CO Unique Identifier For Applications

Recommendation

We recommend that each CO configure at least one identifier assignment in order to create a unique identifier for each CoPerson in the CO that can be provisioned to and consumed by federated applications such as wikis, mail list managers, and domain specific applications.

The advantage of having federated applications consume the unique identifier and use it as the primary identifier or key for the user is that even if a user's organization changes, and hence her federated eduPersonPrincipalName (eppn) changes, the new eppn can be linked in COmanage Registry to the existing CoPerson record and the same unique CO identifier can continue to be provisioned to the application so that the user does not lose access to the application during the transition from one home organization to another.

Often the unique identifier is provisioned to LDAP using the Registry LDAP Provisioner and then either the application is configured to consume it directly from LDAP or a SAML attribute authority (AA) is configured to resolve it from LDAP and then the SAML service provider (SP) for the application queries the AA to consume the identifier.

Since some applications, particularly legacy applications, have specific requirements for user identifiers (eg. the identifier must take the form of an email address but can only have 8 characters) it is fairly common to configure more than one CO unique identifier assignment to support a mix of general and specific application requirements.

Example

The CO administrator for the TestCO configures an identifier assignment so that each user in the CO is assigned an identifier of the form `testcoXXXX` whe re XXXX is an integer, starting at 1000 and assigned sequentially as users are enrolled in the CO.

Mandeep Kamala, a graduate student at Big University, later enrolls in the CO and is automatically assigned the identifier testco1241. Mandeep's eppn is mandeep.kamala@biguniversity.edu and that eppn is recorded during her enrollment to her organizational identity record that is linked to her CoPerson record. The TestCO wiki, however, is configured to consume testco1241 as the primary identifier for Mandeep.

Later Mandeep defends her thesis, graduates, and becomes faculty at Small University where her new eppn is mkamala7@smallu.edu. Mandeep executes a Registry identity linking enrollment flow and links her new organizational identity record with eppn mkamala7@smallu.edu to her existing CoPerson record.

The next time Mandeep accesses the wiki the SP queries the AA using her new eppn mkamala7@smallu.edu and the AA returns the same identifier testco1241 because her same CoPerson record is linked to her new organizational identity. Mandeep's access to the wiki is the same and continuous even though she has transitioned from Big University to Small University.

See Also

- voPerson