IRIS Multifactor Authentication

Hardware Key FAQs

The following provides information about adopting a hardware key as an **alternative to** mobile device usage for IRIS multifactor authentication (MFA).

WHAT IS A HARDWARE KEY?

Hardware keys are physical devices that generate a six-digit code that an IRIS user can use to authenticate when signing into IRIS along with their email and password. Hardware keys are an alternative to a mobile device (e.g., cell phone or tablet).

IS A HARDWARE KEY RECOMMENDED BY IRIS?

While a hardware key is a viable alternative to using a mobile device, IRIS Support is only equipped to provide onboarding and ongoing technical assistance to IRIS users using MFA in conjunction with mobile devices. Therefore, **we recommend a mobile device as the primary method** for setting up and logging in to IRIS using MFA.

WHEN COULD A HARDWARE KEY BE A SOLUTION?

A hardware key is an alternative in instances when organizational staff are unable to use their personal mobile device (and a work-issued device is not available) to set up and manage their MFA connection in IRIS.

However, a hardware key is not meant to be the solution for users having trouble adapting to using MFA with a mobile device. Rather, this is the last option for those who wouldn't otherwise use IRIS due to device accessibility barriers.

WHAT SUPPORT CAN STAFF EXPECT FROM THE IRIS TEAM?

IRIS Support can offer only limited troubleshooting to staff using hardware keys. This means most users who reach out to IRIS Support requesting assistance with downloading, accessing, or troubleshooting their hardware key will be redirected to their organization's IT team.

WHO DETERMINES APPROPRIATE DEVICE USAGE FOR IRIS MFA?

Adoption of hardware keys should be driven by the organization and their needs.

WHAT HARDWARE KEYS ARE RECOMMENDED?

Your organization can select any hardware key that is compatible with Time-Based One Time (TOTP) MFA. A device that our team recommends, and which fits this criteria, is the Yubico Yubikey 5C.

WHAT DO STAFF NEED TO USE A HARDWARE KEY?

Staff will need a computer, the ability to download the hardware key software to that computer, the physical hardware key, and an IT team capable of troubleshooting and assisting with any issues that may come up as they use the hardware key.

HOW DO STAFF SET UP MFA USING A HARDWARE KEY?

If an organization chooses to adopt hardware keys, staff will need to do the following to set up the connection between the key and their IRIS account:

- Obtain a hardware key from their organization.
- Download the associated hardware key's software to their computer.
- Within the hardware key's software:
    - Add a new account.
    - Screenshot the QR code.
    - Follow any further instructions in the hardware key's software.

The connection between IRIS and the key is then set up. The key's software will start generating the six-digit code needed when authenticating a user's IRIS account. The key must be plugged into the computer to receive the authentication code.