Use IDP Federation to enforce zero trust policies on all SaaS Applications integrated with Okta

Use federation capabilities in Okta to enforce Cloud Secure Edge (CSE) policies on and enable Passwordless for your SaaS apps

Updated on 15 minutes to read Contributors  

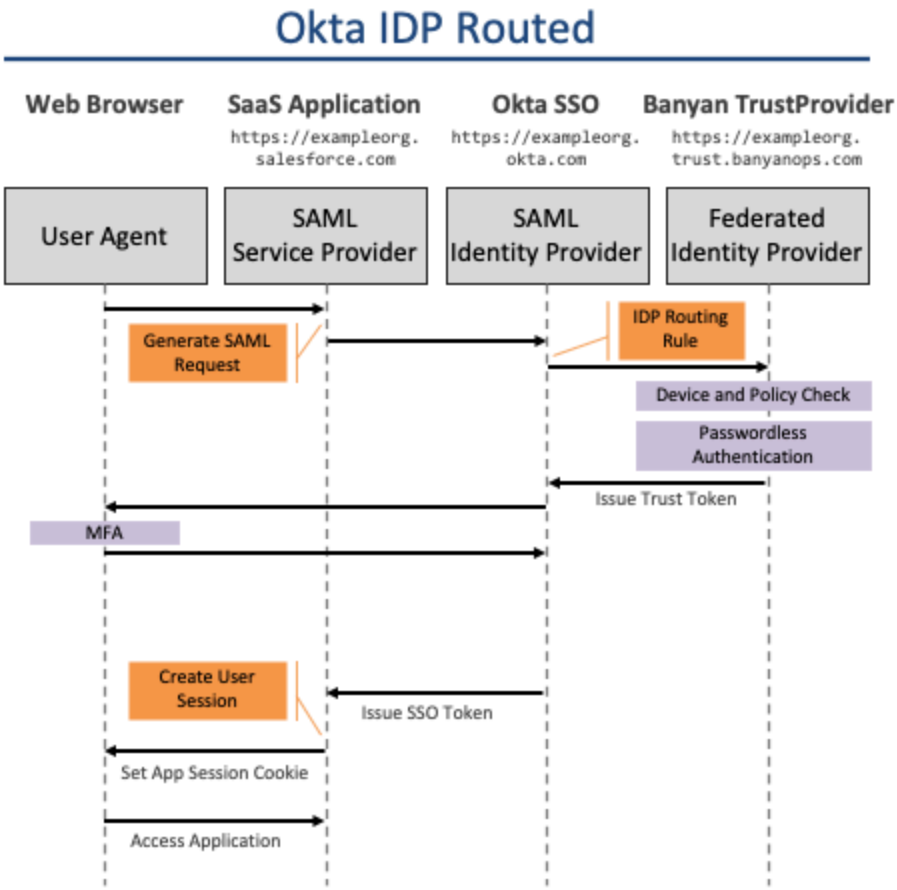
ON THIS PAGE:

Overview
How It Works
Prerequisites
Steps
1. Create a SaaS Application in CSE
2. Add CSE as an Identity Provider in Okta
3. Add a CSE Fallback Routing Rule
4. (Optional) Route Specific Okta Applications to CSE
5. Route All Applications and the Okta Dashboard to CSE
Additional Configurations
Enable Passwordless
Phased Roll out Solution Guide
Exempting Specific Users from CSE Policies
Exempting Non-SaaS Applications from Passwordless
IDP-based Sign On Policy

Overview

This guide details the steps required to set up Okta with SonicWall Cloud Secure Edge (CSE) to enable policy enforcement and Passwordless authentication for any SaaS app.

How It Works



In the IDP-routed authentication flow, you configure your Okta to federate authentication requests to CSE. CSE provides policy enforcement and can also perform Passwordless authentication.

Prerequisites

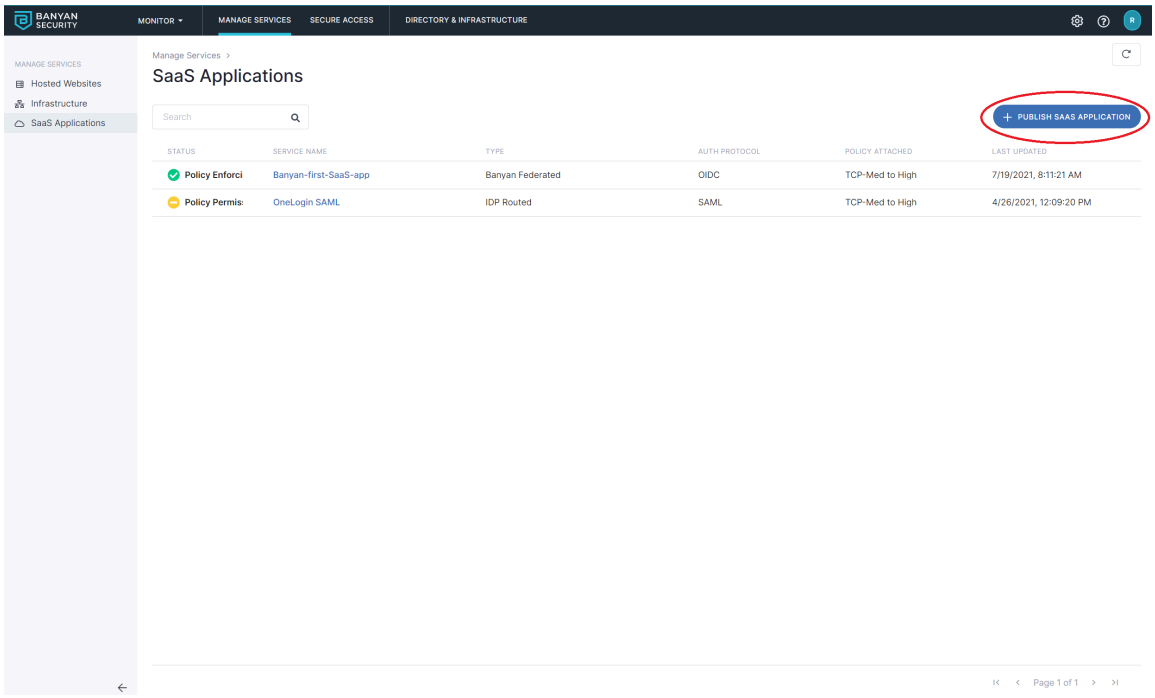
- Configure Okta for CSE Service Access to create a directory of users for accessing CSE services
- Configure Okta for CSE Device Registration to enable device registration with Okta

Steps

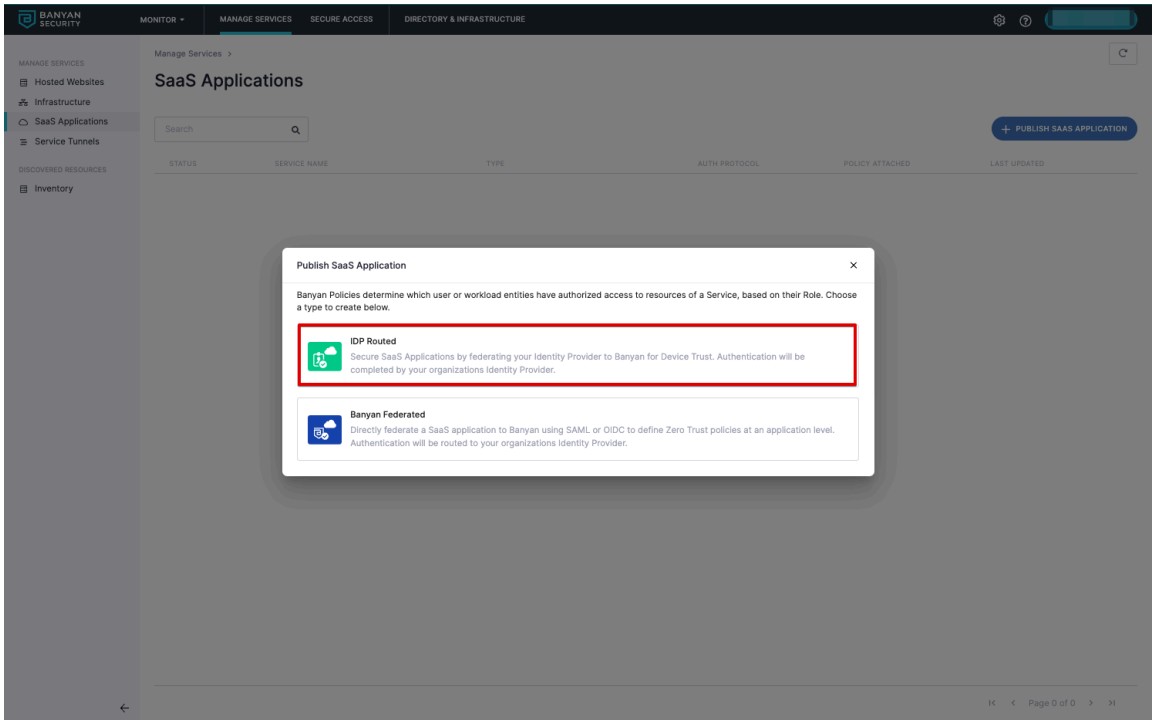
1. Create a SaaS Application in CSE

> Organizations can create one IDP Routed SaaS App for all Okta applications or create multiple IDP Routed SaaS apps for groups of applications such as High Security vs Medium Security.

1.1 Navigate from **Private Access** > **Access Policies** > **+ Create Policy**, and then select **Web Policy**.

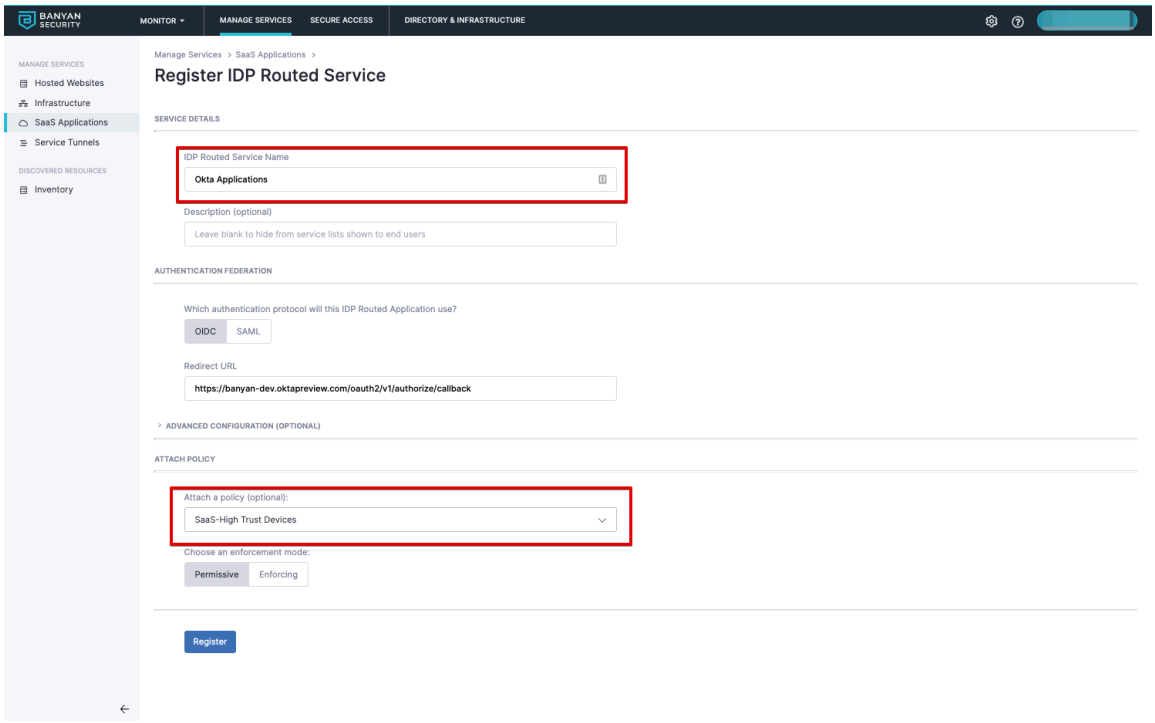


1.2 Select `IDP Routed` for Okta to route to CSE.



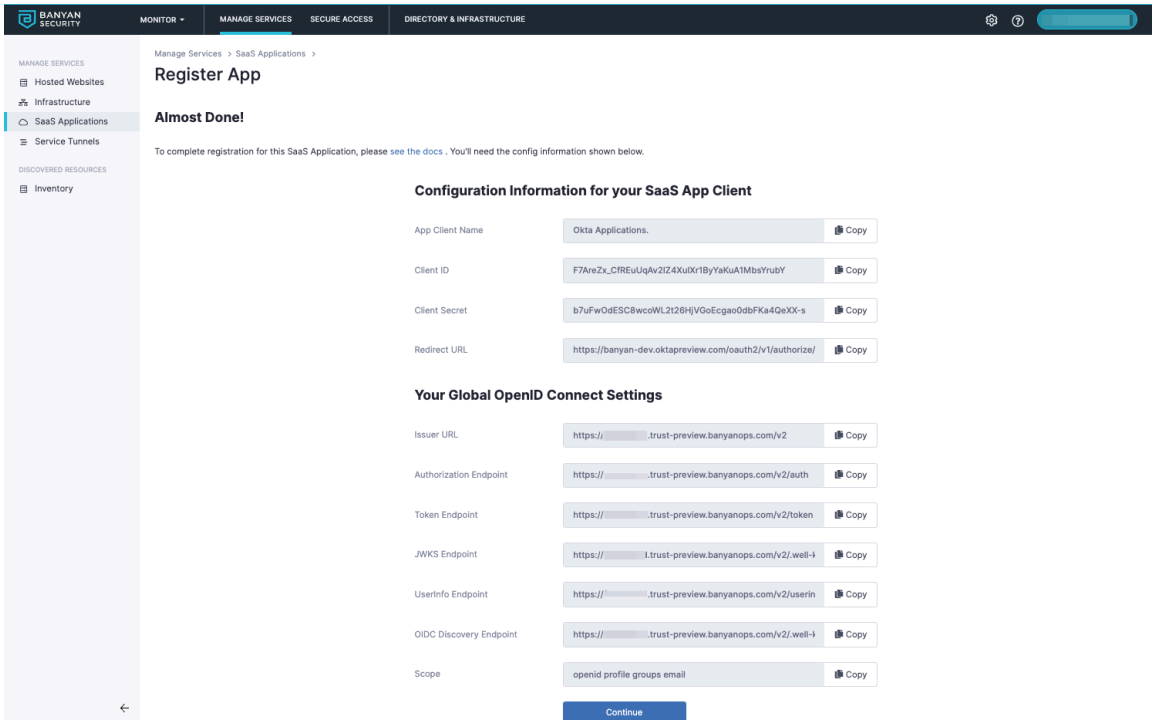
1.3 Name the SaaS app and verify the IDP redirect URL.

1.4 Attach a web policy and set enforcement mode.



1.5 Register.

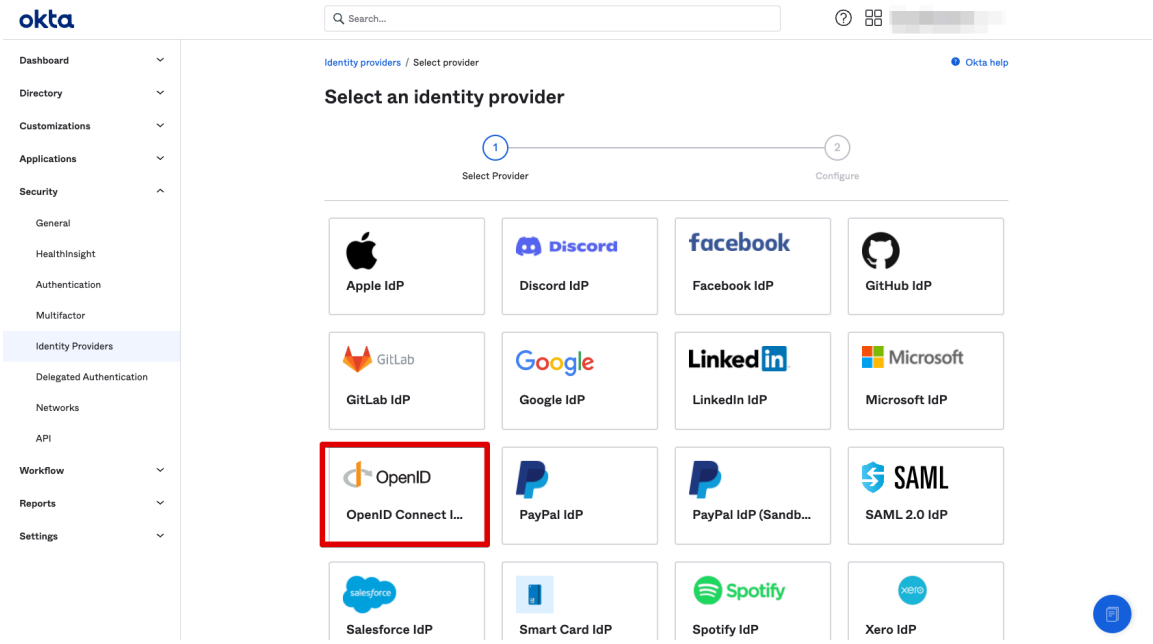
The next screen will give you the details you need to set up Okta to use CSE to enforce your policies.



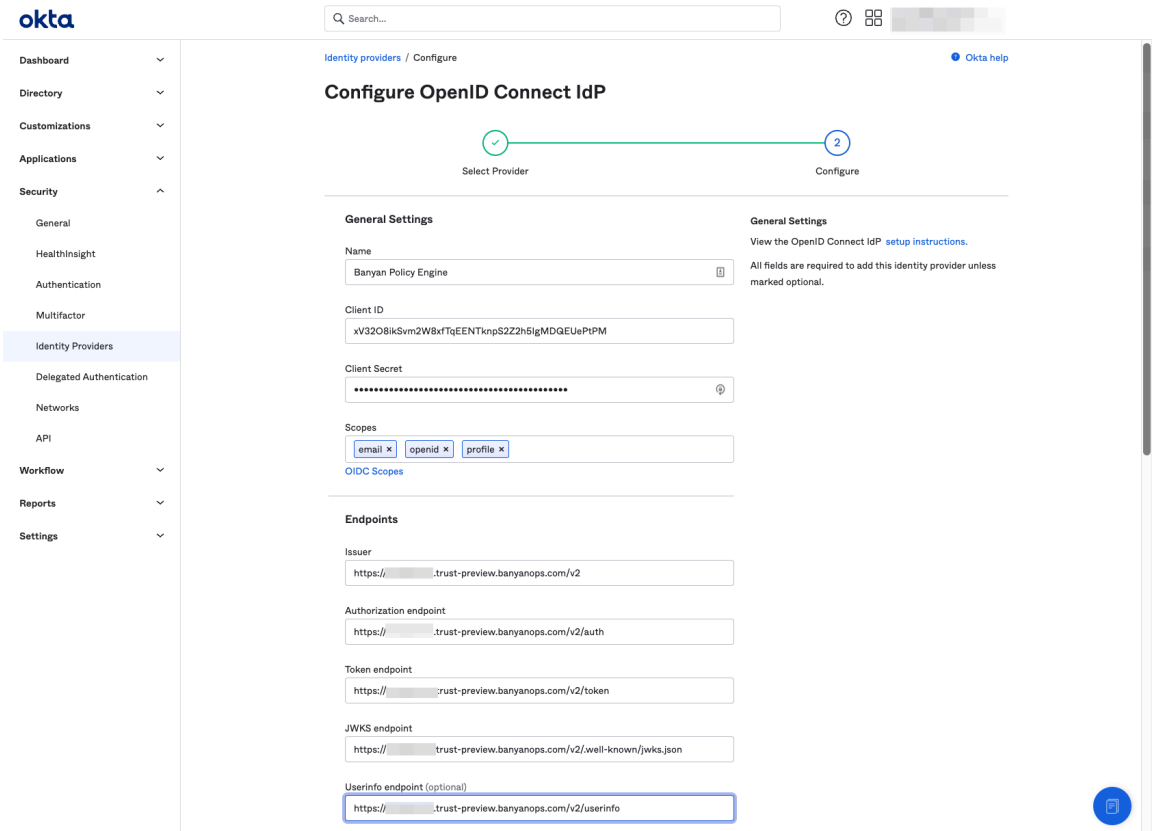
2. Add CSE as an Identity Provider in Okta

2.1 Navigate from **Security** > **Identity Providers**, and then select **Add Identity Provider**.

2.2 Select `Add OpenID Connect IdP` and select **Next**.



2.3 Name the Identity Provider **CSE Policy Engine** and enter the config field values you obtained in **Step 2.5** above.



3. Add a CSE Fallback Routing Rule

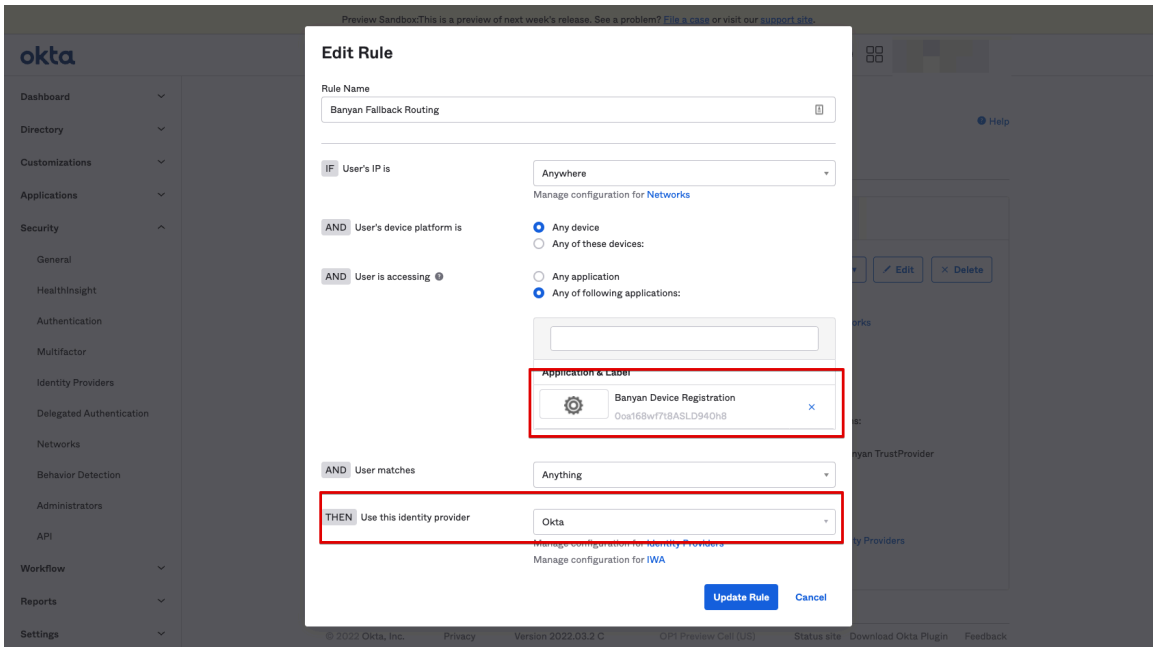
Since all Okta authentication traffic can eventually be federated, you need to ensure that flows involving the CSE Device Registration App Integration bypass federation so that users are not forced into infinite redirect loops.

3.1 Navigate from **Security** > **Identity Providers** > **Routing Rules**.

3.2 Add a Routing Rule called **CSE Fallback Routing**.

3.3 Select the **CSE Device Registration** SaaS Application.

3.4 Select **Okta** as the identity provider.



3.5 Ensure the routing rule has been activated.

4. (Optional) Route Specific Okta Applications to CSE

This step will only protect **SP-initiated** flows for certain selected applications and not flows that start from the Okta dashboard. Routing specific applications is recommended for testing and as part of a broader phased roll out.

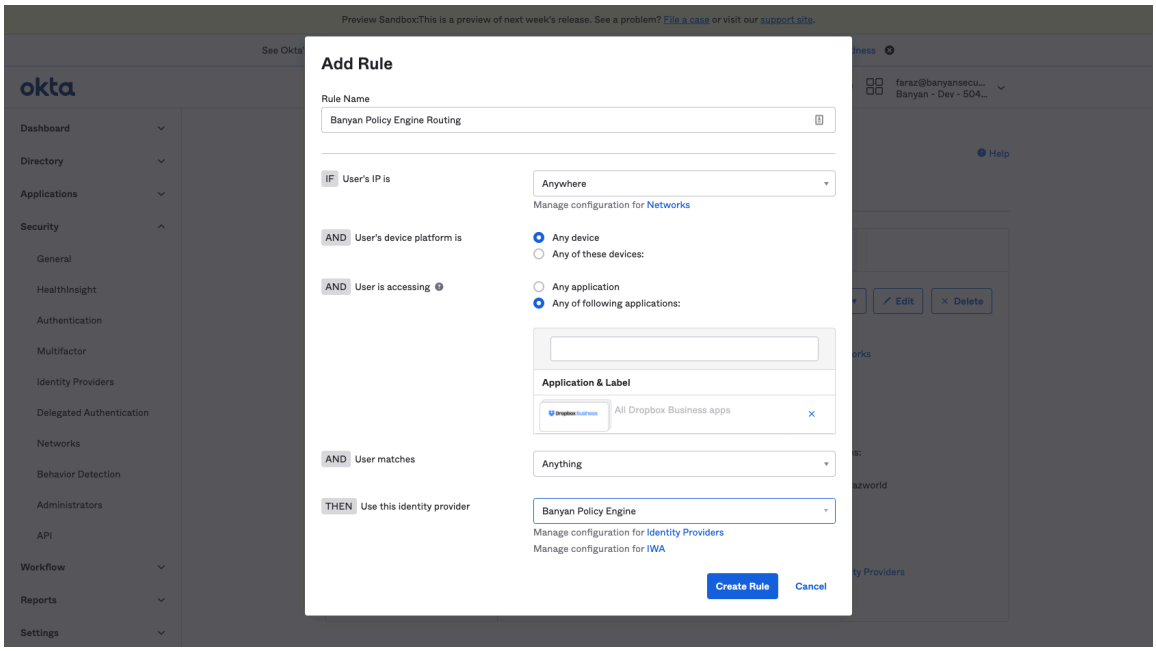
4.1 Navigate from **Security** > **Identity Providers** > **Routing Rules**.

4.2 Add a routing rule called **CSE Policy Engine Routing**, and select the SaaS applications that you wish to secure with CSE Policies.

4.3 Select the **CSE Policy Engine** identity provider you created in **Step 3**.

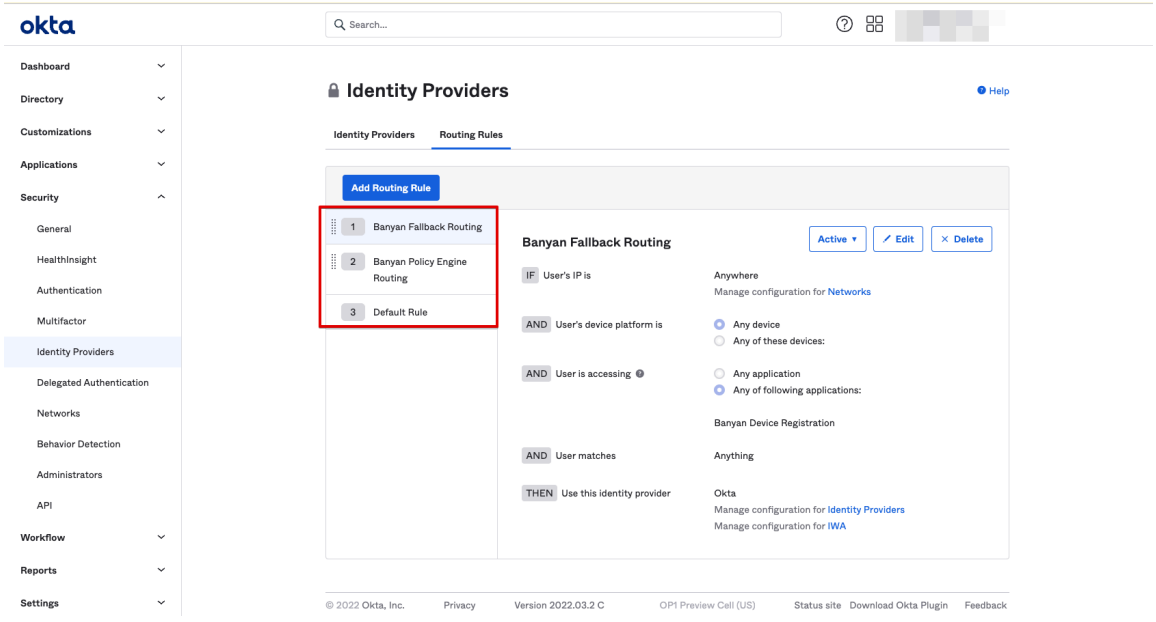
4.4 Select the specific applications that you wish to secure with CSE.

Warning Do not select “Any application” when you set up the routing rule here until you are ready to Route All Applications and the Okta Dashboard to CSE



4.5 Ensure that the routing rule has been activated.

Now, specific SaaS application traffic is routed to CSE for policy enforcement. A summary of your Okta Routing Rules is as follows:



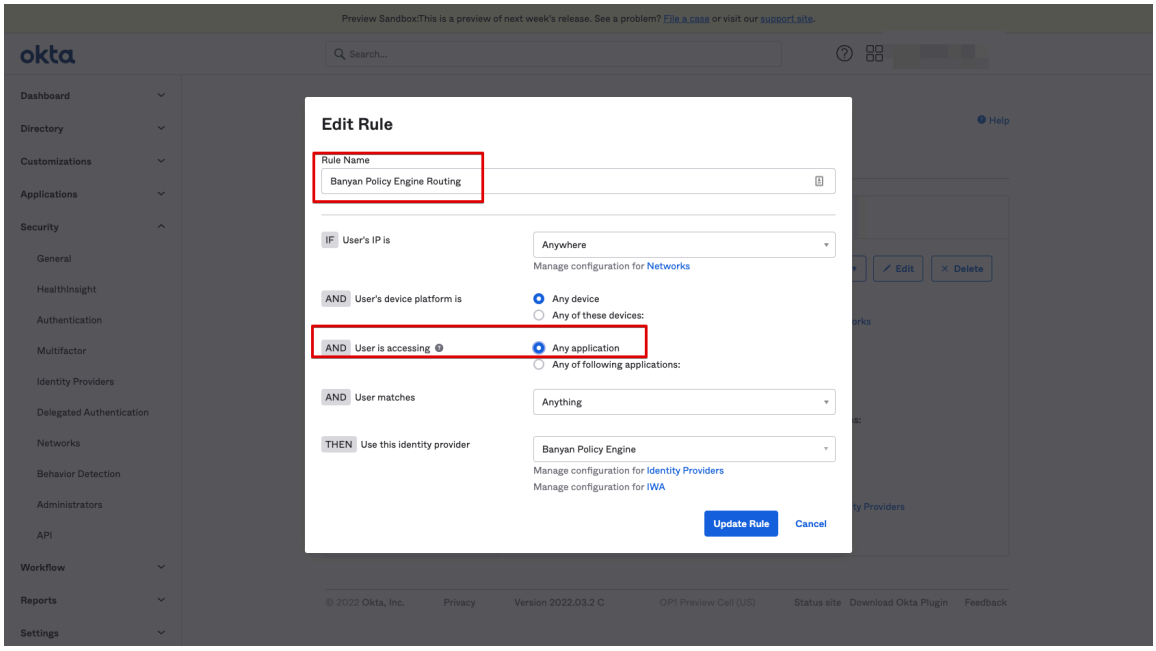
Routing Rule	Applications to Route	IDP to Route to
1. CSE Fallback Routing	CSE Device Registration Provider	Okta
2. CSE Policy Engine Routing	Any Application	CSE Policy Engine
3. Default Rule	Any Application	Okta

5. Route All Applications and the Okta Dashboard to CSE

5.1 Confirm CSE Web Policy attributes

```
- A policy in **enforcement** will not allow any fallback for devices that don't meet trus
- A policy in **permissive** will allow for a fallback for users that are not registered.
```

5.2 Update the **CSE Policy Engine Routing Rule** to route all application traffic.



Now, all Okta authentication traffic is routed to CSE for policy enforcement. A summary of your Okta Routing Rules is as follows:

Routing Rule	Applications to Route	IDP to Route to
1. CSE Fallback Routing	CSE Device Registration Provider	Okta
2. CSE Policy Engine Routing	Any Application	CSE Policy Engine
3. Default Rule	Any Application	Okta

Additional Configurations

Enable Passwordless

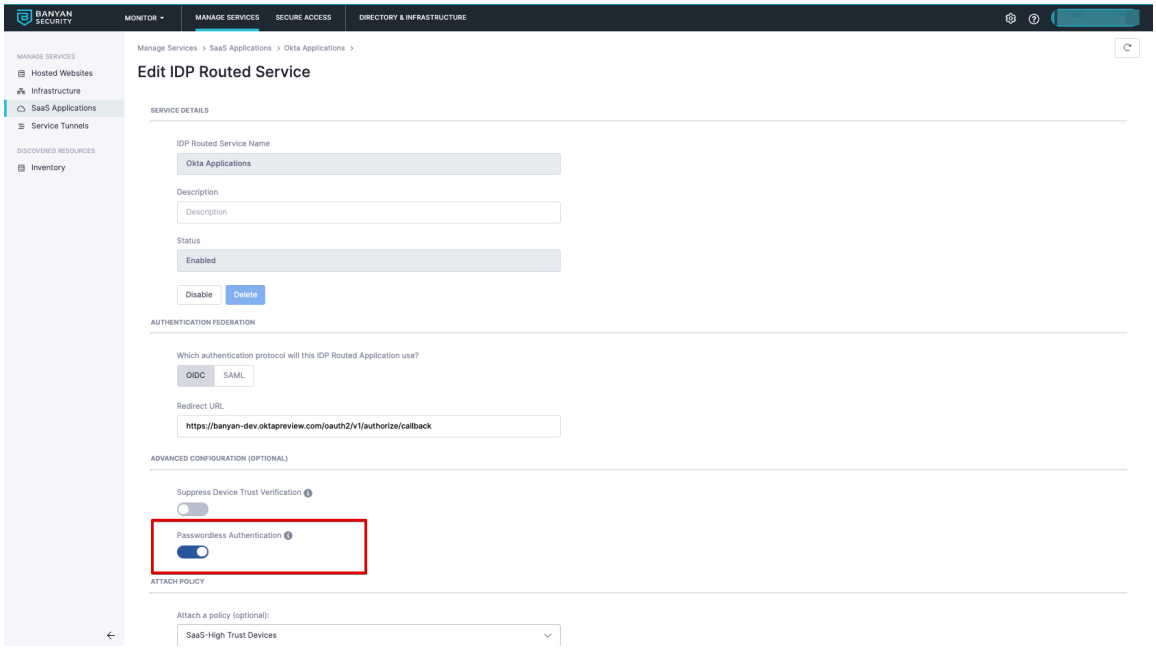
Passwordless is recommended to provide an optimal user experience when accessing applications on CSE registered devices. If Passwordless is not enabled, end users will default to Okta's authentication methods.

Passwordless authentication with CSE leverages the fact that the trusted Device Certificate includes the user's email address in the `UserPrincipalName` SAN extension field.

When Passwordless is enabled, the device certificate that is presented during device trust will be used to extract the user who is attempting to authenticate. The identified user will be issued a TrustToken without requiring username and password. The user will then proceed with Okta's authentication configurations for the user selected application

1. Edit the existing Okta SaaS app.

2. Enable **Passwordless Authentication**.



Phased Roll out Solution Guide

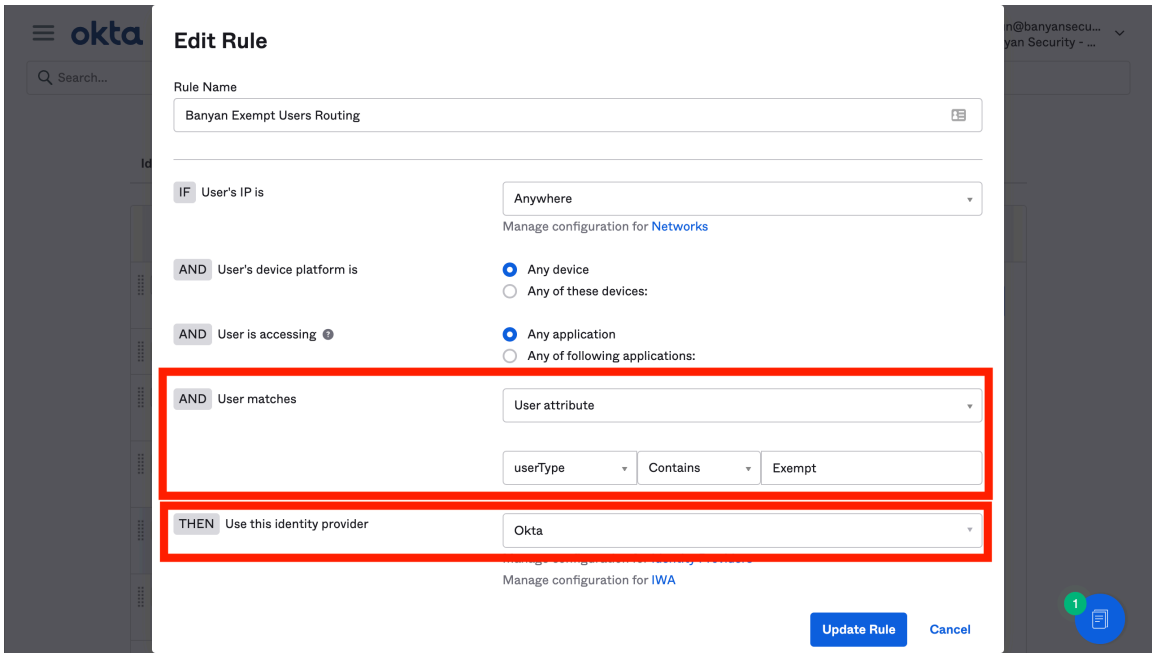
Admins typically need to phase the roll-out of CSE device policies for Okta applications. CSE provides 2 capabilities that support a phased roll out - (1) support for unregistered devices and (2) the ability to set up policies in permissive mode.

Review a prescriptive roll-out process in our Solution Guide on enforcing device trust for Okta applications so you can get visibility into how your CSE rollout is progressing without blocking users and devices immediately.

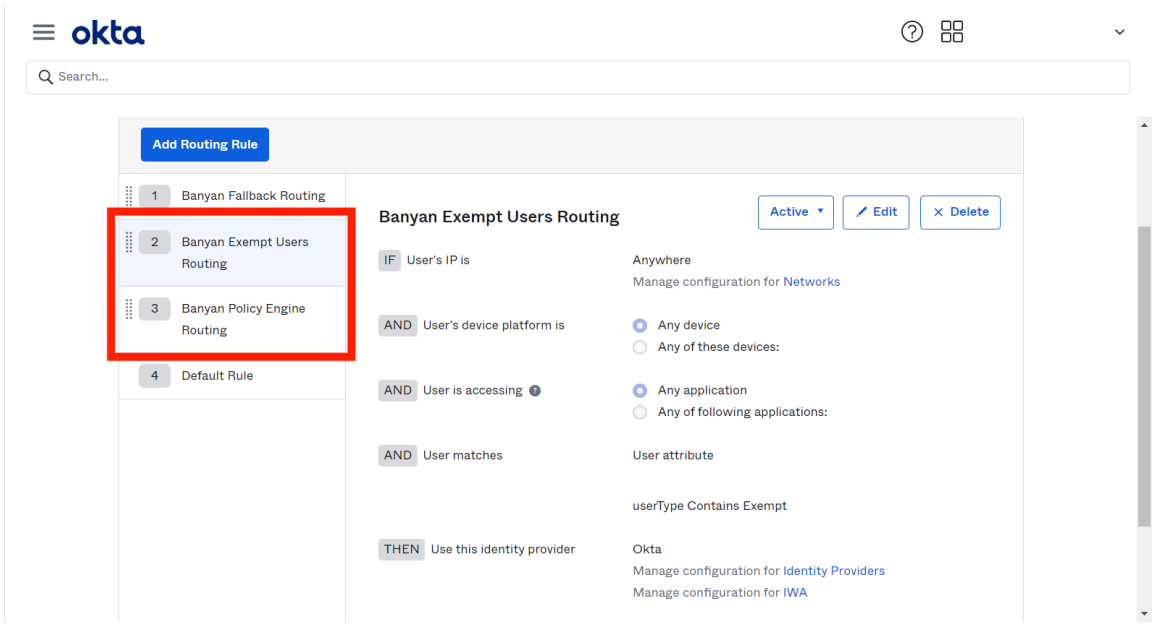
Exempting Specific Users from CSE Policies

In the setup above, all users will get routed to CSE for policy enforcement. You can use leverage the same Okta Routing Rules to exempt specific types of users from CSE policies. We recommend using a user's login attributes (not network zones via Source IP address matching or device platform via browser sniffing) to exempt users.

1. Add a routing rule called **CSE Exempt Users Routing**, and set the match rules based on the attributes of the users to exempt. Select **Okta** as the identity provider.



2. Place this routing rule **above** the **CSE Policy Engine Routing** rule



The summary of your Okta Routing Rules is then as follows:

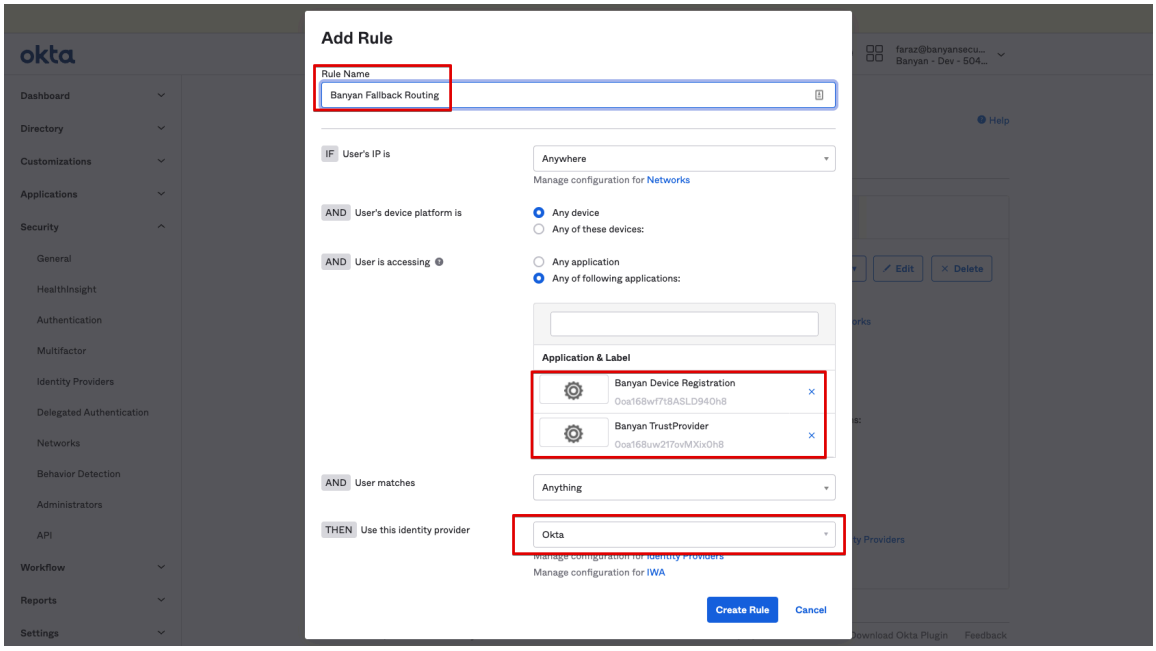
Routing Rule	Applications to Route	IDP to Route to
1. CSE Fallback Routing	CSE Device Registration Provider	Okta
2. CSE Exempt Users Routing	Any Application	Okta
3. CSE Policy Engine Routing	Any Application	CSE Policy Engine
4. Default Rule	Any Application	Okta

Exempting Non-SaaS Applications from Passwordless

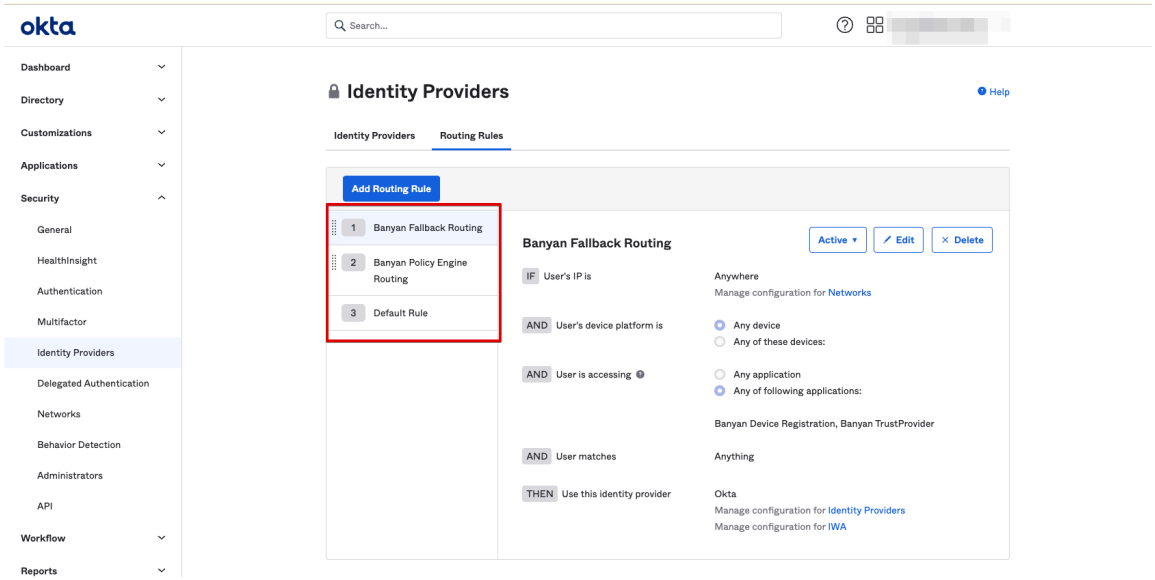
By default, enabling passwordless for Okta will apply to all CSE service access flows. To exempt Hosted Websites and CSE app authentication for Infrastructure Services and Service Tunnels from leveraging passwordless, complete the following steps:

1. Edit the **CSE Fallback Routing** rule in Okta

2. Add the **CSE TrustProvider** application to the rule and **Save**.



Now, all Hosted Websites and CSE app authentication for Infrastructure Services and Service Tunnels will not go through CSE Passwordless and leverage Okta for authentication. A summary of your Okta Routing Rules is as follows:



Routing Rule	Applications to Route	IDP to Route to
1. CSE Fallback Routing	CSE Device Registration Provider, CSE TrustProvider	Okta
2. CSE Policy Engine Routing	Any Application	CSE Policy Engine
3. Default Rule	Any Application	Okta

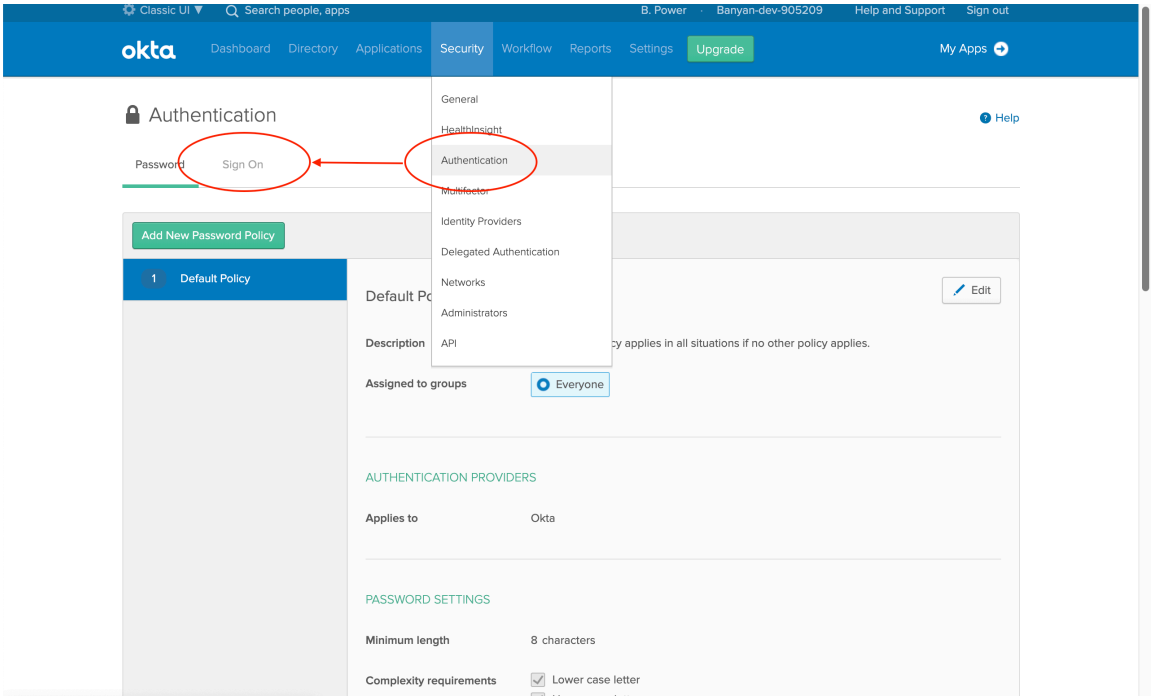
IDP-based Sign On Policy

When using Authentication Sign On rules (specifically MFA) in Okta, and when using third-party IDP and routing rules for SaaS applications, Okta creates an MFA challenge for each IDP in the authentication chain. This results in end users being prompted twice for MFA challenges.

To avoid this undesired end user experience, Okta has a feature (available in early access) that allows the Okta admin to specify which IDP the Authentication Sign On rule(s) will apply to, such as “Okta”.

To configure this early access feature:

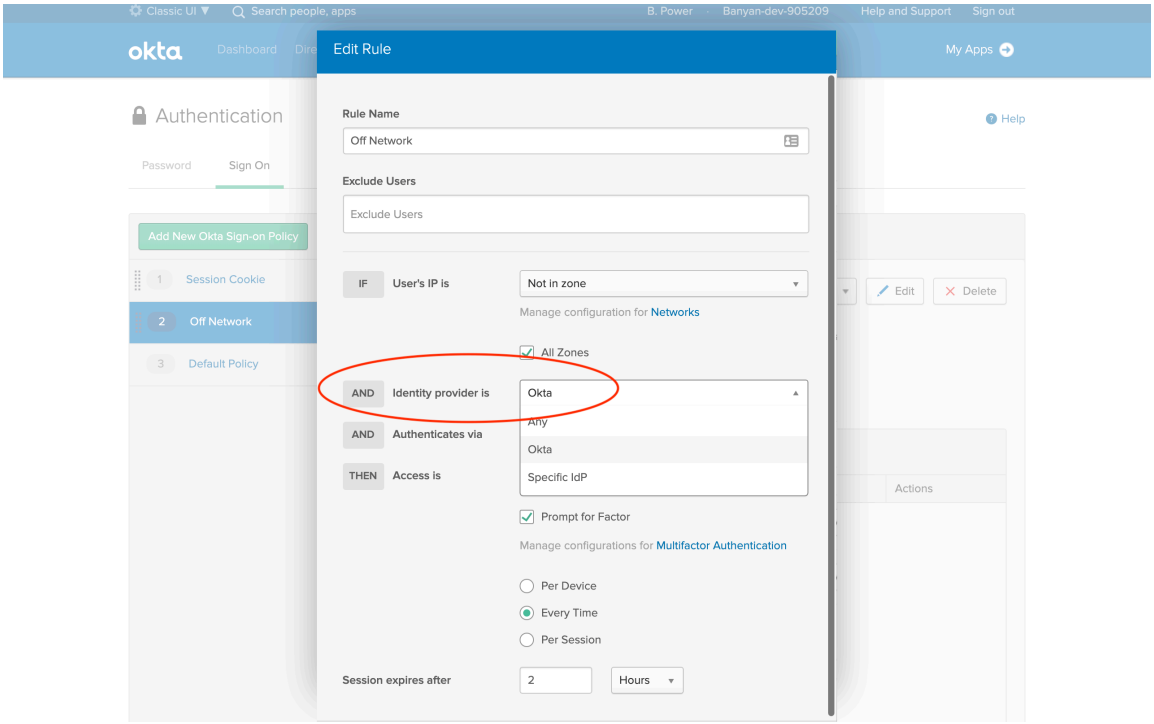
1. Navigate from **Security** > **Authentication** > **Sign On**.



2. Edit an existing sign-on policy, and then add a new rule.

3. Locate the field **AND Identity Provider**, and then select **Okta**.

> If you do not see the `AND Identity Provider` option, you’ll need to file a ticket to Okta Support to “Enable feature - IdP-based sign on policy”. Okta Support will typically enable this feature for you within a few hours.



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts

Components

Release Notes

Guides

Quick Start Guides

Solutions

Feature Guides

API Guide