Single Sign On using SAML2.0 - Entra ID (formerly Azure AD)

Enable SSO authentication to the Command Center via Azure AD using SAML2.0

Updated on

ON THIS PAGE:

Overview

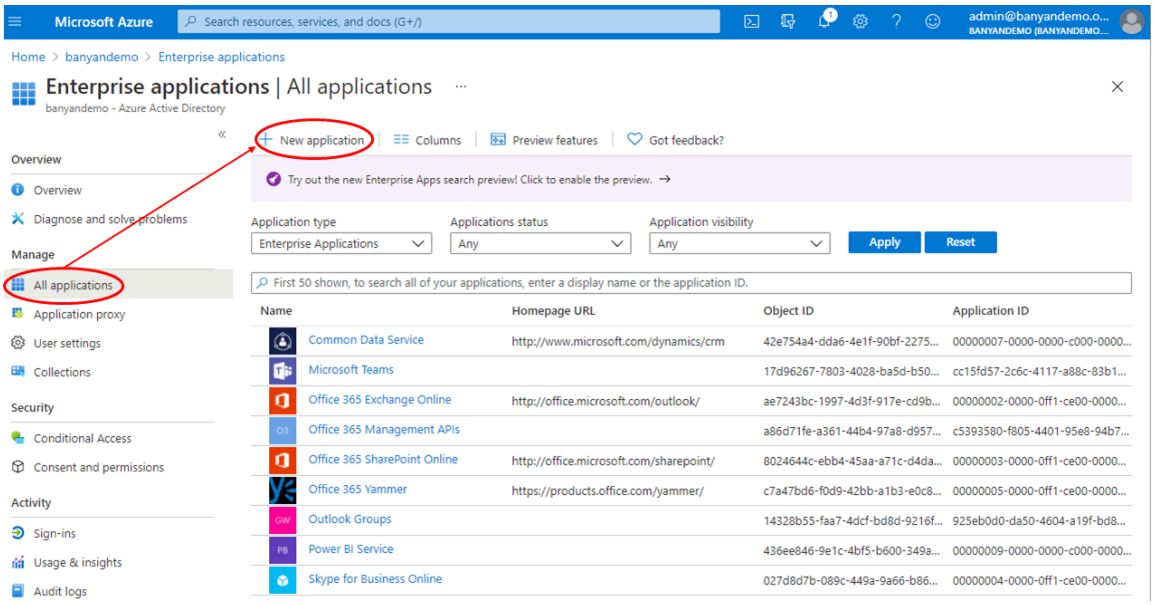
Admin access to the Command Center can be configured for Entra ID via the SAML2.0 protocol.

Steps

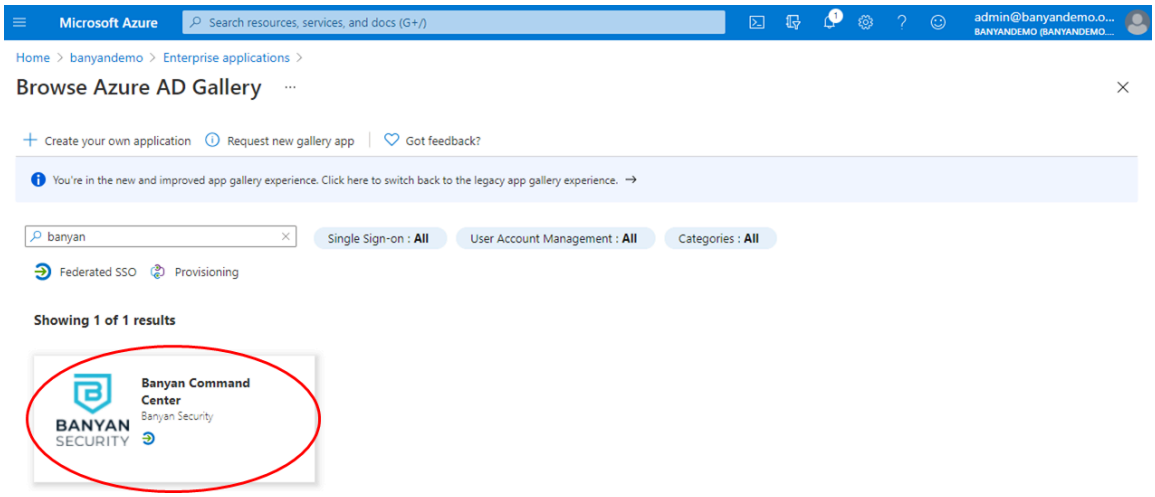
Please review Azure AD’s guide for additional information.

1. Add “Command Center Application” to your Entra ID Gallery

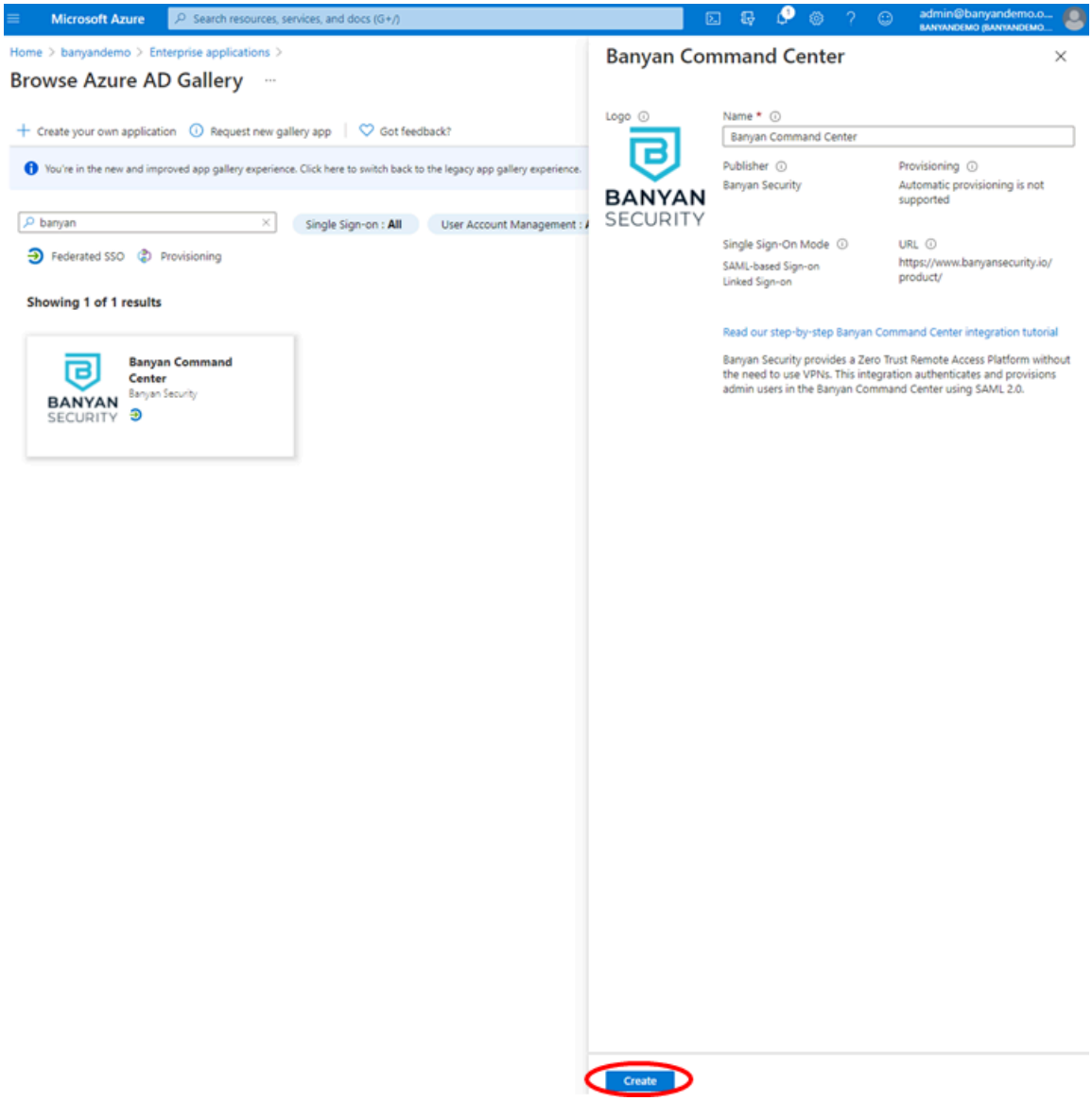
1.1 Log in to your Entra ID Portal, and then navigate to **Enterprise Applications** and select **New application**.



1.2 Search for “Banyan” and then select the **Banyan Command Center** option.

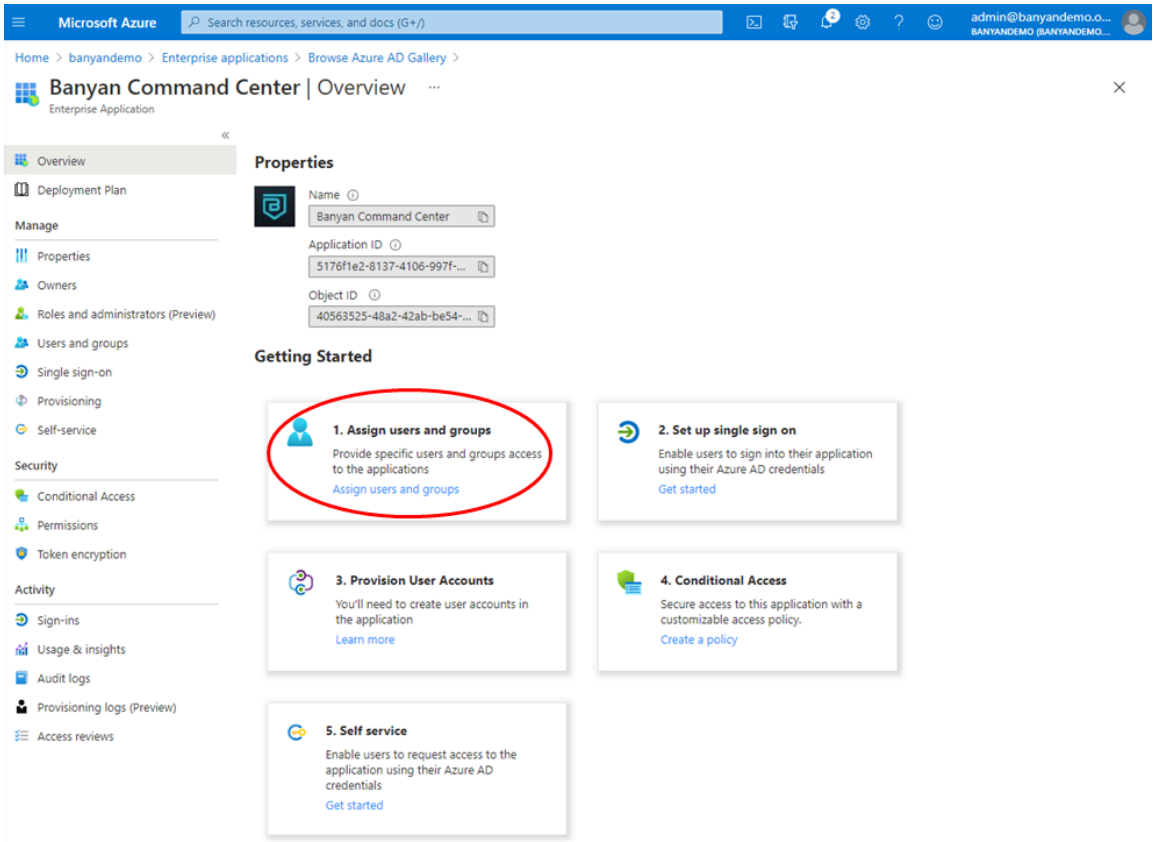


1.3 On the app overview page, select **Create**.

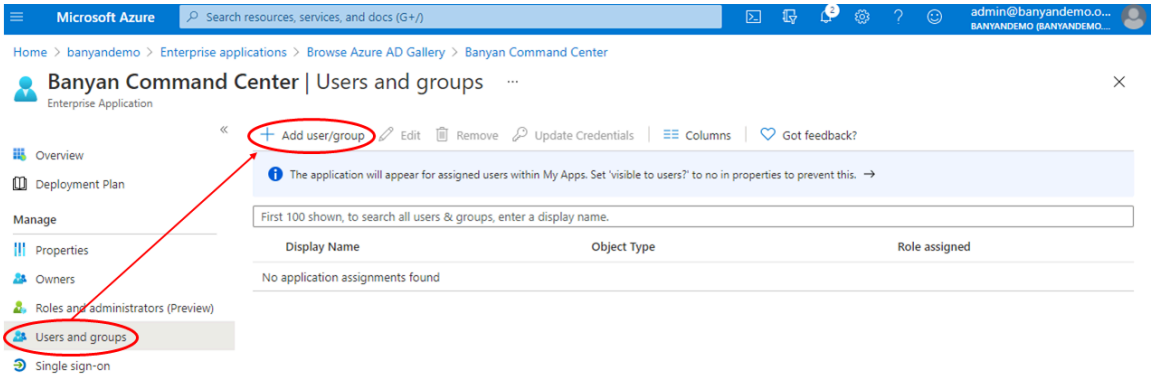


2. Assign users and groups

2.1 On the Overview page, select **1. Assign users and groups** under **Getting Started**.



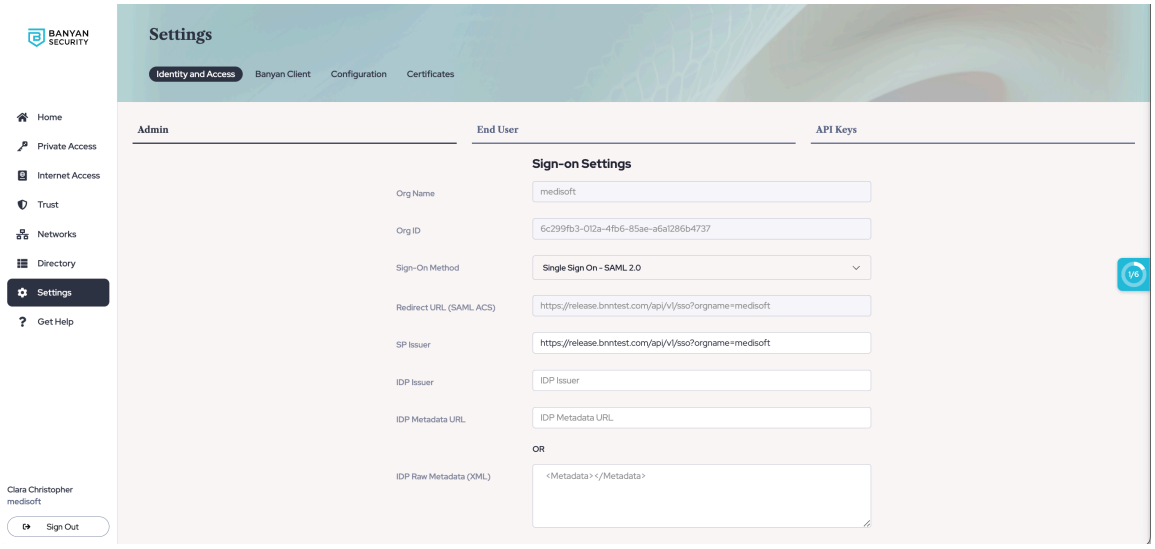
2.2 Assign the users and/or groups who will access the Banyan Command Center.



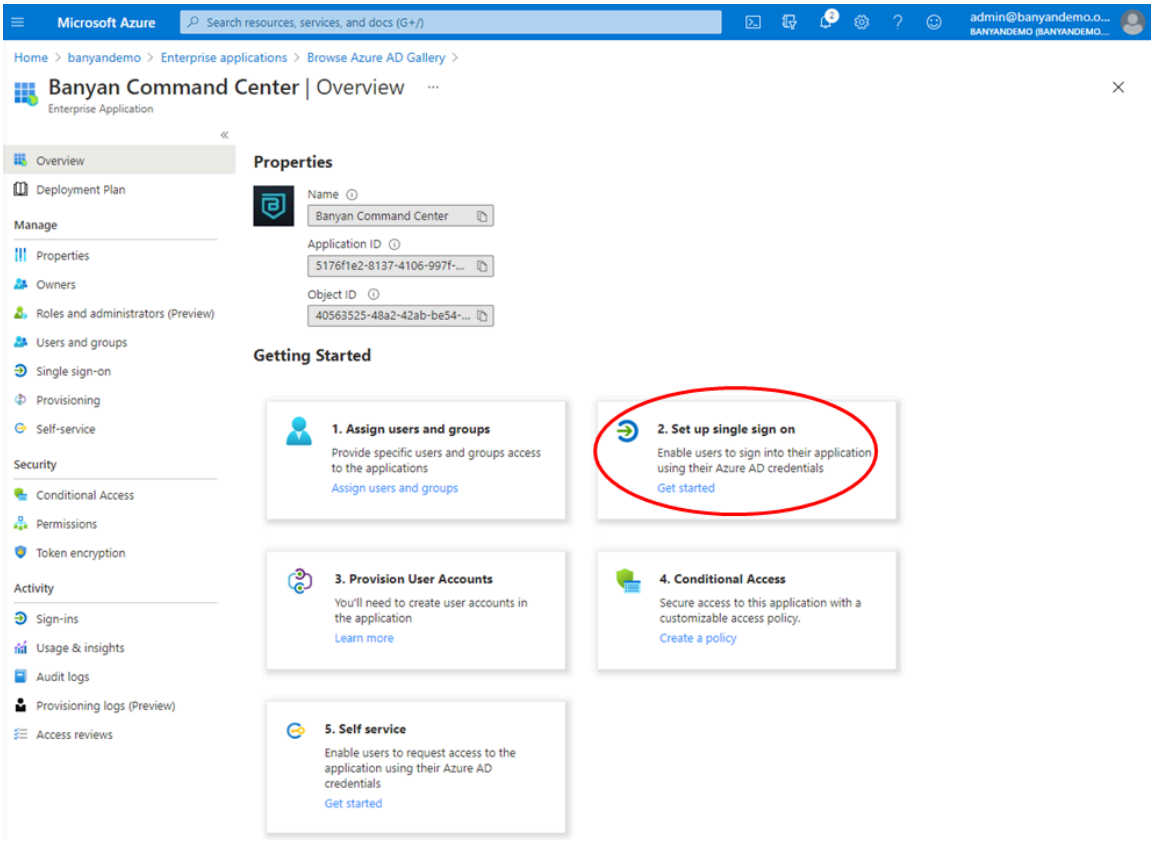
3. Set up single sign on

3.1 In the Command Center, navigate from **Settings** > **Identity and Access** tab > **Admin** tab. Note the **Redirect URL (SAML ACS)** in the form of `https://net.banyanops.com/sso?orgname=your_org_name`. You will use this value in **Step 3.5**.

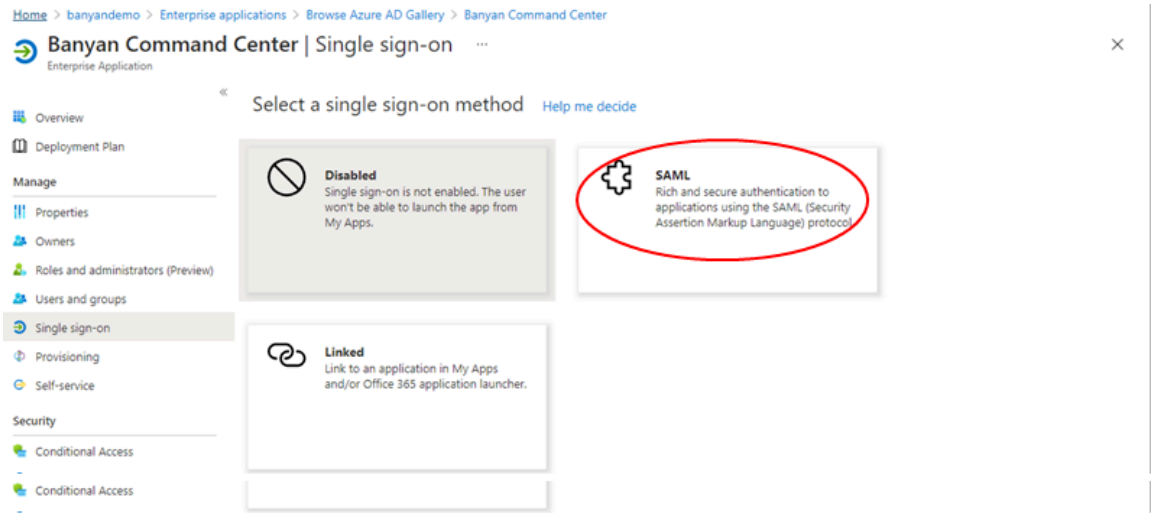
> Replace “your_org_name” with your org name used in the Command Center.



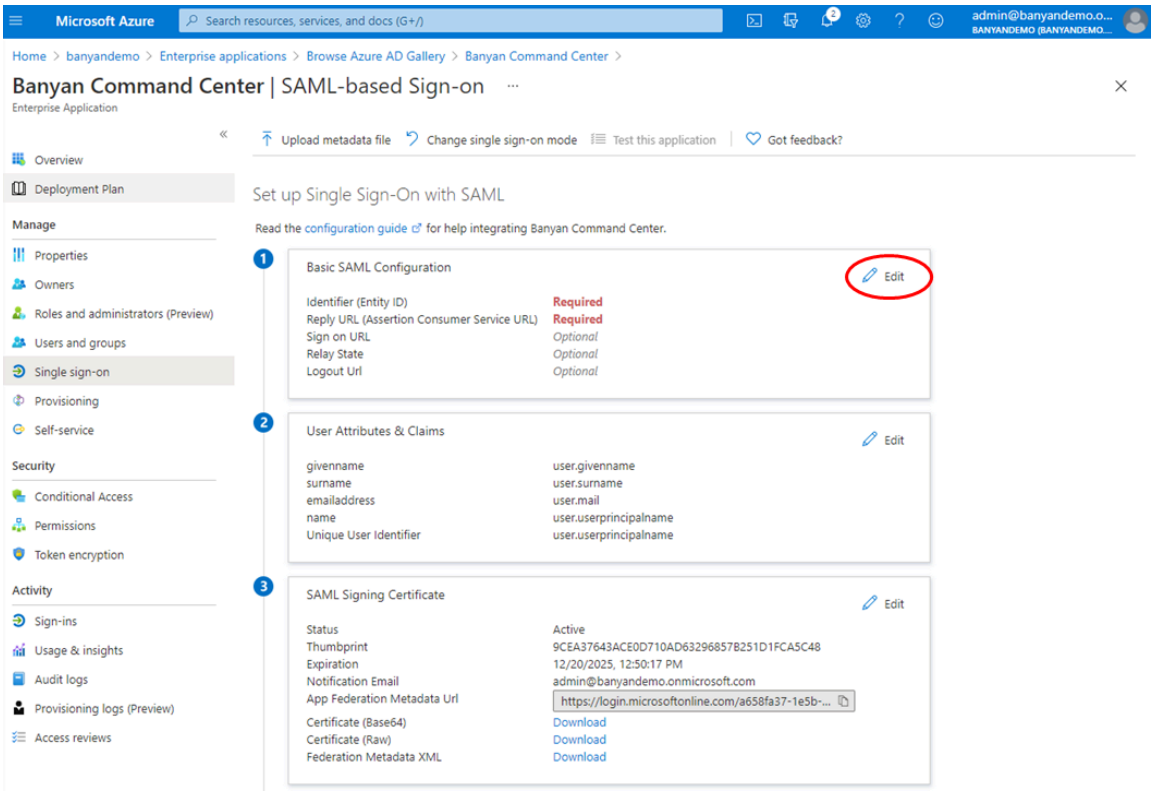
3.2 In the Azure AD Overview page, click **2. Set up single sign on** under **Getting Started**.



3.3 Under **Select a single sign-on method**, select **SAML**.

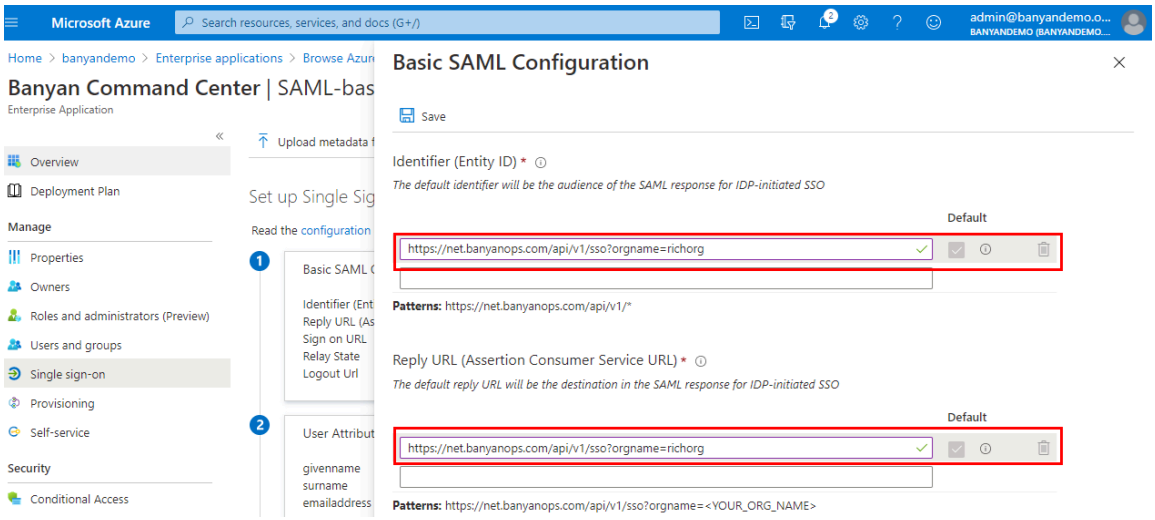


3.4 Under **Step 1 Basic SAML Configuration**, click **Edit**.



3.5 Enter the URL copied from step 3.1 for the values below:

- Identifier (Entity ID)
- Assertion Consumer Service URL



3.6 Save.

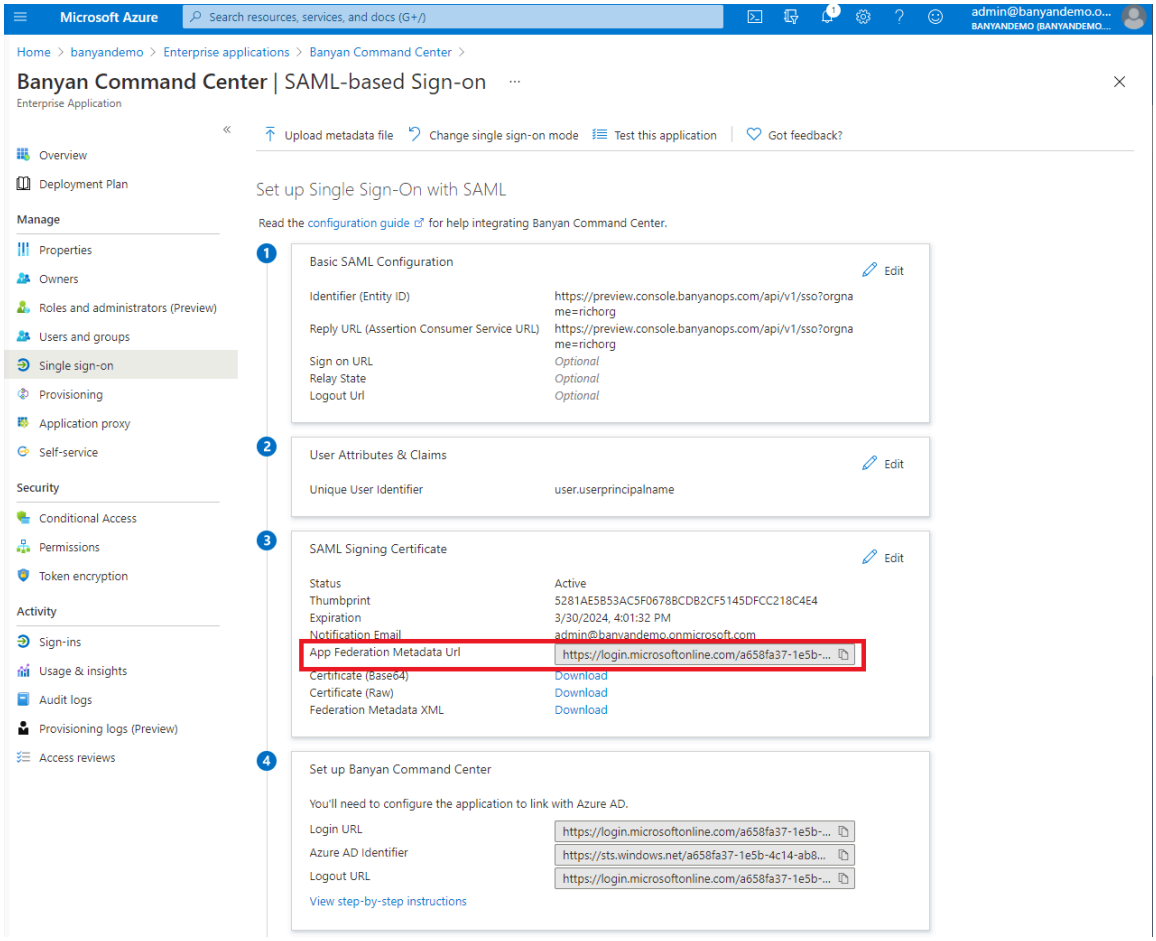
4. Verify your User Attributes & Claims

4.1 Cloud Secure Edge (CSE) uses your email address as your username attribute. Verify your User Attributes & Claims that will be presented to CSE. The Name ID Format should map to Email address or user principal name.

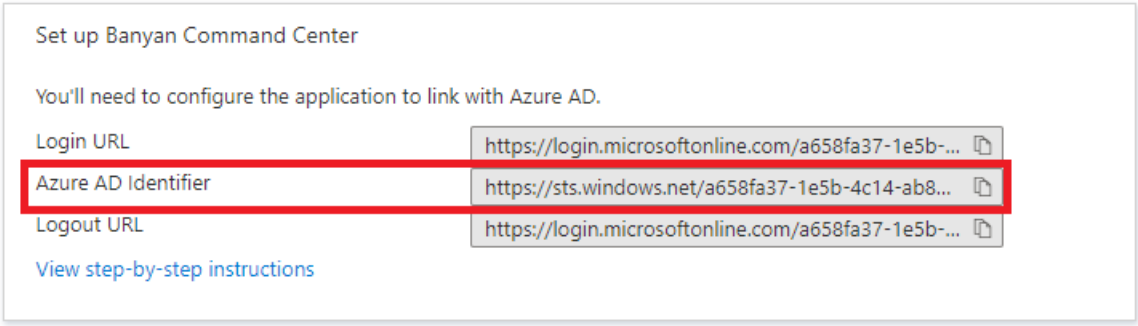
5. Configure your Org Setting in the Command Center

5.1 In the Azure AD Portal, navigate back to the **SAML-based Sign-on** configuration page.

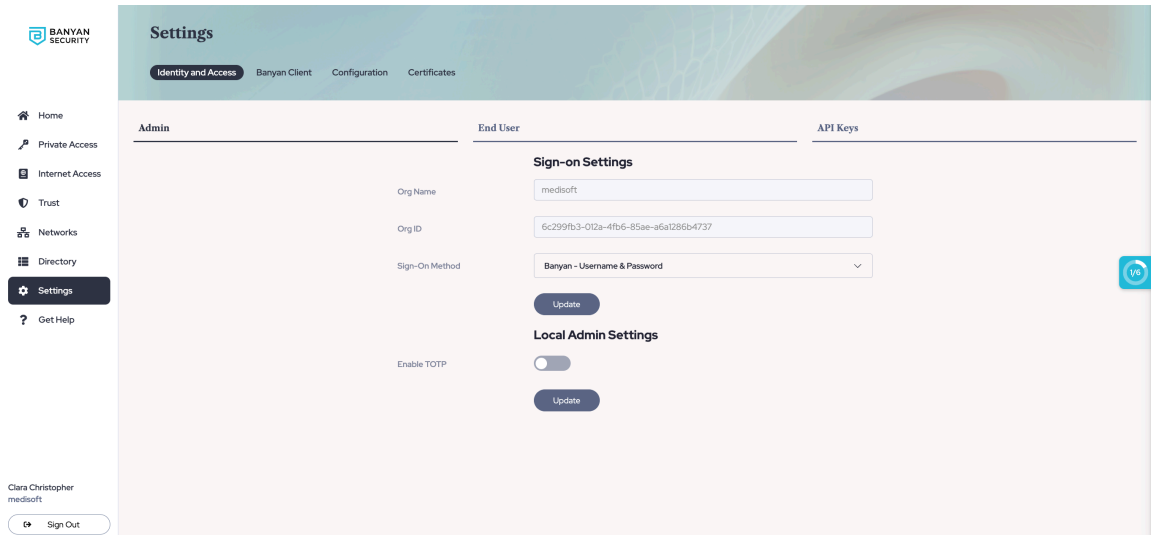
5.2 Under Step 3 SAML Signing Certificate, copy the **App Federation Metadata Url**.



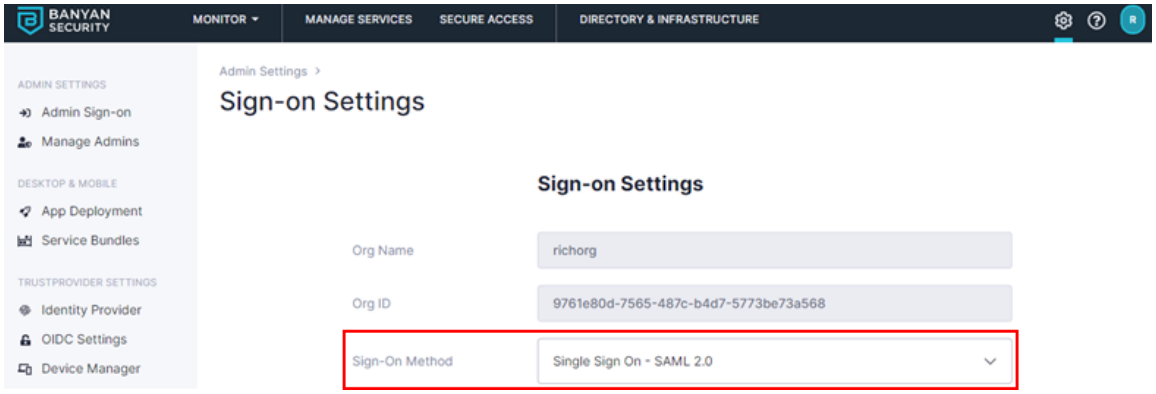
5.3 Under Step 4 Set up the Command Center, copy the **Azure AD Identifier**. This URL should start with https://sts.windows.net



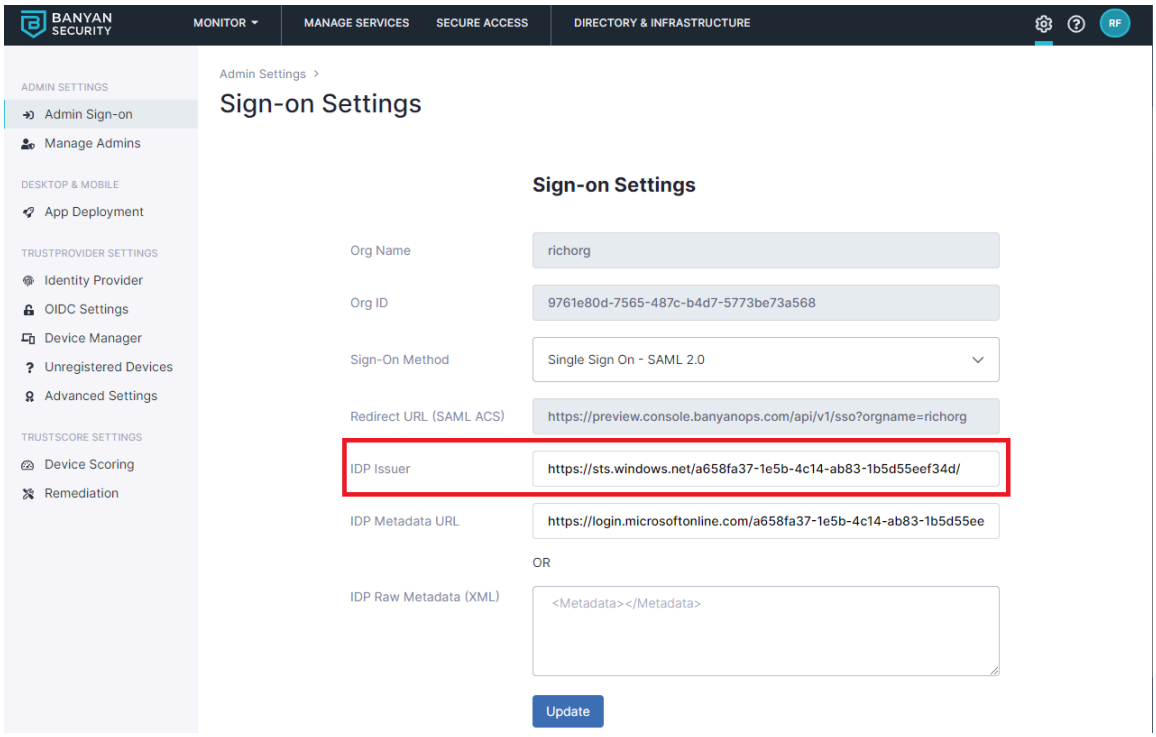
5.4 In the Command Center, navigate from **Settings** > **Identity and Access** tab > **Admin** tab.



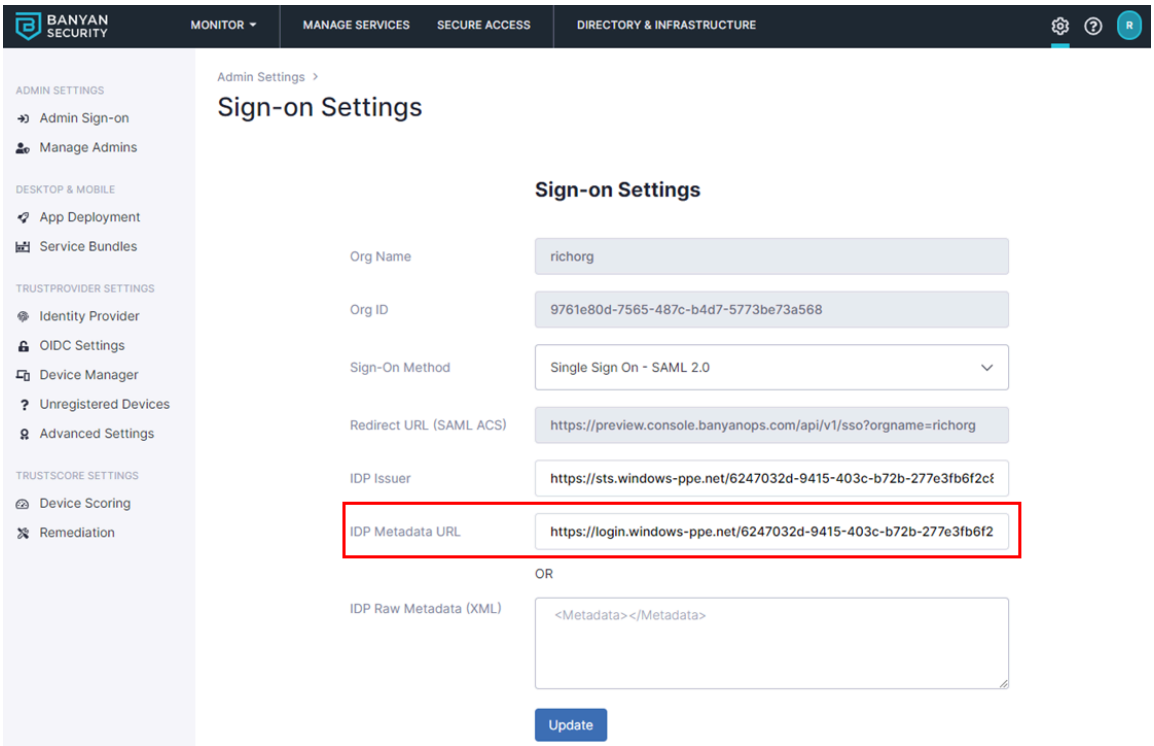
5.5 In **Sign-on Settings**, set **Sign-On Method** to **Single Sign On - SAML 2.0**.



5.6 Enter the IdP Issuer URL (from step 5.3). The URL should start with https://sts.windows.net



5.7 Enter the IDP Metadata URL (from step 5.2). The IDP Metadata URL should start with https://login.

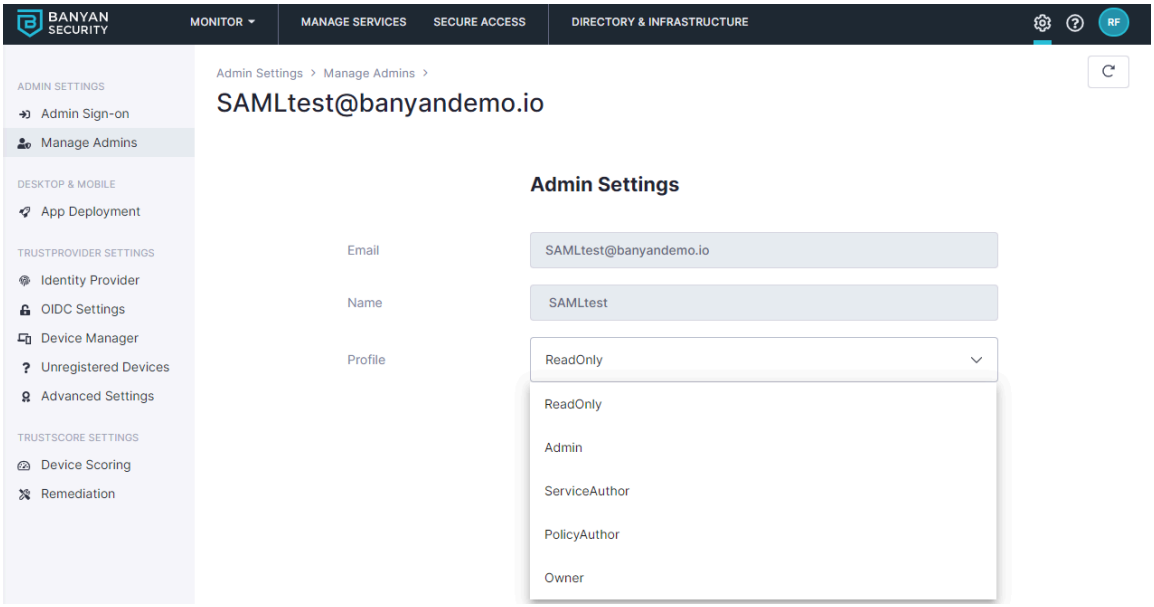


CSE will automatically obtain the IdP SSO URL, IdP Entity ID, IdP x.509 Certificate, and other parameters needed to set up SAML 2.0 with Azure AD.

5.8 Select **Update** to save the configuration.

6. (Optional) Set the Admin Profile in the Org Settings section

By default admins who access the Command Center using SAML are assigned a “ReadOnly” profile. You can update their profile and change permissions by navigating to Manage Admins and clicking on the admin user in the Banyan Command Center.



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts
Components
Release Notes

Guides

Quick Start Guides
Solutions
Feature Guides
API Guide