Enforce Zero Trust Security Policies for Public Applications integrated with Okta

Updated on

This section describes how to enforce the Cloud Secure Edge's (CSE) zero-trust security policies for public applications integrated with Okta. If you're looking to configure CSE so your end-users can use Okta SSO to authenticate with CSE, go to the section on configuring your Okta IDP to manage your directory of users.

As described in the overview on securing public applications with CSE, CSE offers two techniques to provide zero-trust security for SaaS applications - **IP Allowlisting** and **Authentication Federation**. These techniques can be applied at your Identity Provider (IDP) or at the SaaS Application itself.

The follow article provide step-by-step directions to configure your Okta IDP to enforce zero-trust security policies via CSE:

- IP Allowlisting to enforce zero trust policies for specific SaaS Applications integrated with Okta
- IDP Federation to enforce zero trust policies on all SaaS Applications integrated with Okta

Site generated at YYYYMMDD

API Guide