Two-Factor Authentication: Lessons Learned

JANUARY 2019
Two-factor authentication provides a straightforward way to increase the security of online systems and resources, and implementing the technology requires cultural as well as technical change.

**Introduction**

Educational institutions around the globe face an ever-growing number of sophisticated attacks and security breaches, as well as increasing compliance demands. Two-factor authentication (2FA), commonly referred to as multifactor authentication (MFA), has become the go-to method of helping protect user identity during the login process—one of many critical security points.

A typical 2FA implementation today uses a combination of login credentials paired with a soft or hard token or biometrics. Although many vendors still offer short message service (SMS) to push one-time security codes to users as part of 2FA, the National Institute of Standards and Technology (NIST) has deemed SMS delivery of one-time security codes “restricted” and warns that users are at risk using text-based 2FA.

Adoption rates of 2FA (or MFA) among educational institutions are growing. According to the 2016 EDUCAUSE Core Data Service (CDS) survey, 73 percent of respondents were either planning an MFA deployment, had a deployment in progress, or had completed a deployment. The 2018 CDS survey is under way as of this writing, with the report scheduled for release in early 2019.

This paper highlights lessons learned and best practices shared by information security professionals who have implemented 2FA to increase security at their educational institutions.

**Deployment Strategies and Challenges**

In general, colleges and universities have taken a phased approach when rolling out a 2FA solution. Projects typically start with a pilot of mostly information technology (IT) staff participating in multifactor authentication to uncover integration challenges and highlight support changes that need to be addressed.
Planning, Selection, and Procurement

Most of the educational institutions interviewed for this paper deployed Duo Security (Cisco); one deployed Okta, and one institution’s sister organization chose Microsoft’s solution. The institutions use 2FA in conjunction with Central Authentication Service (CAS) and Shibboleth for single sign-on (SSO) and Banner 9 (Admin Pages).

A primary consideration is which platform to choose. Do you select a single platform or multiple platforms? Although most institutions recommend standardizing on a single platform, each institution must evaluate its environment to determine the best option. If you do not have time to research and vet 2FA solutions for your institution, consider seeking assistance from an outside source such as an analyst or consulting firm which can provide valuable expert opinions and relevant research and assist with the request for proposal (RFP) to streamline vendor selection.

Involve your enterprise team—IT security, IT systems engineers, and so on—in the 2FA planning and procurement process to ensure compatibility and connectivity with existing services and applications, such as Active Directory Federation Services (ADFS) and SSO. For example, after selecting Duo, one institution found an incompatibility in its login solution during the pilot, which required a fix. Another found that the Microsoft 2FA solution would not integrate with campus SSO processes, so they selected a different 2FA solution. These problems could have been avoided by engaging the entire team before selecting a solution.

Meet with key stakeholders and campus groups to determine how 2FA integration will impact students, staff, and faculty. Also, estimate the impact on the help desk and service desk once mandatory 2FA enrollment begins, and start training support staff early in the process.

Thoroughly define your 2FA scope, requirements, and use cases (and vet them). This process includes the following:

- Develop workflow processes for onboarding and offboarding.
- Develop a management plan for stale accounts, such those without a login for 90 days. A user might leave for a semester, graduate, or drop out. How long should you maintain a user’s 2FA license? This is especially important if you need to monitor licensing limits.
Look at ongoing and planned projects from a management and resource perspective. Will you have adequate staff to cover those projects once the 2FA rollout begins? A considerable amount of staff time will be needed for the initial rollout, including IT and security, communications, and IT service and support.

**Pilot**

Conduct a pilot with IT staff to uncover technological hurdles, to integrate with your campus SSO system, and to firm up workflow processes. Your pilot might initially include a few administrators and then all IT personnel. Many institutions underscored the importance of including personnel from the service desk and the help desk in this phase when resolving errors and technical issues.

During the pilot phase, begin developing a communications and rollout plan, as well as a marketing and awareness plan.

**Rollout**

The time required to implement 2FA in the interface is short—for example, you can implement Duo in 15–20 minutes. However, an entire 2FA project from initial planning through full campus participation usually takes at least one year and often two or more years.

After a successful pilot, most institutions have chosen to deploy in a phased approach, starting with smaller groups and then expanding more broadly, with time allotted between each rollout for refinements. For example:

1. Roll out to external-facing virtual private network (VPN) users.
2. Roll out to faculty and directors.
3. Roll out to staff.
4. Roll out to students, alumni, emeriti, and all other affiliate accounts.
5. Expand to Shibboleth, and then email, productivity, and other applications.

The institutions interviewed offered several recommendations for deployment:

- Timing is critical. Deploy near the beginning of a term or calendar year, but allow at least a week for campus activities to settle in to a normal routine.
- Monitor your rollouts daily or even hourly during the first few days when a new tier of users is introduced.
Two-Factor Authentication: Lessons Learned

- To differentiate users who are already participating in 2FA (during the voluntary enrollment phase), use an AD group to identify users who are 2FA enabled and then flip that group out by changing its name.

After the voluntary enrollment phase ends, require all new accounts to enroll in 2FA.

Deployment Challenges

Overall, institutions reported relatively few technical issues with their selected 2FA platforms. Older versions of CAS resulted in some application issues with Duo; Canvas access was a particular concern. One institution cited some memory and resource issues prior to upgrading its identity management (IDM) system and CAS. Overhauling the IDM provided a “clean slate” to work from, and a subsequent CAS upgrade resolved any problems.

You also might encounter challenges with certain service provider apps and VPN usage; however, any issues are typically provider dependent.

It’s important to educate users to be responsible for their actions, as with security awareness and phishing. You might assume users vet notifications, but experience shows they tend to automatically click “Yes.” Therefore, it is recommended to require any users who are prone to using weak security practices, such as those who have fallen for a phishing scam, to enroll in 2FA as soon as it is available.

Users who cannot or will not use an authentication app are, in most cases, provided a hardware token or USB key. Because users tend to lose authentication hardware devices, some institutions charge a fee to replace them.

Project Management

Many deployments are managed by an institution’s chief information security officer (CISO) or IT manager; however, bring in a project manager if possible. A project manager can serve as the project sponsor, focusing solely on the project at hand, and providing single-source communications to the CISO.

The Georgia Institute of Technology (Georgia Tech) pointed out that a dedicated project manager may determine the population to be enrolled in advance, coordinate meetings, work closely with other stakeholders on campus, handle or coordinate marketing and awareness, and provide “white glove” treatment to those who are needed as project champions.
The project manager may also serve as a functional tester, identifying technical issues and tracking progress toward resolution.

**Disaster Recovery**

Multifactor authentication platforms, like any cloud-based service, are prone to outages that prevent users from logging in. The University of Alabama at Birmingham highly recommends creating a disaster recovery plan with defined communications and technical roles, incident response scenarios, and step-by-step procedures for remediating 2FA issues. For example, your documentation should include steps for removing 2FA from the authentication process should an outage occur (reverting to single-factor authentication) and for determining how to quickly restore 2FA once the outage is over.

Have your change advisory board (CAB) preapprove all procedures as a standard emergency change, and maintain all relevant documents in a central repository so they are accessible to all relevant staff.

**Enrollment and Change Management Approaches**

The largest portion of a multifactor authentication project is getting users and their devices enrolled in the platform. The main enrollment challenge cited by institutions was user resistance to adding another step (and time) to the login process.

To build in flexibility, most institutions offered a voluntary enrollment phase lasting about one year for most users, followed by a shorter mandatory enrollment phase. However, a few institutions simply “flipped the switch” after a marketing and awareness campaign, forcing users to enroll the next time they logged in to SSO.

Regardless of which enrollment method you choose, consider the following as part of your approach:

- **Create new technologies to enable self-enrollment.** Georgia Tech’s largest uptake in student enrollment came when it rolled out the ability for students to onboard each other. This “web of trust” caught on exponentially, helping the university reach 98 percent adoption within the target deadline.

- **Onboard freshmen before they start classes, if possible.** Reach out to incoming freshman and their parents prior to orientation to briefly explain 2FA and its significance to the institution. During orientation, staff tables to
encourage enrollment and provide information on login options. Georgia Tech provided a QR code that linked to a 2FA overview video on its YouTube channel, which allowed the collection of metrics on number of views per date/time.

- **Inform stakeholders the week before mandatory enrollment begins.** Keep directors informed on the upcoming deadline and be sure your service-desk and help-desk personnel are ready.

- **Send reminders to users.** Send users a link for enrollment, followed by a reminder a few days before the mandatory deadline.

- **Work collaboratively across levels.** All institutions agreed that obtaining leadership buy-in from the start and working closely with each unit’s IT staff throughout the enrollment process are critical to a successful 2FA implementation.

Many methodologies exist to plan change, the predominant one being ADKAR (Awareness, Desire, Knowledge, Ability, Reinforcement). The principal strategy for ADKAR is that for an organization to change, all groups/individuals within the organization should change as well. Therefore, it is important to provide effective change management at an individual level to ensure that the overall project is able to achieve its goals at an organizational level.

### Marketing and Awareness Campaigns

A multifactor authentication rollout changes how users access systems. Therefore, users must feel they are a part of the process and be educated about why the new authentication method is necessary and about the benefits to them.

Most institutions reported that pervasive and multichannel marketing was key to gaining buy-in from users for enrollment and enabled a smoother overall transition to 2FA. Marketing methods included email, social media posts, campus newspaper and department newsletter articles, posters, tables at fairs and student centers, T-shirts, digital signage, and short videos.

Georgia Tech and Baylor University offered several recommendations for a campus-wide marketing and awareness campaign:

- **Create an integrated, branded campaign early.** This helps all user populations identify relevant news and updates and prepares them for enrollment.

- **Consider how to reach all users.** Although marketing efforts are typically successful with those who spend much of their time on campus, how will you
effectively reach remote and international users? Do you have students who live off campus who might not see physical marketing materials around campus?

- **Create a communications toolkit.** The base toolkit should include an email template, PowerPoint presentation, and a template for website content. Consider creating an expanded toolkit for students that includes postcards, flyers, banners, dining-hall tent cards, stickers, T-shirts, and a catchy phrase, such as “Peace of Mind with Two-Factor Authentication” or “Do You Duo?”

- **Customize the website to various audiences.** Create digital content for general users as well as IT administrators, and provide news, videos, FAQs, and quick reference guides. Prominently display links to enroll in 2FA, along with whom to contact for help. Encourage departments that work directly with students, such as residence hall staff, to direct traffic from their site to yours.

- **Help users enroll, and emphasize 2FA benefits.** Staff tables at the Student Center and at orientations for new faculty and students, and provide website links in all materials to help users enroll. Emphasize that 2FA participation means users might not have to change their passwords as often (or, in some cases, never) and that using the app or token adds only seconds to the authentication process while greatly increasing security for them and the institution.

Keep all stakeholders informed by creating communications and rollout plans, as well as a project timeline, and send or present your plans to the president, directors, liaisons, and IT groups. Prior to rollout to each target population, inform your directors and key stakeholders via email and include an enrollment link. Your president or chief information officer (CIO) might be willing to push a campus-wide email to bolster participation and underscore the importance of 2FA to all users.

For most institutions, communications play an important role in meeting multifactor authentication project deadlines. According to Georgia Tech, “When you think you’ve communicated enough, communicate more.”

**Costs**

Costs for a multifactor platform have decreased dramatically over the past five years. However, additional or unexpected costs can occur with 2FA. For example, Duo debits your telephony credit balance for each SMS message or voice call to a user for authentication, beyond the cost of base licensing. Credit usage can be difficult to estimate and has exceeded what some institutions expected. Set a cap
for usage, monitor the account balance, and replenish the account as needed to avoid running out of credits.

One institution struggled to plan adequately for tokens, underestimating the total required by their user populations. Although tokens cost about $20 each, planning for too few tokens resulted in additional, unplanned expenditures after the 2FA rollout was under way.

**Support**

Access to systems is critical for organizations; therefore, quick resolution of access issues is extremely important. Although most multifactor authentication solutions offer self-service, the beginning of the mandatory enrollment phase can result in high call volumes to help-desk and service-desk staff.

Thoroughly train and prepare your lines of support in advance of the rollout to configure tokens; become familiar with screens for iPhone and Android; assist users who lose, break, or change devices; and provide general guidance for frustrated users. Plan for support staff to be available for one-on-one assistance onsite, if possible, and by telephone and email, most heavily during the lead-up to and during the student deadline.

**Documentation**

Step through the personas of campus users and determine appropriate documentation for each type. Consider testing different types of documentation with focus groups to gather feedback and refine your materials for various audiences. For example, Baylor University created a set of videos to help users understand and use 2FA, but a student focus group found the videos inefficient and preferred concise documentation with numbered steps.

Look to your 2FA vendor for documentation in the form of FAQs, walk-throughs, and how-tos, such as setting up a phone, using a token, and enrolling from different devices, and customize that documentation for your audience.

As mentioned previously, create a set of FAQs for general users and another set for IT service and support groups. If you bring service and support groups into the process early, they may be able to create FAQs that you review and approve.
Methods to Verify Remote Users

Resetting a password is a standard tool in self-service 2FA solutions. The user must answer challenge questions to receive a PIN reset code. Many institutions also verify remote users by phone by asking a series of challenge questions or by conducting Skype or video chat sessions. On-premise students might need to visit the help desk in person with a photo ID if there are anomalies or difficulties during verification.

Georgia Tech recommends creating an alternative or backup login option. They suggest printing backup codes to keep in a wallet, purse, or backpack, as well as setting up a secondary device in case your primary device is unavailable.

What’s Next?

As the struggle to keep unauthorized users off of higher education networks continues, stronger MFA will be required. Three-factor authentication (3FA) combines a username and password with a token and a biometric factor. Four-factor authentication (4FA) adds one more factor, such as physical location.

The MFA arena is also witnessing the beginning of a sea change in the use of tokens versus apps, with a shift to a pluggable or touch-based hardware token rather than a changing key. Examples include the YubiKey and Google Titan Security Key, which support FIDO open standards. Keep this technology shift in mind during your next iteration of MFA.

Resources

The following resources may prove useful when planning a 2FA implementation:

- EDUCAUSE Live! “Campus-Wide Two-Factor Authentication (2FA) Saturation Campaign” (October 11, 2018).
Conclusions

A campus-wide 2FA project has wide-ranging implications for an organization’s culture, resulting in some level of reluctance among even the savviest users. To alleviate concerns and ensure project success, bring in all stakeholders early in the process, perform a comprehensive pilot to root out technical and operational issues, follow a phased approach to deployment, and educate all users through a robust marketing and awareness campaign.

Acknowledgments

This paper was prepared as a group effort by a number of higher education information security professionals. We hope you find these recommendations and resources useful in planning and deploying your institution’s 2FA solution.

- Jon Allen (Baylor University)
- Lorrie Burroughs (Georgia Institute of Technology)
- Scott Fendley (The University of Alabama at Birmingham)
- Gaël Frouin (Berklee College of Music)
- Moeen Taj (Montgomery College)
- Ty Tyra (The University of Alabama at Birmingham)
- Trevor Woods (Monash University, Australia)
- Joanna Lyn Grama (Vantage Technology Consulting Group)
- Kim Lindros (on behalf of Vantage Technology Consulting Group)
- Valerie Vogel (EDUCAUSE)

About EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 99,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information please visit educause.edu.

© 2019 EDUCAUSE. Creative Commons BY-NC-ND 4.0.