

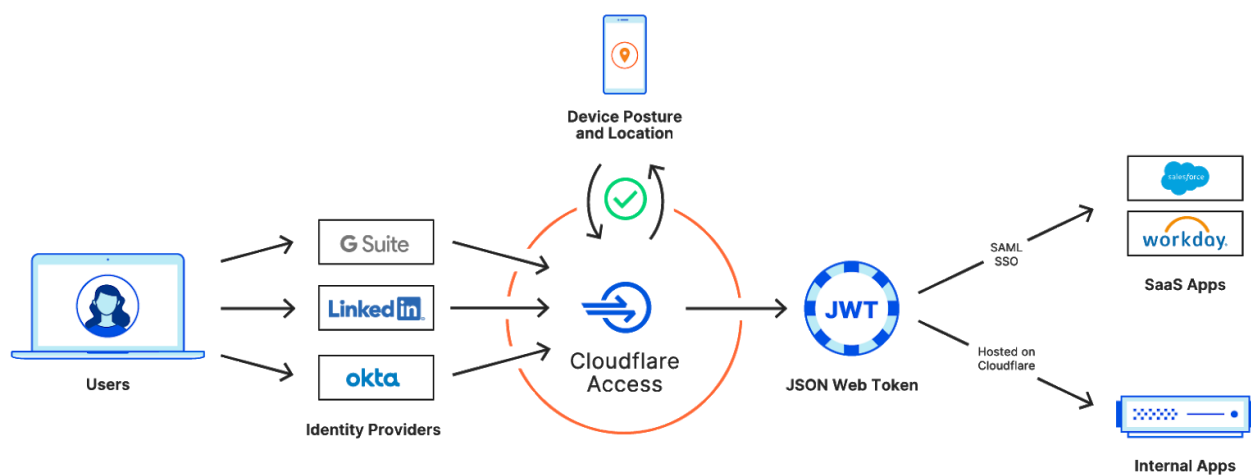
Cloudflare Access

Overview

Cloudflare Access is a zero trust access platform that runs on Cloudflare's global network edge in 200+ cities around the world. With Cloudflare Access, controlling access to your resources based on network location or IP address is no longer necessary. Every request to your applications is evaluated for user identity and device context, and you have the flexibility to aggregate multiple identity providers at once, allowing you to authenticate internal and external users securely without administrative headaches.

How Cloudflare Access works

Cloudflare Access is a zero trust platform that secures self-hosted and SaaS applications by aggregating sources of user identity and trust, and enforcing rules on every request or login. When administrators secure an application behind Access, any request to the hostname of that application stops at Cloudflare's network first. Once there, Cloudflare Access checks the request against the list of users who have permission to reach the application. Cloudflare Access can then apply additional rules to each login or integrate multiple SSO provider types.

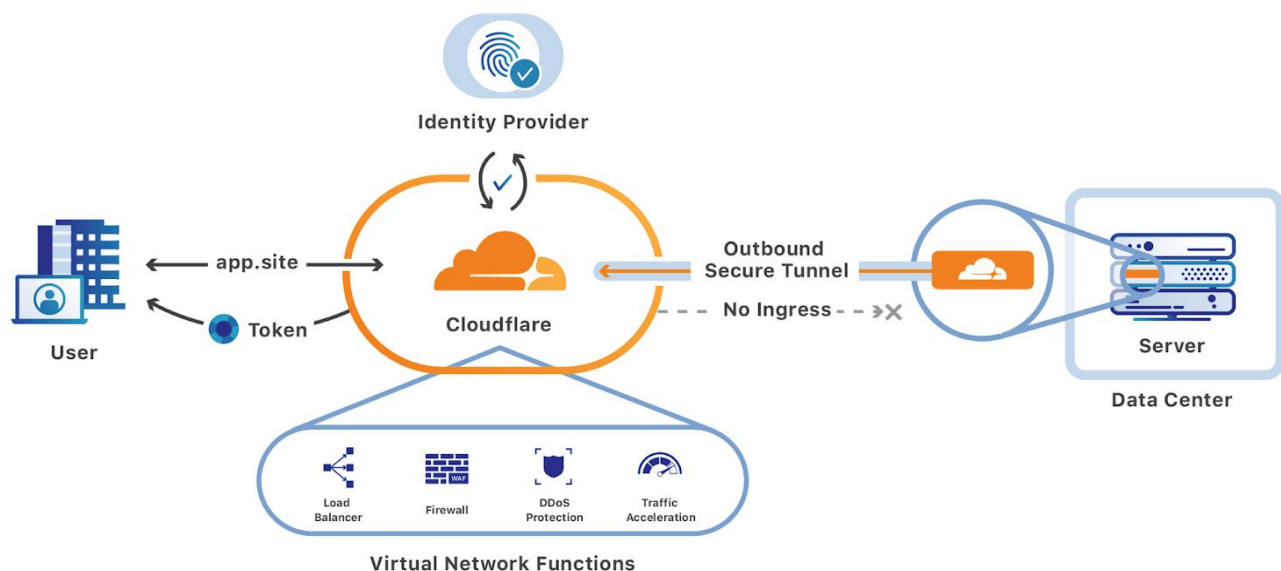


Authentication checks are performed at our edge network of 200+ data centers. This is much faster than, for instance, a VPN backhauling traffic to a home office.

Instead of configuring complex and error-prone network rules, IT teams build rules that enforce authentication using their identity provider. Security leaders control who can reach internal applications in a single pane of glass and audit comprehensive logs from one source.

Key integrations with Cloudflare for Teams

Cloudflare Access and Argo Tunnel connect internal tools to the Internet through a secure outbound connection, which runs in your infrastructure. This allows Cloudflare to protect your applications and machines and enables you to control user access to developer applications, staging sites, cloud infrastructure, and other resources.



Cloudflare Access also integrates with Cloudflare Gateway, a secure web gateway (SWG) that protects users, devices, and networks from threats on the Internet. Gateway allows administrators to log, inspect, and secure traffic from corporate devices and networks using a powerful policy engine.

With the shift to a user-centric network security model, Gateway and Access provide powerful tools to protect end user devices and enforce corporate security and acceptable use policies.

Get the most out of Cloudflare Access

Cloudflare Access allows you to set up policies and rules that let you define who can or cannot access your applications based on user Identity, network attributes, and device posture. Policies are specific to the application they are created for and are enforced in order.

Access Groups define groups of users and their related rules. They can be applied to multiple applications and help make management easier. For example, if you have a rule that allows anyone with a given email domain, such as [user@yourcompany.com](#), to access an internal application, then you will not need to make changes with Cloudflare Access when you add new users to your IdP.

For internally hosted applications, it is recommended that you use Argo Tunnel to tunnel traffic from the Cloudflare network to your application without needing to allow traffic over http or https (port 80 & 443).

Real-world applications

Learn how companies like yours are leveraging our platform

- When Peter Hahn transitioned to working remotely, their VPN caused serious performance issues. Deploying Cloudflare Access in front of the first batch of their internal tools resulted in such a huge increase in performance, reliability, and convenience for the whole team that they decided to gradually transition all tools to use Access.
- One of our customers used Cloudflare Access as a Policy Enforcement Point (PEP) in a Zero Trust architecture setup. They wanted to move away from a traditional VPN-based setup and needed some kind of “identity firewalling” that would allow them to authenticate the users as soon as possible.

How to implement Cloudflare Access














<https://developers.cloudflare.com/access/setting-up-access>

1. Navigate to the Cloudflare for Teams Dashboard (dash.teams.cloudflare.com).
2. If you are setting up your first Access application, you'll first need to add your identity provider:
Access → Authentication → Login Methods → Add.

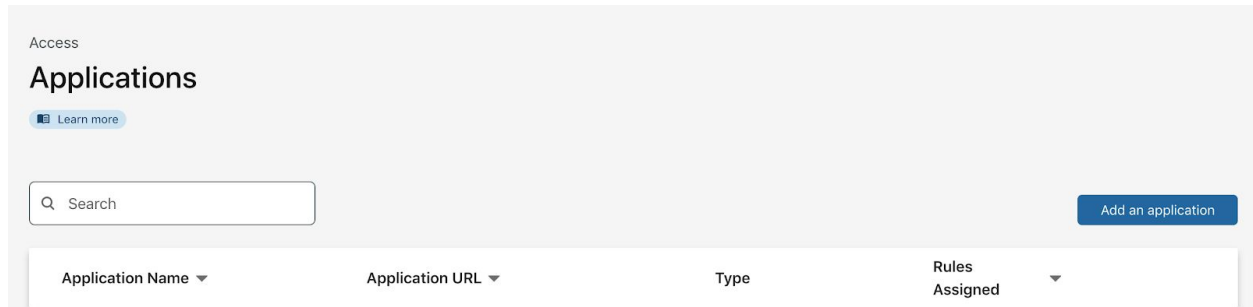
[← Back to Authentication](#)

Add an identity provider

Select an identity provider to add

 Azure AD	 Okta
 Centrify	 OneLogin
 Facebook	 One-time PIN ADDED
 GitHub	 OpenID Connect
 Google Suite	 SAML
 Google	 Yandex
 LinkedIn	

3. Now you can configure your applications. Go to **Access** → **Applications** → **Add an Application**.



Here, you'll be able to:

- Configure the application and link the identity provider you just added.
- Create policies for you application
- Configure CORS and cookies settings

Once created, it will show up in your list of applications.