Apply Device Policies on SaaS Applications

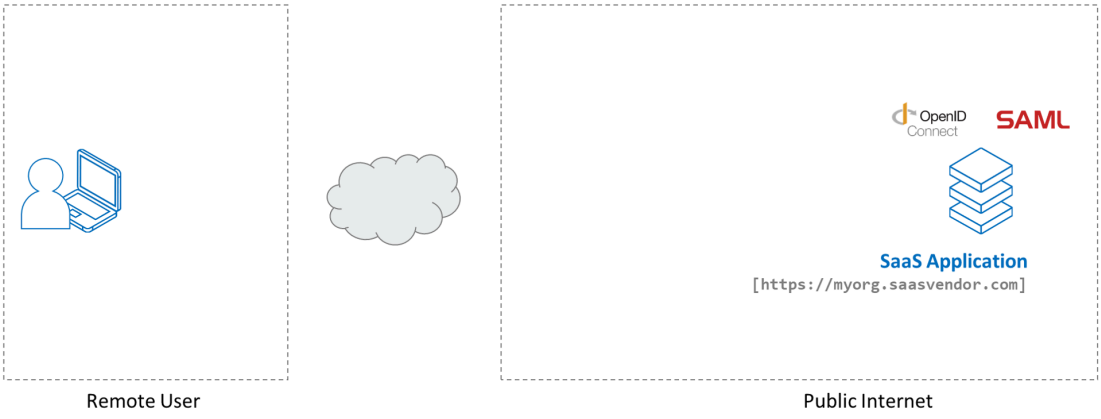
This article will show you how to enable device-based access control policies on a SaaS application using Cloud Secure Edge's zero-trust security framework

Updated on

ON THIS PAGE:

Scenario

For this guide we have a public internet-facing web application - typically a multi-tenant Software-as-a-Service (SaaS) Application - that supports user authentication using OpenID Connect (OIDC).



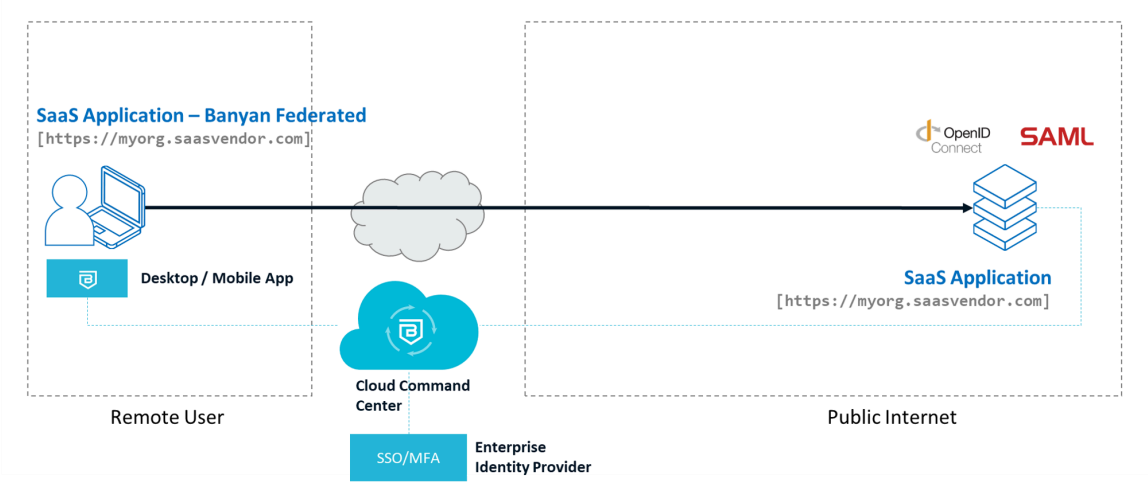
We assume your end users have been added to your Cloud Secure Edge (CSE) directory, and that they have the latest desktop or mobile app installed on devices from which they will access this application.

This guide primarily refers to OIDC-enabled SaaS applications. However, CSE also supports SAML-

enabled SaaS Applications and the same steps can be extended to SAML-enabled SaaS applications.

Setup

The setup is as follows:



1. The SaaS Application we'll secure supports OpenID Connect (OIDC) for authentication.
2. We have the SaaS Application's authentication Redirect URL (aka Callback URL) and have rights to configure its OIDC settings.

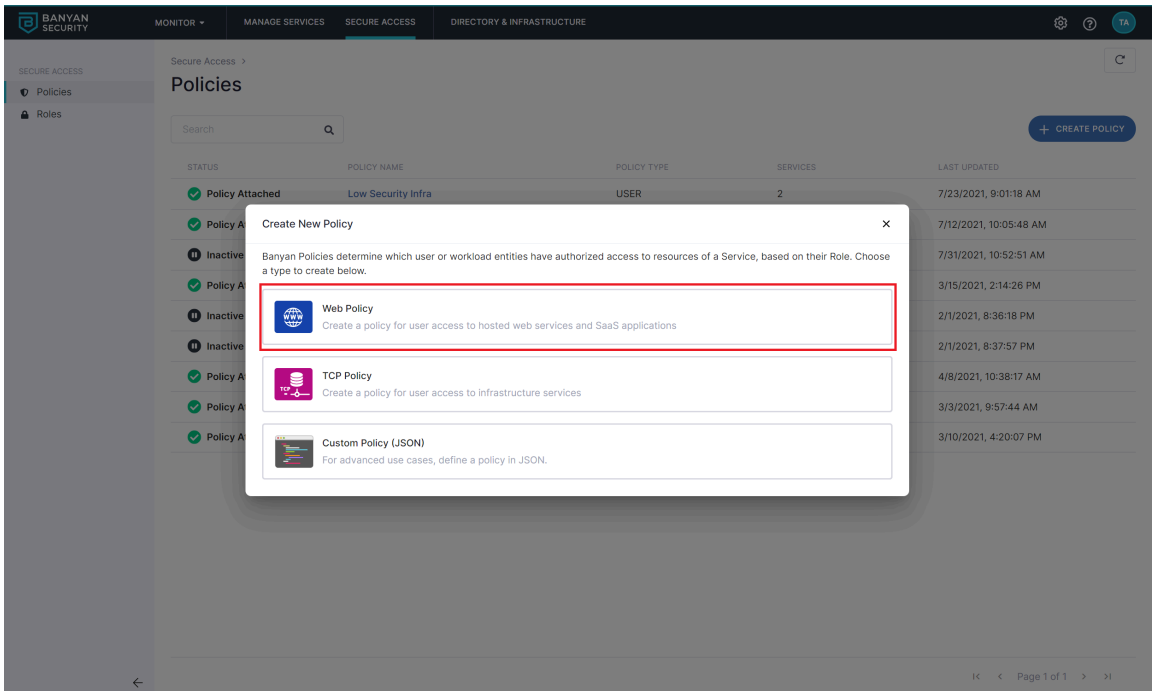
Note: CSE is NOT a primary Identity Provider; instead the Banyan TrustProvider component federates to your organization's Identity Provider upon every login. CSE then evaluates security posture against access policies.

Steps

We will add a security policy to the SaaS Application in 4 steps.

Step 1. Create a Policy for SaaS App Access

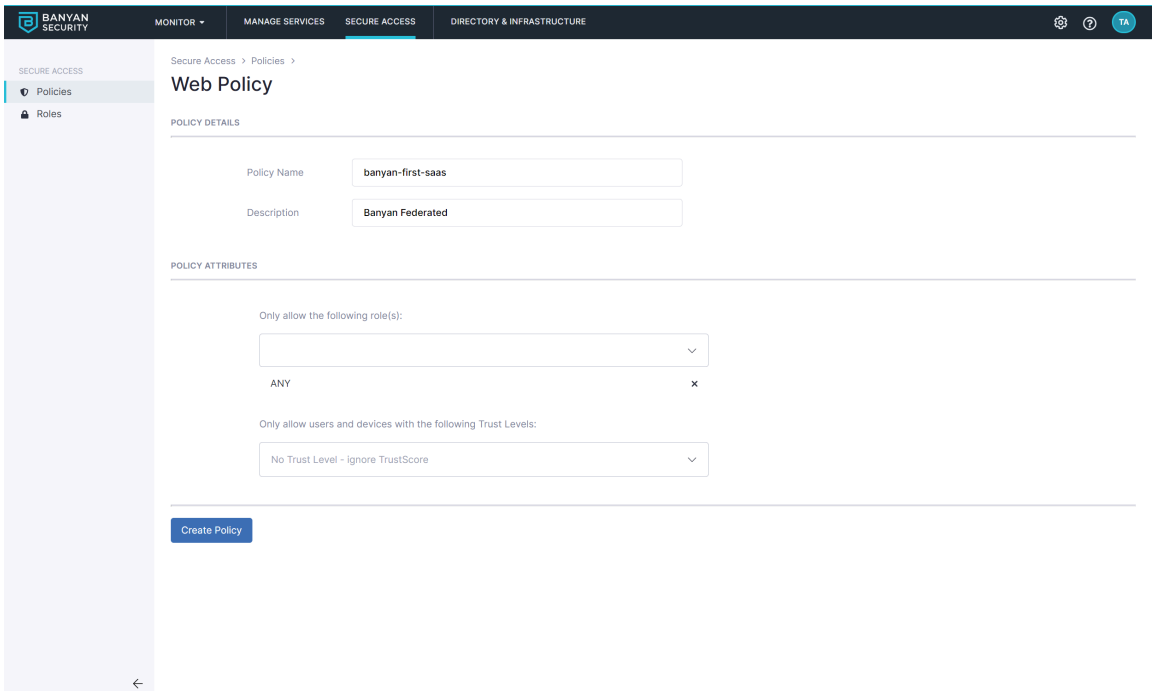
1.1 Navigate to **Private Access** > **Access Policies**, and select **+ Create Policy**. Then select the **Web Policy** template.



1.2 Name the policy `quickstart-user-saas`.

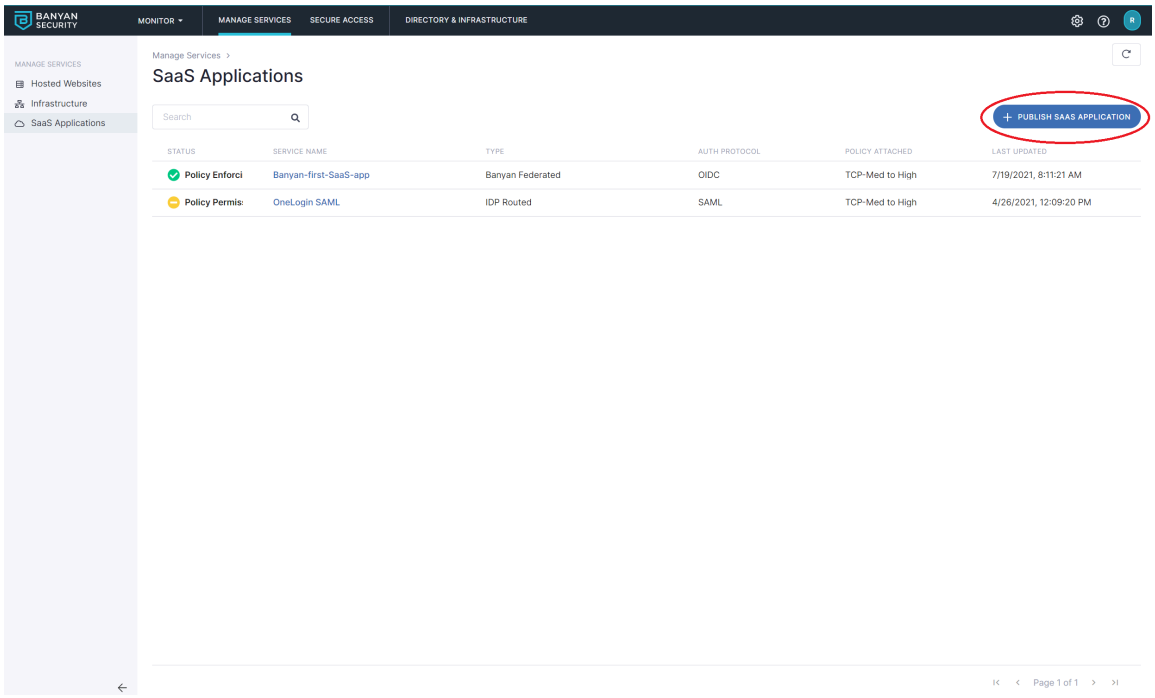
Also set the policy attributes for minimal controls:

- Only allow access from the following role: **ANY**
- Only allow users and devices with the following Trust Levels: **No Trust Level - ignore TrustScore**

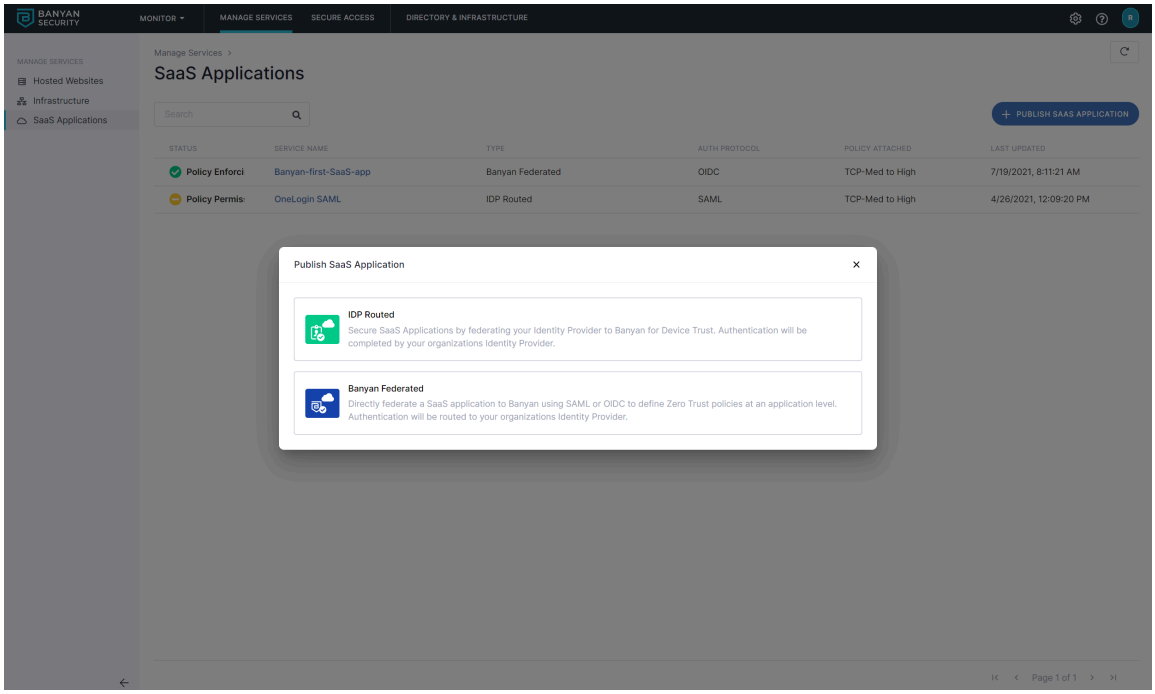


Step 2. Create the SaaS Application

2.1 Navigate from **Internet Access** > **SaaS Apps**, and then select **+ Publish SaaS Application**.



2.2 Select `Banyan Federated` to route to CSE first.

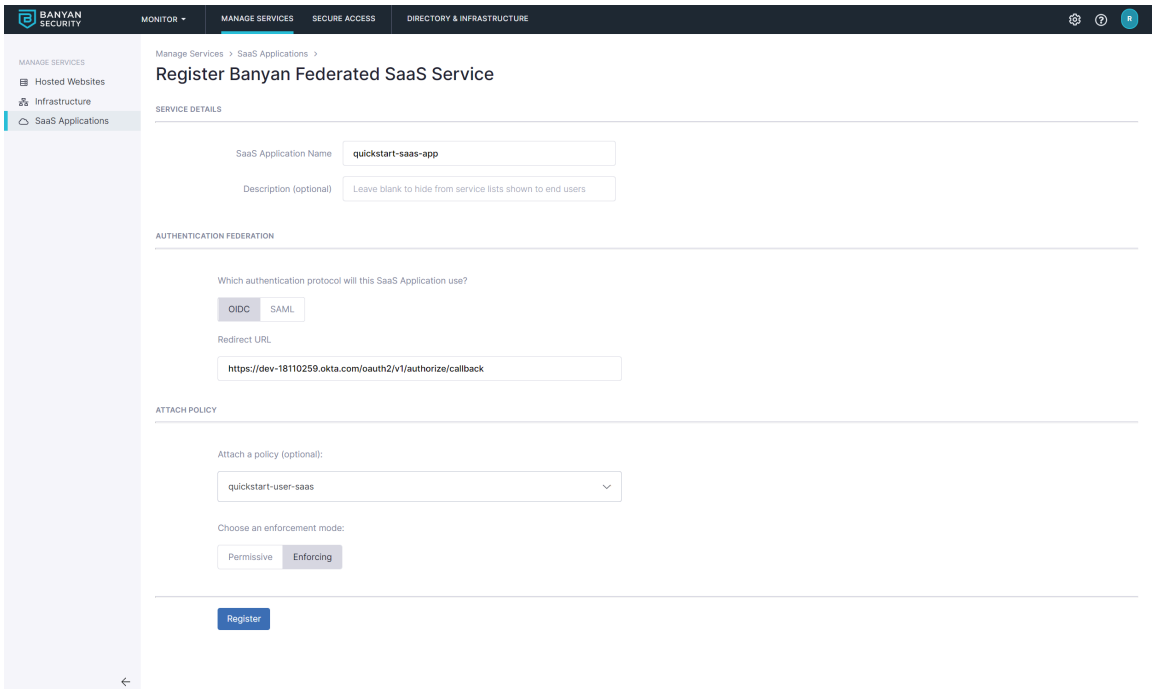


2.3 Name the SaaS App `quickstart-saas-app` and set the attributes:

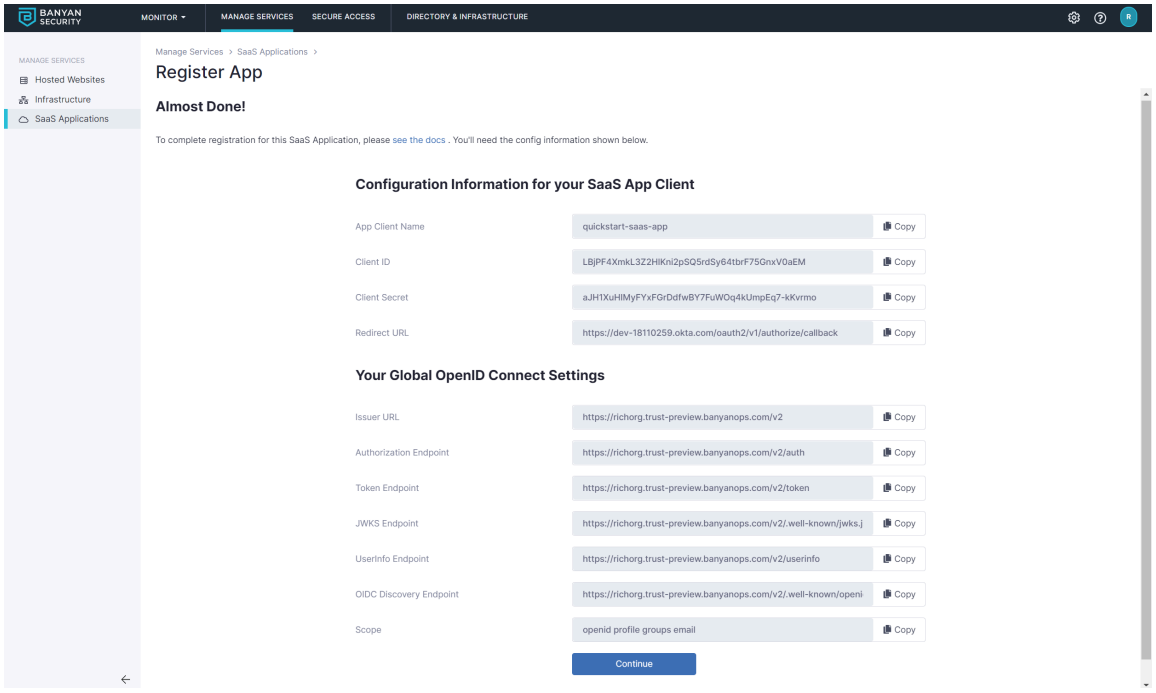
- select the authentication protocol to be `OIDC`
- set the `Redirect URL` to the well-known Redirect URL provided by the SaaS application you are securing

You can also configure device policies on SAML-enabled SaaS Applications.

2.4 Attach the `quickstart-user-saas` policy we had previously created and set enforcement mode to `Enforcing`.

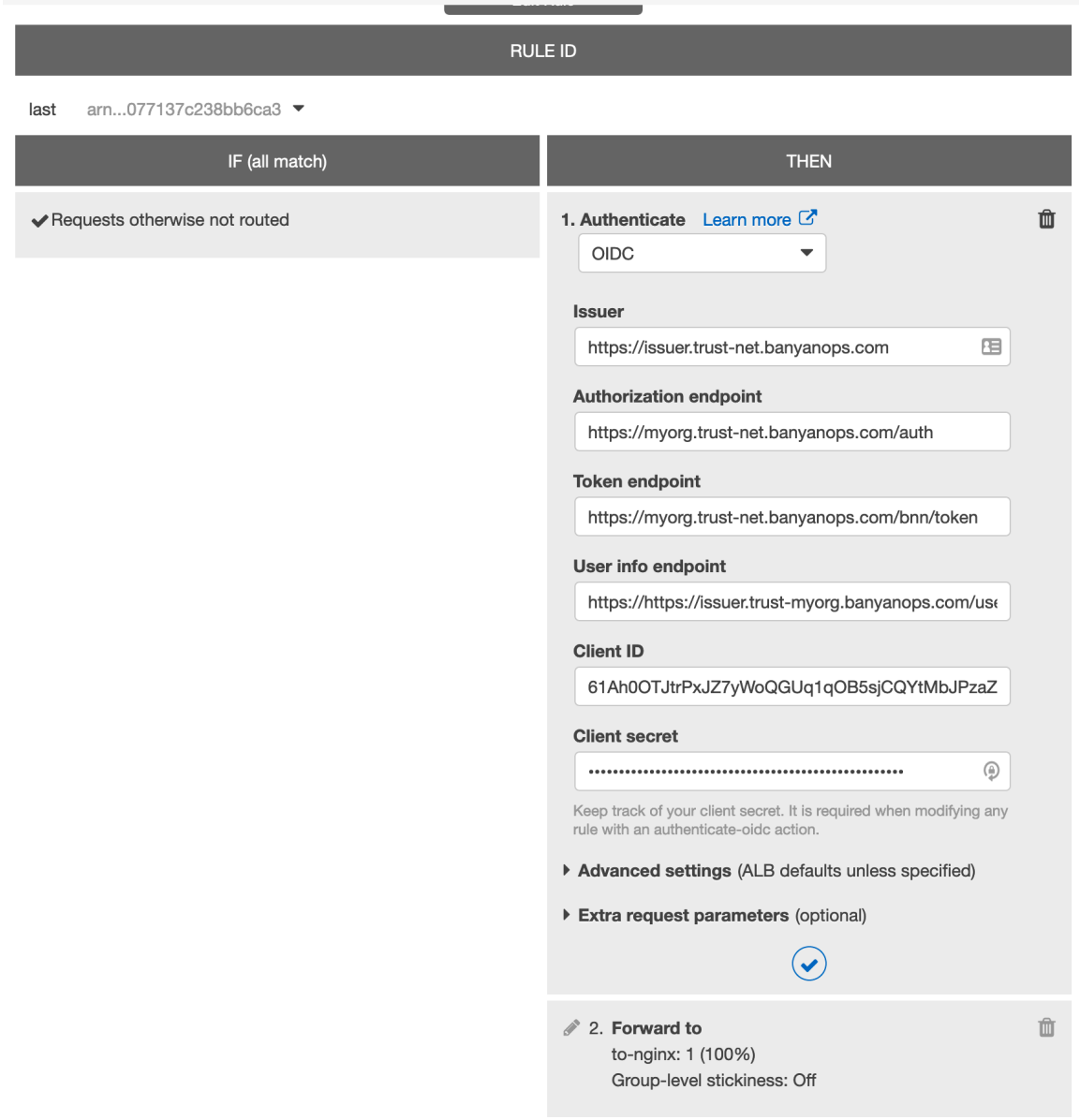


2.5 Select **Register**. The next screen will give you the details you need to enter into your SaaS app.



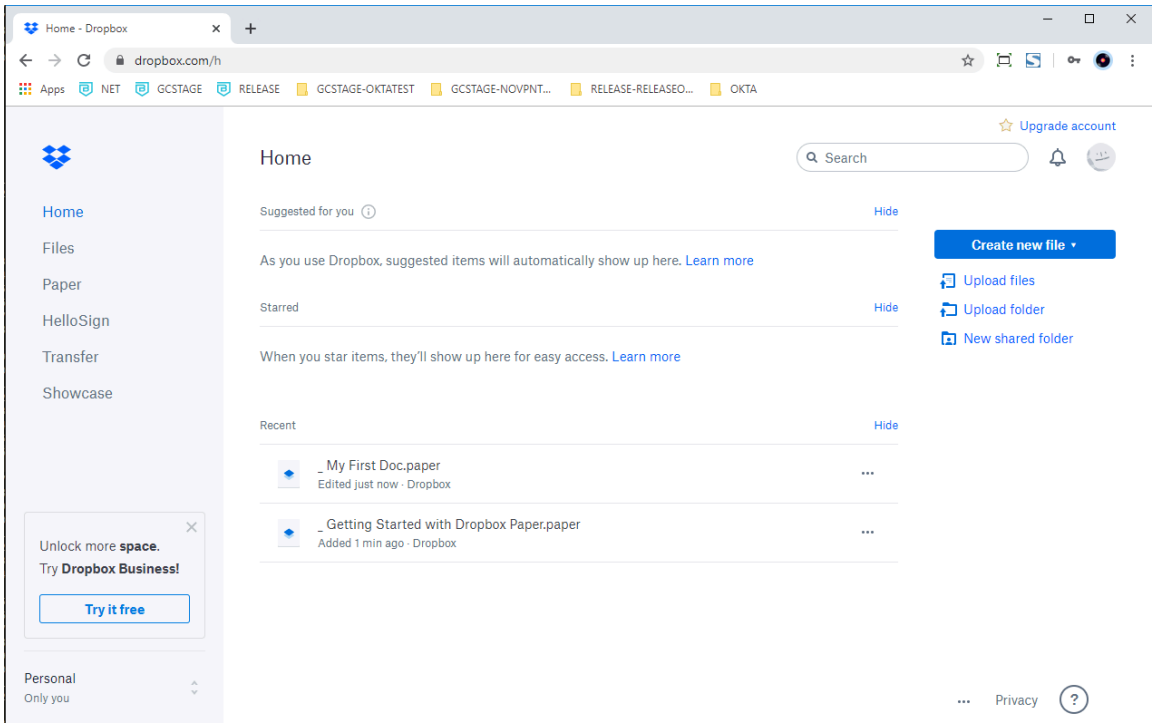
Step 3. Configure your OIDC-enabled SaaS app to use CSE for authentication

3.1 Fill in the data from the Command Center for the SaaS app you are securing.



Step 4. Navigate to the SaaS app and login in via OIDC

4.1 Now, you can navigate to your SaaS app and authenticate. You will be taken to your Identity Provider to login while, behind the scenes, CSE is evaluate device posture and enforcing your security policies.



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

- Concepts
- Components
- Release Notes

Guides

- Quick Start Guides
- Solutions
- Feature Guides
- API Guide