Multi-factor authentication, or MFA, is a security measure that requires anyone logging into an account to use a two-step process to verify their identity.

MFA ensures that it is twice as hard for someone to access your online account without authorization. When it is available, always turn it on because it is not only easy to use but incredibly effective. Data shows us that over 99% of account hacks could have been prevented by use of MFA. Some examples of MFA can include an extra Personal Identification Number, answering security questions, a code emailed or texted to you, facial or fingerprint recognition, and more.

Video of What does MFA mean?

CU System uses Duo for multi-factor authentication, a core component of CU's identify and access management policy and cybersecurity strategy. You've already been using MFA every time you use Duo to access the VPN or specific applications. If your username and password were compromised, someone would still need to gain possession of your phone to verify the second factor of authentication. As more applications require MFS, CU System is moving to Smart MFA, which will eventually reduce the number of times you have to authenticate using Duo.

What is Smart MFA?

As more and more applications require Duo verification to access, UIS is exploring secure options to reduce the number of times users must authenticate.

Adaptive authentication, also known as Smart MFA, analyzes additional factors when a user attempts to log in and assigns a level of risk associated with that login attempt. For example:

- Where is the user who is trying to access information? Is the location different than normal?
- When are they attempting to access information? Is it during regular hours?
- What kind of device are they using? Is it different than the one they normally use?
- Are they on a private network or a public network?
Depending on the risk level calculated, the user may be prompted for an additional authentication factor, such as using Duo.

**How does Smart MFA work?**

For Smart MFA to assess the level of risk associated with a specific login attempt, it first needs to collect data and identify what is “normal” for the four questions outlined above.

Starting in **early October**, Smart MFA will begin collecting basic information, such as the location, time and type of device being used during the authentication process. When you authenticate using Duo, you may see a message letting you know that information is being collected. The following image may appear on your screen:

![Reviewing Authentication](image)

**How will CU System staff be impacted by Smart MFA?**

After enough data is collected, ideally by Oct. 25, you may notice a request to authenticate using Duo when accessing an application that previously only required a password.

Over time, as your device, location and timing are determined to be low risk, you may find that you are being required to authenticate much less often.