Connecting Securely to University Data

Syracuse University's Virtual Private Network (VPN) service enables students, faculty, and staff to access online University information resources and services from off-campus locations in the most secure manner possible. VPN builds an encrypted, virtual tunnel from a client's computing device to the University's network and, by doing so, protects the privacy of the data that is exchanged over the Internet between the device and the SU network.

All faculty and staff who access SU enterprise and confidential data from an off-campus location using unmanaged machines are required to use the University's VPN system.

How to Connect to VPN

Microsoft Windows computers: Syracuse University Remote Access(SURA) is a tool that automatically configures a personal computer to securely connect to University resources via VPN. SURA can be used instead of the older Windows VPN configuration tool.

Macintosh Computers: Students, faculty, and staff who own a Macintosh computer can continue to use the VPN configuration tools that are available on the ITS Web site downloads Web page.

Important Note: "Suite" security software packages that offer multiple security features may also pose a compatibility problem with the VPN service. If so please contact ITS Help Desk for assistance

ITS recommends that clients install only antivirus software and spyware detection packages on their personal computers instead of full-service security suites. Additionally, the Microsoft Windows firewall yields better results with SU's VPN than third-party firewalls.

Students, faculty, and staff who use the following computing services to manage files from off-campus locations will be required to access these services using VPN:

- Remote desktop applications
- FTP services (File Transfer Protocol)
- SSH services (Secure Shell services)
- Netware file sharing