Introduction

Why

After the recent increase in hacker activity and floods of phishing emails, it is clear that the Observatory Compute environment is under constant attack. One of the major deficiencies in our current setup is that it is enough to know a username and password to get access to a wide variety of resources and data. With the improper handling of phishing emails, but also when using public wifi services, it seems easy for people with not so good intentions to get account credential information. After that, there is no easy way to prevent misuse of accounts and computer resources.

We need to put a stop to that, and the only way to do that is to introduce a second step in identifying that you are the rightful owner of the account credentials. This second step is provided throught the Two-Factor Authentication (2FA) mechanism. For this second verification, you need a physical device, for instance a smart phone or personal computer.

Where

In principle for every service where you need to identify yourself, 2FA is needed. In the beginning we will restrict 2FA to two major services: Web pages and ssh remote login. At a later stage 2FA will be implemented for other services as well. You will be informed well in advance.

WEB Pages & 2FA

For all Web pages where you need to login, we will enforce 2FA. This also, and in particular, includes webmail. The Observatory WEBsite has many pages shielded by authentication and each page will be individually added to the 2FA facility.

ssh remote login & 2FA

One other major way to gain access to our resources and data is through the ssh protocol. So this means that using `ssh` to login from remote to the Observatory ssh gateway or to the local desktops or servers, you will be confronted with a second prompt to enter credentials. How this works is explained later on this page. In fact, 2FA is imposed on the ssh protocol, so `scp`, `sftp`, remote `rsync` and even tunnelier (Win) will also be affected.

vpn & 2fa

For the purpose of accessing your home adn data share you used to access the physics ssh3 server. But, due to incompatibilities between the 2FA and automatic mounting of shares that way of accessing your shares will not be available anymore. The VPN facility replaces this functionality and allows your personal computer device to become part of the Physics network. Once that is the case you can mount your personal home and data disks in the usual way through the Windows File Explorer (or samba mount).

How

The 2FA protocol that we have implemented is based on the DUO (a Cisco product) software suite. Using DUO we have implemented two-factor authentication on web server, console login, remote access to your desktop, VPN and ssh.