2023 INTERNET2 TECHNOLOGY exchange

MFA Lessons Learned:
Implementing Large-Scale Change

PRESENTER NAMES:

Jesse Taylor, Sr. Manager of Identity and Middleware Services, University of Nevada, Las Vegas
Summer Scanlan, Business Systems Analyst, University of California, Berkeley

Introductions

Jesse Taylor, MSITM
Sr. Manager of Identity and Middleware Services
Office of Information Technology
University of Nevada, Las Vegas (UNLV)

30,689 Students
3,500+ Faculty and Staff

Started MFA Journey in 2021, after migration from old IAM system.

Okta MFA is our solution as part of the Okta Identity solution.
Last segment of initial MFA enrollment September of 2022.

UNLV

Introductions

Summer Scanlan
Business Systems Analyst
Information Security Office
University of California, Berkeley (Cal or UCB)

We implemented MFA for campus cohorts using a phased approach from October 2017 through December 2018.

Cal currently has **52,000 students**, **27,000 employees and 7,300 HR affiliates**. All of these cohorts now use Duo MFA to login to campus services.

A little history and mystery at UNLV…

- This was not a traditional implementation of MFA.
  - At one point, we had two IAM systems!
  - The old IAM system had nearly 120 service providers and could not move forward with MFA without a major retrofit.
  - We had Okta already with MFA for Workday.

    - Only Staff had access to this.
  - In late 2019, the decision was made to move to Okta, since it was a modern SaaS platform, *and our staff was already in it.*
  - So we started moving apps over one-by-one from late 2021 through the end of last year. (pandemic + licensing)

UNLV

Implementation Strategy

- We had a mandate to not move forward with MFA unless:
  - Proper communications were made ahead of the change.
  - Proper training had occurred with Help Desk staff.
    - A pilot with our OIT team members and QA/Testing Group.
  - Proper documentation and knowledge base articles existed.
  - It was not the start or end of a semester, or midterms.
  - SMS was still available (prior Okta default) since staff was used to it.
  - Extremely minimal interruption to students.
  - Extremely minimal interruption to staff and faculty.

UNLV

Implementation for Staff and Faculty Enrollment (Phase 1)

- The scope of this first phase was to turn it on for ALL applications in Okta, Faculty and Staff, and then add additional MFA methods.
- Communications plan was started on September 8th, 2022, letting end users know that MFA was being turned on for all applications on October 4th, 2022.
- Communication methods: IT News Center, University wide emails, interactions at the desk, announcement in Workday, banner messages on our LMS, talking points for our executive staff to take to intercampus meetings, faculty senate announcements.
- *Workday MFA was our leverage* – you need it to access you benefits and compensation.

Implementation for Staff and Faculty Enrollment (Phase 1)

- As previously mentioned, Workday was already enabled for MFA via SMS.
- MFA was then turned on for all applications on October 4, 2022.
- Within an hour, we had minimal calls.
- Most complaints were that they didn't want to MFA every application.
    - We found using Okta Verify (push) really helped.
- Some employees refused to use a personal device:
    - We had prepared for this by enabling hardware keys on the Okta tenant, and had hardware USB keys ready to go.
    - You could have Okta call and give you a code.
- Most feedback was positive about it being a security enhancement.

UNLV

Implementation for Students (Phase 2)

- On October 4th, 2022 it was announced that Students would be required to use MFA on October 19, 2022.
- Students were given instructions on how to enroll early in order to mitigate any interruptions, and we pushed Okta Verify as the preferred method.
- Methods of communication were the IT News Center, University wide emails, interactions at the desk, pop-up help desks, banner messages on our LMS, talking points for our executive staff to take to student focused meetings.
- One of the reasons Students went second, was the faculty/staff could assist them if needed given their existing experience.
- Between October 4th, 2022 and October 18th, 2022, 21% self-registered ahead of time for MFA.

UNLV

Implementation for Students (Phase 2)

- On October 19th, 2023, launch day, the desk's top request was helping students enroll in different options – we pushed Okta Verify. We expected that.
- Some were not clicking "Send" for the token verification.
- Several weeks later, we were asked to let folks to MFA once every 8 hours on a device, versus 2 hours. That seemed to help.
- We found some software at the time did not support hardware tokens! Mitigation was to use another method.
- By October 27th, 93.1% of Students had enrolled MFA.

UNLV

Continuous Improvement

- We need to retire SMS, campaign ongoing to promote Okta Verify and Hardware Keys.
- We are working on adding deeper service provider integrations (governance), to enable “step-up” authentication.
- We continue to educate our end users on the benefits of MFA and why it is necessary.
- We continue to adjust policies on MFA from end user feedback.
- We continue to upgrade our system to **give MFA more powers**:
  - End users can verify to reset their password over Self-service with Okta Verify.
  - Next up – person verification over Okta Verify.

Technology Used

- **Okta**

  https://www.okta.com
- **Okta Adaptive Multi-factor Authentication**

  https://www.okta.com/products/adaptive-multi-factor-authentication/

UNLV

Implementation Strategy

- Get campus buy-in
  - Make your case, and get campus administration on board
  - Collaborate with your support desks
  - Create a network of MFA Ambassadors
  - Help departments onboard their own users
  - Offer in-person help desks
- Create large cohorts
  - Small pilot with IT employees
  - Roll out to employees in large groups
  - Roll out next to students in large groups
  - Onboard special groups last

Implementation Strategy

- Use a phased approach
  - Phase 1: January - October 31, 2017
  - Phase 2: November 1, 2017 - April 16, 2018
  - Phase 3: July 9, 2018 - December 10, 2018
  - Rolling deadlines means less impact on systems and help desk
- Hotel California
  - Once you're in, you can never leave
- Get creative with communications
  - CAS screen interrupt is vital!
  - Raffle off prizes to encourage cohorts to sign up before the deadline
  - Use dynamic groups to email only folks who need to sign up in a specific group
  - Custom posters and images draw user attention

Implementation Strategy

- Lots of help desk tickets
- Increased security posture!
- Positive unplanned side effects regarding IAM tools

Our hope: users would better understand why campus data and their own data needs to be secure.

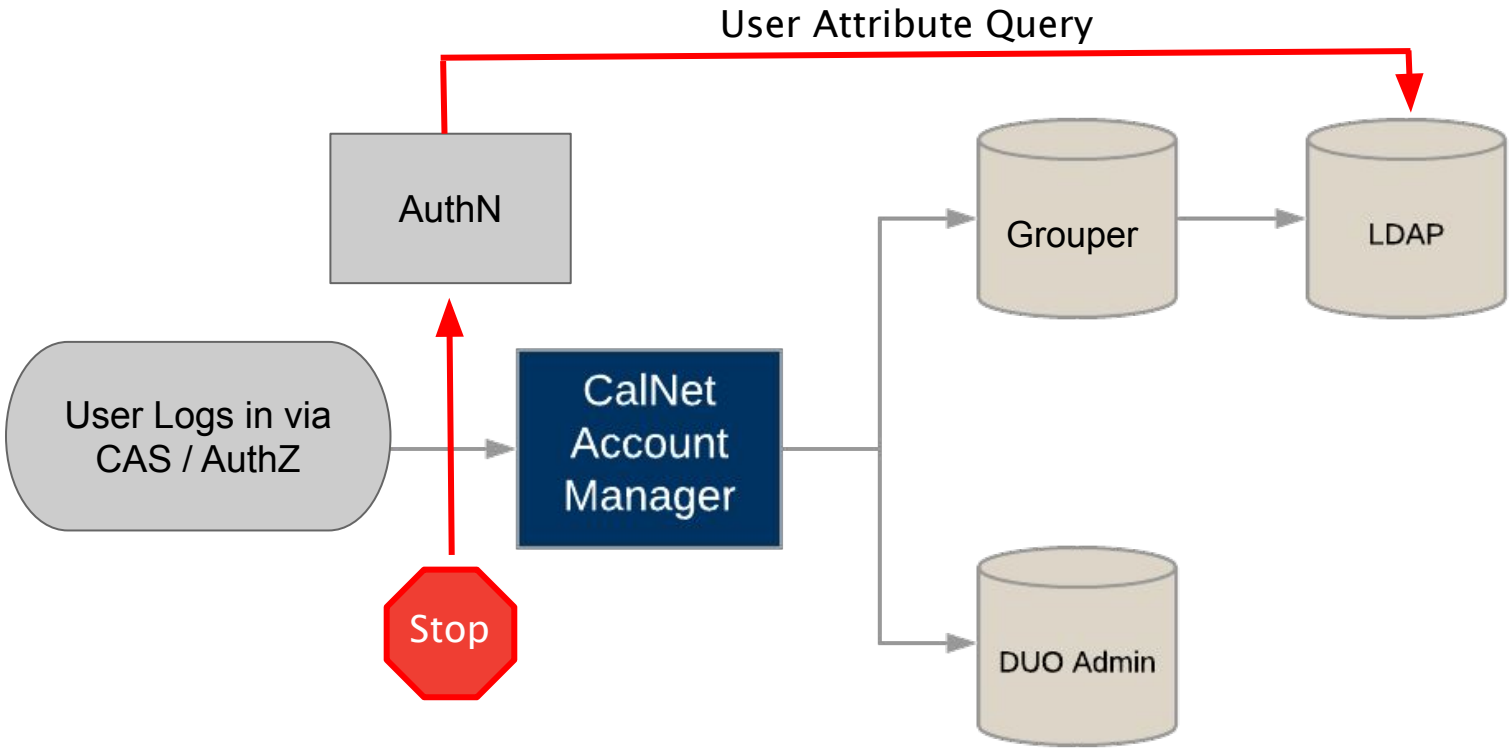
The reality: students don’t think their data is important. Additional socializing is needed.

Continuous Improvement

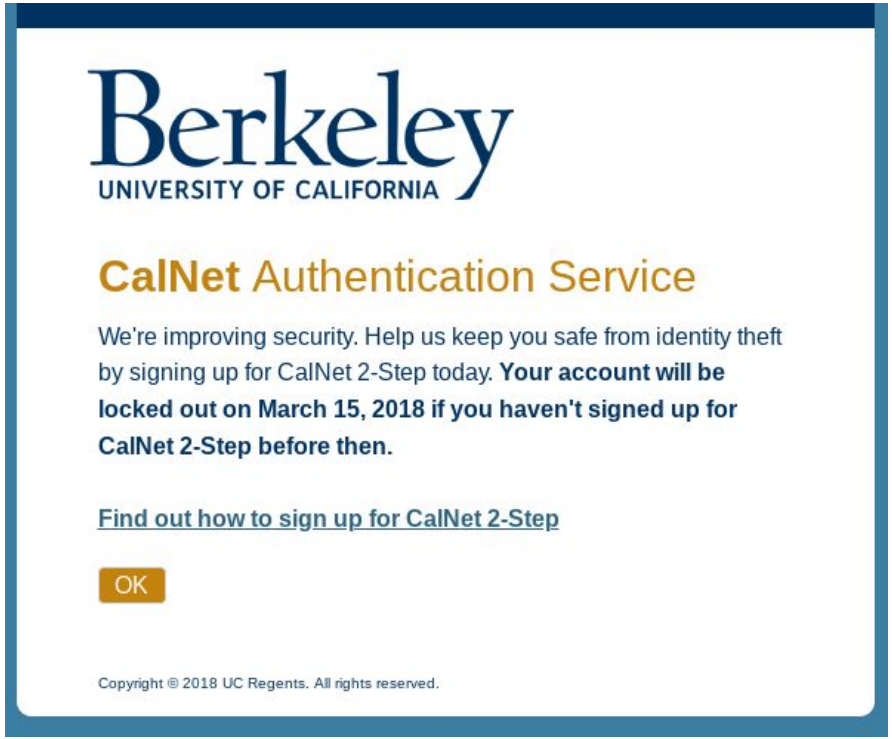
- Feedback from pilot group
- Monitor help desk tickets
- Update documentation
- Adjust processes
- Example: simple hardware tokens.

Be agile! Adapt and improve!

Enrollment Flow



CAS Interrupt Example



This screen allows a user to opt to enroll now, or click OK to enroll later.

We changed the CAS screen once the deadline passes, to force the user to enroll.

Screen only displays to impacted users.

Technology Used

- **Grouper**
  - https://incommon.org/software/grouper/
- **CAS**
  - https://www.apereo.org/projects/cas
- **CAS Interrupt**
  - https://apereo.github.io/cas/6.5.x/webflow/Webflow-Customization-Interrupt.html
  - https://www.unicon.net/insights/blogs/cas-server-interrupt-me-please
- **LDAP**
  - https://backstage.forgerock.com/docs/ds/7/getting-started/ldap.html

Lessons Learned

1. Set realistic expectations
2. Create a what-to-do-when-you-travel page
3. In person support allows edge cases to get what they need
4. Bribery works
5. Documentation, documentation, documentation!
6. You can’t count on emails to get the word out
7. Get student employees to help
8. Do not offer all devices and methods your MFA offers
9. It takes a village!
10. Have hope.

DEMO


?
Q
&
A
!

Contact and Resources

Jesse Taylor - jesse.taylor@unlv.edu
https://www.linkedin.com/in/jessetaylorlv/

Summer Scanlan - sscanlan@berkeley.edu
https://www.linkedin.com/in/summer-scanlan/

For further information on how Cal implements change using Grouper with CAS, you can reach out to Berkeley IAM System Administrator Jonathon Taylor - jonathont@berkeley.edu