Getting started with the Fredonia Virtual Private Network (VPN) Services

Fredonia provides SSL Virtual Private Network ("VPN") Services for employees to remotely and securely perform their work related duties as necessary in accordance with applicable policies and regulations. The SSL VPN Services are designed to minimize the potential exposure to Fredonia from damages, which may result from unauthorized use of Fredonia resources. Damages include the loss of sensitive or University confidential data, intellectual property, damage to public image, damage to critical Fredonia internal systems, etc. This VPN Service is required to remotely access your University computing resources (e.g. Desktop Computer).

Fredonia allows remote access when there is a clear, documented business need. Access may be allowed from State-issued or personally-owned devices, at the discretion of the Fredonia Information Security Officer or designee, and in accordance with the standards below. Such access must be limited to **only** those systems necessary for needed University business functions using the “Principle of Least Privilege.”

The Fredonia VPN Client enables remote users to access internal network resources through a secure tunnel delivered by the end-user installed Fortinet software. NOTE: If your device is not compatible with our VPN service, then please contact the ITS Service Center x3407 for additional options.

Services provided by the Client VPN include the following:

- Hypertext Transfer Protocol (HTTP)
- Hyper Text Transfer Protocol Secure (HTTPS)
- Virtual Network Computing (VNC)
- Remote Desktop Protocol (RDP)
- Secure Shell (SSH)
- Internet Control Message Protocol (ICMP)

Fredonia VPN Services are provided to allow approved employee access to campus-based electronic resources when remote work-related business functions are necessary. Employees with Fredonia VPN privileges understand and agree to the following:

- It is the employee’s responsibility to select, coordinate the installation of, and pay the associated fees for high-speed internet connectivity via a local Internet Service Provider (ISP).
- It is the employee’s responsibility to ensure that unauthorized users are not allowed access Fredonia internal networks via the VPN.
- VPN use is controlled using multi-factor authentication.
- Support and connectivity issues related to VPN access are provided by the ITS Service Center.
- VPN accounts will be annually audited and users no longer requiring VPN access will have such access removed.
- Access may be allowed from either state-issued or personally-owned devices. Such access must be limited to only those systems necessary to meet the required remote business functions.

Getting started with the Fredonia VPN Web Service

1. Fill out the online Fredonia Virtual Private Network (VPN) Service Request.
2. After the Fredonia VPN Service Request has been completed, the Information Security Office will provision access to your Fredonia eServices account to access vpn.fredonia.edu. After this access has been provisioned, users may obtain assistance by contacting the ITS Service Center (716) 673-3407 or tracker@fredonia.edu.

*****NOTE: ALL university owned laptops should have the FortiClient VPN service already installed on the machine.*****

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Fredonia's Remote Mac Computing Lab
- Zoom
- Fredonia's Virtual Windows 10 Computing Lab
- Getting started with the Fredonia Virtual Private Network (VPN) Services
- How to setup the Client VPN Service for Mac OS X