Access Management Improvement
Overview for IT Partners

YALE UNIVERSITY

AMI Project Team

John Barden, Executive Sponsor
Paul Rivers, Project Sponsors
Jeremy Rosenberg, Project Lead
Linda Faust, ISPC Program Director
Amit Poddar, Technical Lead
Beth McKinley, Change Mgmt. Lead
Netal Patel, Test Lead
April Tiddei, UX Design Lead
Michael Tullo, UX Designer
Ed Sokolnicki, Project Manager
Russ Robitaille, Business Analyst

YALE UNIVERSITY • IT
AMI Program Overview

PROGRAM GOALS

• Extend MFA protection to Yale email and all CAS-protected applications.
• Improve accessibility and modernize branding of CAS and NetID Management. Eliminate annual NetID password resets incorporating harder-to-guess passwords.
• Email and phone-based password recovery for forgotten NetID passwords.

BENEFITS OF THE PROJECT

• Fewer Yale email compromises from phished or cracked NetID passwords.
• Annual NetID password reset phased out after one last reset post-AMI-rollout.
• Increase of the DUO “remember-me period” for off-campus access to CAS resources from 1 day to 90 days.

COMMUNITY IMPACTS

• DUO Everywhere – Users will be invited to opt in using a tool that steps them through the process of enrollment and device setup. DUO-authentication will be required upon the first access to O365 or CAS-protected applications per client (browser) per device, including on campus and again every 90 days when the user selects the “remember me for 90 days” checkbox.

• Set recovery information – Users will be asked one-time to register their non-Yale email address or phone number so they can recover a forgotten NetID password. Users will periodically receive a prompt to verify that the recovery information they specified is still accurate.

• Password complexity – All users will be required to update their NetID password only once after the new complexity policy is in place in Summer 2020. They will be required to set a password which meets updated complexity requirements designed to ensure less easily guessed NetID passwords.

• New NetID management screens – The NetID Management application is being upgraded to include accessible screen designs which conform to Yale visual identity standards and practices.

• New CAS screen – CAS will be upgraded to version 6 and will incorporate accessible screen designs which conform to Yale visual identity standards and practices.

• Revised NetID activation with MFA – The current practice of instructing users to enroll in DUO MFA via email to their Yale email will be revised for onboarding of students, faculty and staff.
TECHNOLOGY CHANGES

- **DUO Everywhere** – Yale is extending DUO MFA to provide 2-factor protection to Yale email and CAS-protected resources everywhere. We are using an Azure AD feature to add DUO multi-factor authentication) to the Microsoft O365 login flow. We are adding a new "app" to enable MFA protection for CAS logins everywhere with the option to remember the DUO authentication for 90 days. We are also using the Microsoft default memory period of 90 days for O365 logins.

- **DUO Everywhere Opt-In tool** – A custom tool has been developed to allow the user to opt into DUO Everywhere. It steps users through the process of enrolling device setup.

- **Microsoft AD password filter** – Yale is implementing Microsoft’s AD password filter which will subject all AD passwords to Microsoft’s latest password complexity policies as documented [here](#).

- **Azure AD Self-Service Password Reset (SSPR)** – Yale is implementing Microsoft’s Azure AD SSPR to enable users to set and use email address and cell phone number to recover a forgotten password. This replaces Yale’s legacy custom application using challenge questions.

- **Azure AD SSO** – Yale is expanding our use of Azure AD Single Sign-On in addition to our current CAS Single Sign-on. We expect to increasingly onboard new applications to Azure AD SSO rather than CAS or Shib where feasible. The main difference users will notice is that Azure AD SSO protected applications request (first.last@yale.edu) login whereas CAS-protected applications request NetID-based logon using the CAS screen. Azure AD SSO supports SAML and OAuth protocols. It does not support the CAS protocol.

- **CAS Upgrade** – We are upgrading CAS from version 3 to version 6. This upgrade includes improvements to many background functions of CAS including the addition of a service registry and many more configuration options. Users will notice the upgrade as we are planning to change the CAS screens as part of the upgrade. Otherwise, users would not notice this change.
• **NetID application rewrite** – We are rewriting the existing NetID maintenance application which was written in very old technology (Struts 1.0). We are also redesigning the screens for conformance to Yale branding and accessibility policy. We are keeping this application in place because there are some features (e.g., Dependent NetIDs) and user populations (e.g., Alumni) who are not well-served by the out-of-the-box Microsoft SSPR solution.

• **Bi-directional password sync** – The AMI project will enable bi-directional sync of passwords between local AD and azure AD. Currently, passwords flow asynchronously from local AD to Azure AD which can create a delay/uncertainty of up to a few hours between when a user changes their password locally and when that changed password is reflected in Azure AD. The Bi-directional password sync enables a synchronous password change initiated on Azure AD to be simultaneously and immediately effective in local AD.
Frequently Asked Questions (FAQs)

DUO Everywhere Deployment
DUO Everywhere Authentication Devices
DUO Everywhere Configuration & Technical Questions
NetID Management: Password Change
NetID Management: Other Questions

YALE UNIVERSITY • IT
DUO Everywhere DEPLOYMENT

1. Q: When can people start opting into DUO Everywhere?
   A: We are rolling to roll out our Opt-In tool to groups starting in April. To ensure we have adequate support to handle questions, we will invite subsets of users to opt in each week with the rollout spread over many weeks.

2. Q: Can support staff control enrollment in DUO Everywhere?
   A: Yes. Support staff can be given authority or users can use the Opt-In tool.

3. Q: What about CISCO AnyConnect and NGN logins?
   A: The network team is working to upgrade the VPN login experience to match the DUO prompts seen elsewhere, however, that is separate from the AMI project. NGN will require wired users to login to register devices connected to the wired network via entry of their NetID and password initially and upon password change. This entry is not DUO protected or related to the AMI project.

4. Q: Are Alumni NetIDs in scope?
   A: We do not plan to roll out DUO Everywhere to today’s recent alums. Once DUO Everywhere is fully rolled out, future recent alums (May 2021 and later) will continue to use DUO Everywhere during the period that their undergraduate email box remains active.

5. Q: Are retirees in scope?
   A: Retirees who retain Yale email are in scope. This includes people with emeritus or other active status in Workday as well as those set up with a Sponsored-Identity type of Retiree (28). Retirees who do not retain Yale email are not in scope.

6. Q: What about non-alumni with NetIDs that are not getting prompted for DUO MFA off-campus today?
   A: Please contact the project team if you have any such examples.

7. Q: Can users be put on DUO Everywhere, walked through changing their password subject to revised complexity, and register their NetID recovery email and/or phone in one DSP call or visit?
   A: Yes, but it will be after the new NetID app is turned-on in production, currently scheduled for mid-June.

8. Q: Will new Sponsored Identities (SIs) be required to enroll in DUO Everywhere?
   A: DUO Everywhere will require SIs who use their NetIDs for Yale O365 email or access to any CAS-protected applications to enroll. SIs who only need an ID card and do not use their NetID online do not need to enroll in DUO Everywhere.

9. Q: Are there special implications for union workers?
   A: No. Anyone who does not have a smartphone or would prefer not to use it can authenticate using a landline phone at their desk or be provided a hardware token.
10. Q: Do you need to be on-campus to set up DUO Everywhere?
   A: No. If you previously configured DUO to call your home phone, you will need to register an additional
   method (cell phone, desk phone, or token) so that you can DUO-authenticate from on-campus.

11. Q: What about DUO Everywhere for new community members?
   A: During rollout of DUO Everywhere, new community members will continue to be enrolled in MFA off-campus first, and then converted to DUO Everywhere. This is to ensure that during rollout, current onboarding processes continue to work as they do today. To prepare, we will provide documentation for each of the onboarding processes including staff, SI, faculty, and students by school. Once rollout is well underway, there will be a switch for all new community members to be enrolled directly to DUO Everywhere.

12. Q: What about students in exam situations where phone access is not allowed?
   A: Canvas on-campus will be an exception, and will not require MFA authentication under DUO Everywhere. Other situations where faculty indicates students may not use electronic devices will also be considered for an exception.

13. Q: What about students in schools who are issued iPads, e.g., Nursing?
   A: iPads can be used as a second factor so those users should have a seamless experience where their application access and DUO authentication can be from the same device. They can also use a different phone or device for their DUO authentication.

14. Q: Who are at highest risk for email phishing?
   A: Everyone at Yale is at risk for email phishing as many attacks are launched broadly using a single email. Higher profile individuals (e.g. Deans) are at increased risk for more sophisticated and customized attacks both personally and professionally. Anyone working with HIPAA or other regulated or highly confidential data has higher risk associated with their account.

DUO Everywhere AUTHENTICATION DEVICES

15. Q: Is it OK to use DUO authentication on the same device being used to access the protected application?
   A: Yes.

16. Q: Can I use my phone to read my email and DUO authenticate?
   A: Yes.

17. Q: What if a user does not have a smartphone?
   A: DUO authentication can be accomplished by registering a regular phone number (desk phone, home phone, or cell phone) or by obtaining a DUO hard-token from the Help Desk.
18. Q: What is a DUO hard token?  
A: A DUO hard token (see image) is a key fob which displays a 6 digit number, which changes every several seconds. A DUO hard token must be registered to a user to use it for multi-factor authentication.

19. Q: What if a user needs to DUO authenticate and cannot use or access their cell phone?  
A: We recommend users plan ahead and register multiple ways to DUO-authenticate. If the user does not have a working registered device, the Help Desk can provide them with a bypass code after validating their identity. Note that these codes are called “bypass codes” because they bypass DUO authentication and are inherently less secure.

20. Q: Can you set up DUO on an Apple Watch?  
A: Yes. Download the DUO Apple Watch app. Note that older versions of the watch will require that your phone be near the watch.

A: Today this is implemented for YNHH EPIC logons. This project only covers NetID-based logons for O365 and CAS-protected applications. We are in discussions with other groups working on Tap-and-Go clinical implementations for NetID logon to ensure these work with DUO.

22. Q: What about EPIC controlled substance ordering?  
A: This is unaffected as it uses MFA to protect YNHH individuals’ EPIC IDs. The AMI project scope only includes DUO MFA protection of NetIDs used for Yale University email and CAS-protected applications.

23. Q: Is there a need to CAS into EPIC?  
A: No. This project is strictly limited to NetID protection.

DUO Everywhere CONFIGURATION & TECHNICAL QUESTIONS

24. Q: What about authentication against Active Directory via other means such as the Linux research cluster?  
A: Anything not using CAS or Azure AD for authentication is not affected by the AMI project. Tools such as pam_duo can be used to provide 2FA MFA protection over ssh, but that is outside the scope of the AMI project.

25. Q: What about saving credentials when logging into other applications, e.g., Adobe Creative Cloud?  
A: This project sets configuration options to save O365 and DUO login information for 90 days. CAS will continue to hold a session open on the same browser for 8 hours. All other credential memory methods as implemented by browsers and/or add-ons or operating systems will function as they do today. This project does not affect them.
27. Q: Will connection to network drives require DUO?
A: The AMI project is only affecting O365 and CAS-based logins. If the file share is using OneDrive, which uses the O365 login, DUO will be required. Other means of connecting drives will not change.

28. Q: Could I get a DUO prompt for an O365 login without first getting an O365 login prompt?
A: Yes. For Hybrid-domain joined managed windows workstations, the credentials you provide to log into your workstation and register to the domain are available to O365. A user logging into such a workstation and then trying to access O365 email might see a DUO prompt without first seeing an O365 login prompt.

29. Q: What about shared email accounts?
A: Properly configured shared email accounts where users do not share a common password should work properly and gain MFA protection. If you are aware of a situation where multiple users are accessing a shared mailbox using a single shared password, please contact the Help Desk as this is not secure or supported.

30. Q: What about Microsoft MFA or other MFA?
A: Yale is currently using DUO MFA to protect O365 email and CAS-protected applications campus-wide. Microsoft MFA is used for other types of MFA protection as are other non-DUO forms of MFA. These are outside the scope of the AMI project.

31. Q: What about DUO for VPN?
A: Users will continue to be required to DUO-authenticate every time they use VPN. The networking team is working on a spring upgrade to the interface so that it looks and behaves more like our other DUO prompts.

32. Q: What is the difference between CAS remembering my login for 8 hours and DUO remembering my CAS login for 90 days?
A:

- The CAS prompt – asking for your NetID and password – comes up the first time you access CAS per browser per device. If your browser is configured to remember session info (the default for managed workstations), you will not be asked by CAS to provide your NetID and password again for 8 hours.
- The DUO prompt – asking you to confirm your login using a DUO-registered device – comes up the first time you attempt to use CAS per browser per device. If your browser is configured to remember session info (the default for managed workstations), and you check the “remember me for 90 days” checkbox, you will not be asked by DUO to confirm your login again for 90 days.

33. Q: What about sessions run using Citrix or sessions run on other forms of remote workstations?
A: Please contact a member of the project team as there are many different scenarios with different answers.
34. Q: Is the 90-day memory period synchronized such that every 90 days I’ll get all my DUO prompts again?
   A: No. The memory period is per-client/browser and per device. It starts the first time you use that client on that device, and it resets the first time after 90 days when you re-authenticate on that device for that application.

35. Q: What about using multiple Microsoft clients on the same device? When will I need to re-authenticate?
   A: If you use a browser-based MS client, your DUO-login will be remembered for all browser-based clients running on the same browser. For fat clients, the answer depends on the application. Teams, SharePoint, OneDrive and Exchange fat clients do not share memory tokens. Word, Excel and PowerPoint do share a token. Expect variations by device and software version.

36. Q: I also have an EPIC ID for YNHH and use DUO. How will this work?
   A: If you use the DUO app, you will see two separate DUO entries, one for YNHH and one for Yale University. If you use phone or SMS verification, you can use the same phone to authenticate. DUO will keep track of the push requests and memory periods separately. If you wish to provide a soft-token-generated passcode, just be sure to use the one from the appropriate entry in your DUO app.

37. Q: Can we get a list of all CAS-protected systems?
   A: No. Current CAS allows new applications to be added without registration. There are hundreds of CAS-protected applications. Some are used by most of the community, such as MyTime, Canvas, Banner and Workday. Some are used by a smaller number of users.

38. Q: What about docking and undocking?
   A: Docking and undocking does not affect DUO Everywhere. The initial prompt and memory period are not aware whether you are docked or undocked.

39. Q: What about whether I am on-campus vs. off-campus or transitioning between different networks?
   A: Connecting to different networks does not affect DUO Everywhere. Note that some CAS-protected applications, e.g., MyTime, are currently only accessible when you are on-campus or using VPN. The AMI project does not affect this.

40. Q: What about shared computers and public kiosks?
   A: Managed workstations and Yale-maintained kiosks will act just like any other device for your first login – they will prompt for DUO. It is OK to check the “remember me for 90 days” checkbox if you use a shared Yale computer which is physically secure from public access. Accessing your email or any application with a logon from shared non-Yale computers is risky and should be avoided. Do not check the “remember me for 90 days” checkbox when using public computers.
NETID MANAGEMENT: PASSWORD CHANGE

41. Q: For troubleshooting lockouts with the password change, is there an easy way to tell what devices a user has and their login status?
   A: For O365 logins, Azure AD has device and OS information where a mail client is being used. We'll look into whether the wireless has information we can use since repeated wireless access attempts are the other typical lockout case.

42. Q: What about other places that store NetID passwords, e.g., Mac Keychain, Papercut, and Chrome?
   A:
   • Mac Keychain will remember passwords up to 31 characters in length.
   • Papercut (students) – Most use the web client which will behave like the browser.
   • Papercut (staff) – Papercut fat client will remember up to a 127 byte password and prompt to reset when the password changes.
   • Chrome – Chrome password manager will remember up to a 127 byte password.

43. Q: What are the new password rules?
   A: The new rules are owned by Microsoft. Their guidance is provided here. According to that current guidance, passwords must be 8 characters or more; combine upper and lowercase letters, numbers and symbols; and pass MS complexity validation meant to prohibit use of common terms or easily-guessed variants.

44. Q: What about mailing lists?
   A: Mailing lists are not affected. Access to maintain mailing lists is not affected, provided users have not been sharing a common password to perform list maintenance. If you are aware of a situation where multiple users are using a single shared password to maintain a mailing list, please contact the Help Desk as this is not secure or supported.

NETID MANAGEMENT: OTHER QUESTIONS

45. Q: Will NetID cleanup be bundled with this project?
   A: No. NetID cleanup, meaning disabling NetIDs which should not be active, is being pursued by the IAM team. The main area of intersection with AMI will be the off-boarding of formerly active faculty, staff and students. Otherwise, the scope of the AMI project is strictly limited to authorized NetIDs associated with active affiliates.