# Access Management Overview

Most enterprises rely on one or two teams to manage access manually. With an ever-increasing number of apps and systems, organizations are struggling to manage access at scale. Opal is the identity security platform for the world's best organizations. With a self-service app catalog, employees can get access to systems faster and admins can set powerful guardrails to ensure security and compliance.

Self-service app catalog
Cut down on support tickets for access requests
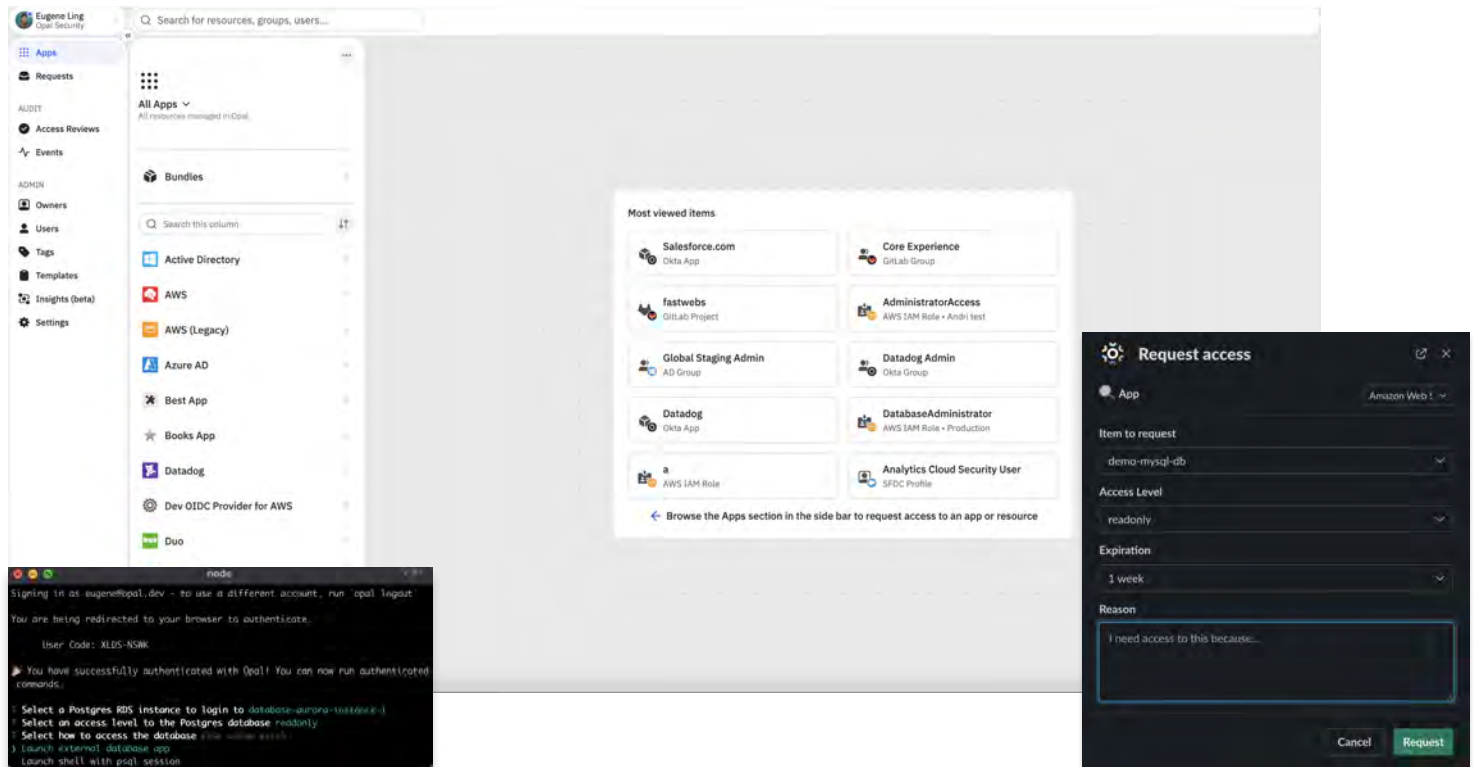
Universal catalog

Opal provides a consistent experience for employees to browse and request access across engineering infrastructure, SaaS applications, and custom internal tools.

Native developer workflows

Developers can use Opal to generate federated and auto-expiring credentials. This will improve security posture as passwords won't be stored locally and eliminate the manual overhead of credential rotation. In addition, engineers can access infrastructure using Opal's CLI or request for the creation of IAM roles natively in the product.

Accelerate access

With Opal, employees can get access to critical systems in minutes not days. Approvals are not bottlenecked by centralized teams. Instead they are delegated to system owners and managers with more context. In addition, access can be approved and provisioned via Slack.

Secure by design

Implement least privilege using granular and time-based access. Employees can request for specific permissions and access levels, rather than coarse grained groups or roles. Also, employees can request for time-bounded access or tie the access to the lifecycle of a support ticket.

Supercharged Engineering Experience
Leveraging native integrations, Opal provides a frictionless experience for engineers
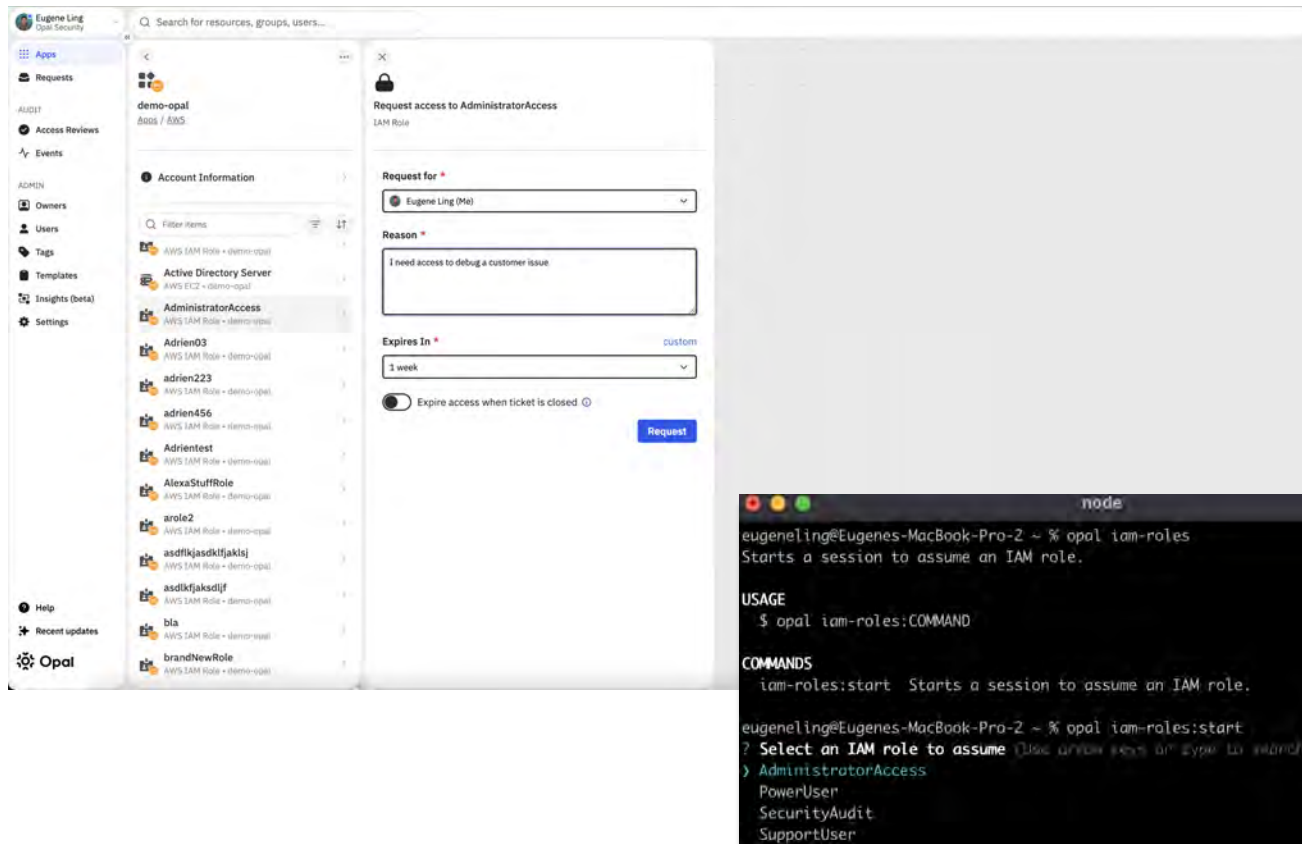
Granular resource level access
Instead of granting access to roles, which are easily over-provisioned, Opal enables engineers to get access to specific access levels in databases, kubernetes, servers, repos, and more. In the platform, admins can also bind access levels to existing groups brought in from identity providers.

Generate short-lived credentials
Opal eliminates the need for manual credential rotation. The platform provides an easy way for developers to generate federated and auto-expiring credentials. This allows admins to attribute session-based access to users and bolster security posture.

Dynamically create IAM roles
If developers can't find the role that they need, they can request for the creation of IAM roles natively in the product. Opal provides a self-service wizard to streamline the experience and DevOps can approve the creation of the role directly out of Slack.

Automate on-call access
Integrated with on-call providers, Opal can automatically grant privileged access when developers are on-call and revoke access when the on-call schedule is over.

Configure App Catalog to meet your security needs

Opal enables teams to customize approval and security configurations based on risk
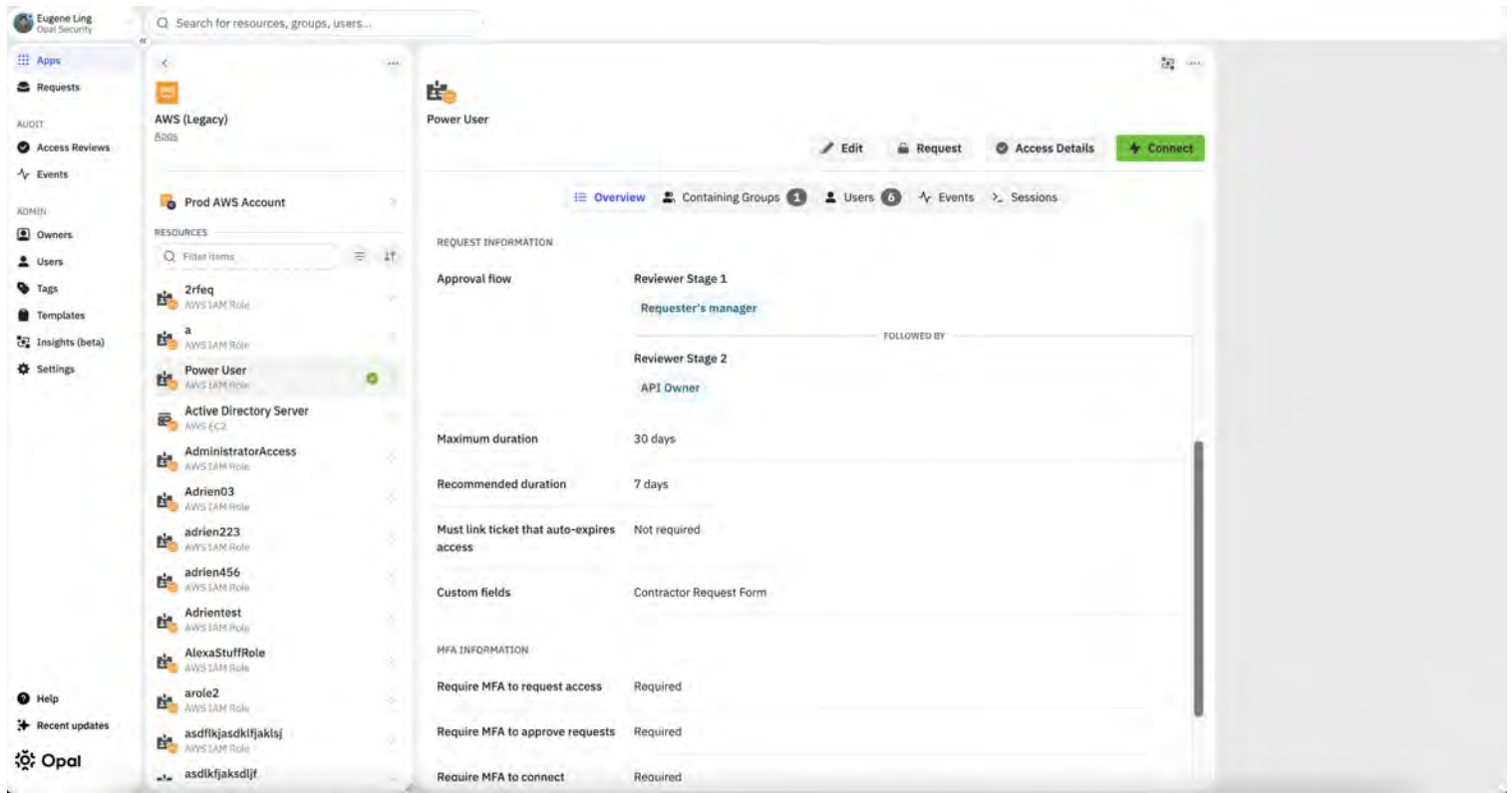
Decentralized management

Access management can only scale through decentralization. With Opal, the management of resource and group policies can be delegated to system owners with the most context. This will alleviate the burden from centralized teams, such as IT and DevOps. Everyone can feel rest assured that access requests are stored in Opal's event logs.

Multi-step approval workflows

Opal supports granular and multi-step approval workflows. For example, read-only database access might require manager approval. However, write-access should require both manager and system owner approval.

Powerful guardrails

Team admins can set powerful configuration, such as requiring 2FA to approve requests, support tickets, or mandating maximum request duration. With an extensible API, Opal enables enterprises to manage policies at scale.

Customized app catalog

Employees will see customized catalogs based on the groups that they are a part of. This will ensure that users get a relevant and secure experience.

Opal secures the identity perimeter for modern enterprises. With Opal, security teams can prioritize risk, delegate management across the company, and measure impact across security, productivity, and compliance. The world's best companies, such as Databricks, Figma, Blend, and Marqeta, trust Opal to govern and adapt sensitive access. Opal is backed by Greylock and some of the top security experts around the world, including Silicon Valley CISO Investments (SVCI).

To learn more, please visit **www.opal.dev**