cnet authentication for hospital

Status & Issues for CNet Authentication of Hospital People

Following are some pertinent facts about the state of integration between CNet authentication and UCHAD, the UC Hospitals Active Directory, which is used by people engaged in the University's clinical activities.

In May 2008 UCHAD IDs became usable to access CNet protected applications. As a result, it is no longer necessary for a person issued a UCHAD ID to also get a CNetID in order to access CNet protected resources.

In March 2010 CNet IDs became usable to access UCHAD protected applications. As a result, it is no longer necessary for a person issued a CNetID to also get a UCHAD ID in order to access UCHAD protected resources.

It remains necessary for a person to be authorized to use a UCHAD- or CNet-protected service. The ability to login is necessary but not sufficient to make use of the service.

LDAP entries for UCHAD accounts

Entries for UCHAD accounts have been added to LDAP alongside those for CNet accounts. This enables applications that rely directly on LDAP for authentication to also authenticate UCHAD users, as well as other authentication technologies that indirectly rely on LDAP for authentication, namely, Shibboleth and RADIUS.

Many people who were issued accounts before the integration of UCHAD and CNet authentication were issued both a UCHAD and a CNet account. If a person has both CNet and UCHAD accounts, only their CNet account appears in LDAP. Hence, people with both a CNet and a UCHAD account must use their CNet account to login to CNet-protected services, but people having a UCHAD account and no CNet account can use their UCHAD account to login. This may be confusing to people having both types of accounts, although no worse than what they have always been used to: they need to know when to use which account.

Occasionally a new UCHAD account is not automatically represented in LDAP due to various issues. When these cases arise IT Services works with CBIS to fix them.

One way to validate that a given person's UCHAD ID is usable via CNet authentication is to have them go to http://whoami.uchicago.edu. They will be asked to authenticate, and if successful, it will show them a few facts about themselves.

UCAD and UCHAD

As of 19 March 2010, the two UCAD domains, adlocal and ad.uchicago.edu, trust the UCHAD Active Directory domain, and vice-versa. This means that UCAD users can lookup UCHAD users and put them into UCAD groups or access control lists, and UCHAD users can access UCAD-protected applications and resources.

The best way to maintain a UCAD group to which both CNet and UCHAD user accounts belong is to use Grouper, the CNet access management service.

Affiliation "hospital"

Having a UCHAD account is not the same as having a "hospital" affiliation. There are many UCHAD account holders that are "staff," for example, because their payroll is run by the folks in Hyde Park but they are engaged in clinical activities. People in the "Employee Business Group" in the Oracle HR system operated by UCMC have "hospital" affiliation. There are some UCHAD account holders that have no affiliations, eg, some consultants employed by UCMC that are given UCHAD accounts. And there are some CNet accounts with a "hospital" affiliation.

UCHAD account holders wanting to claim a CNetID

If a UCHAD account holder says they want or have been told to get a CNetID for any purpose, they should be advised to try using their UCHAD ID. It will be a long time before everyone realizes and gets used to the new reality in which either a UCHAD or a CNet account can be used to get to all services a person is authorized for.

It is not possible for a person with an active UCHAD account to claim a CNetID by normal means. This would be a disservice to the user and makes it more difficult to manage their access to services and to provide IT support to them.

Going from a username to an email address

Some systems rely on the assumption that an email address for a user can be formed by tacking on "@uchicago.edu" to their username. This has been true for usernames that are CNetIDs, and as of 23 February 2009 it is also true for usernames that are UCHAD IDs. Each UCHAD account represented in LDAP has its corresponding uchospitals.edu mailbox as the "mail" attribute.

Who can access what?

Services that merely require a valid CNet authentication to gain access now also allow UCHAD account holders to access them. When mere authentication is not sufficient to authorize a user's access, many applications refer to the list of the user's affiliations to decide whether to let them in. With UCHAD accounts now valid in CNet authentication, many more users having "hospital" affiliation are now able to authenticate to applications than were able to in the past, which raises the question of which services are configured to admit users with a "hospital" affiliation.
There are several general principles that we should try to follow. First, UCMC has a mature suite of user services, and we want to be careful to not inadvertently make a duplicate NSIT-operated service available to those users. Second, we want to be mindful of the added burden and costs to NSIT of enlarging the usership of key services that are already provided freely to many types of affiliations. And third, we want to be equitable in the services offered generally to the U Chicago community and mindful of the incentives or disincentives that offering a service, or failing to offer one, may have on distributed IT decision making.

Access to uchicago wireless and to webshare have interesting stories. At this moment, "hospital" affiliation does not entitle users to access uchicago wireless, pending determination by UCMC whether it is ok to use uchicago wireless to access clinical applications. In the meanwhile, hospital staff can use an existing workaround: associate with uchicago wireless, then fire up the UCH VPN client. UCH VPN is allowed to tunnel through uchicago wireless without prior CNet authentication. Note, however, that UCHAD account holders with a "staff" affiliation (a common situation for new BSD employees) can use uchicago wireless in the normal way, by logging in.

Hospital affiliation does not currently entitle users to personal webshare folders, although UCHAD authentication works with webshare and hospital affiliation does enable the user to fully exercise the access to materials on webshare they've been granted. So, for example, a BSD "staff" using a UCHADid can have a personal webshare folder without having to claim a CNetID.

Also see Who Can Access What for a more detailed and growing list of specific services.