UCAR Visitor Wireless: How it works

The UCAR Visitor wireless network (SSID) is an open, unencrypted wireless network that uses a "captive portal" to require registration before full access is enabled. The registration form is displayed on devices by redirecting web browser requests to authentication servers. Most newer operating systems will detect the presence of a captive portal and immediately pop open a login page. In the remainder of cases, an unregistered user is redirected when attempts are made to browse the web.

Once the registration page is adequately filled in and "Register" button is clicked, the device will have four hours of access. At the same moment, a registration email containing a link is sent to the email address entered on the registration form.

Here's the registration page users see when first accessing the network:
Upon submission of the form, the user should soon receive an email that looks like this:

Wireless access request from: dialp@ucar.edu

Clicking the "click-here" link in the confirmation email opens a receipt page confirming the 90 days of access, but the user must click the "Confirm" button here to complete the process:

Visitor Registration Confirmation

A guest has requested your confirmation for guest access
If the device's MAC address is in the list of devices known to have been on UCAR Internal in the last 90 days, the user will not be permitted to register their device on UCAR Visitor. Instead, they will see a pop-up page like this one, indicating that they can use UCAR Internal network or launch their UCAR AnyConnect VPN:

![Pop-up page](https://clearpass.ucar.edu/guest/employee_device.php?c...Fcaptive.apple.com%2Fhotspot-detect.html&_browser=1)

For more information on the UCAR Visitor wireless network, please see the [UCAR Visitor Wireless FAQ](#).