

Campus Technology Services
Juniata College
814.641.3619
help@juniata.edu
<http://services.juniata.edu/cts>



WIRELESS NETWORK SECURITY

06/10/04 AMW

In an effort to allow further access to network resources, Network Services has extended services beyond the traditional copper and fiber connections through the integration of wireless networks. Upon the decision to integrate wireless on a wide-scale, security measures were taken to protect user integrity and privacy. With the current configuration users must first be authenticated via VPN before obtaining access to EagleNet. VPN provides a very secure tunnel through which data may then flow. Without this secure tunnel EagleNet is vulnerable to attacks from any computer with a wireless network adapter.

Because of this security risk it is imperative that each and every wireless access point attached to EagleNet be secured. The current method of security requires special configurations in the network closets of each building providing wireless access. Because this security may not be administered by the end-user, the use of wireless access points without the permission of computer network support is strictly prohibited.

Remember that services may not be extended or retransmitted according to the policies agreed upon in the **Ethical and Responsible Use of EagleNet** document <http://services.juniata.edu/cts/forms/EthicalUse.pdf>.

Juniata Network Services staff reserves the right to scan buildings for wireless access points. If a non-campus-owned access point is found, Network Services will disconnect the port servicing that wireless access point.

Guest Wireless access is available in specific areas to support connectivity needs for guests of the college. This service is only intended for guests who are on campus attending specific college functions or using specific college services other than Internet connectivity.