Maynooth University myVPN Service

Introduction

The myVPN (Virtual Private Network) Service permits staff to connect securely to the Maynooth University's (MU) internal network when off-campus.

This document outlines the process in which a staff member can gain off-campus access to systems which are usually only accessible on the University's network.

Any other MU account holder who needs VPN access is required to provide approval from their Head of Department.

All users of this service are required to have a secure complex password.

Service Description

All users of this service are responsible for providing their own Internet connection.
Once connected to the Maynooth University internal network over myVPN, access to all resources will be as per working on campus.
IT Services are not responsible for any latency or other issues encountered when accessing resources or applications over myVPN. The myVPN service only provides access to the internal MU network and as such has no control over internet connectivity issues or incompatibility software problems.

An approved operating system (Linux, Windows 7 and higher, and Mac OS X) is required; with sufficient resources available to install and run the client software. The device you are using for remote access must have sufficient protection in terms of malware protection, an up to date OS and any application patches.

The myVPN service must only be used for University related purposes.

Security Considerations

Users of this service, must abide by the Code of Conduct for Users of Computing Resources

- The myVPN service requires Two-Factor authentication, this two-factor authentication is provided by Domain Username/Password combined with Google Authenticator

- Caution should be exercised when accessing any University system or application on an untrusted network. Account holders should not use the myVPN service when accessing confidential systems or sensitive University information on untrusted networks e.g. Open Airport Wi-Fi, Internet Café's, Open Access Hotel Wi-Fi etc.

- If you think your account has been compromised in any way, you should contact IT Services immediately. In the event of the device that are using for the google authenticator is lost or stolen, please contact the IT Services as this can be reset.