IT DIGITAL CHAT

August 11, 2017
AGENDA

Strategic Goals
EndPoint Project Update
Digital Learning Update
Passport Update
Unified Communications Update
Announcements
STRATEGIC GOALS

Transforming Teaching & Learning
Expanding Research
Streamlining Service Delivery
Enhancing Security, Privacy, and Accessibility
Investing in the Workforce
Aligning through Governance & Transparency
Continuously Transforming the Technology Enterprise
SECURITY BRIEFING

Jimmy Lummis
Interim Chief Information Security Officer
HISTORY OF ENDPOINT MANAGEMENT AT GT

• A long time ago in a galaxy far, far away...
  • LanDesk
  • EPO/McAfee

• The Empire strikes back
  • McAfee ate itself
  • OIT LanDesk support staff left
  • Microsoft SCCM and SCEP selected as the central solution for EPM and AV
  • SCCM has support challenges
A NEW HOPE

• Based on feedback from the campus IT community
• Project team formed to select a standard set of Endpoint Protection (EPP), Endpoint Detection and Response (EDR), and Endpoint Management (EPM) solutions
• The goals of the project are:
  • Select solutions that are best of breed and impact end users as little as possible
  • Hire staff to fully support an endpoint service
  • Deploy these standard solutions to all GT owned endpoints
FireEye HX selected as the campus standard solution for EPP/EDR
  • Procurement process has begun

EPM will likely be one of two choices which are being analyzed now
  • Series of best-of-breed point solutions to manage the endpoint computing ecosystem
  • Altiris
  • Deadline for selection is August 31st

The deployment phase of this project will begin this Fall
Pam Buffington
Associate Director, Academic Technology
WHY NEW LMS?

Rich DeMillo,
Center for 21st Century Universities
TRANSFORM: Cutting Edge Research, Development and Testing

Nelson Baker,
Professional Education
GROW: New Methods for Innovative Educational Programs

Bonnie Ferri,
Center for Teaching and Learning
TRANSFORM: Evidence-Based Teaching and Learning Methodologies

Mark Hoeting,
Office of Information Technology
RUN: Technology Infrastructure and Services Support

CREATING THE NEXT
NEW LEARNING MANAGEMENT SYSTEM (LMS)

18 months

53 People

1 Final Choice

canvas
WHO ELSE USES CANVAS?

- Stanford University
- Penn State
- UCLA
- Texas
- Berkeley
- Carnegie Mellon University
- University of Wisconsin
- University of Michigan
- University of Washington
CANVAS TIMELINE

Phase 1
INSTITUTE LMS ANALYSIS
- LMS Pilot
- Requirements Gathering
- Faculty & Student Surveys
- Provost Approval
Oct. 2015 - Aug 2016 Completed

Phase 2
SOLICITATION THROUGH ACQUISITION
- RFP Release
- Evaluation Selection
- Acquisition
Aug 2016 - Aug 4 2017 Completed

Phase 3
IMPLEMENTATION & MIGRATION FOR SELECTED LMS
- Planning
- Early Adopter
- Integration
- Migration
- Training
- Hire & Onboard Production Team
Aug 2017 - Dec. 2018 Ongoing

Phase 4
EOL Project Sites & Isolate T-Square
- Project Sites
- Restrict T-square
- Archive Data
Future
**FAQS**

**Website:** Canvas.gatech.edu  Information and Login link combined

**Support:** Tier 1 24x7 Canvas support for faculty, staff & students.
   Tier 2 GT via canvas@gatech.edu which go to Footprints.
   Multi-organization support channel at GT

**Training:** We have an unlimited training contract with Canvas.
   Canvas.gatech.edu/training

**SSO?:** Yes

**Auto provision courses/faculty/students?** Middleware script using BuzzAPI

**When does T-Square turn off?** Currently Unknown

**Can I have a project site on Canvas?** Try Dropbox, Onedrive, Sharepoint first.

**When will Canvas be generally available?** Midfall

**What can I do now?** Attend training and explore community

**More Questions:** go to canvas.gatech.edu or email canvas@gatech.edu
Passport Student
Two-Factor Tools

Jesse Rankin
Application Developer Sr.
The Challenge

- Two-factor authentication is important for security and to protect against phishing.
- Faculty and staff are already using two-factor.
- We need all students to be using it too.
- The scale creates a support issue.
COLLABORATION

The Two-factor Steering Committee:

- Scheller College of Business
- College of Science
- College of Engineering
- OIT Technology Support Center
- OIT Architecture and Infrastructure
- Cybersecurity
- Student Government
- and others
EFFECTIVE GOVERNANCE

• Steering committee prioritized the schedule and defined features
• All credit students registered in Atlanta will be required to enroll in two-factor by Oct. 16th
• Two technical parts to a successful rollout:
  Onboarding
  Support/Rescuing
Crowdsourcing Two-Factor Support

New tools for students now in Passport:

• Students with two-factor can onboard other students

• Students can specify trusted people who can help them log in

• 24/7 Support/Rescuing

• More convenient for students, less work for us
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:

- **Set up Two-factor Authentication for a GT Account**
  You can grant access to register a phone with Duo to GT credit students not yet set up with two factor.

- **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 People who have added you to their list of trusted people.

[Start Assisting Someone]
Search for a new person

**Assist Mary Friend**

**Set Up Two-factor Authentication for GT Account mfriend3**

Please fill out the form below to start setting up Duo two-factor authentication for this GT Account. After this form is submitted, Mary Friend will have to log into this site with their mfriend3 account to register the phone with Duo.

- **Phone number**

This phone will be used for two-factor authentication. International numbers must start with +

[Submit phone number] [Cancel]
Two-Factor Authentication

OIT is deploying DUO multifactor authentication services to campus constituents to better protect your identity and data at Georgia Tech. Multifactor authentication is a stronger form of authentication than our existing login/password method. When using DUO multifactor authentication with a web service or application, you will still be required to enter your traditional GT login and password at the familiar GT Login page. You will then also be required to use your DUO multifactor token as a second step in the authentication process.

Adam Student has granted you access to set up two-factor authentication with the phone number 404-555-1234. Would you like to set up two-factor authentication using this phone? Please confirm your number was entered correctly.

Yes, use this phone  No, this is not the right number
Set Up Two-Factor Authentication

* Phone Number
404-555-1234

Label for this phone (Cell, home, office, etc.)

My Cell Phone

* Phone Type
Mobile

* Phone Platform
Apple iOS

Send SMS texts with Duo App activation instructions to this phone (SMS charges may apply)

Note: Uncheck if this phone already has the Duo app set up for a GT Account. Sending texts will require you to reactivate.
TRUSTED PEOPLE

Your Trusted People

These people can help you log in when you don't have your device by giving you a Duo rescue code. You can use a rescue code to log in repeatedly for 24 hours. To generate a rescue code, they should log into this site and follow the directions in the 'Assist Another Person' section.

Add a trusted person

Adam Student  Remove
Assist Mary Friend

**Generate Two-factor Rescue Code for GT Account mfriend3**

This GT Account is set up with Duo. If they are having trouble logging in, you can generate a rescue code they can use to log in with Duo for 24 hours.

**Note:** Generating a rescue code will invalidate any current Duo passcodes for this account, including backup codes they might have previously printed.

**Duo rescue code:** 445361234

Please give this rescue code to Mary Friend. It is highly recommended that you do not send it in an email, since email is generally insecure. The rescue code is reusable for 24 hours.

If they need to fix their Duo configuration, Mary Friend should:

1. Log in to Passport at passport.gatech.edu with their GT Account mfriend3
2. At the Two-Factor Authentication page, press the 'Enter a Passcode' button
3. Type in the rescue code above
4. Press the 'Log In' button
5. Select 'Two Factor Authentication' from the Passport menu to correct their Duo settings and/or report their phone missing.
Two-Factor Authentication

Required - To avoid being locked out in the future if you don't have your device, please complete as many of the following as you can:

- Print Duo backup codes that let you log in without your device.
  - Generate codes

- Add a second device to your Duo account.
  - Add a phone
  - Add a token

- Specify at least one trusted person who can give you a Duo rescue code that lets you log in without your device.
  - Select a trusted person

Your Duo devices

Phones

- My Cell Phone (+14045551234)
  - Edit
- Apple iOS
  - Set up a new phone for this number or reinstall Duo app
  - Remove/Report missing

Tokens

- There are no tokens set up for this account.
  - Add a token

Add another phone
CONTINUOUS IMPROVEMENT

- We are steadily improving support tools
- More features on the way
- Please contact us with feedback or suggestions:

iam-support@oit.gatech.edu
UNIFIED COMMUNICATIONS UPDATE

Angi Whatley
Project Manager Principal
Replacement telephony system is needed. Opportunity to focus on a telephony solution that can be leveraged as a strategic investment to support the workforce collaboration needs of the future; creating a single, integrated approach between traditional phone lines, mobile devices, web conferencing, and video conferencing.
BACKGROUND

The current telephony system serving campus is end of life and will soon be end of support. This system supports approximately 11,000 phone lines throughout the institute.

The goal of this project was to replace our outdated technology which utilizes basic telephony to newer technology incorporating voice, video, and data communication. This innovative solution will provide unified communication and collaboration services across the entire institute, enhancing our workforce of the future, specifically around mobility and seamless transitions between voice, video, and data.
CISCO UCC SOLUTION

HD Audio and Video
Conferencing
File Sharing
1:1 and Team Messaging in Virtual Rooms
Mobile App
Desk and Room Devices
PHASED APPROACH

Phase 1 – Phones and Voice Mail
  • Phone replacement for current Polycom device users
  • Voice Mail migration with your phone service
  • Video Conferencing

Phase 2 – Collaboration Tools
  • Soft Clients
  • Cisco Spark
  • Enhanced WebEx
<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication to Early Adopters</td>
<td>Aug 14, 2017</td>
</tr>
<tr>
<td>(Rich, 811 and 845 Marietta)</td>
<td></td>
</tr>
<tr>
<td>Customer Training Starts</td>
<td>Sept 6, 2017</td>
</tr>
<tr>
<td>Early Adopters Building Migration Start</td>
<td>Sept 11, 2017</td>
</tr>
<tr>
<td>Rolling User Migration Starts</td>
<td>Sept 25, 2017</td>
</tr>
<tr>
<td>Migration Complete (12 weeks)</td>
<td>Dec 22, 2017</td>
</tr>
</tbody>
</table>
WHAT DOES THIS MEAN TO ME?

Phase 1 –

New phones to replace Polycom devices
New User Portal for Voice Mail
New Features for the Help Desk

Phase 2 –

Soft Clients (GT phone number on your desktop or mobile device)
Added features for better WebEx experience
Collaboration Tool using Cisco Spark
QUESTIONS??
General Announcements
# ITSM Update

<table>
<thead>
<tr>
<th>Employee</th>
<th>Role</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew Dietz</td>
<td>ITSM Service Manager</td>
<td>Service Delivery</td>
</tr>
<tr>
<td>Henry Jennings</td>
<td>Project Manager</td>
<td>PPMO</td>
</tr>
</tbody>
</table>

- **Finalize Vendor Recommendation Selection ETA very soon**
- **Provide Recommendation**
  - Phase One Business Process Assessment ETA 09/30/17
  - Incident Management
    - Additional areas TBD
  - Phase One Vendor Implementation of ServiceNow ETA before Dec 2017
    - Incident Management
      - Additional areas TBD
## TRANSFERRED EMPLOYEES

<table>
<thead>
<tr>
<th>Employee</th>
<th>Title</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Bryson</td>
<td>System/IT Architect Mg Sr</td>
<td>EIS/IDM</td>
</tr>
<tr>
<td>Christopher Craig</td>
<td>Assoc Director - Int</td>
<td>CyberSecurity</td>
</tr>
<tr>
<td>Kyle Koza</td>
<td>Information Security Engineer Principal - Int</td>
<td>CyberSecurity</td>
</tr>
<tr>
<td>Ambica Letkeman</td>
<td>Technical Analyst II</td>
<td>EIS</td>
</tr>
<tr>
<td>Joseph Schmitt</td>
<td>Support Prof II</td>
<td>AV</td>
</tr>
<tr>
<td>Cari Lovins</td>
<td>IT PM Principal</td>
<td>PPMO</td>
</tr>
</tbody>
</table>
# NEW EMPLOYEES

<table>
<thead>
<tr>
<th>Employee</th>
<th>Title</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ross Lindsay</td>
<td>Network Support Engineer I</td>
<td>Network Engineering</td>
</tr>
<tr>
<td>Henry Jennings</td>
<td>IT Project Manager Principal</td>
<td>PPMO</td>
</tr>
<tr>
<td>Malynda Dorsey Fulton</td>
<td>IT Project Manager Sr</td>
<td>PPMO</td>
</tr>
</tbody>
</table>