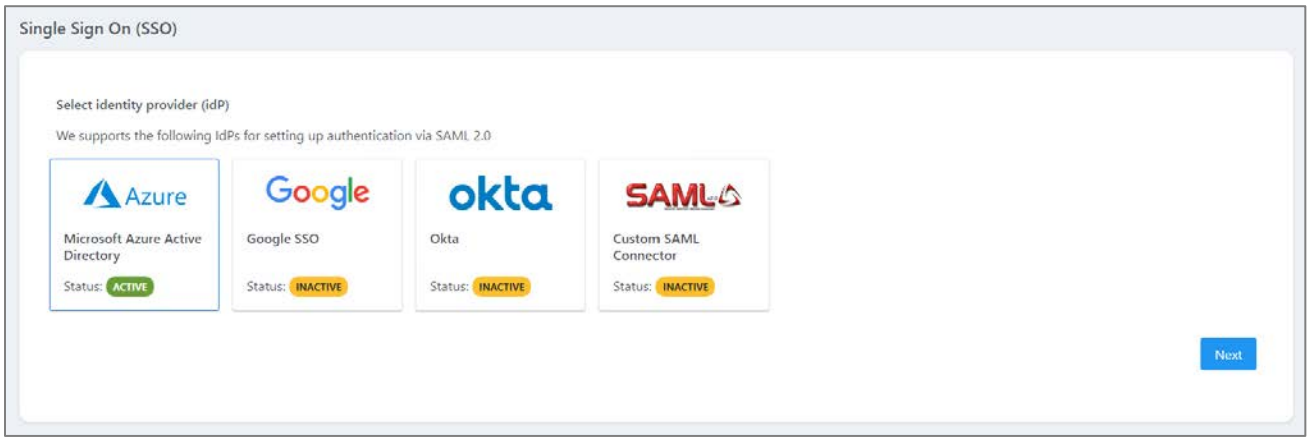
Azure AD - Volt-IoT SAML 2.0

The objective of this article is to demonstrate the steps to be performed in Volt-IoT SAML 2.0 within Azure Active Directory (Azure AD) to enable Single sign-on (SSO) in a centralized and secure way of controlling access to Volt-IoT Application

1. Login to your Volt-IoT super admin account access and select **Configuration** tab on the left-hand navigation bar.

2. Scroll down and go to the section of Single Sign-on (SSO) Configuration.

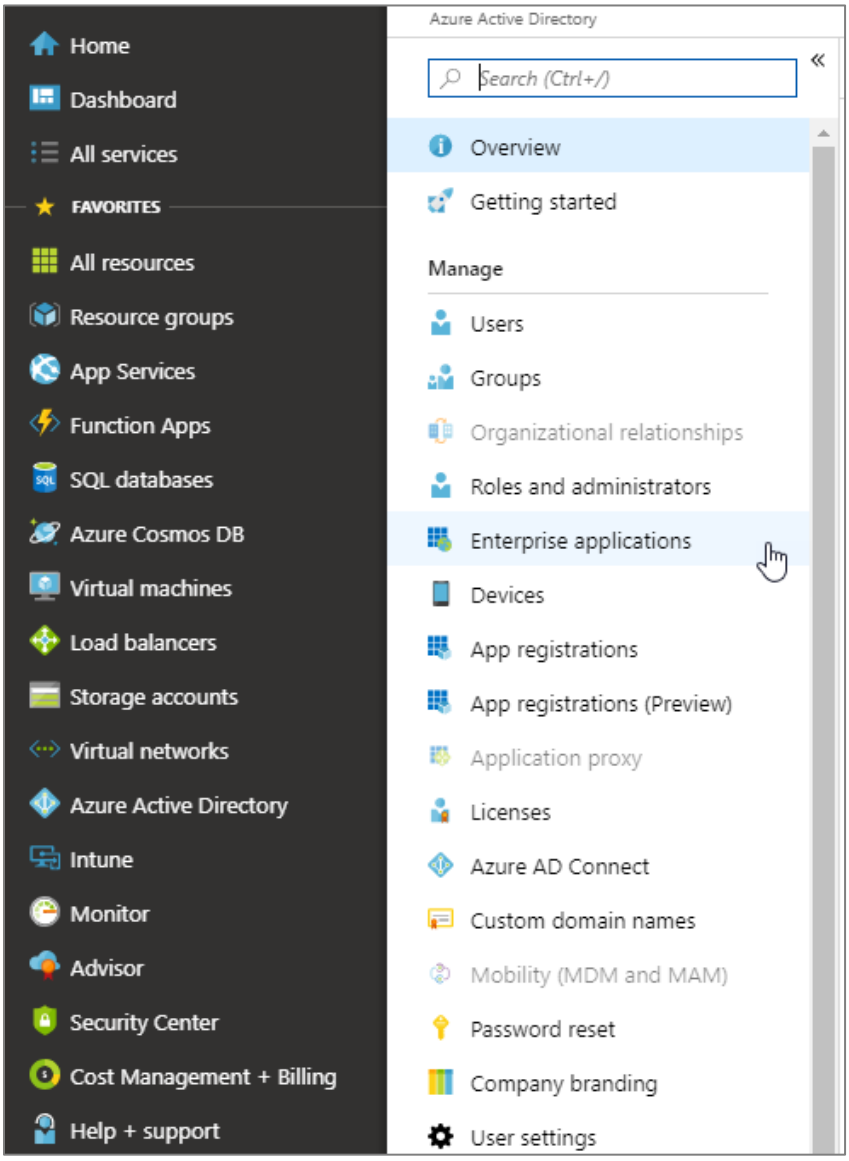
3. Select the Identity Provider **Microsoft Azure Active Directory** and click **Next,** you will be directed to configuration settings which are required to setup **Volt-IoT** app on your IdP.



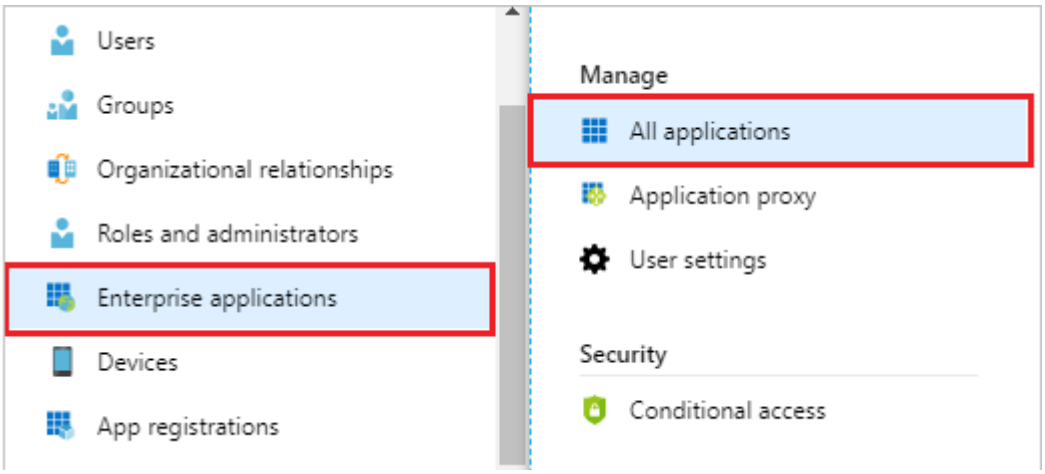
4. Copy the **Entity ID** and **Reply URL** (ACS URL) from configuration page.

5. Go to your Azure Portal and sign in (**Important:** make sure you are in the correct directory!)

6. In the left navigation panel, select **Azure Active Directory**

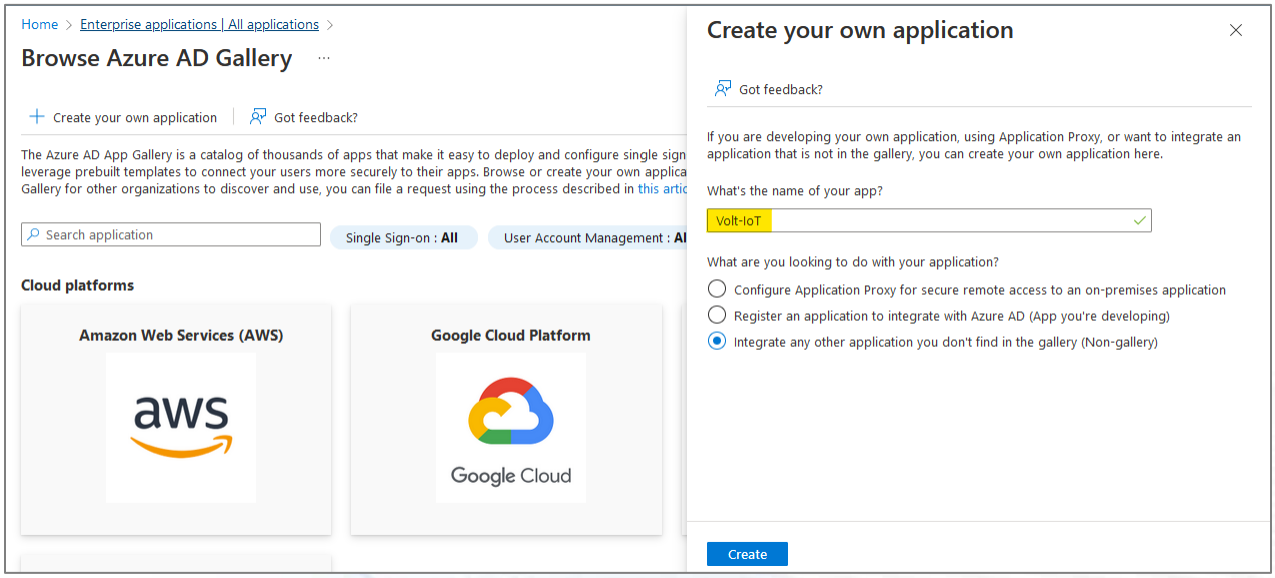


7. Navigate to **Enterprise applications**, and then select **All applications**.

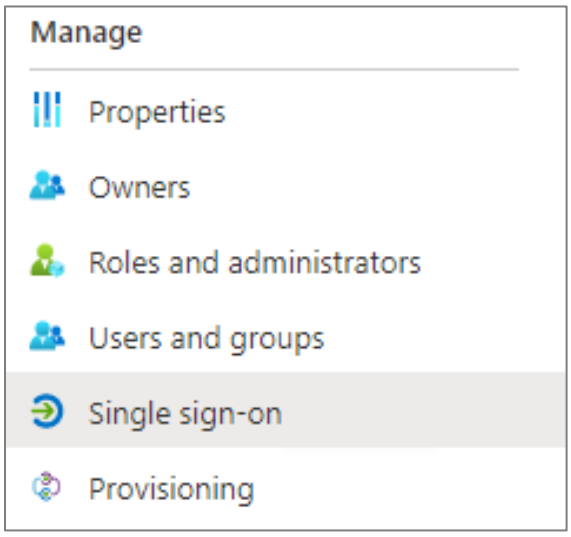


8. To add a new application, select the **New Application** button at the top of the pane.

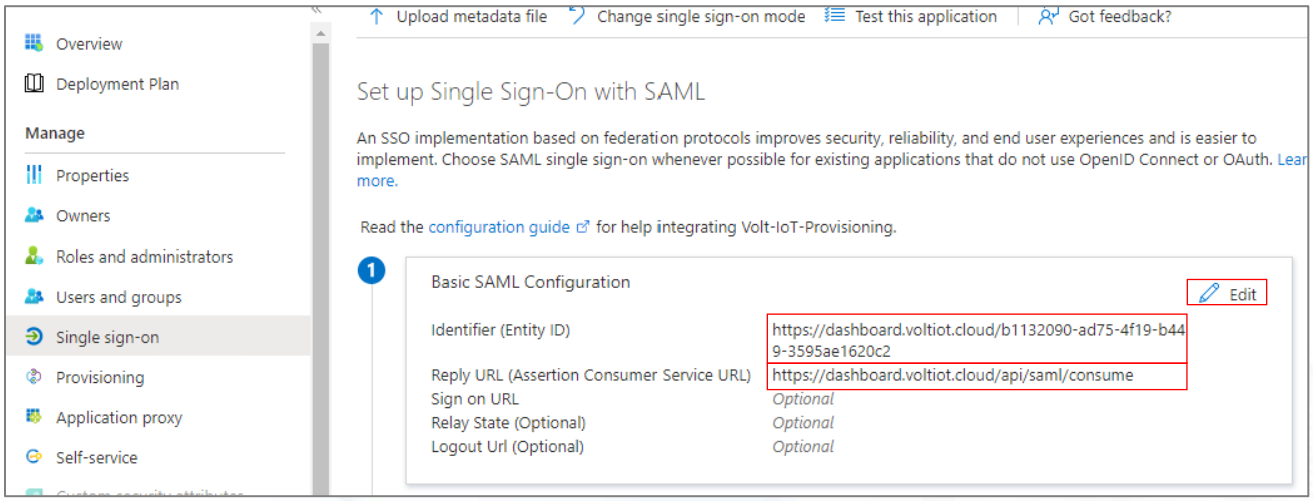
9. Click **Create your own application** and on the right panel type the name of your custom non-gallery app and click **Create** button.



10. Once the Application is added to your directory, navigate to the **Single sign-on** tab

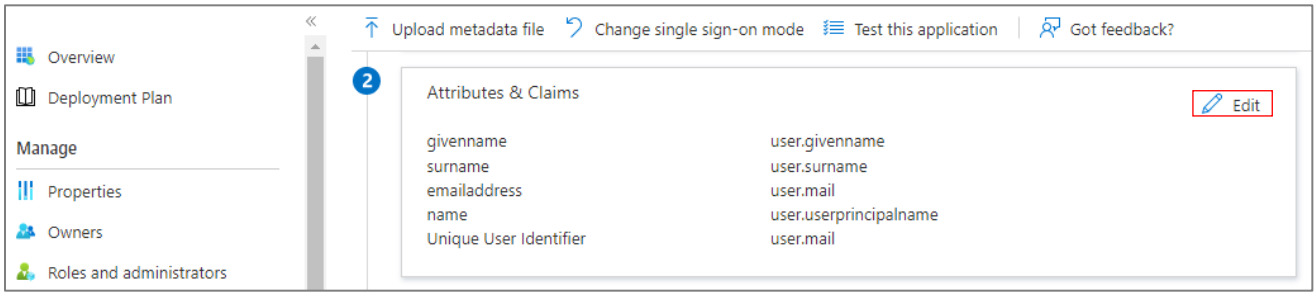


11. Edit the **Basic SAML Configuration** settings and paste the following values from **Volt-IoT SSO Configuration** page.
    - Paste **Entity ID** under **Identifier (Entity ID)**.
    - Paste **Reply URL** (Assertion Consumer Service URL).

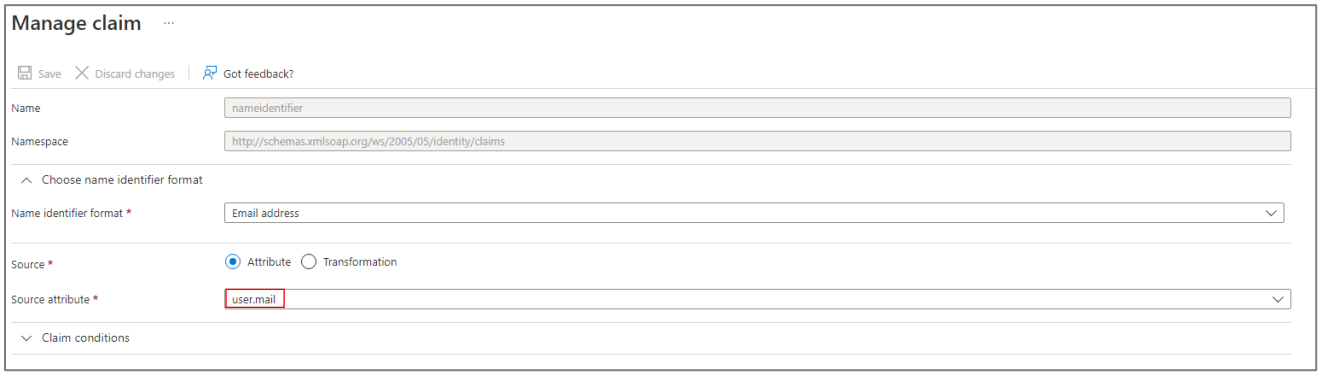


12. **Save** and **Close**

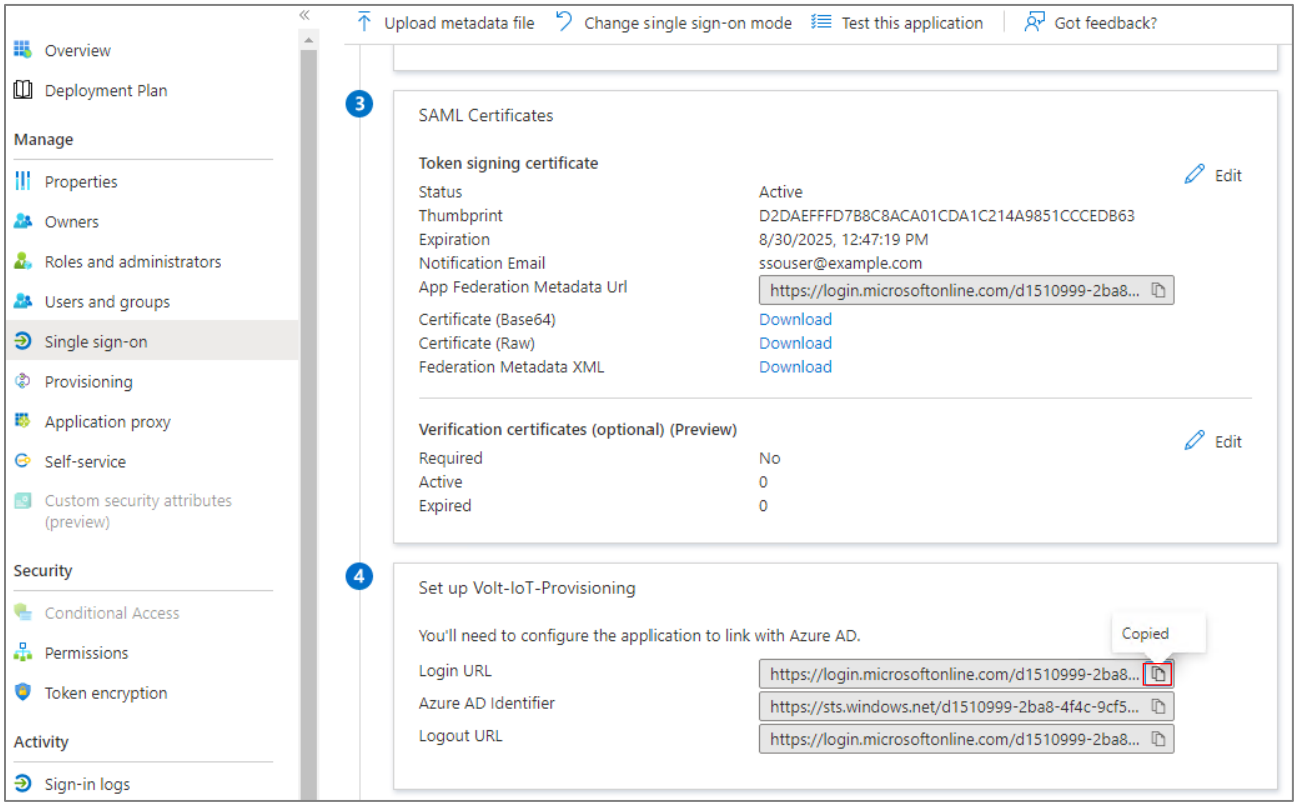
13. Next, edit **User Attributes & Claims**



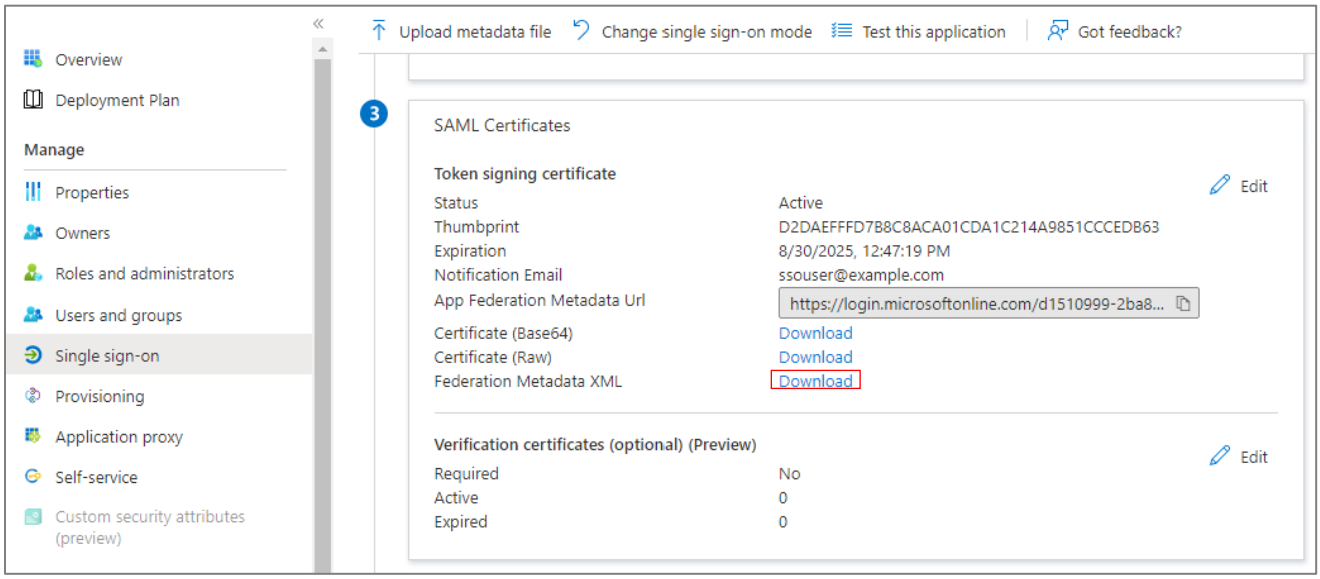
14. Under **Choose name identifier format**
    - Select **Attribute**
    - Enter **user.mail** (or whatever is the attribute for email address)
    - Click **Save**



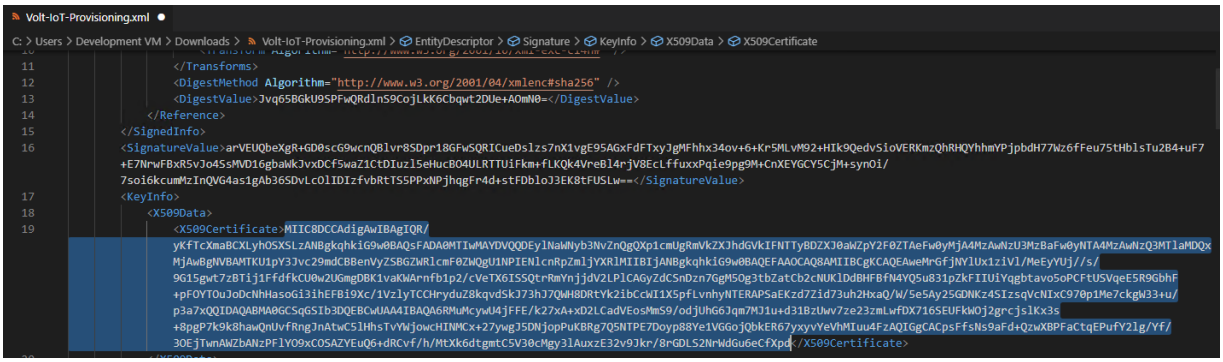
15. Copy the **Login URL**



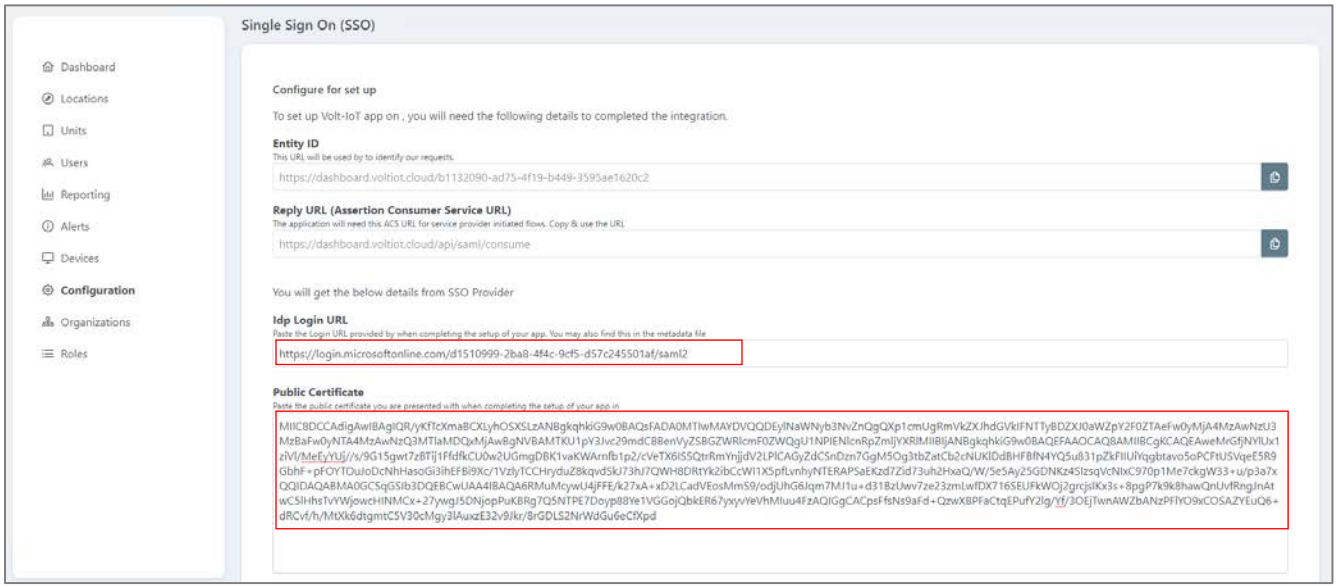
16. Click on **Download** next to **Federation Metadata XML**, present in the **SAML Signing Certificate**.



- Open the file and copy the following
- **Public Certificate**

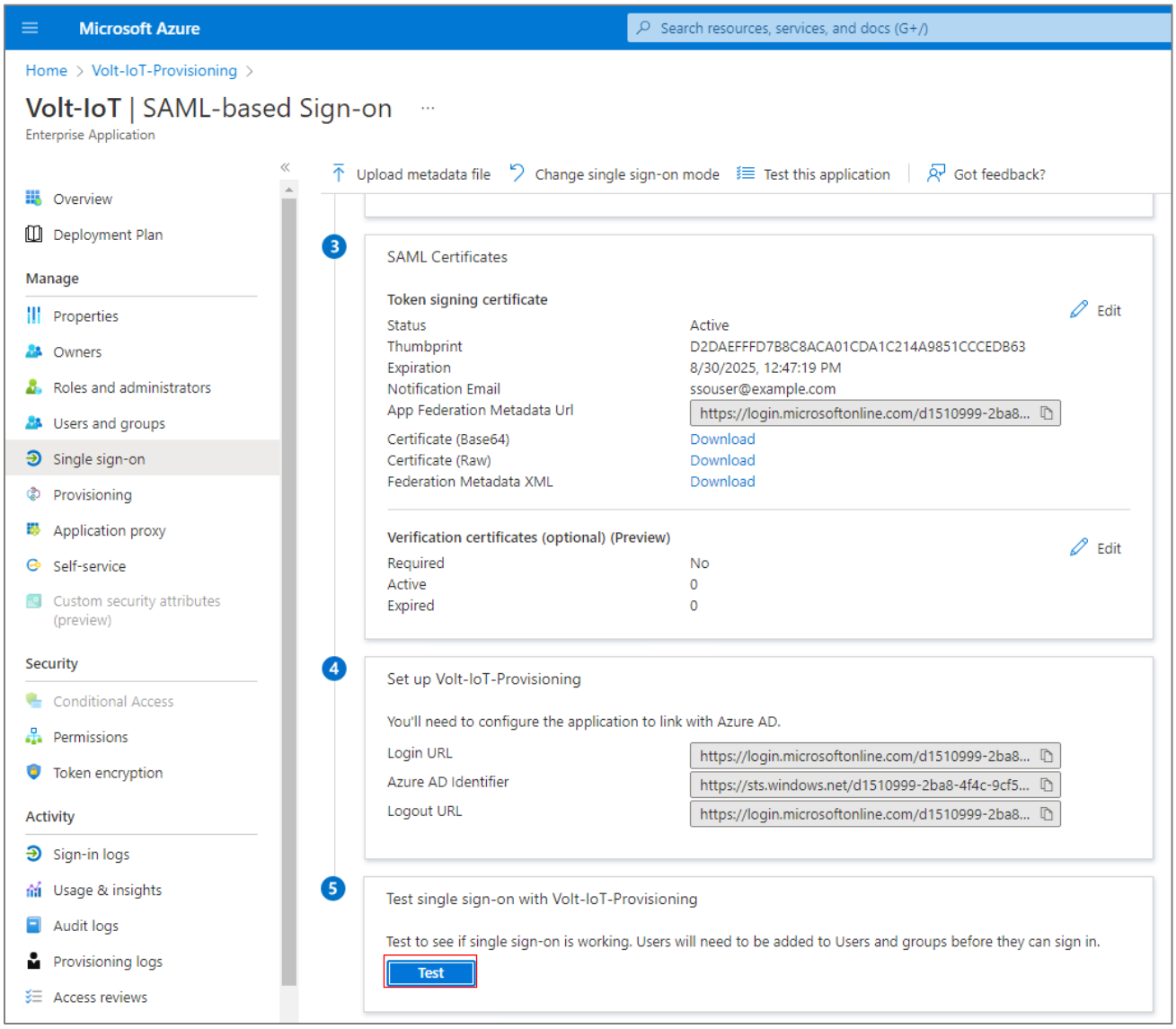


17. Navigate back to **Volt-IoT Single Sign-on configuration page** and paste the following details.
    - **Login URL**
    - **Public Certificate.**

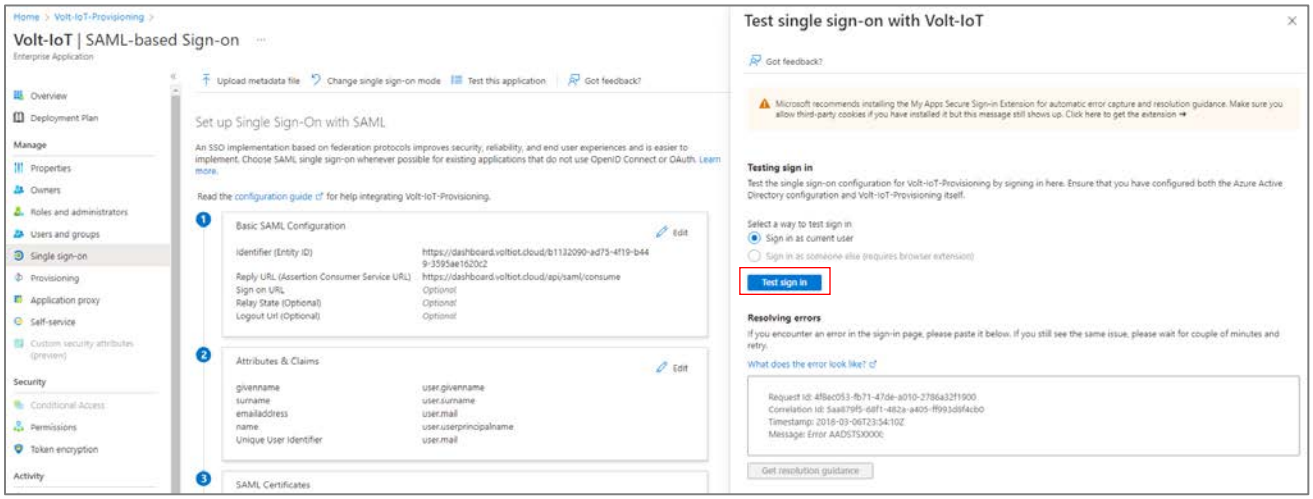


18. Click **Save Configuration**.

19. Test the integration via **Azure Active Directory** Configuration, Click **Test** button



20. Click **Test sign** In button



21. You will be prompted towards **Service Provider** flow and your user be authenticated via **Azure AD**.

> - You have to login with same email address on Volt-IoT Azure AD app before you can test and enable it.

22. Upon successful test, it will enable the **Single Sign-on** feature for your **Organization**

Note

> - Please connect with support@voltiot.cloud for any escalations support.