



Search docs...

Ctrl + /

[Home](#) > [Public Applications](#) >

Enforce Zero Trust Security Policies for Public Applications integrated with OneLogin

Updated on

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

- [IP Allowlisting to enforce zero trust policies for specific SaaS Applications integrated with OneLogin](#)
- [IDP Federation to enforce zero trust policies on all SaaS Applications integrated with OneLogin](#)

SONICWALL[®]
CLOUD SECURE EDGE

© 2026. All rights reserved.

Site generated at YYYYMMDD

Links

[Concepts](#)

[Components](#)

[Release Notes](#)

Guides

[Quick Start Guides](#)

[Solutions](#)

[Feature Guides](#)

API Guide