

XCreds 2

Supercharge the Mac Login Window

Timothy Perfitt
tperfitt@twocanoes.com

Overview

- Who am I and What We Do
- Why Is This Even Needed?
- What XCreds Does
- How XCreds Works
- How You Can Get It

Shoulders Of Giants

- Thanks for NCSU and Everette Allen for supporting the project
- Free, Open Source OIDC (Cloud) Password Syncing for MacAdmin Community
- Joel Rennich (Mactroll) for OIDCLite framework and NoMAD / NoMAD Login codebase

Who Am I?



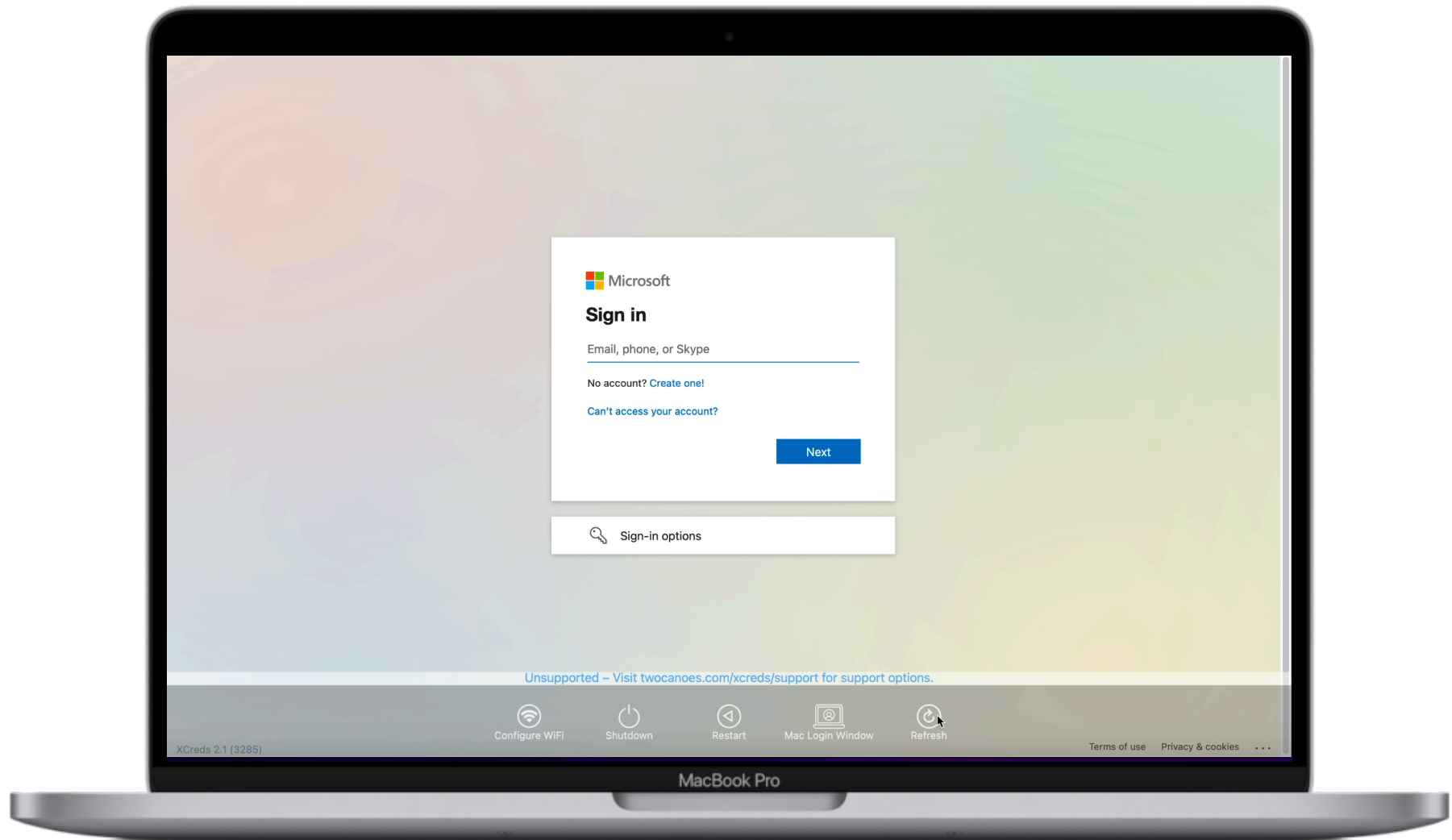
Why Is This Even Needed?

- Managing Passwords is Hard
- Forgotten Passwords are Expensive
 - Help Desk Tickets
 - Data Loss
 - Security

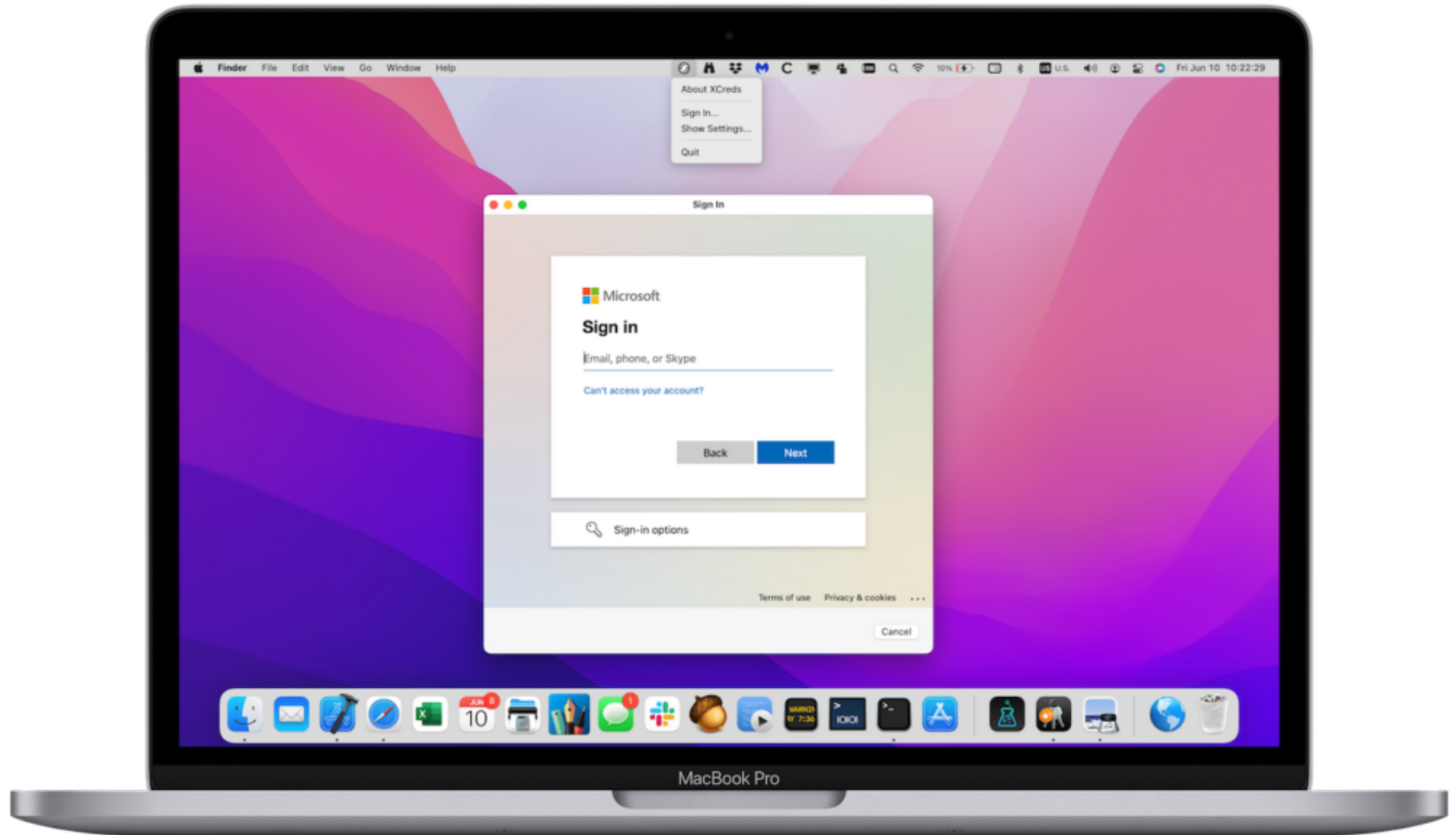
Example

- Bob loves his Mac
- Bob uses his mac every day and is super productive
- Bob access all company resources through Azure sign-in from a browser or interstitial browser in an app
- Bob goes on vacation
- Bob returns refreshed and Bob can no longer remember his login password or FileVault password since he hasn't need it in months
- Bob is sad
- IT is sad

Toto This...



And This



Demo

Login Window

- User Enters Cloud ID and Password (and MFA)
- XCreds uses javascript to retrieve password from webpage
- XCreds receives authentication tokens and verifies successful login.
- XCreds checks local password to see if it matches local password.
 - If no match, prompts for prior password. Verifies and logs in.
 - If match, unlocks user keychain and allows login.
- XCreds saves password and tokens in user keychain

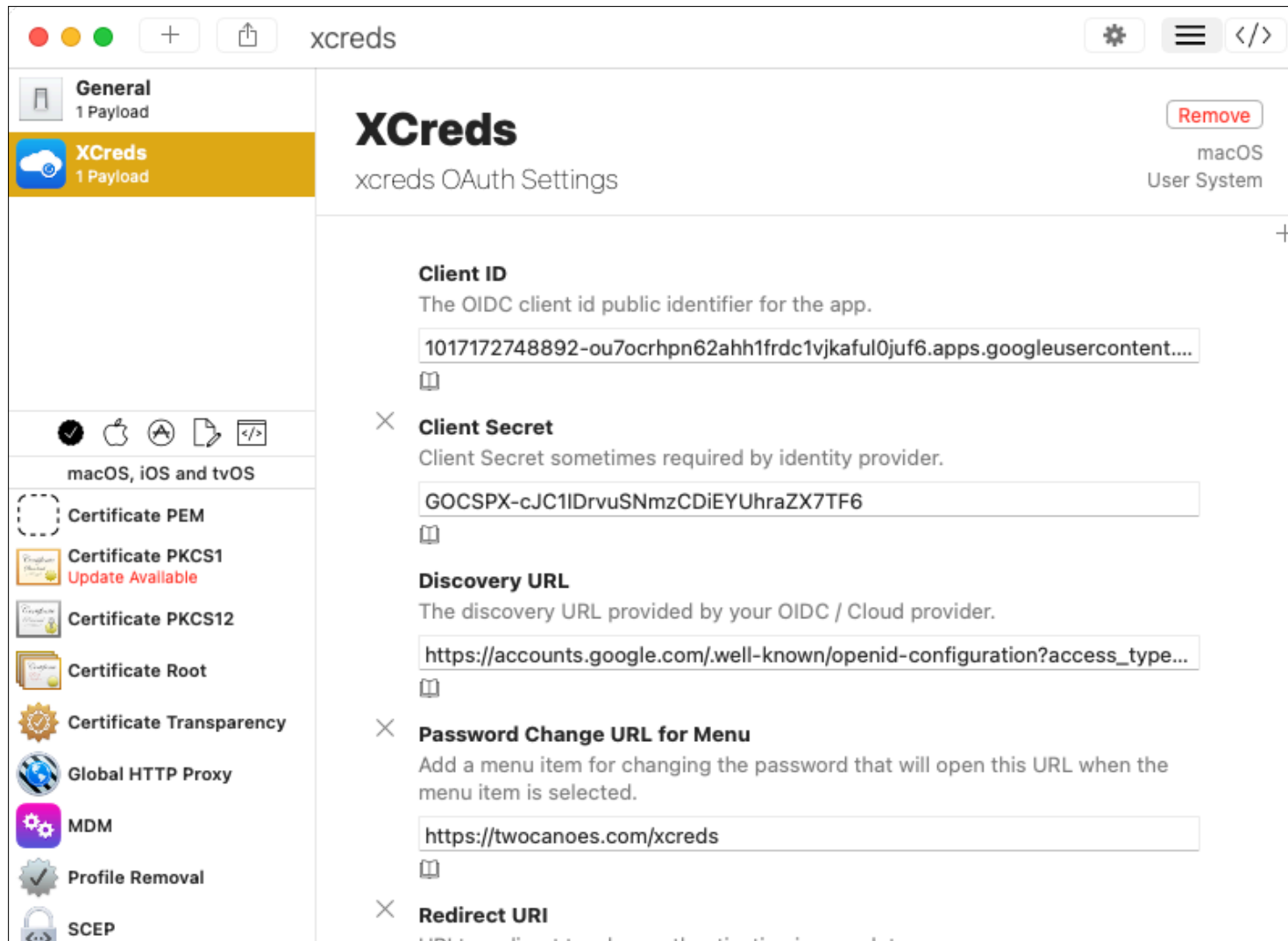
Logged in User

- Every 3 hours, a new refresh token is requested from the prior refresh token
 - If fails, prompt user
 - If succeeds, save new refresh token

Advanced Features

- User Account and Home Provisioning
- FileVault Support
- MDM managed
- Offline access
- Join WiFi at Login Window

How XCreds is Configured



Azure Configuration

The screenshot shows the 'Register an application' page in the Azure portal. The browser address bar shows the URL `portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/Applications`. The page header includes the Microsoft Azure logo, a search bar, and the user profile `tperfitt@twocanoes.com`. The main content area is titled 'Register an application' and includes a close button (X). A text input field contains 'xcreds' with a checkmark icon. Below this, the 'Supported account types' section asks 'Who can use this application or access this API?' and provides four radio button options: 'Accounts in this organizational directory only (twocanoes.com only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. A 'Help me choose...' link is present. The 'Redirect URI (optional)' section explains that the URI is used for authentication responses and provides a dropdown menu set to 'Public client/native (mobile ...)' and a text input field containing 'xcreds://auth/' with a checkmark icon. A note at the bottom states: 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).' At the very bottom, there is a link 'By proceeding, you agree to the Microsoft Platform Policies' and a blue 'Register' button.

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/Applications

Microsoft Azure Search resources, services, and docs (G+)

tperfitt@twocanoes.com TWOCANOE...

Home > App registrations >

Register an application

xcreds ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (twocanoes.com only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... xcreds://auth/ ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

Google Cloud Configuration

The screenshot displays the Google Cloud console interface for configuring an OAuth consent screen. The left sidebar shows the navigation menu with 'APIs & Services' selected. The main content area is titled 'Edit app registration' and contains three tabs: 'OAuth consent screen', 'Scopes', and 'Summary'. The 'OAuth consent screen' tab is active, showing the 'App information' section. This section includes fields for 'App name' (XCredsRedux), 'User support email' (tperfitt@twocanoes.com), and 'App logo' (twocanoes_logo_2020_no_text.png). Below these fields is a preview of the app logo. The 'App domain' section is also visible, showing the 'Application home page' (https://twocanoes.com). On the right side of the console, a preview of the consent screen is shown, titled 'How is this info presented to users?'. This preview includes a 'Sign in with Google' button, a consent screen with a display name, and a section for selecting what the app can access. The preview is annotated with numbered red boxes: 1 for the app logo and name, 2 for the 'Select what [Display Name] can access' section, and 3 for the 'Make sure you trust [Display Name]' section. The bottom of the preview shows 'Cancel' and 'Allow' buttons.

console.cloud.google.com/apis/credentials/consent/edit;newAppInternalUser=tr

Google Cloud Xcreds Test

Search credentials

APIs & Services

Enabled APIs & services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *

XCredsRedux

The name of the app asking for consent

User support email *

tperfitt@twocanoes.com

For users to contact you with questions about their consent

App logo

twocanoes_logo_2020_no_text.png

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

https://twocanoes.com

Provide users a link to your home page

Learn

How is this info presented to users?

This is the consent screen that users see

Sign in with Google

1 [Display Name] wants access to your Google Account

2 Select what [Display Name] can access

3 Make sure you trust [Display Name]

Cancel Allow

1. The logo and name of your app

How You Can Get It

- <https://github.com/twocanoes/xcreds>
- Open Source under an MIT-type License
- No software license fees
- We Accept Pull Requests
- Active community on the mac admins slack
- Can see (and use!) the source code

Questions?