

User Provisioning and Authentication for the SumTotal Learning Management System at the University of California

(8/14/2007)

In the context of user provisioning and authentication, deployment of the SumTotal Learning Management System at UC will be accomplished in two phases. Phase 0 will support system-wide courses for employees only (as defined by the University's payroll systems) and will require no technology implementation by the campuses. Phase 1 will also enable local courses, incorporation of non-employees, and enhancement of employee data with information not available from UCOP.

Phase 0 (System-wide training only, employees only, PPS-originated user data only)

In Phase 0, UCOP will provide user data to SumTotal on a regular basis from UCOP-based systems that, in turn, receive their original data from campus payroll (PPS) systems. This data will include randomly-assigned passwords. Employees' UCnetIDs will be used for the SumTotal userID. Users will not need to know their userIDs and passwords, however, as announcements of classes will incorporate that information in a unique URL that will be sent to each person taking a course.

A detailed description of the Phase 0 data provided to SumTotal will be provided in a separate document.

Phase 1 (Incorporation of local training, non-employees, and enhanced user data)

In Phase 1, UCOP will continue to provide the user data it did for Phase 0, and the URL-based authentication will continue to function.

Also in Phase 1, UC campuses can enhance the user data being sent to SumTotal in two ways:

- The campus can add users who are not employees. The UTrust attribute *UTrustCampusIDShort* will be used as the identifier for those users.
- Certain additional fields can be added to the employee records provided by UCOP.

Each UC location that wishes to enhance its user data provides a file to UCOP that will be merged with the Phase 0 data and enhanced data from the other UC locations and then forwarded to SumTotal. Note that more than one feed from a UC location will not be supported. In particular, campuses and their associated medical centers will need to merge their data before sending it to UCOP.

The detailed content and format of the enhanced user data files will be described in a separate document.

Finally, Phase 1 will provide three additional options for user authentication:

1. **UTrust.** UTrust / InCommon is the preferred authentication method for Phase 1. *UCnetID* will be the attribute that is used to identify employees, and *UTrustCampusIDShort* will be used to identify others. The level of assurance required is the proposed *UTrust Campus*, as contained in the *UTrustAssurance* attribute. If both *UCnetID* and *UTrustCampusIDShort* are provided, then *UCnetID* will be used. Initially, SumTotal will implement an Attribute Acceptance Policy (AAP) that accepts *UCnetID* and *UTrustCampusIDShort* from the UC members of InCommon. Once the *UTrust Campus* level of assurance is implemented, the AAP will be modified to filter assertions on the value of *UTrustAssurance*.

2. **Some Other SumTotal-Supported Single Sign-On Integration.** SumTotal supports a variety of methods for integrating with local Single Sign-On (SSO) systems, including LDAP, Active Directory, and a web-based interface using MD5 that can be adapted to any local SSO. If it is necessary to integrate with a local SSO before UTrust has been implemented at a location, then that location can negotiate with SumTotal to implement that alternative. In order to integrate with the other data provided by UCOP, however, it will be necessary to make *UCnetID* or *UCTrustCampusIDShort*, as appropriate, the userID provided to SumTotal by the SSO.

While SumTotal supports a variety of authentication methods, their MD5-based method is preferred. It may require somewhat more implementation by the campus, but it does not expose user-typed campus passwords to SumTotal (which invokes provisions in IS-3 that would need to be addressed). Also non-MD5 options may be delayed in the implementation schedule, due to time constraints.

3. **SumTotal Basic Authentication.** The userIDs and passwords created in Phase 0 may be used to provide access to local courses. While SumTotal servers will perform the authentication, and UCOP will provide the userIDs (i.e., the UCNetIDs) and passwords to the location, it will be the location's responsibility to manage the distribution of the Phase 0 userIDs and passwords to its community.

Phase 1 can be summarized in the following diagram.

