



Search docs...

Ctrl + /

[Home](#) > [Manage Admins](#) > [SAML Single Sign On](#) >

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

Steps

1. Add "Command Center Application" to your Entra ID Gallery
2. Assign users and groups
3. Set up single sign on
4. Verify your User Attributes & Claims
5. Configure your Org Setting in the Command Center
6. (Optional) Set the Admin Profile in the Org Settings section

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**.

Microsoft Azure | Search resources, services, and docs (G+)

Home > banyandemo > Enterprise applications

Enterprise applications | All applications

Overview

Manage

- All applications
- Application proxy
- User settings
- Collections
- Security
- Conditional Access
- Consent and permissions
- Activity
- Sign-ins
- Usage & insights
- Audit logs

Application type: Enterprise Applications | Applications status: Any | Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
Common Data Service	http://www.microsoft.com/dynamics/crm	42e754a4-dda6-4e1f-90bf-2275...	00000007-0000-0000-c000-0000...
Microsoft Teams		17d96267-7803-4028-ba5d-b50...	cc15fd57-2c6c-4117-a88c-83b1...
Office 365 Exchange Online	http://office.microsoft.com/outlook/	ae7243bc-1997-4d3f-917e-cd9b...	00000002-0000-0000-0000-0000...
Office 365 Management APIs		a86d71fe-a361-44b4-97a8-d957...	c5393580-f805-4401-95e8-94b7...
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	8024644c-ebb4-45aa-a71c-d4da...	00000003-0000-0000-0000-0000...
Office 365 Yammer	https://products.office.com/yammer/	c7a47bd6-f0d9-42bb-a1b3-e0c8...	00000005-0000-0000-0000-0000...
Outlook Groups		14328b55-faa7-4dcf-bd8d-9216f...	925eb0d0-da50-4604-a19f-bd8...
Power BI Service		436ee846-9e1c-4bf5-b600-349a...	00000009-0000-0000-c000-0000...
Skype for Business Online		027d8d7b-089c-449a-9a66-b86...	00000004-0000-0000-0000-0000...

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

Microsoft Azure | Search resources, services, and docs (G+)

Home > banyandemo > Enterprise applications >

Browse Azure AD Gallery

Create your own application | Request new gallery app | Got feedback?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience.

Search: banyan | Single Sign-on: All | User Account Management: All | Categories: All

Federated SSO | Provisioning

Showing 1 of 1 results

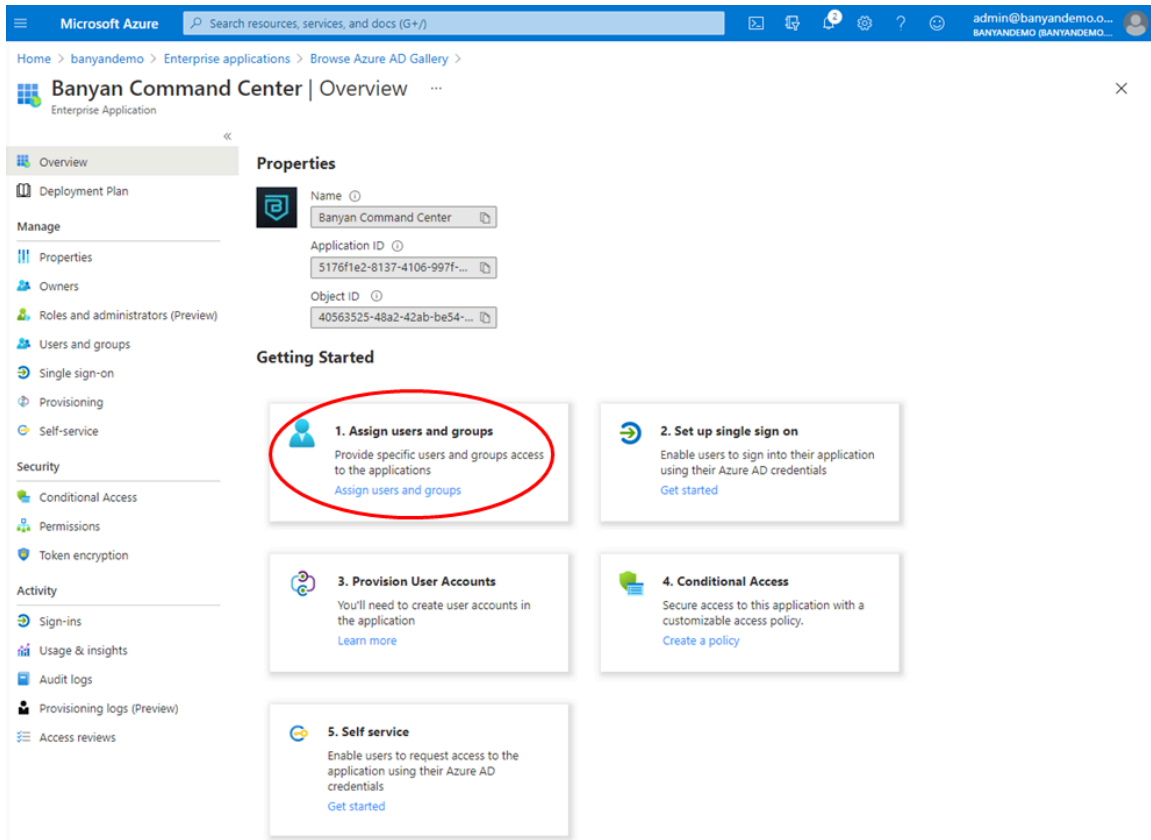
Banyan Command Center
Banyan Security

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

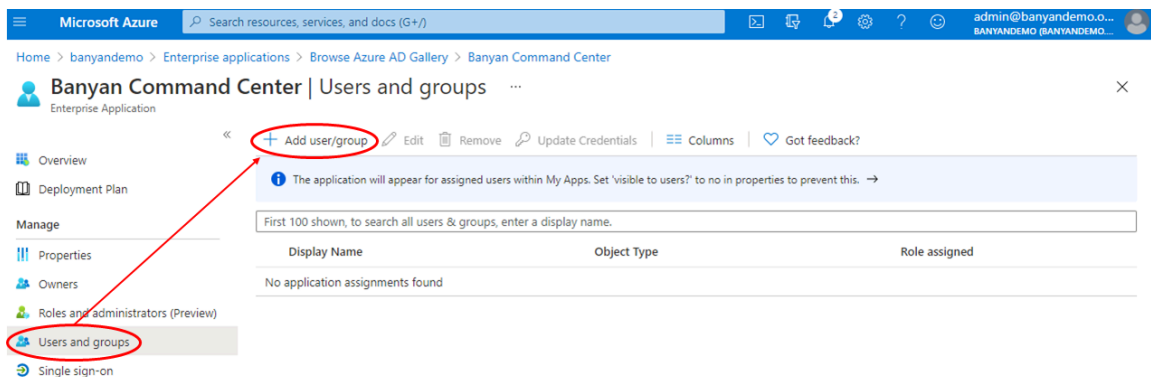
The screenshot shows the Microsoft Azure portal interface. On the left, the 'Browse Azure AD Gallery' page is displayed with a search for 'banyan'. A single result is shown for 'Banyan Command Center' by 'Banyan Security'. On the right, a detailed view of the application is shown. The application name is 'Banyan Command Center', the publisher is 'Banyan Security', and the provisioning status is 'Automatic provisioning is not supported'. The SAML-based sign-on URL is 'https://www.banyansecurity.io/product/'. A red circle highlights the 'Create' button at the bottom of the application card.

2. Assign users and groups

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



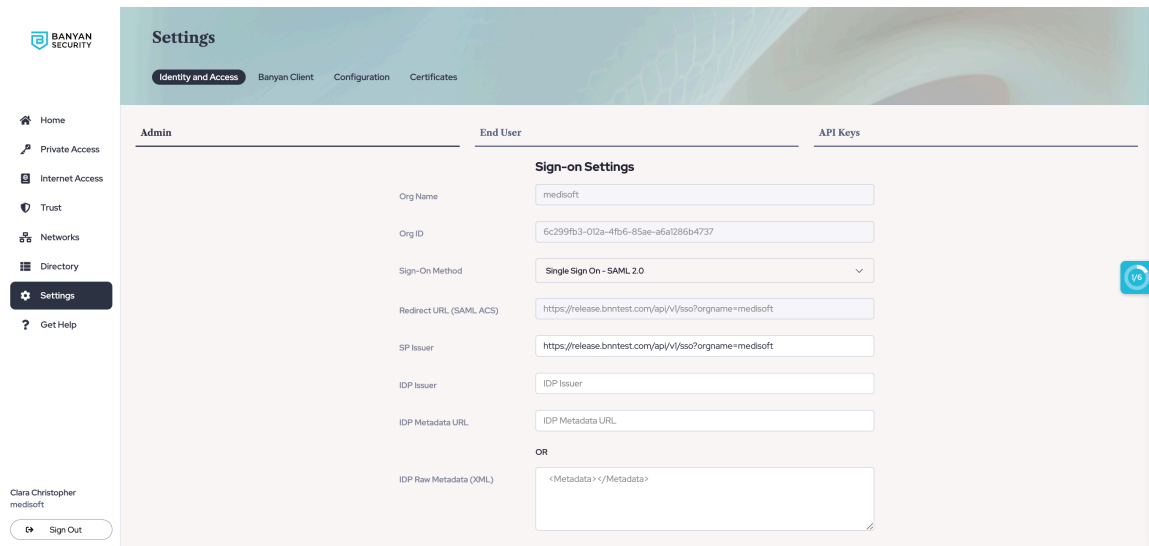
2.2 Assign the users and/or groups who will access the Banyan Command Center.



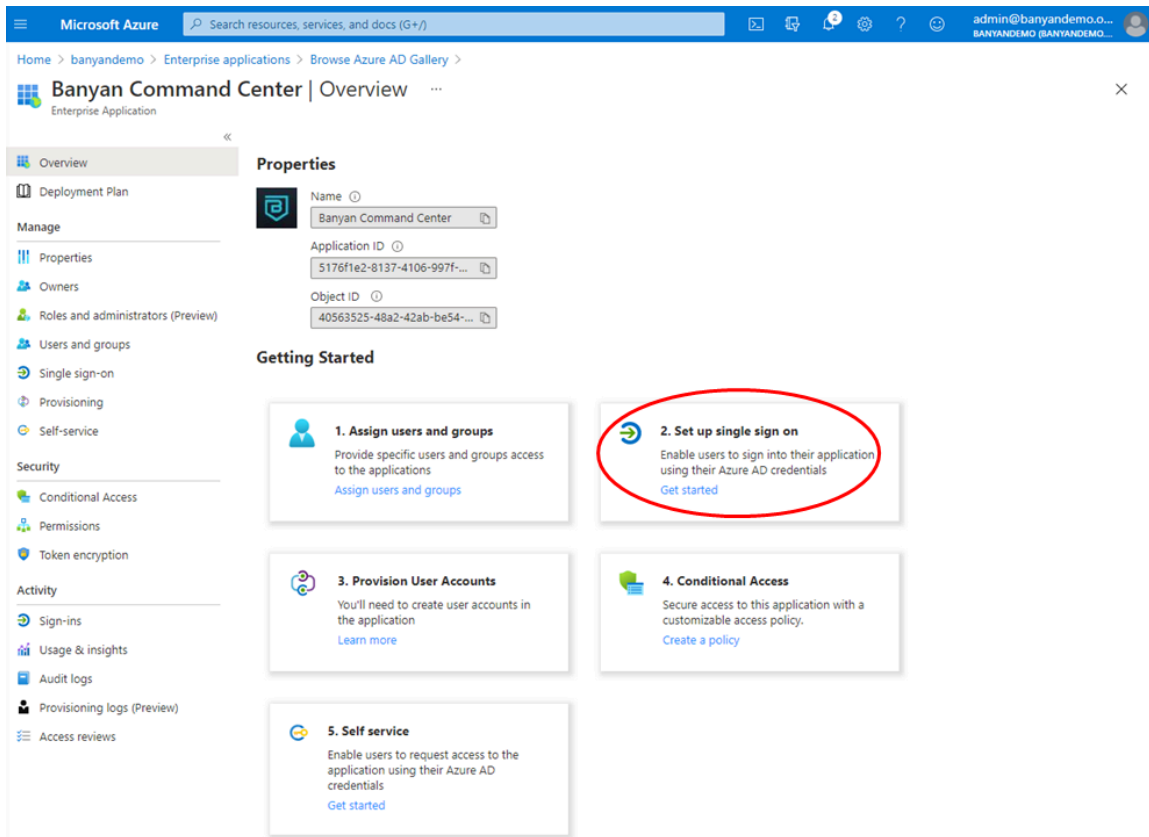
3. Set up single sign on

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**.

Home > banyandemo > Enterprise applications > Browse Azure AD Gallery > Banyan Command Center

Banyan Command Center | Single sign-on

Select a single sign-on method [Help me decide](#)

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Linked**
Link to an application in My Apps and/or Office 365 application launcher.

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

Microsoft Azure Search resources, services, and docs (G+)

Home > banyandemo > Enterprise applications > Browse Azure AD Gallery > Banyan Command Center >

Banyan Command Center | SAML-based Sign-on

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Banyan Command Center.

- Basic SAML Configuration** [Edit](#)
 - Identifier (Entity ID) **Required**
 - Reply URL (Assertion Consumer Service URL) **Required**
 - Sign on URL *Optional*
 - Relay State *Optional*
 - Logout URL *Optional*
- User Attributes & Claims** [Edit](#)
 - givenname user.givenname
 - surname user.surname
 - emailaddress user.mail
 - name user.userprincipalname
 - Unique User Identifier user.userprincipalname
- SAML Signing Certificate** [Edit](#)
 - Status Active
 - Thumbprint 9CEA37643ACE0D710AD632968578251D1FCASC48
 - Expiration 12/20/2025, 12:50:17 PM
 - Notification Email admin@banyandemo.onmicrosoft.com
 - App Federation Metadata Url <https://login.microsoftonline.com/a658fa37-1e5b-...>
 - Certificate (Base64) [Download](#)
 - Certificate (Raw) [Download](#)
 - Federation Metadata XML [Download](#)

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

- Identifier (Entity ID)
- Assertion Consumer Service URL

Microsoft Azure Search resources, services, and docs (G+)

admin@banyandemo.o... BANYANDEMO (BANYANDEMO...)

Home > banyandemo > Enterprise applications > Browse Azure

Banyan Command Center | SAML-based Enterprise Application

Overview Deployment Plan Manage Properties Owners Roles and administrators (Preview) Users and groups Single sign-on Provisioning Self-service Security Conditional Access

Basic SAML Configuration

Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

https://net.banyanops.com/api/v1/sso?orgname=richorg

Default

Patterns: https://net.banyanops.com/api/v1/*

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

https://net.banyanops.com/api/v1/sso?orgname=richorg

Default

Patterns: https://net.banyanops.com/api/v1/sso?orgname=<YOUR_ORG_NAME>

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**.

Microsoft Azure | Search resources, services, and docs (G+)

Home > banyandemo > Enterprise applications > Banyan Command Center >

Banyan Command Center | SAML-based Sign-on

Enterprise Application

Overview | Deployment Plan | Manage | Properties | Owners | Roles and administrators (Preview) | Users and groups | **Single sign-on** | Provisioning | Application proxy | Self-service | Security | Conditional Access | Permissions | Token encryption | Activity | Sign-ins | Usage & insights | Audit logs | Provisioning logs (Preview) | Access reviews

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Banyan Command Center.

- Basic SAML Configuration**

Identifier (Entity ID)	https://preview.console.banyanops.com/api/v1/sso?orgname=richorg	Edit
Reply URL (Assertion Consumer Service URL)	https://preview.console.banyanops.com/api/v1/sso?orgname=richorg	
Sign on URL	Optional	
Relay State	Optional	
Logout URL	Optional	
- User Attributes & Claims**

Unique User Identifier	user.userprincipalname	Edit
------------------------	------------------------	------
- SAML Signing Certificate**

Status	Active	Edit
Thumbprint	5281AE5853AC5F06788CD82CF5145DFCC218C4E4	
Expiration	3/30/2024 4:01:32 PM	
Notification Email	admin@banyandemo.onmicrosoft.com	
App Federation Metadata Url	https://login.microsoftonline.com/a658fa37-1e5b-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
- Set up Banyan Command Center**

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/a658fa37-1e5b-...	
Azure AD Identifier	https://sts.windows.net/a658fa37-1e5b-4c14-ab8-...	
Logout URL	https://login.microsoftonline.com/a658fa37-1e5b-...	

[View step-by-step instructions](#)

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

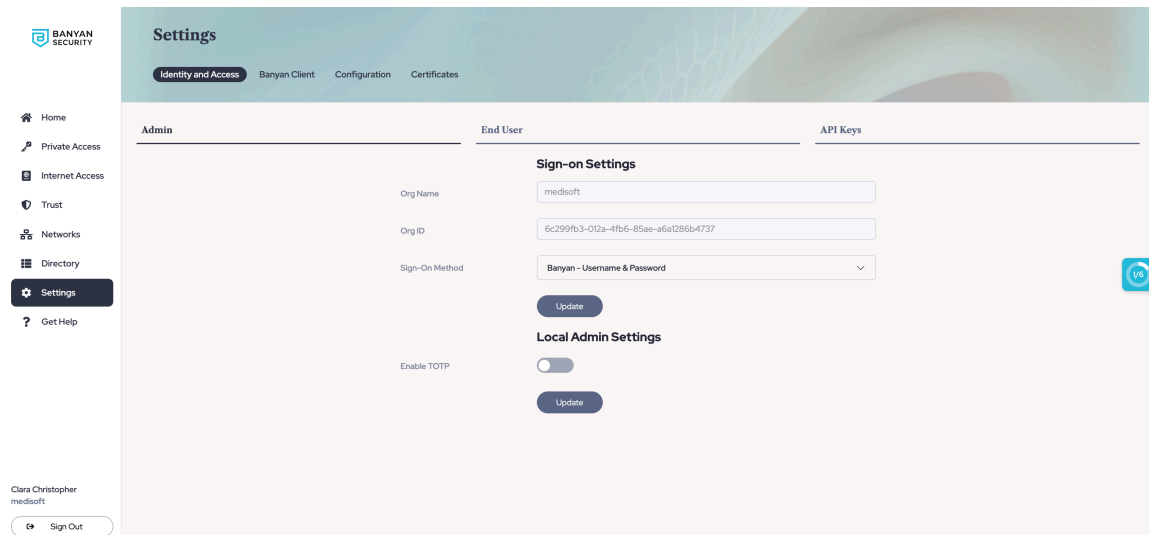
Set up Banyan Command Center

You'll need to configure the application to link with Azure AD.

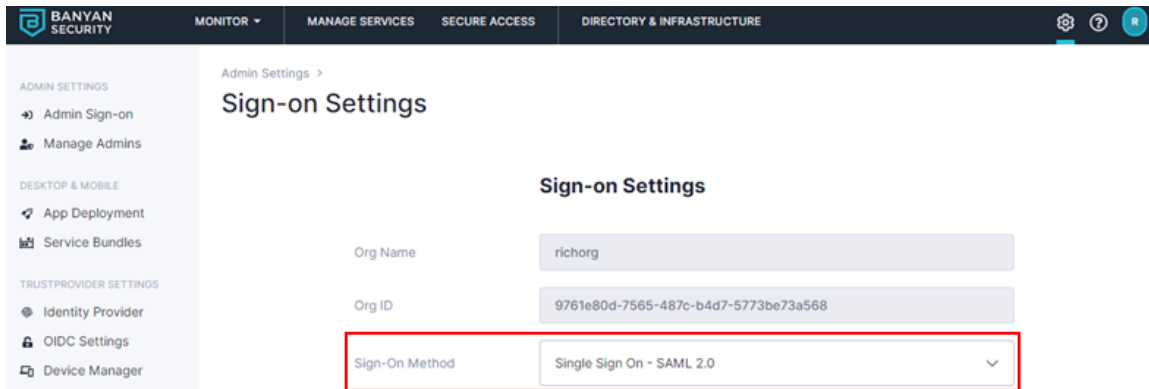
Login URL	https://login.microsoftonline.com/a658fa37-1e5b-...	
Azure AD Identifier	https://sts.windows.net/a658fa37-1e5b-4c14-ab8-...	
Logout URL	https://login.microsoftonline.com/a658fa37-1e5b-...	

[View step-by-step instructions](#)

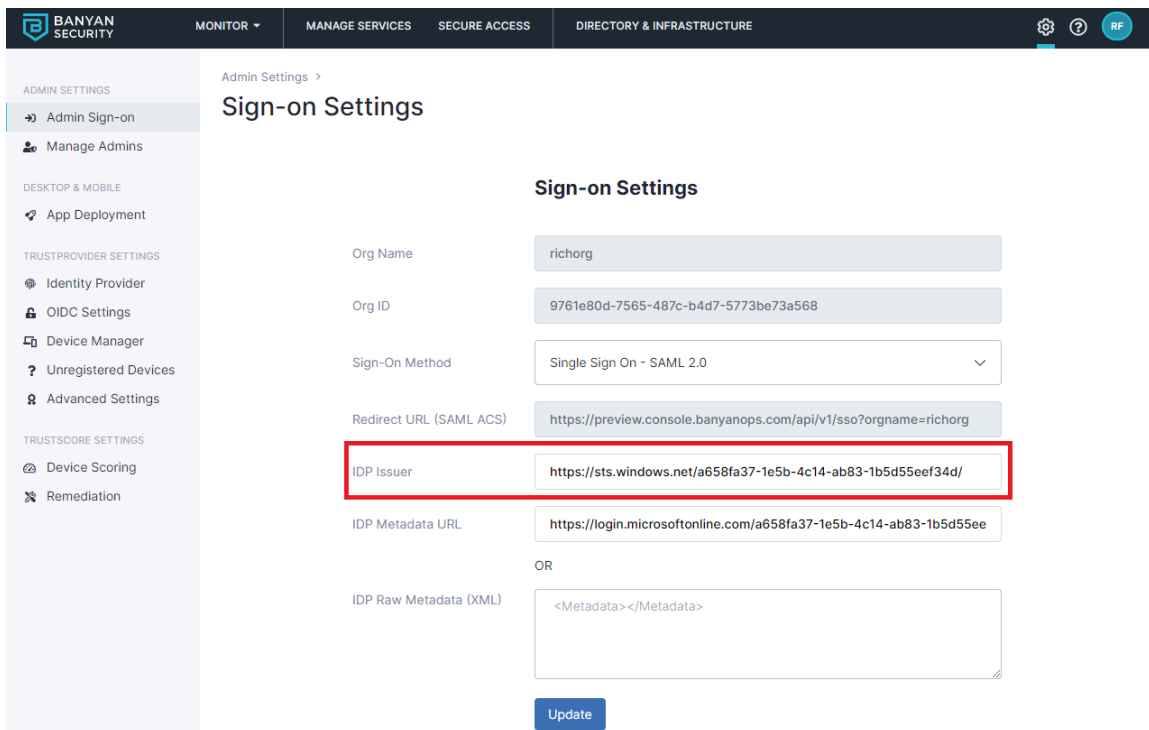
5.4 In the Command Center, navigate from **Settings > Identity and Access** tab > **Admin** tab.



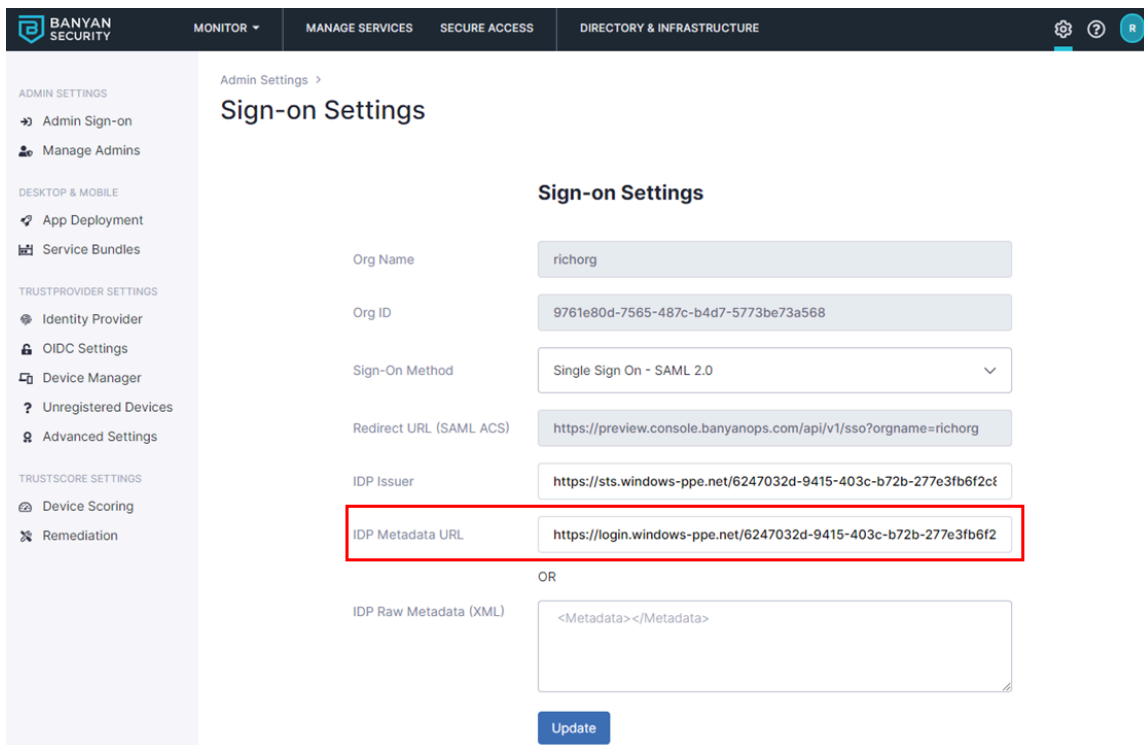
5.5 In Sign-on Settings, set Sign-On Method to Single Sign On - SAML 2.0.



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.

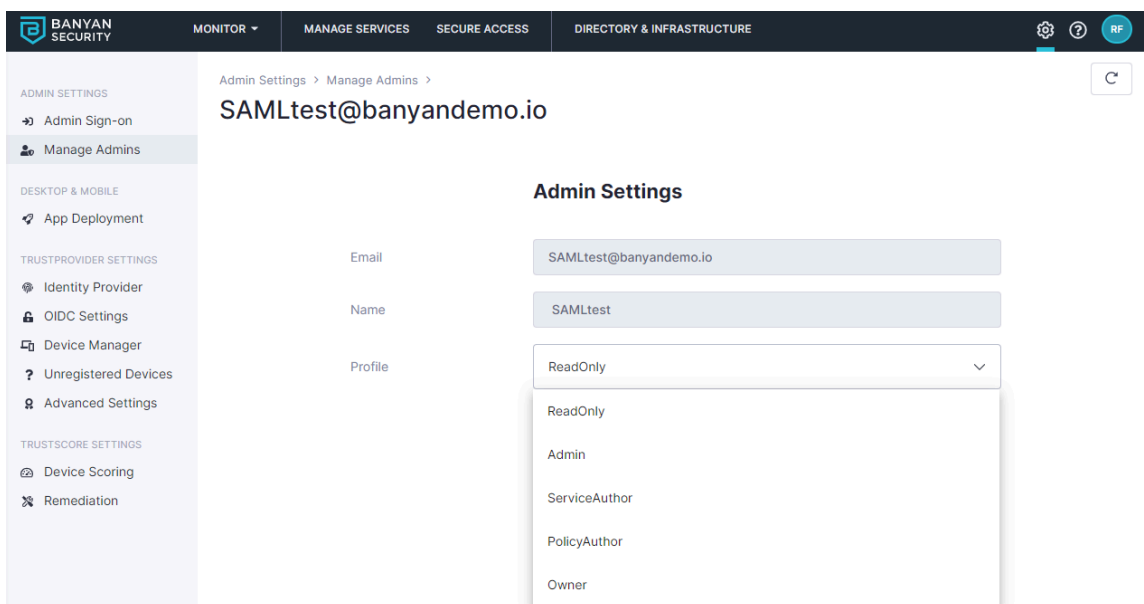


CSE will automatically obtain the IdP SSO URL, IdP Entity ID, IdP x.509 Certificate, and other parameters needed to set up SAML 2.0 with Azure AD.

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.





© 2026. All rights reserved.

Site generated at YYYYMMDD

Links

[Concepts](#)

[Components](#)

[Release Notes](#)

Guides

[Quick Start Guides](#)

[Solutions](#)

[Feature Guides](#)

[API Guide](#)