OMG WTF SSO:
A beginner's guide to SSO (mis)configuration

SREcon EMEA 2024
2024-10-29
Adina Bogert-O'Brien

usenix SRECON EUROPE MIDDLE EAST AFRICA

DUBLIN, IRELAND
29–31 October, 2024

www.usenix.org/srecon24emea

What *exactly* am I going to talk about?

usenix SRECON EUROPE MIDDLE EAST AFRICA

Covered

- Making sure a **vendor's SSO** offering **works for your business**

Not covered

- everything **your IT** needs to set up to make SSO work on your side.

Maybe a bit?

- **how to be a good vendor** to enterprises?

Why am I giving this talk?

Bad SSO can make you **feel safe**,

while **hiding vulnerabilities**

Why am I giving this talk?

Empower yourself and your colleagues
to **ask questions!**

usenix SRE CON EUROPE MIDDLE EAST AFRICA

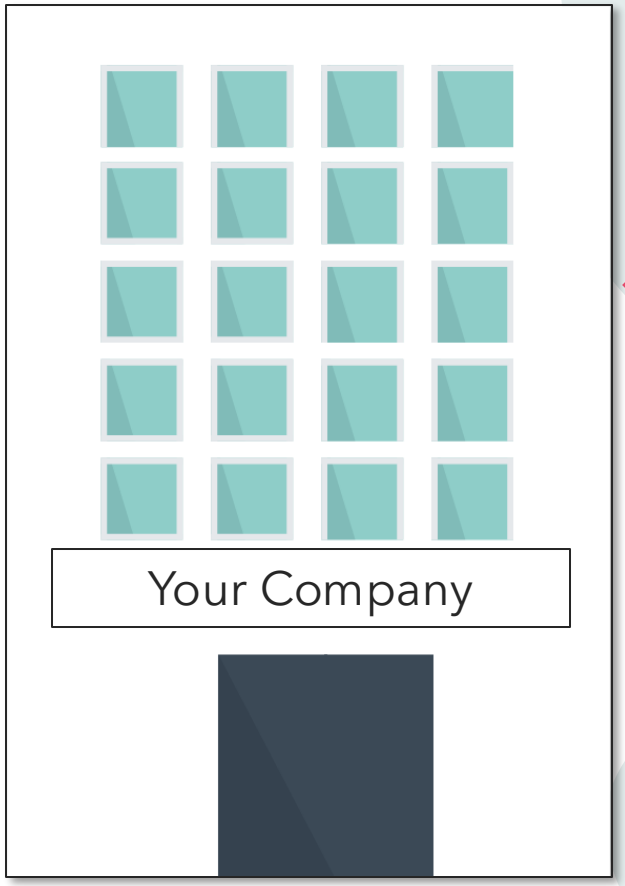
What the heck is SSO anyway?

And why does your company want it?

Single sign-on (**SSO**) is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

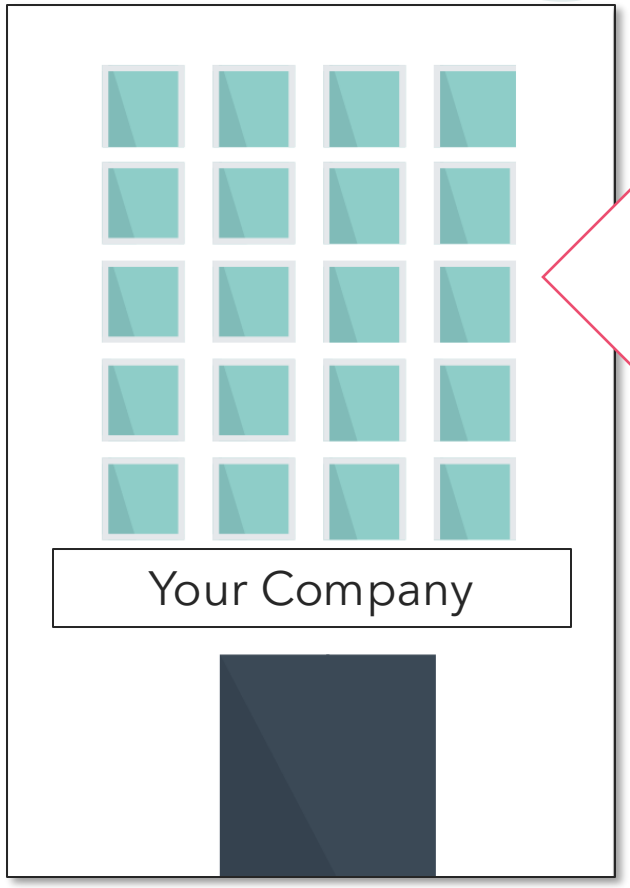
Wikipedia contributors, "Single sign-on", *Wikipedia, The Free Encyclopedia*, 14 November 2023

Your company in the past: under your control



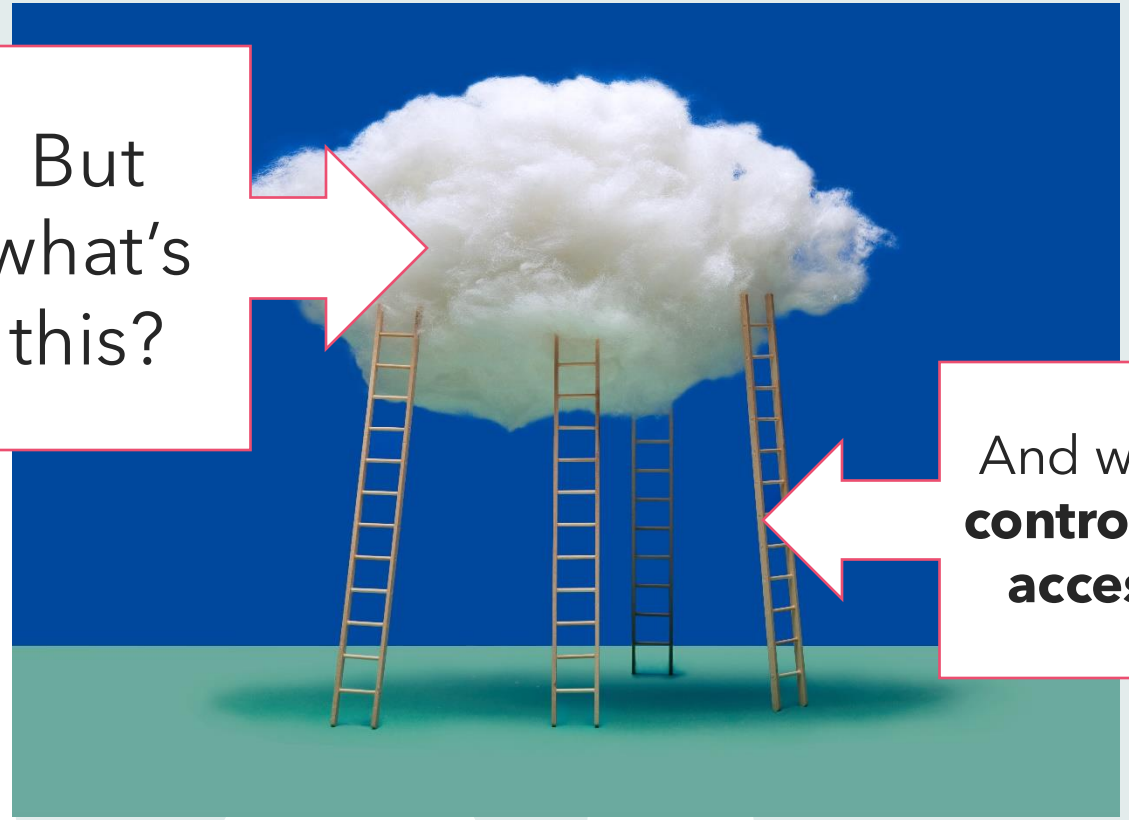
All your stuff
is in
your systems

Your company now: a cloudy mess



Some stuff is still here

But what's this?



And who's **controlling access?**


Vendor stuff

The dream

- **centralize** managing users
- **make life easier** for your colleagues
- enforce consistent **security standards**

The reality

- SSO protocols are just **a way** for your company's Identity Provider **to tell your vendor "Yeah, that's Bob"**

Why am I giving this talk?

Step 1: **Idealism**

- SSO is good!
- My vendors offer SSO
- I'll **just turn it on** and ***everything will be fine***

Me, **recently**

Why am I giving this talk?

Step 2: **OMG WTF SSO**

- What do I actually **need?**
- **What** can my vendor **do?**
- **Ask weird questions:** communication is hard and people make mistakes

Me, **now**

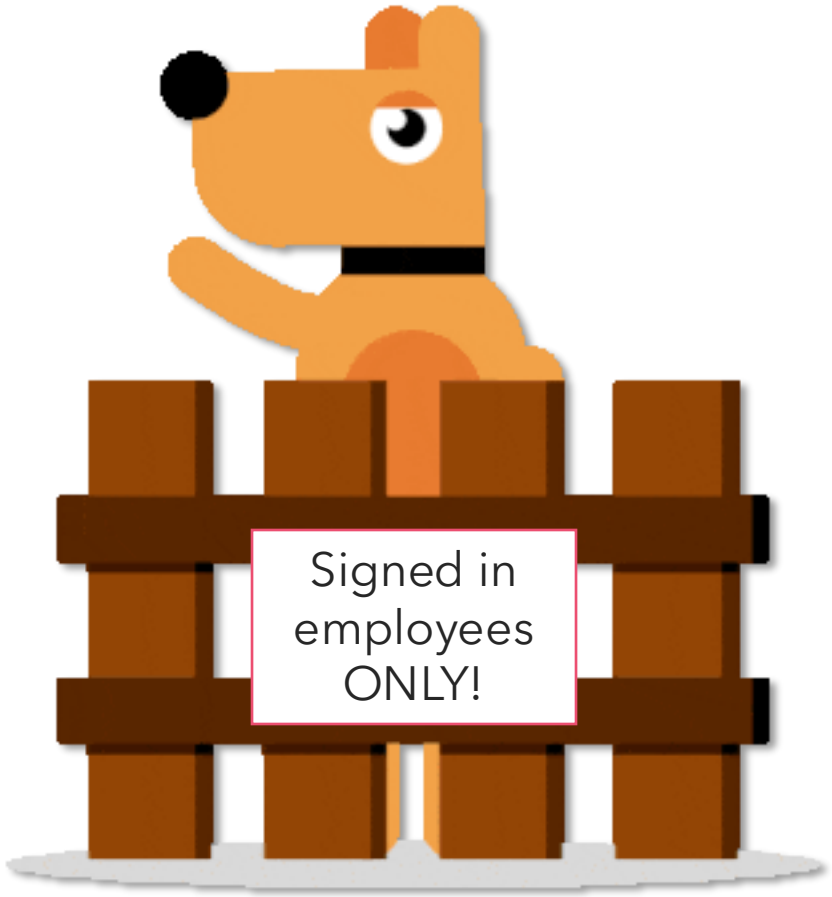
Why am I giving this talk?

Step 2: **OMG WTF SSO**

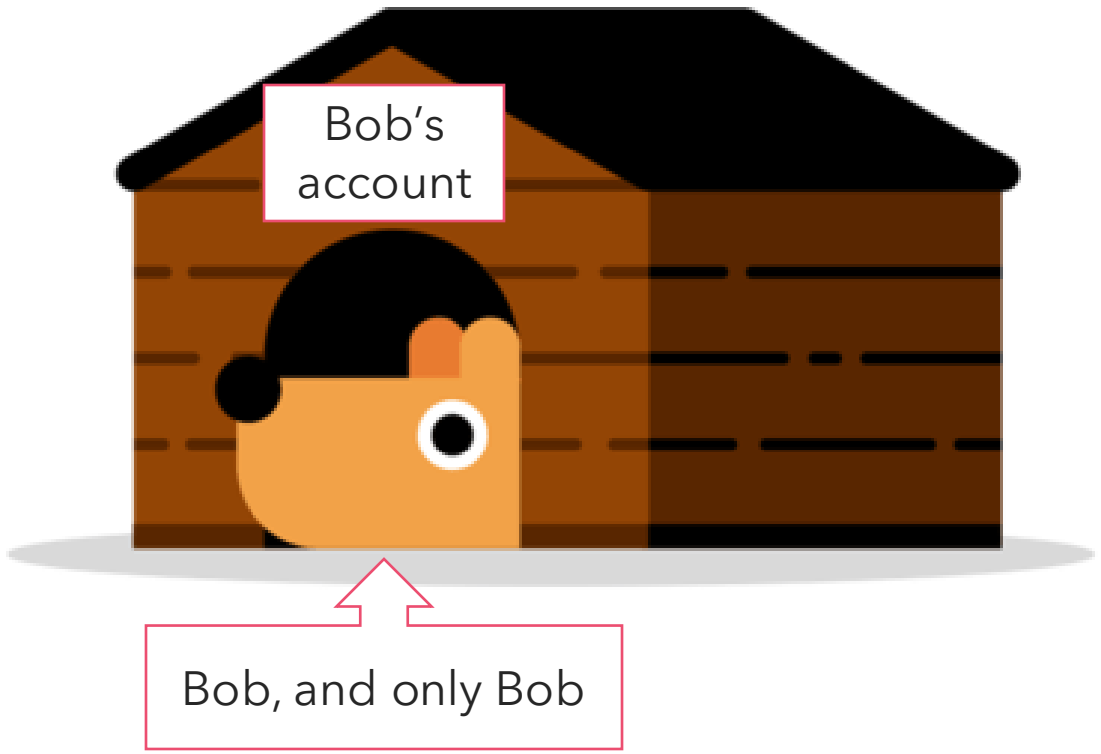
- What do I actually **need?**
- **What** can my vendor **do?**
- **Ask weird questions:** communication is hard and people make mistakes

Me, **now**

usenix SRECON EUROPE MIDDLE EAST AFRICA



Need #1: Users must sign in through **my company**



Need #2: Users can **only access** their **own** stuff

Why am I giving this talk?

Step 2: **OMG WTF SSO**

- What do I actually **need?**
- **What** can my vendor **do?**
- **Ask weird questions:** communication is hard and people make mistakes

Me, **now**

SSO doesn't come first (or even third)

They're building a Cool New Internet Thing!

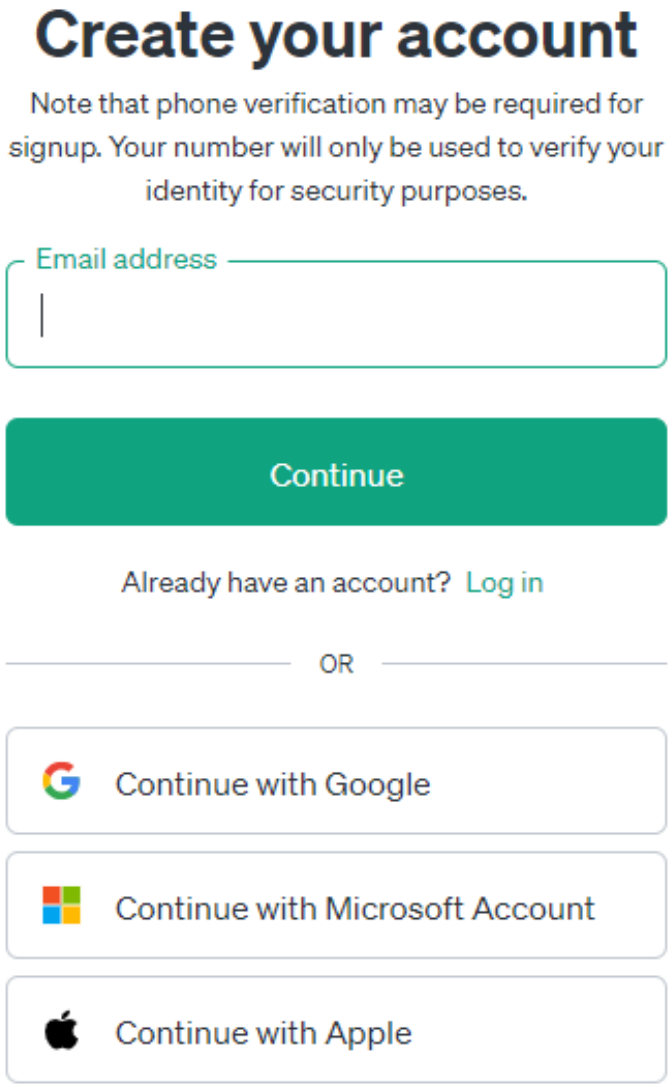
SSO comes wayyyy later, thanks to pesky customers.

usenix SRECON EUROPE MIDDLE EAST AFRICA

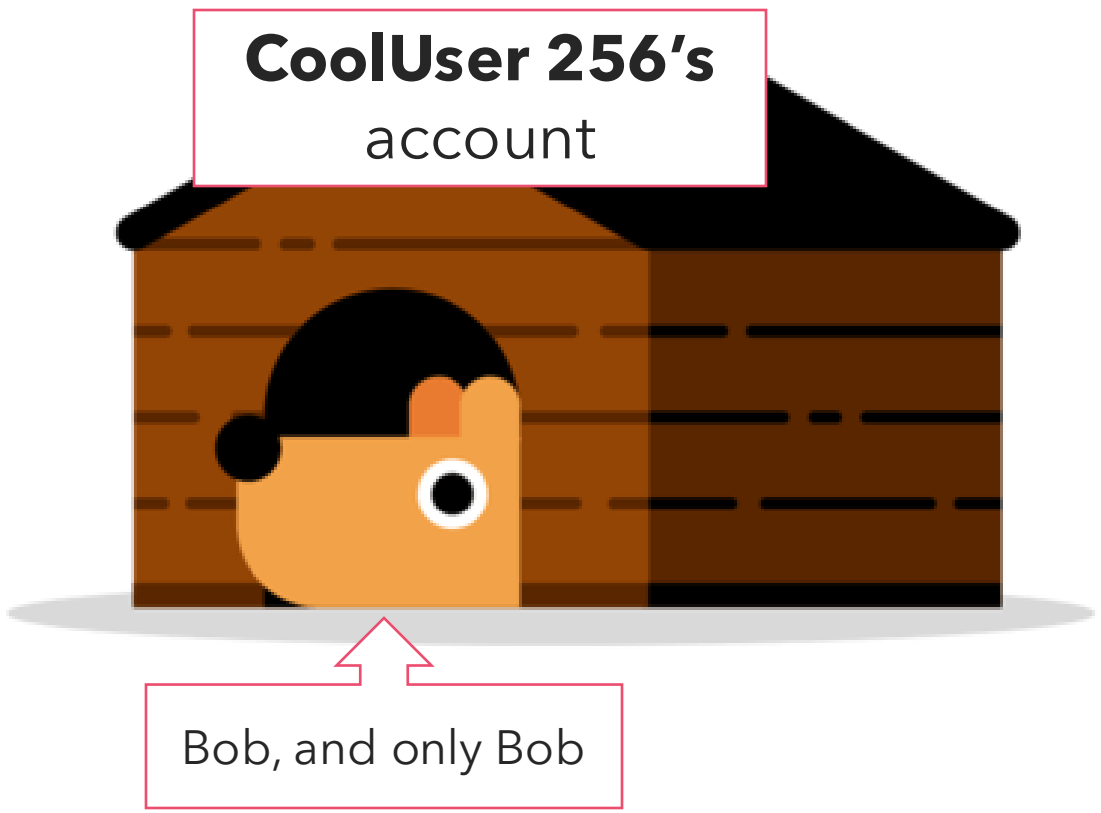
usenix SRECON EUROPE MIDDLE EAST AFRICA

When they do build SSO

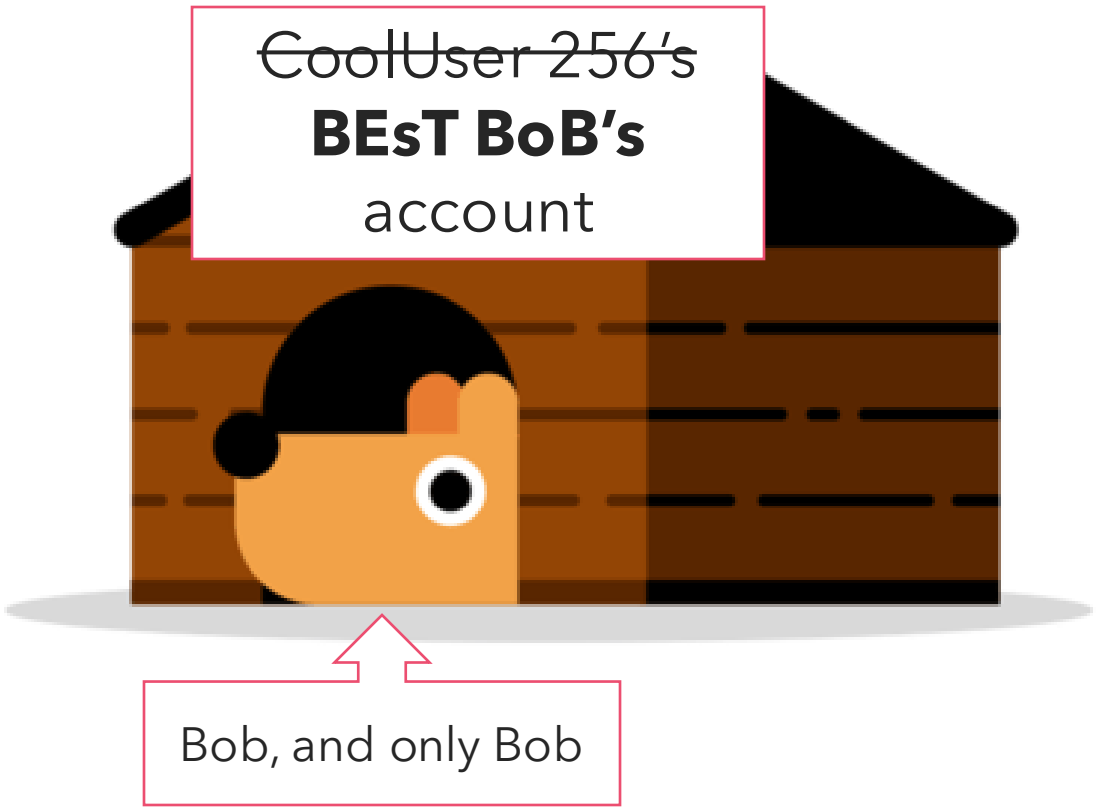
They have **different ideas** about SSO than you!



Maybe they want to **allow** SSO, but **not force it**

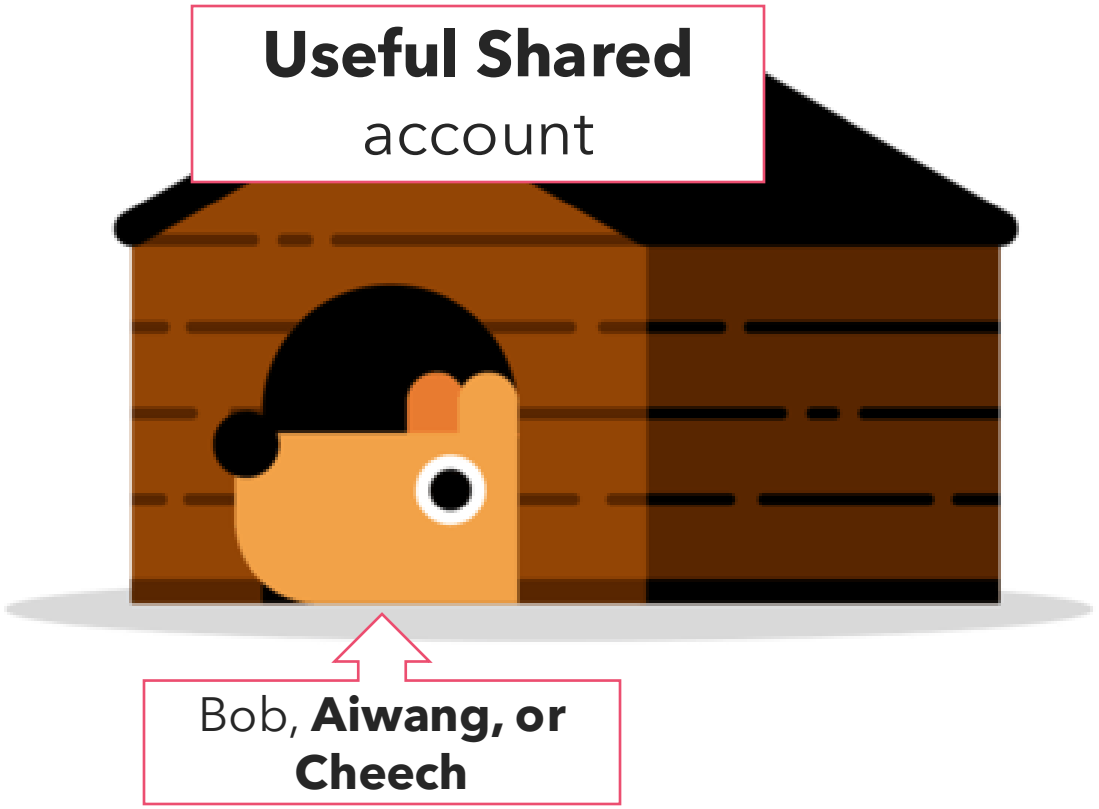


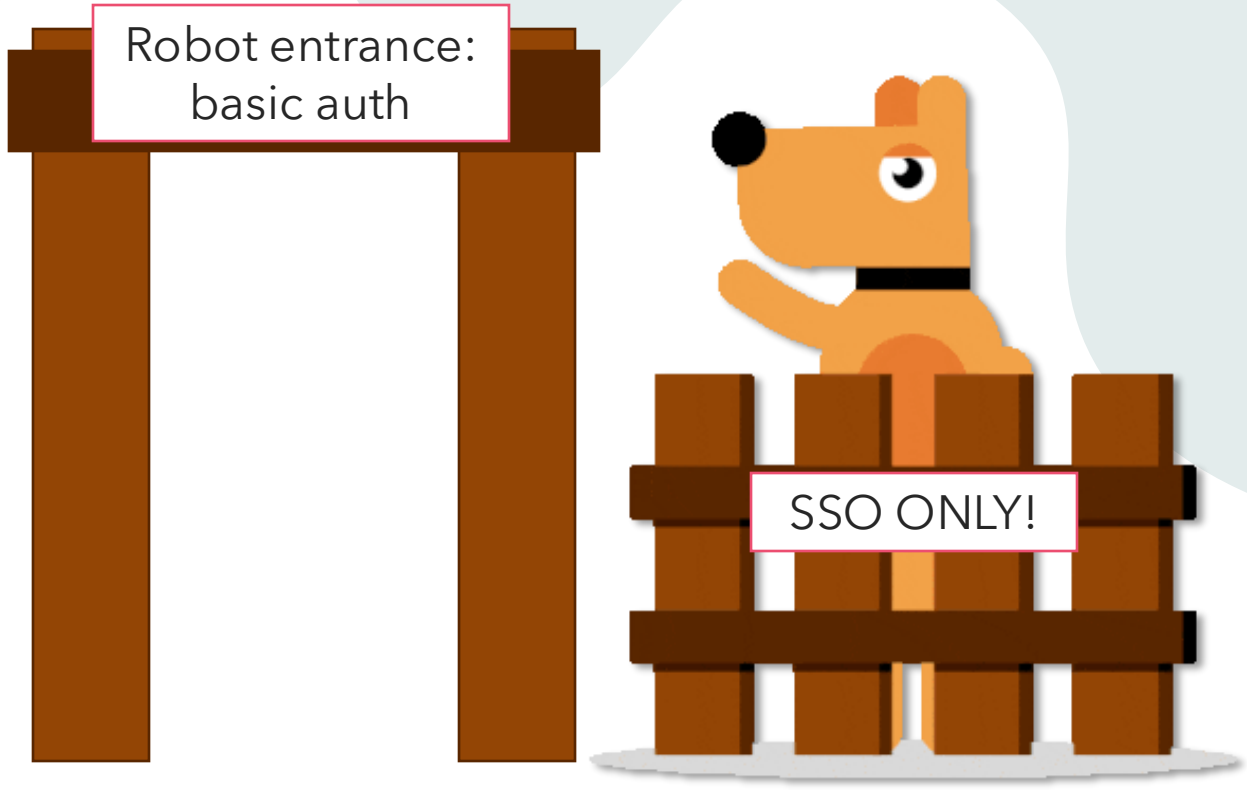
They might not care about usernames matching



They might let users change their own info

They might have good reasons to have different rules



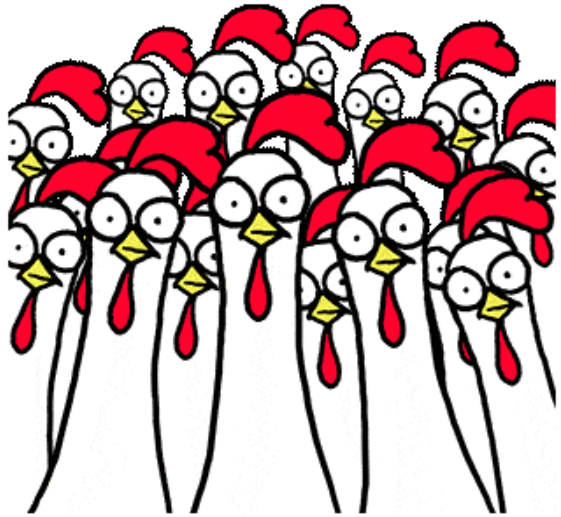


There might be places where username & password is still available

So now we know what **we need**, and what the **vendor can do**

Vendor accounts

Your company identities



How to translate between chickens and broccoli???

ASK QUESTIONS

don’t just assume!

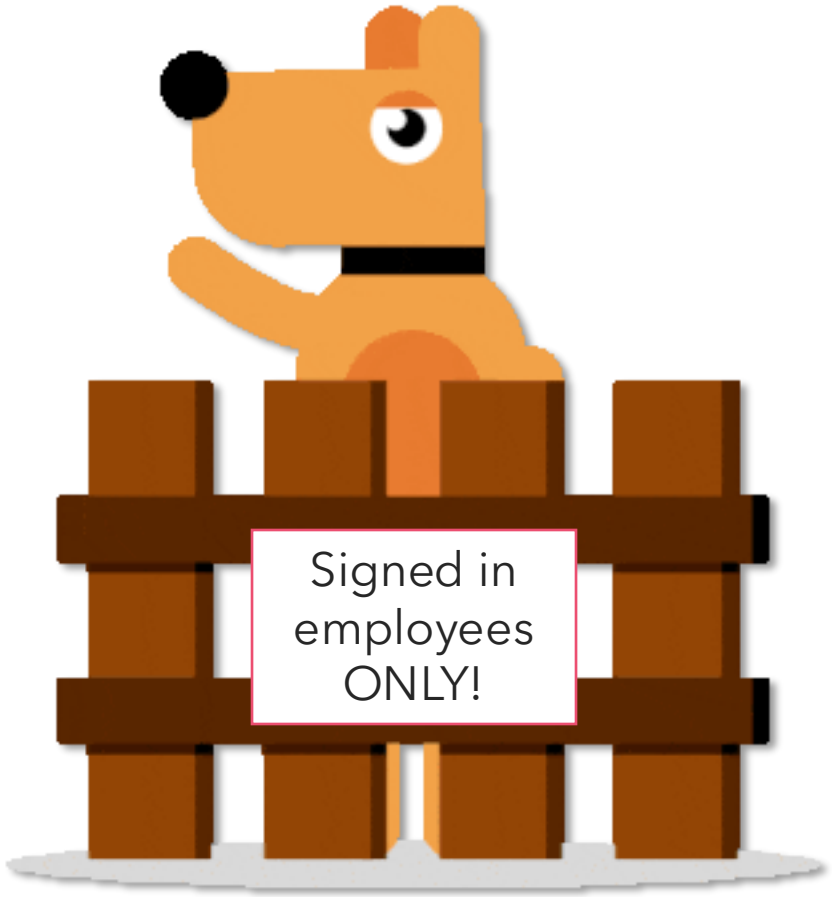
Why am I giving this talk?

Step 2: **OMG WTF SSO**

- What do I actually **need?**
- **What** can my vendor **do?**
- **Ask weird questions:** communication is hard and people make mistakes

Me, **now**

Need #1: Users must sign in through **my company**



a) **Only** use **my company's** sign in

b) **Force** use of SSO

Weird questions about a) **Only** use **my company's** sign in

Is there a way that someone signing in to a **different identity provider** could get into one of **my org's accounts**?

Failure case

Turning “sso on” for your org’s accounts still allows **anyone else** with:

- **Any** signed in identity in any **other SSO setup** connected to the vendor
- The **username/password** for any of **your org’s vendor accounts**

to **link their signed in user identity** to **your** org’s vendor **account**.

Nobody gets notified (not you, not the user)

Weird questions about b) **Force** use of SSO

- Will you ever **fail** over **away** from my sign in?
- What access is enforced for **API users**?

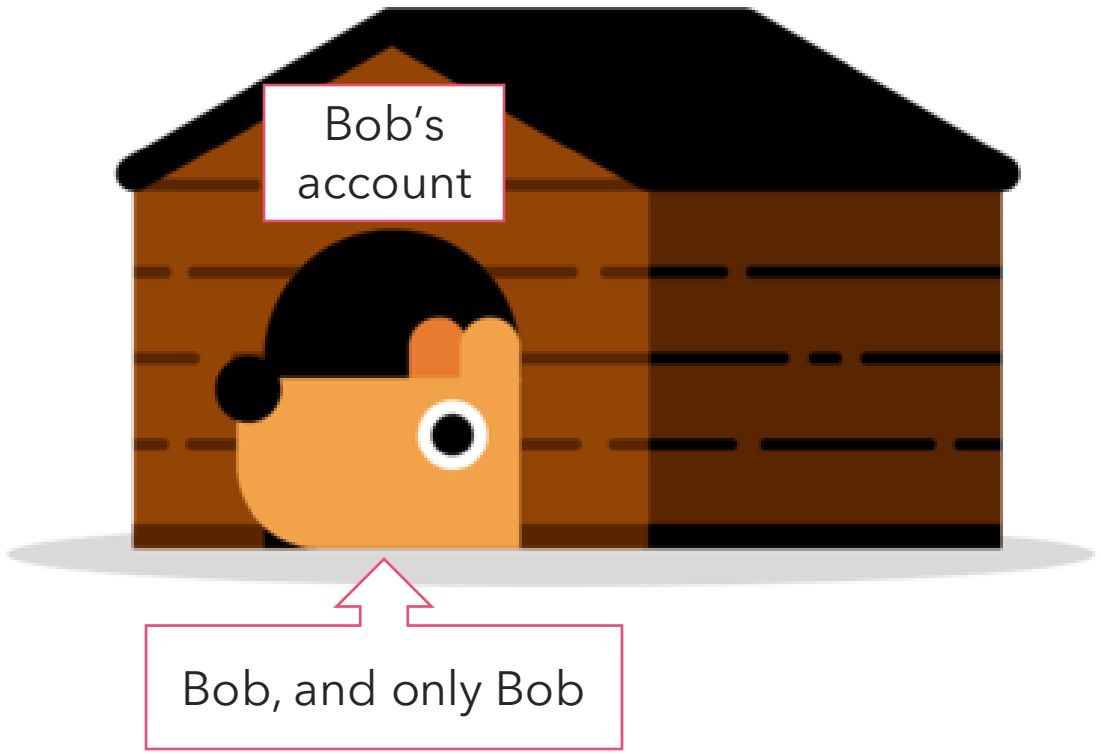
Failure case

The vendor has:

- **enforced SSO** using the **user interface**,
- Given me **control** over how **API** users authenticate

But…

Their own app can’t use SSO



Need #2: Users can **only access** their **own** stuff

a) Bob* can **only** access **Bob's** vendor **account**

b) I don't want **shared accounts**

* Authenticated to Bob's ID with my identity provider

Weird questions about **a)** Bob* can **only** access **Bob's** vendor **account**

If **Bob** has the **username and password** for **Alice's vendor account**, can he access Alice's account too?

Does the **attribute mapping** rely on **non-user-editable** fields?

You do have **attribute mapping**, right?

What happens if I **change everything** possible on my account? Can I still get in?

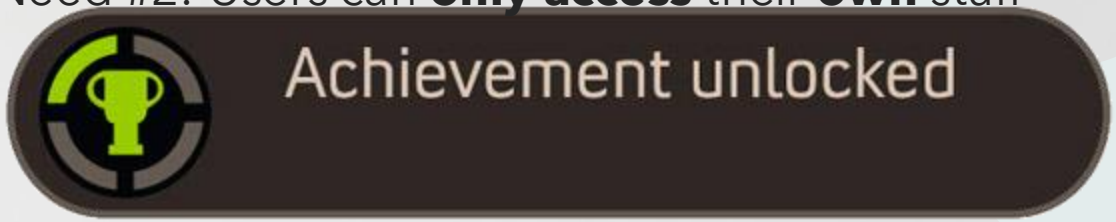
* Successfully signed in to Bob's identity with my identity provider

Failure case

Attribute mapping wasn't in the **MVP**.

The vendor just made a big ol' lookup table of **usernames** linked to UDPs of the linked IdP.

Vendor account username is **editable by the user.**



Failure case

Attack unlocked!

1. **Make an account** in your org with a **username** you think **your competitor** will use: CalCompetitor
2. **Link** that to one of **your identities (eg: Adina)**
3. **Change** the username: testestest
4. **Competitor makes account** with username CalCompetitor
5. **Adina can get in** to that account and no-one will know

Weird questions about **b)** I don't want **shared accounts**

How has the vendor designed shared accounts to work?

Are they SURE they don't allow them? Not anywhere?

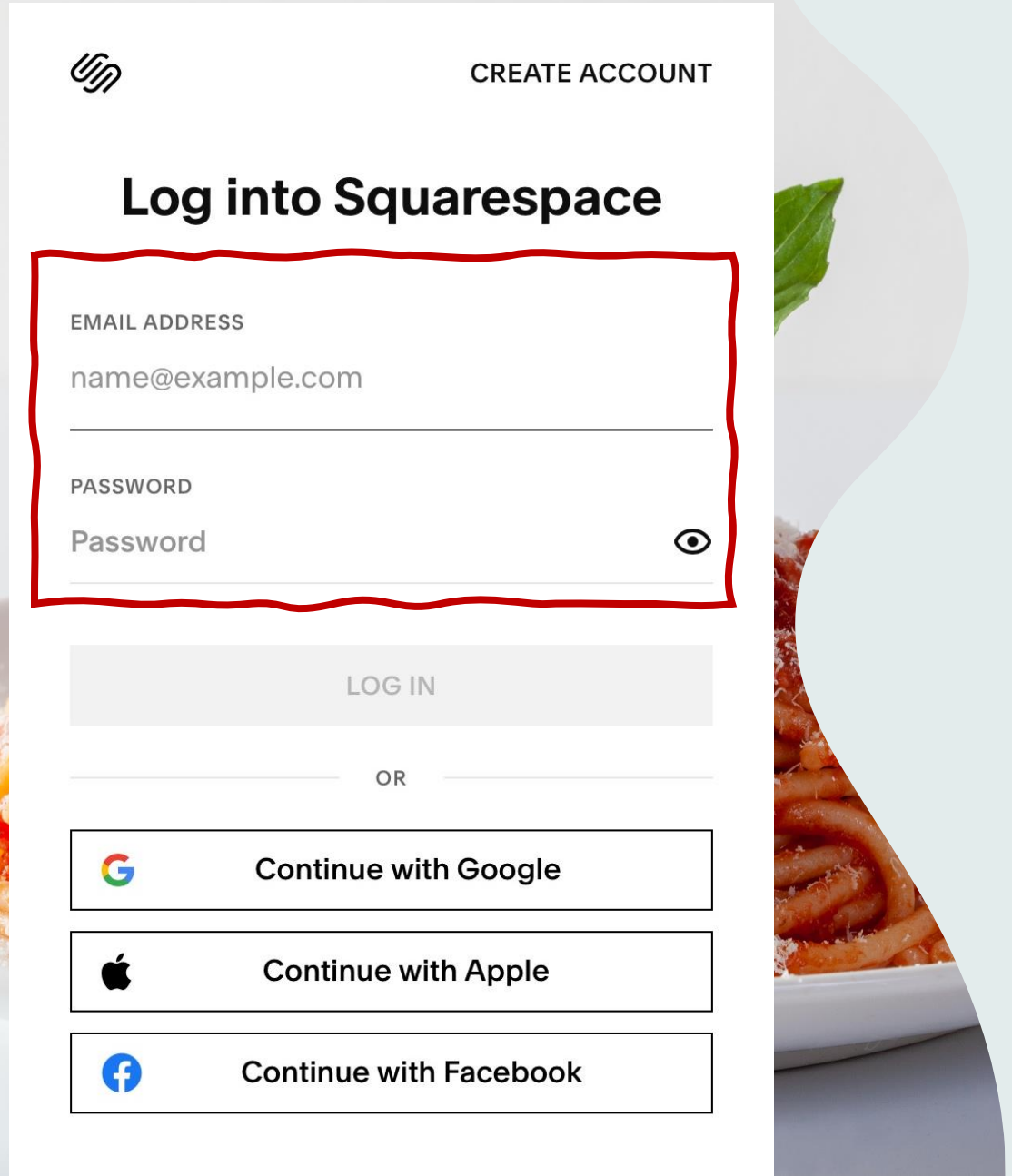
Failure case

You didn't ask, but they do offer shared accounts…

All it takes is:

1. Bob signs in to **my company**
2. Bob enters Alice's **vendor username and password**, and
3. now **Alice's** account can be accessed by **Bob and** Alice.

Need #1: Users must sign in through **my company**



Squarespace / Google domains

After the migration:

- **Domain admin accounts** created for migrated domains
- Can be **email/password combos**: **guess** the right email, **make up** your own password
- **No email confirmation required**

Domain admin accounts are **ALSO Google Workspace admins** (“so your reseller can help with troubleshooting”)

What's the point?

Misconfiguration is nothing new!

This talk is boring and nobody needs it because there are a million ways to fail, just do it right!

What's the point?

Your colleagues, managers, SREs, and key account managers **might not know** that messing this up is easy and common.

What's the point?

Empower your **colleagues**, and **yourself** to **ask questions** and not make assumptions!

usenix SRECON EUROPE MIDDLE EAST AFRICA

So please, **ask me questions!**

- Adina Bogert-O'Brien
- https://discontinuity.ca/