

Overview of Duo 2FA implementation



DePriest Dockins, Assistant Director, Identity and
Access Management, ITS
Unit Liaison Meeting, May 11



Agenda

- Overview
- Timeline
- Duo Options & Benefits
- Pre-enrollment Planning
- Working Together
- Short Enrollment Demo
- Appendix: Authentication Options & Enrollment Screenshots



New U-M IT Security Strategy

- One university-wide security program
- Focus on the most sensitive information first
- Make security the easy choice
- Promote university-wide security culture and capabilities
- Collaborate with faculty to contribute to the domain



CY2016 2FA Objective & Benefits

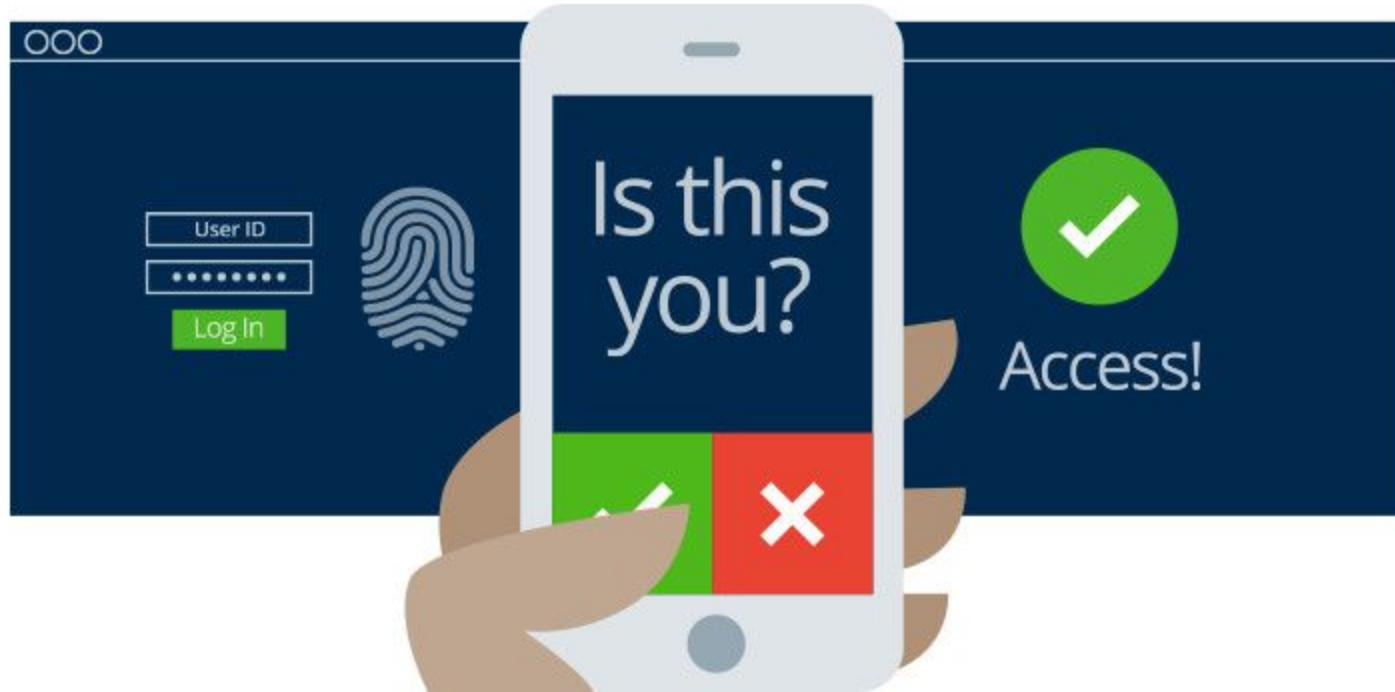
To replace MTokens with a new 2FA solution and then expand to U-M restricted and high-sensitivity information

Benefits





- Improve University security posture to secure personal data and sensitive university data
- More flexible system with advanced authentication methods, including smartphone app, SMS text & more
- Use of a single 2FA solution across campus



Two-factor with Duo



Duo 2FA Options

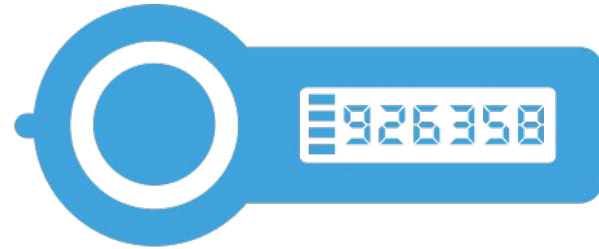
Authentication				
	Push	Passcodes	SMS Passcodes	Phone Callback
Description	Duo sends a login request to your phone. Just tap Approve to authenticate.	Generate a passcode when needed using the Duo app.	Receive a batch of passcodes via text message.	Duo calls your phone. Just press any key to authenticate.
Platforms	iOS Android Blackberry Windows Mobile	All Push platforms, plus Palm, Windows Mobile	All phones with SMS	All phones
Usable without WiFi or Cellular Service		✓	✓	✓

* Hardware tokens are available if you have a specific business need

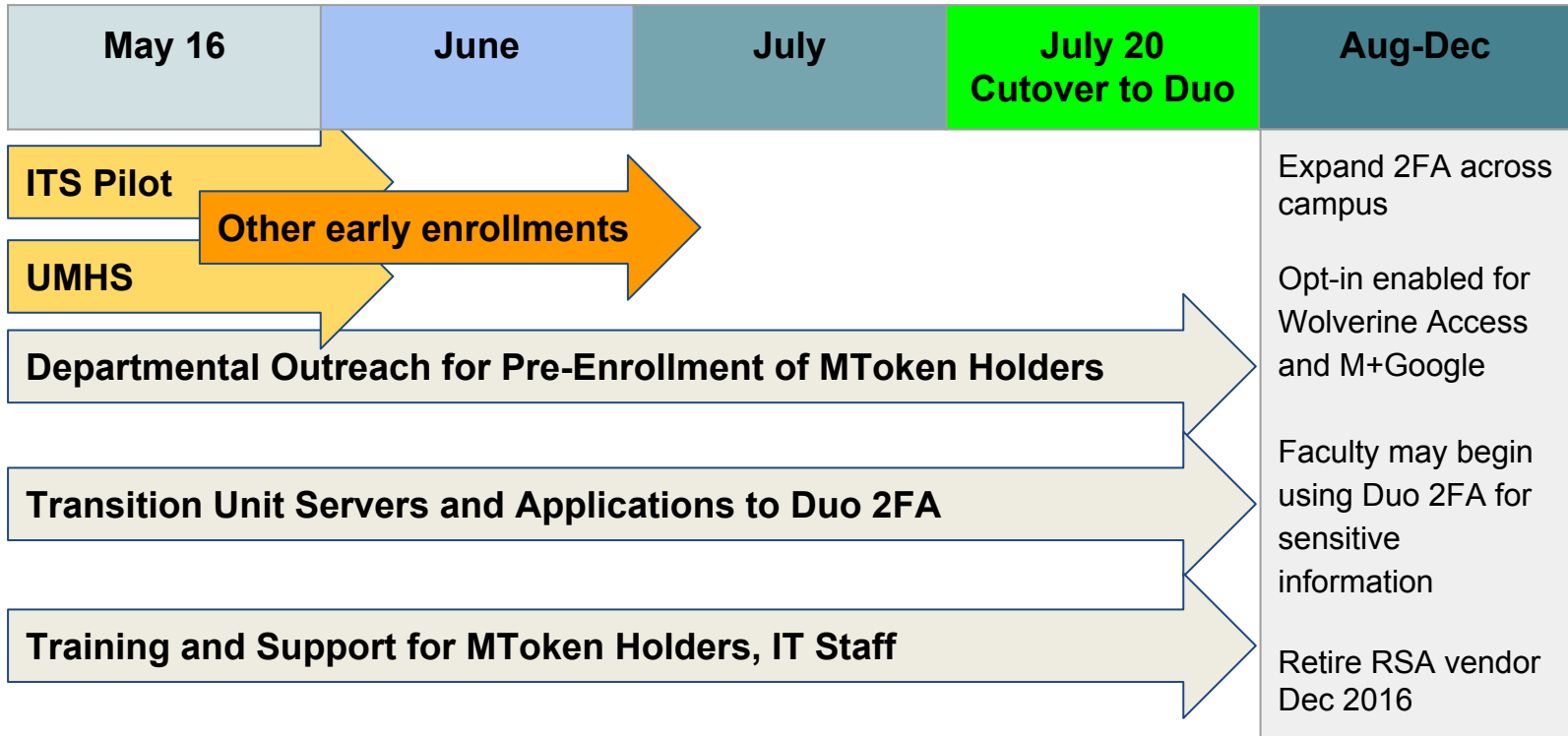


Hardware Tokens

- Current MTokens not compatible with Duo solution
- Must be replaced with new Duo hardware tokens
- Units responsible for cost of hard tokens
- Available for purchase at the Computer Showcase
(\$25)



2FA Pre-Enrollment Timeline



Pre-Enrollment Activities

1. Working with Unit/School/College to
 - a. Pre-enroll MToken Holders
 - b. Pre-enroll any departmental servers or applications
2. Work with IT, Admin, and IT Security Staff in each area
3. Send notices centrally with option for unit to communicate
4. Provide Communications Toolkit, eg email, digital signs
5. Pre-enrollment drop-in stations around campus
6. Training and online support with videos, how-to's



Working Together

- Champion the new Duo 2FA option for smartphones, Duo Mobile
- Encourage early enrollment to minimize disruption for your staff
- Coordinate with your area's [NextGen Unit Representative](#) and [Security Unit Liaison](#).
- If you're interested, volunteer to assist at a pre-enrollment drop-in session in your area.



Questions?

2FA.Project.Contact@umich.edu

New 2FA Option From Duo

<http://www.itcs.umich.edu/identity/2factor/>

MFA Project Website:

<http://its.umich.edu/projects/mfauth/>



Appendix

Authentication Methods & Enrollment Screenshots



Authentication Methods



Push Authentication

Easy, One-Tap Authentication

Users can quickly approve an auth request by pressing a single button. Or, report fraud to admins by tapping the red button.

Generate Codes for Any Two-Factor Service.

The application generates TOTP passcodes for login and can receive push notifications for easy, one-tap authentication on your iPhone, iPad, or Apple Watch.

This is the preferred method, and easiest to use!



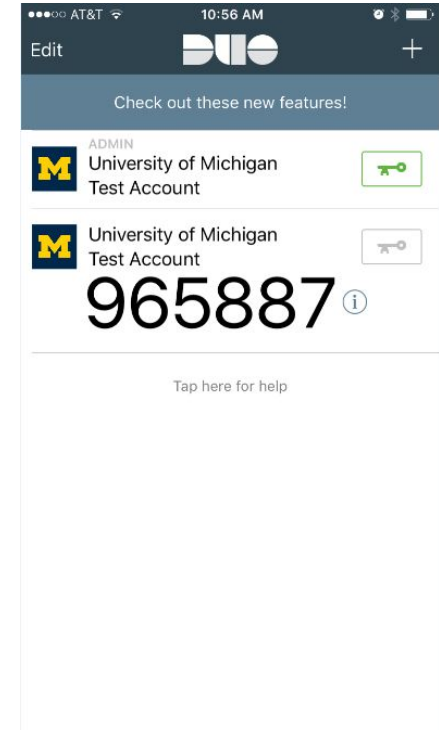
Passcodes

Bypass Codes			
User ^	Bypass Code ◇	Expires ◇	Remaining Uses ◇
kvarnsen (show)	Today 03:17 PM UTC	1
sogilby (show)	Never	10

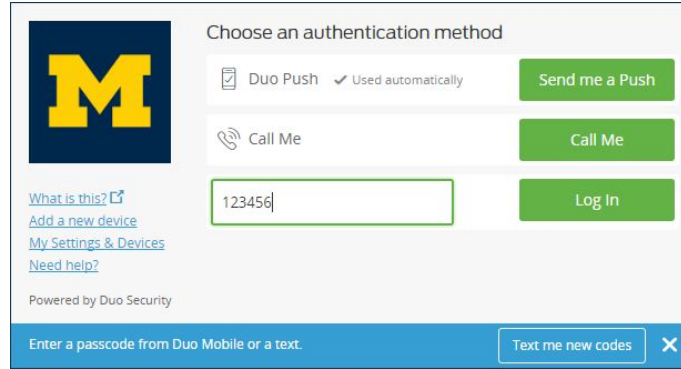
Generate bypass codes with Duo's administrative interface or API - no internet or data connection required

Single, event or time-based codes can also be generated for temporary contractors that may only need one-time or limited access.


To ensure security, codes expire after being used the allowed number of times or after 12 hours




SMS Passcodes



Choose an authentication method

 Duo Push ☒ Used automatically [Send me a Push](#)

 Call Me [Call Me](#)

[Log In](#)

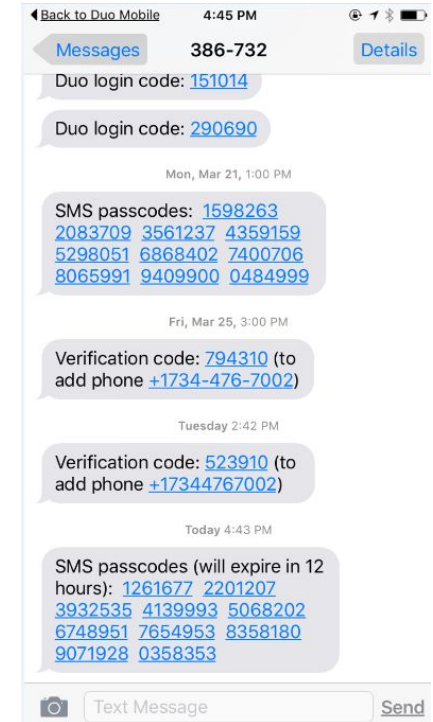
[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Enter a passcode from Duo Mobile or a text. [Text me new codes](#) [X](#)

For users without Internet connectivity, authenticate easily with Duo Security's SMS passcode method. After completing primary authentication, Duo's service sends you a one-time passcode via SMS on your phone.

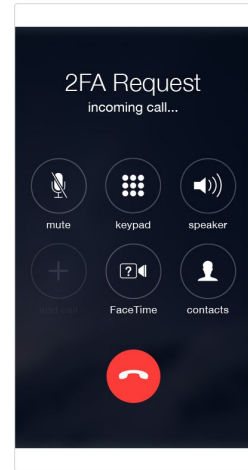
Simply type in the passcode and press enter to authenticate and access your accounts. Users can have new passcodes sent to their phones at any time.



Telephony

For users without a smartphone, authenticate easily with Duo Security's phone callback method. Call any phone registered to a user and let them authenticate by pressing a key.

Use smartphones, mobile phones or landlines to authenticate.



Enrollment Screenshots



Enrollment in the Duo Mobile App




The screenshot shows the 'UMICH ACCOUNT MANAGEMENT' page for the University of Michigan. The page has a dark blue header with the yellow 'M' logo and the text 'UMICH ACCOUNT MANAGEMENT' and 'UNIVERSITY OF MICHIGAN'. Below the header is a navigation bar with two tabs: 'Security Questions' and 'Two-Factor Management'. The 'Two-Factor Management' tab is highlighted with a red oval. Below the navigation bar is a list of links:

- [Choosing and Changing a Secure UMICH Password](#)
- [What Is My UMICH Password?](#)
- [What Is a Level-2 Password?](#)
- [Password Security Checklist](#)
- [Two-Factor Management](#)



Enrollment in the Duo Mobile App



[What is this?](#) 

[Need help?](#)

Powered by Duo Security

Protect Your University of Michigan Test Account


Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.


This process will help you set up your account with this added layer of security.

[Start setup](#)



Enrollment in the Duo Mobile App



[What is this?](#) 

[Add a new device](#)

[My Settings & Devices](#)

[Need help?](#)


Powered by Duo Security


What type of device are you adding?

- ☒ **Mobile phone** RECOMMENDED
- ☐ **Tablet** (iPad, Nexus 7, etc.)
- ☐ **Landline**

[Continue](#)

Enrollment in the Duo Mobile App



[What is this?](#) 

[Need help?](#)

Powered by Duo Security

Enter your phone number

United States ▼

+1 734-555-1212 ✓

ex: (201) 234-5678


☒ (734) 555-1212 This is the correct number.


Back

Continue



Enrollment in the Duo Mobile App



[What is this?](#) 

[Need help?](#)


Powered by Duo Security


What type of phone is 734-555-1212 ?

- ☐ iPhone
- ☒ Android
- ☐ BlackBerry
- ☐ Windows Phone
- ☐ Other (and cell phones)

BackContinue

Enrollment in the Duo Mobile App




[What is this?](#) 

[Need help?](#)

Powered by Duo Security

Install Duo Mobile for Android





1. Launch the Google Play Store app and search for "Duo Mobile".
2. Tap "Install" to install the app.

BackI have Duo Mobile installed



Enrollment in the Duo Mobile App




[What is this?](#) 

[Need help?](#)

Powered by Duo Security

Activate Duo Mobile for Android




1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.


[Or, have an activation link emailed to you instead.](#)

BackContinue



Enrollment in the Duo Mobile App




[What is this?](#) 

[Need help?](#)

Powered by Duo Security

Activate Duo Mobile for Android

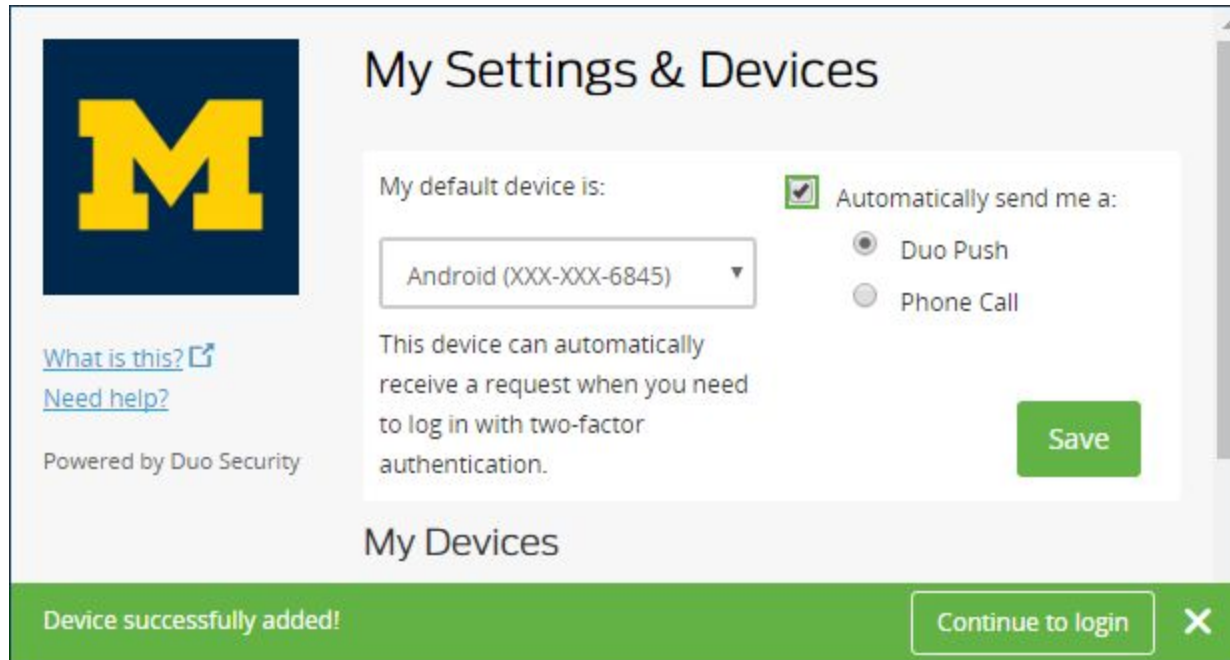


1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

[Or, have an activation link emailed to you instead.](#)

BackContinue

Enrollment in the Duo Mobile App



The screenshot shows the 'My Settings & Devices' page in the Duo Mobile app. On the left is a blue square with a yellow 'M'. Below it are links for 'What is this?' and 'Need help?', and the text 'Powered by Duo Security'. The main section is titled 'My Settings & Devices' and contains a dropdown menu for 'My default device is:' showing 'Android (XXX-XXX-6845)'. To the right, there is a checked checkbox for 'Automatically send me a:' with radio button options for 'Duo Push' and 'Phone Call'. A green 'Save' button is at the bottom right of this section. Below the settings is a 'My Devices' section. At the very bottom, a green banner displays the message 'Device successfully added!' with a 'Continue to login' button and a close 'X' icon.

My Settings & Devices

My default device is: Android (XXX-XXX-6845)

☒ Automatically send me a:

- ☒ Duo Push
- ☐ Phone Call

[What is this?](#) [Need help?](#)

Powered by Duo Security

This device can automatically receive a request when you need to log in with two-factor authentication.

Save

My Devices

Device successfully added! [Continue to login](#) ✕



Authentication with the Duo Mobile App



Authentication Required

Please enter your Login ID (username or Friend ID) and password to continue.

Need a Login ID?

[Create a Login ID now.](#)

Important Security Tips

Login ID

Password


Log In


[Forgot your password?](#)

[Login Help](#)



Authentication with the Duo Mobile App



[What is this?](#) 


[Add a new device](#)


[My Settings & Devices](#)


[Need help?](#)

Powered by Duo Security

Choose an authentication method

 Duo Push ☒ Used automatically Send me a Push

 Call Me Call Me

 Enter a Passcode Enter a Passcode



Authentication with the Duo Mobile App

