How To Impersonate Users

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

User Impersonation is a feature that allows system administrators and certain staff members to log in as another Veracross user for testing purposes. Impersonation is supported in all Veracross apps except for Composer.

Allowing Impersonation

Users with the *SysAdmin_1* security role can use impersonation without further setup. For other users, one of the special User Impersonation security roles need to be granted. Each role has other security roles as prerequisites. If a user does not have one of the prerequisite roles, an error will be displayed when trying to grant an impersonation role. Similarly, if a user has an impersonation role and their prerequisite role is removed, the impersonation role will also be removed.

There are three Impersonation roles:

Impersonate Current Families

This role allows users to impersonate Students, Future Students, Parents, and Parents of Future Students. A user must have a Staff or Division Head role before being given this role.

Impersonate Admissions Families

This role allows users to Applicants, Prospects, and Parents of Applicants/Prospects. A user must have a Staff or Admissions role before being given this role.

Impersonate Faculty

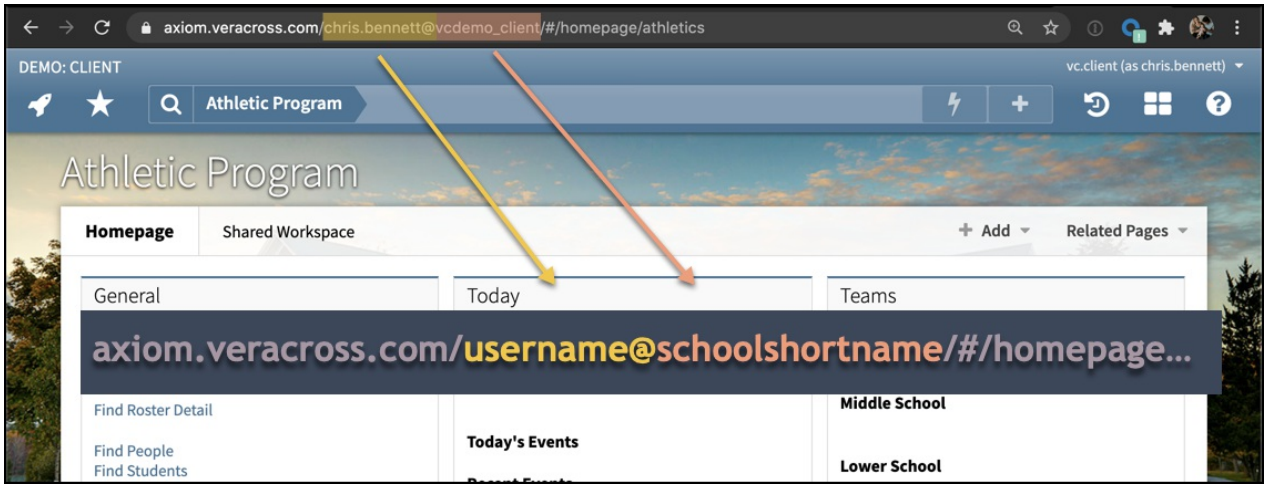
This role allows users to impersonate Faculty. A user must have a Staff or Division Head role before being given this role.

Using Impersonation

Using impersonation is simple. As long as you have permission, you can log in as another user by entering your credentials in the following format:

```
username: your_username/their_username
password: your_password
```

That is to say, in a username field, enter your username, followed by a forward slash, followed by the username of the person you wish to impersonate. Use your own password. Assuming you have permission to impersonate that user, you will be logged in as that user. Note that schools using Active Directory integration must log in with each user's full username (i.e. john.smith@veracross.com rather than john.smith) in order to successfully log in with user impersonation.



Additionally, you an impersonate a user by directly manipulating your URL. Before your school's short name, insert the username of the person you want to impersonate, followed by an "@" symbol.

Impersonating Users with Multiple Roles

This applies primarily when you impersonate a faculty member who is also a parent, but only have permission to impersonate either faculty or parents. In that case, you will not be able to access the portal for the role you do not have access to. For example, if John Smith is a faculty and parent, and you only have permission to impersonate faculty, you will not have access to John's parent portal.

Audit Log of Impersonation Records

AUDIT LOG

Update Date	Field Updated	Old Value	New Value	Update User	Update Machine
10/26/16 15:35:49	>> Dependent Role Removed (Required Staff_1) ...		Impersonate_Current_Families	@jfraser	axiom2.dfw
10/26/16 15:35:49	*** Security Role Removed ***		Staff_1	@jfraser	axiom2.dfw

Impersonation-related Security Roles requires the user to have one or more prerequisite roles (*Staff_1*, *Division_Head_3*, etc., as detailed above). Removing a prerequisite role automatically removes dependent roles with it, which is logged in by the system.

Additionally, changing who is being impersonated without signing out and back in is recorded in the Login Log (even thought it's not a "login"), and there are two new result values: Impersonation Allowed and Impersonation Denied.