IDP Routed SaaS Applications

Use IDP routing capabilities in your Identity Provider to enforce Cloud Secure Edge Policies on your SaaS applications

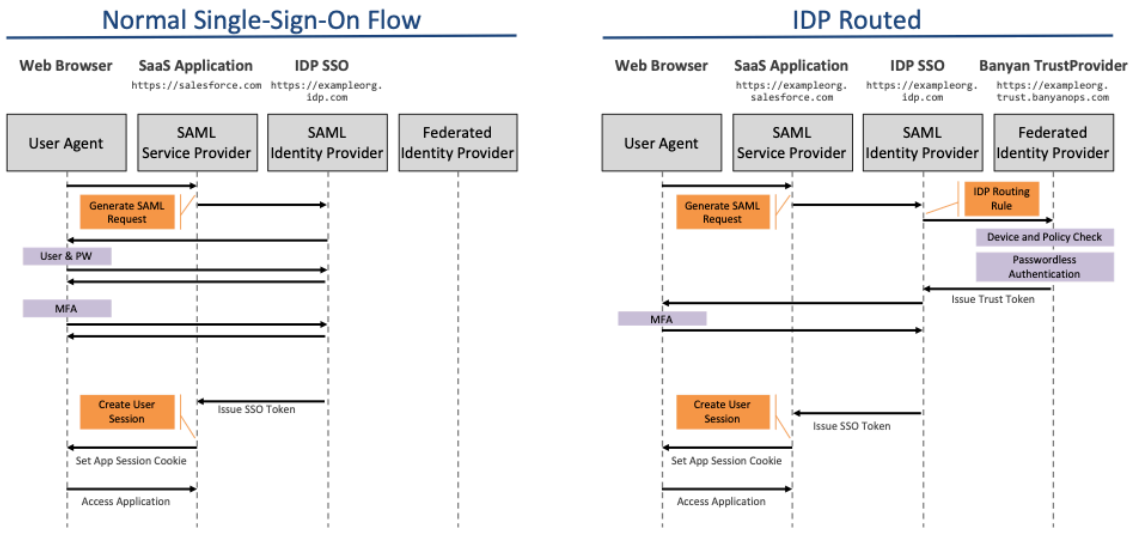
Updated on

ON THIS PAGE:

This topic details *IDP Routed* authetication to secure your SaaS apps; in this technique, the SaaS Application is configured for SAML/OIDC authentication using your Identity Provider and your Identity Provider is configured to federate to Banyan's TrustProvider component. Zero Trust policies are defined for groups of SaaS applications you route via IDP Federation logic. You can also configure CSE-federated authentication to secure your SaaS apps.

How It Works

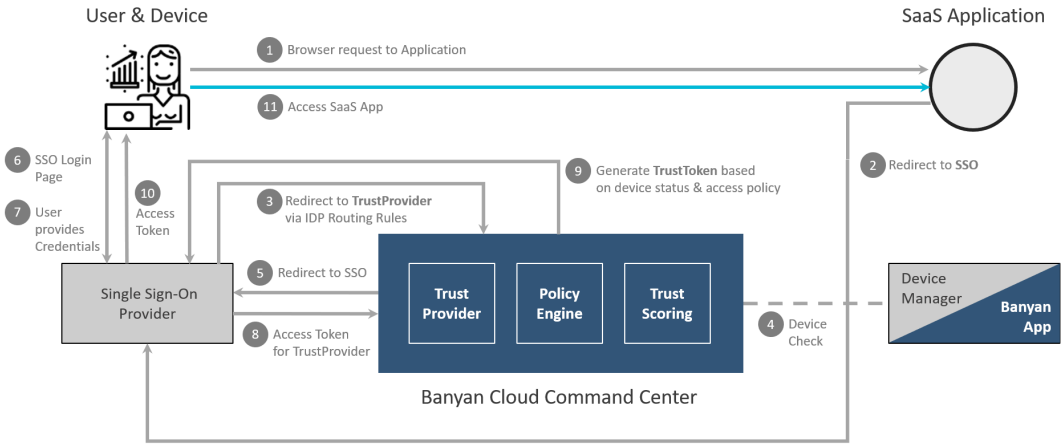
The diagram below provides a conceptual overview of how you can use Cloud Secure Edge (CSE) via Identity Federation for Device Policies on SaaS Apps.



In the Normal Single-Sign-On flow, your SaaS application redirects to your Identity Provider to authenticate the user.

In the IDP-first authentication flow, you configure your Identity Provider to federate authentication requests to Cloud Secure Edge's TrustProvider component. Since the Cloud Secure Edge (CSE) is now in the authentication flow, it is able to enforce zero-trust security policy.

The step-by-step flow is detailed in the diagram below:



Identity Provider Setup Guides

- Okta
- Azure AD
- OneLogin

SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts
Components
Release Notes

Guides

Quick Start Guides
Solutions
Feature Guides

API Guide