EAB

RESEARCH BRIEF

# Multi-Factor Authentication

## Implementation of Duo Security at Large Research Institutions

# IT Forum

**Eric Ferguson**
*Research Associate*

**Daniel Gordon**
*Research Manager*

**LEGAL CAVEAT**

EAB is a division of The Advisory Board Company ("EAB"). EAB has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and EAB cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, neither EAB nor any of its affiliates (each, an "EAB Organization") is in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. No EAB Organization or any of its respective officers, directors, employees, or agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by any EAB organization, or any of their respective employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by any EAB Organization, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

EAB, Education Advisory Board, The Advisory Board Company, Royall, and Royall & Company are registered trademarks of The Advisory Board Company in the United States and other countries. Members are not permitted to use these trademarks, or any other trademark, product name, service name, trade name, and logo of any EAB Organization without prior written consent of EAB. Other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names, and logos or images of the same does not necessarily constitute (a) an endorsement by such company of an EAB Organization and its products and services, or (b) an endorsement of the company or its products or services by an EAB Organization. No EAB Organization is affiliated with any such company.

**IMPORTANT: Please read the following.**

EAB has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to EAB. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

1. All right, title, and interest in and to this Report is owned by an EAB Organization. Except as stated herein, no right, license, permission, or interest of any kind in this Report is intended to be given, transferred to, or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.
2. Each member shall not sell, license, republish, or post online or otherwise this Report, in part or in whole. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.
3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.
4. Each member shall not remove from this Report any confidential markings, copyright notices, and/or other similar indicia herein.
5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.
6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to EAB.

# Table of Contents



©2017 EAB • All Rights Reserved

# 1) Executive Overview

## Key Observations

**Institutional IT departments first deploy multi-factor authentication (MFA) to a small internal audience, such as IT security staff and senior administrators, before expanding to a broader audience.** Next, IT departments secure their virtual private network (VPN), enterprise resource management (ERP) system, and selected administrative systems. Profiled institutions prioritize these systems due to the quantity of sensitive data (e.g., student information, financial information, library resources) they contain.

**While IT departments are concerned with security when implementing MFA, each institution faces trade-offs between security and convenience.** For example, all profiled institutions except **Institution C** decided to enable Duo's "trusted device" feature, which requires users to authenticate via Duo less frequently when they use a specific device. While **Institution B, Institution A,** and **Institution D** all find the trusted device feature secure enough for their purposes, contacts at Institution C cite vulnerability to cookie hijacking as a key reason why the institution has not enabled the feature. Additionally, administrators at Institution C do not waive the second factor requirement even when the Duo service is interrupted, which maintains security at the price of usability in that rare circumstance.

**Profiled institutions implement Duo and single-sign on (SSO) on independent timelines. Institution A**, **Institution C**, and **Institution D** used SSO before selecting Duo as a vendor for MFA. Contacts at Institution A report that Duo provides clear instructions on how to integrate the service into SSO.

**Existing opinions about IT services affect how users react to a new service like Duo.** At **Institution D**, instructional faculty had been exempt from using MFA since the technology came to campus nearly a decade earlier. Faculty had opposed MFA then on the basis that it was a potential impediment to instructional quality. The same argument has resulted in the IT department pursuing an opt-in model with faculty for the foreseeable future. To mitigate this and other opposition (e.g., users not wanting to use their personal devices with Duo), profiled institutions launch extensive information campaigns, hold one-on-one talks about security, develop alternative deployment timelines, and set up tables around campus to help users activate Duo for their own accounts.

©2017 EAB • All Rights Reserved

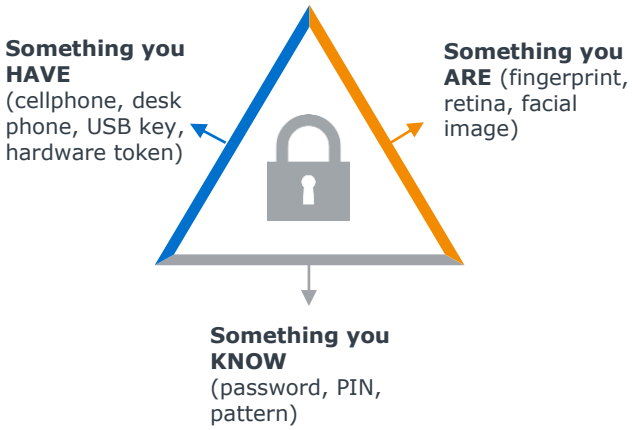
# 2) Technical Implementation of MFA

## MFA Overview

### Profiled Institutions Use Multi-Factor Authentication (MFA) Provider Duo Security

Multi-factor authentication (MFA) is a computing security system that requires users to provide more than one type of credential to log into an account. The credentials required can include a password, a fingerprint, a physical hardware device, or other information. Credentials fall into one of three categories: something you *know*, something you *have*, or something you *are*. Compared to a system that requires only one factor in one of these categories to authenticate, a system secured with MFA is safer in the face of hackers who steal usernames and passwords to gain unauthorized access to sensitive information.

**Three Types of Credentials**




Many higher education institutions in the US and Canada use MFA to secure their networks against phishing attacks and enhance overall IT security. Duo Security is one commonly-used vendor in the MFA space, currently in use at over 100 institutions. All institutions profiled in this report use the Duo service, and all except **Institution D** have deployed the service on an application-by-application basis.

### Multiple Authentication Options Provide Flexibility On and Off Campus

All profiled institutions also make hardware tokens available to users in case they cannot use other authentication methods.

Duo permits users to authenticate with a second factor in several ways: a push notification or software token generated through the Duo smartphone application, a text message, a phone call, and/or a hardware token. Profiled institutions prefer the app-based options because both rely on a user's pre-existing device. The app options allow institutions to avoid purchasing many expensive hardware tokens for users. It also circumvents charges from Duo that occur when a user requests a text message or phone call to authenticate.

©2017 EAB • All Rights Reserved

### Duo Authentication Methods and Sample User Types

**Push Notification**
- Students
- Connected staff and administrators

**SMS Text Message**
- Self-supporting students without data plan
- Smartphone users who prioritize simplicity

**Phone Call**
- Faculty member unwilling to use personal device
- Part-time staff member without smartphone

**Hardware Token**
- Researcher abroad
- Longtime faculty member without a cell phone

**Software Token**
- Administrator working via in-flight WiFi
- International student without a US cell carrier

The app-based push notification and software token options provide flexibility that the SMS text and phone call options do not. The app-based options ensure staff traveling abroad or in areas with poor cellphone reception can still authenticate when signing onto the institutional network remotely. Like the hardware token, the smartphone application can generate login codes even if the phone has no network connection.

Some institutions lower security expectations for off-campus populations (e.g., retirees and consultants) using institutional resources. Contacts at **Institution A** do not plan to require MFA for retirees due to that population's limited proficiency with technology. However, **Institution B** requires retirees to activate Duo, and contacts suspect that the culture around information security will soon change to a point where most users will intuitively understand the importance of MFA.

## Implementation and Re-Authentication

**Institution A** deployed to VPN users first in part to capitalize on their above-average technical proficiency.

### Prioritize Applications for MFA Based on Security Impact

Administrators at **Institution B** recommend deploying Duo to applications according to security implications. Both Institution B and **Institution A** first deployed Duo on their virtual private network (VPN), since potential attackers could use the networks to gain access to the suite of institutional resources available to faculty, students, and staff. Profiled institutions also prioritize data centers, ERP platforms, and single sign-on services for Duo deployment.

An institution's ability to prioritize specific applications when deploying MFA depends on both the population required to use MFA and whether the institution uses a single sign-on (SSO) portal. Because administrators at **Institution D** placed much of the institution's online resources behind a Shibboleth SSO portal, IT staff had to deploy Duo to those resources in one "big bang." However, instructional faculty and staff can log in without using MFA due to exception rules built into the SSO portal logic.

©2017 EAB • All Rights Reserved

**Duo Implementation and Re-authentication Requirements at Profiled Institutions**

| Institution Name | MFA Rollout Sequence | Future MFA Plans | Re-Authentication | Notes |
|---|---|---|---|---|
| **Institution A** | • VPN<br>• SSO | • Banner ERP<br>• Self-service portal<br>• Library access | • Each time logging into VPN service<br>• Seven days per trusted device for SSO | • Still working out bugs in Office 365 integration<br>• Open to extending the trusted device timeout if faced with user pushback |
| **Institution B** | • VPN<br>• Banner ERP<br>• Portal<br>• SSO | • Box | • Every seven days on trusted devices-not yet active | • MFA deployed to all user groups |
| **Institution C** | • Data center | • ERP service<br>• SSO | • Not currently using the trusted device feature | • Concerns about cookie hijacking have prevented activation of trusted device |
| **Institution D** | • SSO portal | • Opt-in model for MFA | • Every 4 hours-extended to 12 soon | • No plans to require student use of MFA |

## Shorter Re-Authentication Periods are More Secure, but May Provoke Pushback

When IT administrators introduce MFA, they must decide how long a user can access a system before they are forced to re-authenticate. While shorter re-authentication times (e.g., four or twelve hours versus a week or more for trusted devices) are more secure, shorter times require users to log in more frequently. This can feel like a hassle to users accustomed to single-factor authentication. In some cases, user pushback can impede institution-wide rollout of MFA. For example, instructional staff and faculty at **Institution D** cited the additional time taken by MFA as an unnecessary impediment to the teaching and learning process. These groups remain opposed to MFA despite IT administrators' efforts to convey the security benefits of MFA.

IT leaders must also consider how to integrate Duo into a single-sign on (SSO) portal. Institutions can use a vendor such as Unicon, use the latest Shibboleth release, or follow Duo's own instructions for integration. How many applications an institution's SSO portal gives access to also affects the integration process. At **Institution A**, integrating Duo into SSO for the 100-150 users currently enrolled in MFA took only about an hour. At **Institution B**, IT administrators recently added support for MFA through their SSO login. However, they do not guarantee SSO functionality due to environment resiliency issues.

©2017 EAB • All Rights Reserved

## Create Plan for Handling Service Interruptions

Contacts at **Institution C** emphasize the importance of preparing for the rare cases in which the Duo service could be unreachable or temporarily offline. While failing into a non-secure mode where the second factor requirement is waived would maintain access to institutional resources, doing so creates a security vulnerability. On the other hand, failing into a secure mode makes it impossible for users to log into their accounts for as long as the Duo service is interrupted. After weighing these options, Institution C decided to take the secure route.

### Multiple MFA Solutions Introduce Complexity For IT Departments

Contacts at **Institution B** report that while they are aware of services like ERP firewalls (e.g., GreyHeller) that embed MFA into specific services accessible in an ERP system, many ERP systems are highly customized and therefore more difficult to work with than the Duo MFA service. ERP firewalls also require greater diligence to ensure that no avenue to sensitive information in the ERP system is left unprotected, an issue that requiring the second factor at login avoids entirely.

©2017 EAB • All Rights Reserved

# 3) Deploying MFA to End Users

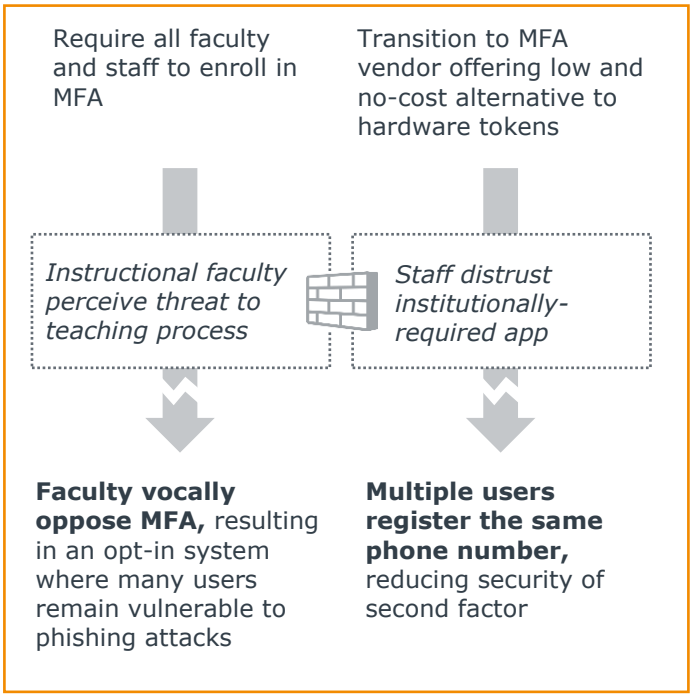
## Deployment Strategy

### Anticipate Potential Obstacles to Smooth Deployment Process

Because early opposition to MFA can inhibit its long-term acceptance on campus, institutions must design a deployment strategy that goes according to plan on the first try. At **Institution B**, the deployment process was relatively smooth due to widespread knowledge of successful hacking attempts (e.g., emails in the 2016 presidential election, customer information stolen from major retailers) which resulted in cultural acceptance of MFA as a necessary—if perhaps inconvenient—step for the institution to take. Conversely, faculty and staff at the **Institution D** who have instructional responsibilities have traditionally been exempt from MFA.

In addition to replacing a legacy token-based system, contacts at Institution D hoped that Duo's additional login options would facilitate transition of all faculty and staff over to MFA. However, a combination of continued faculty and staff opposition and lack of leadership buy-in has stalled MFA rollout to these groups. Instructional faculty and staff are attached to the exemption to MFA they secured in 2006, when the institution began using a token-based system. Additionally, the institution's current provost is serving in an interim capacity, creating a lack of political capital required to push for MFA expansion.

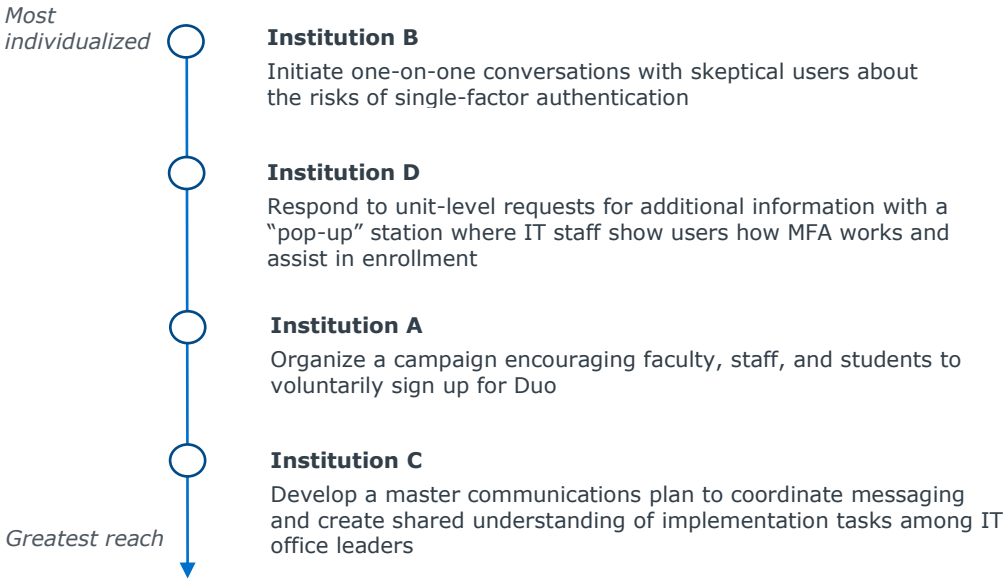
**Obstacles Encountered at Institution D**




©2017 EAB • All Rights Reserved

To prevent obstacles to MFA deployment, IT departments must coordinate across campus and consider which second-factor options skeptical user groups are likely to find least objectionable. **Institution C** IT administrators worked with their project management office to ensure Duo implementation would have a project manager dedicated to coordinating the deployment process. Additionally, contacts at Institution D reported that considering additional second-factor options might have eased faculty and staff backlash. One option is a USB security key (e.g., Yubikey), which Institution D IT staff have begun to use and find more convenient than other MFA methods. Once inserted into a USB port, users only need to press a button on the key to authenticate.

### Sample Approaches to Promote Community Acceptance of MFA




## Work with Campus Stakeholders to Secure Buy-In

Profiled institutions work across units on campus to promote acceptance of MFA. **Institution D**'s central information security officers created a presentation to explain the institution's new IT security strategy and introduce the Duo service. The central IT office also offers "pop up" sessions, in which IT staff visit a specific unit to help new Duo users set up the system. **Institution C** and Institution D both convened a security working group comprised of IT security representatives from over two dozen units. The groups provide advice to central IT staff on MFA implementation based on their respective units' computing habits. More broadly, they serve as a forum for discussion, as well as the creation and implementation of IT security policies and practices.

In some cases, contacts believe a more personal approach is necessary to convince users of MFA's value. **Institution B** found that one-on-one conversations with those reluctant to use MFA successfully changed some minds. In these conversations, IT administrators emphasized the personal privacy benefits that MFA provides and deemphasized the inconvenient aspects of MFA. Contacts report that illustrating the consequences of a stolen password, such as having paychecks redirected and identity information stolen from tax forms, helped mollify skeptical users.

©2017 EAB • All Rights Reserved

## Deploy Communications and Marketing Tactics to Reach User Groups

When **Institution B** reached the stage where all faculty, staff and students were required to use Duo, they prepared an extensive marketing campaign. Tactics included print, social media, and email outreach, on-campus tabling where users could come and get help signing up, online tracking of sign-ups, and T-shirts with clever slogans about Duo. Similarly, **Institution C** recently completed a communications plan for its campus-wide deployment of Duo via its SSO portal. IT administrators worked with the institution's communications department to identify key staff members to inform and educate about Duo and to design communication strategies specific to individual population segments. Then, contacts created a focus group of 8-10 people who would eventually be required to use Duo to test and refine the communications plan.

©2017 EAB • All Rights Reserved

# 4) Research Methodology

## Project Challenge

Leadership at a member institution approached the Forum with the following questions:

- Which applications require MFA at other institutions?
- How often do institutions require users to re-authenticate using MFA?
- Do institutions use different MFA solutions for different applications? Are some MFA solutions better suited for certain applications than others?
- Which segments of the University community are required to use MFA?
- What exceptions, if any, are made to MFA requirements?
- How do institutions develop MFA deployment strategies?
- How do institutions deploy MFA to off-campus constituencies?
- How do institutions ensure faculty abroad or in areas with poor telecommunications infrastructure can access applications that require MFA login?
- What strategies have eased community acceptance and created positive attitudes towards MFA? What approaches have proven especially effective?
- When do institutions implement single sign-on in relation to MFA implementation?
- How do institutions assess the impact of MFA implementation on individuals' privacy?

## Project Sources

The Forum consulted the following sources for this report:

- EAB's internal and online research libraries (eab.com)
- The Chronicle of Higher Education (http://chronicle.com)
- National Center for Education Statistics (NCES) (http://nces.ed.gov/)
- Institutional websites
- Duo Security
- InCommon Federation: Duo Service Subscribers
- GreyHeller
- CNET: "Two-Factor Authentication: What You Need to Know FAQ"
- Institution D Presentation-Overview of Duo 2FA Implementation
- Institution C Communications Plan

©2017 EAB • All Rights Reserved

## Research Parameters

The Forum interviewed chief information security and identity management personnel at four-year, public and private institutions in the United States.

### A Guide to Institutions Profiled in this Brief

| Institution | Location | Approximate Institutional Enrollment (Total/Undergraduate) | Classification |
|---|---|---|---|
| **Institution A** | Midwest | 20,000/15,000 | Doctoral Universities: Higher Research Activity |
| **Institution B** | South | 15,000/14,000 | Doctoral Universities: Highest Research Activity |
| **Institution C** | Midwest | 20,000/15,000 | Doctoral Universities: Highest Research Activity |
| **Institution D** | Midwest | 40,000/30,000 | Doctoral Universities: Highest Research Activity |

©2017 EAB • All Rights Reserved