UCTrust Names and UC GRLN Policy FAQ

The UCTrust group has agreed to release only Lived Name information to applications that leverage the systemwide SSO services outlined in the UCTrust SSO integration process. This page provides answers to frequently asked questions about the UCTrust SSO use of Lived Names and how we think it can help applications comply with the UC Gender Recognition and Lived Names policy.

Note: This information was shared with the ITLC (system-wide CIOs) in March of 2023, and no objections or concerns were raised by that group to this approach for supporting the UC GRLN policy for UCTrust SSO-enabled applications.

FAQs

What is the UCTrust practice for Lived Names?

All name values released via UCTrust SSO will contain a user's Lived Name information. Conversely, there is no support for providing Legal Names to applications through the UCTrust SSO process.

Note: This does not prohibit a location from storing and managing Legal Names in support of local SSO implementations, This practice only applies to systemwide UCTrust SSO-enabled applications.

Why was this defined as a formal practice?

Prior to formalizing this practice, it was unspecified what “name” information (Legal, Lived, etc.) was provided as part of the UCTrust SSO login process when name information was included. Without this clarification, applications leveraging UCTrust SSO could not make an informed assessment of how they are complying with the UC GRLN policy.

Why was Lived Name chosen over Legal Name?

In most cases, the UC GRLN policy requires applications to use and display a person's Lived Name rather than their Legal Name. Releasing Lived Name information via UCTrust SSO will - hopefully - simplify compliance with the UC GRLN policy for UCTrust SSO-enabled applications.

Why is Legal Name not an option via UCTrust SSO?

First, by only providing Lived Name via UCTrust SSO, there should not be any confusion about which name is being made available to applications,

Second, by only providing Lived Name, we avoid the need to create a systemwide approval process for granting exceptions for any applications requesting Legal Name information from locations.

Finally, several locations plan to only store Lived Name information in their local user profiles. This means the Legal Name won't be available from these locations *even if* an application has a valid reason to request it.

What UCTrust SSO name values are affected by this agreement?

This practice affects the following standard UCTrust data elements

- *first name (aka givenName)*
- *last name (aka sn)*
- *full name (aka cn)*
- *displayname*

Note that email address and other identifiers might include all or part of a person's actual name. This practice statement only applies to the four name fields listed above. UCTrust will rely on locations to take actions locally to ensure that these additional account identifiers comply with the GRLN policy.

How can an application be sure the UCTrust SSO “Lived Name” is accurate for a user?

The GRLN policy defines a location's responsibility for collecting Lived Name information from its constituents. UCTrust presumes that each location will collect and maintain Lived Name information in compliance with these requirements, and does not specify any additional expectations about how the data is collected.

This UCTrust practice specifies that whenever a location has received/collected a Lived Name for a user, the UCTrust SSO information sent to applications will include that Lived Name rather than the user's Legal Name. UCTrust does not define any special treatment for handling users who have not specifically provided a Lived Name, and again defers to the location's GRLN implementation. (Practically speaking, it is likely that if no separate Lived Name has been collected for a user, that person's Legal Name will be treated as their Lived Name.)

How can a UCTrust SSO-enabled application comply with the GRLN policy?

During the login process, a UCTrust SSO login message that include "name" information will always provide the user's "current" Lived Name during the login. If an application updates its users profiles when they login, the user profile will always have up to date Lived Name information for those users.

This approach to compliance with the GRLN policy was shared with both the the GRLN policy owner (Graduate, Undergraduate and Equity Affairs) and the system-wide CIOs (via the Information Technology Leadership Council - ITLC) in the spring of 2023, and no objections or concerns were raised by either group.

What happens if a user's Lived Name changes (outside of my application)?

Lived Name data provided via UCTrust SSO is only sent during an active user login. This means that through SSO, applications will only receive Lived Name information that is current as of the user's last login. If a user changes their Lived Name designation at their location *after* logging into an application, the application will not receive the updated Name information until the user next logs in to that application.

This is a limitation of using SSO to transmit user information. UCTrust does not support any other mechanism for directly communicating this kind of user "name" information to applications.

My UCTrust SSO-enabled application requires Legal Name information. What should I do?

Because Legal Name information will not be available, if your application requires official Legal Name information for its users, you will need to find a different way to collect this information. Example approaches might include prompting the user to provide a Legal Name within your application, or working with alternate source systems (like UCPath or a campus Student Information System) to collect this information.