Existing Campus Wireless Authentication

Existing Campus Wireless Authentication

Campus	Wireless Authentication "Portal"	Backend Authentication System	Information Requested of Guest Users	How Authorization Decision Is Made	Does your IdP assert the "member of community" affiliation? If so, how is it defined?
UCB	locally designed and supported web-based captive portal.	"CalNet": campus auth'n system based on Kerberos.	no information is requested of guests. a campus sponsor must create and distribute guest accounts; sponsor is responsible for collecting name and email or other information sufficient to identify and contact the guest.	guest accounts must be created by the faculty or staff member sponsoring the guest(s). guest accounts are ephemeral (1-7) days, may be refreshed (by sponsor) as needed. longer-lived accounts are available after review.	we do not currently assert "member of community," and do not have an official definition of "member of community."
UCD	Aruba	Kerberos	Name, e-mail, phone, and password are required. Title, organization and address are also requested. The sponsor must login to access the registration page.	Must be sponsored by a UCD faculty or staff member. The guest access is good for 7 days but may be renewed for up to 30 days.	Member is defined as current UCD Staff/faculty /student or long-term guest.
UCD HS	Cisco	There are 3 different networks. 1. Prod uses AD - Access to enterprise and Internet 2, Student uses AD - Access to Internet and selected resources, 3 Guest None - Internet only	None on guest, Name, email, last 4 SSN for prod and student	N/A for Guest, Staff Sponsor for student or prod	
UCLA	**UCLA_WEB** A non-authenticated SSID that provides HTTP/HTTPS/VPN access to external IP address space, and internal access according to individual department policies. **UCLA_WIFI** A web-based authentication portal using Aruba wireless controllers. This will be augmented with a locally developed web-based interface for Shibboleth authentication of wireless guests. Shibboleth has been demonstrated in our lab environment **UCLA_SECURE** A WPA2/802.11x SSID. The SSID will be renamed "eduroam" in the future. eduroam is now running in our lab environment.	RADIUS interface to UCLA Logon ID system	Name, e-mail address, and phone number of guest and sponsor	Faculty and staff may sponsor guest accounts via http://www.bol.ucla.edu/services/accounts/info/guest.html	UCLA defines "member" as current UCLA employees and students. For additional information, see UCLA's attribute dictionary entry on eduPersonAffiliation
UCR	Unencrypted: Cisco Webauth (with custom portal page), Encrypted: WPA2-Enterprise PAP	RADIUS to LDAP (via IDEngines Appliance)	Library guest users have unimpeded access; those who sponsor other guests must provide name, purpose, and lifetime of guest credentials.	(Does this question refer only to guests?) Anyone may use library guest wireless; other guests must be sponsored by faculty or computing staff; all other campus affiliates have access.	We do not currently assert this. UCR would define member as Student/Faculty/Staff. It is possible we'd later include Affiliate which is formally defined at UCR, tightly regulated and must be renewed every 6 months.
UCSD	Locally developed web based access for non WPA2 network using Cisco wireless controllers. 802.1x authentication for WPA2 network.	Our guest access, which has restrictive ACLs doesn't require strong authentication. The WPA2 network backends through RADIUS to Active Directory.	Email address, Accept AUP.	Anyone physically here can get on restricted guest. With WPA2 get unrestricted access. Note that our thought is to adapt the non WPA2 guest network to allow one to use InCommon to login to get unrestricted access. You still wouldn't be on a WPA network, so there are some security concerns there.	If you have an account, we consider you a member of community.
UCSC	Unencrypted: Clean Access capture portal. Planning to migrate to a new lightweight WAP solution in a few months that may replace Clean Access. Encrypted: WPA-Enterprise MS-CHAPv2	Unencrypted: RADIUS to Kerberos Encrypted: RADIUS to LDAP	Unencrypted: Portal Guest button offers limited functionality to wireless. Divisions/Users may request temporary sundry accounts. Encrypted: No guest access today	Guest button is automatic. Campus account management team grants sundry accounts. Note: Sundry accounts provide access to more than just campus wireless.	We do not currently assert this value.