Creating an OAuth Application: School Workflow

Updated Jul 13, 2021

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 knowledge content has moved to the new Veracross Community. Please update your bookmarks.

Here is the new version of this article in the Veracross Community.

Overview

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.

Some parts of an OAuth Applications need to be provided by a vendor ahead of time, such as:

- **Name:** This is how the OAuth Application will be displayed in Axiom, theVeracross Login page, and in the Login Log. We recommend using a name tied to the vendor or their product.
- **Internal Notes:** A brief description for easy reference to the functionality of the application. This field is only visible to administrators in Axiom.
- **Contact Email:** A technical support email provided by the vendor or creator of the connected application.
- **Scopes:** "Scopes" define access permissions for an application.
  Note: The "sso" scope enables Single Sign On, which enables users to log in to vendor websites securely with their Veracross Account. If you are setting up an SSO integration, then this scope is required.
- **Redirect URIs**: This is the list of URLs that a user can be redirected to after a successful login via SSO. These URLs need to be provided by vendorsand must support OAuth.

Security Roles

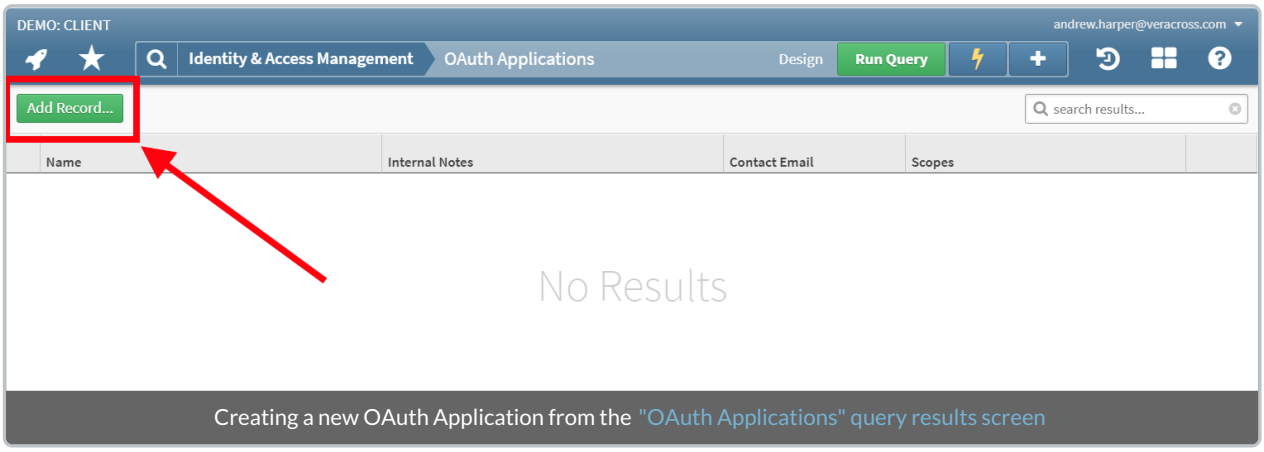
To create an OAuth Application record, you**must** have the OAuth_App_Admin supplemental security role (even if you have a SysAdmin security role). You can read more about the OAuth_App_Admin supplemental role in this update.

Workflow

To create an OAuth Application first navigate tothe Identity & Access Management homepage. Run

the “OAuth Applications” query in the “Configuration” section.

From that query you can click "Add Record...". See the list of fields above for how to fill in the new record.

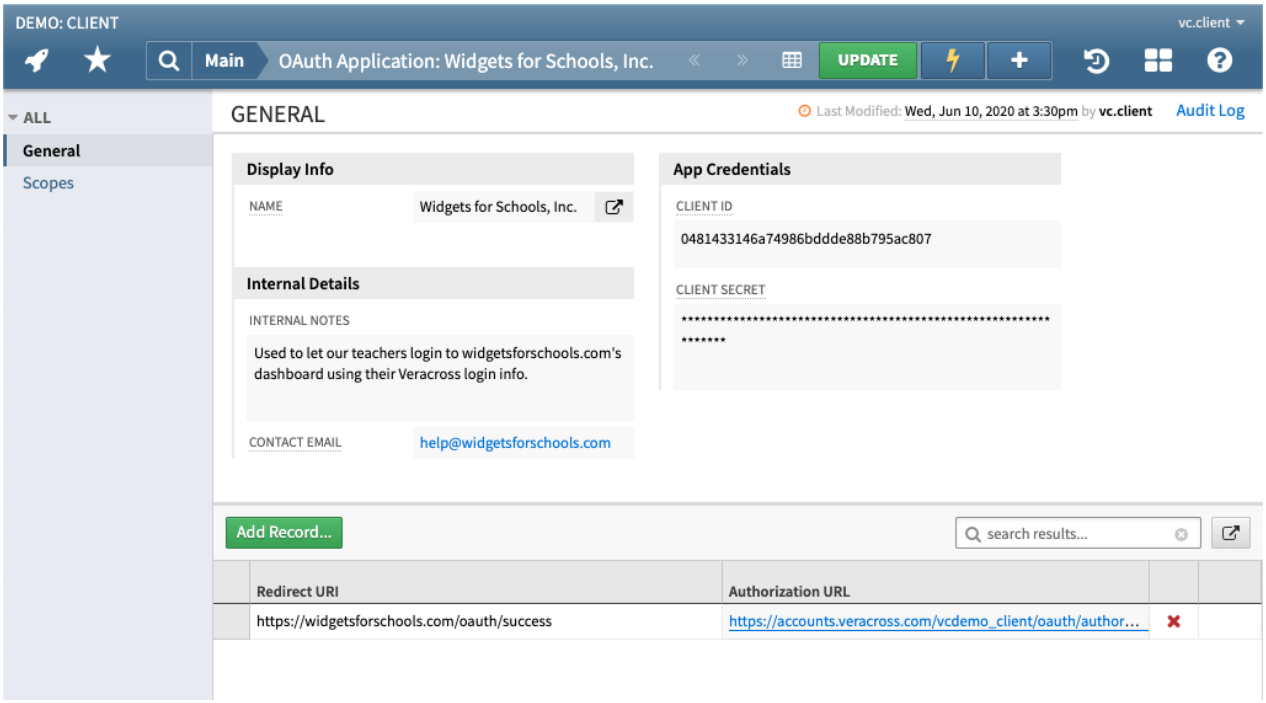


Creating a new OAuth Application from the "OAuth Applications" query results screen

Once the application is set up, an OAuth App Admin user will need to send certain information to the vendor, so that the vendor can complete the setup process:

- The OAuth Application's "client ID"
- The OAuth Application's "client secret"
- The list of scopes attached to the OAuth Application
  Note: for SSO integrations, the "sso" scope must be added first.

For SSO integrations, youcan also share the “Authorization URL” connected to any of the redirect URLs. These are the pre-built links that the vendor will need to send their users through the OAuth SSO login flow. However, vendors familiar with OAuth authorization should be able to construct these URLs themselves. These links are provided in Axiom for your convenience.



Troubleshooting

- If a user doesn't have the "Add Record..." button on the OAuth Applications query, check if they have the OAuth_App_Admin security role. This role is required to create/update/delete OAuth Applications, and access security sensitive fields such as the "client secret". This role isn't implicit for SysAdmin users, so they'll need the role too for these workflows.
- If a user sees the OAuth Application record as "read only", or the "client secret" field is masked (shows asterisks), check if they're missing the OAuth_App_Admin security role.
- If a vendor gets a "403 Forbidden" error during SSO, check that the "sso" scope has been added to the OAuth Application record. OAuth Applications without the "sso" scope won't work for SSO.