Introducing Multi-Factor Authentication for the SCO Enterprise Dashboard

As the Luma Project propels our State Government HR and Finance data onto a new path of technology, functionality, and collaboration, it also motivates our office to enhance the defense of that data, beyond what has been provided before.

With identity theft at an all-time high, the number of successful data breaches going up every year, and social engineering scams becoming more believable and widespread every day, it is time to make a considerable reinforcement to state employee authentication.

This reinforcement comes in the form of adaptive multi-factor authentication via a product known as **Cisco DUO Mobile.**

With the integration of DUO Mobile into the SCO Enterprise Dashboard sign-in, state employees will now have an additional *factor* of authentication beyond their StateID and strong dashboard password. An additional *factor* does NOT mean users must create another username and password, or information "like" a password, such as our present implementation of a security question and answer.

An additional factor means something you "have", rather than something you "know". DUO Mobile considers the thing that you "have" to be a personal device and/or private phone number. No SCO Enterprise Dashboard account may be signed into unless the user:

1. Knows the StateID and strong password

   AND

2. <u>Has</u> the personal device or private phone number in their possession

   This protects the user from Phishing schemes (since the perpetrator might get the StateID and password, but would not have access to the personal device) and from any breach due to personal device loss or compromise (since the perpetrator might have the personal device, but not the StateID and password).

Cisco DUO Mobile presents multiple methods of using a personal device and/or private phone number to provide a second-factor of authentication.

1. **DUO Verified Push:** This is the preferred method of second-factor authentication for users who want to use a Smartphone or tablet device, or any other device with an App Store and the ability to download the DUO MOBILE app, including smartwatches. To be utilized, the device used will need to be turned on and connected to a WIFI network or an active service provider data plan at the time of authentication.

   This option is the most resilient against technical weaknesses that allow attackers to steal passcodes in transit.

   In this case, the user will receive a push-based notification on their personal device, from the DUO Mobile app, and must verify that the push is from their own attempt to authenticate. This verification is done by displaying a 3-digit code on the browser, and the user types the 3-digit code into their DUO Mobile app screen, then tap “Verify” to authenticate. The user can also tap “I'm not logging in” to deny the authentication attempt which reports it to SCO ServiceDesk.

2. **DUO Mobile Passcode:** This is the next preferred method of second-factor authentication for users and can be used if you have registered and activated your smartphone, but you do not seem to be receiving DUO Pushes due to location or connectivity, and cannot take phone calls, the DUO Mobile passcode is a secure and acceptable method.

   In this case, the user opens the DUO Mobile App, taps the "Idaho State Controllers Office MFA" account, and a 6-digit code displays, that changes ever 30 seconds. The user enters the 6-digit code into the browser, and is authenticated.

3. **Text message Passcode:** This is the next preferred method of second-factor authentication for users and can be used if you only have a feature phone with a text plan.

   In this case, the user will receive a SMS/Text (with a passcode), then enter that passcode into the browser, and is authenticated .

4. **Phone Call:** This is the least preferred method of second-factor authentication for users and can be used if the personal device is:

   a. A feature-phone (non-smartphone);

   b. A smart-phone without a data or text plan;

   c. No personal device is owned at all, so a landline is used;

   In this case, the user will receive a call and must press a key on the phone call to authorize the authentication. The user can also press a key to report the call as potential fraud if they did not request it.

5. **Security Key:** This is an alternate form of authentication that involves the use of a USB-connected device that holds security information. It may be utilized if...

    a. The user cannot use their personal smartphone as an MFA device or a landline

    b. The user does not own a personal smartphone or have a useable landline

    The SCO recommends the use of Yubikey 5 NFS FIPS security keys, and can provide them to state agencies for purchase.

    State Employees can prepare in advance, by deciding which authentication method best fits their personal circumstances, bearing in mind that the methods above are listed in order of most preferred to least preferred.

- DUO Mobile does NOT offer email-based passcode verification, and it cannot be enabled.

Enrollment in Cisco Duo will begin in March 2021 and soon after be required to use it for accessing the SCO Enterprise Dashboard and Luma Applications. This enrollment will continue as an automated part of the State HR Onboarding process and will ensure the State Controller's Office grants access within 24 hours of any employee's HR processing at their agency of employment.

DUO Mobile device registration will be completed by the state employee on the first sign-in after enrollment. Thorough and illustrative documentation on device registration, sign-in methods, and what to do when issues occur will be provided on the SCO website prior to this time.

Please direct all questions to our IT support team by email (servicedesk@sco.idaho.gov) or phone (208-334-3100, Option 1).

This information will be enhanced periodically by our SCO Technical teams. For the latest version of this information, please check the SCO website.