# Single Sign On Extensions

## Less typing, more authing

# Joel Rennich

NoMAD/Jamf

**“I love typing my password many times a day. I love it even more when I have to change my password every 30 days.**

**Coming up with unique 12 character passwords really adds meaning to my life.”**

***– No user ever***

# Before we start...

# SSO Extensions are cool

# SSO Extensions need work

Instance Property

# authorizationOptions

Options that control the authorization process.

## Declaration

```
var authorizationOptions: [URLQueryItem] { get set }
```

SDKs

iOS 13.0+

macOS 10.15+

Mac Catalyst 13.0+

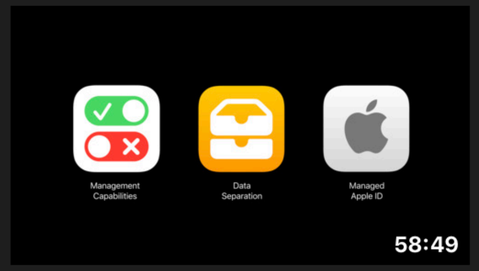
Framework

AuthenticationServices

# Apple Developer Videos


## Introducing Extensible Enterprise SSO

Tech Talks




## What’s New in Managing Apple Devices

iOS, macOS, tvOS, watchOS

Learn about the latest management enhancements for iOS, macOS, and tvOS and the evolution of management tools over the past year. You'll discover how new MDM features help administrators manage devices more effectively, how new technologies deliver support for centrally managed authorization, and...


13

# Golden Path

# What they aren’t…

# SSO Extensions are not...

- Directory Services
- A way to sign in to your user account
- No relation to Managed Apple IDs

11

# Requirements

## What you need first


13

# URL Session

- Apple-supplied URL loading system
- Used by Safari and most native applications
- Easy to use in your own code

# Things that don’t use URLSession

curl://

SMB

# MDM Required

- User Approved MDM
- Domains and/or endpoint configuration
- Extension installed and run - not required for Apple’s Kerberos extension

# Where do you get an SSOE?

- Built in Kerberos extension from Apple
- Identity Provider
- BYO

# App Extension

- Needs to be launched at least once, unless it’s from Apple
- Runs as the user

# Basic Flow

## Making the magic happen

# SSO Extension Types

Redirect

Credential

# SSO Extension Types

Modern Auth

Kerberos

# Kerberos Authentication

Kerberos

# Credential Extension

- Easiest to set up
- Kerberos is primary use, but not only use
- Built in Kerberos Extension on iOS 13 and macOS Catalina

# Credential Extension

- Engages when a 401 occurs connecting to a specified location
- Extension creates auth header which is added to the request

URLSession

URLSession

401

URLSession

URLSession

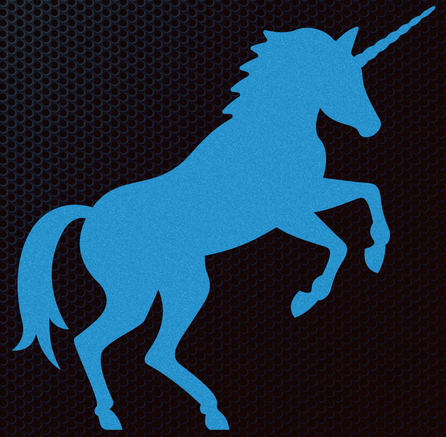
401

URLSession

401

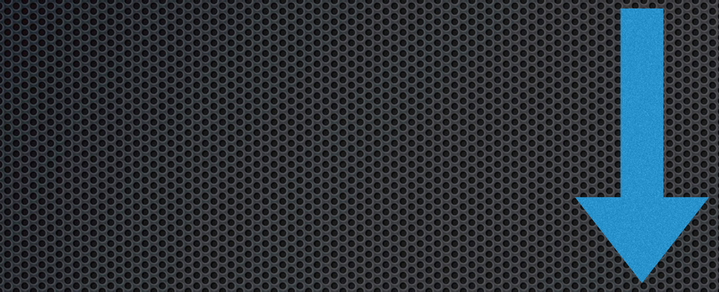
URLSession

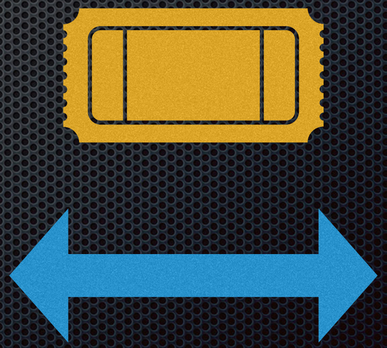
401

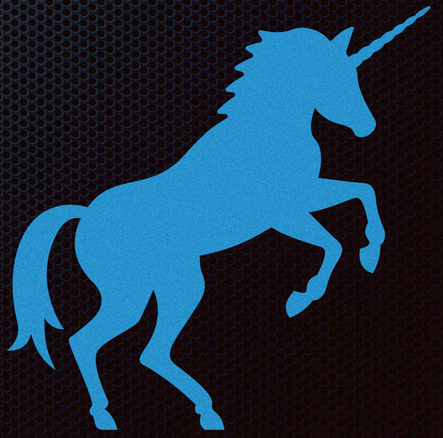


URLSession

401

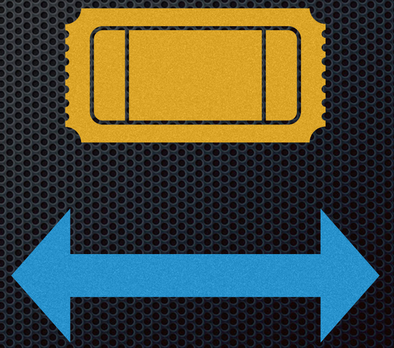


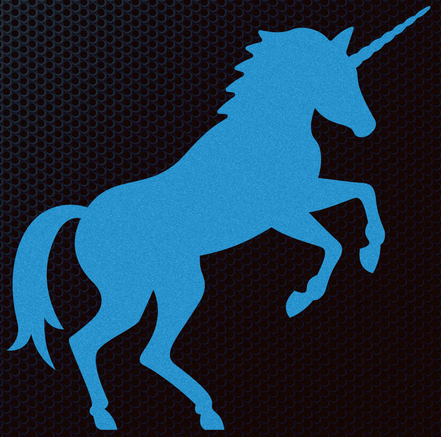




URLSession

Auth Header





# URLSession


macsysadmin.se
PROGRAM
SPEAKERS
REGISTRATION
MAC · SYS · ADMIN · GOTHENBURG
CONTACT
GÖTEBORG
SPONSORS
On October 1 – 4, we proudly present
MacSysAdmin 2019
MacSysAdmin 2019 is the event for macOS and iOS administrators to gain new knowledge, meet colleagues and exchange experiences.
Our main audience are system administrators from enterprises, schools and organisations, as well as technical consultants and resellers focusing on the Apple ecosystem. In other words, anyone working where Apple devices in any shape or form make up a large part of the environment.
The hallmark of the MacSysAdmin conference has always been our great speakers and among our illustrious alumni you will acctually find the people who literally wrote the books on this topic.
These world leading experts on all things Apple and related technologies will lecture on subjects of vital importance during the conference.
During the evening activities you can mingle, discuss, argue and have a great time with your peers.
The conference will be held at Chalmers Conference Centre in the center of Göteborg, Sweden.
Seats are limited to 250.
All sessions are held in English.
Welcome!

## Single Sign-On Extensions

**EXTENSION IDENTIFIER** Bundle identifier of the app extension that performs single sign-on

com.apple.AppSSOKerberos.KerberosExtension

**TEAM IDENTIFIER** Team identifier of the app extension that performs single sign-on

apple

**SINGLE SIGN-ON TYPE**

- (•) Credential
- ( ) Redirect

**REALM** Realm name for the Credential-type payload. This value must be properly capitalized.

NOMAD.MENU

## Single Sign-On Extensions

**EXTENSION IDENTIFIER** Bundle identifier of the app extension that performs single sign-on

com.apple.AppSSOKerberos.KerberosExtension

**TEAM IDENTIFIER** Team identifier of the app extension that performs single sign-on

apple

**SINGLE SIGN-ON TYPE**

- (•) Credential
- ( ) Redirect

**REALM** Realm name for the Credential-type payload. This value must be properly capitalized.

NOMAD.MENU

# Live Demo!

# Troubleshooting Credential Ext.

- `app-sso` allows you to trigger the extension on macOS
- DNS

# Redirect Extension

- Requires apple-app-site-association file
- Signature and Associated Domains need to match
- Most likely will require your IdP to be involved


ADFS


Ping
Identity

# Redirect Extension

- Triggered by connecting to explicit endpoints
- Does magic then adds headers to the request

# URLSession

```
https://nomad.okta.com/oauth2/
v1/authorize
```

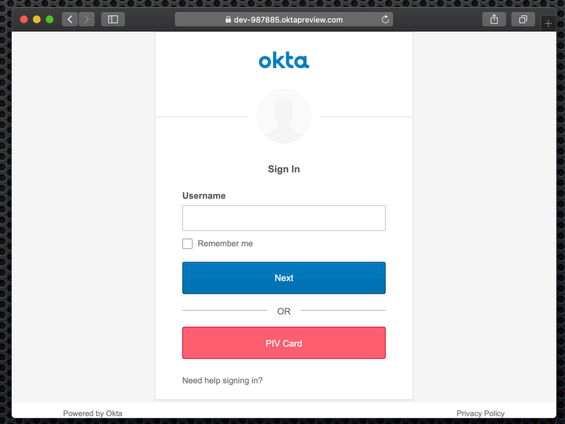
URLSession

https://nomad.okta.com/oauth2/v1/authorize

# URLSession

https://nomad.okta.com/oauth2/v1/authorize

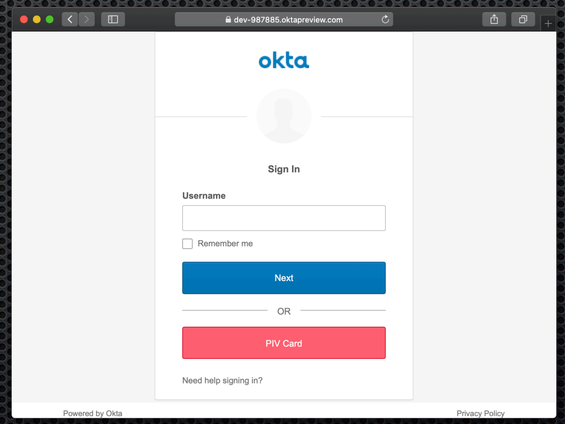
okta



# URLSession

https://nomad.okta.com/oauth2/v1/authorize





# URLSession

https://nomad.okta.com/oauth2/v1/authorize


# URLSession

https://nomad.okta.com/oauth2/v1/authorize

okta


macsysadmin.se
PROGRAM
SPEAKERS
REGISTRATION
MAC · SYS · ADMIN · GOTHENBURG
CONTACT
GÖTEBORG
SPONSORS
On October 1 – 4, we proudly present
MacSysAdmin 2019
MacSysAdmin 2019 is the event for macOS and iOS administrators to gain new knowledge, meet colleagues and exchange experiences.
Our main audience are system administrators from enterprises, schools and organisations, as well as technical consultants and resellers focusing on the Apple ecosystem. In other words, anyone working where Apple devices in any shape or form make up a large part of the environment.
The hallmark of the MacSysAdmin conference has always been our great speakers and among our illustrious alumni you will acctually find the people who literally wrote the books on this topic.
These world leading experts on all things Apple and related technologies will lecture on subjects of vital importance during the conference.
During the evening activities you can mingle, discuss, argue and have a great time with your peers.
The conference will be held at Chalmers Conference Centre in the center of Göteborg, Sweden.
Seats are limited to 250.
All sessions are held in English.
Welcome!


okta

# URLSession

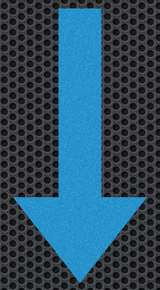
```
https://nomad.okta.com/oauth2/
v1/authorize
```

# URLSession

https://nomad.okta.com/oauth2/v1/authorize

# URLSession

https://nomad.okta.com/oauth2/v1/authorize



# URLSession

https://nomad.okta.com/oauth2/v1/authorize

# URLSession

https://nomad.okta.com/oauth2/v1/authorize




# URLSession

https://nomad.okta.com/oauth2/v1/authorize


General

Associated Domains
1 Payload Configured

Single Sign-On Extensions
1 Payload Configured



## Single Sign-On Extensions

**EXTENSION IDENTIFIER** Bundle identifier of the app extension that performs single sign-on

menu.nomad.sso.redirect

**TEAM IDENTIFIER** Team identifier of the app extension that performs single sign-on

VRPY9KHGX6

**SINGLE SIGN-ON TYPE**

- Credential
- Redirect

### URLs

URLs of identity providers where the app performs single sign-on. The URLs must begin with http:// or https:// and be unique for all configured Single Sign-On Extensions payloads. Query parameters and URL fragments are not allowed.

| URL |
| --- |
| https://adfs.nomad.menu/adfs/oauth2/authorize |
| https://adfs.nomad.menu/adfs/oauth2/token |

# Troubleshooting Redirects

- `swcutil`
- `pluginkit`
- `curl`
- Authenticated service
- `com.apple.AppSSO` subsystem

# swcutil

- `/System/Library/PrivateFrameworks/SharedWebCredentials.framework/Support/swcutil`
- Used to troubleshoot Shared Web Credentials, but also covers associated domains for this

# pluginkit

- `pluginkit -m -i menu.nomad.sso`
- Used to determine which app extension is registered for which uses and domains

# Live Demo?

11

# Q+A?

# Thanks!