Clearlogin - Overview

In This Article

Overview

Clearlogin is a highly available & scalable SaaS platform providing identity and access management (IAM) services for web-based applications. Clearlogin allows an IT team to easily secure access to cloud applications, and gives users a streamlined, single location to access web applications they use every day, from anywhere.

How Does Clearlogin Work?

Clearlogin acts as a proxy service hosted between your identity source (Active Directory, Azure AD, LDAP, Okta, etc.) and one or more target applications.

When Clearlogin has a trust relationship (federation) with an application using **SAML** (Security Assertion Markup Language) or **JWT** (JSON Web Token), Clearlogin can provide a seamless **SSO** (Single Sign On) experience by providing the federated application everything it needs to authenticate the user.

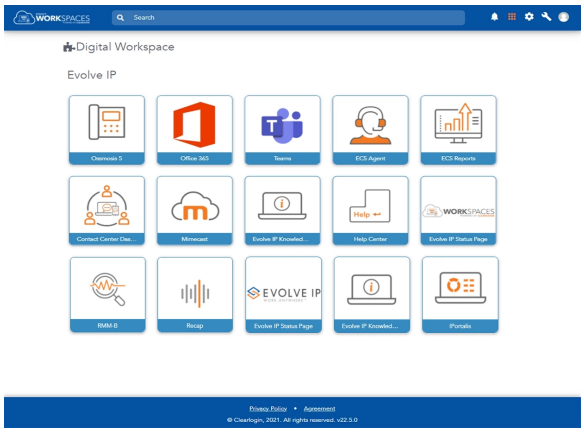
From an end-user perspective, they login to Clearlogin, and when they launch a federated application from their dashboard, Clearlogin provides the user's identity and access permissions directly to the application – the user is not prompted by the application to sign in.

If an application does not support SAML/JWT, Clearlogin's browser-integrated **Password Manager** can secure the user's credentials, and then provide those credentials to the application when the site is visited by the user.

Clearlogin also supports bookmarking, or linking to, websites that don't require authentication. For example, you can give users easy access to your company website, vendor sites, news sites or other frequently visited websites.

Features

Cloud Application Dashboard
The Cloud Application Dashboard is the single gateway to your cloud-based tools and resources. Securely log in once to access the apps you leverage every day, enable multi-factor authentication, manage groups, and monitor user access.



Password Management
Implement strong password policies that also streamline access for your users. Clearlogin offers zero-knowledge password management that increases security while minimizing login issues.

Multi-Factor Authentication
Requiring strong passwords isn't always enough to keep your sensitive data secure. Configure multi-factor authentication for an additional layer of security that will plug up any leaks in your perimeter and halt spoofing attacks.

Access Management
Access Rules let you define rules and policies to allow or deny your users access to Clearlogin. Access Rules also leverage a tagging system to further fine-tune your access criteria.

Multi-Domain Support
If your organization uses multiple directories or authentication methods, Clearlogin lets you configure separate settings to authenticate users based on their domain.

Clearlogin Anywhere
Clearlogin Anywhere is a simple, secure JavaScript login form that can be embedded into any site or application. Users only have to log in one time to gain access to your company's cloud applications and intranet portals.

Custom Branding
Add your company logo and custom styles to the Sign In, Sign Out, and Change Password pages for a more seamless integration for your end users.

Detailed Reporting
Gain insight into all aspects of user access, including unsuccessful login attempts, password changes, geography and browser data.

Concepts & Technologies

Clearlogin uses multiple technologies to provide seamless integration into your application environment. Here is some information about these technologies to get you started and comfortable with the features and terminology.

Identity & Access Management (IAM)

Identity and Access Management (IAM) is a general, umbrella-type term used to describe solutions that help you manage identities and their access to resources and data under your control. Features in an IAM solution generally include identity integration and provisioning, application federation, access management (conditional access), single sign on and self-service processes like password reset and account recovery.

Application Federation

Application Federation is a configuration where an Application and an Identity Provider (IdP) have a trust relationship, which allows the application to accept an identity and authentication claim created by the IdP. For example, after an end-user successfully authenticates with the IdP, the IdP generates a digitally signed token, using SAML or JWT protocols, that is presented when the user connects to the application, and since the application is configured to trust the IdP, the user does not need to sign in.

Single Sign-On (SSO)

Single Sign-On (SSO) is a term that describes the process of authenticating once and having that single authentication used with any federated application that supports SSO. However, since not all applications support SSO, Clearlogin's Password Manager credential vault feature allows end-users to safely secure their username and password for non-SSO applications.

Security Assertion Markup Language (SAML)

SAML is an SSO framework for authentication and authorization and consists of the following:

- **Identity Provider (IdP)** - The IdP is a proxy between the user and the SSO application. Clearlogin is an Identity Provider.
- **Service Provider (SP)** - The SP is an SSO application that supports SAML.
- **X.509 certificates** - SAML uses certificates to establish a federation (trust) between the Identity Provider and the Service Provider.
- **XML** - SAML uses XML for configuration settings and for the tokens passed between the the user, the Identity Provider and the SSO application (Service Provider).
- **SAML Metadata** - The Identity Provider and the Service Provider exchange a SAML metadata document (using XML) with one another to establish a federated trust between them. The XML metadata document also contains certificate information for token signing and encryption.
- **SAML Assertion (Token)** - This is a signed XML document from the Identity Provider that contains information about the user.


Clearlogin supports both SAML 1.1 and 2.0 standards.

SAML Sign In Process
The sign in process can be initiated using one of two methods, and an SSO application can support one or both. Clearlogin supports both.

- **Application (Service Provider) Initiated**
  - The user tries to access the SSO application directly.
  - The user doesn't have a token, and is redirected to the Identity Provider to authenticate.
  - The Identity Provider authenticates the user, then sends the user back to the application with a token proving their authentication and authorization.
  - The application reads the token and allows the user into the app.
- **Identity Provider Initiated**
  - The user accesses and authenticates with the Identity Provider directly.
  - The Identity Provider supplies a token to the user.
  - The Identity Provider redirects the user to the SSO application with the token proving their authentication & authorization.
  - The application reads the token and allows the user into the app.

More Info About SAML >>

JSON Web Token (JWT)

JWT is a fairly new standard that utilizes the JSON data format, and may be the simplest type of SSO integration. While being potentially slightly less flexible than SAML, it is definitely the easiest to set up and is more self-contained than SAML. Authentication is done via a token that is signed with a "secret" that is generated with the HMAC algorithm.

More Info About JWT >>

OpenID Connect & OAuth

Not to be confused with OpenID, which is for authentication only, OpenID Connect is a decentralized authentication protocol for both authentication via JSON (JWT) and authorization via OAuth 2.0. OpenID Connect functions both as an Identity Provider (IdP) or OpenID Provider (OP), and also as an authorization method for a Service Provider (SP).

OAuth, which is based on JSON, is a newer authorization standard for SSO developed by Google and Twitter. They developed OAuth because SAML didn't work well on mobile platforms. OAuth provides authorization services, and OpenID Connect provides authentication services. Both OAuth & OpenID Connect are normally used together.

More Info About OpenID Connect >>

Learning Tools Interoperability (LTI)

LTI is a standard developed by IMS Global Learning Consortium for Learning Management Systems (LMS) and is primarily utilized by education-focused organizations. LTI is built on OAuth 2.0, OpenID and JWT. It's primary function is to automatically serve a student with the tools and courses that they require contextually based on metadata containing education-centric information.