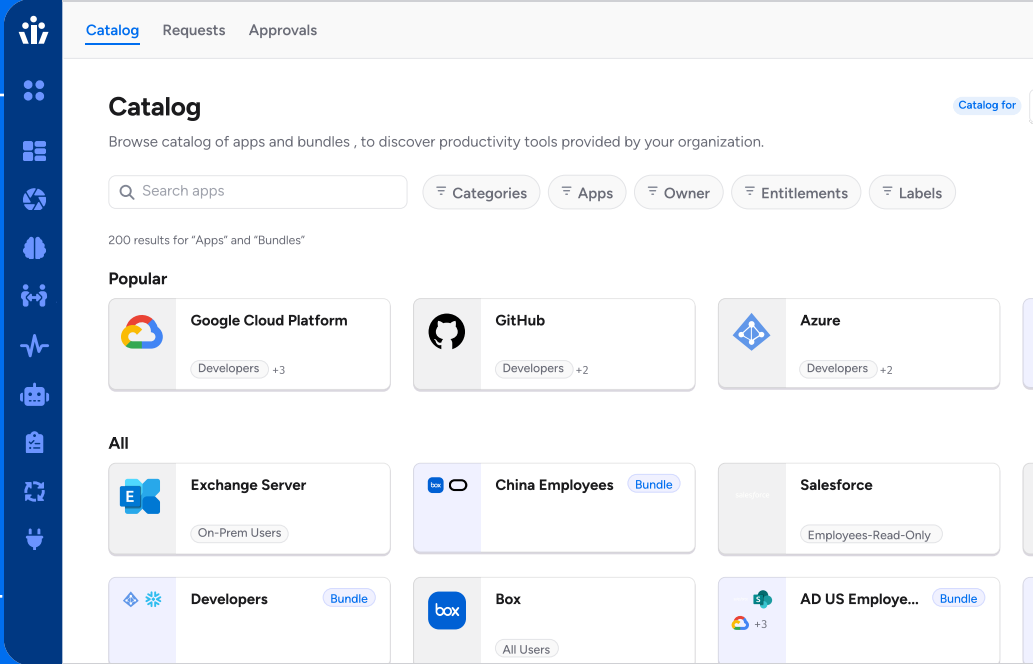


Access Requests

Increase user productivity and reduce standing privilege by quickly and accurately provisioning access across enterprise applications and resources.



Key Benefits

Consistent and Accurate Provisioning

Manage and fulfill access requests with least privilege

Real-time Access Governance

Eliminate privilege creep and minimize the risk of standing privilege with just-in-time access and auto-expiration

Assured Compliance

Provision access in accordance with security policy in a consistent and compliant manner

Enhanced Employee Experience

Increase employee productivity by accelerating access grants through a self service access request portal and automated provisioning

Complete Transparency

Monitor team member permissions in a centralized manager dashboard and grant or revoke access directly in Veza

Key Capabilities

My Teams and Manager's Access Dashboard

Managers gain complete visibility into their direct reports' entitlements and resource permissions, as well as revoke inappropriate access or grant access to applications

Self-Service Access Requests

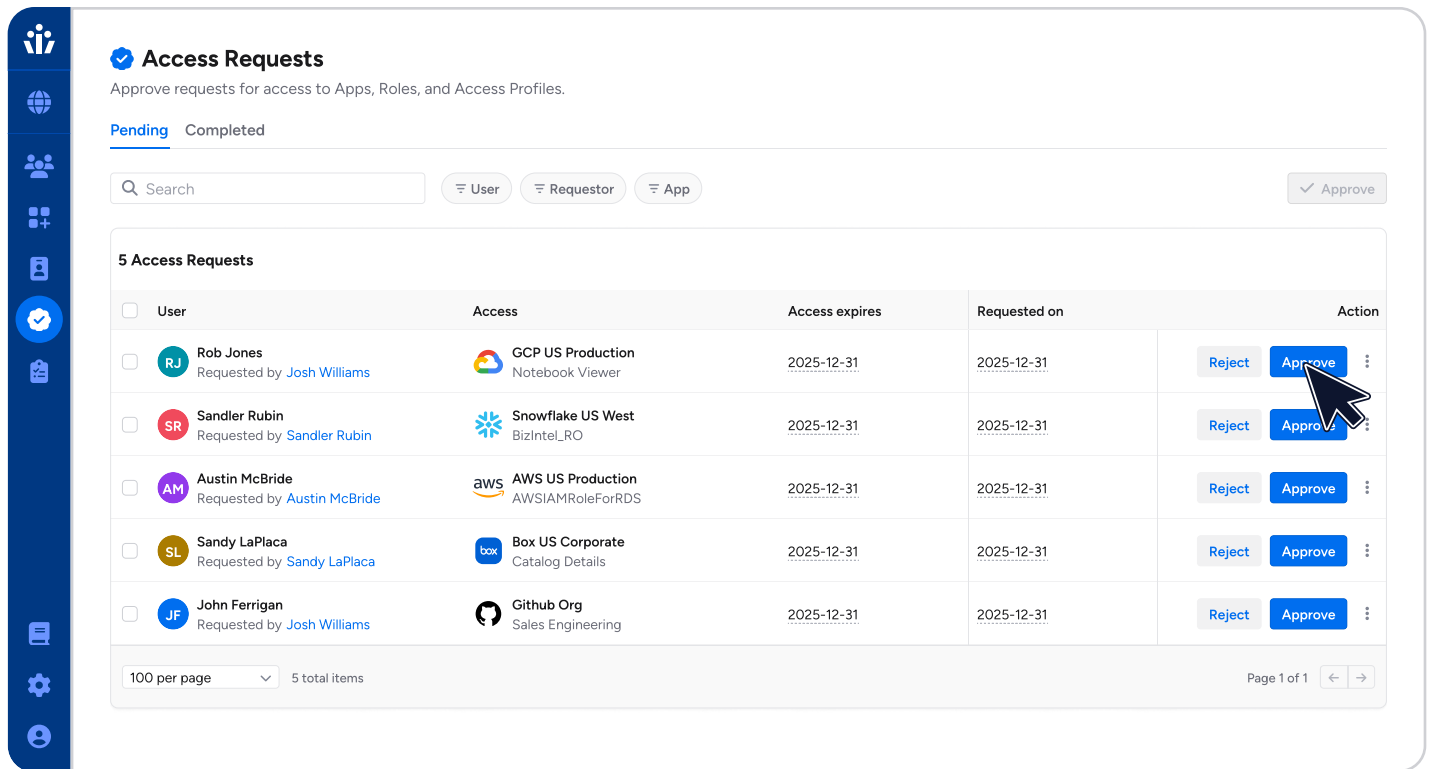
Empower users to view, request, and remove their own access without the need for ticket creation

Just in Time Access

Request time-bound privileged or non-privileged access to resources and applications to reduce the risk of standing privilege

Built on the Veza Access Platform

Veza is the identity security company that powers Intelligent Access. The platform enables companies to monitor privilege, investigate identity threats, automate access provisioning, requests, deprovisioning and reviews to bring access governance to enterprise resources like SaaS apps, data systems, cloud services, infrastructure services, and custom apps.



Access Requests
Approve requests for access to Apps, Roles, and Access Profiles.

Pending Completed

Search [] User Requestor App Approve

5 Access Requests

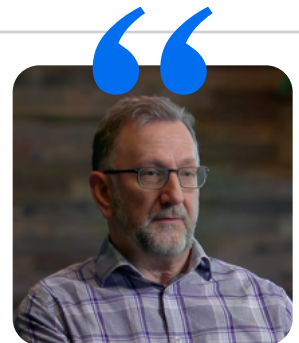
User	Access	Access expires	Requested on	Action
<input type="checkbox"/> RJ Rob Jones Requested by Josh Williams	GCP US Production Notebook Viewer	2025-12-31	2025-12-31	Reject Approve
<input type="checkbox"/> SR Sandler Rubin Requested by Sandler Rubin	Snowflake US West BizIntel_RO	2025-12-31	2025-12-31	Reject Approve
<input type="checkbox"/> AM Austin McBride Requested by Austin McBride	AWS US Production AWSIAMRoleForRDS	2025-12-31	2025-12-31	Reject Approve
<input type="checkbox"/> SL Sandy LaPlaca Requested by Sandy LaPlaca	Box US Corporate Catalog Details	2025-12-31	2025-12-31	Reject Approve
<input type="checkbox"/> JF John Ferrigan Requested by Josh Williams	Github Org Sales Engineering	2025-12-31	2025-12-31	Reject Approve

100 per page 5 total items Page 1 of 1

Veza provides our Identity and Access Management Cloud team an easy, self-service interface that enables them to visualize and understand privileged, over-provisioned and unused account access. This helps ensure teams have the right level of access when they need it and confirms our identity footprint while reducing risk.



Scott Thomas
Director, Identity and Access Management



Extended Feature List

Self-Service and Third-Party Access Requests

Self-service access requests

Support for self-service access requests to allow end-users to initiate their own requests for access on-demand

Third-party access requests

Support for third-party access requests to allow a requester to initiate self-service access requests on-demand on behalf of another beneficiary, such as a manager requesting access for a direct report

Access revocation

Support to optionally allow requesters to request on-demand revocation of previously-granted access

Requests integrated into the Access Hub

Access request workflows integrated within the Veza's Access Catalog in the Access Hub

Web-based Access Catalog

Easy-to-use Web-based Access Catalog facilitates requester searches for requestable catalog items; allows requesters to initiate access requests within a modern, consumer-style "app store" experience

Support for applications, application entitlements, and bundles of applications

Full support for requesting new application accounts, application access with specific entitlement(s) granted, and bundles of applications (i.e. role-based access to many different applications and entitlements in a single request)

Automatically provision a new user account and access upon approval

Ability to provision a new account and access on approval, if not previously provisioned for the beneficiary

Ability to request guest account access

For supported applications, ability to provision a new guest account and access on approach

Configurable options for distributing initial user credentials

Configurable notification options with support for customizable email templates for distributing initial logon credentials, such as sending to end-user and/or end-user's manager

Allow requesters to justify their access requests

Requester can optionally add a business justification to any access requests that they initiate

Allow requesters to set access expiration

Governed by administrative just-in-time policy settings, requesters can set their own access expiration with a policy-controlled range

Approval Workflow

Manager, administrator, and named approver approval workflows

Ability for people managers, system administrators, and any named approver (i.e. app owners) to be assigned approval responsibility

Multi-level, multi-party approval

Support for multi-party, multi-level approval workflows prior to fulfillment

Approval reassignment

Ability to reassign approval authority to other approvers

Stakeholder notifications

Automatic system notifications to inform requesters, approvers, and beneficiaries that an access request has been initiated, decided, granted, or revoked

Auto-approval support

Ability to automatically auto-approve and grant certain access requests per administrative policy without escalation to and intervention by a human-based approver

Approve, reject, and return for more information

Allow approvers to approve, reject, and return for more information any access request

Approval workflow integrated with Access Hub and Veza console

Access request approval workflows integrated within the Veza's end-user-facing Access Catalog in the Access Hub

Target Application Support

Support for identity providers

Support for access requests/revocation for leading identity providers, including Microsoft Active Directory, Entra ID (Azure Active Directory), and Okta

Support for cloud platforms

Support for access requests/revocations for leading cloud providers, including AWS Console, AWS Identity Center, Google Cloud, and Microsoft Azure

Support for productivity applications

Support for access requests/revocations for productivity applications, including Google Workspace and Microsoft Office 365

Support for CRM, ERP, and PLM applications

Support for access requests/revocations for leading CRM, ERP, and PLM applications, including Salesforce, Oracle Fusion Cloud, SAP, and PTC Windchill

Support for developer and database platforms

Support for access requests/revocations for GitHub and Snowflake

SCIM support

Support for access requests/revocations for generic SCIM-based applications.

Guest account provisioning

Support for provisioning guest account access (Microsoft Entra ID only)

Privileged account/role provisioning for privilege escalation

Support for privileged account/privileged role provisioning

Support for creating and managing entitlements on target applications

Support for creating and managing Microsoft Active Directory, Microsoft Entra ID (formerly known as Azure Active Directory), Okta, Google Cloud, and AWS groups and roles

Just-In-Time Access Policy and Auto-Expiration

Just-in-time access policy

Support for policy-based just-in-time access settings per requestable item; optionally allow requester to adjust settings within policy-defined limits

Enforced auto-expiration

Support for adjustable, policy-enforced auto-expiration time ranges

Access Profiles and Access Profile Intelligence

Access Profile Intelligence

Automate the creation and setting of entitlement on Access Profiles. Powered by the Veza Access Graph, Access Profile Intelligence allows you to quickly build Access Profiles based on entitlements belonging to a typical user or a set of existing users and groups

Support for Access Profiles

Model bundles of entitlements to target applications to ensure consistency in the provisioning and deprovisioning process

Support for Business Roles

Model a bundle of multiple Access Profiles as a Business Role to ensure all users of a similar role always have consistent access across applications and resources

Custom Access Profile types

Allow administrators to create their own custom Access Profile types

Role-based access control for Access Profiles

Apply role-based access controls to Access Profiles to limit who can view, edit, or delete them. Limit access to specific Access Profile owners

Self-service Access Profile management

Empower applications owners, people managers, and others. to manage Access Profiles in a self-service manner from the Access Hub

Draft mode support

Save work-in-progress Access Profiles to draft, before publishing changes to production

Integrated with Veza Lifecycle Management

Leverage Access Profiles across Veza Lifecycle Management and Veza Access Requests - deploy Access Profiles to easily support both birthright and ad-hoc access provisioning

Integrated with Veza Access Graph

Access Profiles are automatically propagated to the Veza Access Graph making it simple to see how users and individual application entitlements are linked to individual Access Profiles

Granular and Customizable Policies

Policy-based access provisioning

Enforce policy-based governance of source-to-target user attribute mappings and transformations as well as target entitlement assignments

Visual policy editor

Effortlessly create, view, and update policies with Veza's highly intuitive visual policy editor

Policy versioning and rollback

Maintain version control and rollback capabilities for policies and workflows

Draft mode support

Save work-in-progress policies to draft, before publishing changes to production

Policy dry run

Test the impact of policies using "dry run" execution

Attribute mapping

Define mappings of standard and custom user attributes from identity sources to target applications to ensure all relevant user attributes are properly enriching the target accounts

One-time or continuous attribute synchronization

Choose from continuous syncing of users attributes from identity sources to target applications or opting for one-time synchronization of attributes at provisioning time

Attribute transformations

Optionally perform transformations on identity source user attributes at mapping time to automatically derive other user attributes for target applications and resources

Pipeline transformations

Chain multiple attribute transformations in sequence with pipeline transformations

Attribute normalization

Normalize attribute values containing accented characters or diacritics for use with legacy target applications that do not support such characters

Attribute lookup

Lookup attribute values against entities in the access graph or custom lookup tables with the ability to use the resulting lookup value as the transformed attribute

Attribute overrides

Manually override individual attribute values on specific identities

Custom lookup tables

Upload custom lookup tables for use by the attribute lookup transformation

Identity-Centric, Audit-Ready, and API

Identity-centric view

See actual identities of access request beneficiaries for both investigating access as well as monitoring identity-centric events. Drill-down into individual identities to see properties, attributes, and an activity log

Auditing for access request and revocation events

Capture a mandatory audit trail for all provisioning and deprovisioning events, jobs, actions, and workflows tasks

Activity log export

Export Access Request events to CSV and PDF files

REST-based management API

REST-based management API for system administration, managing policy, Access Profiles, and downloading logs

Access grant API

REST-based Access Grant API to programmatically grant access to an application

About Veza

Veza is the identity security company. Identity and security teams use Veza to secure identity access across SaaS apps, on-prem apps, data systems, and cloud infrastructure. Veza solves the blind spots of traditional identity tools with its unique ability to ingest and organize permissions metadata in the Veza Access Graph. Global enterprises like Wynn Resorts, and Expedia trust Veza to visualize access permissions, monitor permissions activity, automate access reviews, and remediate privilege violations. Founded in 2020, Veza is headquartered in Los Gatos, California, and is funded by Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, and True Ventures. Visit us at veza.com and follow us on [LinkedIn](#), [Twitter](#), and [YouTube](#).