Single Sign On using SAML2.0

Enable SSO authentication to the Command Center using SAML2.0

Updated on

ON THIS PAGE:

Overview

Admin access to the Command Center can be configured for Single Sign On Identity Provider via the SAML2.0 protocol. Most SSO SAML providers can be configured following these instructions, however you can also review step-by-step instructions for Okta and Azure AD.

Steps

1. Configure your SAML2.0 Identity Provider (IdP)

In your IDP, enter the following values so Cloud Secure Edge (CSE) is set up as a Service Provider (SP).

A) Single Sign On URL

The CSE Org Settings page will provide you a **Single Sign On (SAML ACS) URL** of the form `https://net.banyanops.comapi/v1/sso?orgname=your_org_name` .

Place this parameter where your IdP asks for:

- **Assertion Consumer Service URL** (also called **Recipient** or **Single Sign On URL**)
- **Service Provider Entity ID** (also called **Audience URI** or **Service Provider Issuer**)

B) Assertion Subject Statements

CSE uses your email address as your username, so set that in the Assertion Subject Statements.

- **Name ID Format** should be `EmailAddress`
- **Application Username** should be `Email`

C) Other Notes

Some IdP's ask for the Service Provider Certificate - this is used to verify the signature of SAML requests, but it is safe to skip this step.

2. Configure your Org Setting in the Command Center

In the Command Center, in the Org Settings page, set the Identity Provider to `SAML 2.0`. Then, enter the following details.

A) Identity Provider Metadata

You can enter either your Identity Provider's Metadata URL or the "raw" Metadata XML file from your Identity Provider.

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

B) Identity Provider Issuer URL

As a configuration check, also provide the IDP Issuer URL.

C) Save the configuration

Click on the "Update Settings" button to save the configurations.

D) (Optional) Set the Admin Profiles

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

Site generated at YYYYMMDD

Links

Concepts

Components

Release Notes

Guides

Quick Start Guides

Solutions

Feature Guides

API Guide