Authentication Events

Beginning with Registry v2.0.0, authentication events are recorded for logging and audit purposes. The following types of events are recorded:

- API Login: Access to the REST API v1 by an API User
- Registry Login: Access to the Registry UI by an identifier flagged for login

Authentication events are recorded by authenticated identifier (ie: $REMOTE_USER), which may correlate to zero or more Organizational Identities, which in turn may correlate to zero or more CO People.

To view authentication events associated with an individual's identifier, find the appropriate Organizational Identity, then select the *Identifiers* tab. Select *Authentication Events* for the appropriate identifier.

> Because identifiers can be registered in multiple COs (if organizational identities are not pooled) or are implicitly available in all COs (if organizational identifies are pooled), and because a login event is not correlated to a specific CO, any CO administrator with permission to view authentication events can see all authentication events for an identifier visible to the CO, even if the user intended to login for access to another CO to which they happen to belong. The Registry log records will not indicate which CO was accessed (though web server logs may hold this information).

Platform administrators may view the entire authentication event log via *Platform* >> Authentication Events.

See Also:

- Understanding Registry People Types
- cm_authentication_events