Hawk Multi-factor Authentication Plans and User Guidance

This is an important document to inform you about upcoming plans to introduce Hawk Multi-factor Authentication (MFA) to improve Hawk's security by safeguarding its login nodes behind the University's Virtual Private Network (VPN).

Introduction

To enable MFA for Hawk, access from outside campus will from April 8th, 2024, mandate use of the University's Palo Alto VPN software client, in the same way that some of you may already access other services that are only available when using a machine connected to the campus network.

As a user of Hawk, please take the time to read the following three (3) sections to help you to prepare for this service change and to help us to minimise any service disruption.

1. What Will Change?

Accessing Hawk from off campus (anywhere else in the world) will first require the VPN client to be installed and enabled on your connecting host machine. The VPN service requires the use of MFA to authenticate connections. Once your VPN client is connected, you will then be able to connect to Hawk in the usual way, by either using an SSH client or the Open OnDemand web interface.

Instructions for installing and using the VPN client can be found on the Intranet.

Staff: Virtual Private Network (VPN) - Staff Intranet - Cardiff University

Students: Virtual Private Network (VPN) - Student intranet - Cardiff University

Additional points of note:

- Your Hawk specific login credentials will be unaffected by the change.
- Accessing Hawk from a computer on campus will be unaffected by the change.
- Cardiff University external guest users with external Cardiff accounts will connect to Hawk in the same way (with the VPN client enabled using their Cardiff external user credentials prior to connecting to Hawk). **ALL users will need to ensure suitable MFA sign-in methods are registered against their Cardiff University account. See Section 3 below for further instructions.**
- It is likely that the VPN will inhibit large data transfer (1TB+) performance to/from Hawk. A future dedicated SFTP only access route into Hawk is planned to support users with large data transfer requirements on request. Further details about this will be provided in due course.

2. When will the Change Take Place?

The change will be implemented on April 8th, 2024.

3. Important Preparation and Getting Help

MFA service specific access problems are managed by the IT service desk. Please note that current wait times to validate and resolve MFA lock out can take several weeks to fully resolve – although additional support is being sought to improve resolution times. However, please note that the overwhelming majority of such issues are preventable as long as users ensure registration of a suitable backup MFA sign-in method.

We strongly advise therefore, that you please check that you have at least two (2) sign-in methods registered where both methods are NOT solely dependent upon access to a single device such as a mobile phone.

This typically necessitates one of the following approaches.

- Having two (2) phones registered e.g., a mobile phone as well as a suitable landline phone (home/work). If you have a suitable landline phone, then this should be straight forward to register.

- Having the MS Authenticator App registered on an alternative device e.g., mobile device, computer (requires install and configuration of the authenticator web browser extension).

NB: A second sign-in method cannot be approved and registered without an existing working registered sign-in method, so it is important that you do not delay adding a second method. If you do not have a suitable backup sign-in method, then we strongly advise that you add one at your earliest convenience. Your MFA sign-in methods can be managed at: https://aka.ms/mfasetup

NB: Please be careful NOT to delete an existing sign-in method.

Instructions for setting up new sign-in methods can be found on the Intranet.

Staff: Setting up Multi-Factor Authentication (MFA) - Staff - Cardiff University

Students: Setting up Multi-Factor Authentication (MFA) - Students - Cardiff University

These methods include the following options.

1. An automated phone call (landline phone)
2. The Authenticator App (Instructions are provided for the Microsoft Authenticator App which is recommended although alternative authenticator apps should also work)
3. The Authenticator web browser extension

If you have any concerns or queries about this planned service change, please contact us at arcca-help@cardiff.ac.uk

It is essential that we improve the security of the current Hawk service.

Many thanks in advance for your cooperation.

Best wishes,

The ARCCA Team