



TWO-FACTOR AUTHENTICATION PROJECT

*A QUICK INTRODUCTION TO
2FA AND ITS USE AT
GEORGIA TECH*

CREATING THE NEXT

AGENDA

What is Two-Factor Authentication (2FA)?

Why Two-Factor?

Two-Factor Project Goals

Cas + Duo Project Scope

Project Progress

Project Ahead

Project Considerations

Demo

TWO-FACTOR IS....



WHAT IS TWO-FACTOR AUTHENTICATION (2FA)?

Computer access control requiring two or more types of authentication factors

1. Knowledge Factor

- Something you know (*Password/hints*)
- Typical single factor method

2. Possession Factor

- Something you own/possess
 - Tokens

3. Inherence Factors

- Something you are (*Fingerprint(biometric)*)

4. Location Factors

5. Time Factors

WHY TWO-FACTOR?

- Because hackers are gonna hack!
- Passwords are not secure
- Successful phishing attacks escalate need for more secure system access
- Administrative Access
 - Data Access Risk



WHY TWO-FACTOR AUTHENTICATION?

- Currently, many critical applications are secured with a single authentication method using CAS
- Early phases of Two-factor Authentication with Duo for specific applications have been successful in limited release
- Institute directive to implement a multi-factor integrated solution on a more comprehensive scale

TWO-FACTOR PROJECT GOALS



CREATING THE NEXT

TWO-FACTOR PROJECT GOAL

- Maintain the integrity of Institute data and computing resources
- Build a framework for OIT and campus unit resources
- Provide two-factor authentication to faculty, staff, and students
- Leverage familiar access method with added multifactor capability to ease change impact

CAS + TWO-FACTOR PROJECT SCOPE

Slow and Steady!

- First: Experienced Duo users
 - Leverage existing tools for support used today
 - Cas
 - Passport
 - Technology Support Center (TSC)
 - Duo administrators

Identify opportunities for improved deployment in next phase

- President's Office and Cabinet
- Development Office

Campus Deployment for Administrative Departments in Phases

Deployment has been multi-phased to date:

- Phase 0: Campus Multi-Factor Infrastructure and VPN
- Phase 1: IT Systems
 - ✓ Users Impacted: IT Personnel
- Phase 2: Banner Grades
 - ✓ Users Impacted: Grade submitters (Limited faculty)
- Phase 3: Two-factor VPN for Campus Unit Firewalls
 - ✓ Users Impacted: Faculty and Staff
- Phase 4: Enforcement of all existing users of two-factor authentication
 - ✓ All of OIT
 - ✓ Primarily IT personnel on campus
- Phase 5
 - ✓ Development Office
 - ✓ Presidents Office and Cabinet

PROJECT AHEAD – NEXT STEPS

Phase 6 – forward

- Administration and Finance
- Academic Departments
- Faculty
- Students
- Retirees?

Current Use:

- Approximately over 4000 registered users



PROJECT PROGRESS CONSIDERATIONS

In progress

- Change management
- Out-reach to off campus users


NEW FEATURES

Self-service enablement methods

- Passport

- Two-factor menu – add or change a device
- Assist Another Person (Web of Trust) (Passport)
- CAS (login@gatech.edu) status of app

ASSIST ANOTHER PERSON (WEB OF TRUST)

Passport

[HOME](#)Logged in as GT Account **lburroughs7** [Logout](#)

Password
[Change Password](#)
[Hints](#)
[Information](#)
[Two-Factor](#)
[Assist Another Person](#)

Email
[Email Preferences](#)


Contact Info
[Directory Entry](#)
[Directory Nicknames](#)
[Your Photo](#)
[Emergency Notifications](#)

Sponsored Guests
[Manage Guests](#)


Assist Another Person

Note: Only use this tool to help people that you know well or whose government-issued ID you have checked.

You can assist other people with two-factor authentication in the following ways:



Set up Two-factor Authentication for a GT Account
You have access to register a phone with Duo for **everyone without Duo, except users with elevated privileges.**



Help someone log in by giving them a Rescue Code
A rescue code will let someone login without their phone or token for 24 hours. You have access to give them to **everyone with Duo, except users with elevated privileges.**

[Start Assisting Someone](#)

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

© 2014 Georgia Institute of Technology

[Emergency Information](#) | [Legal & Privacy Information](#) | [Accessibility](#) | [Accountability](#) | [Accreditation](#) | [Employment](#)

SINGLE SIGN-ON WITH DUO - DEMO

Enter your GT Account and Password
Login requested by: mail.gatech.edu

GT Account:

Password:

☐ Warn me before logging me into other sites.

LOGIN clear



[Settings](#)

Device:

Send me a Push

Call Me

Enter a Passcode

☐ Remember me for 1 day

RESOURCES

Website

www.twofactor.oit.gatech.edu

FAQ's

<https://faq.oit.gatech.edu/security>

<https://faq.oit.gatech.edu/duo-2fa>

<https://faq.oit.gatech.edu/content/using-2-factor-authentication-vpn-windows>

<https://faq.oit.gatech.edu/content/vpn-2-factor-authentication-osx>

Related References

<http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821>

Referenced in News Report: Symantec's Internet Security Threat Report

https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

QUESTIONS

