Role-Based Access Control and Single Sign-On Features Improve User Security and Compliance

Manage User Access to VividCortex with Confidence and Ease

VividCortex's capabilities for Role-Based Access Control (RBAC) and Single Sign-On (SSO) introduce enterprise-grade user provisioning and management to the powerful, SaaS database monitoring platform. Enterprise organizations can now use VividCortex to integrate with a SAML-based identity provider and apply existing company credentials to access the application, so that users no longer need to remember additional login information or passwords. Security and compliance concerns are also covered, as RBAC makes it possible for system administrators to quickly and easily change or revoke users' access, while every action is documented via a detailed audit trail.

With these features, a cloud-hosted solution is the superior database monitoring choice over on-premise alternatives for the first time. RBAC and SSO continue VividCortex's initiative to deliver world-class security features and support to its users, providing the safest available platform for customers' data.

Automate User Access and Management

Know exactly who has access to what information within VividCortex, in every area of the organization. Use customizable team and environment assignments to restrict system access based on roles.

Improve Compliance and Security

Easily modify and revoke access privileges as team members change roles or leave the organization. Access audit trails for compliance purposes and keep an ongoing log of access capabilities based on role.

Increase Team Productivity and Efficiency

Minimize the amount of time and effort it takes administrators to assign and modify privileges. Keep end users focused on the part of VividCortex that matters most to their responsibilities.

Automate User Access and Control to Streamline Security

Role-Based Access Control

Role-Based Access Control enables enterprise organizations to create teams, assign users to those teams, and grant roles and permissions ("read-only" and "read-write") to those team members, based on the users' specific responsibilities within VividCortex.

- **Enhanced security.** Engineering and application managers can view and assign user roles, access, and security in a single view. For example, Tier I support may be permitted Read-Only access to a Production environment, only able to view reports and access non-sensitive data of the environment. Developers with Read-Write access can update host credentials, add new hosts, access Query Samples or API tokens. Application and engineering team managers with Administrator privileges have full access.
- **Flexible administration.** Administrators have the flexibility to assign a role to a team or to an environment.
    - **Team access.** By assigning a role to a team, an administrator defines the default privileges afforded to that team. Available actions include adding users to your organization, inviting people to a team, managing teams, and creating new environments.
    - **Environment access.** By assigning a role to an environment-team couple, you can grant different privileges per environment to a team. For example, if a team of "Developers" has access to both "Production" and "Staging" environments, the administrator may grant full read-write access to the "Staging" environment, but read-only access to the "Production" environment.

Single Sign-On

SAML-based SSO is a simple and secure solution for teams aiming to manage employee access to VividCortex. End users are afforded an easy way to use their existing credentials to log in to VividCortex, while IT departments can use their existing identity management system to grant and revoke access and credentials.

- **Provider integration.** Administrators can use a directory of users inside of their identity provider and assign service applications to them. Once users have been assigned to the VividCortex Application in the provider, they will have single-click access available for log in.
- **Automated user provisioning.** VividCortex supports SAML authentication and SMIC provisioning. Administrators are able to access the following functions of your identity provider's services:
    - ***Import users.*** New users created in VividCortex can be downloaded and matched against existing users.
    - ***Create users.*** New users created through the identity provider are automatically created in the VividCortex application.
    - ***Update user attributes.*** Updates made to the users' profiles through the identity provider will be pushed to the VividCortex application.
    - ***Deactivate users.*** Deactivating the user through the identity provider will remove the user from the organization and all teams in the VividCortex application.
- **SAML Security.** VividCortex uses the secure and widely adopted industry standard Security Assertion Markup Language 2.0 (SAML 2.0), which means our implementation of SSO integrates easily with any identity management provider that supports SAML 2.0.