



Shared IT Services for Higher Education & Research

Conference 2017



Keeping the “single” in single sign-on

Sean Feil

University of Calgary

Video

“The dream”



Sean Feil

Identity, Messaging, and Middleware



UNIVERSITY OF CALGARY
Information Technologies

- Why is usability so important for security?
- Does Single Sign-on help with usability?
security?
- What challenges are there with building a truly
Single Sign-on environment?

Usability

Nielsen Norman Group

Learnability
Efficiency
Memorability
Errors
Satisfaction

Nielsen Norman Group

Enter LOGON parameters below:

Userid ==> KC03A00

Password ==> █

Procedure ==> IKJACCNT

Acct Nmbr ==> ACCT#

Size ==> 4096

Perform ==>

Command ==>

RACF LOGON parameters:

New Password ==>

Group Ident ==>

Enter an 'S' before each option desired below:

-Nomail

-Nonotice

-Reconnect

-OIDcard

PF1/PF13 ==> Help PF3/PF15 ==> Logoff PA1 ==> Attention PA2 ==> Reshow

You may request specific help information by entering a '?' in any entry field

softsmith

Central Authentication Service



UNIVERSITY OF
CALGARY

Sign In

[Create an eID](#) | [I cannot access my account](#) | [About CAS](#) | [Disclaimer](#)

Usability

Accessibility

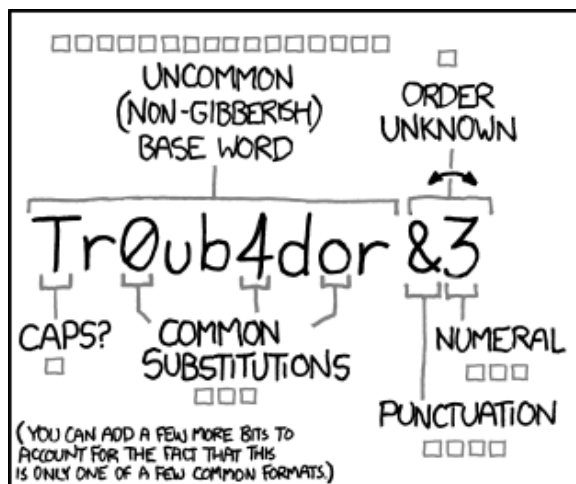


Security

AviD's Rule of Usability:

**Security at the expense of usability
comes at the expense of security.**

<https://security.stackexchange.com/a/6116>



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

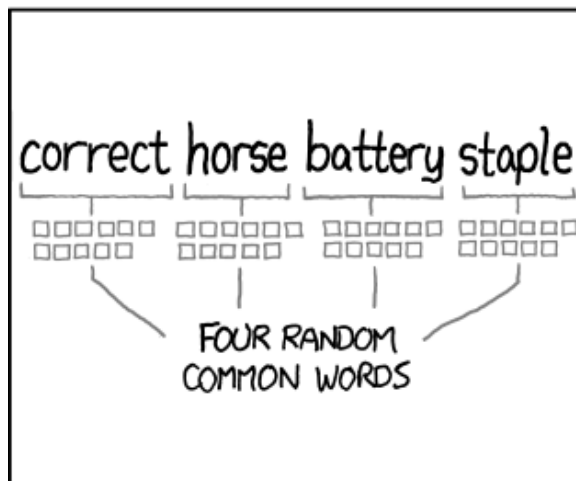
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<https://xkcd.com/936/>

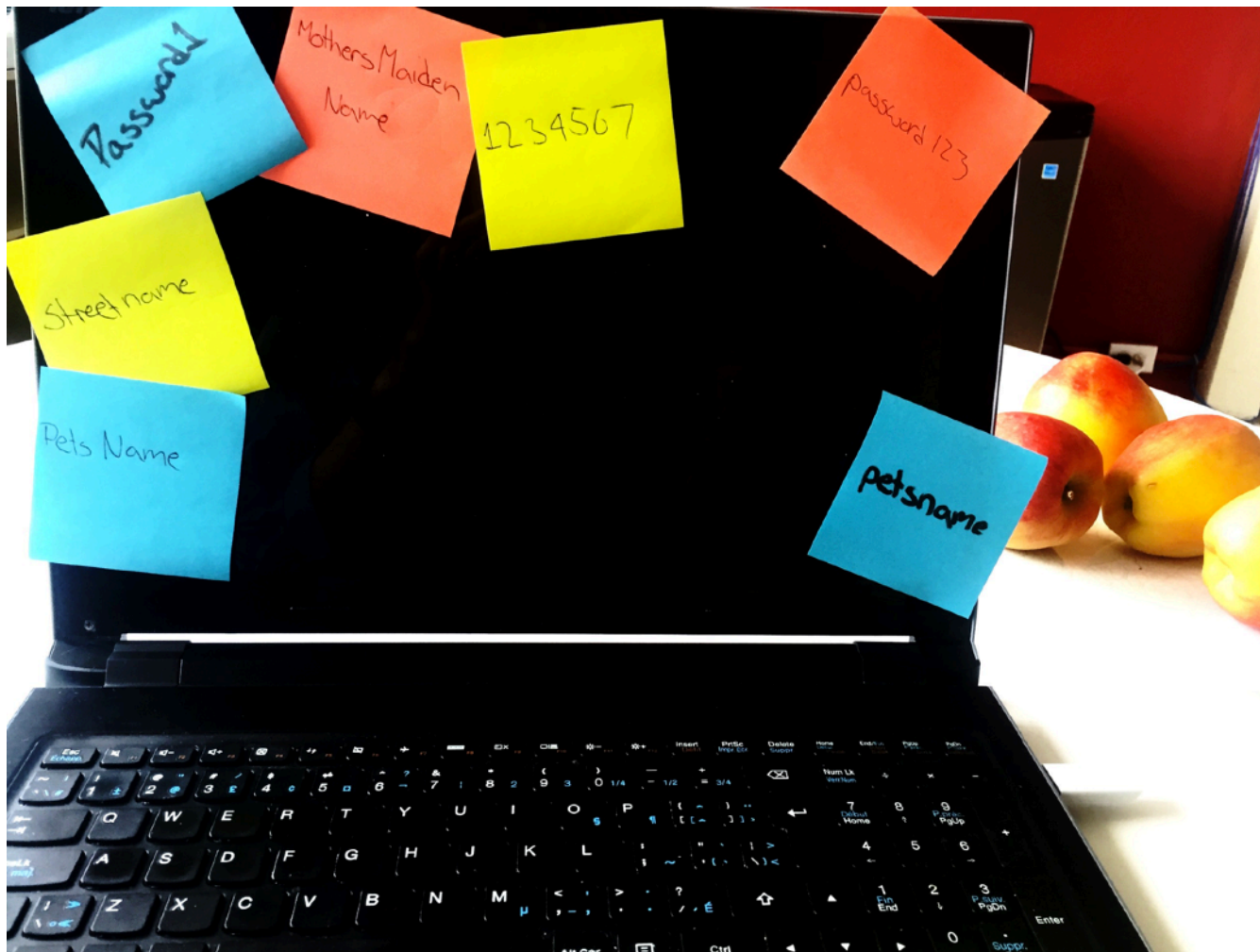
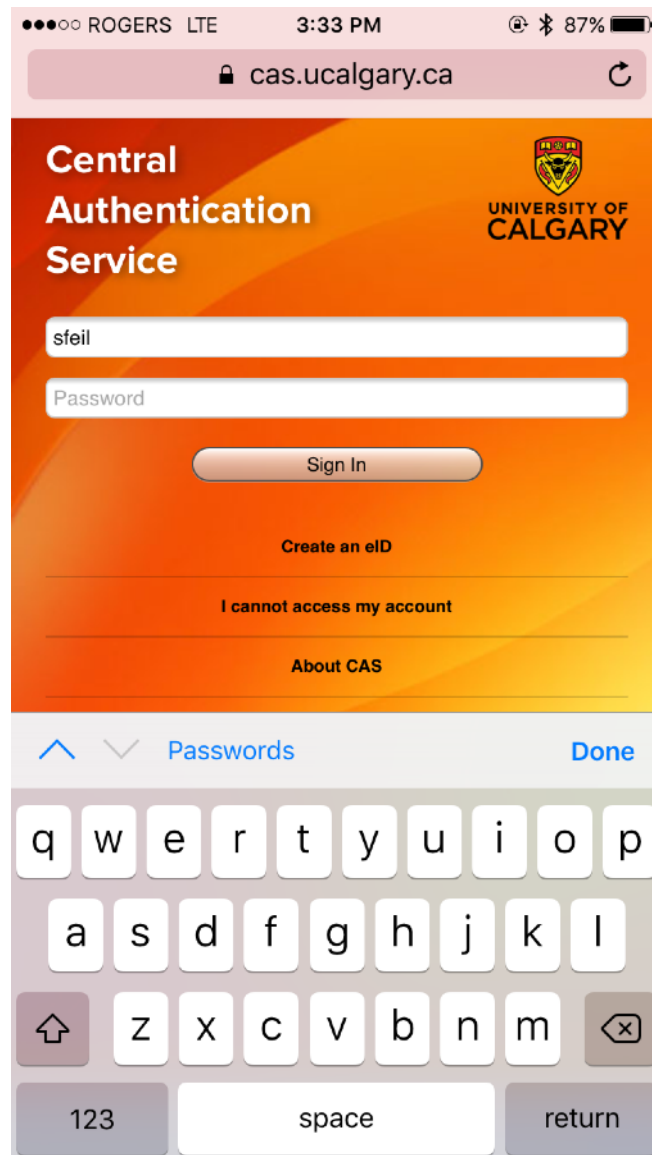


Image from <https://www.vendasta.com/>



Upgrade Form

* Email Address

* Password

* Verify Password

* Country

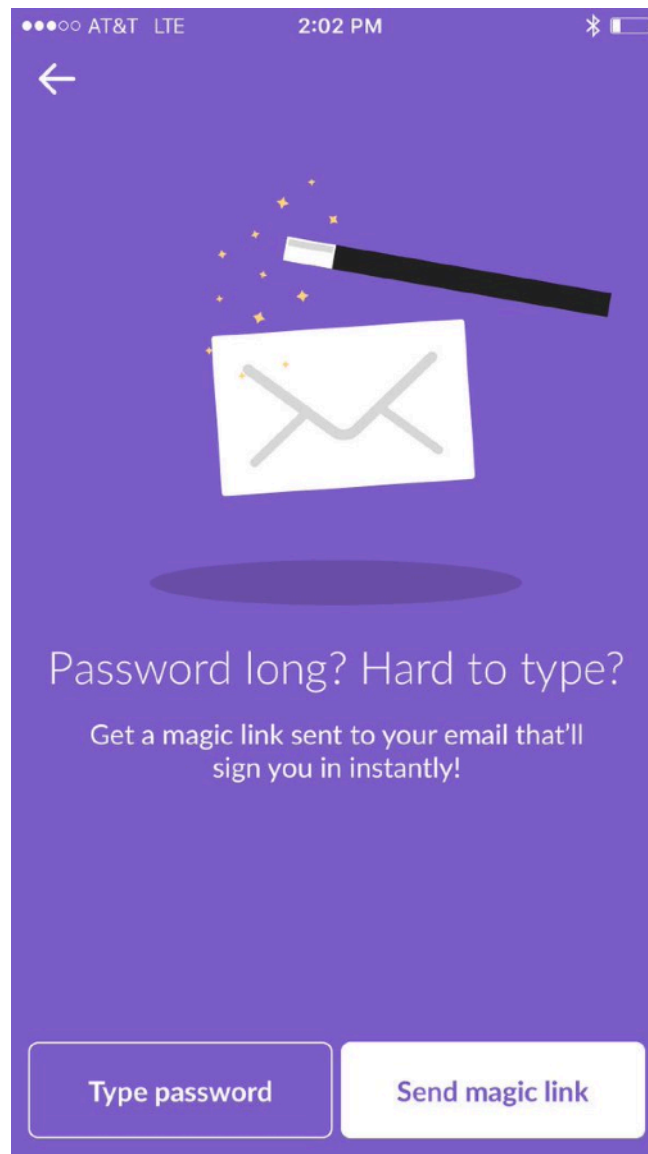
* First name/Last name

Submit

[Compose your survey with www.my4m.com](http://www.my4m.com)



The image shows a screenshot of the Outlook webmail login page for the University of Calgary. The page has an orange and yellow gradient background. At the top left is the Outlook logo, and at the top right is the University of Calgary crest and name. The main heading is "Outlook". Below it, the text "Enter your webmail username and password" is displayed. There are three input fields: "User name:", "Password:", and "Confirm Password:". A "Confirm your account" button is located below the "Confirm Password" field. At the bottom, there is a small icon and the text "Connected to Microsoft Exchange" and "© 2010 Microsoft Corporation. All rights reserved."



Slack



Apple

...making something as important as security so effortless, so simple. We believe that technology is at its very best, at its most empowering, when it simply disappears.

- Jonathan Ive, 2013



09 Aug 2011

67 Percent of Consumers Don't Have Password Protection on Their Mobile Phones

IT security and data protection firm Sophos today published findings of independently commissioned research by TNS, which reveals consumer attitudes toward mobile security and data loss prevention. Although almost a quarter of consumers (22%) have lost a mobile phone in the past, and a further 12% have had a phone stolen, 67% don't have passwords set up on their mobile phones to protect stored data.

60% of those surveyed acknowledged that device theft or loss was the biggest security threat to mobile devices; however, only 57% have password protection enabled even on their laptops, with 18% admitting to using the same password for everything.

Sophos

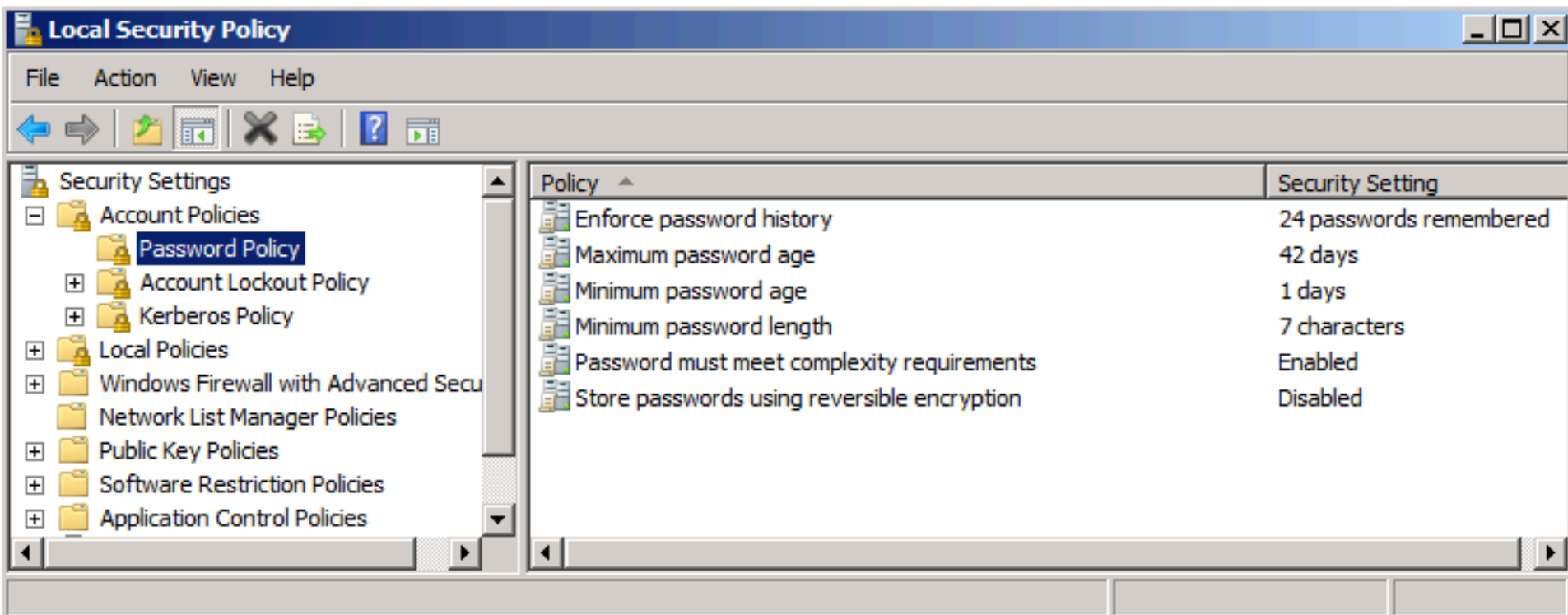


Macworld

Please enter your phone number:

(216) 409-9989





Problem?



Azure Active Directory



Shibboleth.



Microsoft

Active Directory
Federation Services



OpenLDAP



Microsoft
Active Directory



Passwords stored in
internal databases somewhere??

(I really hope not but probably)

Central Authentication Service



Username

Password

[Create an eID](#) | [I cannot access my account](#)

Login Service



Please enter your UCalgary email address and password:

Example: username@ucalgary.ca

Ucalgary email address

Password:

Password

[I cannot access my account](#) | [IT Support](#)



Security ([show explanation](#))

- ☒ This is a public or shared computer
- ☐ This is a private computer
- ☐ Use the light version of Outlook Web App

User name:

Password:

[Sign in](#)

 Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.



GitLab Community Edition

Open source software

Manage Git repositories with your code secure. Perform code reviews with merge requests. Each project has a wiki.

Welcome to the GitLab service

LDAP

Standard

Authentication Required

<https://spse.ucalgary.ca> requires a username and password.

User Name:

Password:

User Login

Student Login

I have an account already

Log in using your existing account information.

UCID (case sensitive):

[Forgot UCID](#)

Password (case sensitive):

[Forgot Password](#)


Continue


Who does this well?



One account. All of Google.

Sign in to continue to Gmail





Sean Feil

Sign in

☒ Stay signed in [Forgot password?](#)


[Sign in with a different account](#)

One Google Account for everything Google



Log in as Sean Feil

****@****.com • [Not You?](#)

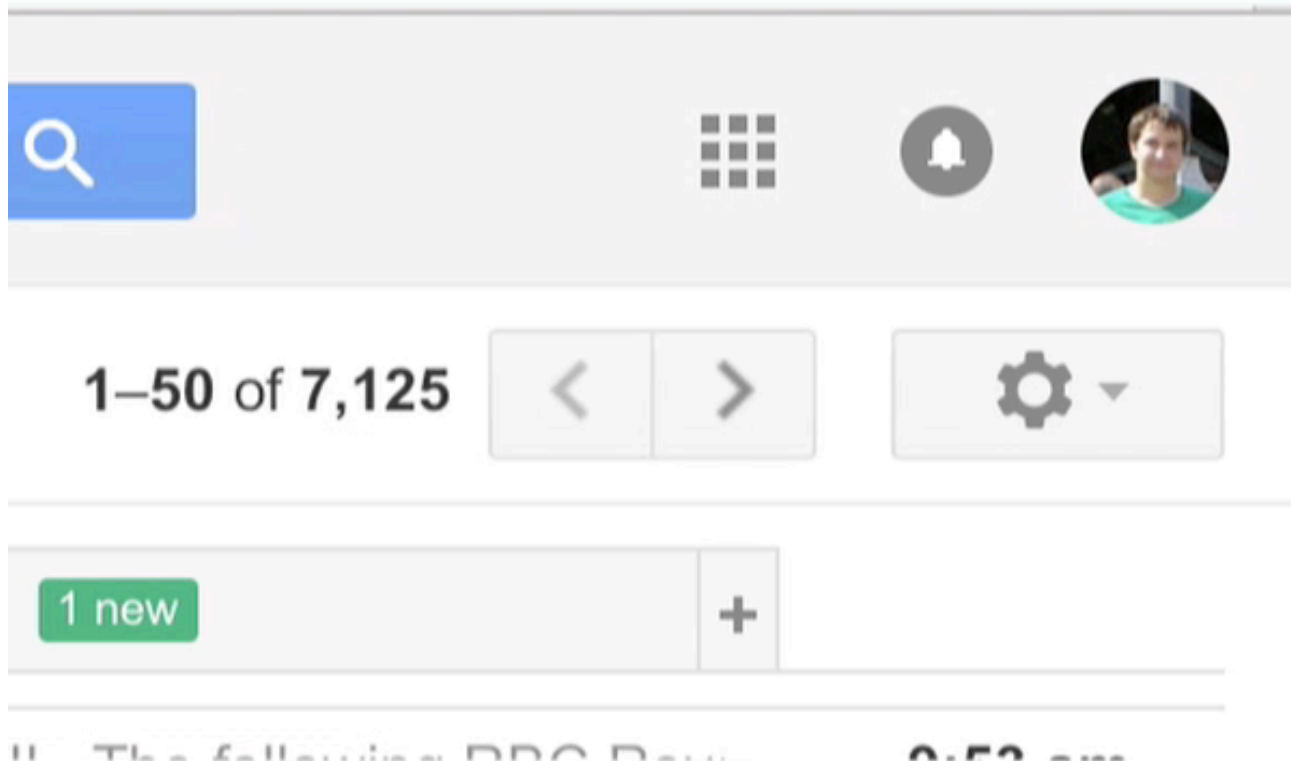


Log In

[Recover Your Account](#)

[Sign up for Facebook](#)







Work or school, or personal Microsoft account

Email or phone

Password

☐ Keep me signed in

Sign in

Back

[Can't access your account?](#)

© 2017 Microsoft

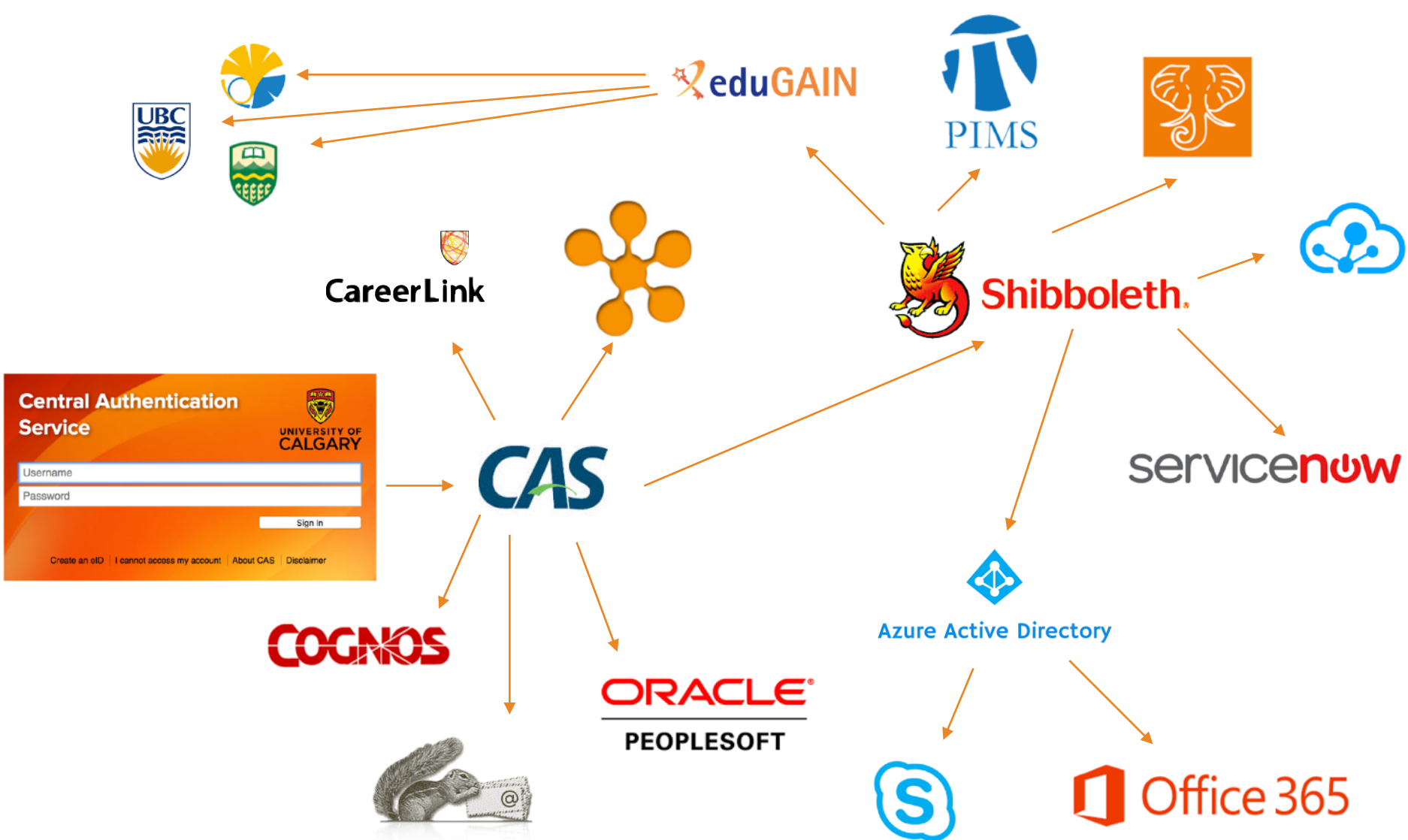
[Terms of use](#) [Privacy & Cookies](#)







Apple



Single Sign-on Rules

- Sign in once
- Sign out once
- Prompt the user only for new information



You have logged out

You have been logged out successfully.

myUofC Login

Copyright © 2017

Video review

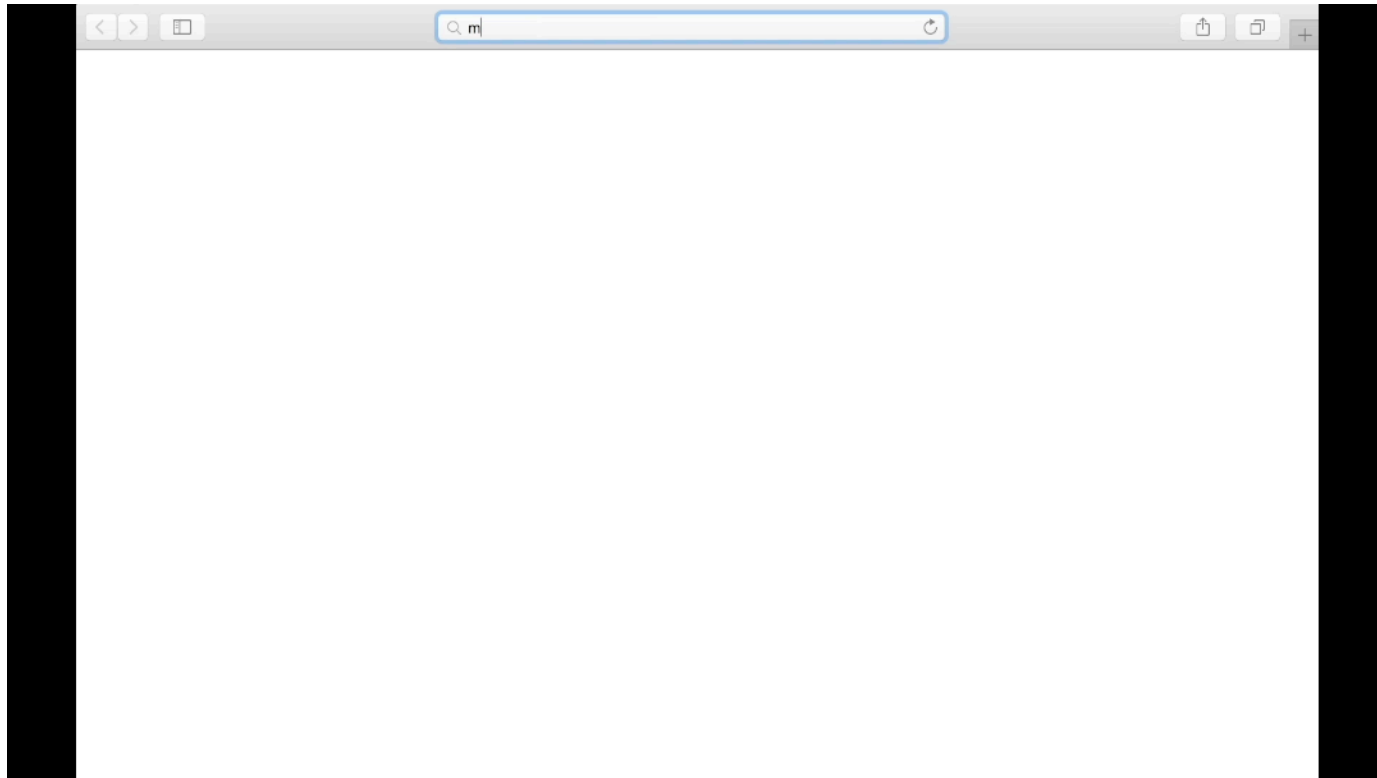
“The dream”



PeopleSoft Portal



CAS





PeopleSoft Finance

PeopleSoft SSO

The screenshot shows the University of Calgary PeopleSoft SSO portal. The browser address bar displays `my.ucalgary.ca/psp/paprd/EMPLOYEE/EMPL/h?tab=UCIH_HP`. The page features a red header with navigation links: Home, Account, Help, and Sign out. Below the header, the University of Calgary logo is on the left, and a search bar is on the right. A navigation bar contains links: Dashboard, All about me, My work, Academic, Around campus, and My favorites. The main content area is divided into two columns. The left column, titled 'Announcements', contains three items: 1. 'IT service outage reminder | Campus-wide March 10 - 11' with details about a network outage and a 'READ MORE' link. 2. 'What does a pluralistic campus look like?' with details about Pluralism and Religious Diversity Week and a 'READ MORE' link. 3. 'Don't miss out - Alberta Ballet offers UCalgary reduced rate for Alice in Wonderland performance' with details about a 25% ticket reduction and a 'READ MORE' link. The right column, titled 'Quick Links', contains a list of links: Desire2Learn, Service Now, My paycheque, Report time, PS Finance & Supply Chain, PS Student Admin, Office 365, and Schedule Builder.



Password Management

CAS



Desire2Learn



CAS

The screenshot shows the myUofC portal for a user named Sean. The header includes the University of Calgary logo, a greeting, and navigation links like Home, Account, Help, and Sign out. A search bar is also present. The main content area features an 'Announcements' section with three items: an IT service outage reminder for March 10-11, a notice about Pluralism and Religious Diversity Week, and a reminder about the Alberta Ballet performance. Each announcement has a 'READ MORE' link. To the right, a 'Quick Links' section lists various services such as Desire2Learn, Service Now, My paycheck, Report time, PS Finance & Supply Chain, PS Student Admin, Office 365, and Schedule Builder.



Service Now



Shibboleth

The screenshot displays the my.ucalgary.ca employee portal. The browser address bar shows the URL `my.ucalgary.ca/psp/paprd/EMPLOYEE/EMPL/h?tab=UCIH_HP`. The page header includes navigation links: Home, Account, Help, and Sign out. A personalized greeting reads "Hello Sean, Welcome to myUofC". The University of Calgary logo is on the left, and a search bar is on the right. A secondary navigation bar contains links: Dashboard, All about me, My work, Academic, Around campus, and My favorites. The main content area is divided into two columns. The left column, titled "Announcements", features three articles: "IT service outage reminder | Campus-wide March 10 - 11", "What does a pluralistic campus look like?", and "Don't miss out - Alberta Ballet offers UCalgary reduced rate for Alice in Wonderland performance". The right column, titled "Quick Links", lists various services: Desire2Learn, Service Now, My paycheck, Report time, PS Finance & Supply Chain, PS Student Admin, Office 365, and Schedule Builder.



PeopleSoft Student Admin



Azure AD (MFA)

my.ucalgary.ca/psp/paprd/EMPLOYEE/EMPL/h?tab=UCIH_HP

Home Account Help Sign out

Hello Sean,
Welcome to myUofC

UNIVERSITY OF CALGARY

All Search Advanced Search

Dashboard All about me My work Academic Around campus My favorites

Announcements

IT service outage reminder | Campus-wide March 10 - 11

Please be reminded between Friday, March 10 at 10:00 p.m. and 9:00 p.m. Saturday, March 11, there will be a three-hour full network outage impacting the majority of IT services. Please be advised intermittent network outages continue to allow for building-specific wired services work. The next outages will occur between [Mar. 5-8 in CCIT](#) and [Mar. 6-12 in ICT](#).

[READ MORE](#)

What does a pluralistic campus look like?

Pluralism and Religious Diversity Week from Mar. 13 - 17 is an opportunity for the campus community to explore religious diversity and dialogue focused on creating a more inclusive and pluralistic campus. Events include opportunities to participate in the internationally acclaimed What I Be project, film screenings, a powered by Pechakucha event, keynote speaker Stephen Prothero and much more! All events are free, though some require [registration](#).

[READ MORE](#)

Don't miss out - Alberta Ballet offers UCalgary reduced rate for Alice in Wonderland performance

UCalgary and Alberta Ballet are both celebrating 50th anniversaries this year. We work together through a dance-science partnership that brings ongoing mutual benefits. Enjoy a 25 per cent reduction on tickets to Alberta Ballet's Alice In Wonderland performance on March 17 (Calgary) and March 24/25 (Edmonton) with promo code UOFCALICE25. [Tickets available](#) until performance dates while supplies last.

[READ MORE](#)

Reminder | U Make a Difference award nomination deadline March 10

Nominate a deserving colleague or team for a 2017 [U Make a Difference award](#). These awards provide university-employed faculty, staff, graduate students and postdoctoral scholars the opportunity to

Quick Links

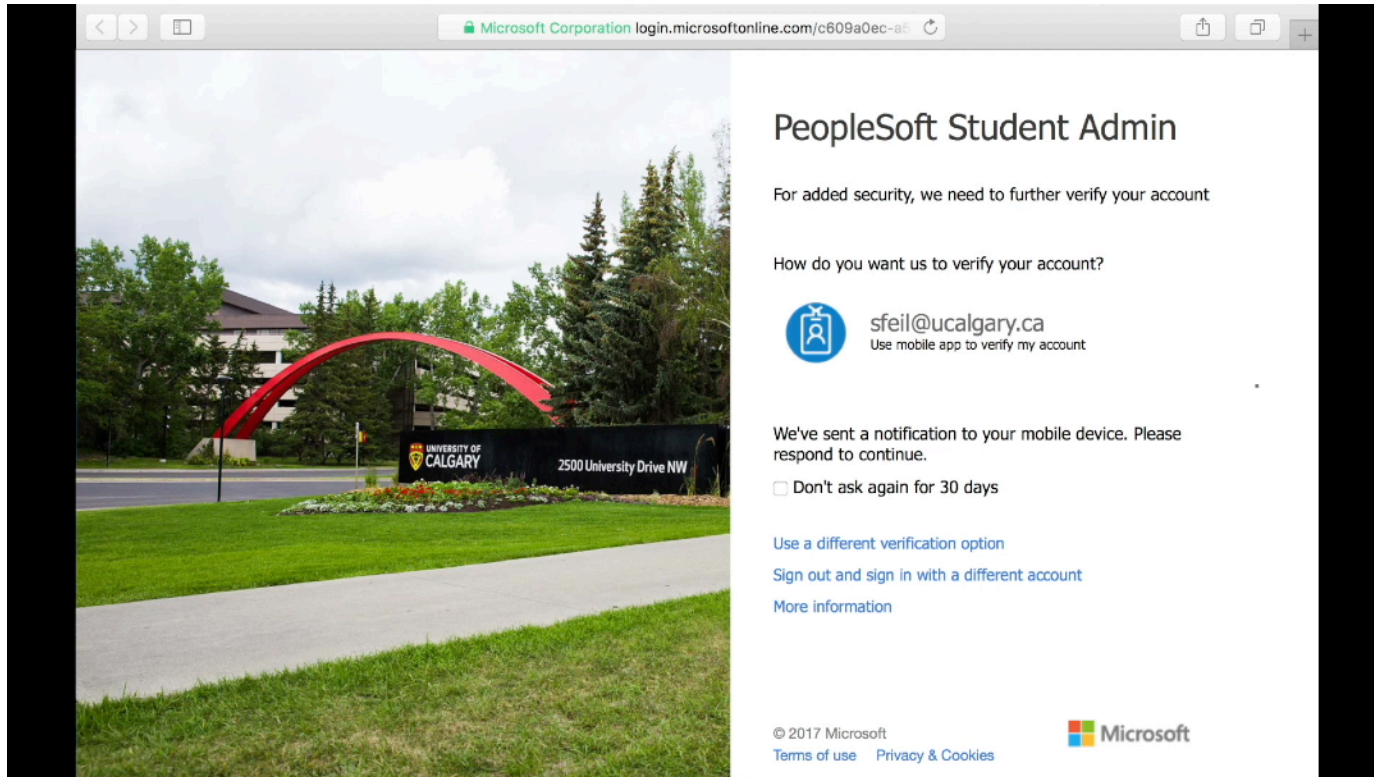
- [Desire2Learn](#)
- [Service Now](#)
- [My paycheck](#)
- [Report time](#)
- [PS Finance & Supply Chain](#)
- [PS Student Admin](#)
- [Office 365](#)
- [Schedule Builder](#)



PeopleSoft Student Admin



Azure AD (MFA)

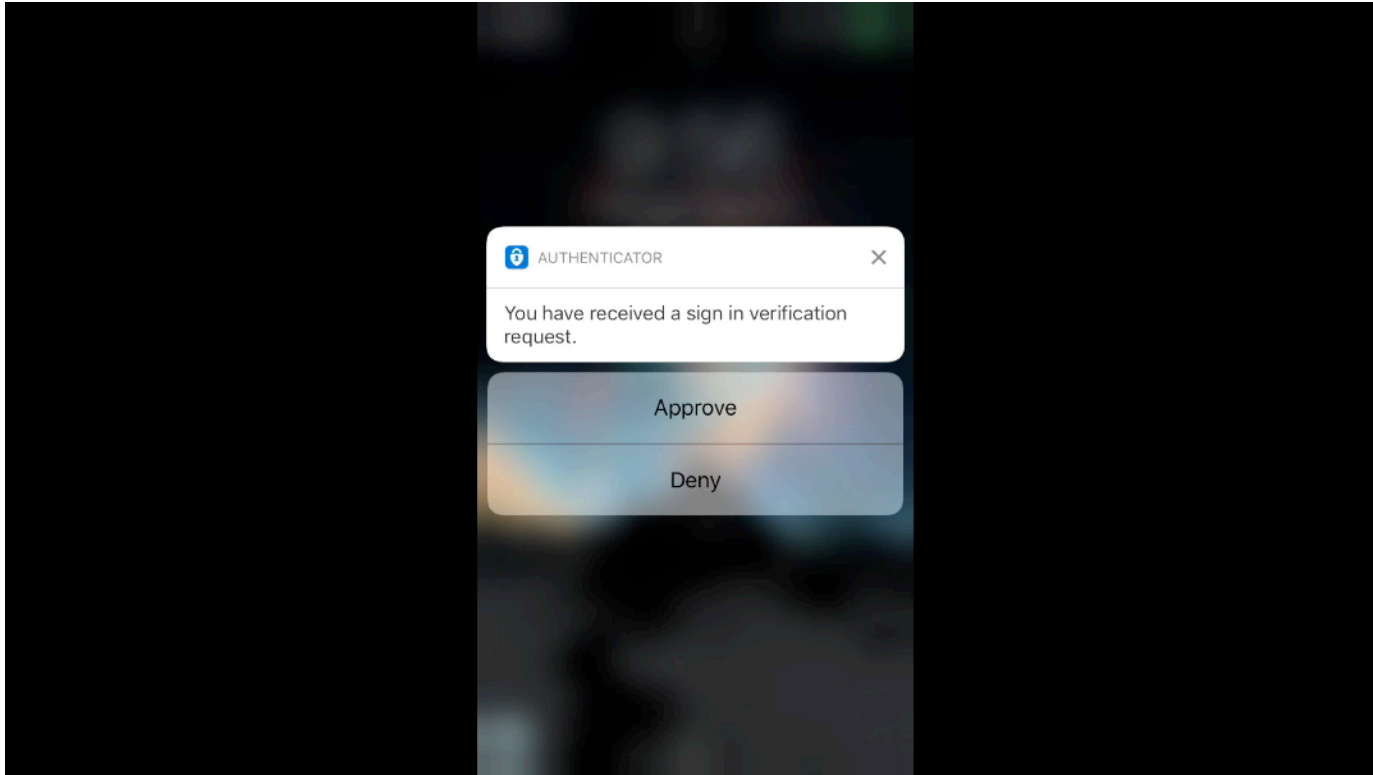




PeopleSoft Student Admin



Azure AD (MFA)





Office 365



Azure AD

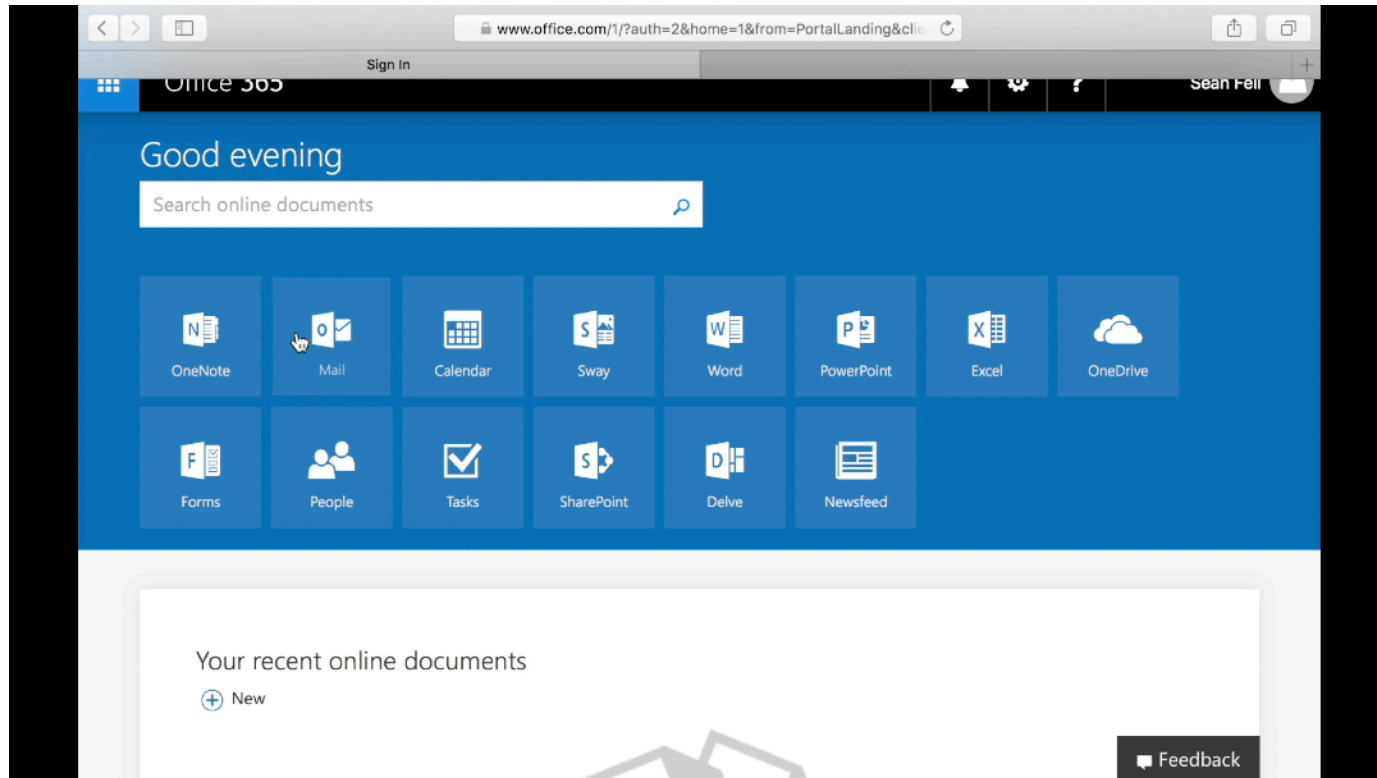
The screenshot displays the my.ucalgary.ca portal. At the top, a red navigation bar contains links for Home, Account, Help, and Sign out. Below this, a grey header area shows the University of Calgary logo, a personalized greeting 'Hello Sean, Welcome to myUofC', and a search bar. A secondary navigation bar includes links for Dashboard, All about me, My work, Academic, Around campus, and My favorites. The main content area is divided into two columns. The left column, titled 'Announcements', features three articles: 'IT service outage reminder | Campus-wide March 10 - 11', 'What does a pluralistic campus look like?', and 'University's protocol regarding political activity'. The right column, titled 'Quick Links', lists various services such as Desire2Learn, Service Now, My paycheck, Report time, PS Finance & Supply Chain, PS Student Admin, Office 365, and Schedule Builder.



Exchange Online



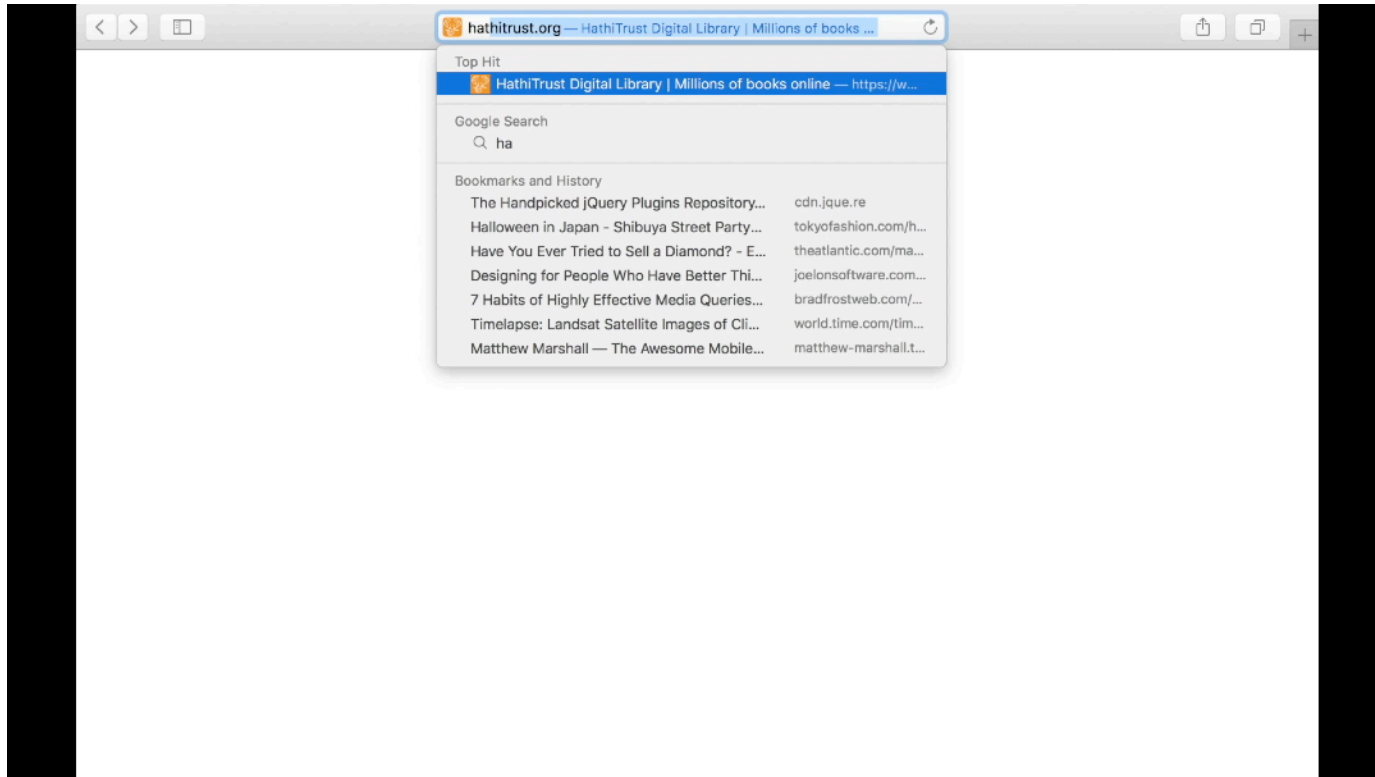
Azure AD





HathiTrust

Shibboleth (via eduGAIN)

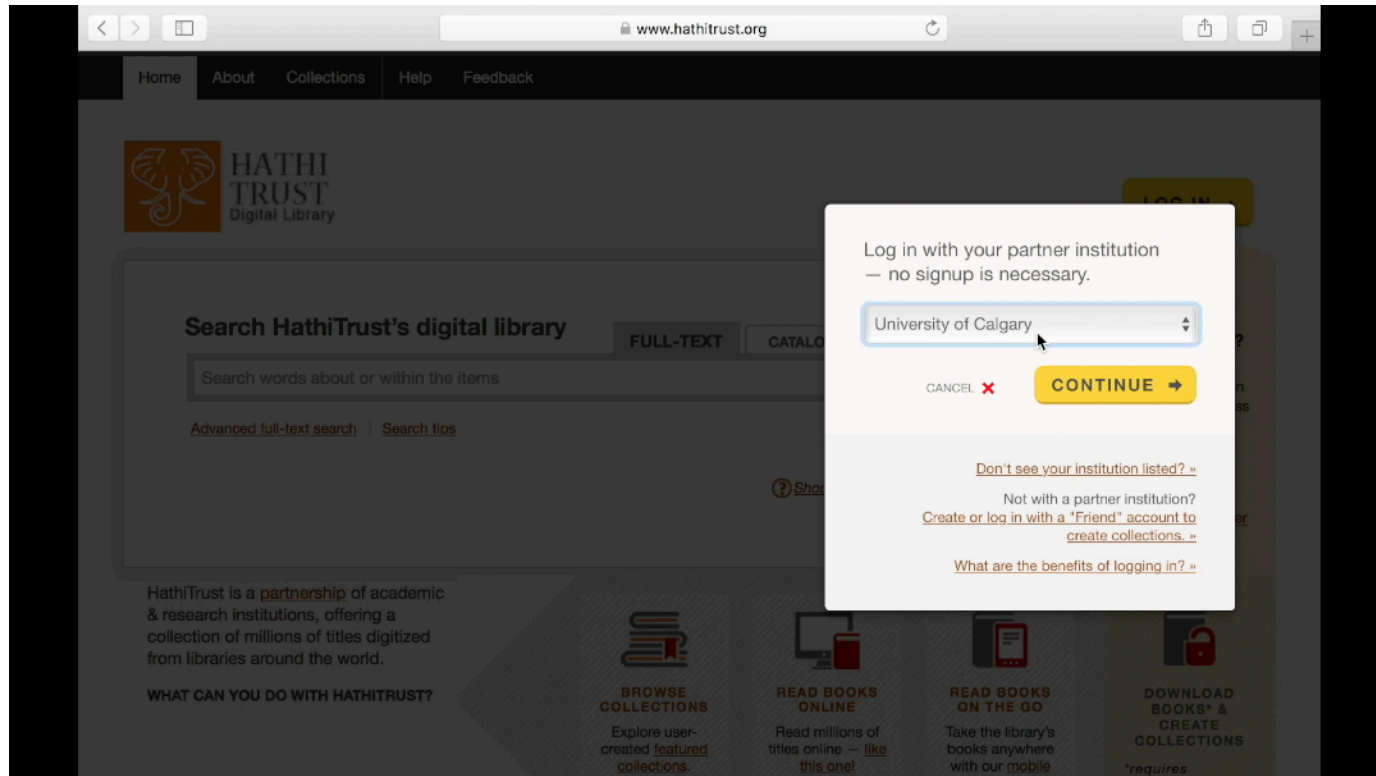




HathiTrust



Shibboleth (via eduGAIN)







HathiTrust

Shibboleth (via eduGAIN)

shibboleth.ucalgary.ca/idp/profile/SAML2/Redirect/SSO?execut...

 **UNIVERSITY OF CALGARY**

 **HATHI TRUST** Digital Library

You are about to access the service:
HathiTrust of University of Michigan

Description as provided by this service:
HathiTrust is an international partnership of academic and research institutions working together to ensure the long-term preservation and accessibility of the cultural record.

[Additional information about the service](#)

Information to be Provided to Service	
eduPersonScopedAffiliation	member@ucalgary.ca employee@ucalgary.ca staff@ucalgary.ca

[Data privacy information of the service](#)

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

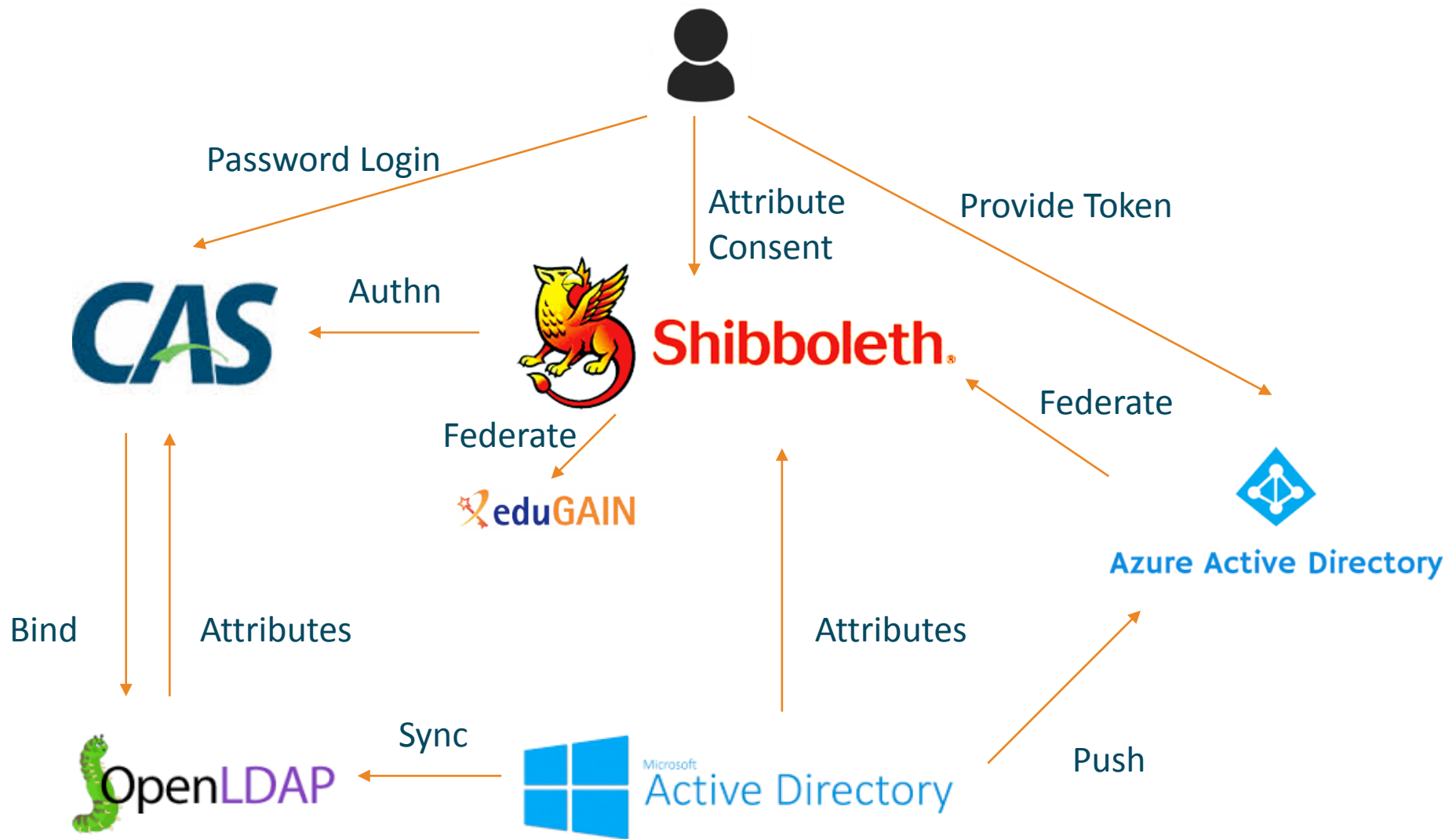
Select an information release consent duration:

☐ Ask me again at next login



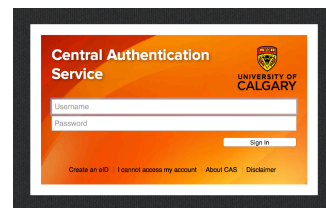
Single Logout

The screenshot shows a web browser window displaying the myUofC portal. The address bar shows the URL: my.ucalgary.ca/psp/paprd/EMPLOYEE/EMPL/h?tab=UCIH_HF. The page header includes navigation links: Home, Account, Help, and Sign out. A personalized greeting says "Hello Sean, Welcome to myUofC". Below the header is a search bar with a dropdown menu set to "All" and a search button. A secondary navigation bar contains links: Dashboard, All about me, My work, Academic, Around campus, and My favorites. The main content area is divided into two columns. The left column, titled "Announcements", contains four items: "IT service outage reminder | Campus-wide March 10 - 11", "What does a pluralistic campus look like?", "Don't miss out - Alberta Ballet offers UCalgary reduced rate for Alice in Wonderland performance", and "Reminder | U Make a Difference award nomination deadline March 10". Each announcement has a "READ MORE" link. The right column, titled "Quick Links", contains a list of links: Desire2Learn, Service Now, My paycheck, Report time, PS Finance & Supply Chain, PS Student Admin, Office 365, and Schedule Builder.



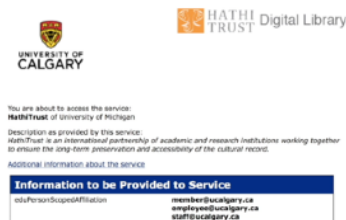


Password Login



Shibboleth®

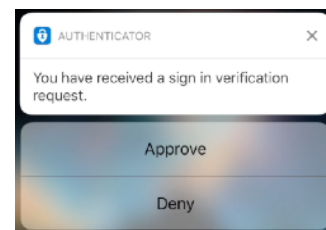
Attribute
Consent



Provide Token



Azure Active Directory





CAS 1.0
CAS 2.0
Legacy apps



Shibboleth®

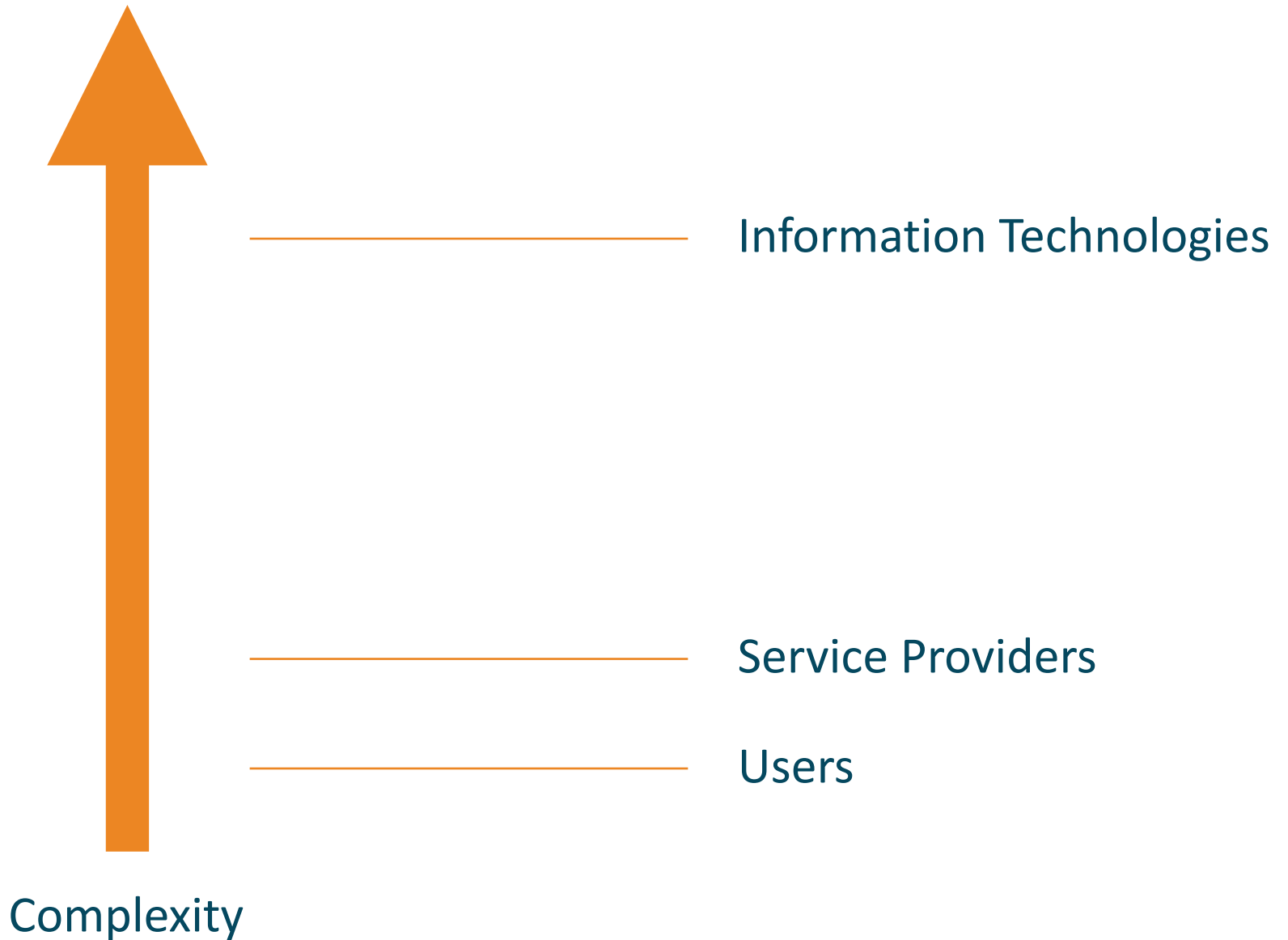
SAML1
SAML2
eduGAIN



Azure Active Directory

SAML2
OpenID
WSFed
Azure App Store
Multi-Factor Auth







Eyes High Strategy Statement

The University of Calgary will be a global intellectual hub located in Canada's most enterprising city. In this spirited, high-quality learning environment, students will thrive in programs made rich by research and hands-on experiences. By our 50th anniversary in 2016, we will be one of Canada's top five research universities, fully engaging the communities we both serve and lead.

Your turn

- ➡What are your big challenges on sign on?
- ➡How important is single sign on in your organization?
- ➡Do you apply usability to any of your practices?
- ➡Do you analyze your user behaviour?
- ➡What security improvements could you make by applying usability?