Registry Authentication Events

Registry records *Authentication Events* whenever a login to the application occurs. Authentication Events are tied to the *authenticated identifier*, which is typically the value of `$REMOTE_USER`. For interactive logins, this usually, but not always, correlates to a login Identifier. For API logins, this typically correlates to the API username.

Administrators may view Authentication Events via the Identifiers list of the Person Canvas. Login Identifiers will have an *Authentication Events* link as an available action.

Because Authentication Events are tracked by authenticated identifiers, they are not bound to any specific CO (AR-AuthenticationEvent-1). For an identifier registered in multiple COs, it is not possible at login to know the intent of the authenticated user, and as such which CO the event should be bound to. As a result, a CO Administrator may view all Authentication Events associated with any authenticated (login) Identifier associated with any Person within their CO (AR-AuthenticationEvent-2). Similarly, a Privileged CO API User may retrieve all Authentication Events associated with any authenticated (login) Identifier associated with any Person within its CO (AR-AuthenticationEvent-3).

ⓘ Because Authentication Events are not part of any CO, they are never deleted from the database, including (for example) if the CO is deleted. (AR-AuthenticationEvent-4)

See Also

- Registry Table: authentication_events
- Authentication Event API v2
- Registry Identifiers