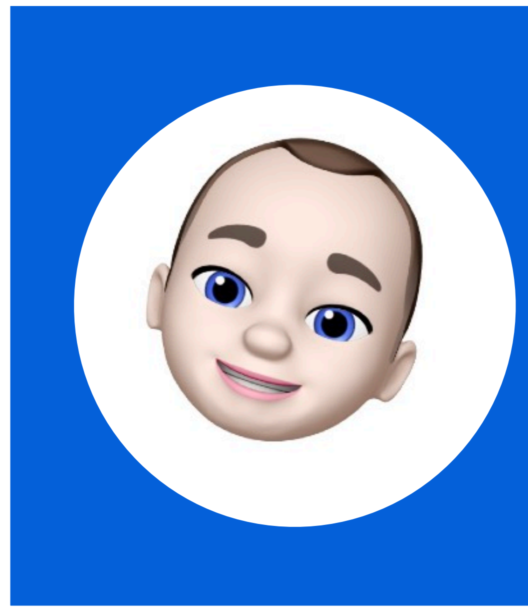
Jamf & Microsoft:

Safe Internet & SSO Extension

JAMF
NATION
LIVE



Scott Mackay

Systems Engineer

Agenda

1 | What is SSO?

Breakdown what SSO is and the benefits it can bring

2 | Setup SSO

Best practice and how to setup SSO

3 | Workflows

Jamf workflows to best utilise SSO

4 | Points of Note and Recommendations

Some gotchas, points to watch out for and resources

What is **SSO?**

SSO = Single Sign On

Or

No more passwords*

maybe

🏫

Standard

=

always needing to
unlock or enter a password

🏡

SSO

=

Authenticate once and done.

What is **SSO?**

SSO = Single Sign On

Or

~~No more passwords~~

What is **SSO?**

SSO = Single Sign On

Or

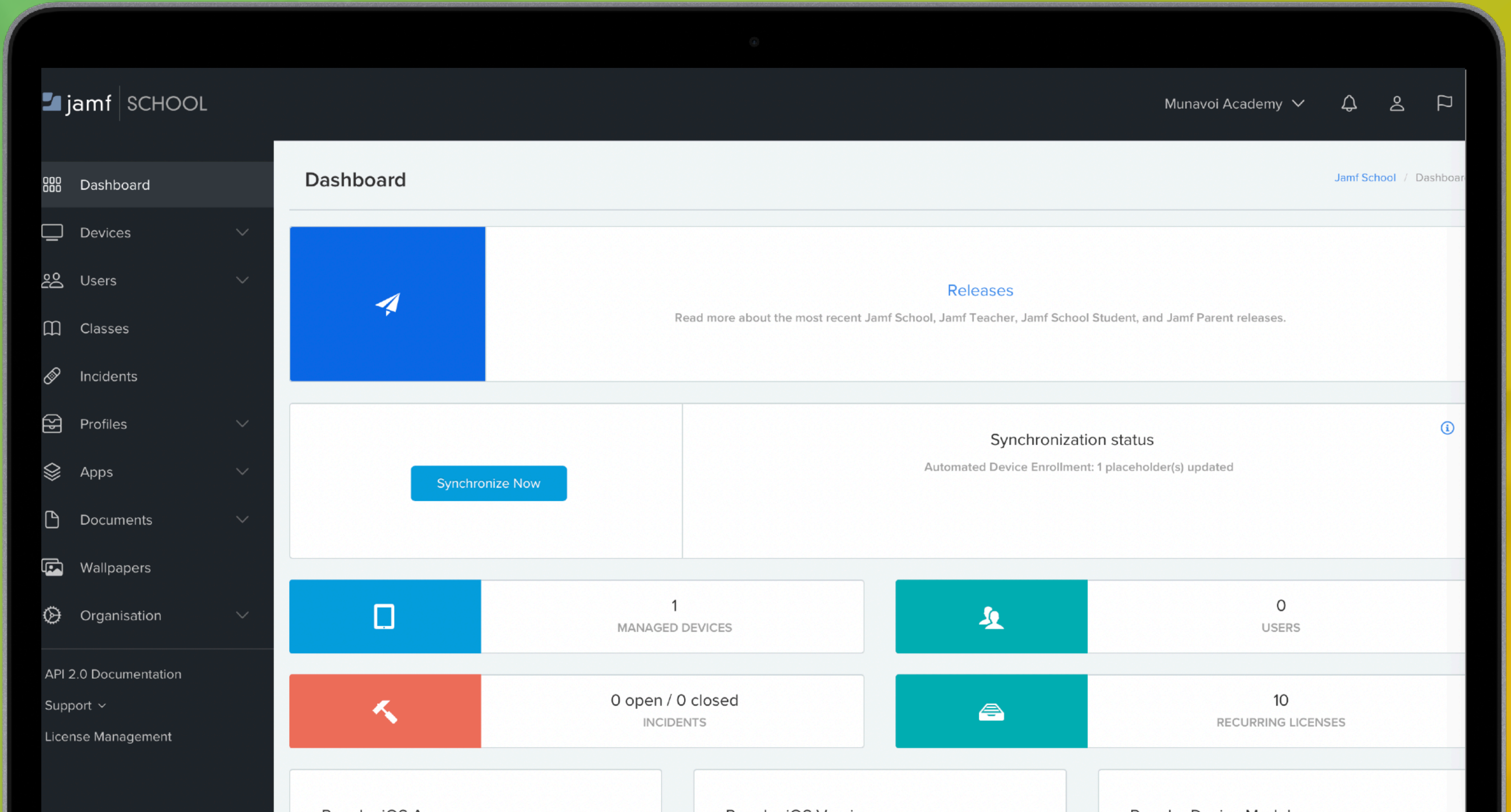
~~No more passwords~~

Less password entry

I CHANGED MY **PASSWORD** EVERYWHERE TO **INCORRECT** SO THAT WHEN I **FORGET** IT IT ALWAYS **REMINDS** ME, **YOUR** PASSWORD IS **INCORRECT**.

What Jamf **MDM**?

Jamf School



Dashboard

Releases

Read more about the most recent Jamf School, Jamf Teacher, Jamf School Student, and Jamf Parent releases.

Synchronization status

Automated Device Enrollment: 1 placeholder(s) updated

1 MANAGED DEVICES

0 USERS

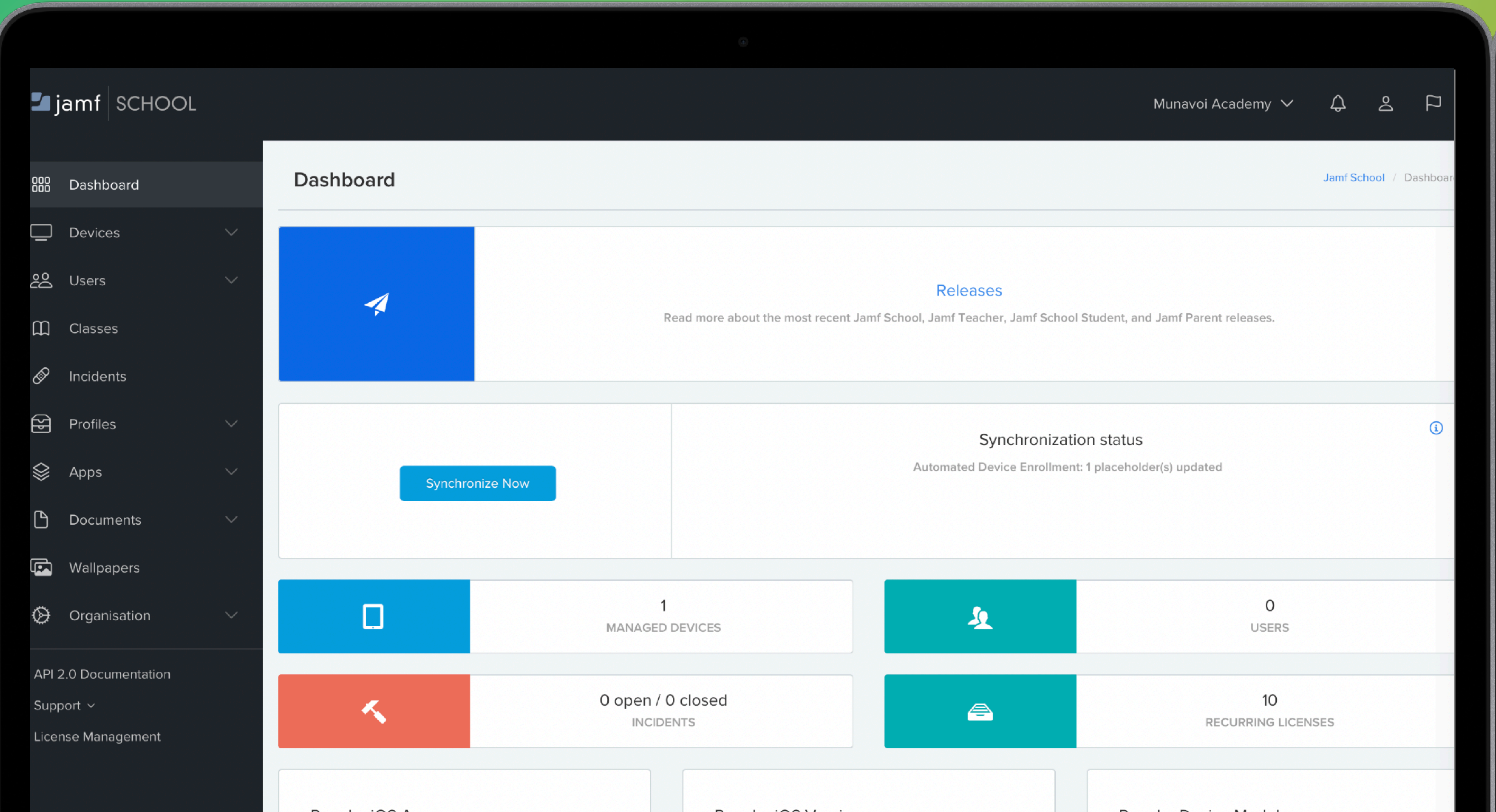
0 open / 0 closed INCIDENTS

10 RECURRING LICENSES

JAMF NATION LIVE

What Jamf **MDM**?

Jamf School or Pro - it doesn’t matter!



Dashboard

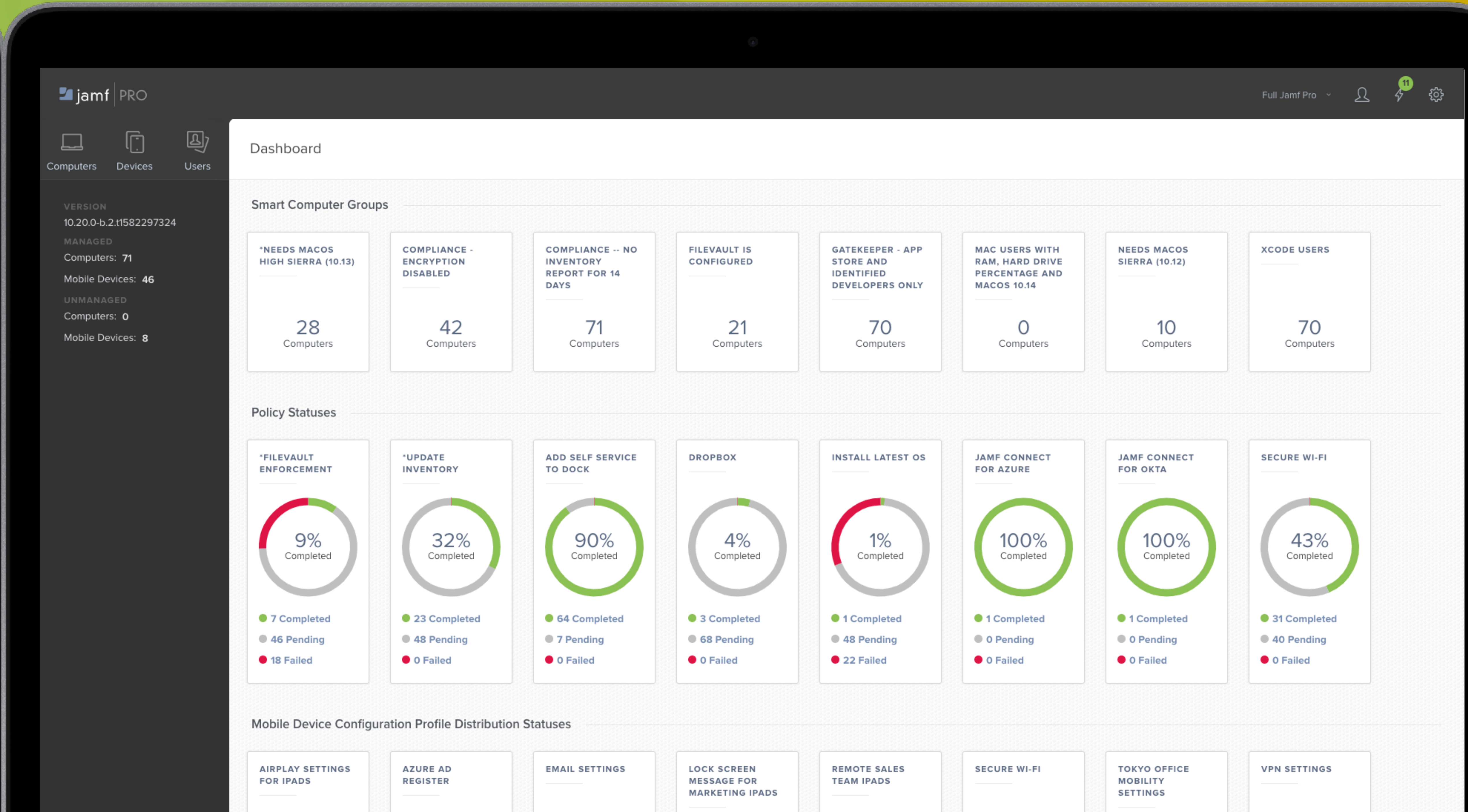
Releases

Read more about the most recent Jamf School, Jamf Teacher, Jamf School Student, and Jamf Parent releases.

Synchronization status

Automated Device Enrollment: 1 placeholder(s) updated

1 MANAGED DEVICES	0 USERS
0 open / 0 closed INCIDENTS	10 RECURRING LICENSES



VERSION
10.20.0-b.2.t1582297324
MANAGED
Computers: 71
Mobile Devices: 46
UNMANAGED
Computers: 0
Mobile Devices: 8

Dashboard

Smart Computer Groups

*NEEDS MACOS HIGH SIERRA (10.13)	COMPLIANCE - ENCRYPTION DISABLED	COMPLIANCE -- NO INVENTORY REPORT FOR 14 DAYS	FILEVAULT IS CONFIGURED	GATEKEEPER - APP STORE AND IDENTIFIED DEVELOPERS ONLY	MAC USERS WITH RAM, HARD DRIVE PERCENTAGE AND MACOS 10.14	NEEDS MACOS SIERRA (10.12)	XCODE USERS
28 Computers	42 Computers	71 Computers	21 Computers	70 Computers	0 Computers	10 Computers	70 Computers

Policy Statuses

*FILEVAULT ENFORCEMENT	*UPDATE INVENTORY	ADD SELF SERVICE TO DOCK	DROPBOX	INSTALL LATEST OS	JAMF CONNECT FOR AZURE	JAMF CONNECT FOR OKTA	SECURE WI-FI
9% Completed	32% Completed	90% Completed	4% Completed	1% Completed	100% Completed	100% Completed	43% Completed
● 7 Completed ● 46 Pending ● 18 Failed	● 23 Completed ● 48 Pending ● 0 Failed	● 64 Completed ● 7 Pending ● 0 Failed	● 3 Completed ● 68 Pending ● 0 Failed	● 1 Completed ● 48 Pending ● 22 Failed	● 1 Completed ● 0 Pending ● 0 Failed	● 1 Completed ● 0 Pending ● 0 Failed	● 31 Completed ● 40 Pending ● 0 Failed

Mobile Device Configuration Profile Distribution Statuses

AIRPLAY SETTINGS FOR IPADS	AZURE AD REGISTER	EMAIL SETTINGS	LOCK SCREEN MESSAGE FOR MARKETING IPADS	REMOTE SALES TEAM IPADS	SECURE WI-FI	TOKYO OFFICE MOBILITY SETTINGS	VPN SETTINGS

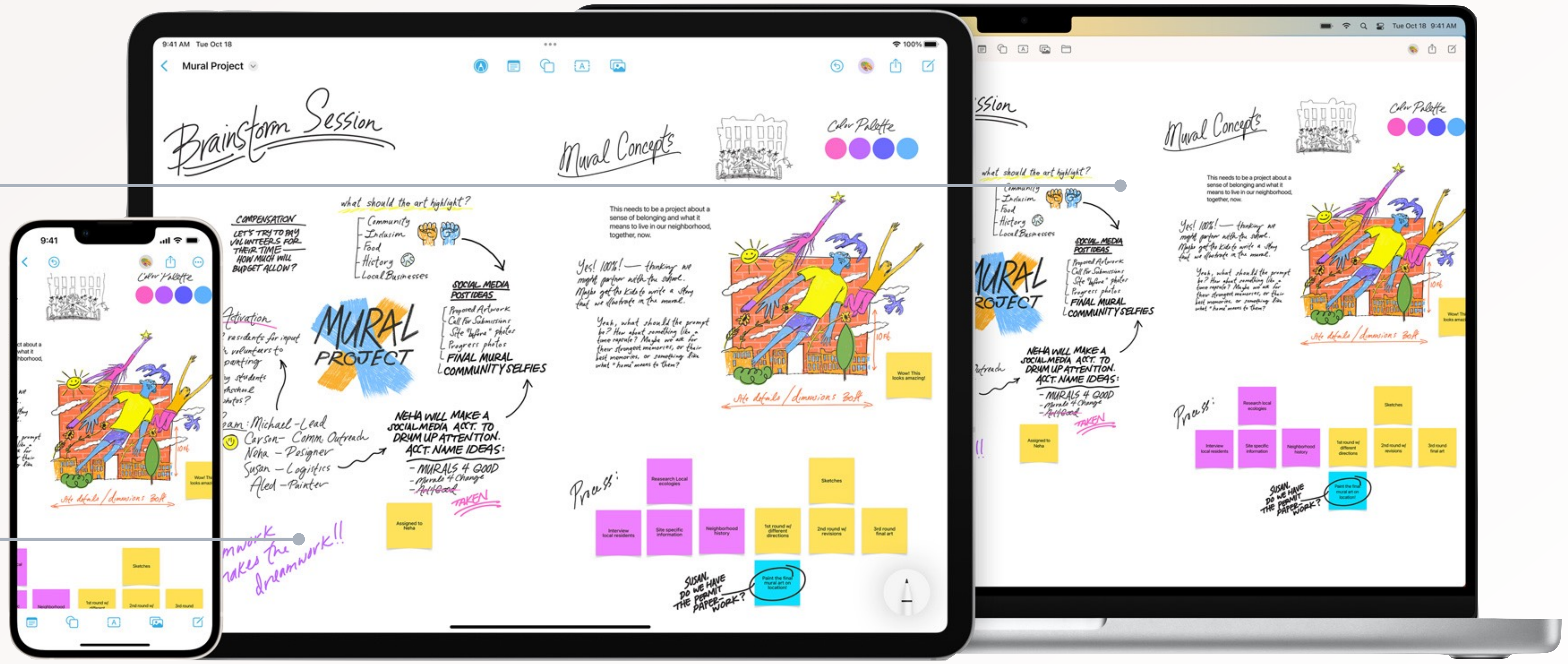
Also
Device Agnostic

macOS

Support users in 1:1 or macOS Labs

iOS and iPadOS

Stop sign in fatigue during setup



Prerequisites of SSO

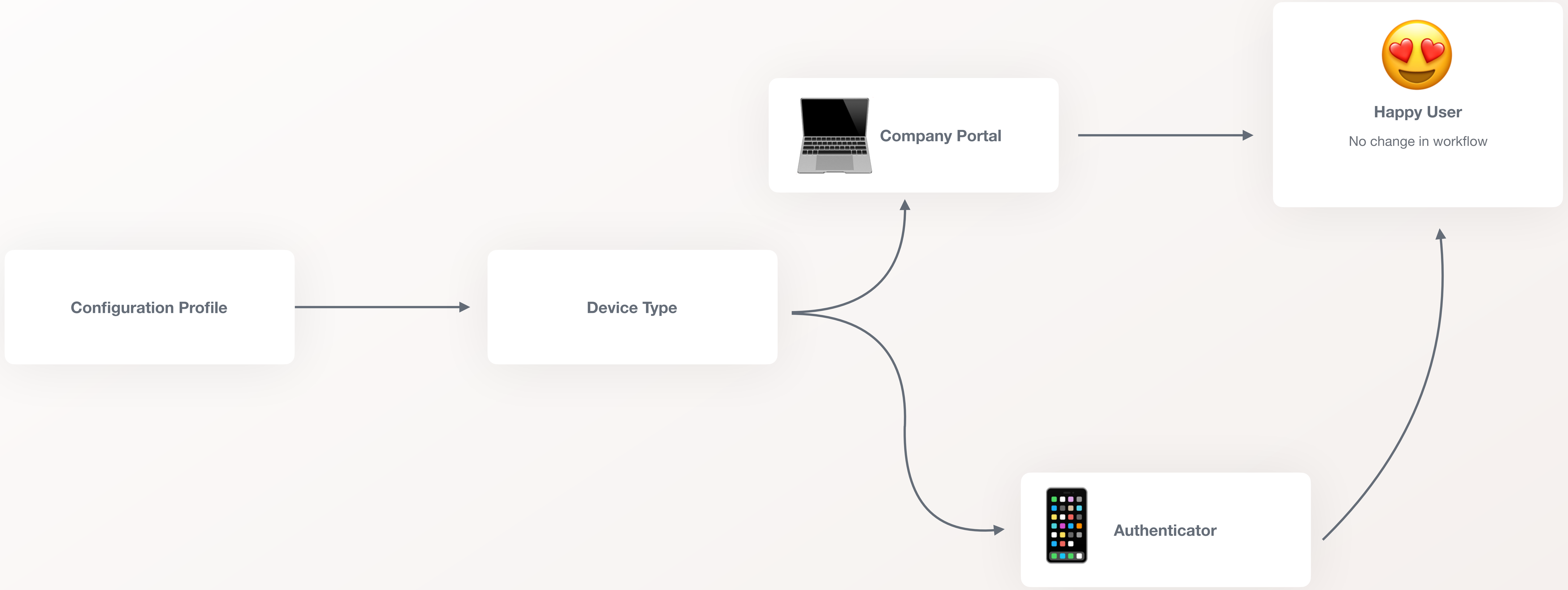
Device **<u>must</u>** be enrolled in **MDM**

1. **iPadOS** 13 or newer with Auth App
2. **macOS** 10.15 or newer with Auth App
3. **Configuration** Profile with **SSO Extension**

Deployment Requirements

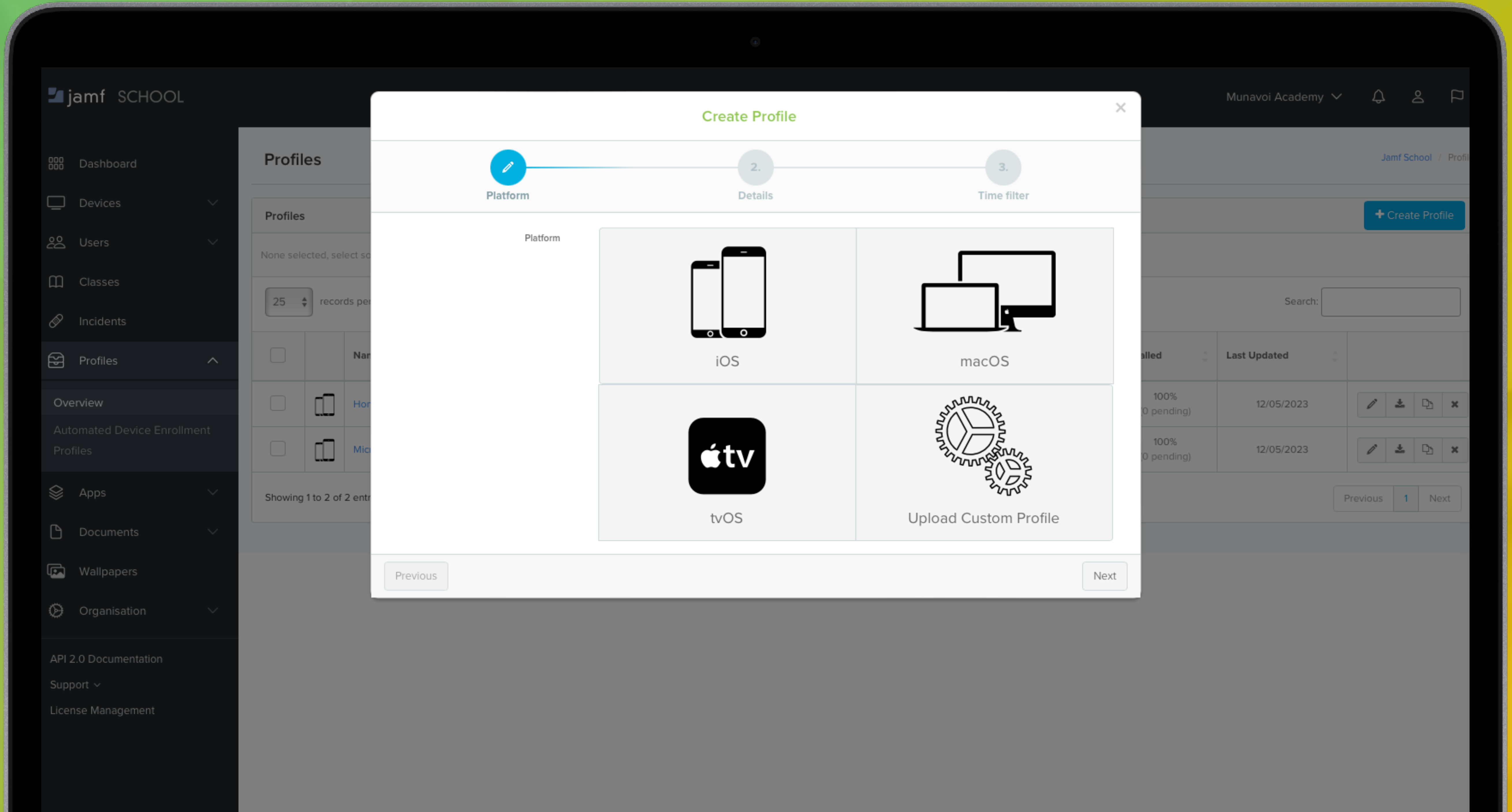
Configuration Profile

Deployment Requirements

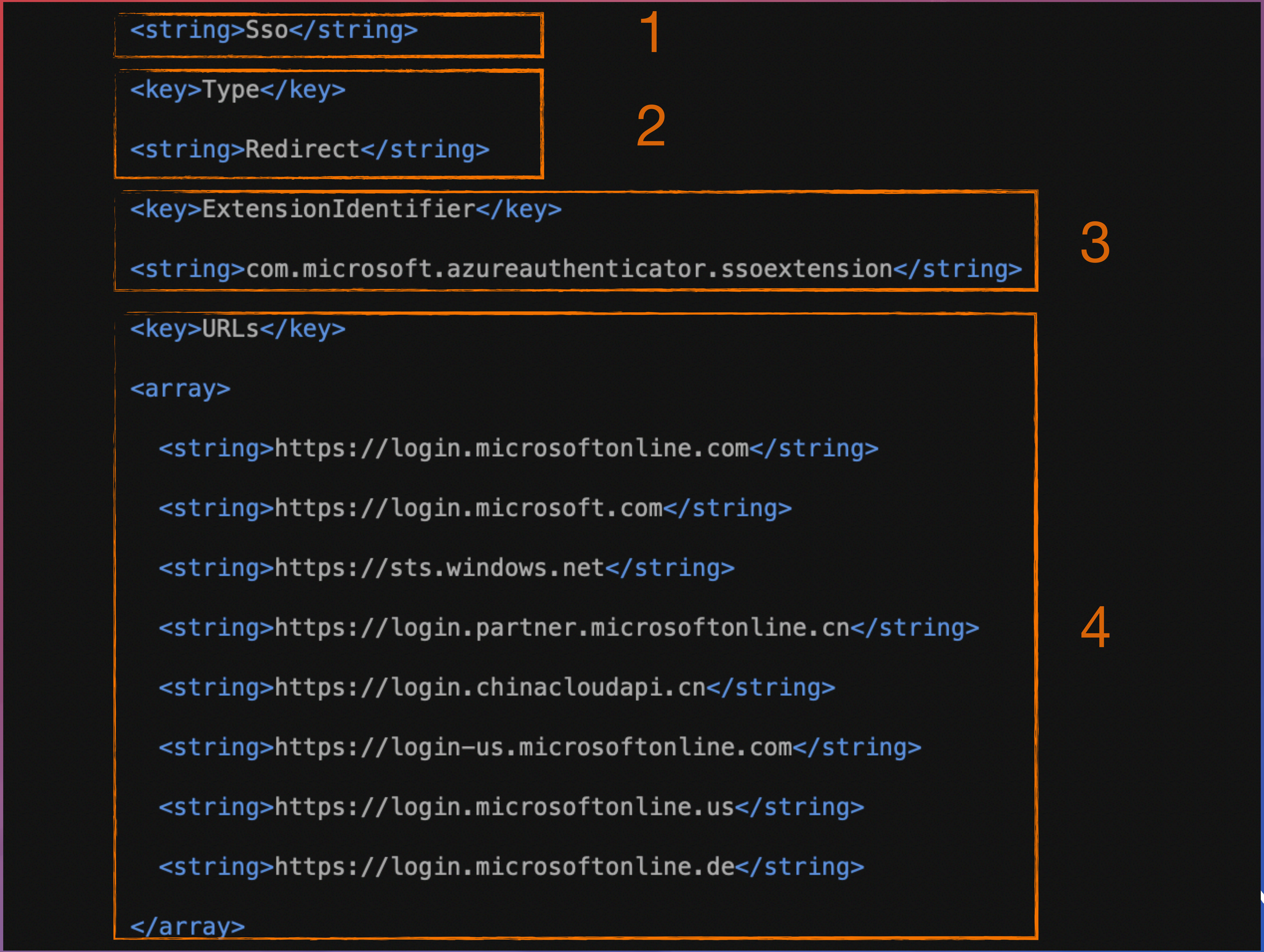


Configuration

The simpler. The Better. Magic 4



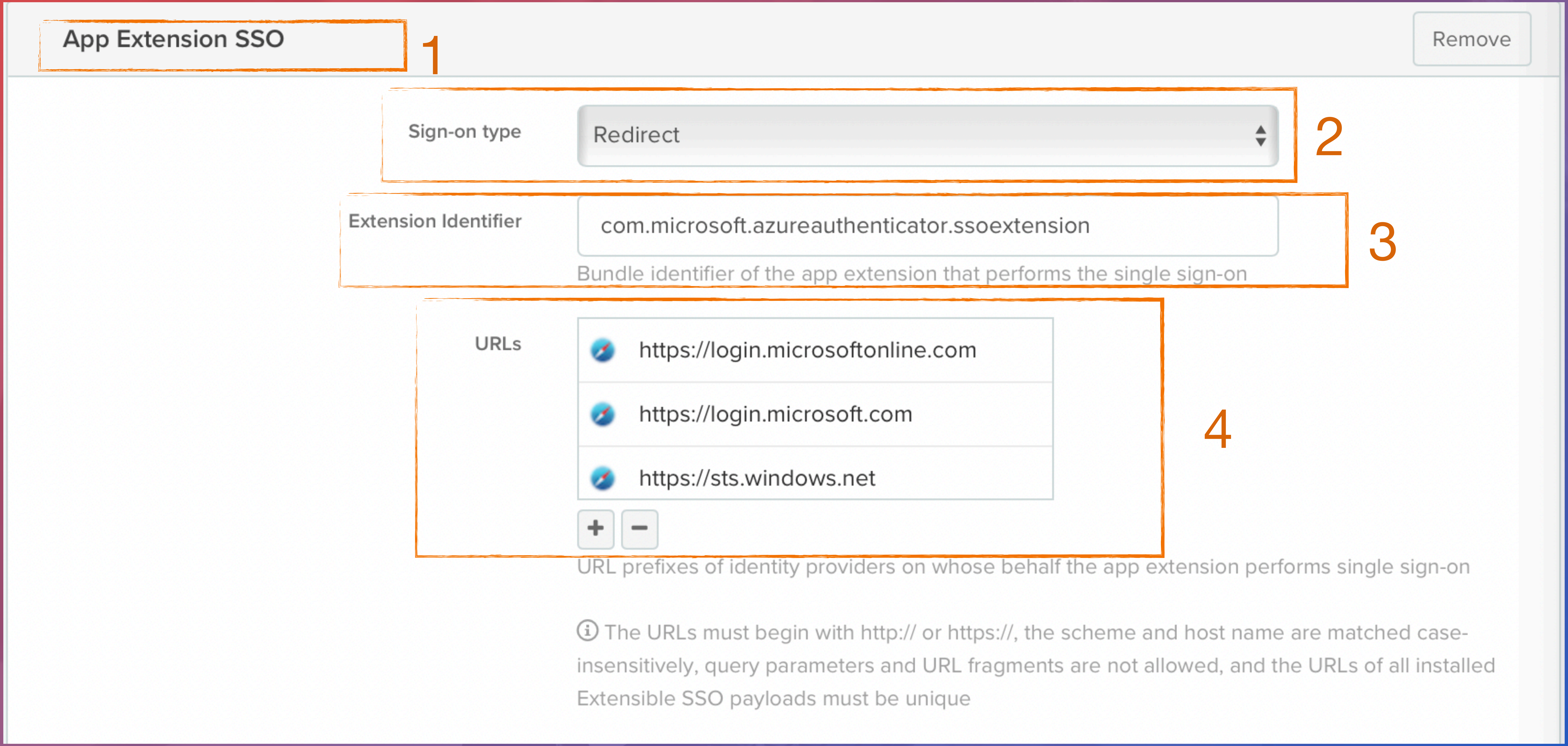
JAMF NATION LIVE



```
<string>Sso</string>
<key>Type</key>
<string>Redirect</string>
<key>ExtensionIdentifier</key>
<string>com.microsoft.azureauthenticator.ssoextension</string>
<key>URLs</key>
<array>
  <string>https://login.microsoftonline.com</string>
  <string>https://login.microsoft.com</string>
  <string>https://sts.windows.net</string>
  <string>https://login.partner.microsoftonline.cn</string>
  <string>https://login.chinacloudapi.cn</string>
  <string>https://login-us.microsoftonline.com</string>
  <string>https://login.microsoftonline.us</string>
  <string>https://login.microsoftonline.de</string>
</array>
```

EVERYONE IN THE AUDIENCE AT THIS MOMENT

Ok, now you have lost me.



App Extension SSO

Sign-on type: Redirect

Extension Identifier: com.microsoft.azureauthenticator.ssoextension

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

URLs:
- https://login.microsoftonline.com
- https://login.microsoft.com
- https://sts.windows.net

URL prefixes of identity providers on whose behalf the app extension performs single sign-on

ⓘ The URLs must begin with http:// or https://, the scheme and host name are matched case-insensitively, query parameters and URL fragments are not allowed, and the URLs of all installed Extensible SSO payloads must be unique

The **Magic** 4

Payload Type = SSO

We all need a payload. Similar to Passcode, Restrictions or Network. Top level directions.

SSO Type = Redirect

How will the user authenticate. Multiple options here but the requirements from Microsoft are Redirect for simple experience with Azure.

Extension Identifier = Authenticator

This is our Broker. What will pass through and confirm our identity.

iOS = Authenticator
macOS = Company Portal

URLs = Check with your vendor

URLs of identity providers to perform SSO.

The **Magic** 4

Payload Type = SSO

We all need a payload. Similar to Passcode, Restrictions or Network. Top level directions.

SSO Type = Redirect

How will the user authenticate. Multiple options here but the requirements from Microsoft are Redirect for simple experience with Azure.

Extension Identifier = Authenticator

This is our Broker. What will pass through and confirm our identity.

iOS = Authenticator
macOS = Company Portal

URLs = Check with your vendor

URLs of identity providers to perform SSO.

Remove all
+ Add
1
2
3
4
+ Add

Single Sign-on Extensions

1 payload configured

Single Sign-on Extension

Configure app extensions that perform single sign-on (iOS 13 or later).

Payload Type

Use the Kerberos payload type for the "com.apple.AppSSOKerberos.KerberosExtension" Extension Identifier.

[✓ SSO] Kerberos

Extension Identifier

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

com.microsoft.azureauthenticator.ssoextension

Team Identifier

The team identifier of the app extension that performs single sign-on

Sign-on Type

Sign-on authorization 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.

https://login.microsoftonline.com/

https://login.microsoft.com/

https://sts.windows.net/

https://login.partner.microsoftonline.cn/

https://login.chinacloudapi.cn/

https://login.microsoftonline.de/

https://login.microsoftonline.us/

https://login.usgovcloudapi.net/

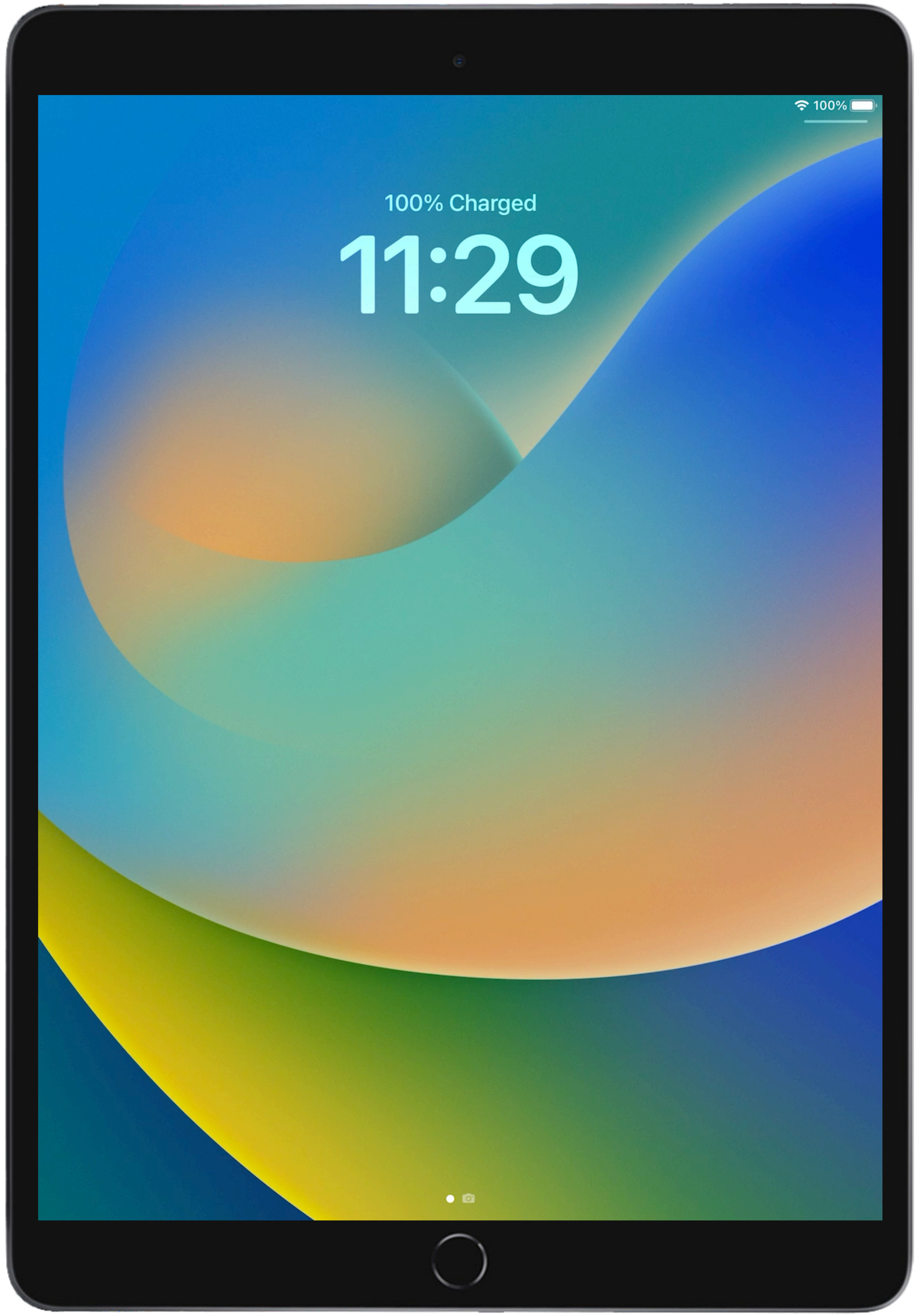
https://login-us.microsoftonline.com/

EVERYONE IN THE AUDIENCE AT THIS MOMENT

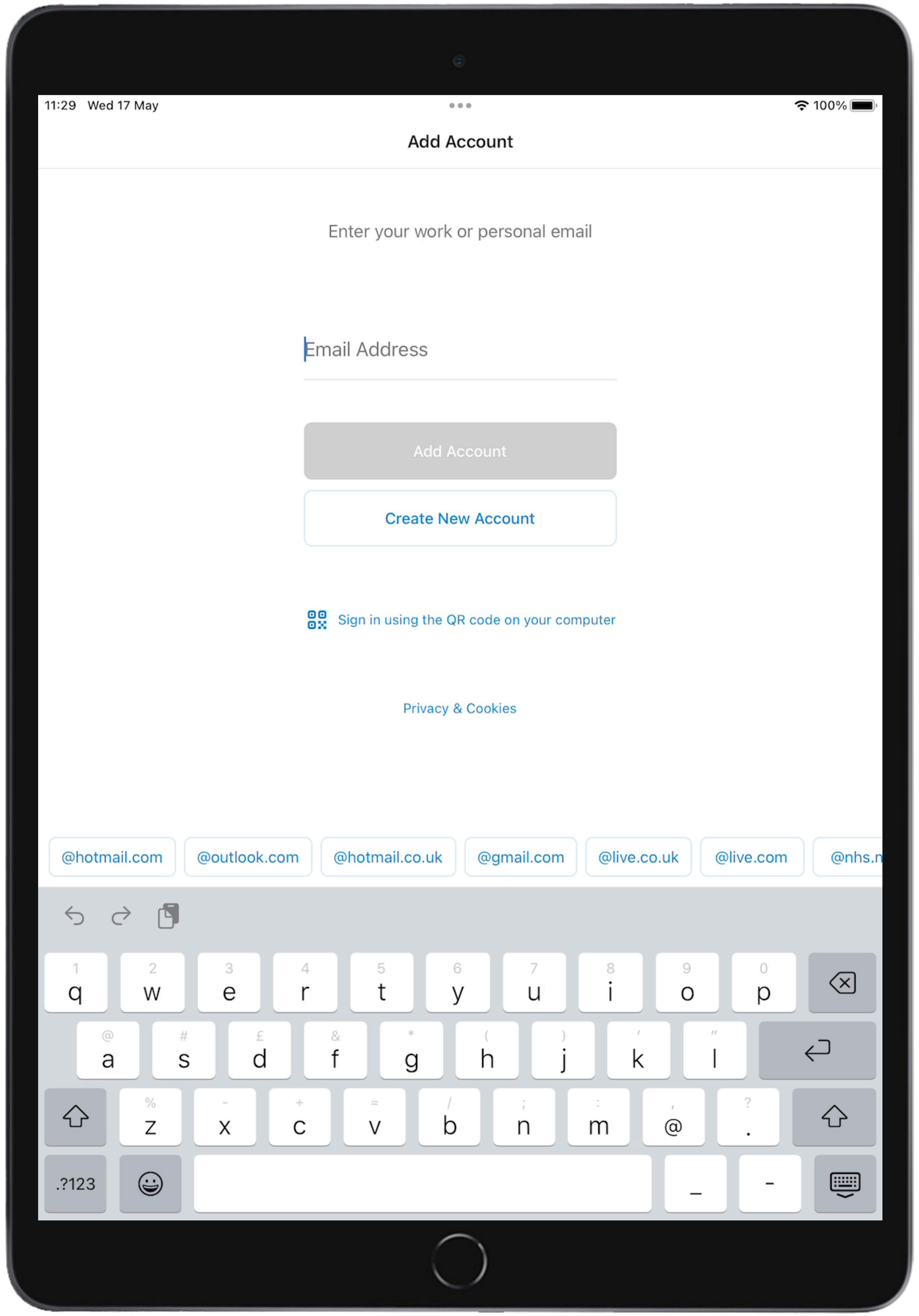
But what does that actually look like?

iPad **SSO** Examples

🏫



iPad **SSO** Examples



11:29 Wed 17 May

100%

Add Account

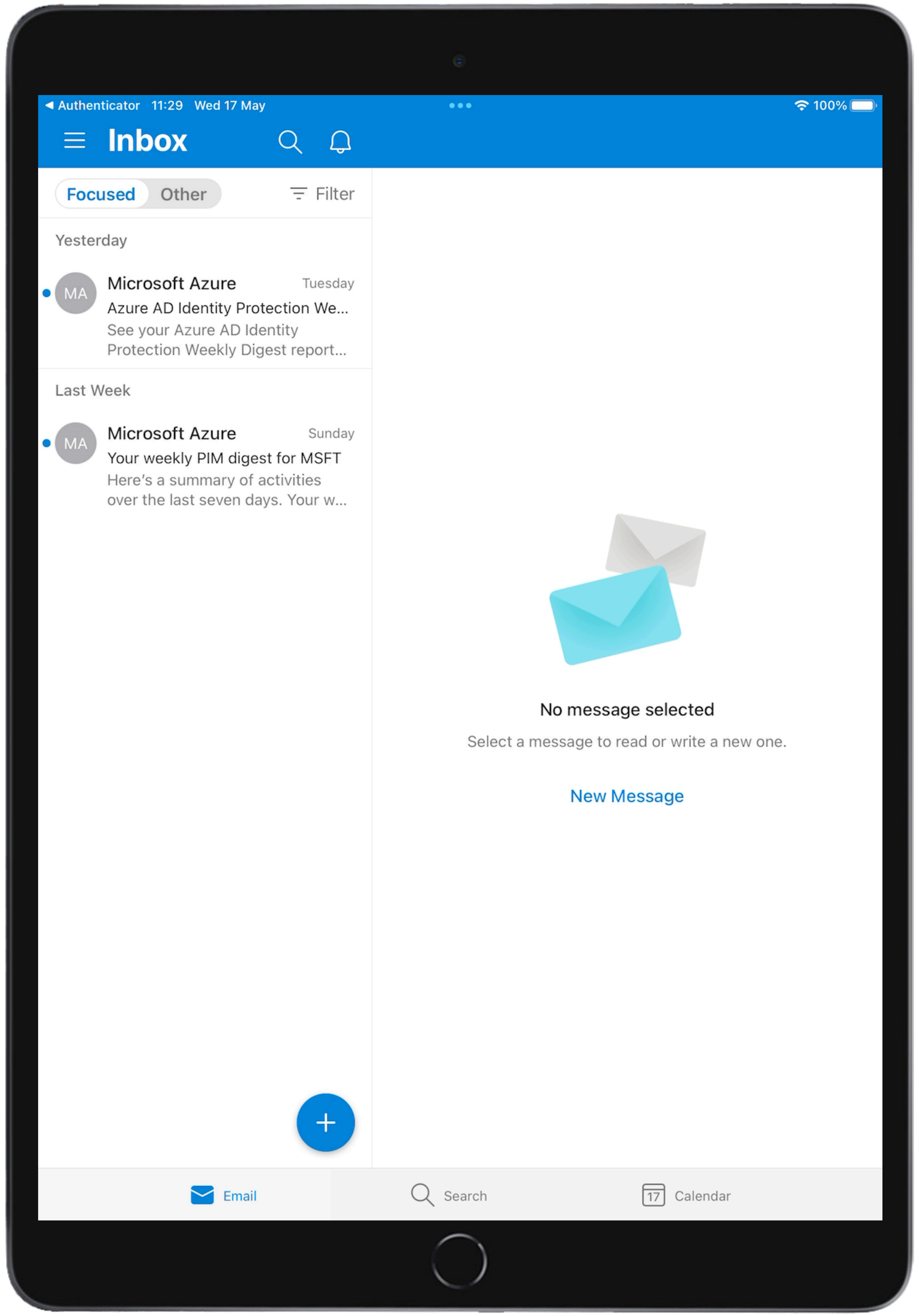
Enter your work or personal email

Email Address

JAMF NATION LIVE

iPad **SSO** Examples

Outlook ✅
Authenticator ✅
portal.office.com ❌



Yesterday

MA Microsoft Azure Tuesday
Azure AD Identity Protection We...
See your Azure AD Identity Protection Weekly Digest report...

Last Week

MA Microsoft Azure Sunday
Your weekly PIM digest for MSFT
Here's a summary of activities over the last seven days. Your w...

No message selected

Select a message to read or write a new one.

🏫

Standard

=

always needing to unlock or enter a password

🏡

SSO

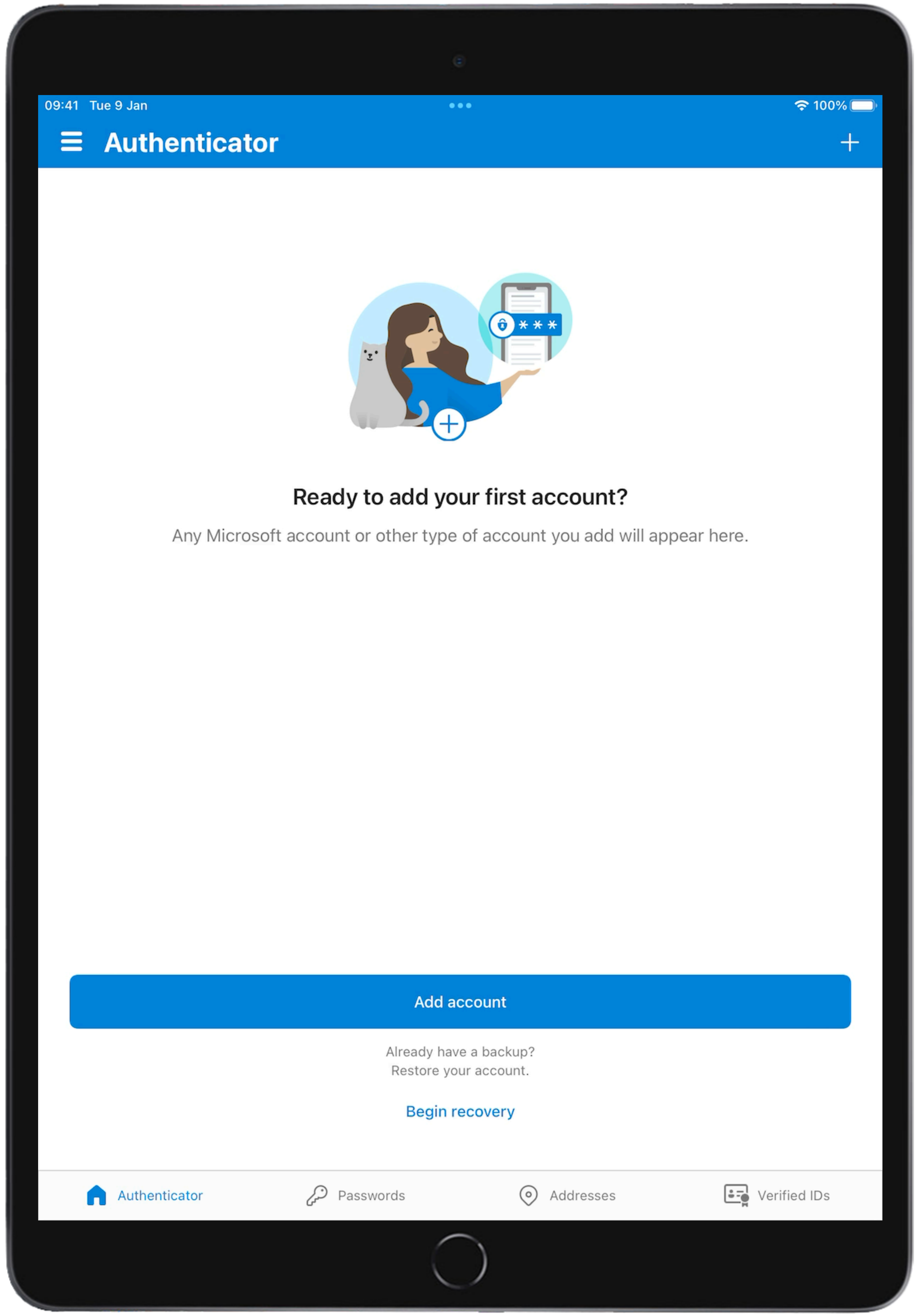
=

Authenticate once and done.

iPad **SSO** Examples

🏡

iPad **SSO** Examples



09:41 Tue 9 Jan 100%

Authenticator

Ready to add your first account?

Any Microsoft account or other type of account you add will appear here.

Already have a backup?
Restore your account.

🏫

Standard

=

always needing to unlock or enter a password

🏡

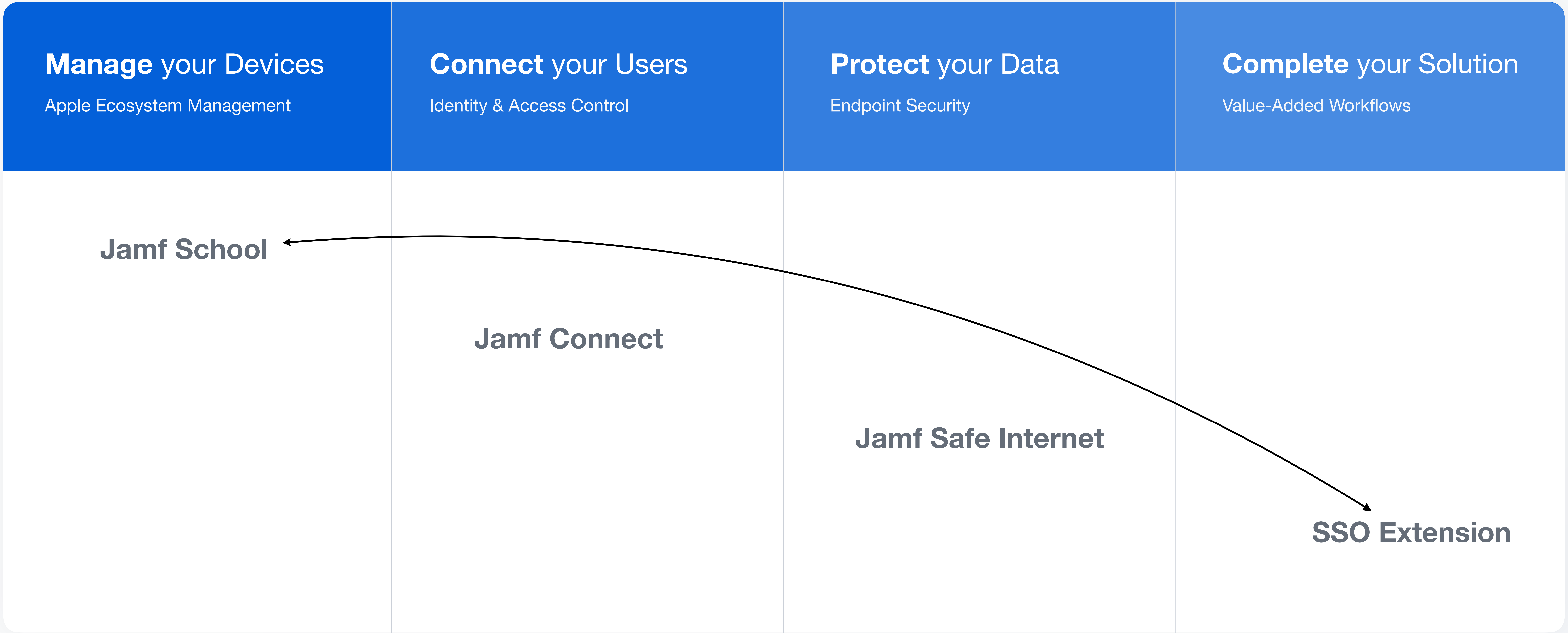
SSO

=

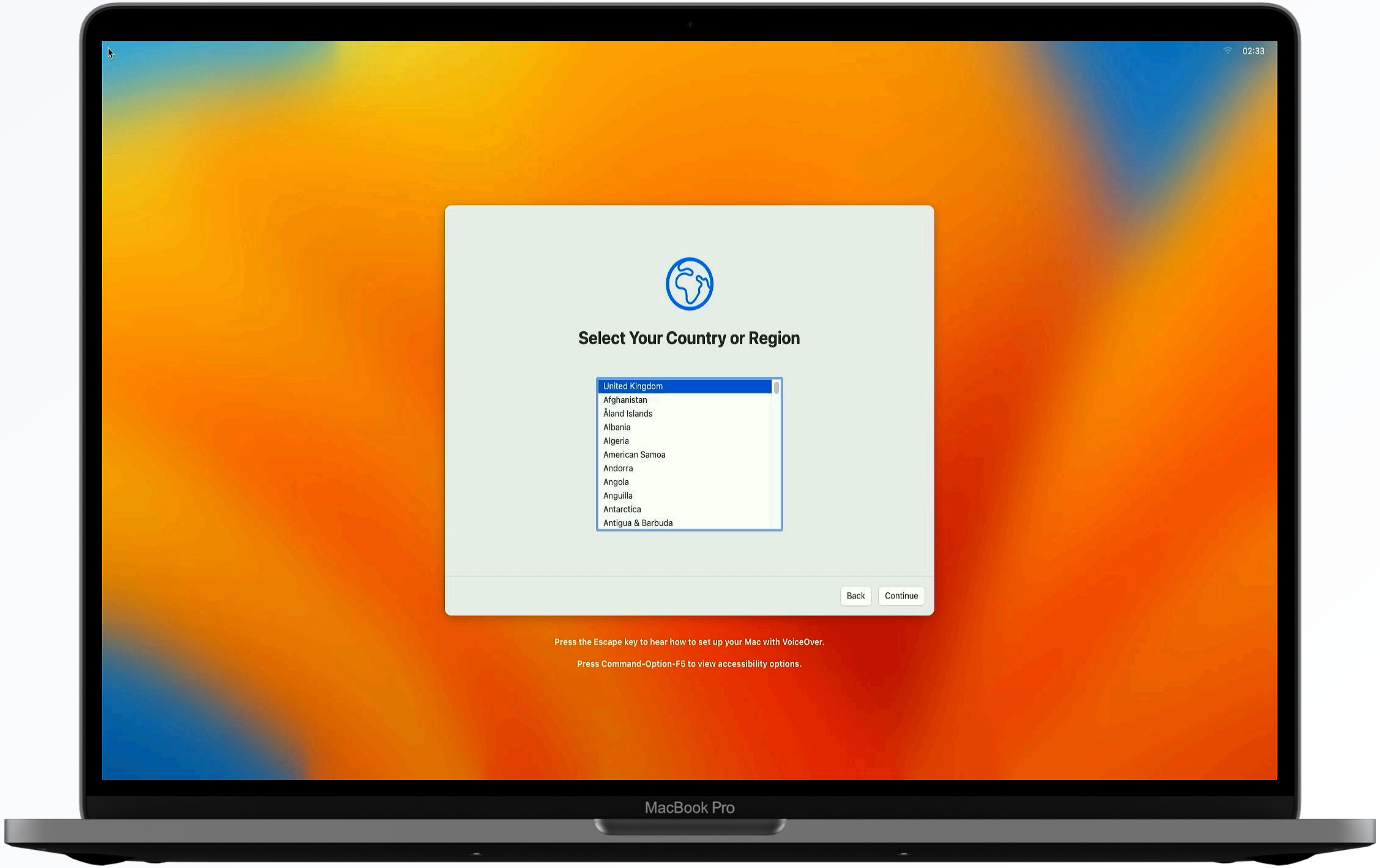
Authenticate once and done.

Workflows

Jamf **Platform**



Manage your Devices Apple Ecosystem Management	**Connect** your Users Identity & Access Control	**Protect** your Data Endpoint Security	**Complete** your Solution Value-Added Workflows
Jamf School	**Jamf Connect**	**Jamf Safe Internet**	**SSO Extension**



Select Your Country or Region

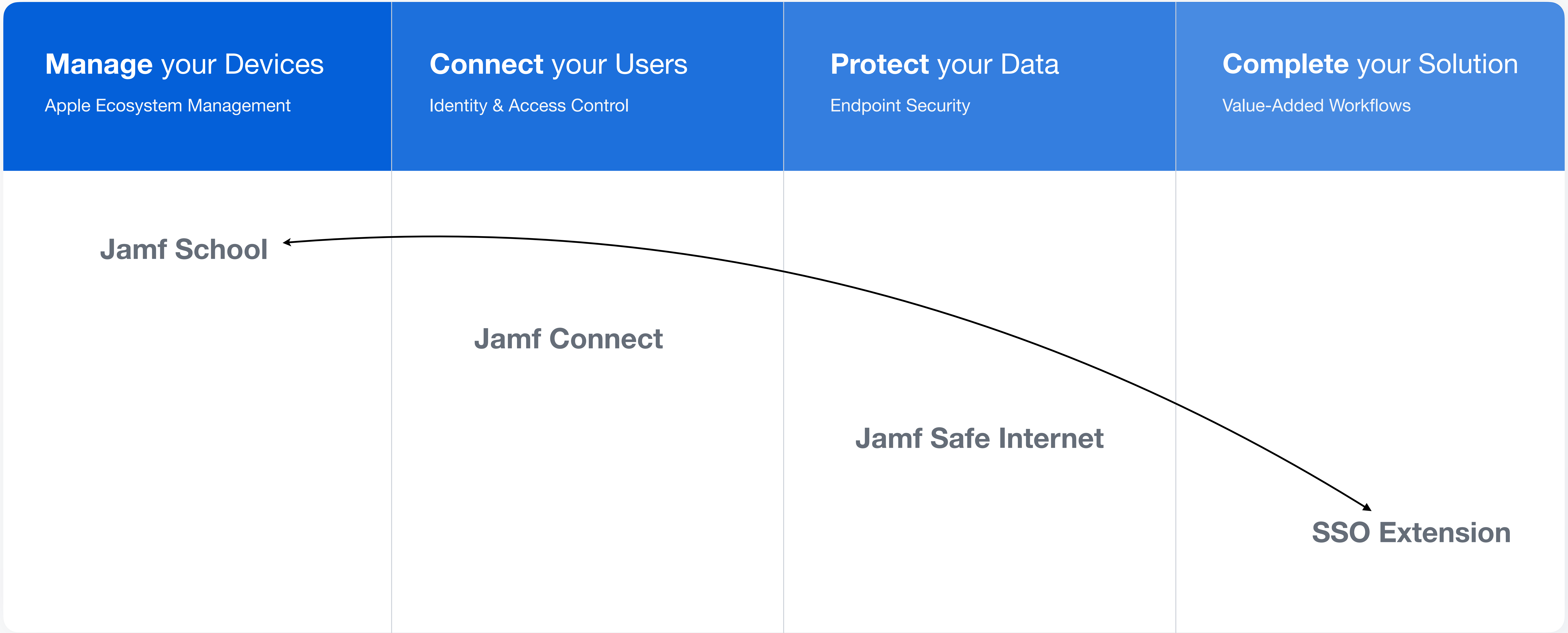
- United Kingdom
- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua & Barbuda

Press the Escape key to hear how to set up your Mac with VoiceOver.

Press Command-Option-F5 to view accessibility options.

Safari
File
Edit
View
History
Bookmarks
Window
Help
Wed 24 May 11:08
Macintosh HD
jamf
MacBook Pro

Jamf **Platform**



Manage your Devices Apple Ecosystem Management	**Connect** your Users Identity & Access Control	**Protect** your Data Endpoint Security	**Complete** your Solution Value-Added Workflows
Jamf School	Jamf Connect	Jamf Safe Internet	SSO Extension

Points of Note and Recommendations

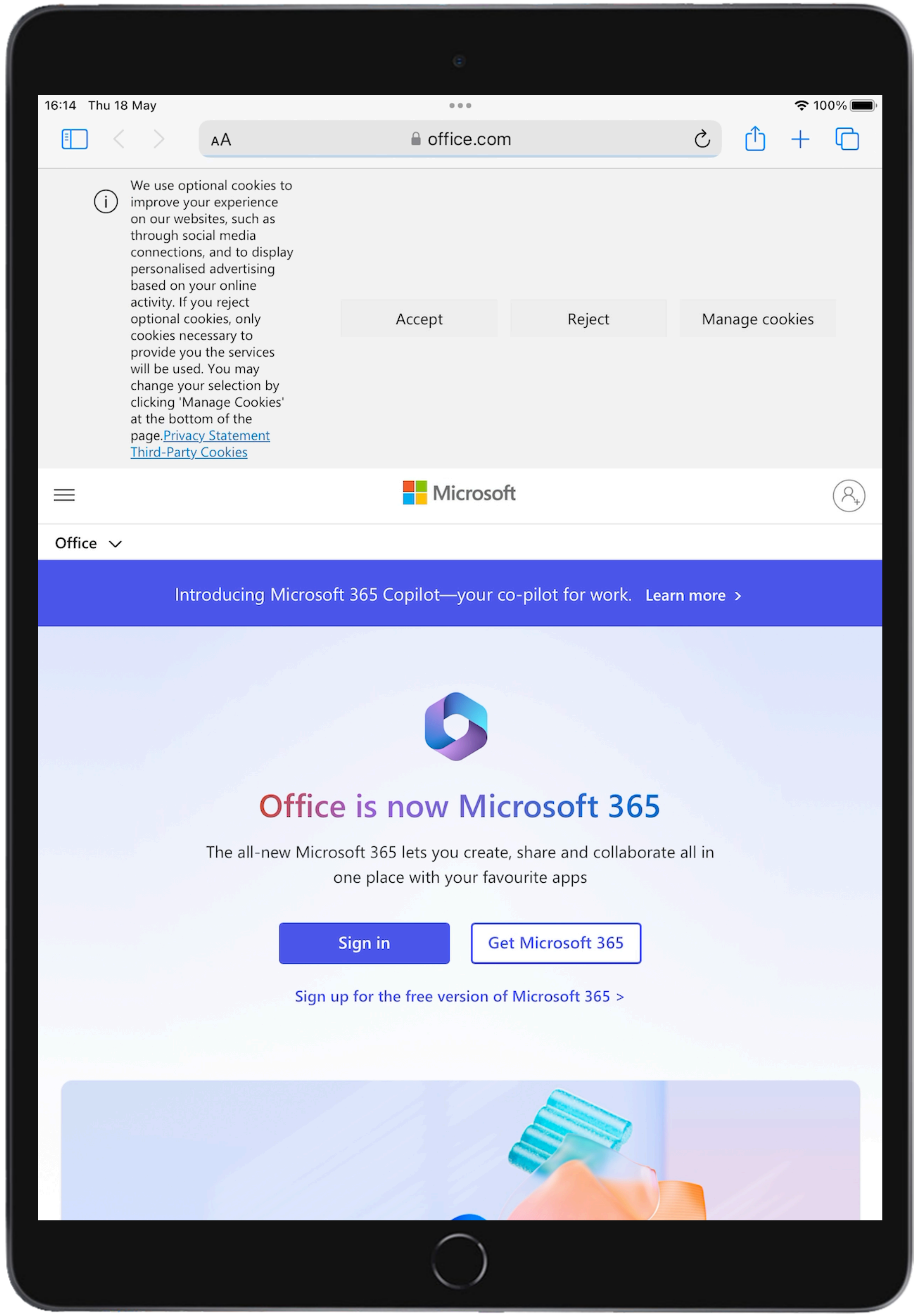
Is there bad SSO?

Yes!

iPad **SSO** Examples

iPad **SSO** Examples

portal.office.com ✅



16:14 Thu 18 May

100%

AA office.com

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalised advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking 'Manage Cookies' at the bottom of the page.Privacy Statement Third-Party Cookies

Accept Reject Manage cookies

Microsoft

Office

Introducing Microsoft 365 Copilot—your co-pilot for work. Learn more >

Office is now Microsoft 365

The all-new Microsoft 365 lets you create, share and collaborate all in one place with your favourite apps

Sign in Get Microsoft 365

Sign up for the free version of Microsoft 365 >

iPad **SSO** Examples

portal.office.com ✅

Outlook 🤷‍♀️

iPad **SSO** Examples

portal.office.com ✅
Outlook 🤷‍♀️
Word ❌

How often would my user need to re-authenticate after the first SSO?

It Depends!

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days. Asking users for credentials often seems like a sensible thing to do, but it can backfire: users that are trained to enter their credentials without thinking can unintentionally supply them to a malicious credential prompt.

Microsoft

HTTPS://LEARN.MICROSOFT.COM/EN-US/AZURE/ACTIVE-DIRECTORY/CONDITIONAL-ACCESS/HOWTO-CONDITIONAL-ACCESS-SESSION-LIFETIME#USER-SIGN-IN-FREQUENCY

What if a user changes their password?

Prompt for sign in!

What if we don’t want a specific app to use SSO?

We have a key for that!

Bundle IDs of applications not allowed to participate in SSO.

```
<key>AppBlockList</key>
<string>com.google.Gmail</string>
```

All Managed applications allowed to participate in SSO.

```
<key>Enable_SSO_On_All_ManagedApps</key>
<integer>1</integer>
```

Bundle IDs of applications allowed to participate in SSO.

```
<key>AppAllowList</key>
<string>com.showbie.showbiePad</string>
```

Ok, I want more info?

We have you covered!

Merill Fernando

Principal Product Manager - Azure Active Directory
Microsoft

Guides, Troubleshooting & More

The Magic 4

Jamf, Apple & Microsoft ❤️

Recap

🔒

SSO is good

Secure
IT Approved
Unified across Apple Devices

😎

SSO is easy

IT
Users
Deploy it today

😍

Users will love it

Simple
Won’t break current workflows
Secure