

Update: New OAuth Supplemental Security Role

Published 06/12/2020

As of July 12, 2021, this "Learn Veracross" site has been deprecated. It will remain live at least through October 1, 2021, but will no longer be updated. All Veracross Product Recent updates have been migrated to the [Product Updates](#) section of the [Veracross Community](#). Please update your bookmarks.

Module: Core Foundation (OAuth)

Affects: Schools interested in SSO

Effective: June 12, 2020

Summary

We are releasing the OAuth_App_Admin supplemental security role, effective immediately. This security role gives users the ability to create, edit, and delete OAuth applications in Axiom. OAuth applications, in turn, allow for vendors to use Veracross OAuth SSO to enable login to their vendor applications.

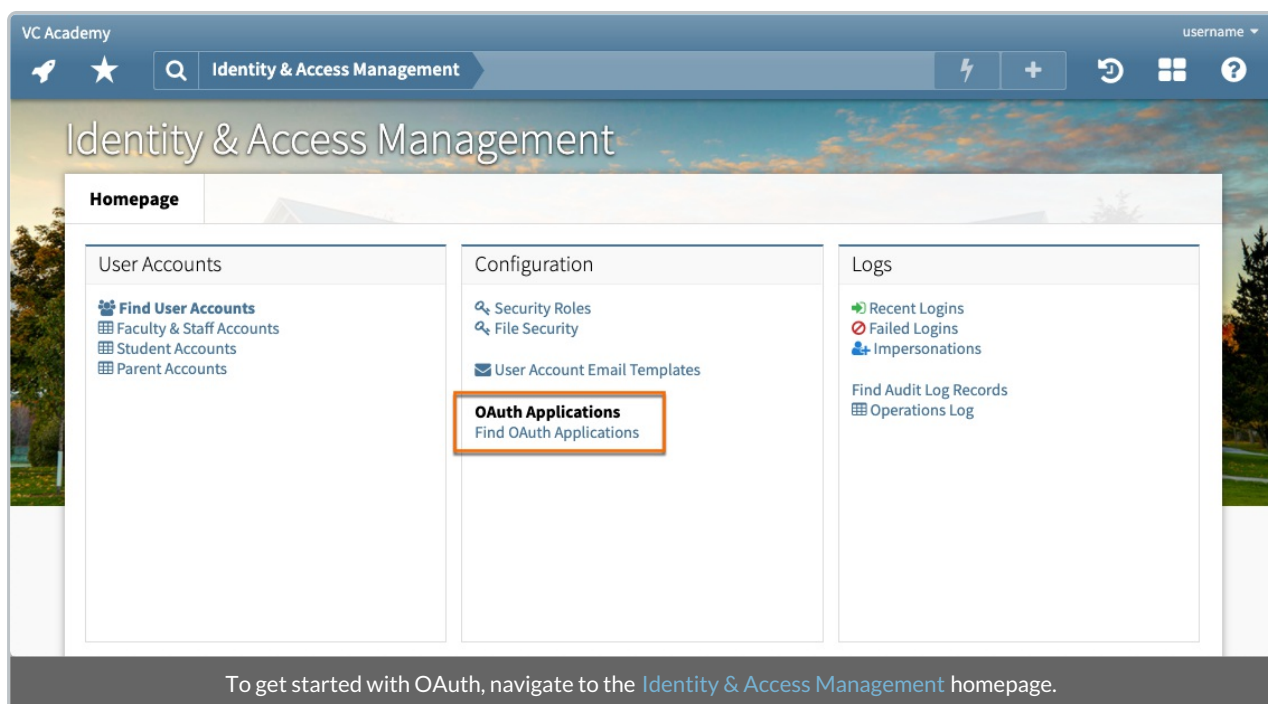
Unlike most record types, SysAdmin_1 doesn't have automatic permission to create/update/delete OAuth application records. OAuth_App_Admin can be combined with SysAdmin_1 to enable access for those users. Users with SysAdmin_1 have read-only access to all parts of OAuth application records, except the client secret (which is only visible for OAuth_App_Admin users). Other users have no access to this record type.

The Details

Creating OAuth applications will be necessary to enable Single Sign On (SSO) for vendors working with your school. Creating OAuth applications is a self-serve workflow and doesn't require approval or involvement from Veracross support.

To create an OAuth application:

1. Navigate to the **Identity & Access Management** homepage.
2. Run the linked “**Find OAuth Application**” query in the “**Configuration**” section.
3. From that query, open the Organize menu and click “**Add Record...**”



Veracross' OAuth SSO login flow provides several benefits for Veracross end users:

- **User experience:** If all of a school's vendors are integrated via OAuth SSO, then Veracross users only need to manage one account. (Note: Veracross OAuth SSO will work for all Veracross account types, including MFA, Google accounts, and school domain accounts).
- **Security:** No user passwords are shared to vendors. Vendors also benefit from Veracross' preexisting security infrastructure.
- **History:** All logins via OAuth SSO are tracked in the Login Log.

Because OAuth is a standard approach for enabling SSO, there are a lot of resources and libraries available to learn how to set up and utilize OAuth. We will also be releasing additional documentation of our own early next week.

Combining This New Security Role With SysAdmin_1

Unlike most record types, SysAdmin_1 doesn't have automatic permission to create/update/delete OAuth application records. OAuth_App_Admin can be combined with SysAdmin_1 to enable access for those users. Users with SysAdmin_1 have read-only access to all parts of OAuth application records, except the client secret (which is only visible for OAuth_App_Admin users). Other users have no access to this record type.