Published on *University of Colorado* (https://www.cu.edu)

Smart MFA provides a double win for CU faculty and staff [1]

November 30, 2022 by ES & UIS Communications [2]

As cybercriminals continue their attempts to compromise the valuable data held within university systems, the University of Colorado has added the extra protection of multi-factor authentication (MFA) to all CU applications.

CU faculty and staff, used to using Duo for MFA when accessing the university VPN, now may encounter a similar MFA challenge when accessing CU applications that previously only required a password, such as Zoom and the employee portal. Smart MFA distinctly protects System Administration credentials, so campus affiliates and users without a System Administration account will not encounter it.

University Information Services chose to use Smart MFA because it provides an additional layer of security with a customer focus that avoids MFA fatigue. Smart MFA eventually reduces the number of times you must authenticate using Duo.

Toby Lutz, UIS assistant director of identity management, explained the concept of Smart MFA as “a set of thresholds that recognize anomalies and assess risk. When anomalies are recognized, you can still access the resource if you can meet the additional authentication challenge.”

Lutz said, “It’s a win-win solution. In addition to hardening CU’s security, Smart MFA provides better and more efficient usability, so that employees don't have to step up their authentication constantly.”

MFA fatigue isn’t just about the inconvenience or annoyance of having to take an additional step — it might lead a user to not give a request the attention it deserves or to absent-mindedly hit the “accept” button, even when they aren’t signing in. Push phishing attacks are a new cybersecurity threat wherein the attacker sends MFA requests repeatedly in hopes that the authentic user caves and accepts the request just to stop receiving push notifications. By reducing overall MFA requests, user fatigue can decrease, ideally causing users to pay more attention to each individual authentication request.

What is multi-factor authentication (MFA)?

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.

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 complete the second factor of authentication.

What is Smart MFA?

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?

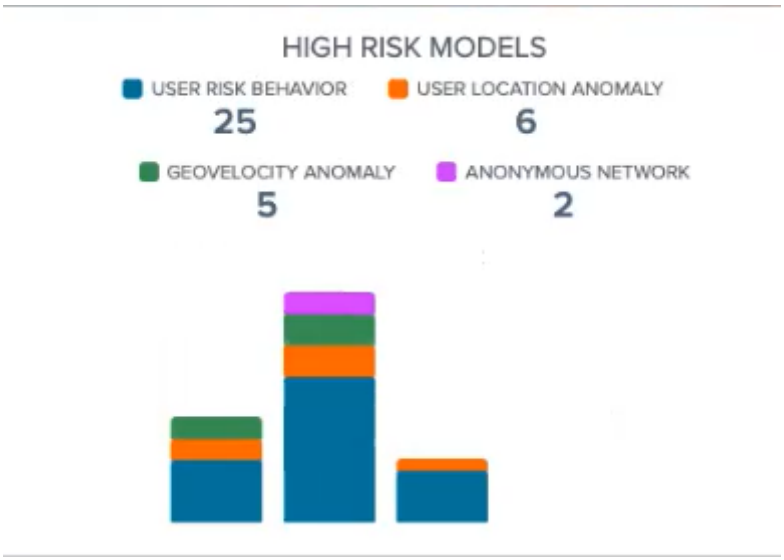
Depending on the risk level calculated, the user may be prompted for an additional authentication factor, such as using Duo.

How does Smart MFA work?

Smart MFA leverages the following predictors (below) to assess risk and predict threats to detect anomalies. The machine-learning model characterizes abnormal activity as low, medium or high risk.

The predictors include:

- Organizational risk
- User-based risk
- User velocity
- Anonymous network detection
- IP reputation
- IP velocity
- Geo-velocity anomaly
- User location anomaly



User-based risk

Smart MFA leverages user risk behavior and machine learning. It continuously learns the behavior patterns of users inside an organization by analyzing many data points, including the activity time frame, geolocation and operating system.

Using these data points, the machine-learning model characterizes abnormal activity as low, medium or high risk and prompts the user for the appropriate authentication action.

User Location Anomaly Model

Smart MFA supports a user location anomaly model, assessing whether user sign-on attempts originate from their usual location perimeter. Sign-on attempts originating from outside a user's perimeter are regarded as an anomaly and result in a high-risk score. The user location anomaly model enhances overall organizational security by increasing the user assurance level and reducing the risk of unintentional push notification approval and account takeover.

Anonymous network detection

Malicious actors typically use anonymous networks, such as unknown VPNs, Tor and proxies to mask their IP address. Smart MFA analyzes IP address data from a user's device to determine if the address is originating from any type of anonymous network. If so, the user can then be prompted for step-up authentication.

Geo-velocity anomaly

Users frequently sign on to the same application from multiple locations throughout the day. However, if a time lapse between the current sign-on location and the previous location is shorter than the time it would take to travel between the two points, it could indicate potentially suspicious activity. Smart MFA analyzes location data to calculate if travel time between two session locations is physically possible. If the elapsed time is calculated to be impossible, the user can be prompted with an authentication request or denied access.

A Smart MFA example

While traveling over a holiday, you may need to access the employee portal from a different device than you normally use, from a location far from where you typical work, outside of your usual hours. In such a situation, you should be prepared for an MFA challenge.

Likewise, if a cybercriminal was attempting to access CU's data and resources from a foreign country on an unfamiliar device, Smart MFA would immediately identify them as a high risk.

What can we expect to experience going forward?

Smart MFA will lead to fewer authentication requests using Duo.

Even when you access common applications in your normal work location during normal hours on your regular device, there will be occasional requests for you to authenticate using Duo — but much less frequently than without Smart MFA.

Cybersecurity at CU continues to evolve as attackers attempt to find new ways to gain fraudulent access. With your help, CU is committed to keeping your data and the university's assets protected.

Display Title:

Smart MFA provides a double win for CU faculty and staff
Send email when Published:
No

Source URL:https://www.cu.edu/blog/uis-news/smart-mfa-provides-double-win-cu-faculty-and-staff

Links
[1] https://www.cu.edu/blog/uis-news/smart-mfa-provides-double-win-cu-faculty-and-staff
[2] https://www.cu.edu/blog/uis-news/author/65709