

# Penn two-step verification

October 2013

# Agenda

- Drivers
- Build vs buy
- Roll-out plan
- Description of system
- Technology choices
- UI features
- Experience to date



# Drivers

- Prevent stolen credentials to web applications
- Users ask about how they can protect their own data (tax forms etc)



# Build vs buy

- We decided to build in 2011(not sure exactly when)
  - Duo has less adoption
  - Duo was more expensive
- Looked at various options
- Decided to use google authenticator with a custom app for provisioning
- If we were doing it again, we would probably lean towards Duo
  - More integrations
  - Don't have to support the database/WS/UI



# Description of system

- Open Two Factor
  - Jasig incubated project (not sure the exact status)
  - Not Penn-specific
  - Can run on Oracle, MySQL, or Postgres
- Database with a few tables
- Internet2 subject API
- Java webapp for WS and UI



# Description of WS

- Restful
- JSON or XML
- One resource which tells the caller if the user is enrolled or if the two factor code is correct
- We have this integrated into Cosign
- PAM integration which can be used by, among other things, SSH (we don't have this rolled out yet)
- Java client that can be used command line



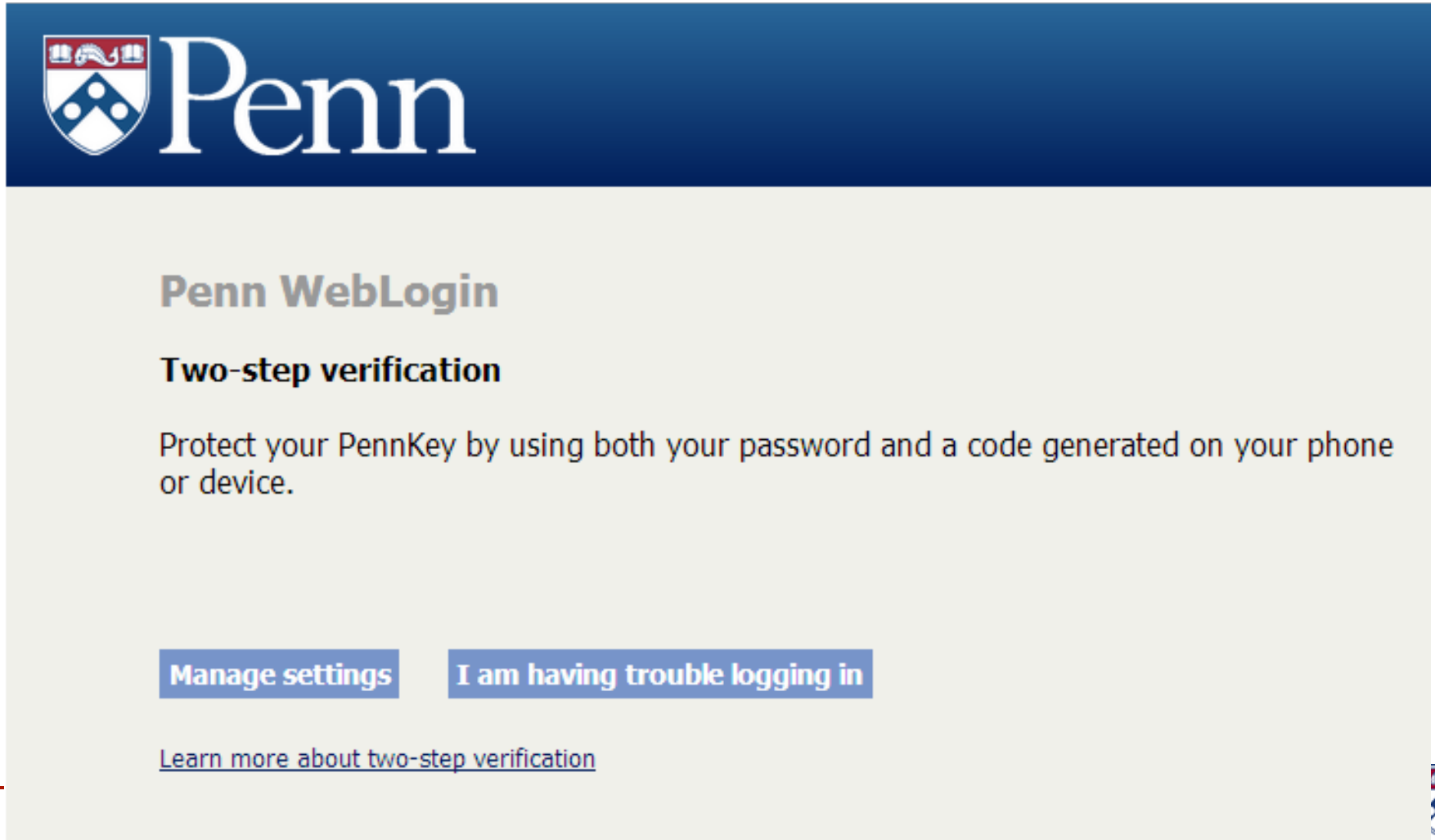
# Description of trusted browser

- Users can trust their browser for 30 days (if they don't clear cache)
  - This is a very useful feature
- The WS tells the caller which cookie value to set



# Description of UI - main

- Users can get to the main page without logging in



The screenshot displays the Penn WebLogin interface. At the top left is the University of Pennsylvania logo, featuring a shield with a book and a ship, followed by the word "Penn" in a large, white, serif font. Below the logo, the text "Penn WebLogin" is displayed in a bold, dark grey font. Underneath, the heading "Two-step verification" is shown in a bold, dark grey font. A paragraph of text explains: "Protect your PennKey by using both your password and a code generated on your phone or device." Below this text are two blue buttons with white text: "Manage settings" and "I am having trouble logging in". At the bottom left, there is a blue link that says "Learn more about two-step verification". The bottom right corner of the page features a small version of the Penn logo and the text "UNIVERSITY OF PENNSYLVANIA".





# Description of UI – trouble

- Users having trouble logging in can get to this screen by logging in with their pass (1 factor)

**Penn WebLogin** [Log out](#)

**Two-step verification: trouble logging in**

You are currently enrolled in this service

Trouble logging in? You have three options:

1. Enter the next unused single-use code on your printed list, generated when you opted in or later from the "Manage settings" page.
2. Send a single-use code to your backup phone:
  - Text: 21# ### ##47      Voice: 21# ### ##47
  - Voice: 21# ### ##12
  - Voice: 61# ### ##45
3. Authorize previously identified friends to opt you out of two-step verification:

You can authorize these friends to opt you out:

Br\*\*\* W H\*\*\*\*\*  
Ja\*\*\* C\*\*\*\*\*  
Ma\*\*\*\*\* F S\*\*\*\*\*

**Authorize friend(s) to opt you out**

To be opted out of two-step verification, [authorize your friend\(s\) to opt you out](#). Then call one of the friends listed above, ask them to log in to <https://twostep-test.apps.upenn.edu>, click "Manage settings" and then click "Help a

UNIVERSITY OF PENNSYLVANIA



# Description of UI – main not enrolled

## Penn WebLogin

[Log out](#)

### Two-step verification

Protect your PennKey by using both your password and a code generated on your phone or device.

[Opt in to this service](#)

### How it works

1. Enter your PennKey and password as usual.
2. When prompted, enter a code from your phone or other device.
3. Make your browser trusted (optional). If no one else uses that browser, you only need to enter a code every 30 days.

### Why you should use it

Two-step verification dramatically reduces the risk of someone stealing your data and your Penn identity. Even if they acquire your password, they still can't log in unless they also have your device.

Opt in

Profile

Activity

Help a friend

Admin console



# Description of UI – opt in

## Two-step verification: opt in

**Step 1 of 3:** [Install an authenticator app](#) on your mobile device or obtain a hardware token.

Once activated, your app or token will display a verification code that changes at frequent intervals.

**Step 2 of 3:** Activate the token and/or app(s).

[Activate a hardware token](#)

[Activate an app](#)

**Step 3 of 3:** Test the activation.

Enter the digits displayed by the authenticator app or token.  
(If activating both, enter digits from the token):

Enter six digits

[Test and continue](#)

Your enrollment is not complete until you test the activation.



# Description of UI – opt in fob

Step 2 of 3: Activate the token and/or app(s).

## Activate a hardware token

[Close](#)

Enter the secret value that came with the token

[Submit secret value](#)

Enter secret value from Deepnetsecurity or Gemalto keychain TOTP token, or any OATH TOTP 30 second or 60 second token. Store this secret value in a secure place. Note: hex and base32 formats are accepted and auto-detected. HOTP (non-time-based) tokens are not supported.

**b2 da c3 97 c6 9f 33 de d1 d**

(Hex code to enter into your Yubikey if applicable)

[Activate an app](#)



# Description of UI – opt in app

## Activate an app

[Close](#)

Scan the [QR code below](#) or enter this secret value into your device:

**WLNA YOL4 NHZT 33I5**

(Base32 for most authenticator apps.

Account name: mchyzer@test.upenn.edu. Select "time based".)

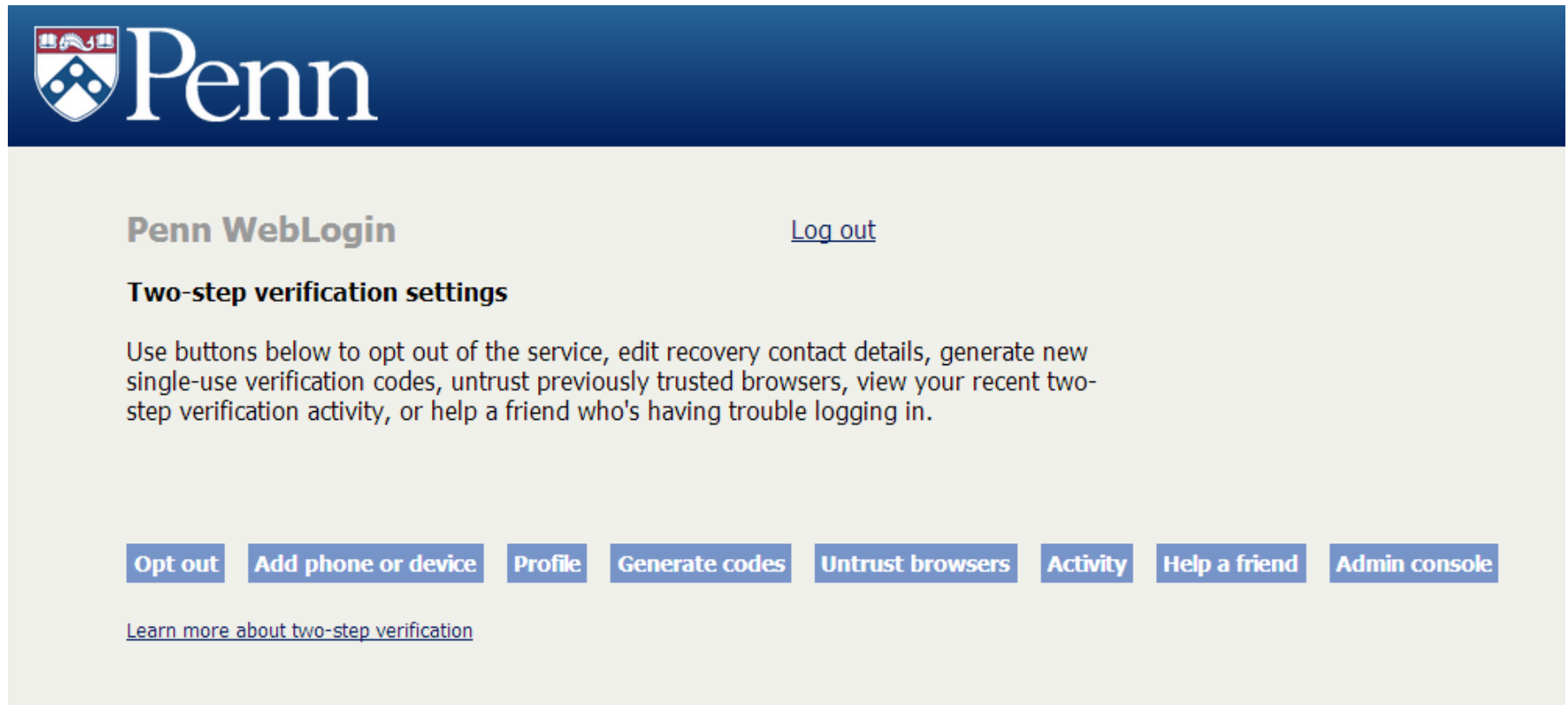
Do not store this QR code or secret value anywhere except in this device.

Note: if you want to use both a hardware token and an app, you must submit the token's secret value before activating the app.



# Description of UI – main opted in

- Main screen



The screenshot shows the 'Penn WebLogin' interface. At the top left is the Penn logo. To the right of the logo is the text 'Penn WebLogin' and a 'Log out' link. Below this is the section 'Two-step verification settings'. A paragraph of text explains the purpose of the buttons: 'Use buttons below to opt out of the service, edit recovery contact details, generate new single-use verification codes, untrust previously trusted browsers, view your recent two-step verification activity, or help a friend who's having trouble logging in.' Below the text is a row of seven buttons: 'Opt out', 'Add phone or device', 'Profile', 'Generate codes', 'Untrust browsers', 'Activity', and 'Admin console'. At the bottom left of the section is a link: 'Learn more about two-step verification'.



# Description of UI – profile

- Edit email, phone numbers, friends

Penn WebLogin

[Log out](#)

## Two-step verification profile

We can use your email address to notify you of updates and remind you of your settings. If you have trouble logging in, we can send a single-use verification code to the backup phone(s) you list below (via test or voice). You can use that code to log in once.

You can also identify one or more friends who may be authorized to opt you out of the service if you are having trouble logging in. Each should be someone who knows your voice, will answer your call, and is willing to help. To identify a friend, enter a PennKey, then select the correct person from the list that appears. (They will be notified by email that you have selected them.)

You **must** have an email address in the Penn Directory **and** choose at least two ways to help yourself in case of problems. So designate at least two phone numbers, two friends, or one of each.

<b>Email</b>	mchyzzer@isc.upenn.edu ( <a href="#">edit email address</a> )
<b>Phone number</b>	215-777-7777 <input checked="" type="checkbox"/> Voice <input checked="" type="checkbox"/> Text
<b>Phone number</b>	215-222-2222 <input checked="" type="checkbox"/> Voice <input type="checkbox"/> Text
<b>Phone number</b>	610-555-5555 <input checked="" type="checkbox"/> Voice <input type="checkbox"/> Text
<b>Friend</b>	B...s
<b>Friend</b>	J...
<b>Friend</b>	M...
<b>Friend</b>	
<b>Friend</b>	

[Edit](#)

# Description of UI – printed codes

**Penn WebLogin**

[Log out](#)

## Two-step verification: generate codes

**Note:** If your activated device is not available or not working, use one of the single-use verification codes below to log in.

Print the codes and instructions now using your browser, and keep them safe.

You can use each code once, in sequence. If you forget which code you used last, enter any **two** unused codes in sequence (separated by a space). If you lose your printed codes, or use them all, go to the "Manage settings" page and click the "Generate codes" button to create a new set. Any previously unused codes will be invalidated.

Currently valid codes:

---

1.	7		11.	3	
2.	6		12.	1	
3.	6		13.	0	
4.	2		14.	3	
5.	2		15.	0	





# Description of UI – activity log

Penn WebLogin

[Log out](#)

## Two-step verification history

Recent two-step verification actions are shown for Chris Hyzer.  
Browser and operating system are reported by the browser.

Date	Action	IP address	Domain name	Operating system	Browser	Trusted browser checked?	User logged in	Description
2013-Oct-16 08:02:10 AM	Trusted browser use	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 07:59:56 AM	Generate single-use codes	130	AI	Windows 7	Chrome	no	Chris Hyzer	
2013-Oct-16 07:59:50 AM	Trusted browser use	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 07:59:49 AM	Trusted browser use	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-15 06:01:34 PM	Trusted browser use	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-15 06:01:34 PM	Two-step verification	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was not previously trusted, password correct
2013-Oct-15 06:01:33 PM	Two-step verification required	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was not previously trusted
2013-Oct-15 06:01:16 PM	Two-step verification required	130	AI	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was not previously trusted



# Description of UI – help a friend

**Penn WebLogin**

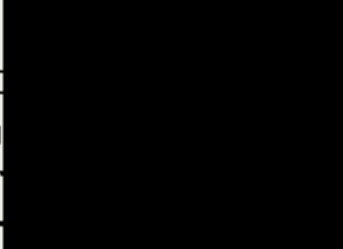
[Log out](#)

## Two-step verification: help a friend

Anyone who enrolls in two-step verification may identify one or more friends who can be authorized to opt them out of the service. Should they ever be without a valid verification code, they can click "Trouble logging in?" from the Penn WebLogin screen and authorize their friends to opt them out. They may then contact one of their authorized friends to complete the process.

If you have been authorized to opt someone out of two-step verification, a button will appear below allowing you to do so. Should you receive a request, be sure to verify the requester's identity. Voice recognition is best; email can be forged.

The following people have identified you as friends but have not yet authorized you to opt them out:

Lisa  
Rand  
Brya  
penn  
Char vey

# Description of UI – admin main

**Penn WebLogin**

[Log out](#)

Two-step verification admin

Person to manage

Submit

Opted-in users: 419

Opted-out users: 20

[Manage settings](#)

[Admin home](#)

[Email all users](#)

[Learn more about two-step verification](#)



# Description of UI – admin manage

Penn WebLogin

[Log out](#)

Two-step verification admin

Person to manage

Chris Hyzer is currently enrolled in this service

Date	Action	IP address	Domain name	Operating system	Browser	Trusted browser checked?	User logged in	Description
2013-Oct-16 08:13:25 AM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 08:13:24 AM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 08:13:18 AM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 08:13:14 AM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-16 08:13:14 AM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted
2013-Oct-15 09:21:09 PM	Trusted browser use	130	ait-sc-ait.edu	Windows 7	Chrome	no	Chris Hyzer	service does not require two factor, user enrolled in two factor, browser was already trusted



# Description of UI – admin email

Penn WebLogin

[Log out](#)

Two-step verification admin email all opted in users

Send email?

Email subject

Email body

Submit

# Description of UI – login screen



**Penn**  
UNIVERSITY of PENNSYLVANIA

## Penn WebLogin

### Two-step verification

Additional authentication is required.

Enter the code generated on your phone.

✓ PennKey and password accepted.

Verification code

Trust this browser for 30 days

[About two-step verification](#)

[Manage settings](#)

[Trouble logging in?](#)



# Documentation

- Doc page (google “penn two step”)
- FAQ
- Training videos
- Docs for support people



# Technology choices

- OATH
  - TOTP (preferred) or HOTP
- Google authenticator / Microsoft authenticator
- Duo client works too
- WinAuth is cool
- App is Java / SQL / Rest / PAM
- If someone doesn't have phone, they can use fob (DeepnetSecurity blade is recommended fob, approx \$15 each)
- Voice / text with Twilio and SMS matrix (HA)





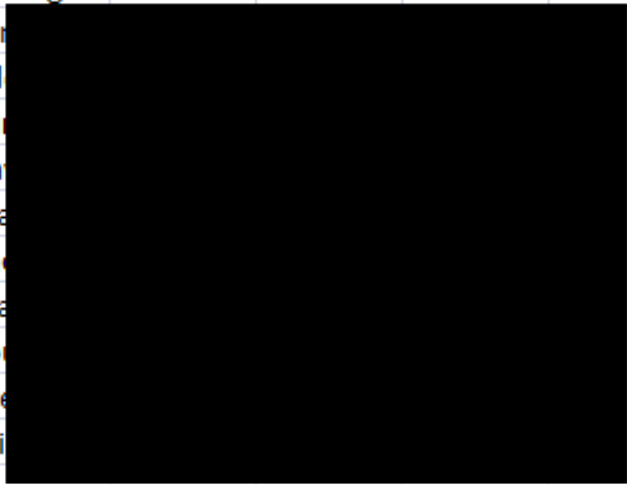
# Experience to date

- 400 opted in users
- CIO mandated all 270 central IT employees opt in
  - We reached 100% participation in central IT
- Users generally have a good experience, trusted browser helps
- We will do a survey in a month for official feedback
- Currently we consider it a “pilot”, we will see what we need to do to productionize it, and discuss switching to Duo



# Reports to managers

Org	Opted in	Requested fob	Total	Opted in or fob	Managers
isc misc 9100	6	1	10	70%	tor
isc finance and hr 9101	4	3	9	78%	gd
isc ait 9142	47	8	72	76%	cu
isc seo 9143	13	2	24	63%	da
isc ops 9145	8	16	24	100%	ma
isc astt infosec 9147	11	0	11	100%	ch
isc ait project office 9148	8	0	8	100%	ma
isc communications 9156	3	1	4	100%	co
isc tss 9157	20	5	33	76%	ase
isc n and t 9166	38	8	78	59%	mi
TOTAL ISC	158	44	273	74%	



em

