#WWDC19

# What's New in Managing Apple Devices

Todd Fernandez, Senior Manager, Device Management

# Same tools for all

Same tools for all

Balance values

Same tools for all

Balance values

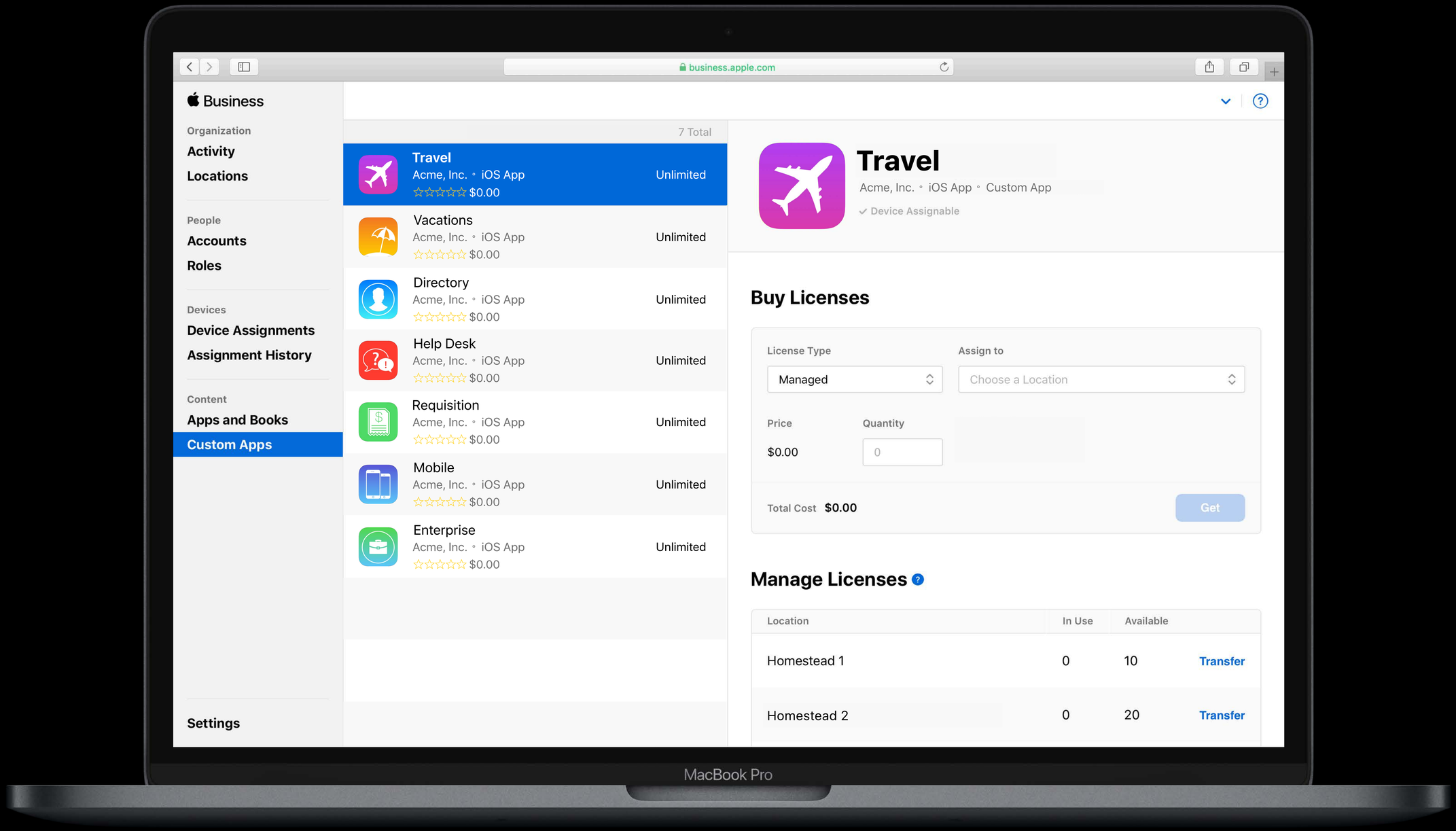
Fits in and stands out

Same tools for all

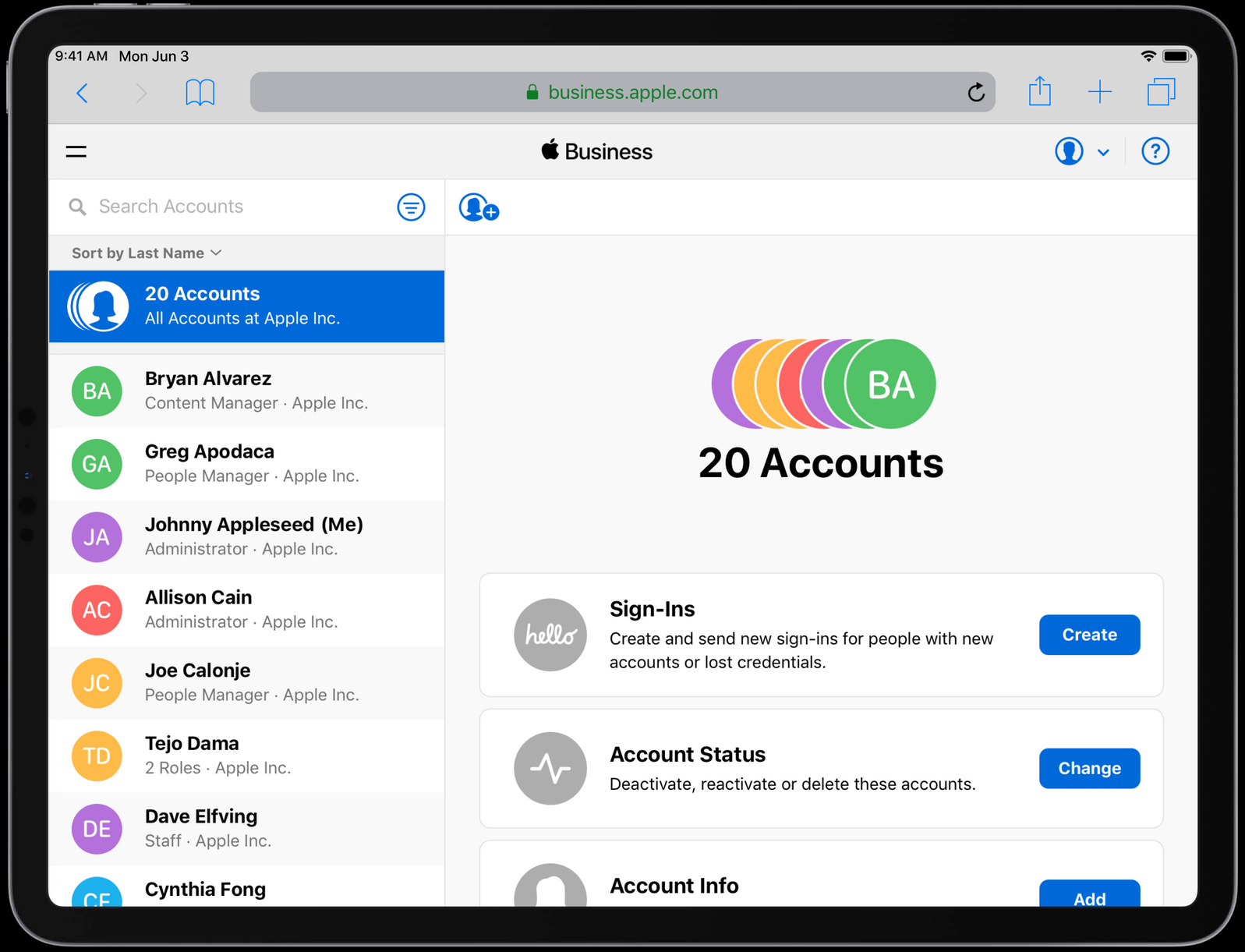
Balance values

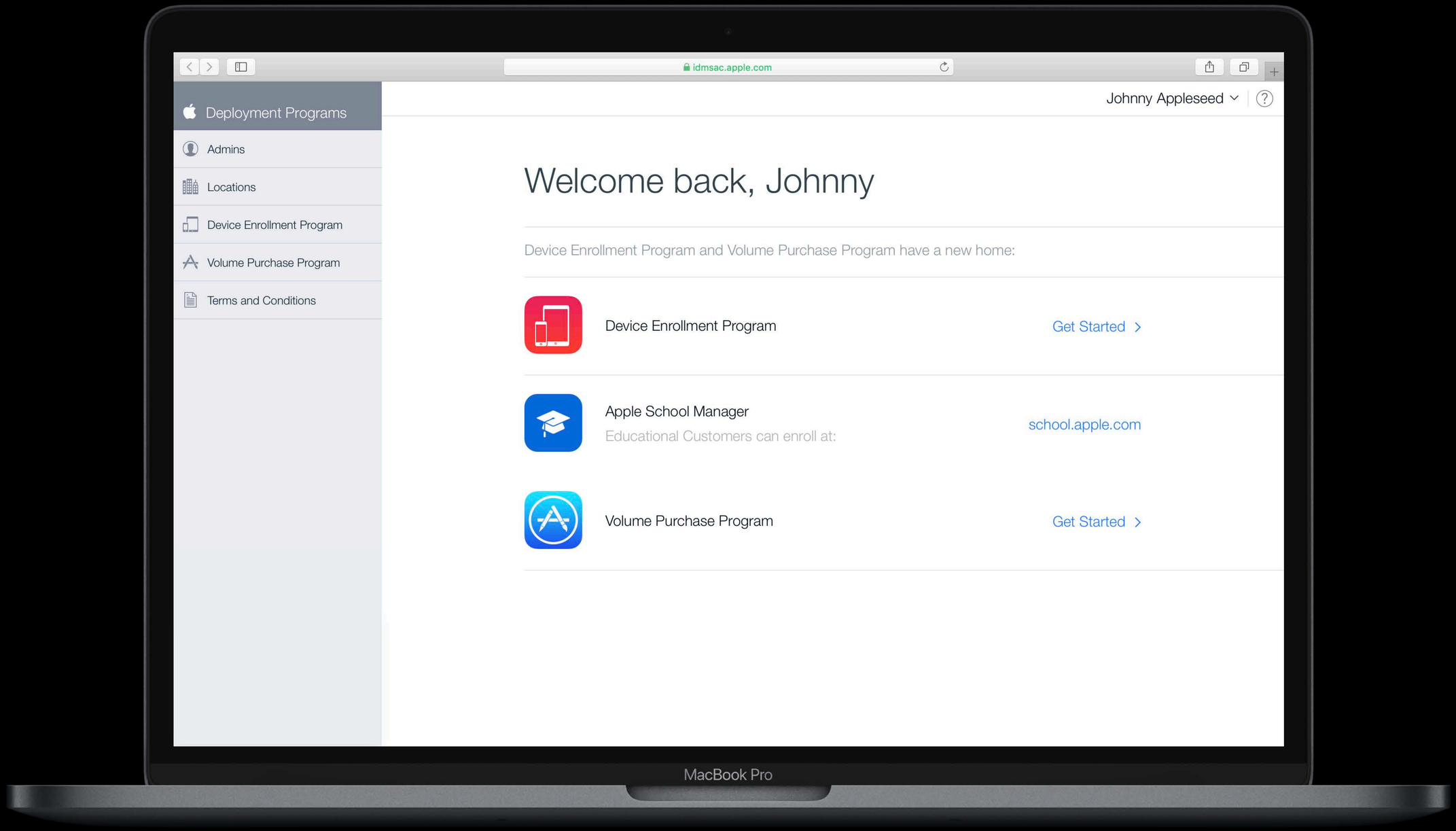
Fits in and stands out

# Same tools for all


business.apple.com
Business
Organization
Activity
Locations
People
Accounts
Roles
Devices
Device Assignments
Assignment History
Content
Apps and Books
Custom Apps
Settings
7 Total
Travel
Acme, Inc. • iOS App
$0.00
Unlimited
Vacations
Acme, Inc. • iOS App
$0.00
Unlimited
Directory
Acme, Inc. • iOS App
$0.00
Unlimited
Help Desk
Acme, Inc. • iOS App
$0.00
Unlimited
Requisition
Acme, Inc. • iOS App
$0.00
Unlimited
Mobile
Acme, Inc. • iOS App
$0.00
Unlimited
Enterprise
Acme, Inc. • iOS App
$0.00
Unlimited
Travel
Acme, Inc. • iOS App • Custom App
Device Assignable
Buy Licenses
License Type
Managed
Assign to
Choose a Location
Price
$0.00
Quantity
0
Total Cost $0.00
Get
Manage Licenses
Location
In Use
Available
Homestead 1
0
10
Transfer
Homestead 2
0
20
Transfer
MacBook Pro


business.apple.com
Business
Organization
Activity
Locations
People
Accounts
Roles
Devices
Device Assignments
Assignment History
Content
Apps and Books
Settings
Search Accounts
Sort by Last Name
20 Accounts
All Accounts at Apple Inc.
Bryan Alvarez
Content Manager · Apple Inc.
Greg Apodaca
People Manager · Apple Inc.
Johnny Appleseed (Me)
Administrator · Apple Inc.
Allison Cain
Administrator · Apple Inc.
Joe Calonje
People Manager · Apple Inc.
Tejo Dama
2 Roles · Apple Inc.
Dave Elfving
Staff · Apple Inc.
Cynthia Fong
Staff · Apple Inc.
Janelle Gee
Staff · Apple Inc.
Kim Kilgo
Device Manager · Apple Inc.
Jeena Kim
Device Manager · Apple Inc.
Johnny Appleseed
20 Accounts
Sign-Ins
Create and send new sign-ins for people with new accounts or lost credentials.
Create
Account Status
Deactivate, reactivate or delete these accounts.
Change
Account Info
Add a new Role and Location to these accounts.
Add
Accounts
Edit the username and domain of each Managed Apple ID.
Edit
MacBook Pro


9:41 AM Mon Jun 3
business.apple.com
Business
Search Accounts
Sort by Last Name
20 Accounts
All Accounts at Apple Inc.
BA
Bryan Alvarez
Content Manager · Apple Inc.
GA
Greg Apodaca
People Manager · Apple Inc.
JA
Johnny Appleseed (Me)
Administrator · Apple Inc.
AC
Allison Cain
Administrator · Apple Inc.
JC
Joe Calonje
People Manager · Apple Inc.
TD
Tejo Dama
2 Roles · Apple Inc.
DE
Dave Elfving
Staff · Apple Inc.
CF
Cynthia Fong
BA
20 Accounts
hello
Sign-Ins
Create and send new sign-ins for people with new accounts or lost credentials.
Create
Account Status
Deactivate, reactivate or delete these accounts.
Change
Account Info
Add


idmsac.apple.com
Deployment Programs
Admins
Locations
Device Enrollment Program
Volume Purchase Program
Terms and Conditions
Johnny Appleseed
Welcome back, Johnny
Device Enrollment Program and Volume Purchase Program have a new home:
Device Enrollment Program
Get Started
Apple School Manager
Educational Customers can enroll at:
school.apple.com
Volume Purchase Program
Get Started
MacBook Pro

# AppleSeed for IT

Apple Business Manager and Apple School Manager

Access with Managed Apple ID

Access software, documentation, and test plans

Associate feedback with your organization


System Preferences Edit View Window Help
Classroom
Search
Classroom allows teachers to access and control your Mac, including opening apps and navigating to websites, chapters, and pages.
Classes
Permissions
New Class Invitations
History
Mr. Roland
Classes
Science
Mrs. Abeles
Reading
Ms. Davis
Geography
Ms. Burke
Writing
Mr. Jones
Science
Remove Class...
Teacher
Mrs. Abeles
My Information
Use Name & Photo from My Card
Aaron Barnes
MacBook Pro
9:41 AM Mon Jun 3
100%
End Class
Science
Select
Open
Navigate
Lock
Mute
Screens
Add
Group
Sharing
All (29)
Safari (14)
Books (8)
Notes (7)
Aaron Notes
Addison Safari
Aiden Books
Alex Books
Anthony Safari
Aubrey Notes
Ava Safari
Avery Books
Brayden Notes
Brooklyn Books
Chloe Notes
Claire Safari
Elizabeth Safari
Ella Books
Gabriel Safari
Gavin Safari
Isabella Safari
Julia Books
Kaelyn Notes
Logan Safari
Lucas Safari
Mason Books
Mia Safari
Natalie Safari
Noah Notes
Owen Safari
Riley Notes
Tristan Books
Zoe Safari

# Bring Existing iOS Restrictions to macOS

## Classroom

Automatically join classes

Request permission to leave classes

Don’t prompt for app and device lock

Don’t prompt for screen observation

# Bring Existing iOS Restrictions to macOS

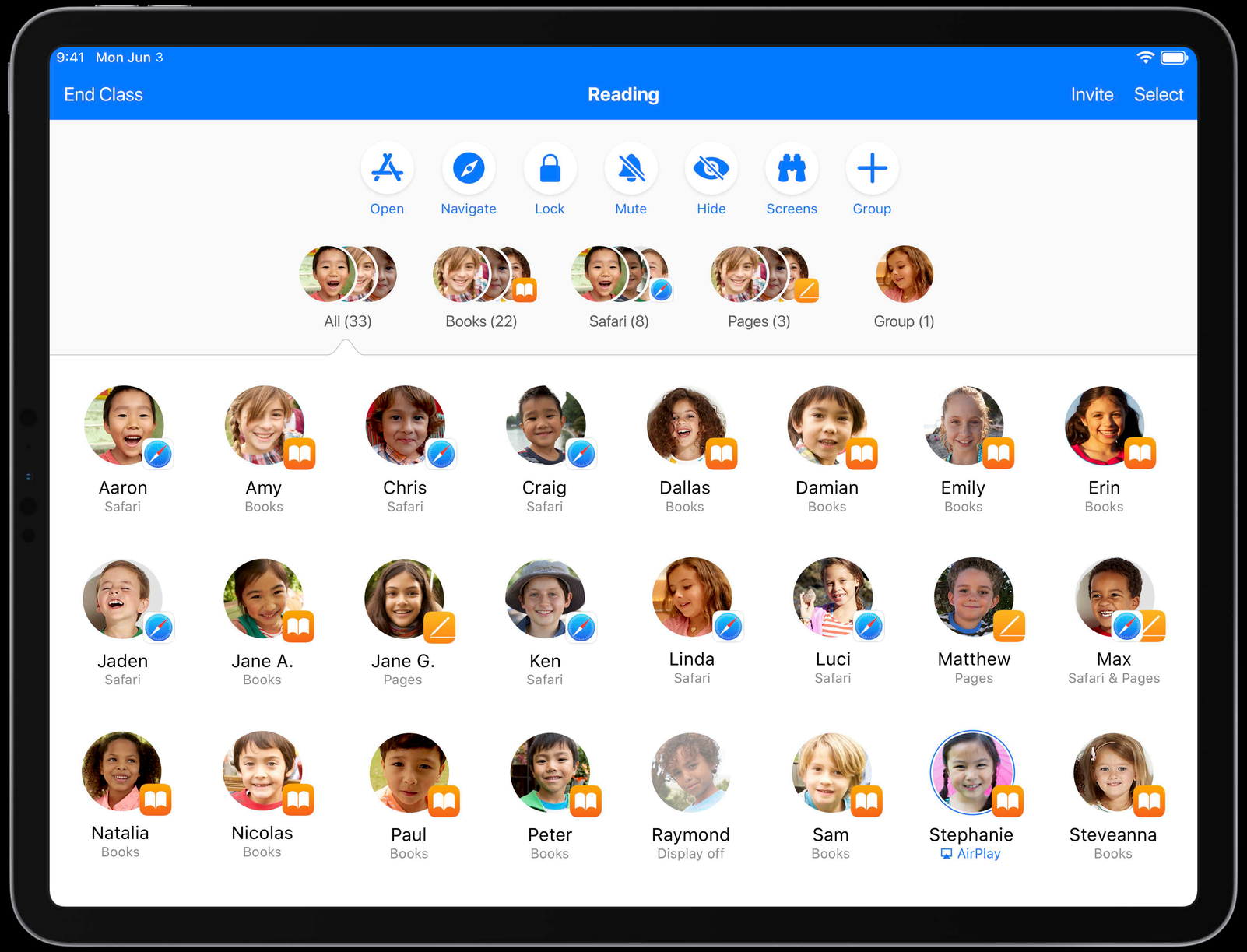
## Screen viewing

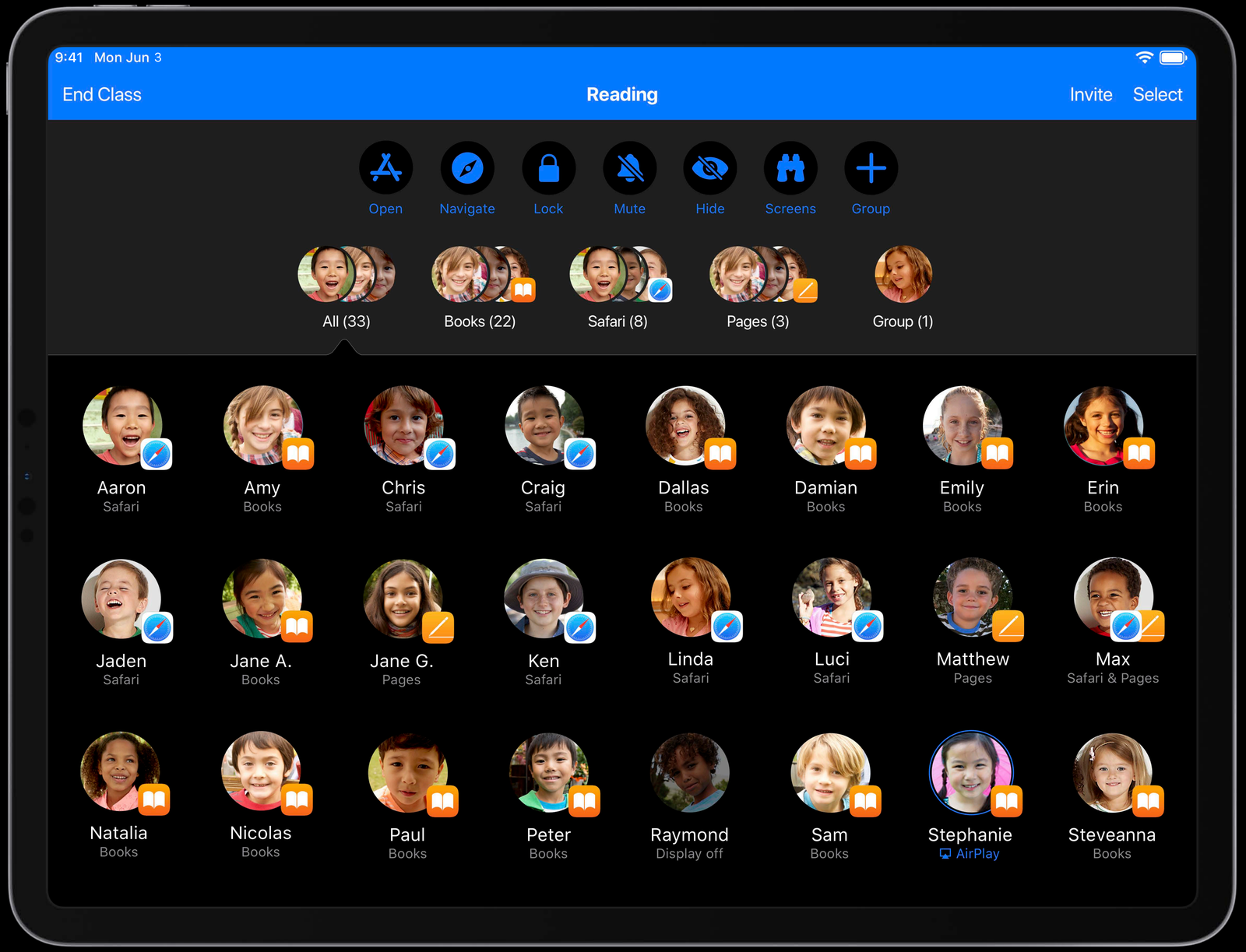
Allow remote screen observation

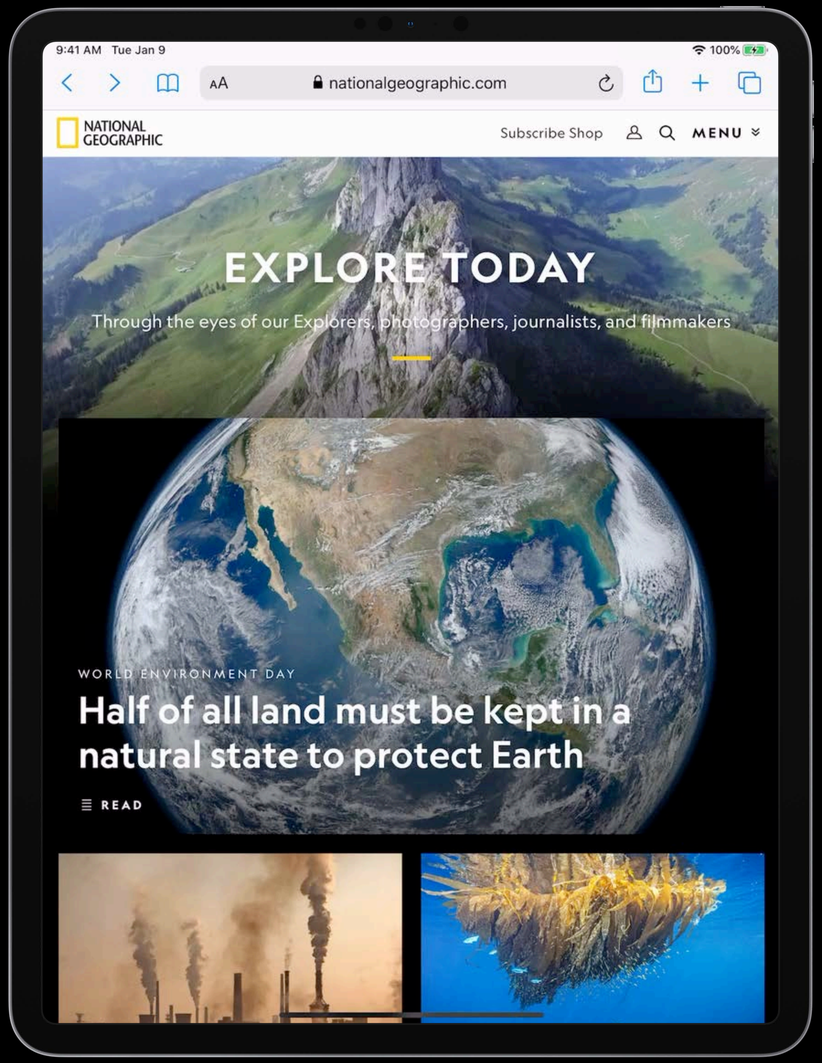
Allow screenshot

Affects

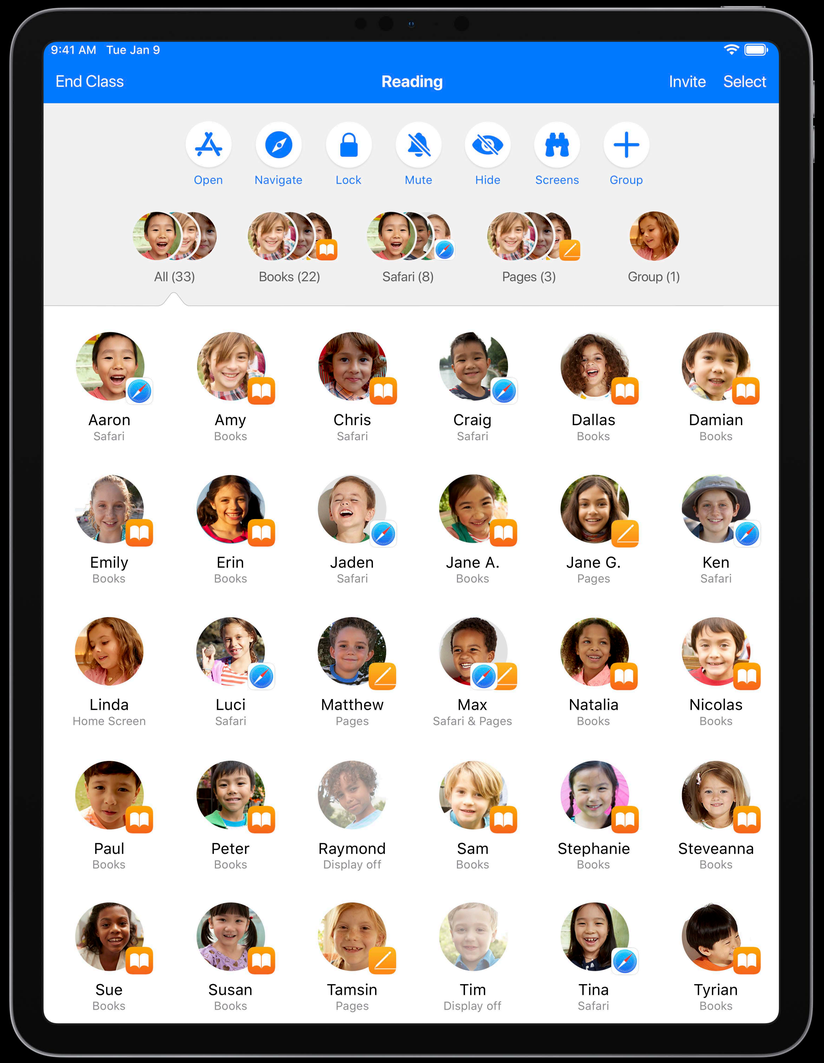
- Remote Desktop
- Screen Sharing
- Screenshot


9:41 Mon Jun 3
End Class
Reading
Invite
Select
Open
Navigate
Lock
Mute
Hide
Screens
Group
All (33)
Books (22)
Safari (8)
Pages (3)
Group (1)
Aaron
Safari
Amy
Books
Chris
Safari
Craig
Safari
Dallas
Books
Damian
Books
Emily
Books
Erin
Books
Jaden
Safari
Jane A.
Books
Jane G.
Pages
Ken
Safari
Linda
Safari
Luci
Safari
Matthew
Pages
Max
Safari & Pages
Natalia
Books
Nicolas
Books
Paul
Books
Peter
Books
Raymond
Display off
Sam
Books
Stephanie
AirPlay
Steveanna
Books

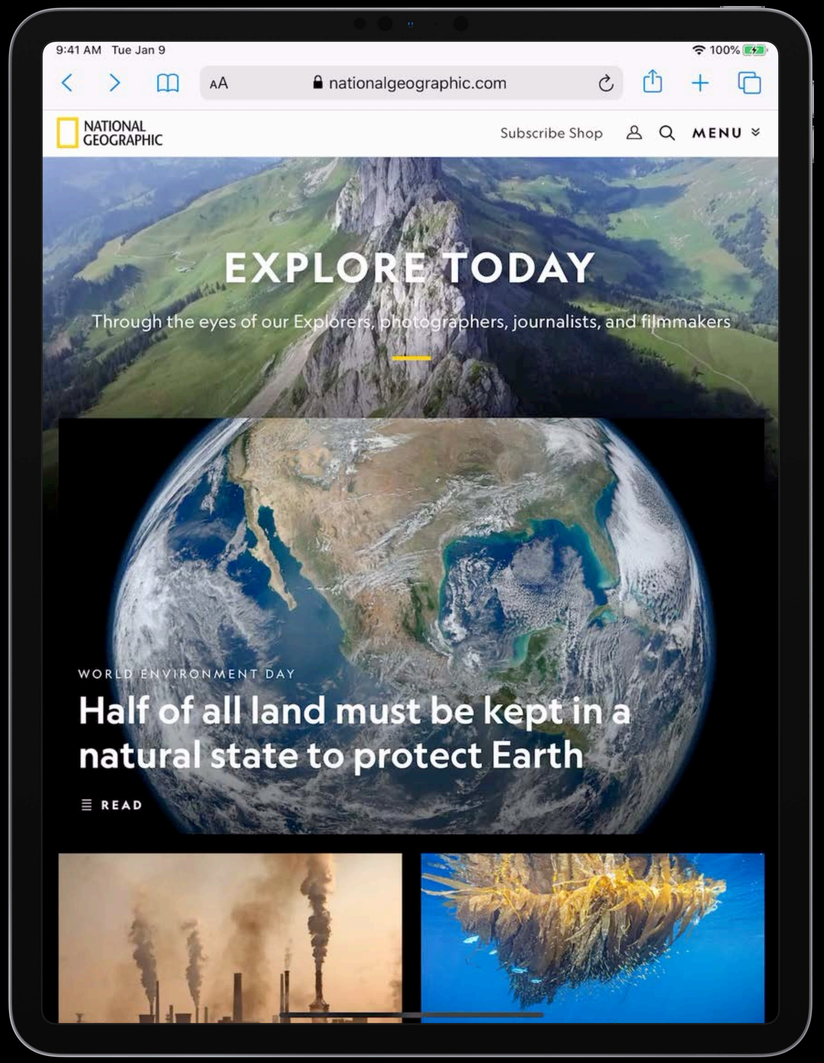

9:41 Mon Jun 3
End Class
Reading
Invite
Select
Open
Navigate
Lock
Mute
Hide
Screens
Group
All (33)
Books (22)
Safari (8)
Pages (3)
Group (1)
Aaron
Safari
Amy
Books
Chris
Safari
Craig
Safari
Dallas
Books
Damian
Books
Emily
Books
Erin
Books
Jaden
Safari
Jane A.
Books
Jane G.
Pages
Ken
Safari
Linda
Safari
Luci
Safari
Matthew
Pages
Max
Safari & Pages
Natalia
Books
Nicolas
Books
Paul
Books
Peter
Books
Raymond
Display off
Sam
Books
Stephanie
AirPlay
Steveanna
Books



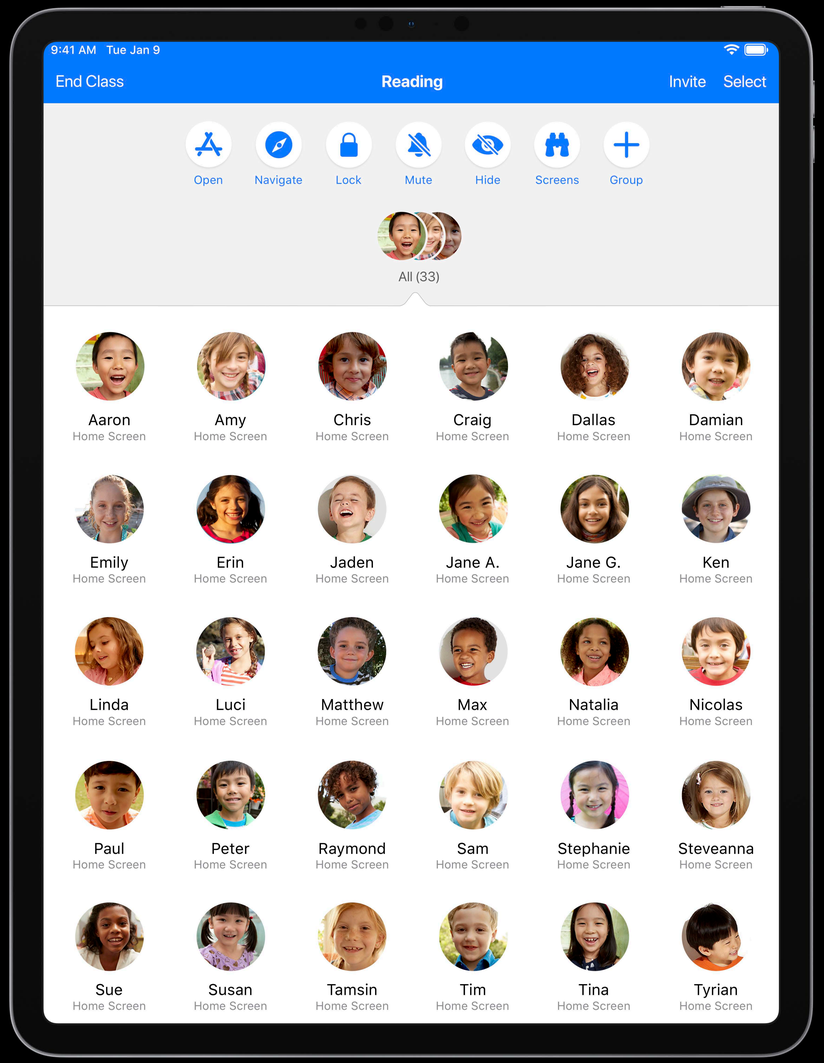

Student




Teacher




Student




Teacher

# Desktop-Class Browsing on iPad

NEW

- iPad identifies as Mac
- May break MDM UI or enrollment flows
- Stop using UserAgent

# Desktop-Class Browsing on iPad

NEW

- iPad identifies as Mac
- May break MDM UI or enrollment flows
- Stop using UserAgent

# Platform Parity
## tvOS

Managed Software Updates

Force automatic date and time

Content Caching for screen savers

# Same tools for all

Same tools for all

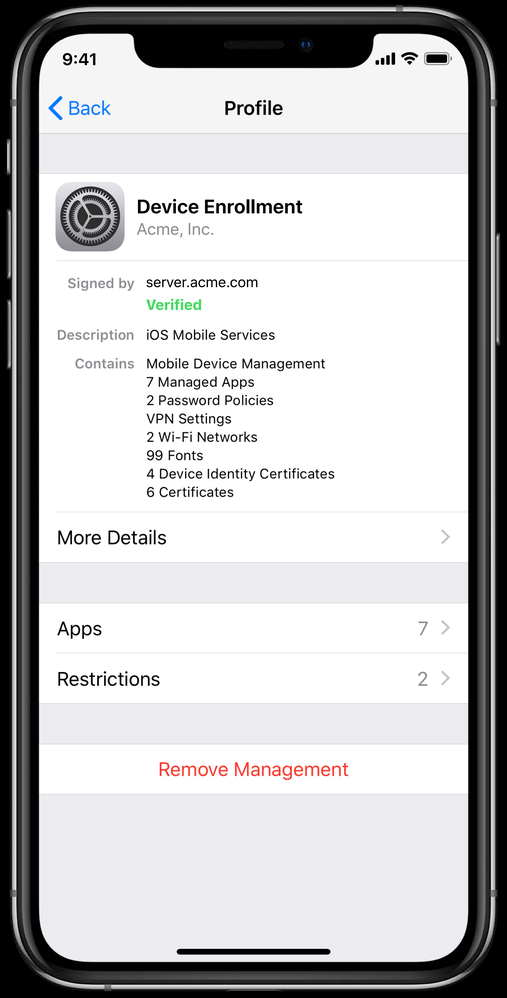
Balance values

Fits in and stands out

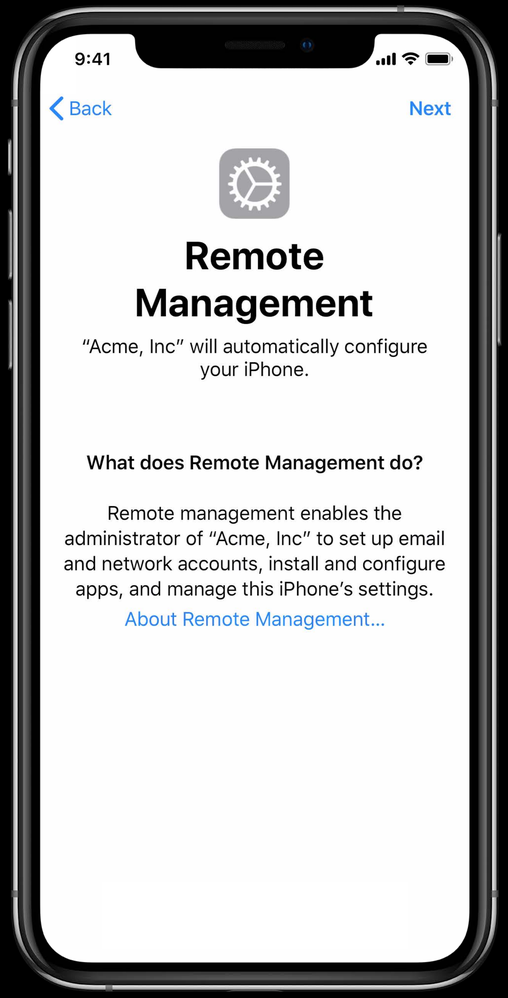
# Balance values

# User Enrollment

Bob Whiteman, Senior Device Management Engineer



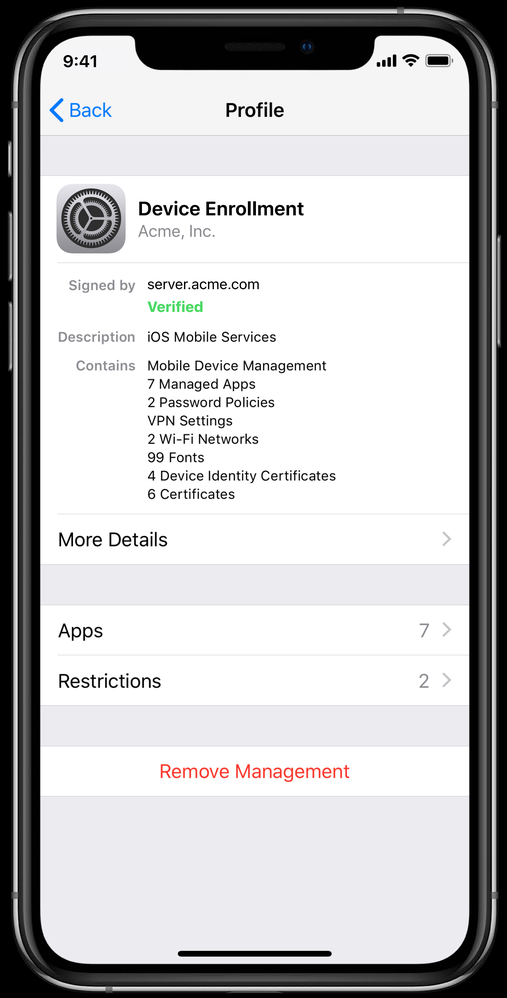

Device Enrollment



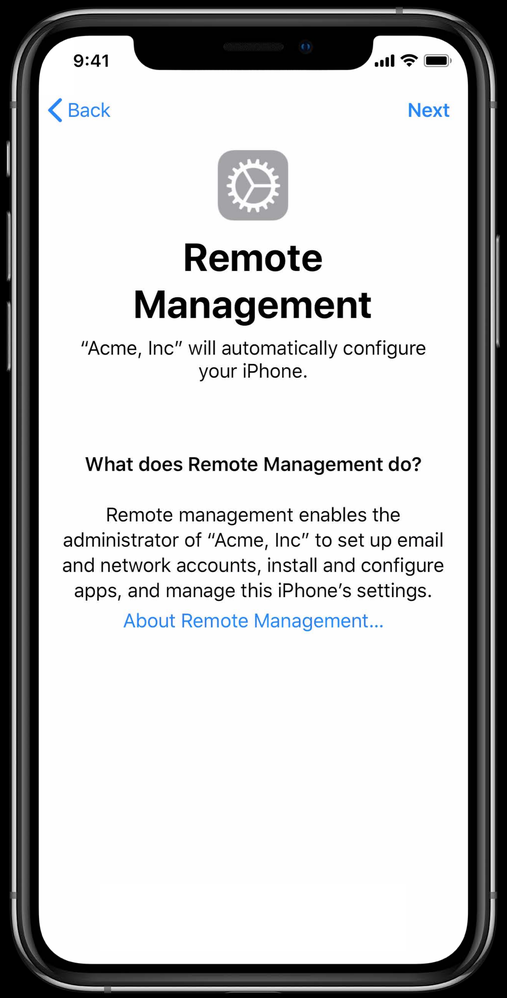

Automated Device Enrollment

SUPERVISED


BYOD

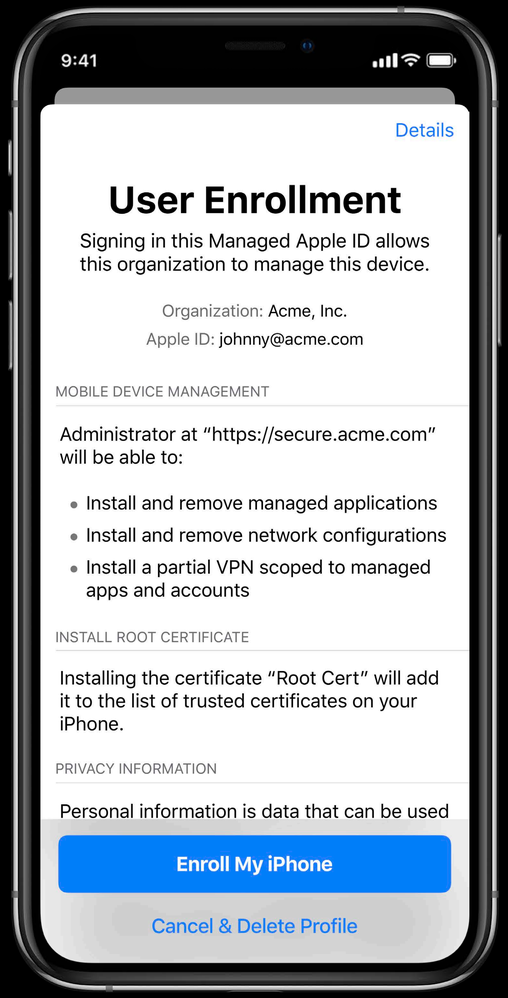



Device Enrollment

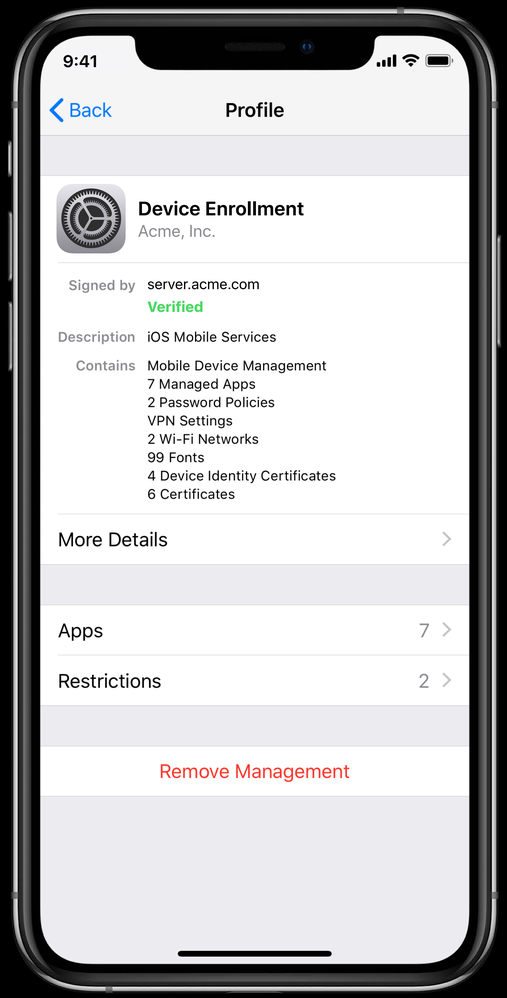



Automated
Device Enrollment

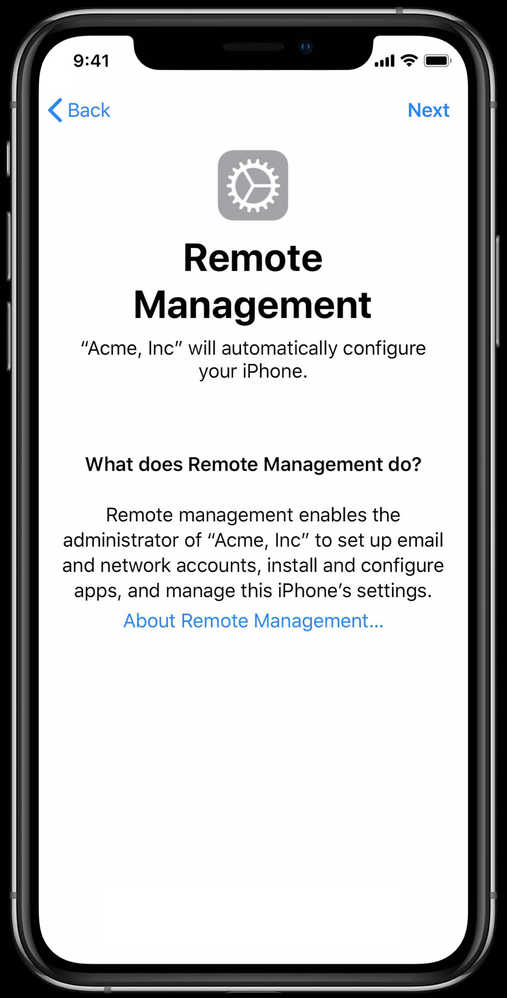
SUPERVISED




User Enrollment




Device Enrollment




Automated Device Enrollment

SUPERVISED

# User Enrollment

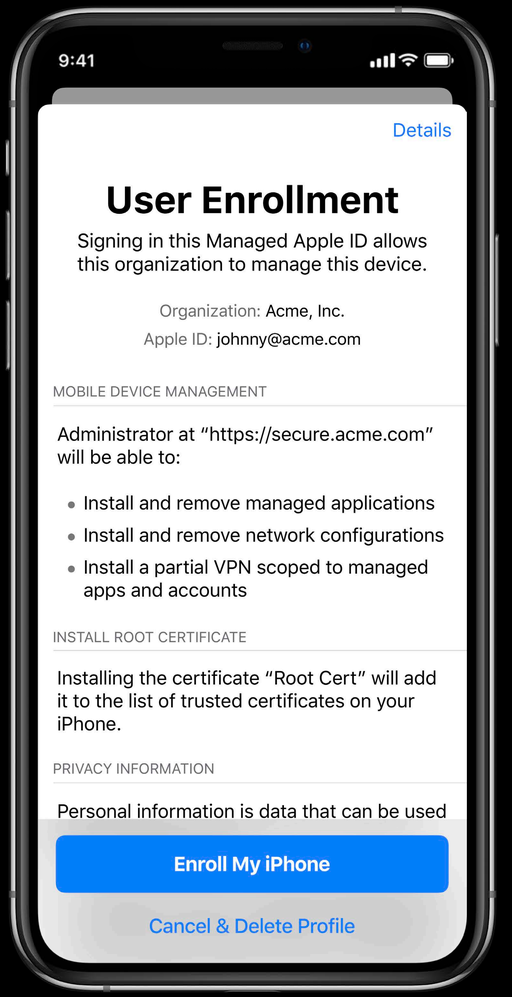
NEW

New MDM enrollment option

Better balance for BYOD

Protects privacy of personal data

Secures corporate data



Managed
Apple ID

Data
Separation

Management
Capabilities

# User Enrollment and Apple IDs

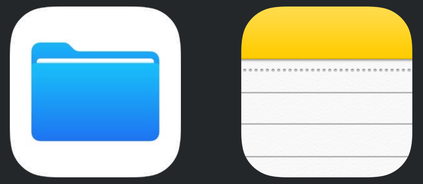
Managed Apple ID required

Apps and accounts use correct Apple ID

Unenrolling removes Managed Apple ID

Apple Services

Managed Apple ID



Data Separation

Personal Apple ID





# Data Separation

Managed APFS volume created during user enrollment

Unenrolling destroys the volume and its cryptographic keys

# How is data separated?

Managed APFS volume contains managed:

- App containers
- Notes
- iCloud Drive documents
- Keychain
- Mail attachments and full email bodies
- Calendar attachments





```
// Enrollment profile

<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadType</key>
            <string>com.apple.mdm</string>
            <key>ManagedAppleID</key>
            <string>RickW@example.com</string>
            <key>PayloadOrganization</key>
            <string>Example, Inc.</string>
            <key>CheckInURL</key>
            <string>https://mdm.example.com:2001/checkin</string>
            <key>ServerURL</key>
            <string>https://mdm.example.com:2001/mdm</string>
            <key>CheckOutWhenRemoved</key>
            <true/>
            <key>IdentityCertificateUUID</key>
```

NEW

```
// Enrollment profile

<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadType</key>
            <string>com.apple.mdm</string>
            <key>ManagedAppleID</key>
            <string>RickW@example.com</string>
            <key>PayloadOrganization</key>
            <string>Example, Inc.</string>
            <key>CheckInURL</key>
            <string>https://mdm.example.com:2001/checkin</string>
            <key>ServerURL</key>
            <string>https://mdm.example.com:2001/mdm</string>
            <key>CheckOutWhenRemoved</key>
            <true/>
            <key>IdentityCertificateUUID</key>
```

NEW

```
// Enrollment profile

<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadType</key>
            <string>com.apple.mdm</string>
            <key>ManagedAppleID</key>
            <string>RickW@example.com</string>
            <key>PayloadOrganization</key>
            <string>Example, Inc.</string>
            <key>CheckInURL</key>
            <string>https://mdm.example.com:2001/checkin</string>
            <key>ServerURL</key>
            <string>https://mdm.example.com:2001/mdm</string>
            <key>CheckOutWhenRemoved</key>
            <true/>
            <key>IdentityCertificateUUID</key>
```

NEW

# User Enrollment — Protocol

- ✕ Profile Service Profiles
- ~ UDID or other persistent device identifiers
  - EnrollmentID
  - EASDeviceIdentifier
- ✕ Unlock Token in TokenUpdate

# User Enrollment — Commands

- EraseDevice, ActiveSync RemoteWipe
- Managed results only:

```
InstalledApplicationList
CertificateList ProfileList
ProvisioningProfileList
```

# User Enrollment — Commands

- ~ `InstallApplication`
  - App is always removed on unenroll
  - Enterprise app distribution or user-based VPP with `PurchaseMethod` 1
- × Commands related to cellular

# User Enrollment — Payloads

- Per-app VPN
  - `MailDomains`, `ContactsDomains`, `CalendarDomains`
- Passcode - 6 digit, non-simple
- Wi-Fi - use WPAD for proxying
- Defaults, Logging not supported

# User Enrollment — Restrictions

Limited set of restrictions

- Managed Open In, allowLockScreen*, forceEncryptedBackup
- Any supervised restriction
- ratings*, allowCloud*

# *Demo*

## User Enrollment

Huiyuan Ren, Device Management Engineer

# User Enrollment — macOS

User Enrollment with Managed Apple ID

Managed APFS volume

Notes data separation

Management capabilities similar

# It's time to evolve BYOD.

# Certificate Transparency

iOS, macOS, tvOS, and watchOS

Security enhancement

Opt out sensitive certificates or domains

New payload

Multiple payloads unioned together

# WPA3

iOS, macOS, and tvOS

NEW

Wi-Fi payload supports WPA3 security type

- Personal
- Enterprise

# Apple Push Notification Service

Support for token-based authentication

# Device Enrollment Settings

iOS, macOS, and tvOS

NEW

Now always

- Supervised
- Mandatory

allow_pairing deprecated

Use configuration profile restriction

# Apple Remote Desktop

macOS

Enable and disable via MDM

Sets Remote Management to All Users

Enables options

- observe
- control
- show observe

# Manage SecureTokens

macOS

NEW

Allow mobile accounts to boot FileVault system

MDM Server manages bootstrap token

Used to generate SecureToken when user signs in

# Privacy Policy

macOS

NEW

Enable key loggers

Enable screen recording

Whitelist non-notarized internal apps

# FileVault

macOS

NEW

- Now requires user-approved MDM enrollment
- Can’t pass username/password auth to fdesetup
- Changes may break scripts or MDM agents

# Activation Lock

macOS

NEW

Clear Activation Lock via MDM

Same endpoint and API as iOS

MDM server APIs available soon

Service available later this summer

# Deprecations

## macOS

NEW

Non-UI profile installation

Parental Controls Application Access

User-channel-only enrollments

# Deprecated Unsupervised Restrictions

iOS

NEW

For transition period

- Remain in effect after upgrade
- Not honored after backup and restore

MDM servers

- Don’t install on unsupervised devices
- Don’t assume they will take effect

# Unlock Token

iOS

NEW

Available only in first token update after enrollment

- Remember it and don't count on getting one later

Also affects Apple Configurator

- Only available before passcode is set

# Balance values

Same tools for all

Balance values

Fits in and stands out

# Fits in and stands out

# Single Sign-On

Matt Chanda, Consulting Engineer

# Too Many Methods, Too Many Places

OpenID Connect

Kerberos

Smart Cards

Cloud

WS-Fed

2FA

SAML

PKINIT

OAuth

Federation

# Why Single Sign-On?

Suite of apps and web sites

Improved user experience

No passwords

Trust score data

# What is Single Sign-On?

NEW

iOS and macOS

Native apps and Safari

MDM managed

UI can be native, web, or silent


Single Sign-On
Sign In with Apple

# Single Sign-On Components

Apps and Web Sites

Single Sign-On
Extension

Identity Provider

# Single Sign-On Components

Apps and Web Sites

Single Sign-On
Extension

Identity Provider

Redirect

Credential

Redirect

Credential

# Redirect Extensions

Modern authentication

OpenID Connect, OAuth, or SAML2

HTTP based

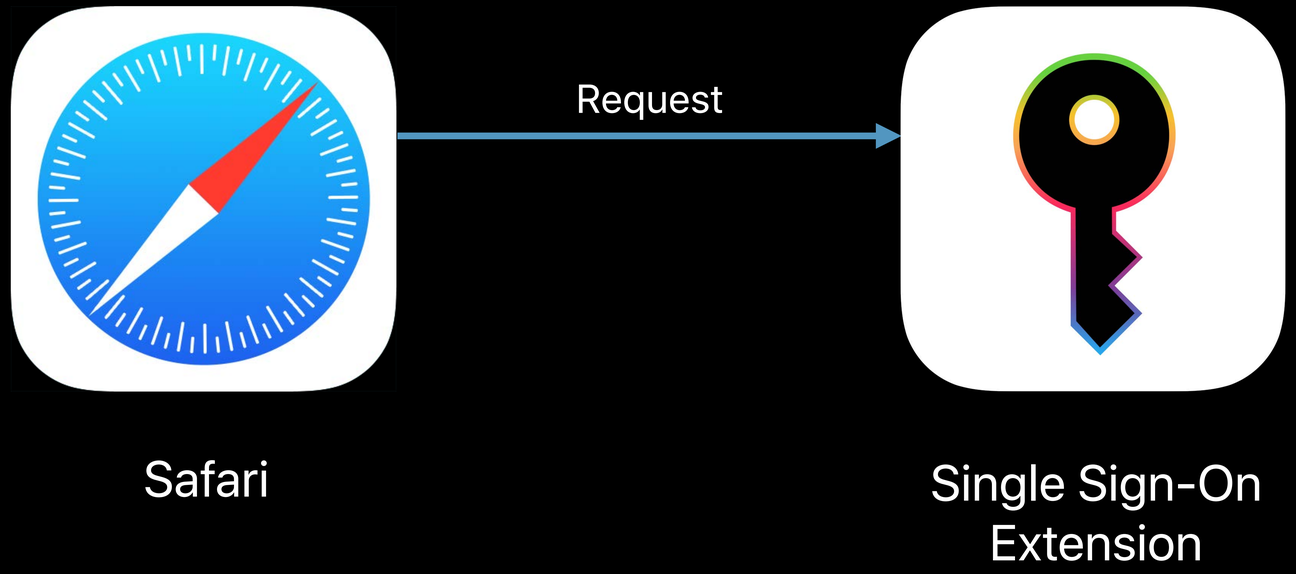
Federation

# Safari — Redirect Extension

# Safari — Redirect Extension

Safari

# Safari — Redirect Extension



# Safari — Redirect Extension

Safari

Single Sign-On Extension

Identity Provider

# Safari — Redirect Extension

Safari

Single Sign-On Extension

Identity Provider

# Safari — Redirect Extension

# Safari — Redirect Extension

Safari

Single Sign-On
Extension

Identity
Provider

# What Can Extensions Do?

Native screen

Multifactors

SEP generated keys

Trust score data

Federated auth

WebAuthN

# Native App — Redirect

Native Apps can send operations

Better fit into the app flow

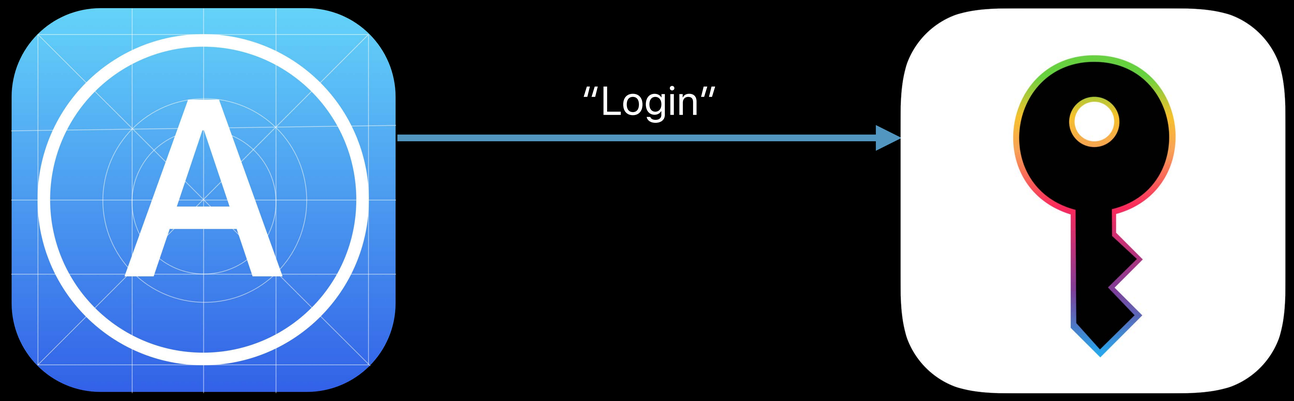
Authentication library not needed

# Native — Redirect Extension

# Native — Redirect Extension

Native App

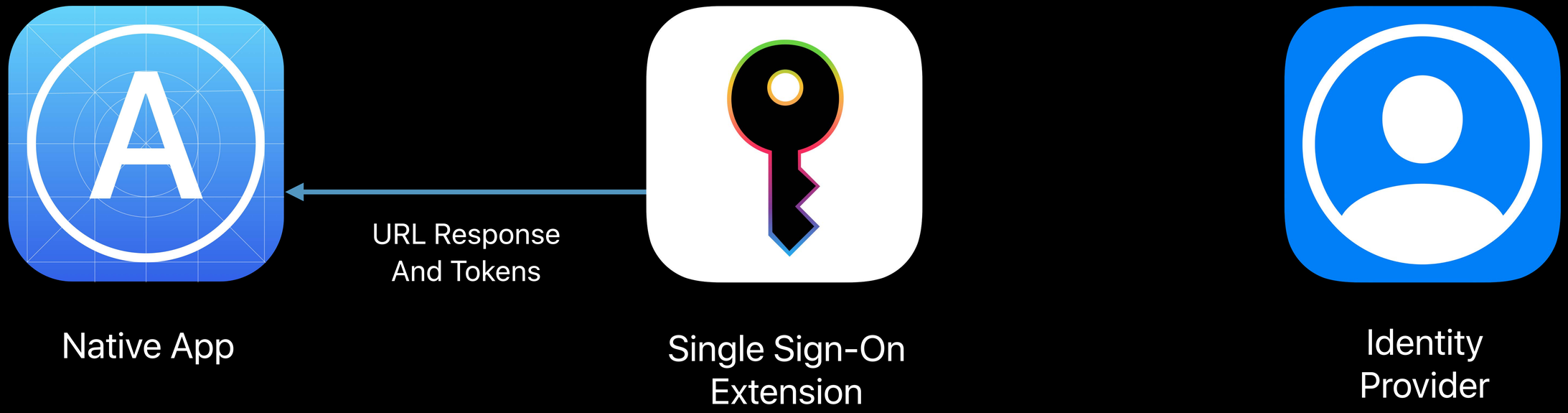
# Native — Redirect Extension



# Native — Redirect Extension

# Native — Redirect Extension

# Native — Redirect Extension



# Native — Redirect Extension

Native App

Single Sign-On
Extension

Identity
Provider

NEW

```
//Extensible SSO Profile

<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
```

NEW

```
//Extensible SSO Profile

<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
```

```
<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
```

NEW

```
<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
```

NEW

```
<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
```

NEW

```
<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
```

NEW

```
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
</dict>
```

NEW

```
        <key>ExtensionIdentifier</key>
        <string>com.example.sso.redirect</string>
        <key>TeamIdentifier</key>
        <string>4JMSJJRMAD</string>
        <key>Type</key>
        <string>Redirect</string>
        <key>URLs</key>
        <array>
            <string>https://auth.example.com/connect/authorize</string>
            <string>https://auth.example.com/connect/token</string>
        </array>
        <key>ExtensionData</key>
        <dict>
            <key>UserName</key>
            <string>john.appleseed@example.com</string>
        </dict>
    </dict>
</dict>
</dict>
```

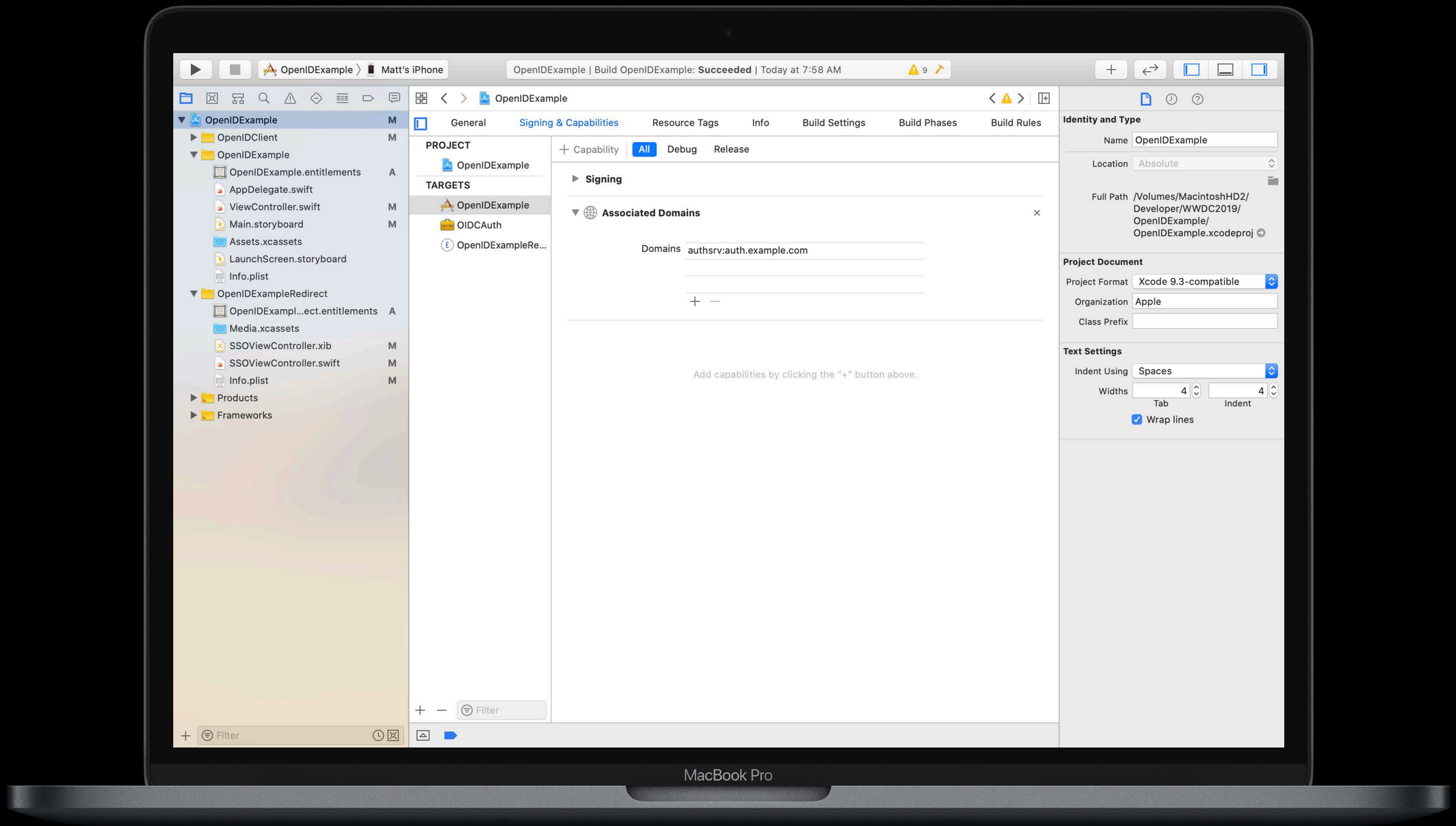
NEW

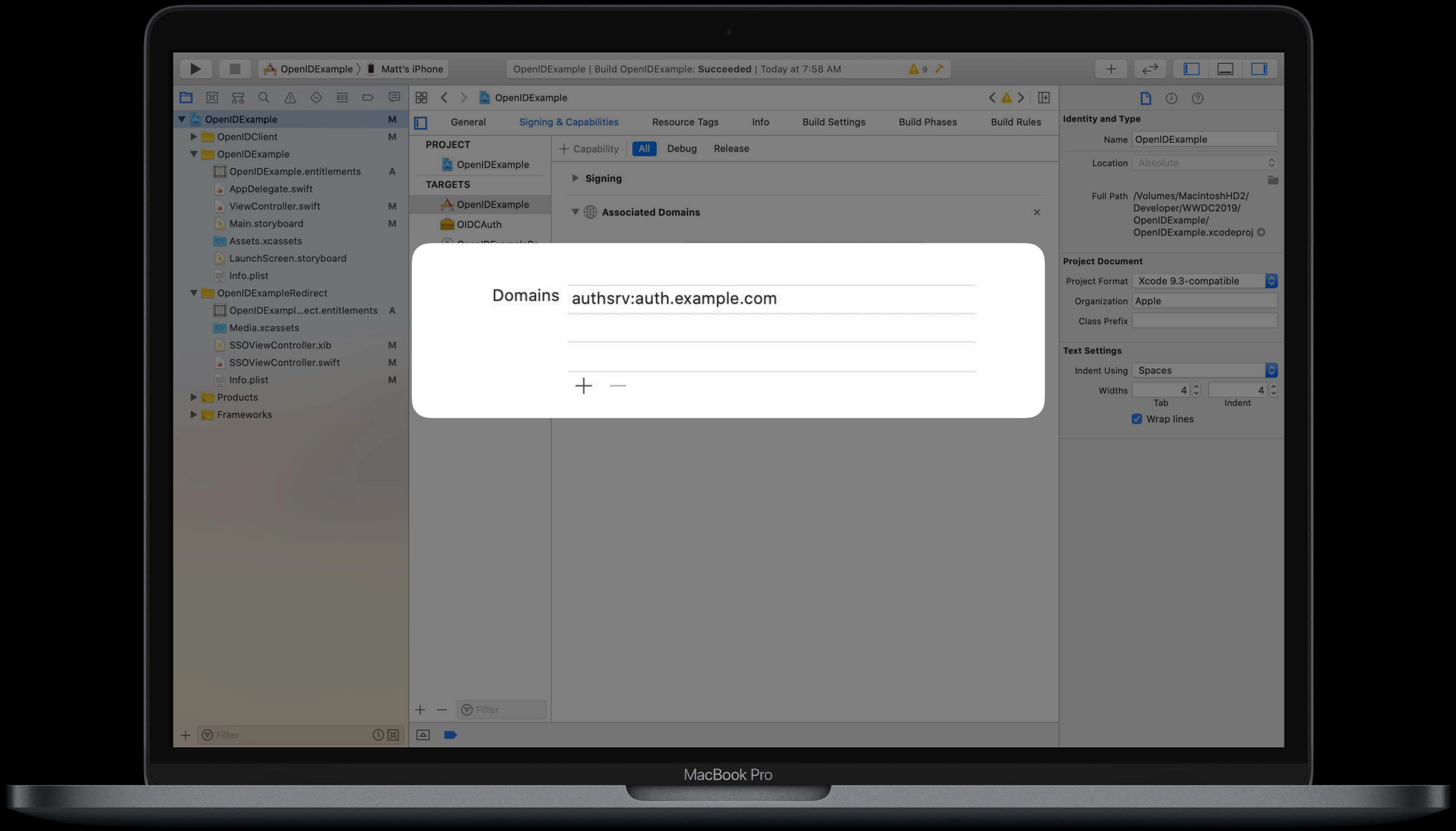
```
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMAD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
  </dict>
</dict>
</dict>
```

NEW

```
        <key>ExtensionIdentifier</key>
        <string>com.example.sso.redirect</string>
        <key>TeamIdentifier</key>
        <string>4JMSJJRMAD</string>
        <key>Type</key>
        <string>Redirect</string>
        <key>URLs</key>
        <array>
            <string>https://auth.example.com/connect/authorize</string>
            <string>https://auth.example.com/connect/token</string>
        </array>
        <key>ExtensionData</key>
        <dict>
            <key>UserName</key>
            <string>john.appleseed@example.com</string>
        </dict>
    </dict>
</dict>
</dict>
```

NEW


OpenIDExample 〉 Matt's iPhone
OpenIDExample | Build OpenIDExample: Succeeded | Today at 7:58 AM
OpenIDExample
OpenIDExample M
OpenIDClient M
OpenIDExample
OpenIDExample.entitlements A
AppDelegate.swift
ViewController.swift M
Main.storyboard M
Assets.xcassets
LaunchScreen.storyboard
Info.plist
OpenIDExampleRedirect
OpenIDExampl...ect.entitlements A
Media.xcassets
SSOViewController.xib M
SSOViewController.swift M
Info.plist M
Products
Frameworks
Filter
General
Signing & Capabilities
Resource Tags
Info
Build Settings
Build Phases
Build Rules
PROJECT
OpenIDExample
TARGETS
OpenIDExample
OIDCAuth
OpenIDExampleRe...
Capability
All
Debug
Release
Signing
Associated Domains
Domains
authsrv:auth.example.com
Add capabilities by clicking the "+" button above.
Filter
Identity and Type
Name
OpenIDExample
Location
Absolute
Full Path
/Volumes/MacintoshHD2/
Developer/WWDC2019/
OpenIDExample/
OpenIDExample.xcodeproj
Project Document
Project Format
Xcode 9.3-compatible
Organization
Apple
Class Prefix
Text Settings
Indent Using
Spaces
Widths
4
Tab
4
Indent
Wrap lines
MacBook Pro


OpenIDExample 〉 Matt's iPhone
OpenIDExample | Build OpenIDExample: Succeeded | Today at 7:58 AM
OpenIDExample
General
Signing & Capabilities
Resource Tags
Info
Build Settings
Build Phases
Build Rules
PROJECT
OpenIDExample
TARGETS
OpenIDExample
OIDCAuth
Capability
All
Debug
Release
Signing
Associated Domains
Domains
authsrv:auth.example.com
Identity and Type
Name
OpenIDExample
Location
Absolute
Full Path
/Volumes/MacintoshHD2/Developer/WWDC2019/OpenIDExample/OpenIDExample.xcodeproj
Project Document
Project Format
Xcode 9.3-compatible
Organization
Apple
Class Prefix
Text Settings
Indent Using
Spaces
Widths
Tab
Indent
Wrap lines
OpenIDExample
OpenIDClient
OpenIDExample
OpenIDExample.entitlements
AppDelegate.swift
ViewController.swift
Main.storyboard
Assets.xcassets
LaunchScreen.storyboard
Info.plist
OpenIDExampleRedirect
Media.xcassets
SSOViewController.xib
SSOViewController.swift
Info.plist
Products
Frameworks
Filter
MacBook Pro

# Security and Privacy

## Associated domains

Requires Site Association File on Server

- auth.example.com/.well-known/apple-app-site-association

```
{
    "authsrv": {
        "apps": [ "4JMSJJRMAD.com.example.sso" ]
     }
}
```

# Security and Privacy

NEW

Use managed associated domains on macOS

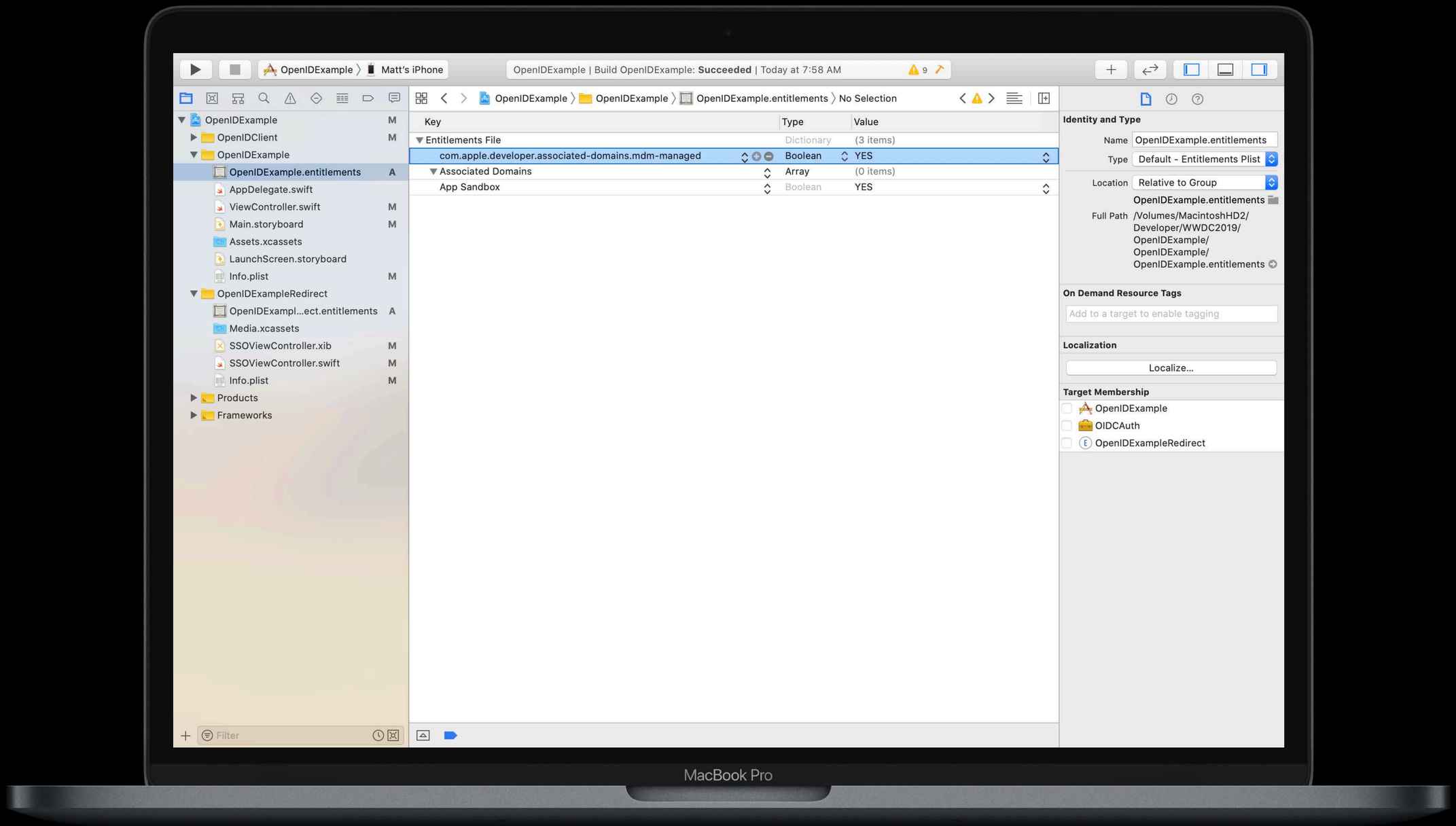
```
<key>ApplicationIdentifier</key>
<string>4JMSJJRMAD.com.example.sso</string>
<key>AssociatedDomains</key>
<array>
    <string>authserv:auth.example.com</string>
</array>
```

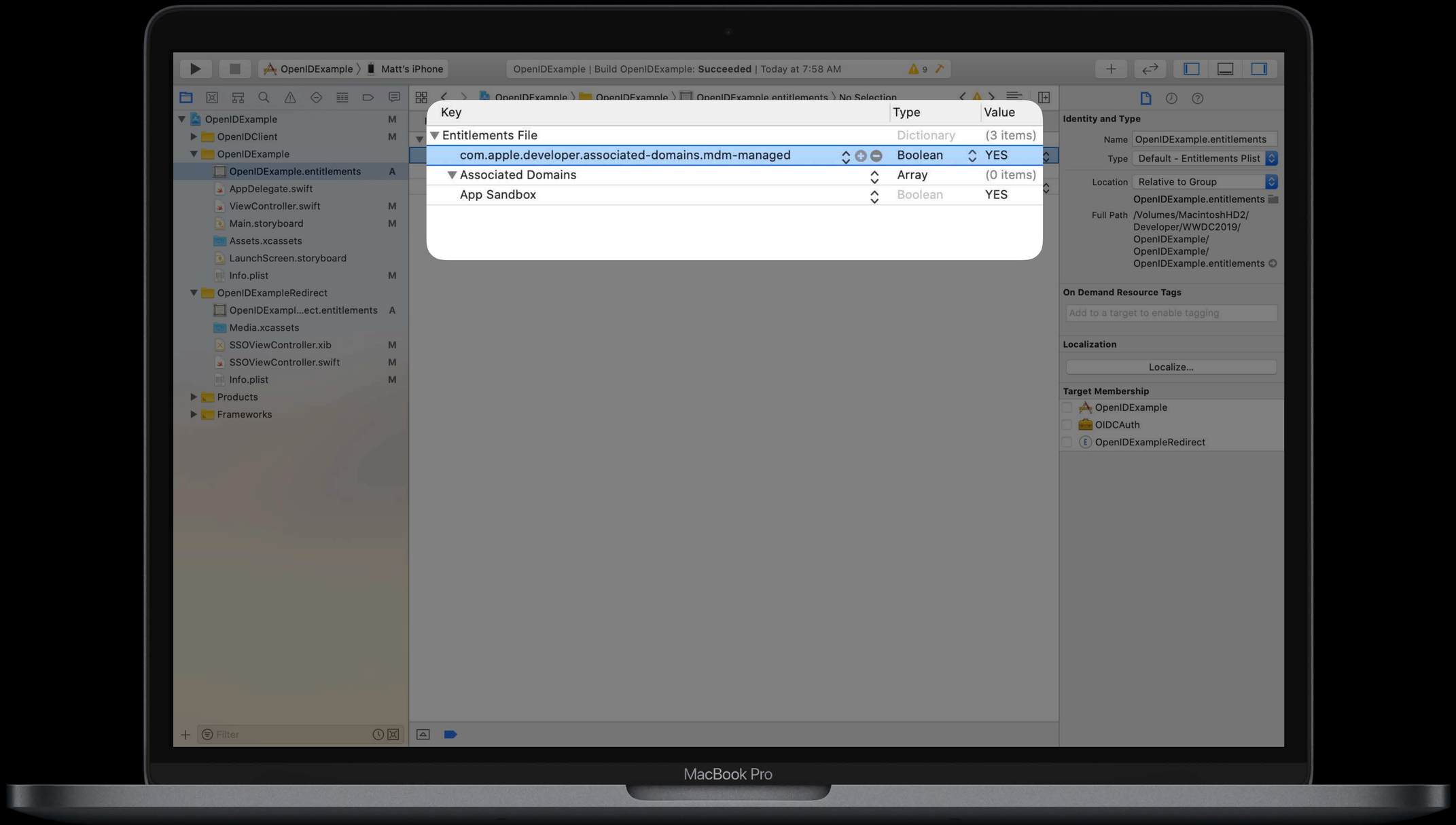
# Security and Privacy

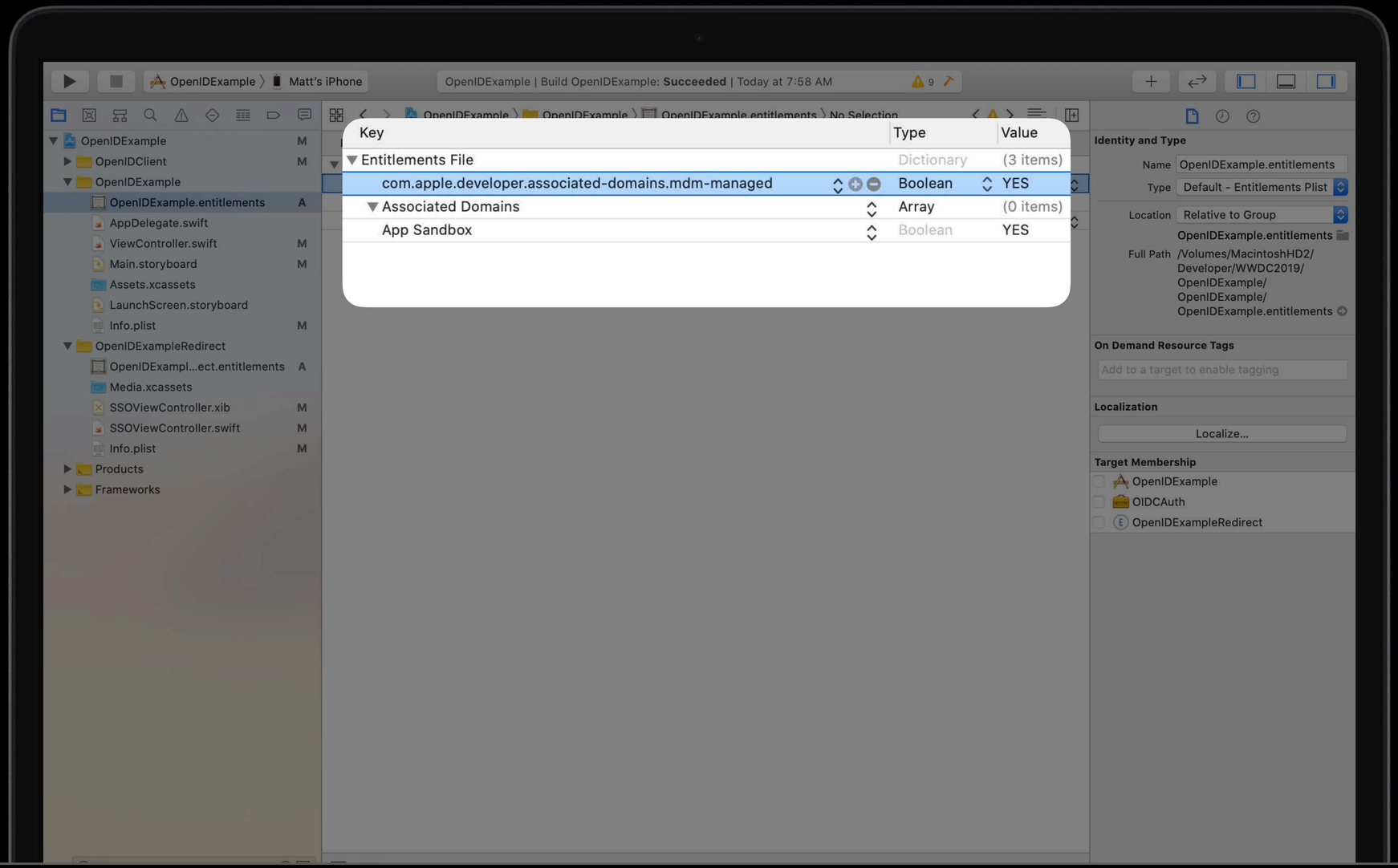
NEW

Use managed ApplicationAttributes on iOS

```
<key>AssociatedDomains</key>
<array>
    <string>authserv:auth.example.com</string>
</array>
```


OpenIDExample 〉 Matt's iPhone
OpenIDExample | Build OpenIDExample: Succeeded | Today at 7:58 AM
OpenIDExample 〉 OpenIDExample 〉 OpenIDExample.entitlements 〉 No Selection
OpenIDExample M
OpenIDClient M
OpenIDExample
OpenIDExample.entitlements A
AppDelegate.swift
ViewController.swift M
Main.storyboard M
Assets.xcassets
LaunchScreen.storyboard
Info.plist M
OpenIDExampleRedirect
OpenIDExampl...ect.entitlements A
Media.xcassets
SSOViewController.xib M
SSOViewController.swift M
Info.plist M
Products
Frameworks
Filter
Key
Type
Value
Entitlements File
Dictionary
(3 items)
com.apple.developer.associated-domains.mdm-managed
Boolean
YES
Associated Domains
Array
(0 items)
App Sandbox
Boolean
YES
Identity and Type
Name
OpenIDExample.entitlements
Type
Default - Entitlements Plist
Location
Relative to Group
OpenIDExample.entitlements
Full Path
/Volumes/MacintoshHD2/
Developer/WWDC2019/
OpenIDExample/
OpenIDExample/
OpenIDExample.entitlements
On Demand Resource Tags
Add to a target to enable tagging
Localization
Localize...
Target Membership
OpenIDExample
OIDCAuth
OpenIDExampleRedirect
MacBook Pro


OpenIDExample 〉 Matt's iPhone
OpenIDExample | Build OpenIDExample: Succeeded | Today at 7:58 AM
OpenIDExample
OpenIDClient
OpenIDExample
OpenIDExample.entitlements
AppDelegate.swift
ViewController.swift
Main.storyboard
Assets.xcassets
LaunchScreen.storyboard
Info.plist
OpenIDExampleRedirect
OpenIDExampl...ect.entitlements
Media.xcassets
SSOViewController.xib
SSOViewController.swift
Info.plist
Products
Frameworks
Filter
Key
Type
Value
Entitlements File
Dictionary
(3 items)
com.apple.developer.associated-domains.mdm-managed
Boolean
YES
Associated Domains
Array
(0 items)
App Sandbox
Boolean
YES
Identity and Type
Name
OpenIDExample.entitlements
Type
Default - Entitlements Plist
Location
Relative to Group
OpenIDExample.entitlements
Full Path
/Volumes/MacintoshHD2/
Developer/WWDC2019/
OpenIDExample/
OpenIDExample/
OpenIDExample.entitlements
On Demand Resource Tags
Add to a target to enable tagging
Localization
Localize...
Target Membership
OpenIDExample
OIDCAuth
OpenIDExampleRedirect
MacBook Pro


OpenIDExample 〉 Matt's iPhone
OpenIDExample | Build OpenIDExample: Succeeded | Today at 7:58 AM
OpenIDExample
OpenIDClient
OpenIDExample
OpenIDExample.entitlements
AppDelegate.swift
ViewController.swift
Main.storyboard
Assets.xcassets
LaunchScreen.storyboard
Info.plist
OpenIDExampleRedirect
OpenIDExampl...ect.entitlements
Media.xcassets
SSOViewController.xib
SSOViewController.swift
Info.plist
Products
Frameworks
Key
Type
Value
Entitlements File
Dictionary
(3 items)
com.apple.developer.associated-domains.mdm-managed
Boolean
YES
Associated Domains
Array
(0 items)
App Sandbox
Boolean
YES
Identity and Type
Name
OpenIDExample.entitlements
Type
Default - Entitlements Plist
Location
Relative to Group
OpenIDExample.entitlements
Full Path
/Volumes/MacintoshHD2/
Developer/WWDC2019/
OpenIDExample/
OpenIDExample/
OpenIDExample.entitlements
On Demand Resource Tags
Add to a target to enable tagging
Localization
Localize...
Target Membership
OpenIDExample
OIDCAuth
OpenIDExampleRedirect

Redirect

Credential

Redirect

Credential

# Credential Extensions

Challenge/response authentication

Kerberos

Custom challenges

# Credential Extensions

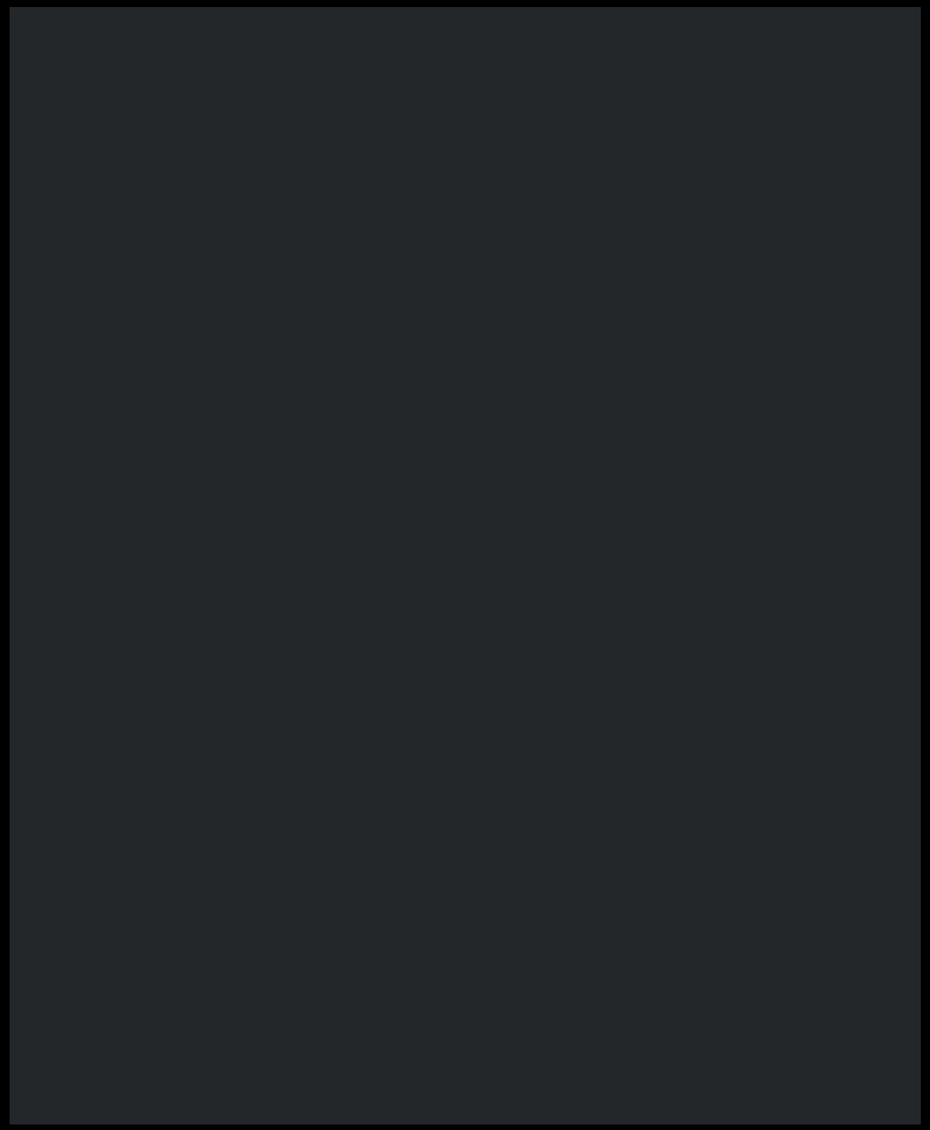
HTTP challenge

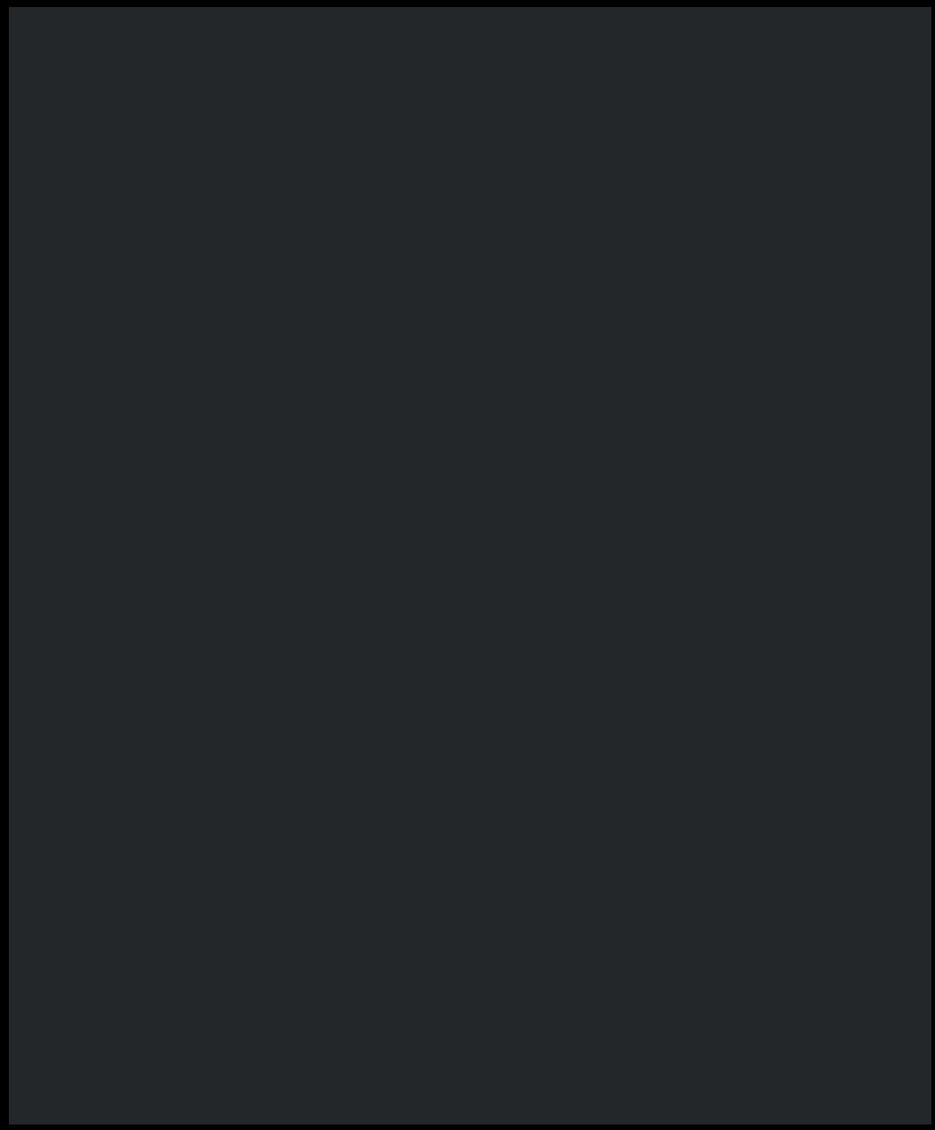
Hosts or host suffixes

Operations are supported

No associated domains

# Any App — Credential Extension

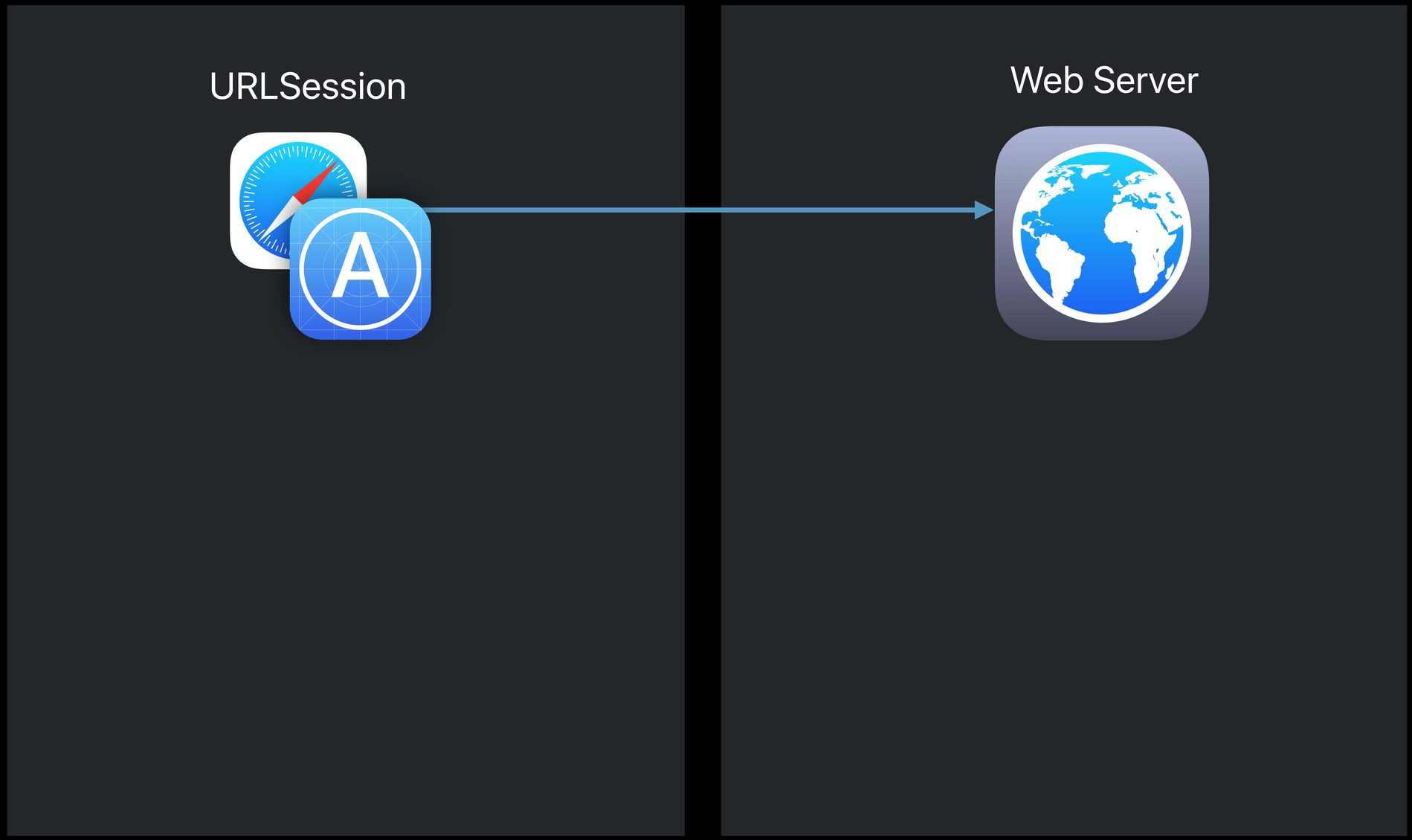




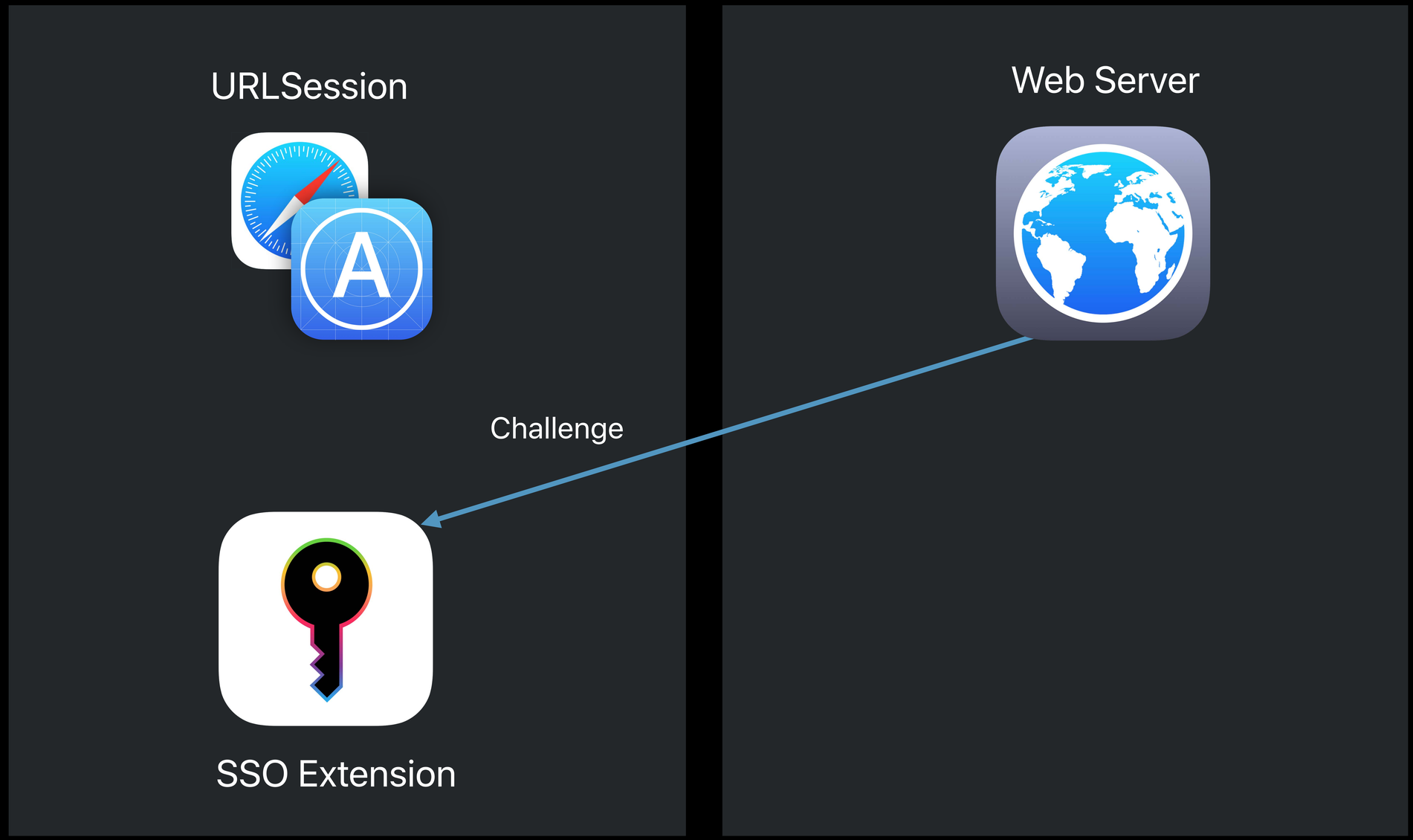
# Any App — Credential Extension

URLSession

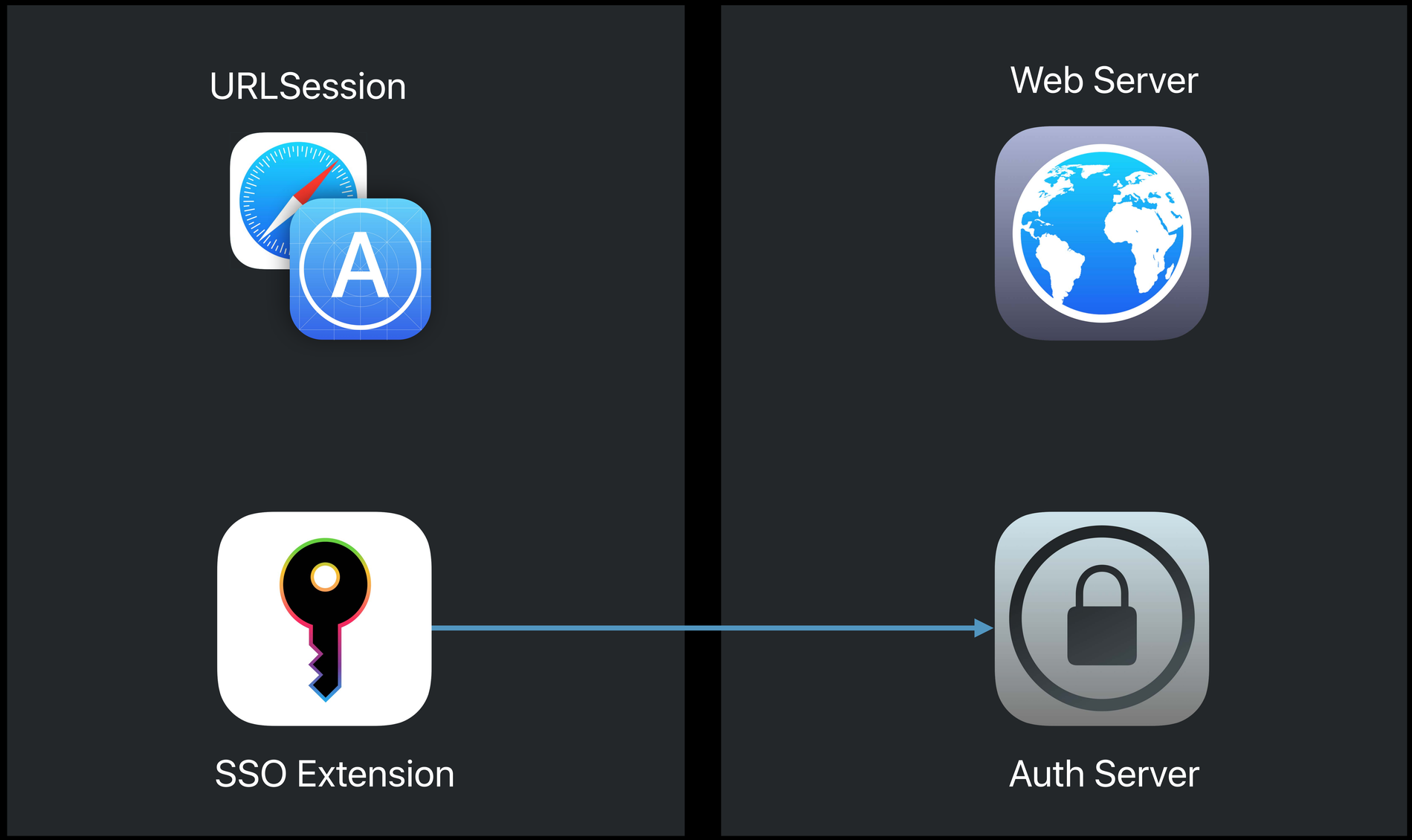
# Any App — Credential Extension



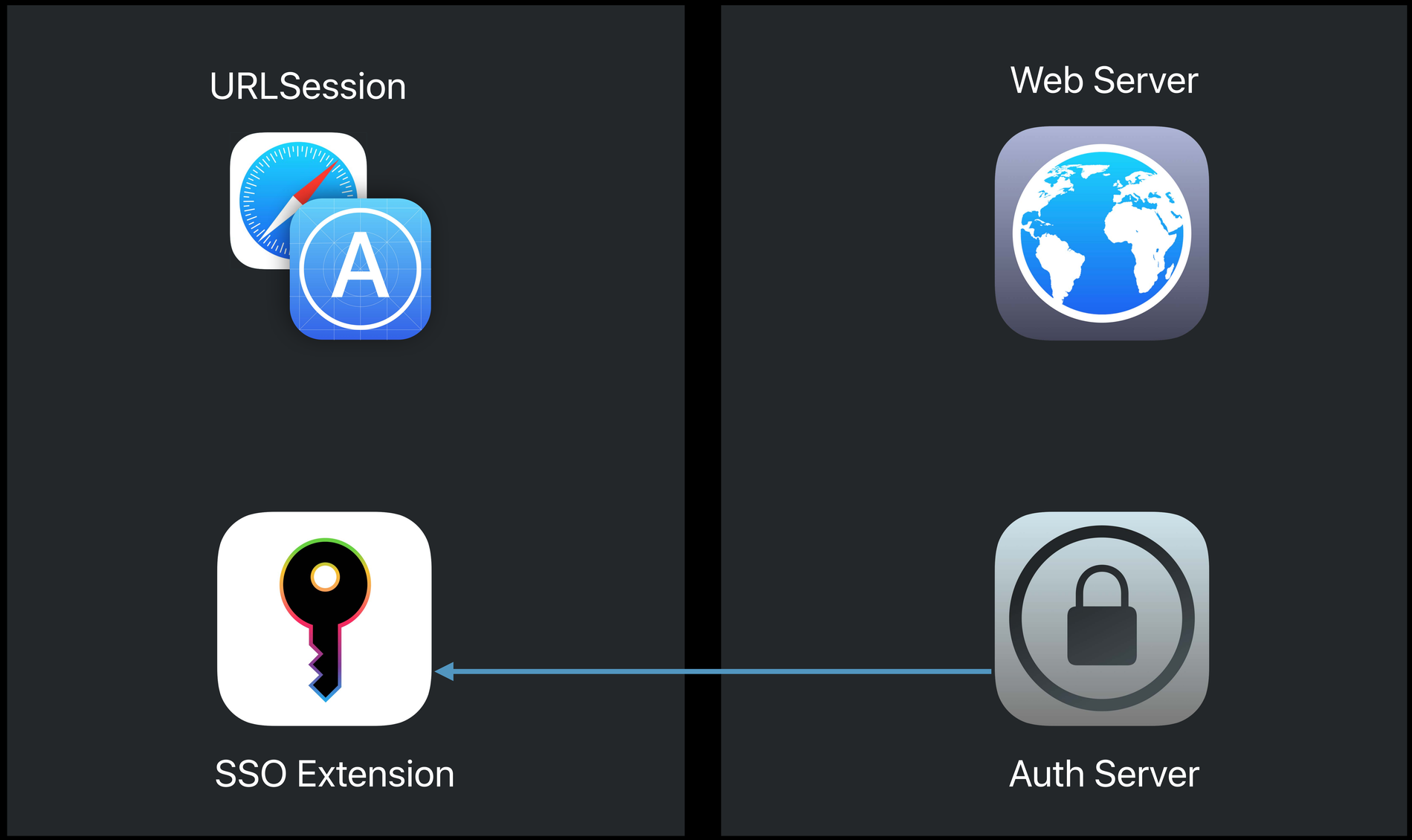
# Any App — Credential Extension



# Any App — Credential Extension

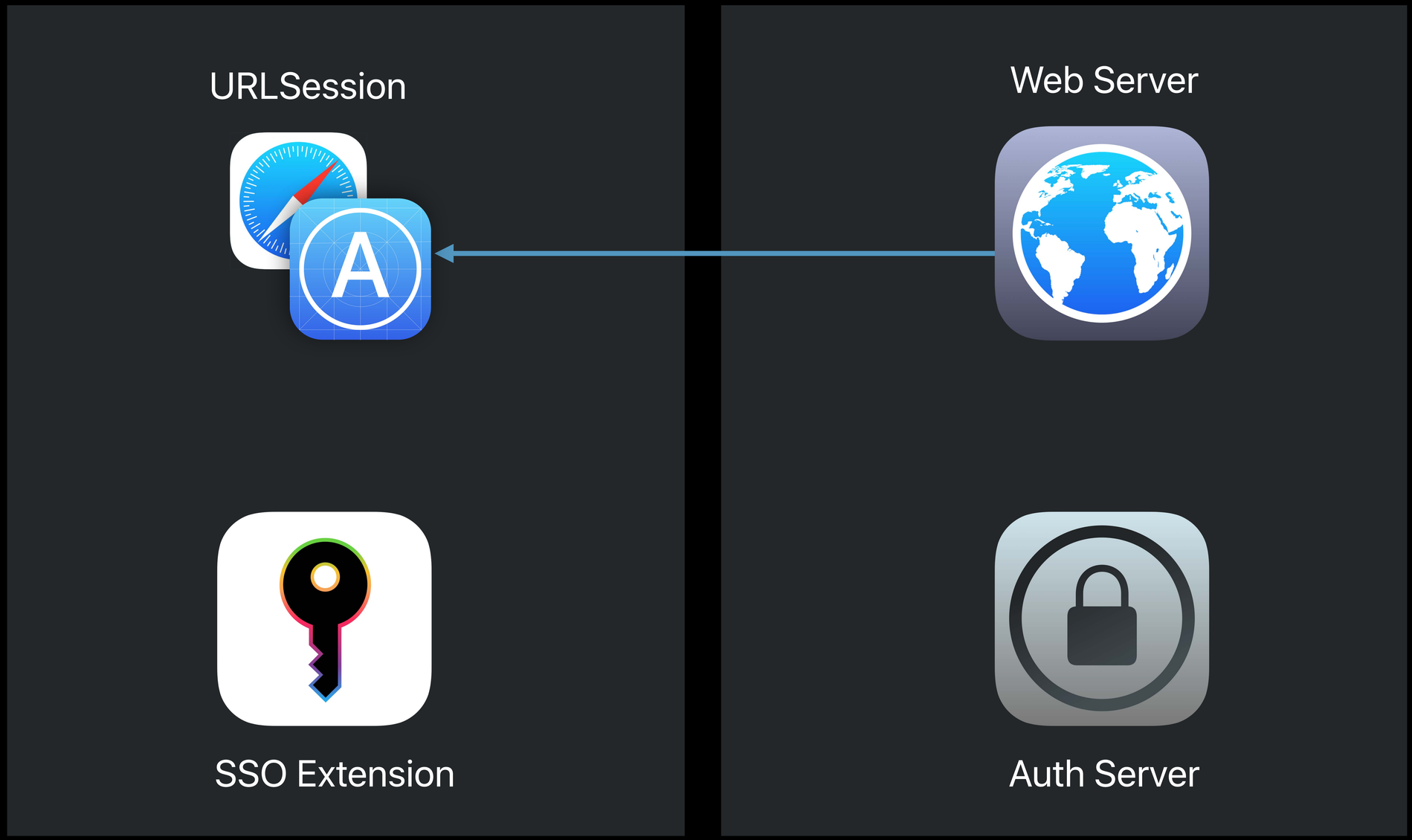


# Any App — Credential Extension



# Any App — Credential Extension

# Any App — Credential Extension



# *Demo*

## Credential mode extension

Rick Lemmon, Services Consulting Engineer

# Kerberos Extension

NEW

Included with macOS Catalina and iOS 13

Provides Active Directory password management and local password sync

Smart card and certificate-based authentication support

Redirect

Credential

Redirect

Credential

# Single Sign-On

## Summary

Enables Single Sign-On for apps and web sites

macOS and iOS

Two types available

Let’s see what you do with them!

Watch Single Sign-On video for more details

# Associated Domains

Can manage via MDM

Not just for Single Sign-On!

Other service types supported

# Associated Domains

Can manage via MDM

Not just for Single Sign-On!

Other service types supported

# Federated Authentication

Supports Microsoft Azure Active Directory

Managed Apple ID coming to ABM

User Enrollment requires Managed Apple ID

# Enrollment Customization

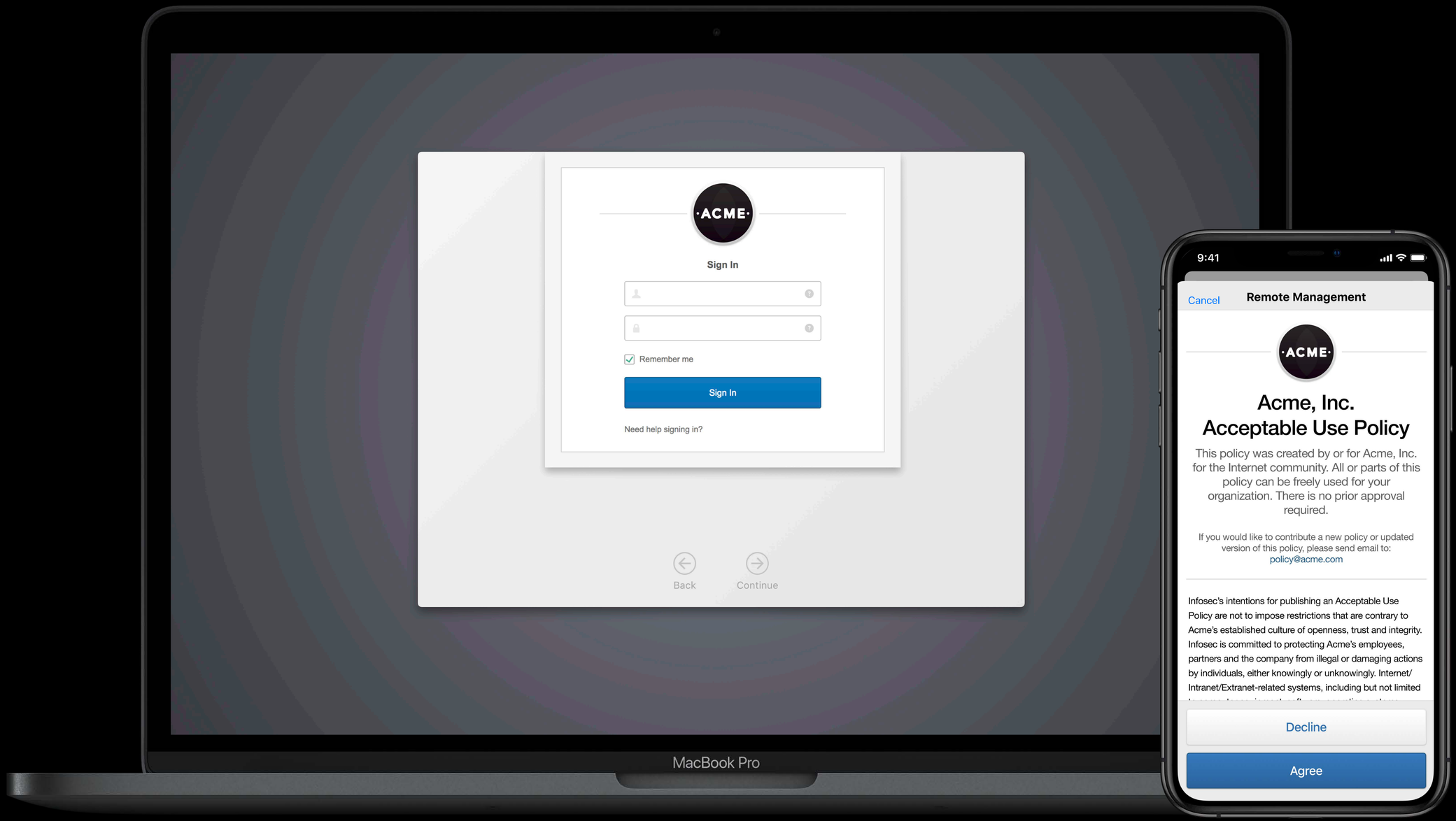
NEW

Provide custom web UI for enrollment

Use for

- Authentication
- Branding
- Consent text
- Privacy policy


Remote Management
Remote management enables the administrator of "Acme, Inc" to set up email and network accounts, install and configure apps, and manage this computer's settings.
"Acme, Inc" can automatically configure your computer.
Learn more about remote management
Back
Continue
MacBook Pro
9:41
Back
Next
Remote Management
"Acme, Inc" will automatically configure your iPhone.
What does Remote Management do?
Remote management enables the administrator of "Acme, Inc" to set up email and network accounts, install and configure apps, and manage this iPhone's settings.
About Remote Management...


·ACME·
Sign In
Remember me
Sign In
Need help signing in?
Back
Continue
MacBook Pro
9:41
Cancel
Remote Management
·ACME·
Acme, Inc.
Acceptable Use Policy
This policy was created by or for Acme, Inc. for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required.
If you would like to contribute a new policy or updated version of this policy, please send email to:
policy@acme.com
Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Acme's established culture of openness, trust and integrity. Infosec is committed to protecting Acme's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/ Intranet/Extranet-related systems, including but not limited
Decline
Agree

# Content Caching

NEW

Configure for best effort vs infrastructure

Tell devices to prefer specific content caches

# Setup Assistant
## iOS

NEW

Skip Dark Mode pane in Setup Assistant

Skip Welcome pane in Setup Assistant

# Setup Assistant
## macOS

NEW

Skip Screen Time pane after enrollment

Skip Screen Time or Touch ID pane in Setup Assistant payload

# Exchange ActiveSync
## iOS

NEW

Enable Mail, Calendar, Contacts, and Reminders individually for managed accounts

# Supervised-Only Restrictions
## iOS

NEW

Allow Hotspot Modification

Allow Find My Devices

Allow Find My Friends

Allow QuickPath keyboard

Allow Wi-Fi modification

# Supervised-Only Restriction
## tvOS

NEW

Have Apple TV always ready to AirPlay

Allow Device Sleep

# TargetDeviceType
## iOS, macOS, tvOS, and watchOS

Avoids iOS destination prompt

Target type must match device type

# Documentation

# Documentation

Import new keys and values from code

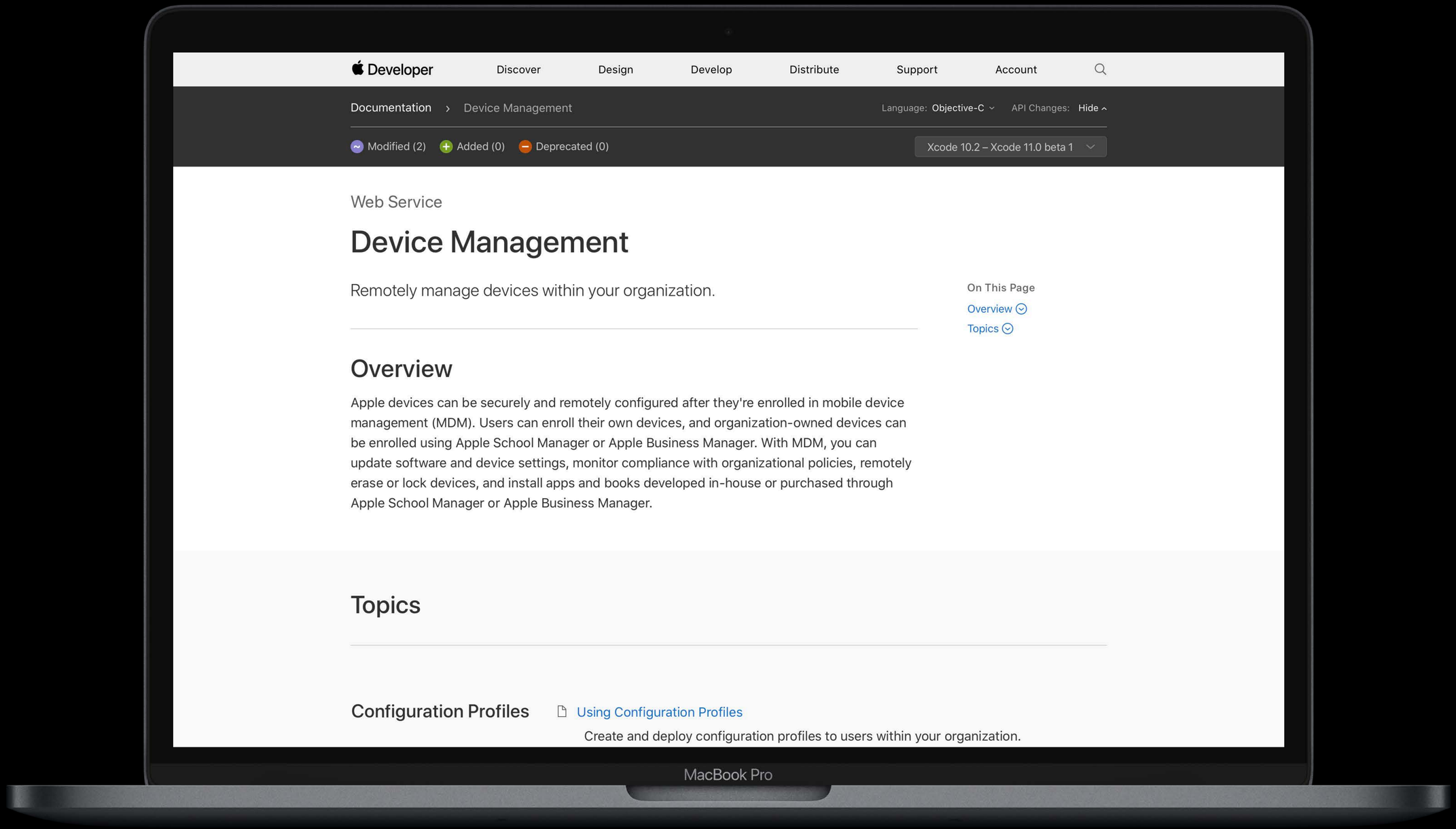
Format matches developer documentation

Highlight changes in OS releases

# *Demo*

## Device Management Documentation

Graham McLuhan, Device Management Engineer


Developer
Discover
Design
Develop
Distribute
Support
Account
Documentation
Device Management
Language: Objective-C
API Changes: Hide
Modified (2)
Added (0)
Deprecated (0)
Xcode 10.2 – Xcode 11.0 beta 1
Web Service
Device Management
Remotely manage devices within your organization.
On This Page
Overview
Topics
Overview
Apple devices can be securely and remotely configured after they're enrolled in mobile device management (MDM). Users can enroll their own devices, and organization-owned devices can be enrolled using Apple School Manager or Apple Business Manager. With MDM, you can update software and device settings, monitor compliance with organizational policies, remotely erase or lock devices, and install apps and books developed in-house or purchased through Apple School Manager or Apple Business Manager.
Topics
Configuration Profiles
Using Configuration Profiles
Create and deploy configuration profiles to users within your organization.
MacBook Pro

# Summary

Support Single Sign-On and Data Separation

Enable enrollment customization

Support new payloads and restrictions

Don’t rely on UserAgent

Handle newly supervised-only restrictions

# More Information

developer.apple.com/wwdc19/303

| | |
|---|---|
| Device Management Lab | Friday, 1:00 |
| What's New in Universal Links | WWDC 2019 |
| Introducing Desktop-Class Browsing on iPad | WWDC 2019 |


WWDC19