veza

Authorization-Based Access for Any App: Meet Veza's Open Authorization API

Critical customer data is spread across an ever-increasing number of systems, including applications, data platforms, and infrastructure. These systems or even individual components may be purchased from a vendor, developed completely in-house, or open-source; they may be delivered via SaaS, or software run in cloud resources or on-premise. To provide the most comprehensive view of data security, customers need visibility across all these systems. Many of the most critical integrations (such as Snowflake, Azure SharePoint, etc) are built natively into the Veza platform and work out of the box; however, often there is a need to integrate applications into Veza to help understand and manage who can and should take what action on critical applications (customer success application, customer analytics application, etc).

To enable these custom integrations, Veza has developed the Open Authorization API (OAA) to enable easy integration to a wide range of applications and data systems, via a standard interface. OAA enables customers and partners to create new integrations faster and in a self-service model. It also allows the integration of custom apps without having to leverage internal expertise about how these custom apps grant authorization. OAA enables customers to have a complete view of permissions across most systems and, provides an even more comprehensive answer to who can and should take what action on what data, on what app, on what service.

Integration Requirements

OAA integrations require a connector that performs 3 basic functions:

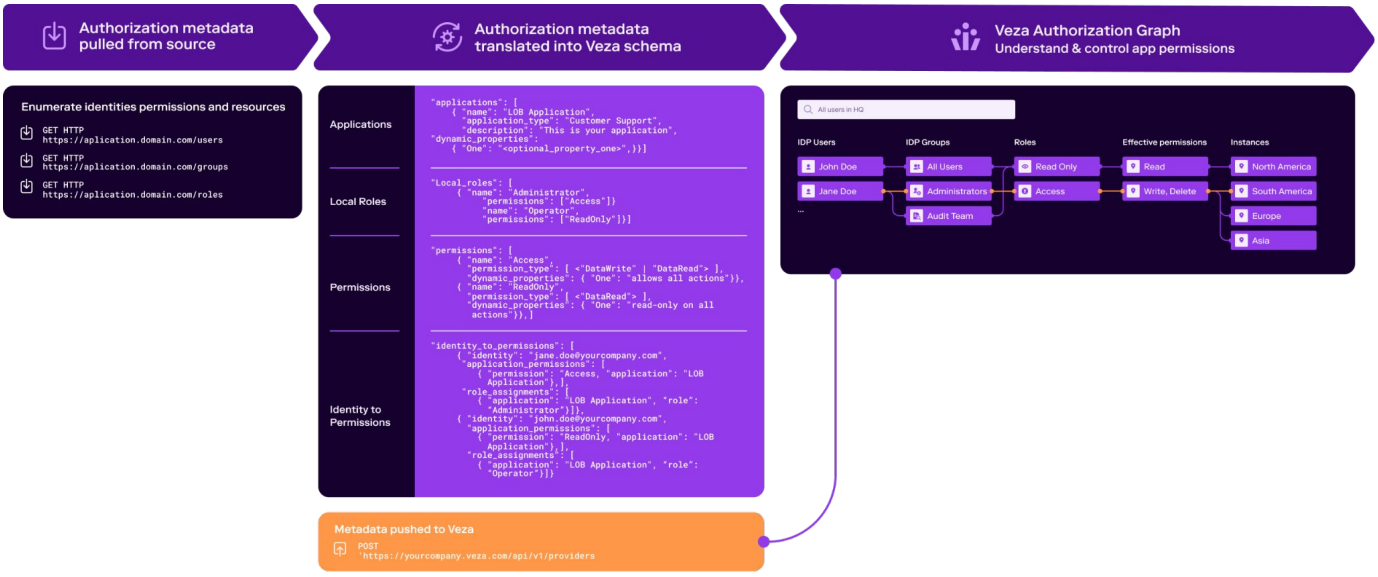
1. pulling the authorization metadata from the target system (application, data system, etc.),
2. transforming the metadata into the Veza schema, and
3. calling the OAA REST API to upload the transformed schema into the Veza platform.

Veza maintains an OAA Community site where contributors have provided OAA Connector code that others may use free of charge. Veza can also provide custom OAA Connectors (please reach out via GitHub or our OAA Community on Slack).

Any system that can be queried for authorization information (e.g., identities, permissions, and resources) via an API (or other interfaces) and has sufficient documentation can be integrated via OAA.

How it works

OAA works by providing a mechanism to upload authorization information to Veza in a standardized format. To integrate a new system (application, data systems, et al), you utilize that system's API (or other interfaces) to enumerate the identities, permissions, and resources that you want available in Veza. This information is then formatted into Veza's OAA JSON schema and uploaded to Veza using the OAA REST API.



Veza processes this schema mapping to integrate the new application into Veza's Authorization Metadata Graph, which maps which identities have what permissions (actions) to what resources (e.g. GitHub repository, Zendesk org, etc). Veza combines this information with discovered data from Identity providers to expand group memberships and correlate identities. Identities can be local to that application or linked to external Identity Providers (IdP) like Okta or Azure AD.

The Veza schema can capture and represent both standard Effective Permissions (around CRUD: Create, Read, Update, and Delete) as well as system-specific permissions (like "Admin" or "Operator").

Once the application is integrated via OAA into Veza, it acts like any other system configured with Veza. OAA-integrated applications are visible in Veza when searching and querying the list of application-specific resources a user has access to, viewing Insights and Heatmaps, configuring Alerts, and many more.

OAA Integration Examples

To integrate an application with OAA a user needs to be able to retrieve the list of resources and authorizations. This often happens through the application's API. Many of the most popular applications today provide API or SDK interfaces to automate tasks and monitor status. These APIs often provide all the information necessary to query the application's authorization.

To represent an application in the OAA schema the general pieces of information needed are:

- List of users and groups for the application
- List of permissions (this may be enumerated from documentation or retrieved dynamically depending on the application)
- List of resources
- Most importantly, for each resource, the list of authorizations for that resource (i.e., users or groups who have permissions)

Examples - OAA for GitHub:

Veza provides tools and documentation to help you get started with using OAA, including:

- GitHub - Community-provided OAA integration that utilizes the GitHub API to list an organization's repositories (i.e., resources), users, and groups. Provides insight into which users have access to sensitive source code or who can modify infrastructure as code to impact critical IT operations.
- Custom App (e.g., Customer Support Portal) - integrate a Veza customer-created application used by its' customer support team to assist in resolving support issues. This portal allows access to sensitive customer information necessary as context for the support issue. The integration uses OAA to report which employees have what level of permissions to ensure customer data is safe.

Additional Resources

Veza provides tools and documentation to help you get started with using OAA, including:

- Documentation
- A Python library that can be used to write custom integrations
- Sample code
- Integrations with common applications that can be utilized direct, modified, or used as a reference to integrate other applications

Veza's Open Authorization API (OAA) allows customers to integrate their most important systems and in-house applications to Veza's Authorization Metadata Graph and allows organizations to gain visibility and control over the key question of "who can and should take what action on what data?".

Learn more about how Veza secures any application at www.veza.com/platform.

- sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.