

# Platform SSO

Revenge of the Golden Triangle

Joel Rennich

# Agenda

- What PSSO is
- A bit of how it works
- Demos!



**What it is**

# Platform SSO

- macOS 13+
- Connects your Mac to your IdP
- Can synchronize passwords, but primary function is to extend single sign on
  - Users always have SSO tokens
  - Tokens are refreshed on login, screen saver unlock
  - Tokens leveraged by the Single Sign On extension for use with Safari and other applications

# Announced Support



Microsoft



okta

# New in macOS 14 Sonoma

- User creation at login window
- Tokens at login window
- Authorization database integration

# User Authentication Methods

- Password - password is sent to Identity Provider in either clear or encrypted forms
  - Only way to get password synch
- User Secure Enclave Key - user generates a key pair out of the Secure Enclave to use for ongoing authentication
- SmartCard - use existing certificate on SmartCard
- WS-Trust

# User Authentication Methods

- Password - password is sent to Identity Provider in either clear or encrypted forms
  - Only way to get password synch
- User Secure Enclave Key - user generates a key pair out of the Secure Enclave to use for ongoing authentication
- SmartCard - use existing certificate on SmartCard
- WS-Trust



# Pieces

- App with the Extensible Single Sign On app extension
  - Associated Domains listing all IdP URLs
  - App supports Platform SSO
- MDM Profile configuring eSSO and associated domains
  - Locally installed won't work
- Apple App Site Association file hosted on URL
  - Apple tests from their CDN at random times
  - Must be public IP and generally trusted CA

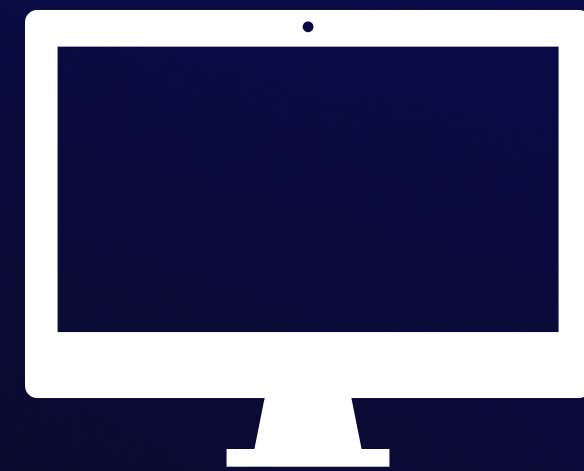
# How it works



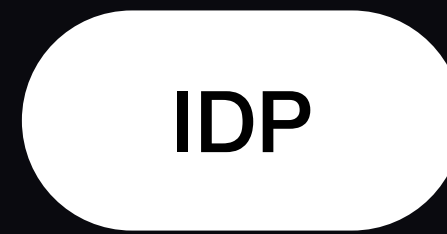
**Note: Network flows have been simplified for your learning pleasure. Nonces, heavy crypto and encryption have been glossed over for the purposes of fitting everything on the slide in a legible format.**

# Prep Work

IDP

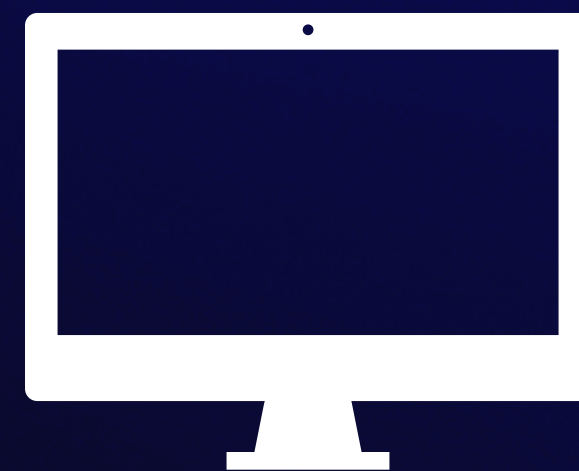


# Prep Work

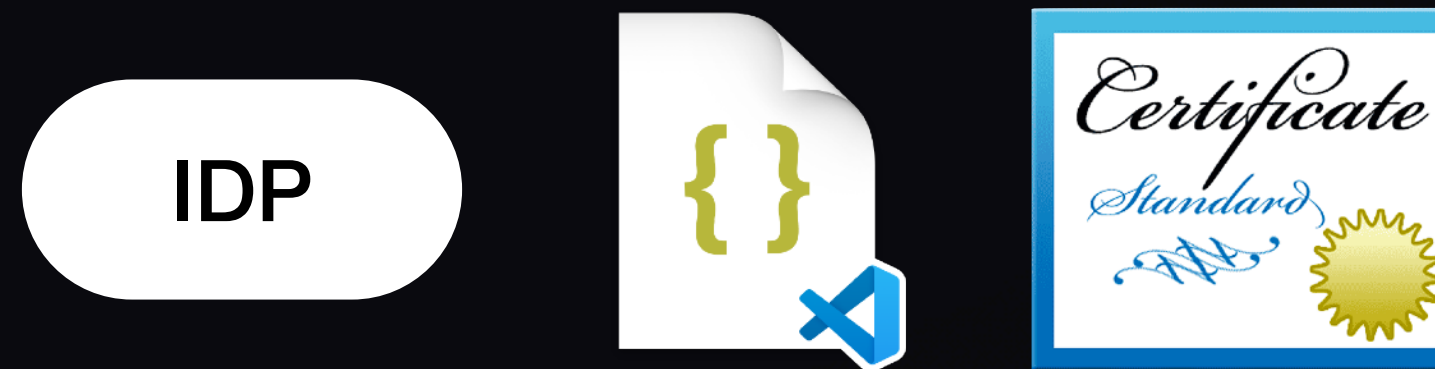


## IdP has

1. .well-known/apple-app-site-association
2. valid and trusted SSL cert
3. support for PSSO

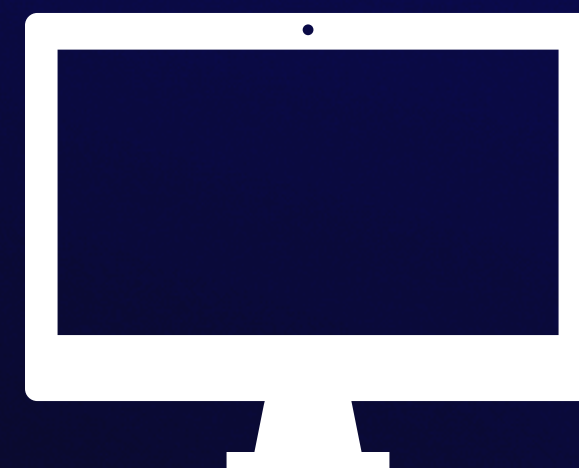


# Prep Work



## Mac has

1. IdP PSSO app installed in /Applications
2. MDM profile for PSSOE



# Device Registration

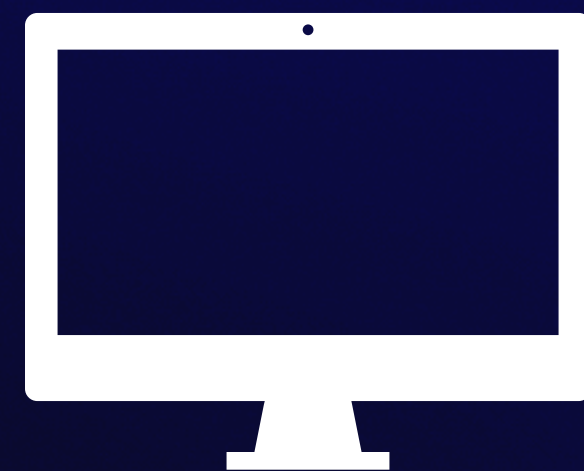
IDP

On sign in and every 15 mins, user is prompted to register the Mac



## Registration Required

Use your Demon Imp Cloud password to log in to your Mac.



# Device Registration

IDP

On registration the PSSO app sends a Device encryption and a Device signing cert to the IdP

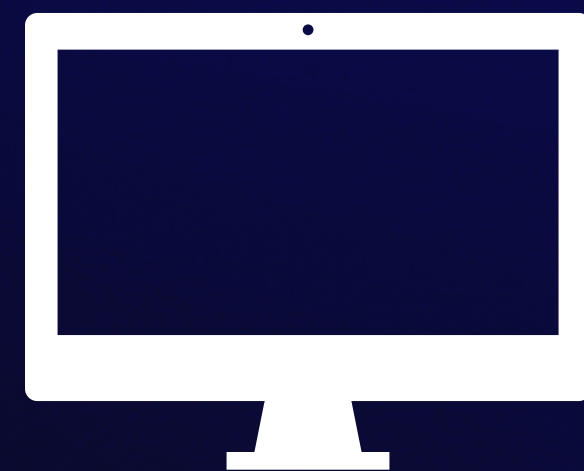


Signing  
Encryption



**Registration Required**

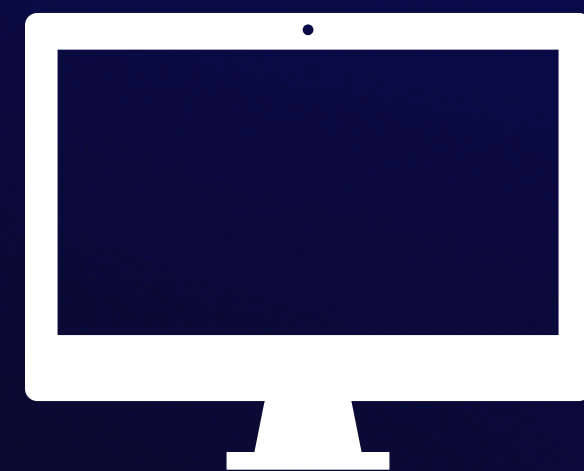
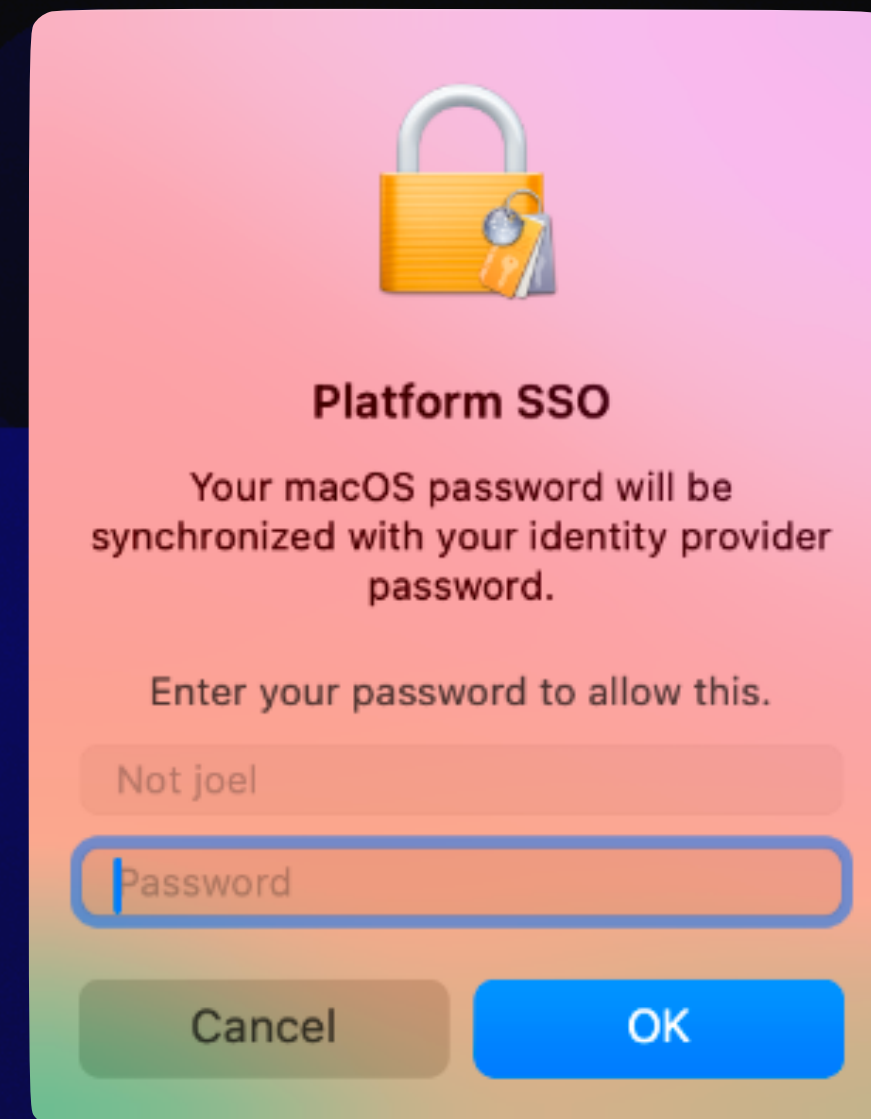
Use your Demon Imp Cloud password to log in to your Mac.





# User Authentication

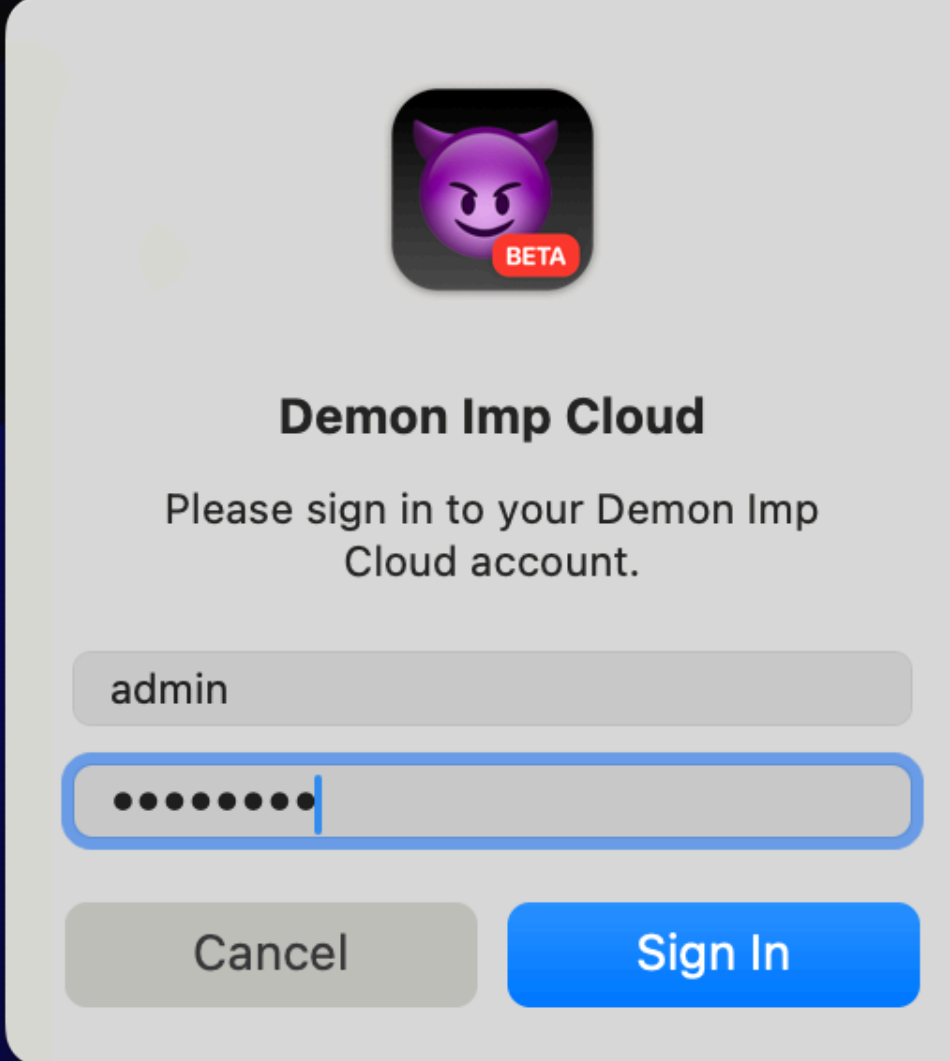
IDP



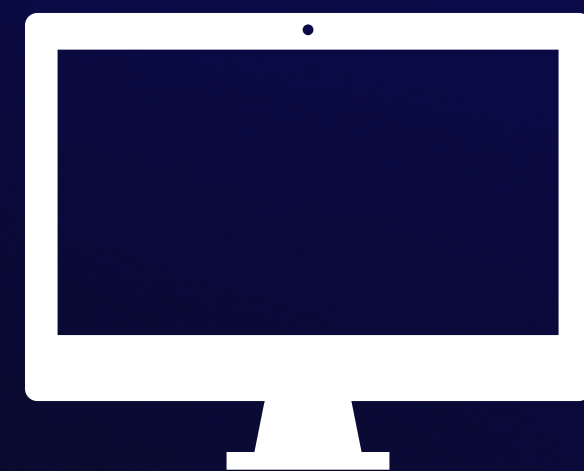
System authentication

# User Authentication

IDP



The screenshot shows a login dialog box for 'Demon Imp Cloud'. At the top is a purple devil emoji icon with a red 'BETA' badge. Below the icon, the text reads 'Demon Imp Cloud' and 'Please sign in to your Demon Imp Cloud account.' There are two input fields: the first contains the text 'admin', and the second is a password field with seven dots. At the bottom, there are two buttons: a grey 'Cancel' button and a blue 'Sign In' button.

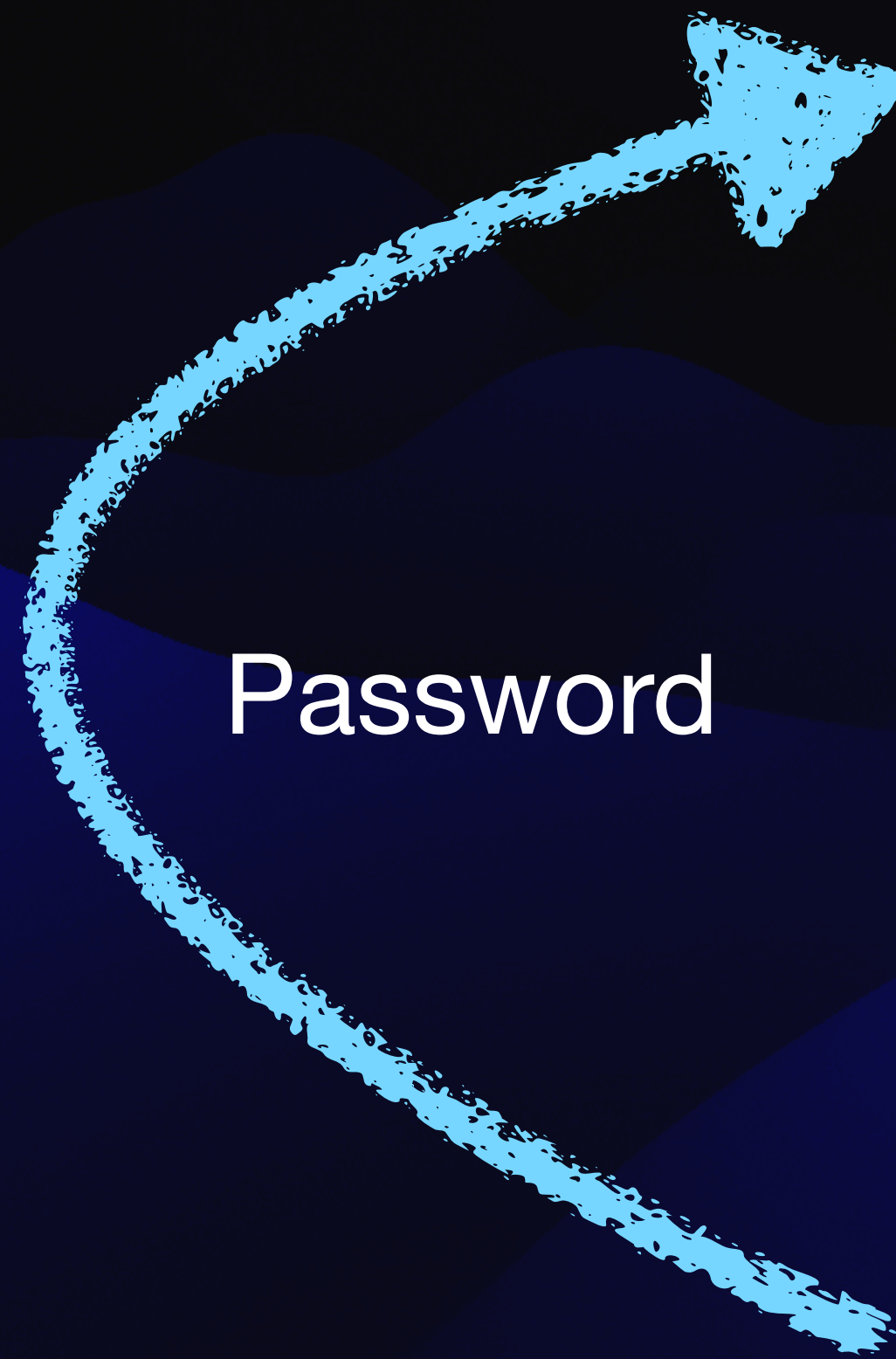


IdP User Authentication

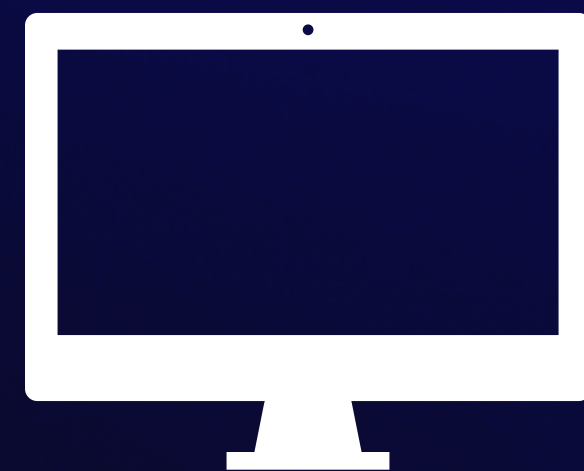
\* only seen with password-based auth

# User Authentication

IDP



Password

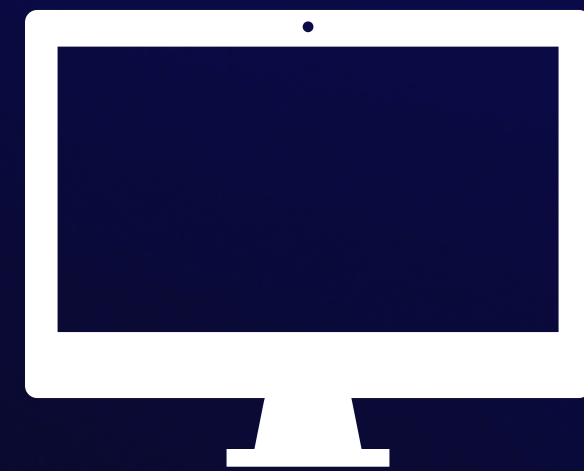
A screenshot of a login form for 'Demon Imp Cloud'. At the top is a purple demon head icon with a 'BETA' badge. Below it, the text reads 'Demon Imp Cloud' and 'Please sign in to your Demon Imp Cloud account.' There are two input fields: the first contains the text 'admin', and the second contains seven dots. At the bottom are two buttons: a grey 'Cancel' button and a blue 'Sign In' button.

\* on non-password flows signatures are sent

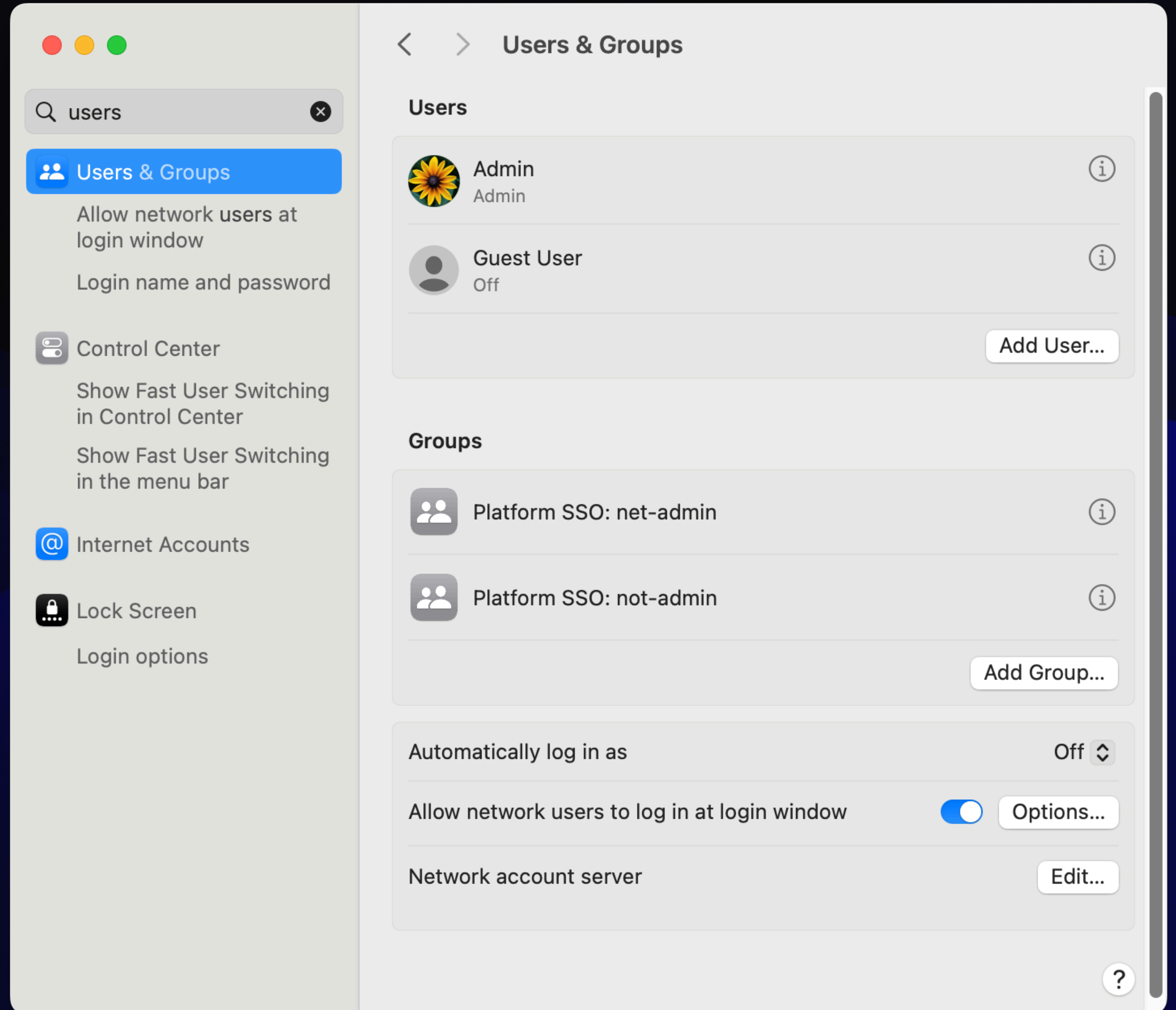
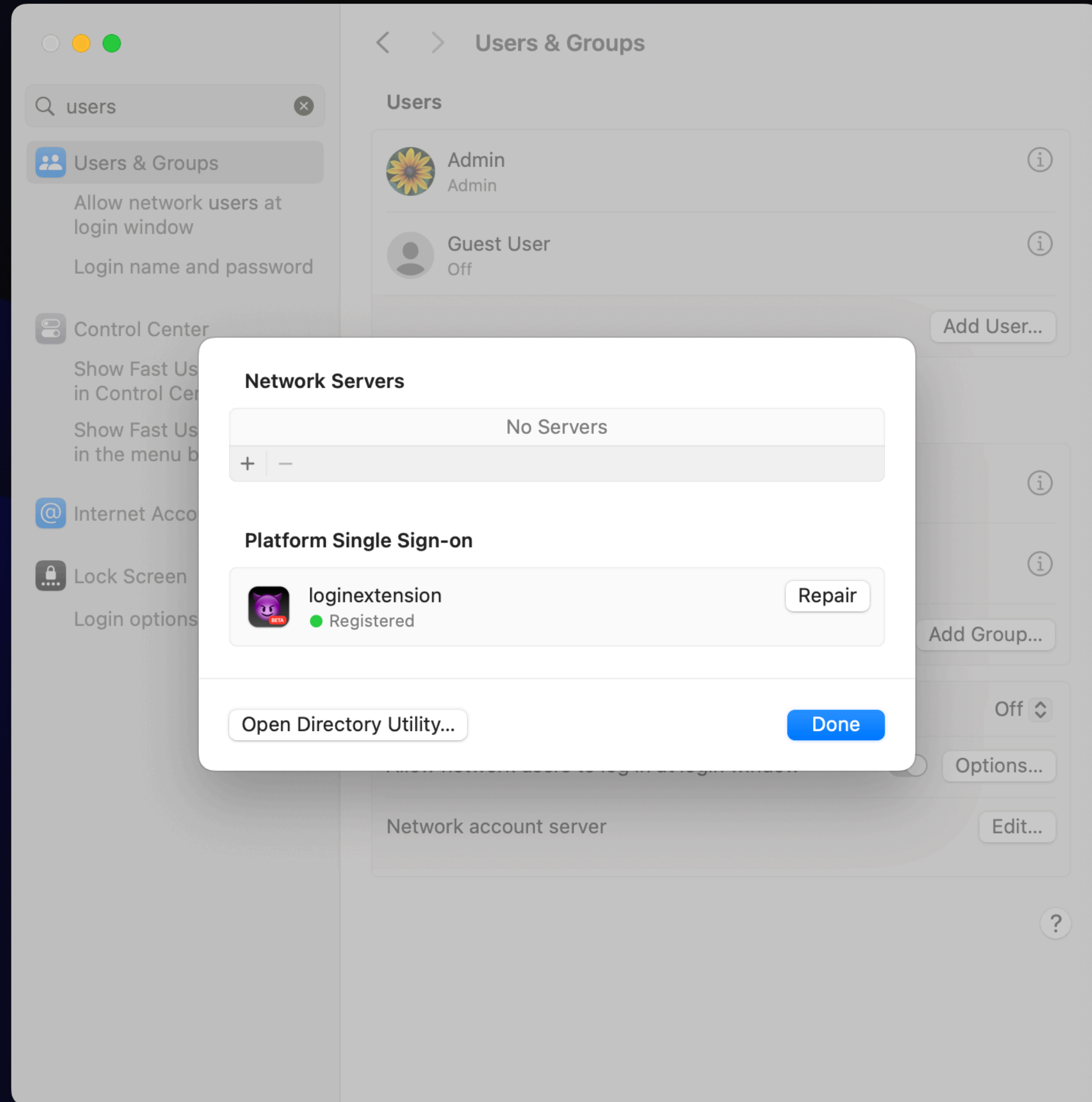
# User Authentication

IDP

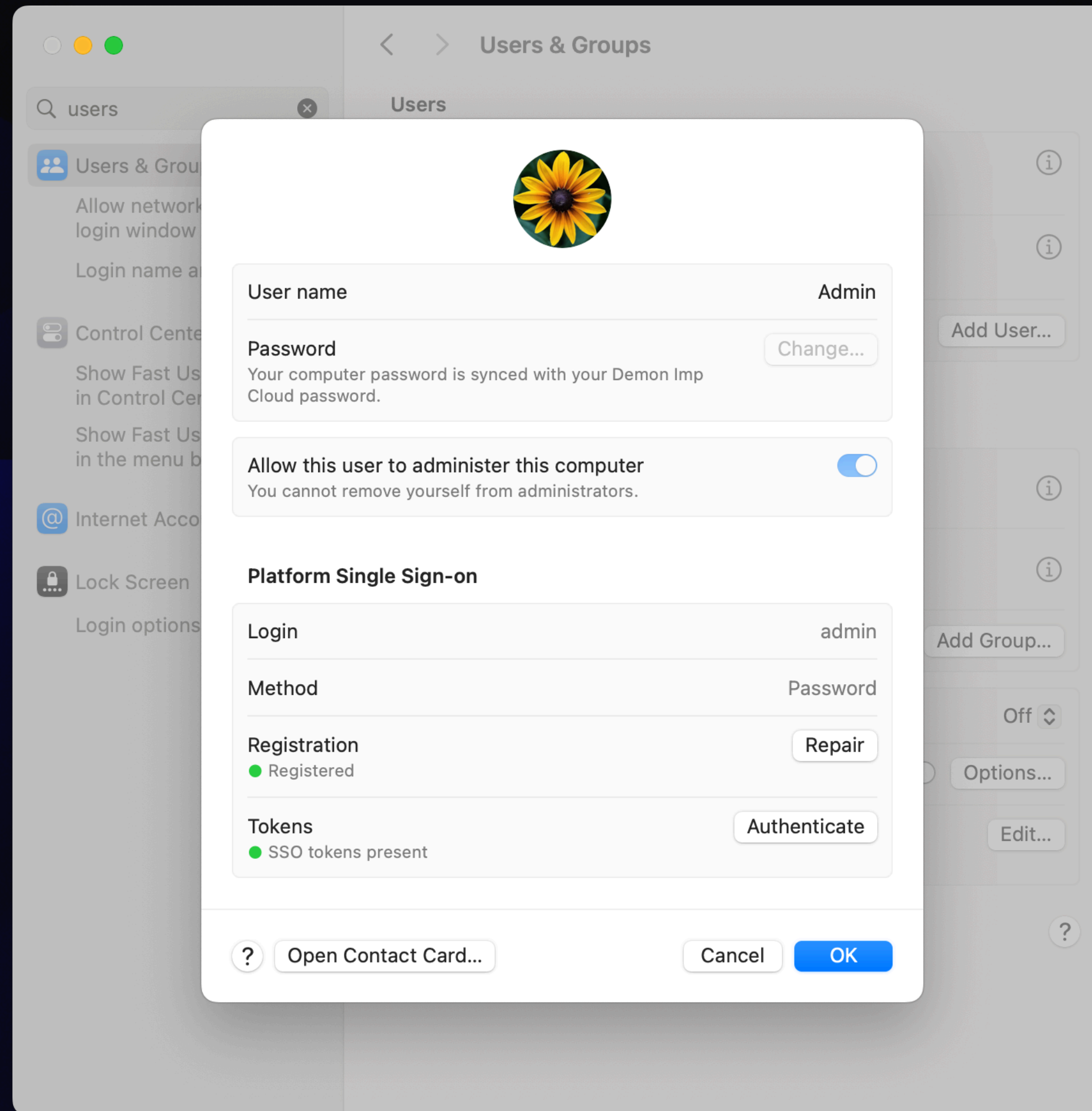
ID Token

A screenshot of a login form for 'Demon Imp Cloud'. At the top is a purple devil emoji icon with a 'BETA' badge. Below the icon, the text reads 'Demon Imp Cloud' and 'Please sign in to your Demon Imp Cloud account.' There are two input fields: the first contains the text 'admin', and the second contains seven dots. At the bottom, there are two buttons: a grey 'Cancel' button and a blue 'Sign In' button.

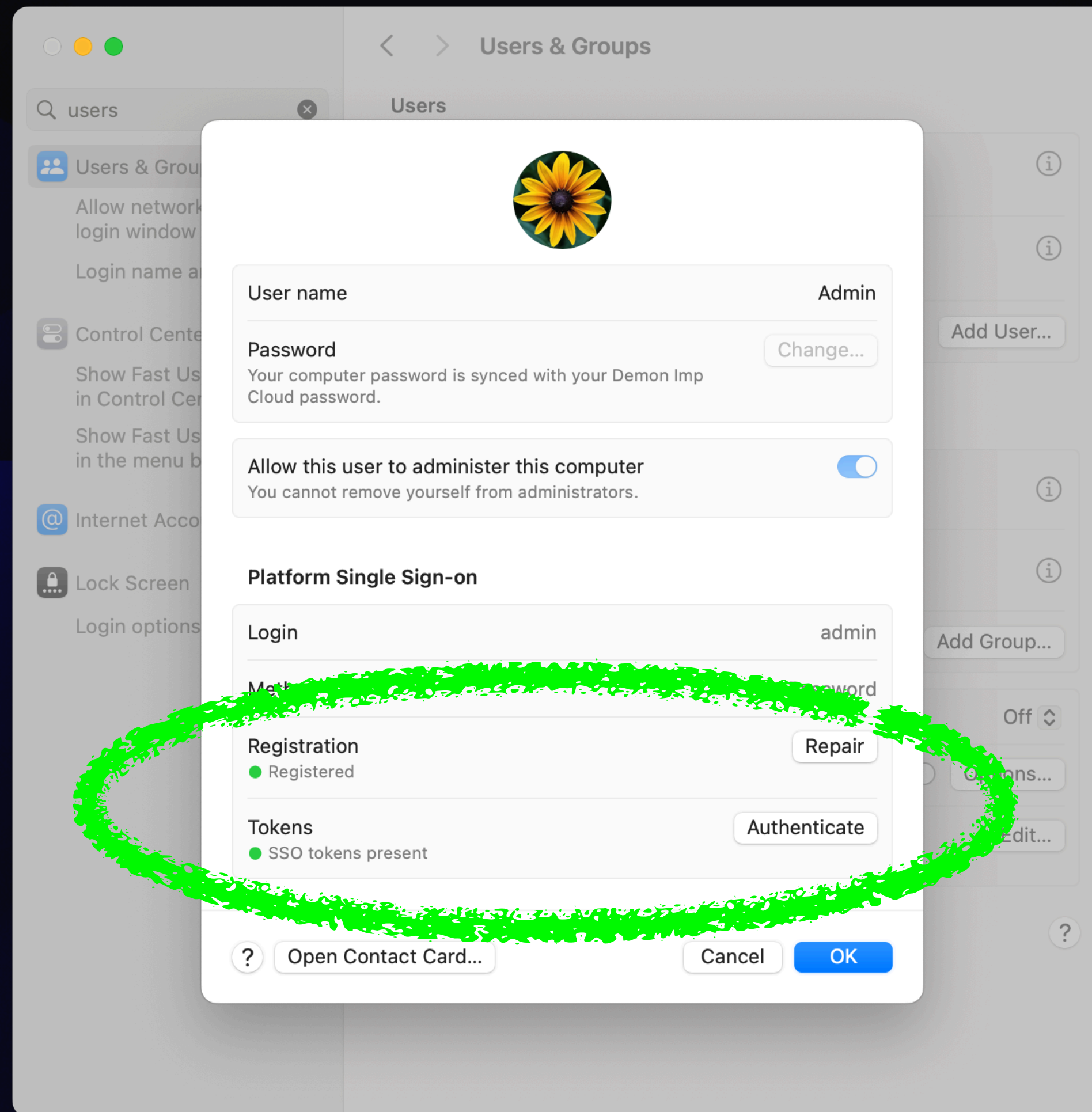
# Prefs



# Prefs



# Prefs





Let's see it!



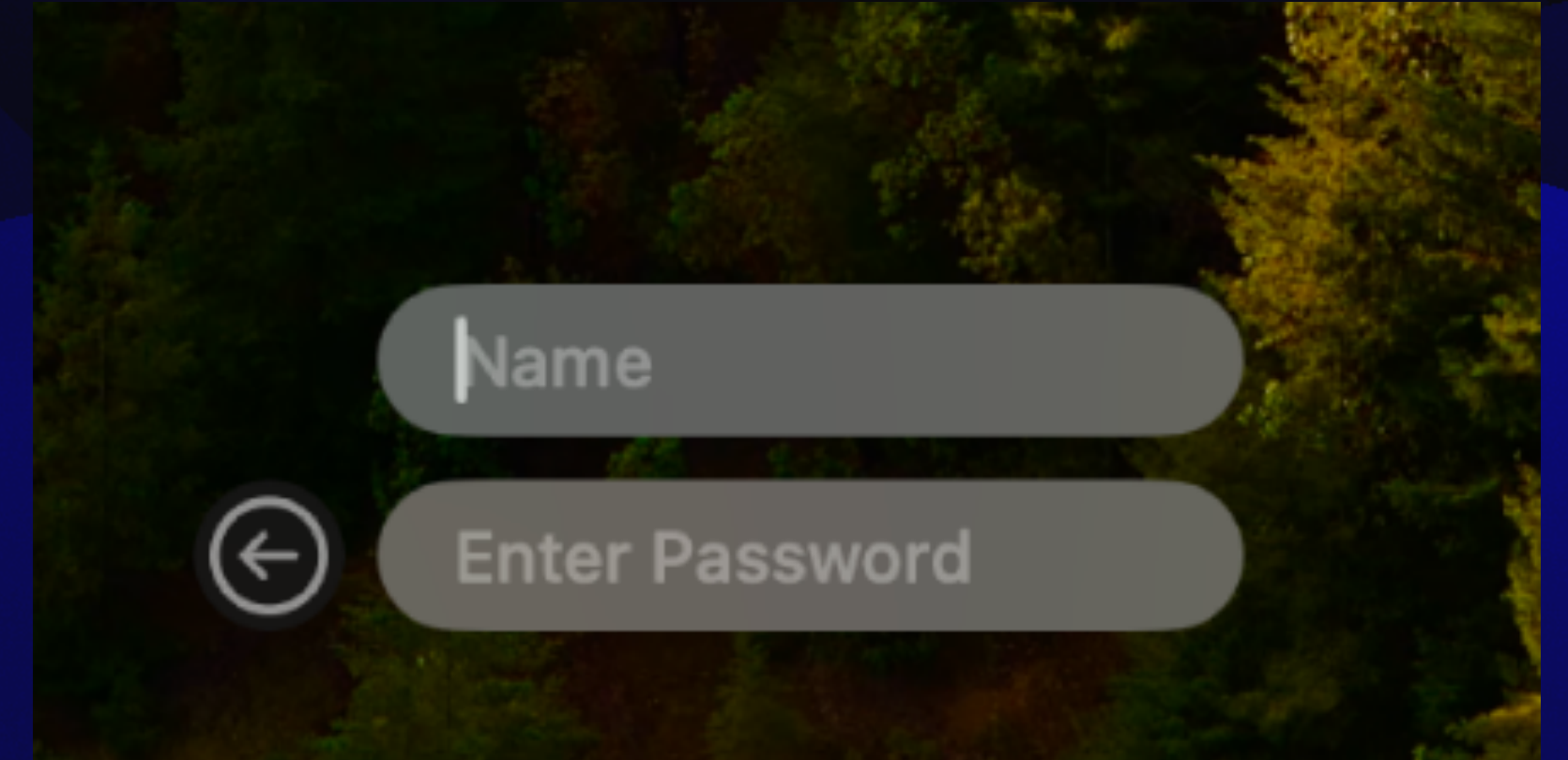
**Version 2**

# New User Creation

- Requires Bootstrap Token via MDM
- Option for admin user or non-admin user
- IdP can supply additional groups
  - Need to be referenced in the PSSO config profile
  - Standard groups claim in ID Token

# Login Window

IDP



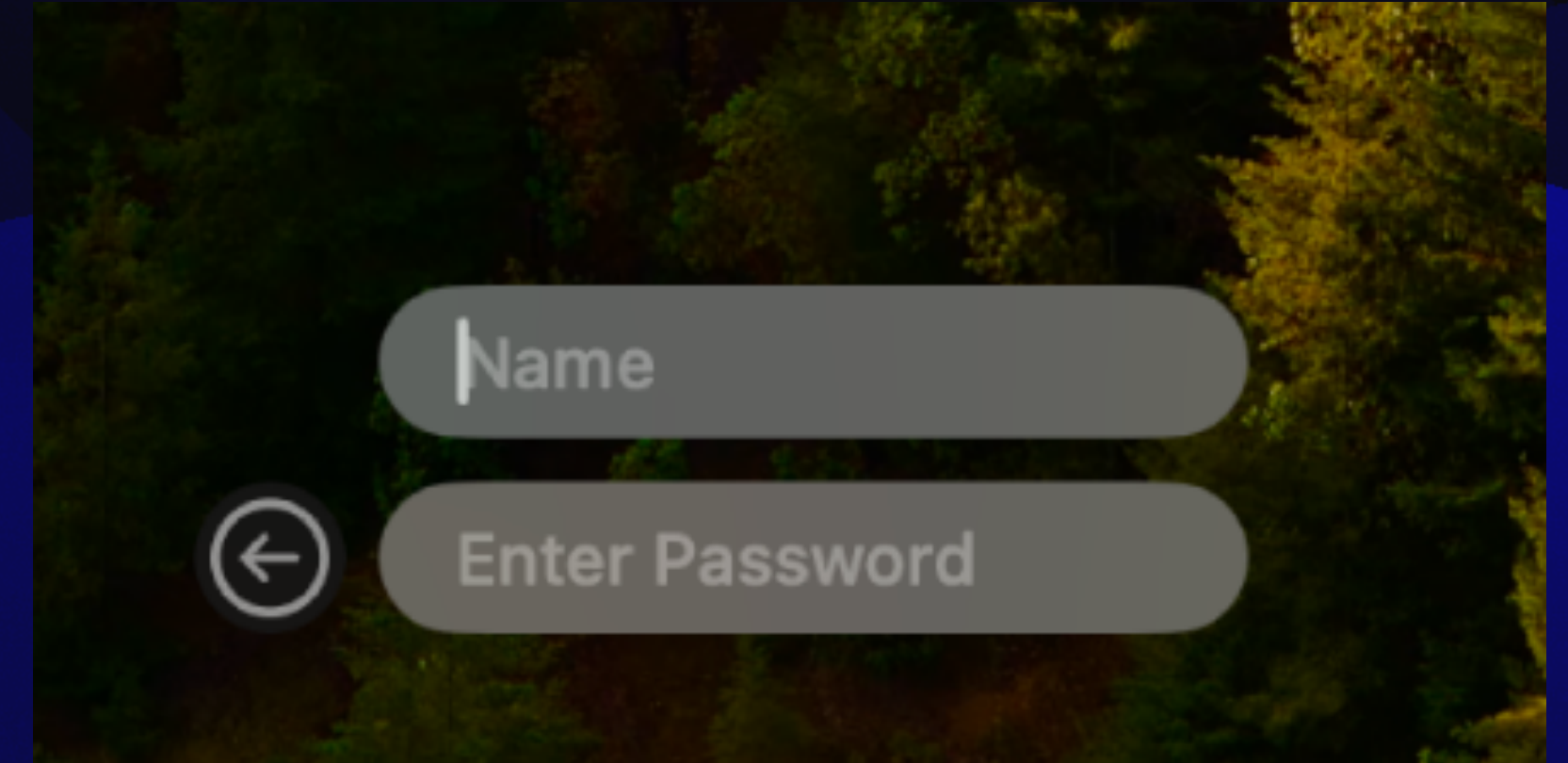
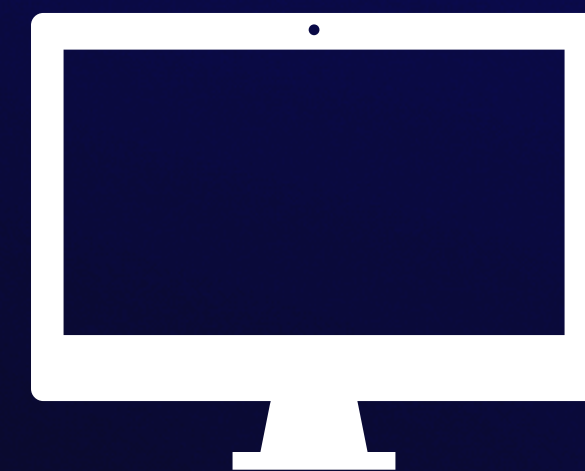
Username that has an “@” in it

# Login Window

IDP



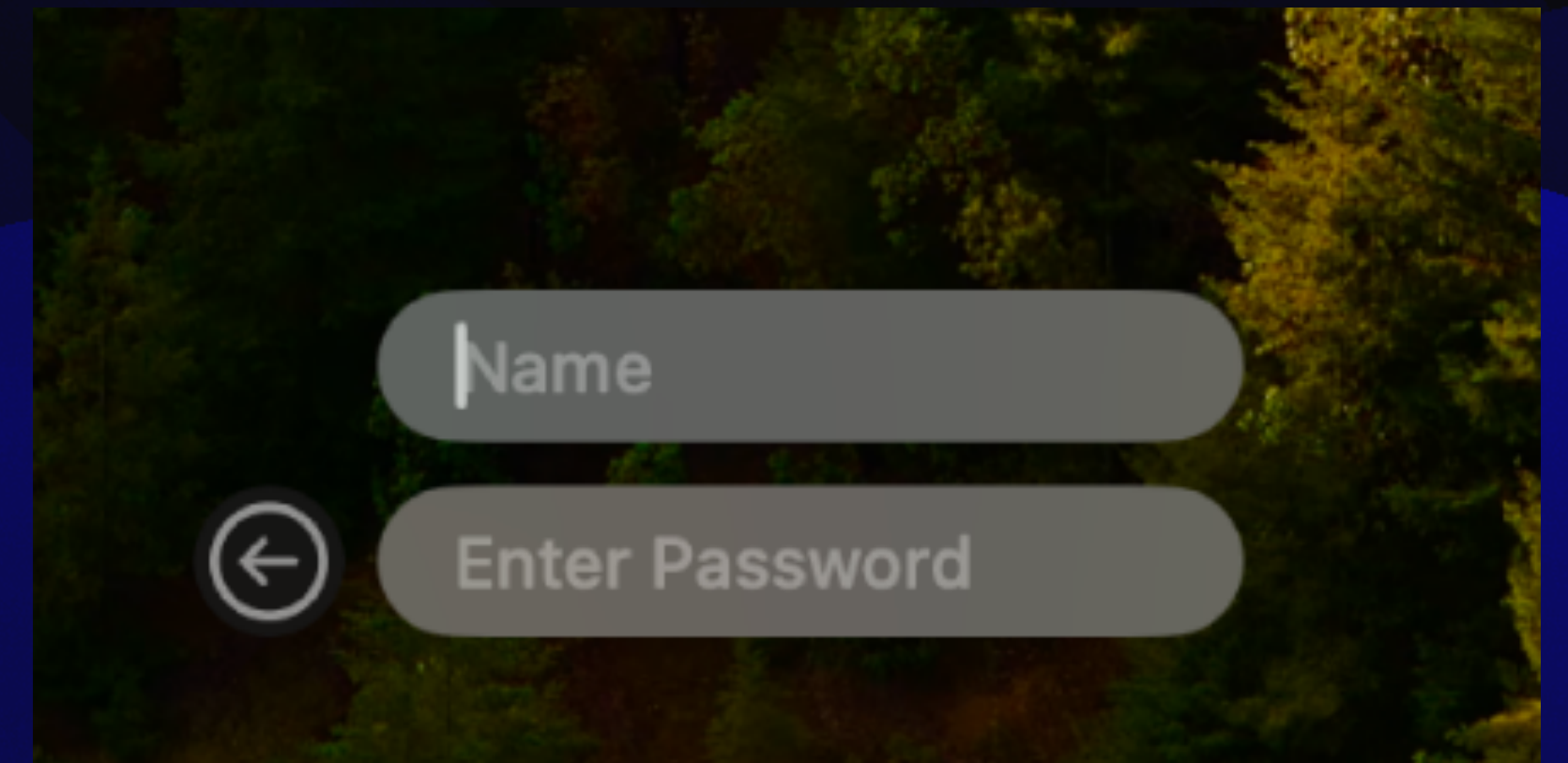
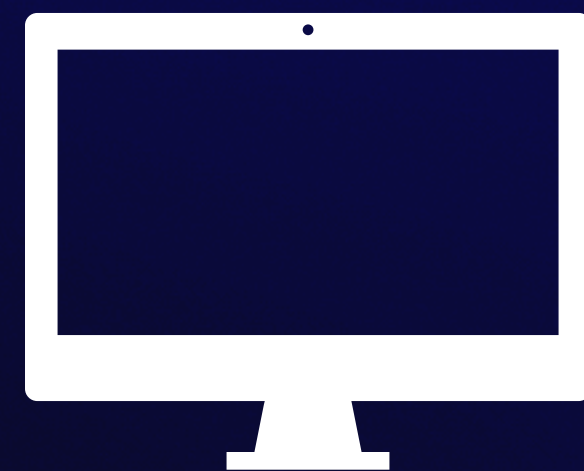
Password



# Login Window

IDP

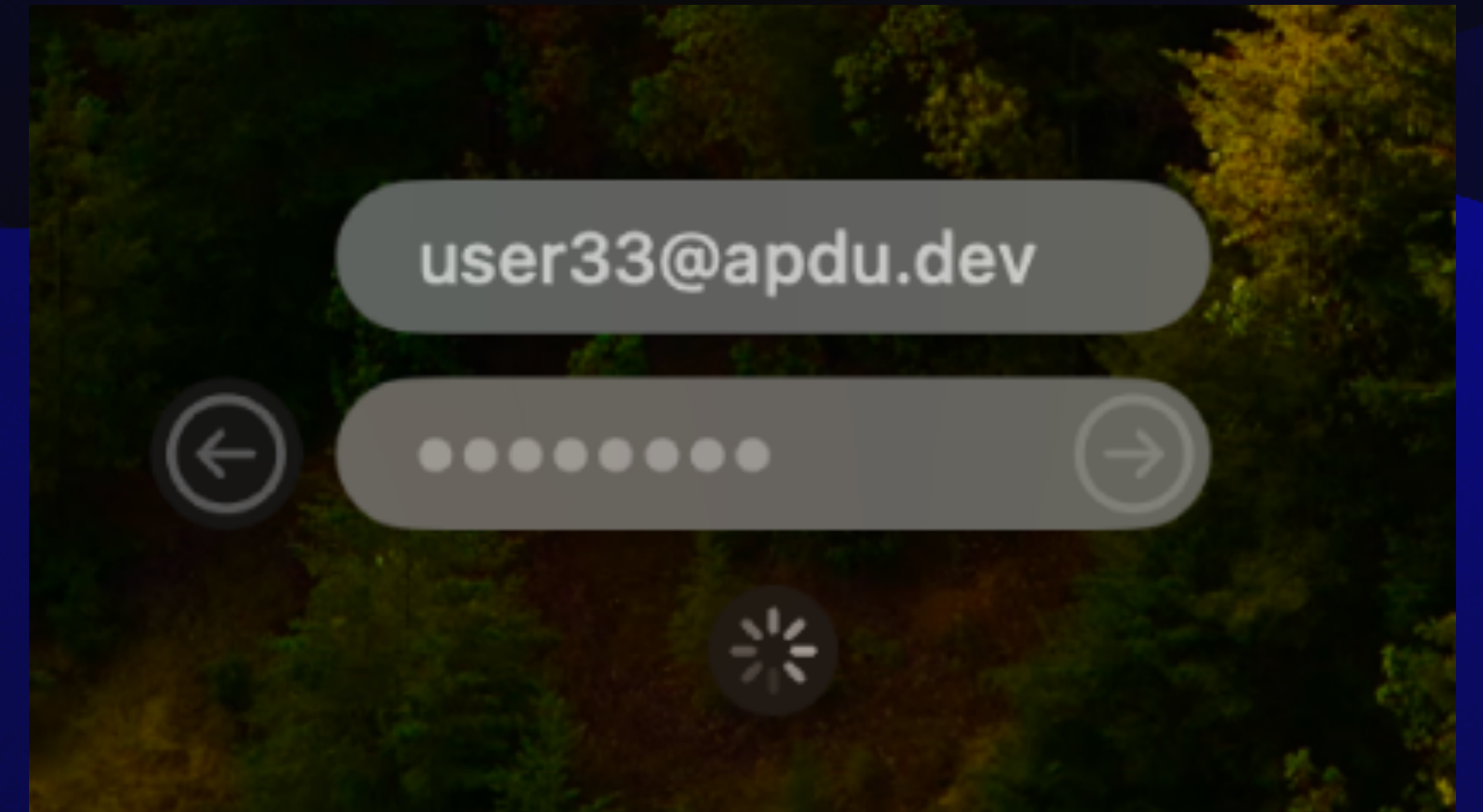
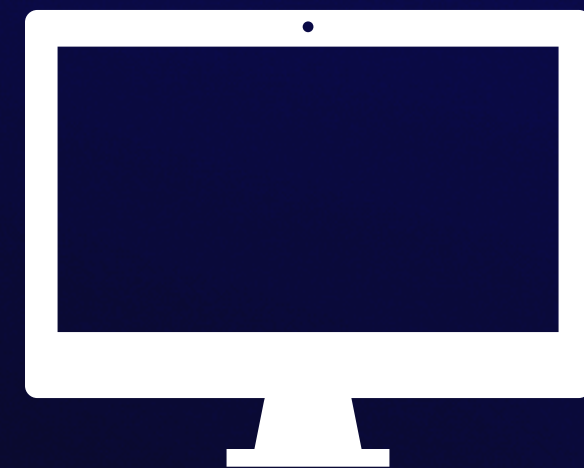
ID Token



# Login Window

IDP

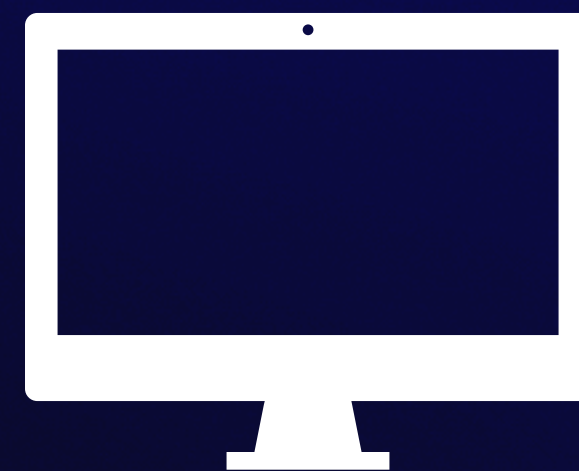
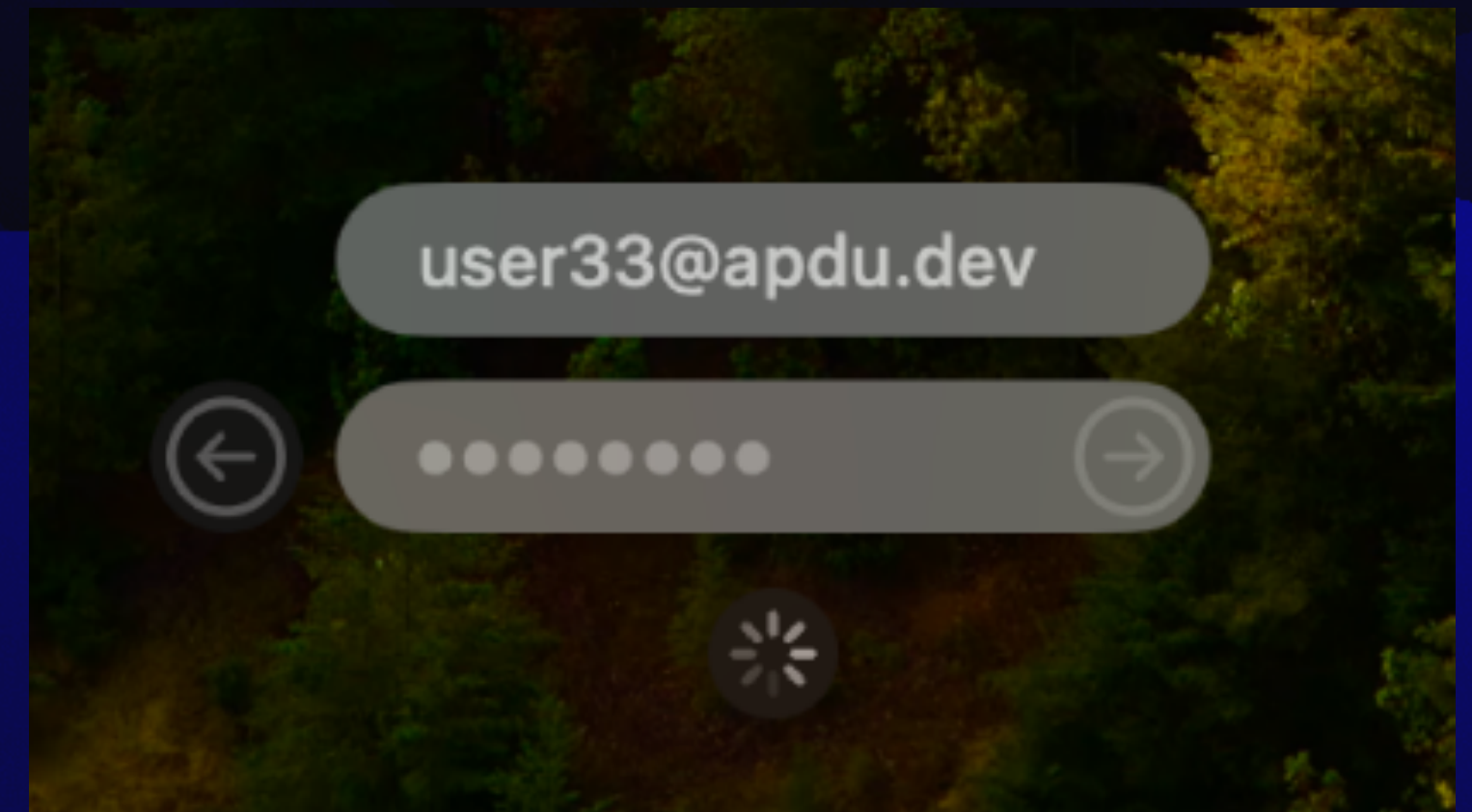
ID Token



# Login Window

IDP

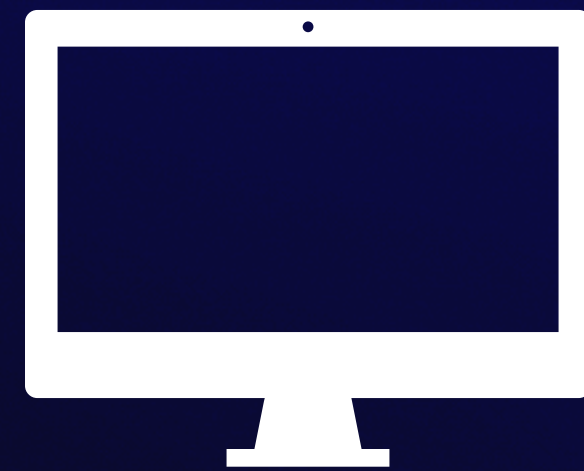
ID Token



# Login Window

IDP

Can has cert?



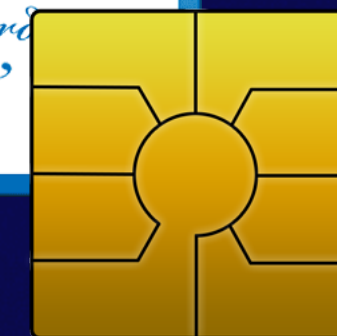
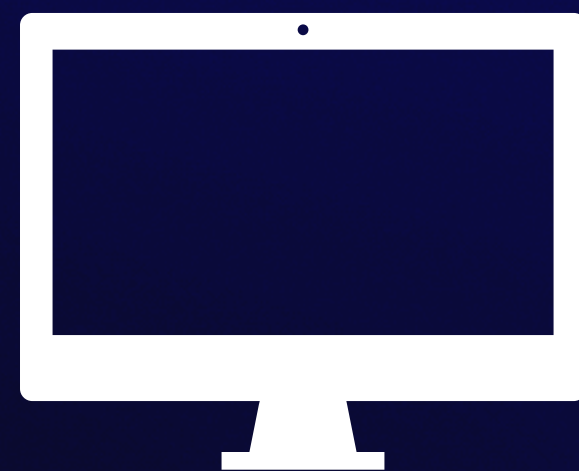


# Login Window



IDP

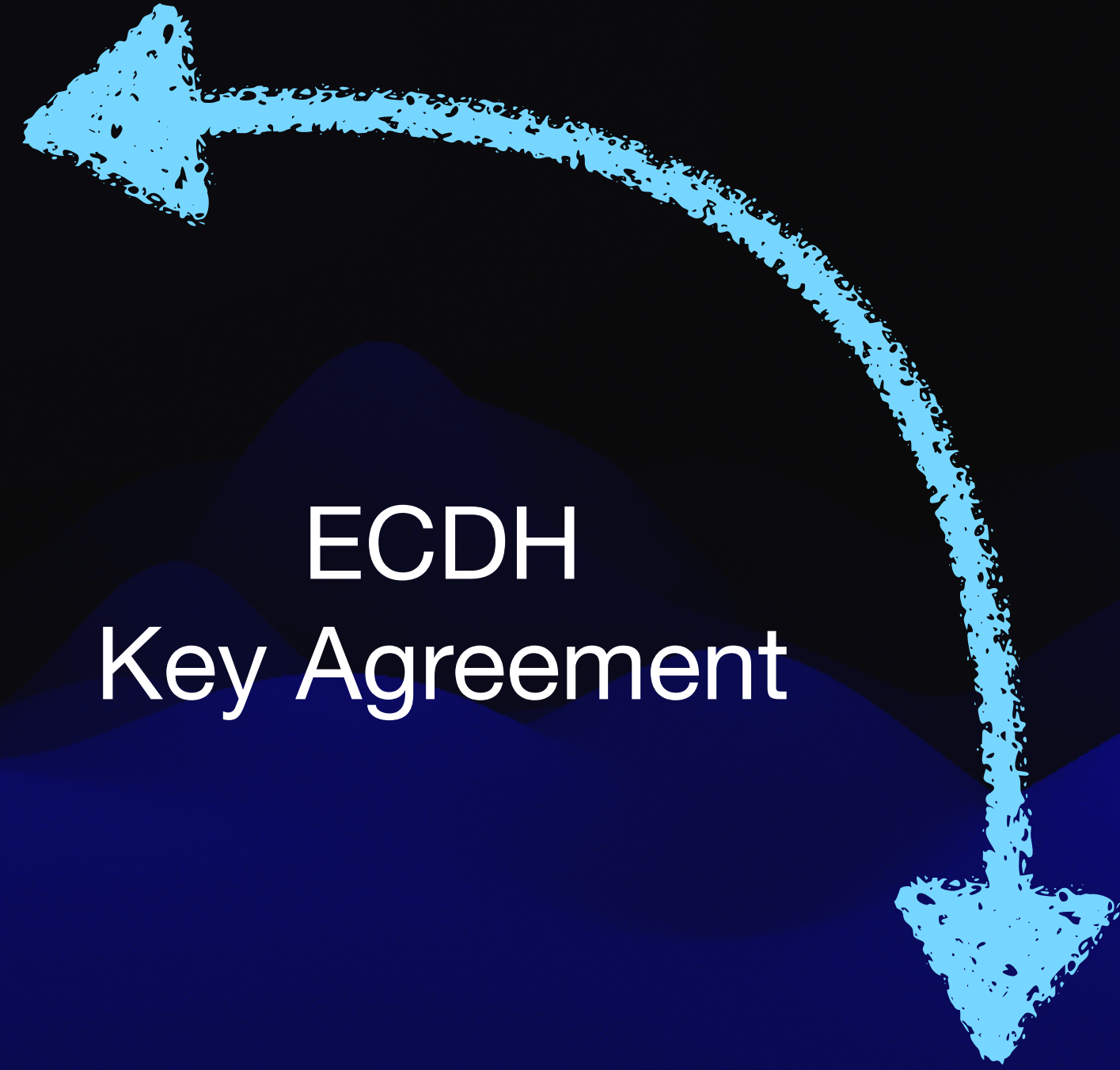
Yes!



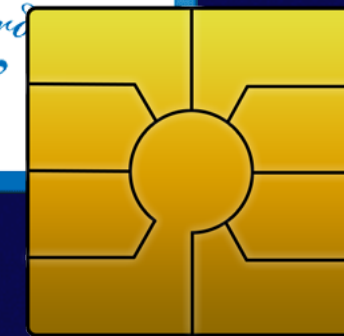
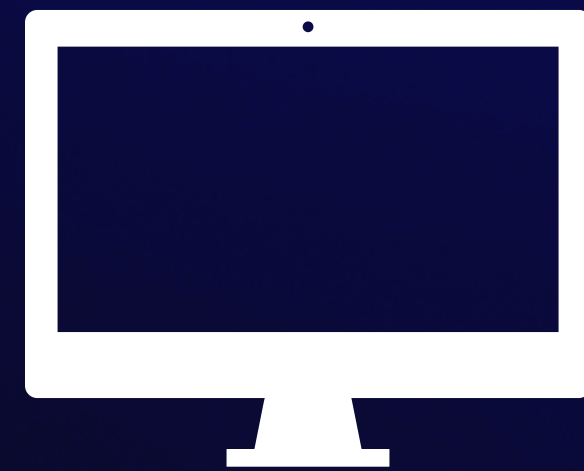
# Pass change



IDP



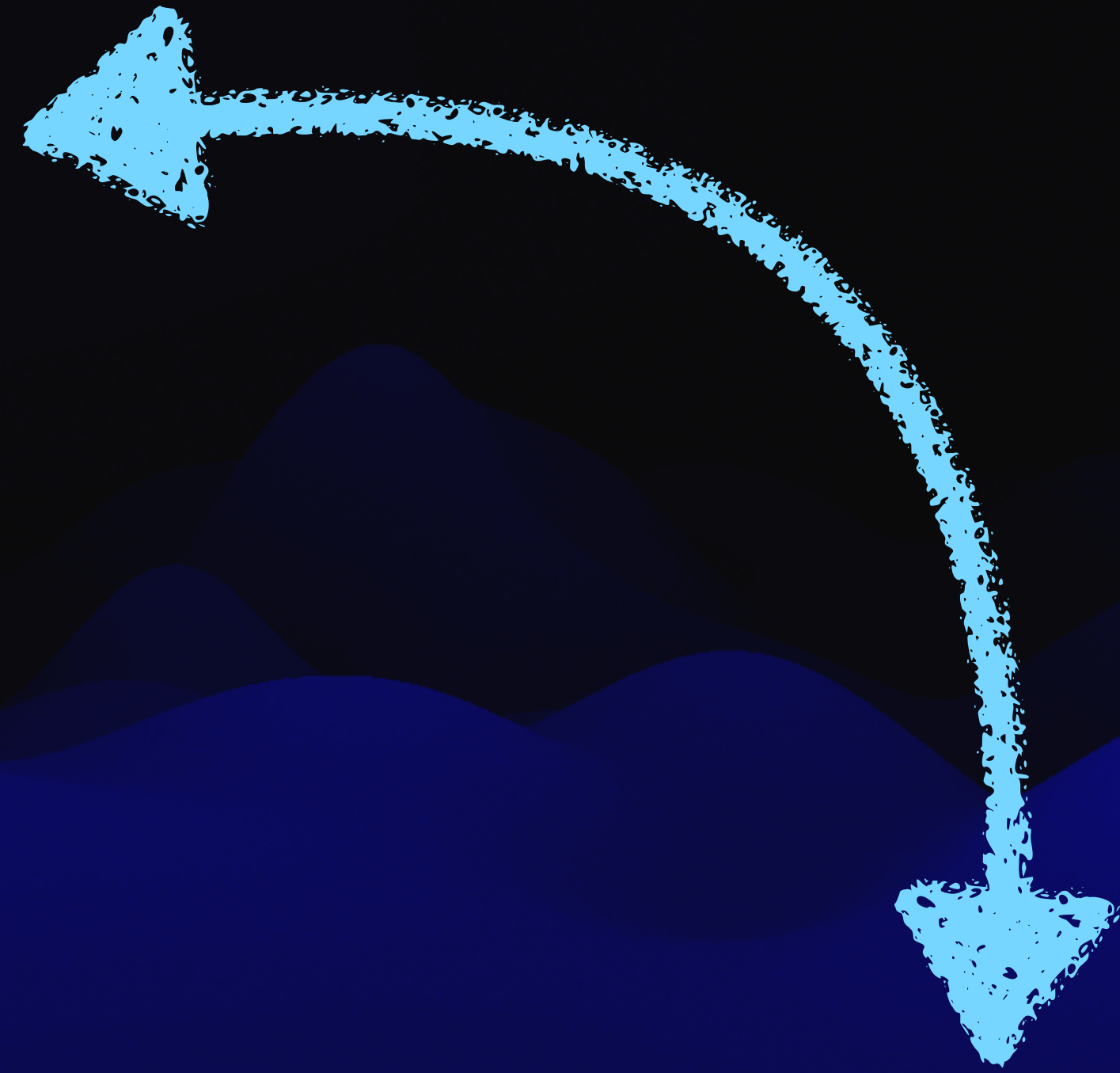
ECDH  
Key Agreement



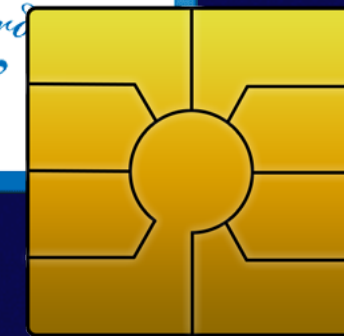
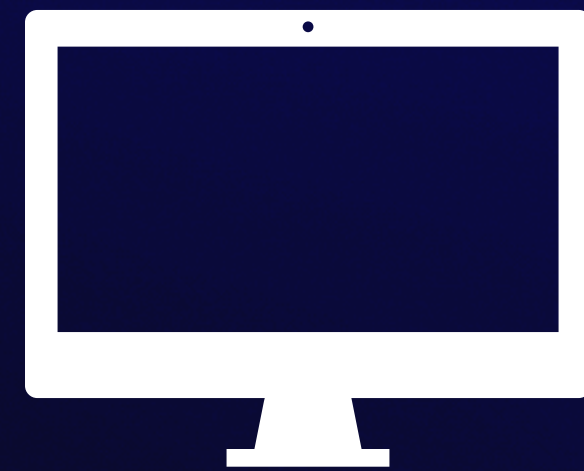
# Pass change



IDP



FileVault  
Keychain





Kaname Uten Day  
World Premier

# Authorization Groups

- Functionally similar to twiddling `security authorizationdb` yourself
- Best when used during account creation
  - No method to force an update to groups - need a user authentication event
  - May require a user logout/login cycle

# Guided Q and A

# Best ways to troubleshoot?

app-ssso platform -s

Logging on subsystem  
*com.apple.AppSSO* and category  
*PODiagnostics*

Does this have to come from my  
Identity Provider?

Pretty much, yes it does.



**Can I have only some users on the Mac using Platform SSO?**

**Not really**

Is Platform SSO connected to  
Apple Device Enrollment in any  
way?

No

Can my Identity Provider push a password change?

No

**How often is the password synched?**

**Every 4 hours when logging in, or when the user puts in a new password at a login dialog.**

**How does this work with  
FileVault?**

**Reasonably well, as long as  
you've caught the password  
change.**

How does this work with MFA?

It doesn't

Does the user have to interact  
with PSSO to get it set up?

Yes

Other questions.....?



**Thanks!**