



Search docs...

Ctrl + /

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

Single Sign On using SAML2.0 - Okta

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

Updated on

ON THIS PAGE:

Overview

Steps

1. Add "Command Center Application" to your Okta Organization
2. Assign Okta users and/or groups
3. Note the Okta IdP Settings and enter them in the Banyan Command Center
4. (Optional) Set the Admin Profile in the Org Settings section

Overview

Admin access to the Command Center can be configured for [Okta](#) via the SAML2.0 protocol.

Steps

Please review [Okta's guide](#) for additional information.

1. Add "Command Center Application" to your Okta Organization

1.1 Log in to your Okta admin console, and then navigate to **Applications** and click **Add Application**.

Dashboard

Directory

Applications

Self Service

Security

Workflow

Reports

Settings

okta

Search...

Applications

You have 4 apps remaining

Upgrade to add more than 5 apps.

Upgrade to a paid plan to create more apps and get more monthly active users.

Add Application Assign Applications More

STATUS

ACTIVE	1
INACTIVE	3

Banyan TrustProvider

Client ID: 0oa1lk6m0tQvQd7c44x7

Thanks for trying the Okta free plan. Upgrade to a paid plan to create more apps and get more Monthly Active Users.

Upgrade

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

okta

Search...

← Back to Applications

Add Application

Create New App

CATEGORIES

Featured	
API Management	6
Apps	6298
Apps for Good	13
CASB	2
Directories and HR Systems	13
Security Applications	709
Okta Applications	16
VPN	22

INTEGRATIONS

Banyan Command Center	SAML
Yanomo	SWA
Voyanta	SWA
Filesanywhere	SWA
23Company	SWA

See All Results

CATEGORIES

Core Banking

1.3 On the app overview page, click **Add**.

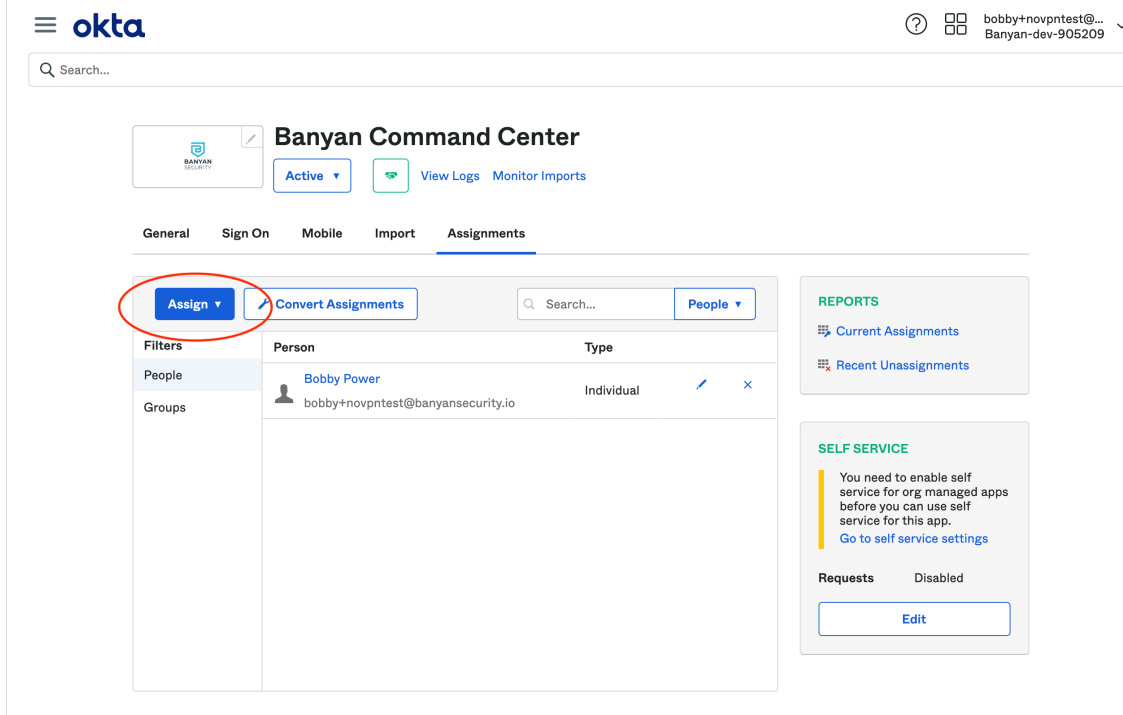
The screenshot shows the Okta Admin Console interface. At the top left is the Okta logo. A search bar is located below the logo. The main heading is "Banyan Command Center". To the left of the main content is a sidebar with the Banyan Security logo and a blue "Add" button circled in red. Below the sidebar, there are sections for "CATEGORIES" (Security Applications) and "LAST UPDATE" (2021-02-25T14:48:17). The main content area has an "Overview" section with a description of Banyan Security's Zero Trust Remote Access Platform. Below the overview is a "Capabilities" section with two columns: "Access" (SAML, OIDC, WS-Federation) and "Provisioning" (Create, Update, Deactivate).

1.4 On the **General Settings** page, select **Done**.

The screenshot shows the "Add Banyan Command Center" configuration page. At the top is the Okta logo and a search bar. The main heading is "Add Banyan Command Center". Below the heading is a tab labeled "1 General Settings". The "General Settings - Required" section contains the following fields: "Application label" (Banyan Command Center), "Application Visibility" (Do not display application icon to users, Do not display application icon in the Okta Mobile App), and "Cancel" and "Done" buttons. The "Done" button is circled in red. To the right of the form is a "General settings" section with the text "All fields are required to add this application unless marked optional." At the bottom of the page is a footer with copyright information and links for Privacy, Version 2021.02.2, OK11 Cell (US), Status site, Download Okta Plugin, and Feedback.

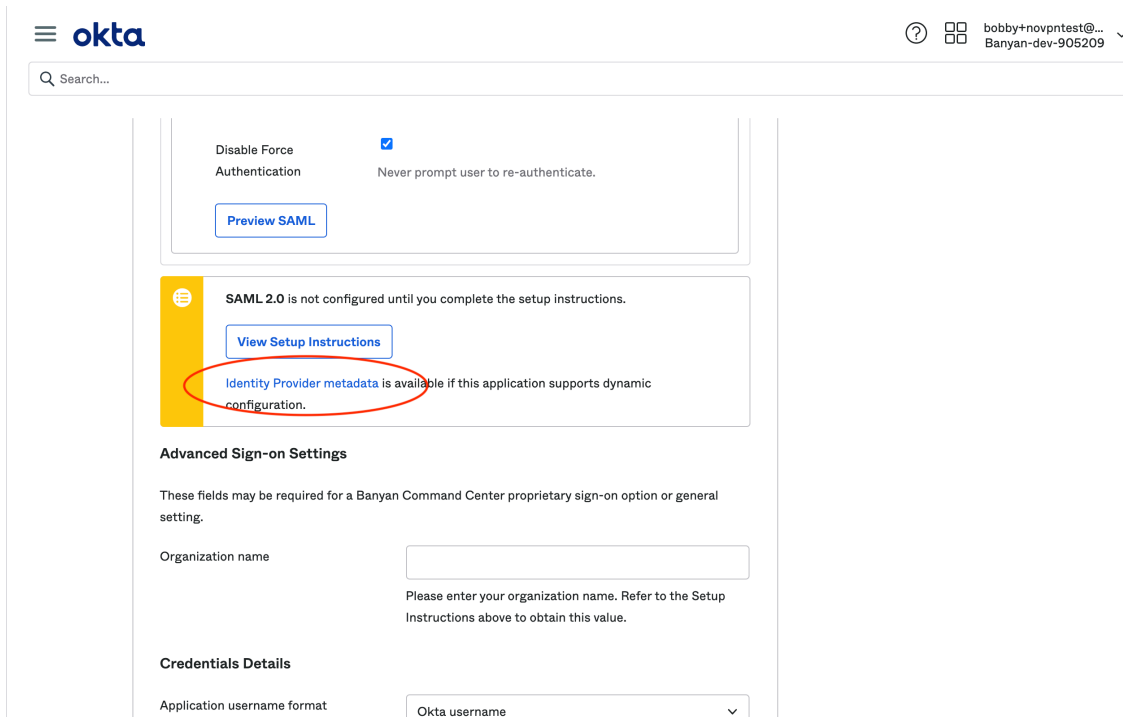
2. Assign Okta users and/or groups

2.1 Assign the Okta users and/or groups who will access the Command Center.



3. Note the Okta IdP Settings and enter them in the Banyan Command Center

3.1 Navigate to the **Sign On** tab and then right-click the **Identity Provider metadata** link to note the URL (which you will enter in the Command Center in step 3.5).



3.2 Select the **Identity Provider metadata** link to open the metadata contents in a new browser tab.

3.3 From the metadata contents, note the **Entity** URL or ID (which you will enter in the Banyan Command Center in step 3.5).

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk2d5mkm8ecxK8c14x7">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <md:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            [REDACTED]
          </ds:X509Certificate>
        </ds:X509Data>
      </md:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="..." />
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="..." />
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

3.4 Log into the Banyan Command Center, and navigate from **Settings > Identity and Access tab > Admin** tab.

The screenshot shows the Banyan Security Settings interface. The left sidebar contains navigation options: Home, Private Access, Internet Access, Trust, Networks, Directory, Settings (selected), and Get Help. The main content area is titled 'Settings' and has tabs for 'Identity and Access', 'Banyan Client', 'Configuration', and 'Certificates'. Under 'Identity and Access', there are sub-tabs for 'Admin', 'End User', and 'API Keys'. The 'Admin' tab is active, showing 'Sign-on Settings' for the 'medisoft' organization. The settings include: Org Name (medisoft), Org ID (6c299fb3-012a-4fb6-85ae-a6a286b4737), Sign-On Method (Single Sign On - SAML 2.0), Redirect URL (SAML ACS) (https://release.bnntest.com/api/vj/sso?orgname=medisoft), SP Issuer (https://release.bnntest.com/api/vj/sso?orgname=medisoft), IDP Issuer (IDP Issuer), IDP Metadata URL (IDP Metadata URL), and IDP Raw Metadata (OXML) (<Metadata> </Metadata>). A 'Sign Out' button is visible in the bottom left corner.

3.5 Set **Sign-On Method** to **Single Sign On - SAML 2.0** and then enter the IdP details from Okta:

- For **IDP Issuer URL**, enter the Entity URL or ID noted in step 3.3.
- For **IDP Metadata URL**, enter the Identity Provider metadata URL noted in step 3.1.

3.6 Select **Update**.

3.7 Copy the **Org Name**, which will be used in step 3.9.

3.8 In the Okta admin console, select the **Sign On** tab for the Command Center app, then click **Edit**.

3.9 Scroll down to the **Advanced Sign-on Settings** and then enter the Org Name noted in step 3.7.

Identity Provider metadata is available if this application supports dynamic configuration.

Advanced Sign-on Settings

These fields may be required for a Banyan Command Center proprietary sign-on option or general setting.

Organization name

Please enter your organization name. Refer to the Setup Instructions above to obtain this value.

Credentials Details

Application username format

Password reveal Allow users to securely see their password (Recommended)

i Password reveal is disabled, since this app is using SAML with no password.

Save

Sign On Policy

3.10 Select **Save**.

4. (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](#) in the Org Settings section of the Command Center.

SONICWALL
CLOUD SECURE EDGE

© 2026. All rights reserved.

Site generated at YYYYMMDD

Links

[Concepts](#)

[Components](#)

[Release Notes](#)

Guides

[Quick Start Guides](#)

[Solutions](#)

[Feature Guides](#)

[API Guide](#)