SALLE ÉDUCATION

JAMF NATION LIVE

Jamf & Microsoft: Safe Internet & Extension SSO

Vincent Bonnin Technical Enablement Manger, Jamf

Jamf & Microsoft :
Safe Internet & Extension SSO

JAMF NATION LIVE

Vincent Bonnin

Technical Enablement Manager

Agenda

1 | Qu’est-ce que l’authentification unique ?

Découverte de l’authentification unique (SSO) et de ses bénéfices.

2 | Mettre en place l’authentification unique

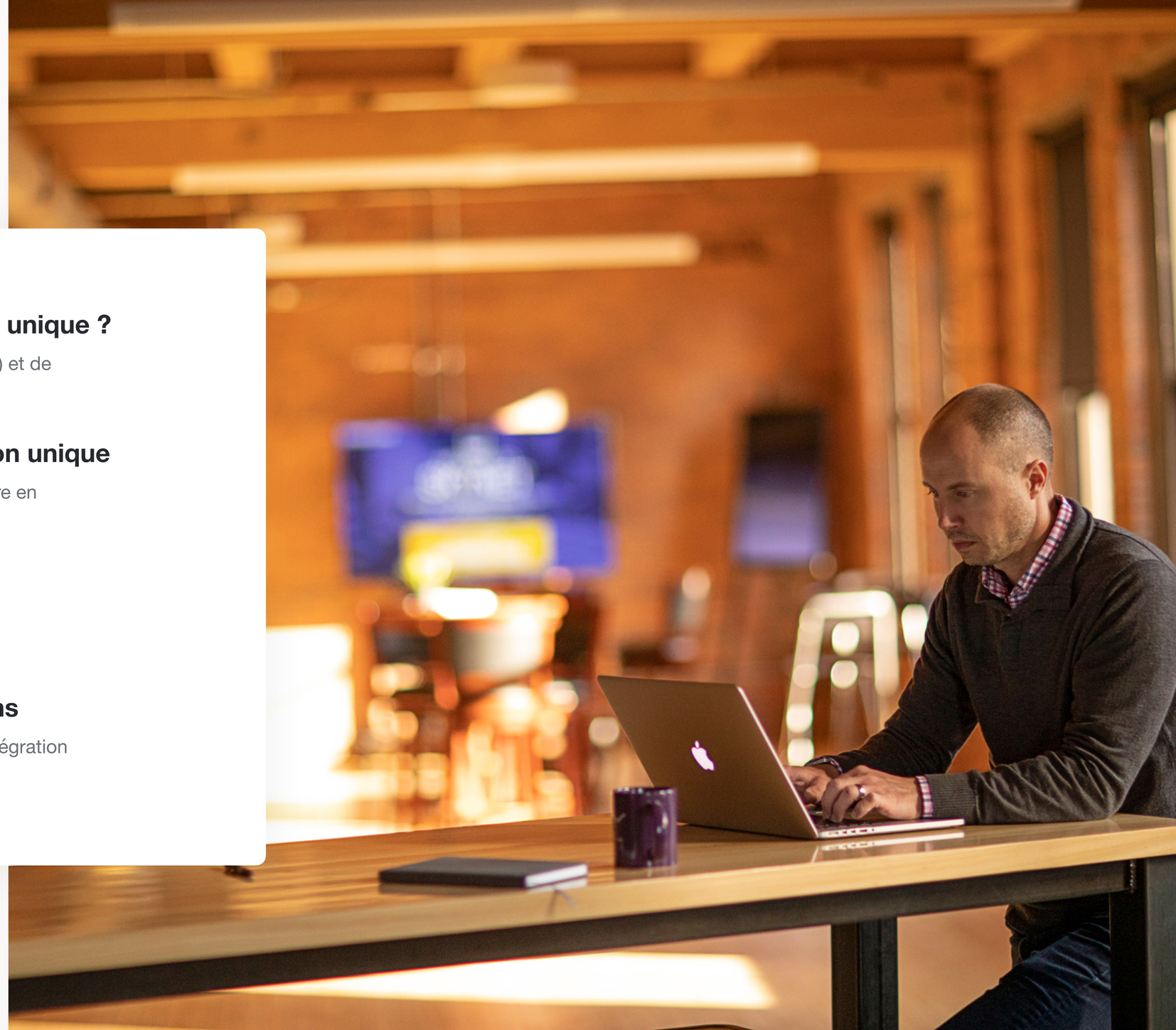
Quelles sont les bonnes pratiques pour mettre en place une architecture SSO ?

3 | Workflows

Exemples d’utilisation du SSO avec Jamf.

4 | Remarques et recommandations

Quelques conseils d’expert pour faciliter l’intégration des extensions SSO !



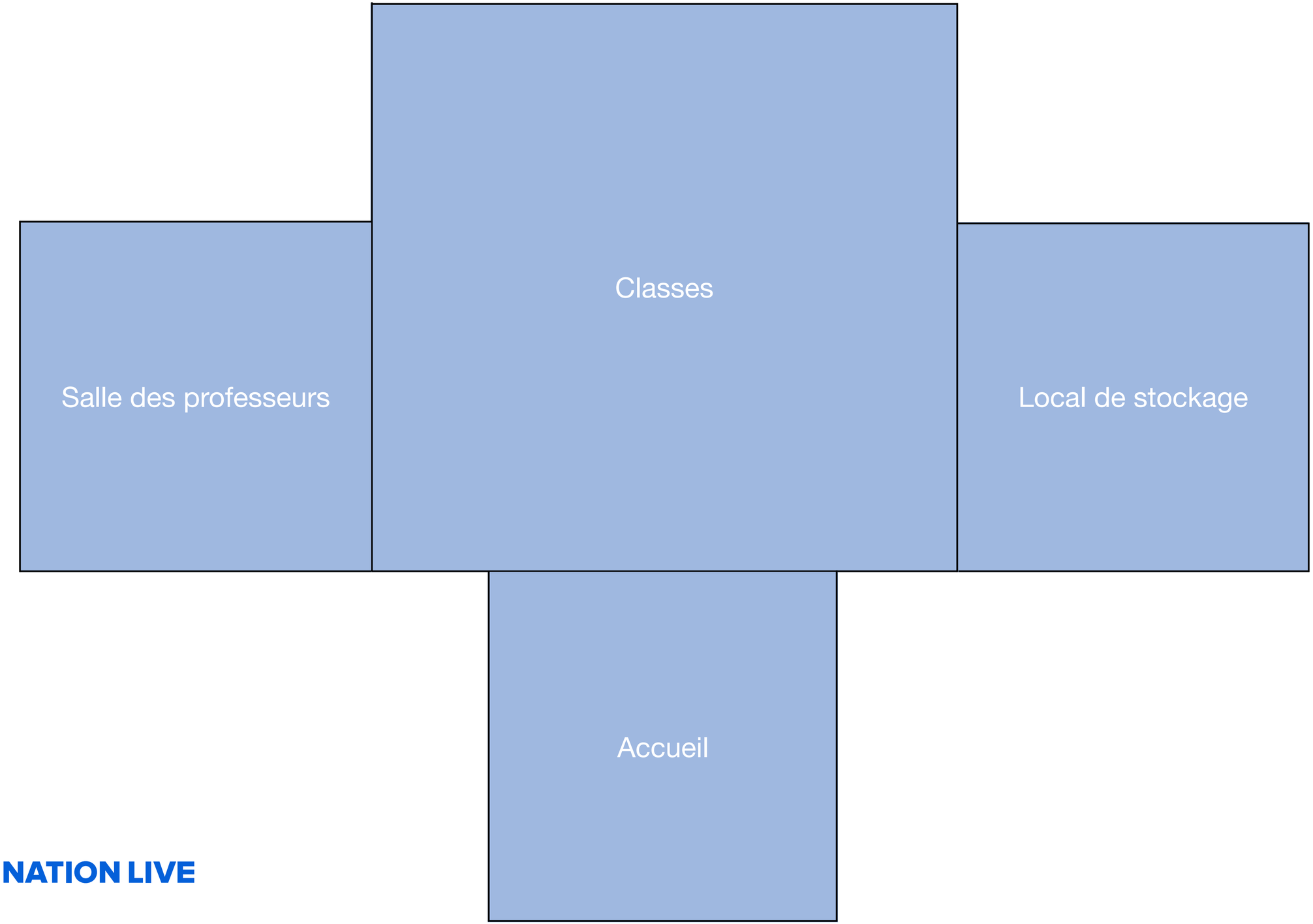
JAMF NATION LIVE

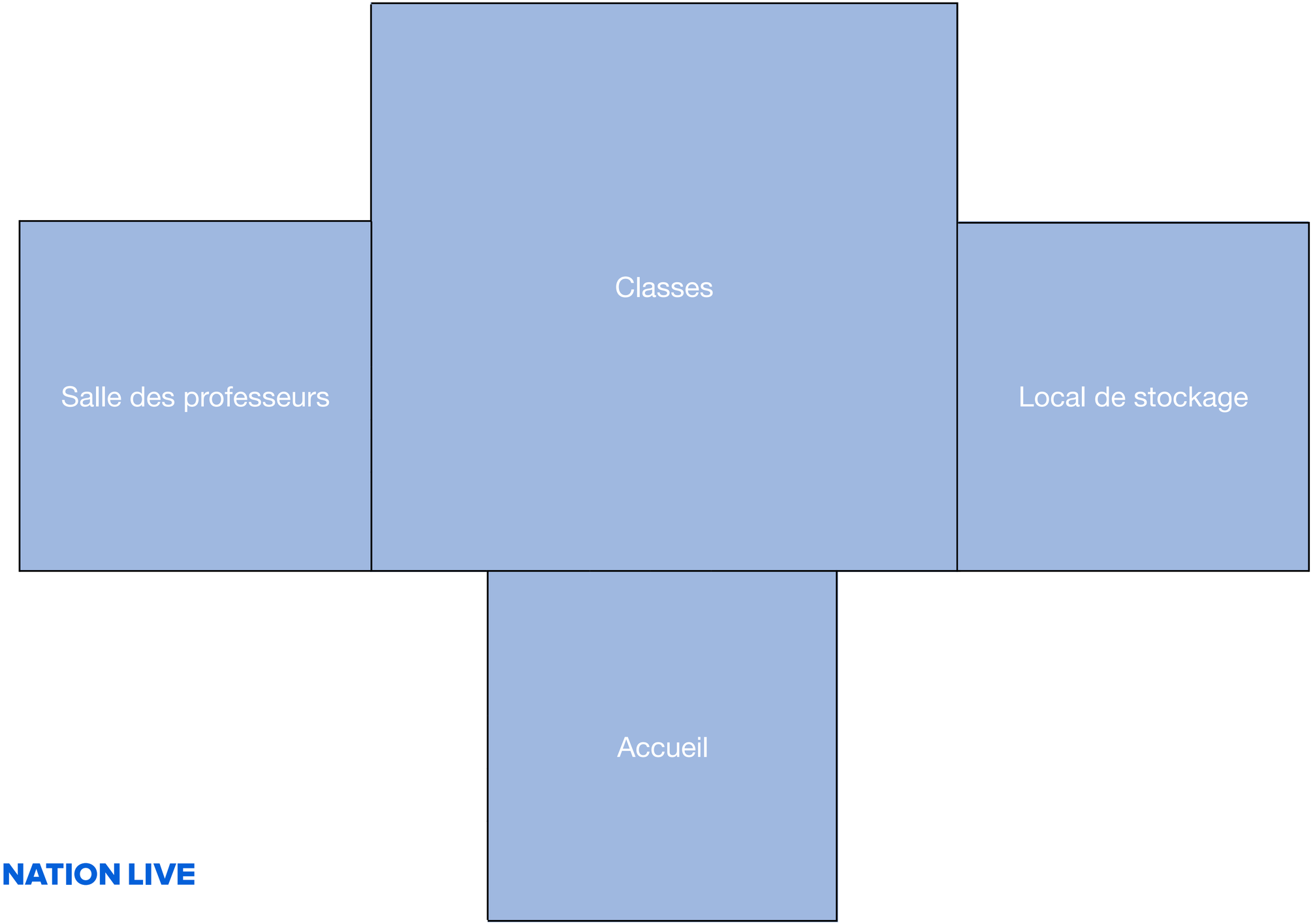
Qu’est-ce que le **SSO?**

SSO = Single Sign-On = Authentification unique

Ou

La fin des mots de passe ?


Classes
Salle des professeurs
Local de stockage
Accueil

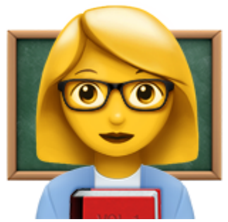

Classes
Salle des professeurs
Local de stockage
Accueil

Salle des professeurs

Classes

Local de stockage

Accueil

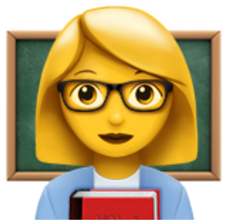


Salle des professeurs

Classes

Local de stockage

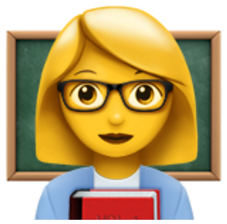
Accueil



Salle des professeurs

Classes

Local de stockage

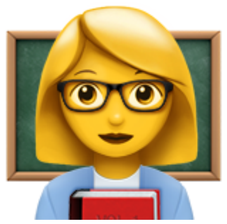


Accueil

Salle des professeurs

Classes

Local de stockage

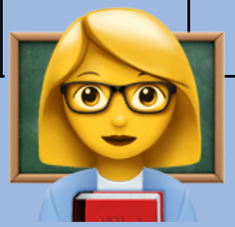


Accueil

Classes

Salle des professeurs

Local de stockage



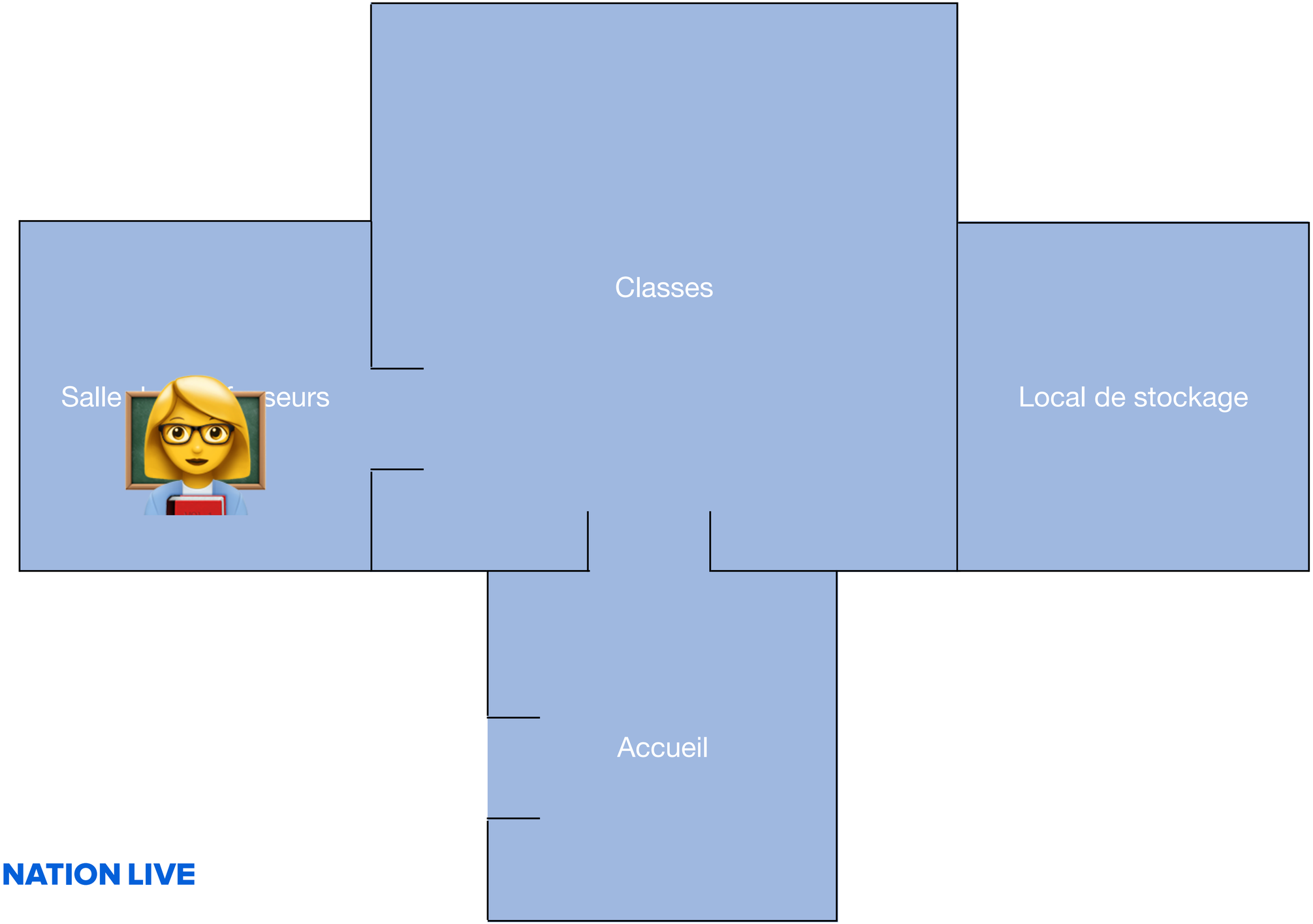
Accueil

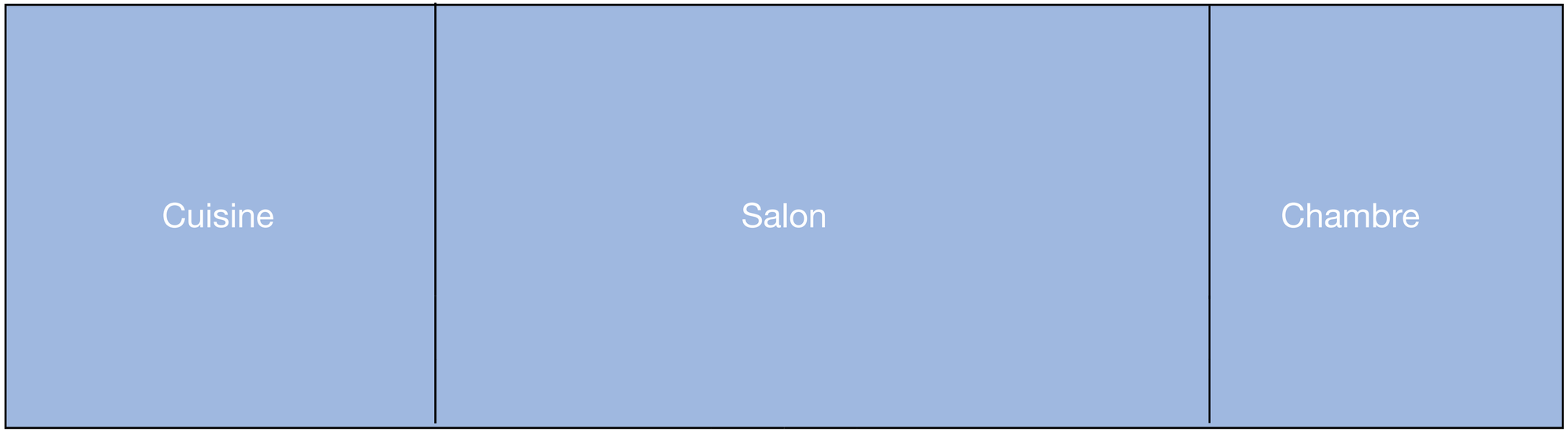
Classes

Salle des professeurs

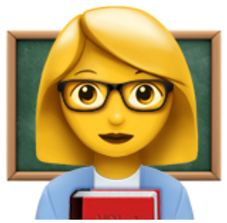
Local de stockage

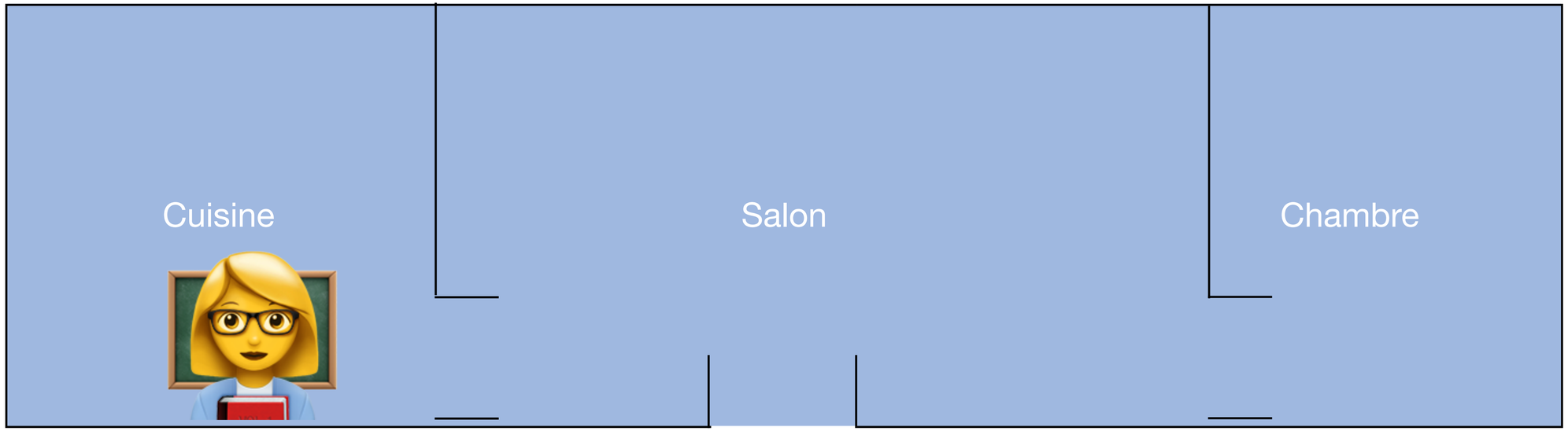
Accueil


Classes
Local de stockage
Accueil


Cuisine
Salon
Chambre

Cuisine	Salon	Chambre




Cuisine
Salon
Chambre

Sans SSO
=
Plusieurs authentification nécessaires

Avec SSO
=
Une seule authentification nécessaire

Qu’est-ce que le **SSO?**

SSO = Single Sign-On = Authentification unique

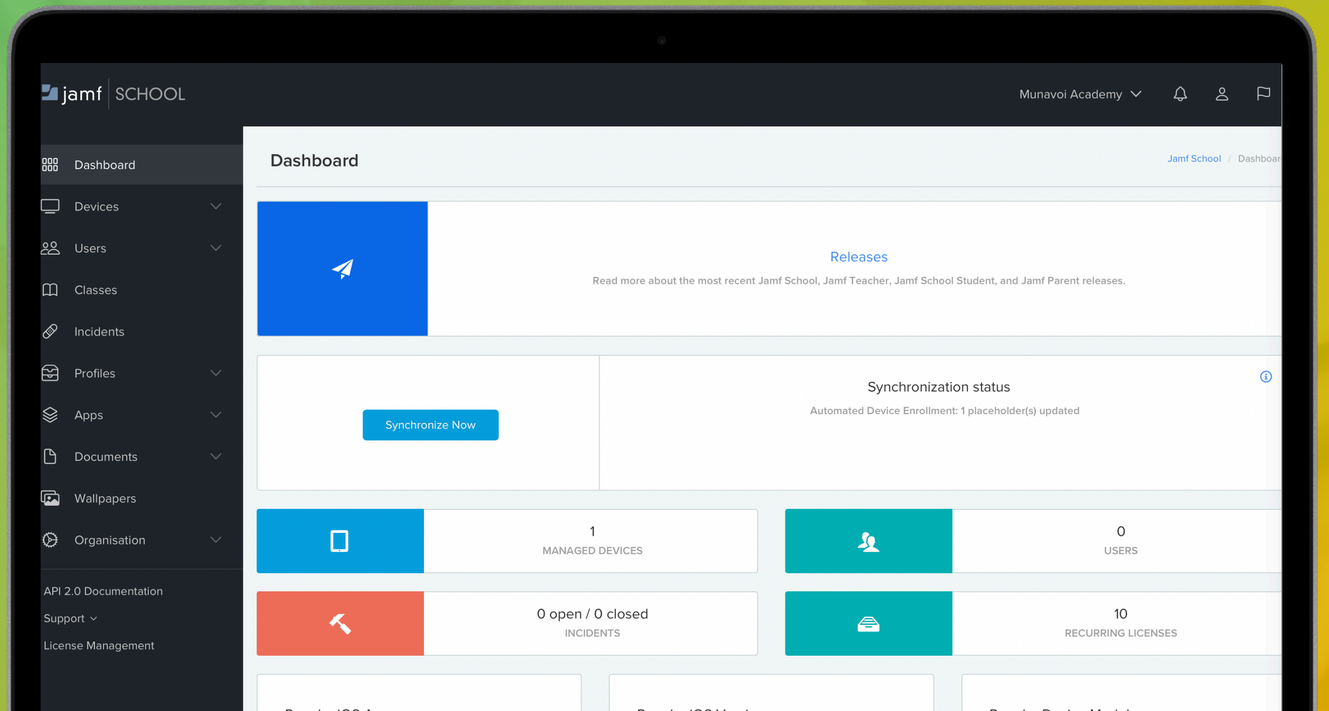
Ou

~~**Fin des mots de passe**~~

Réduction des mots de passe

Quelles solutions **MDM Jamf**?

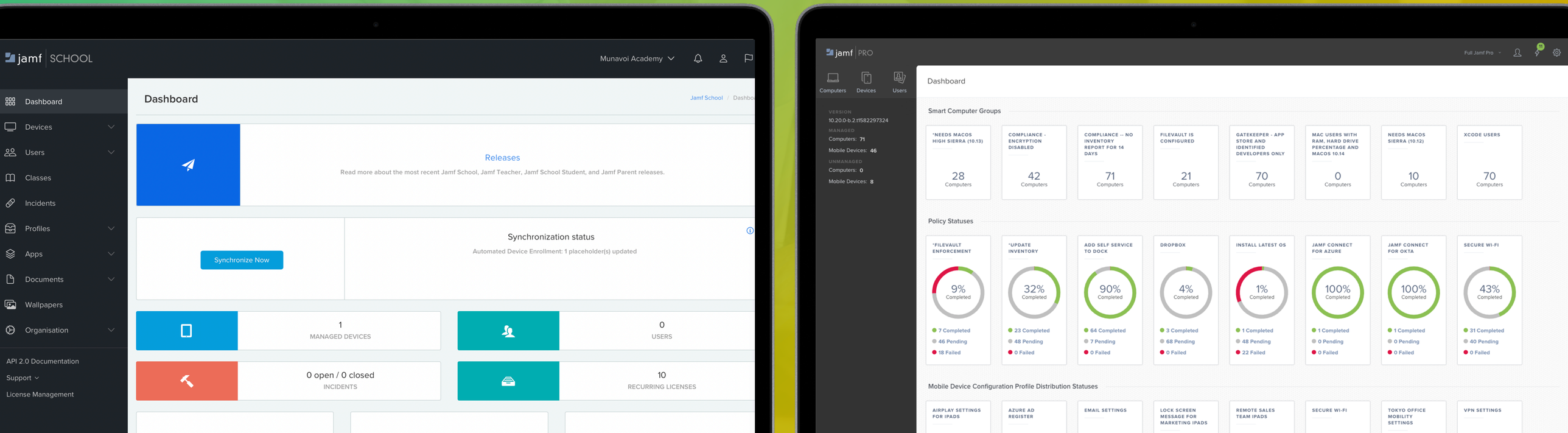
Jamf School



JAMF NATION LIVE

Quelles solutions **MDM Jamf**?

Jamf School ou Jamf Pro, peu importe !



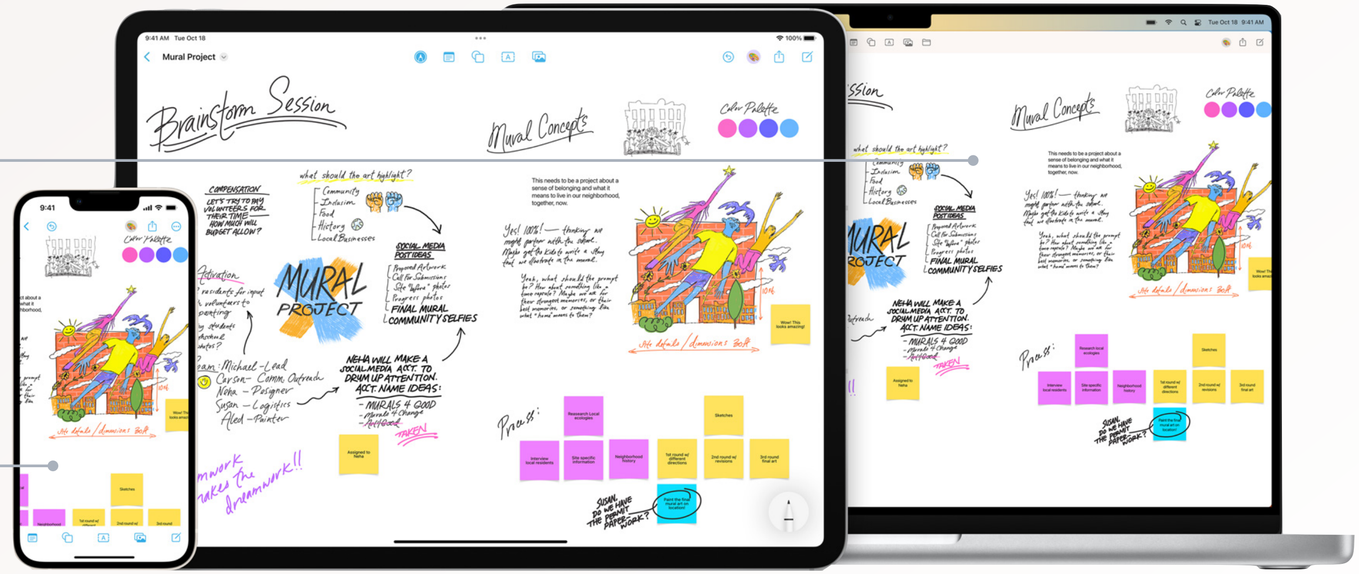
Toutes plateformes bienvenues

macOS

Utilisation du SSO sur Mac en laboratoire informatique

iOS and iPadOS

Éliminez la fatigue du mot de passe pendant le processus d'enrôlement



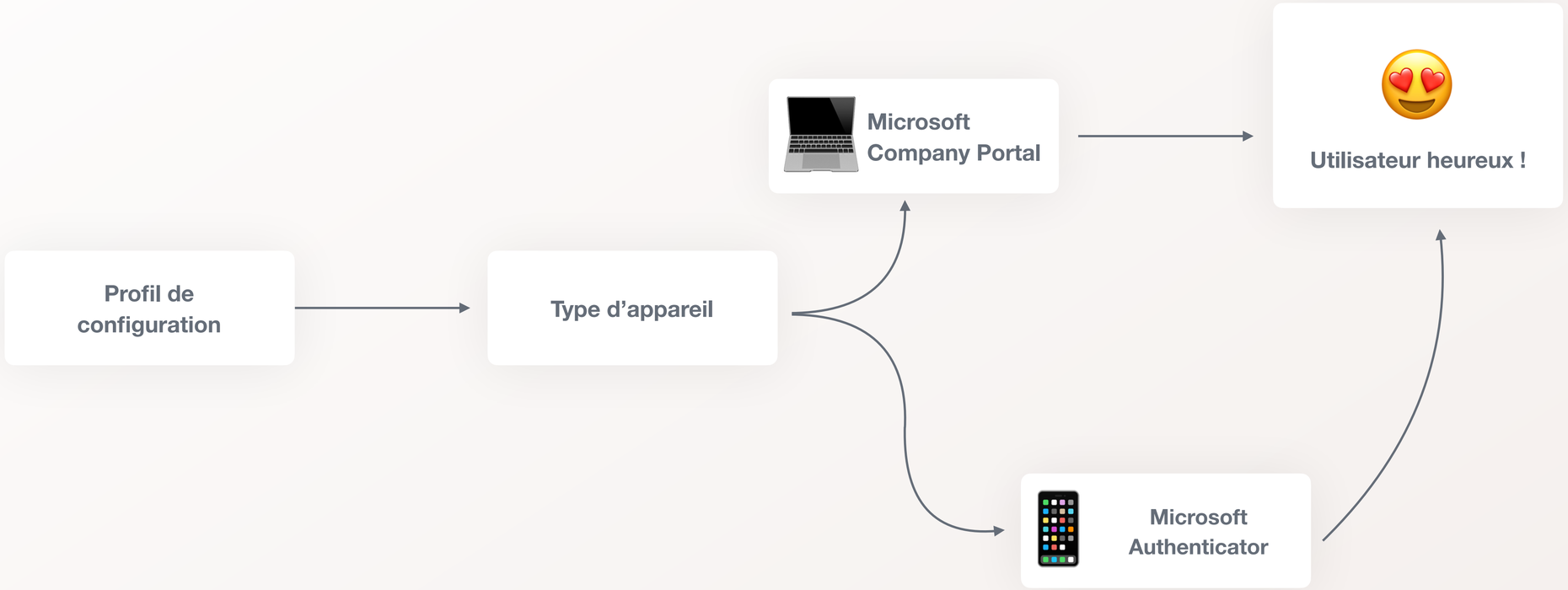
JAMF NATION LIVE

Prérequis à la mise en place du SSO

Les appareils **doivent** être enrôlés dans un **MDM**

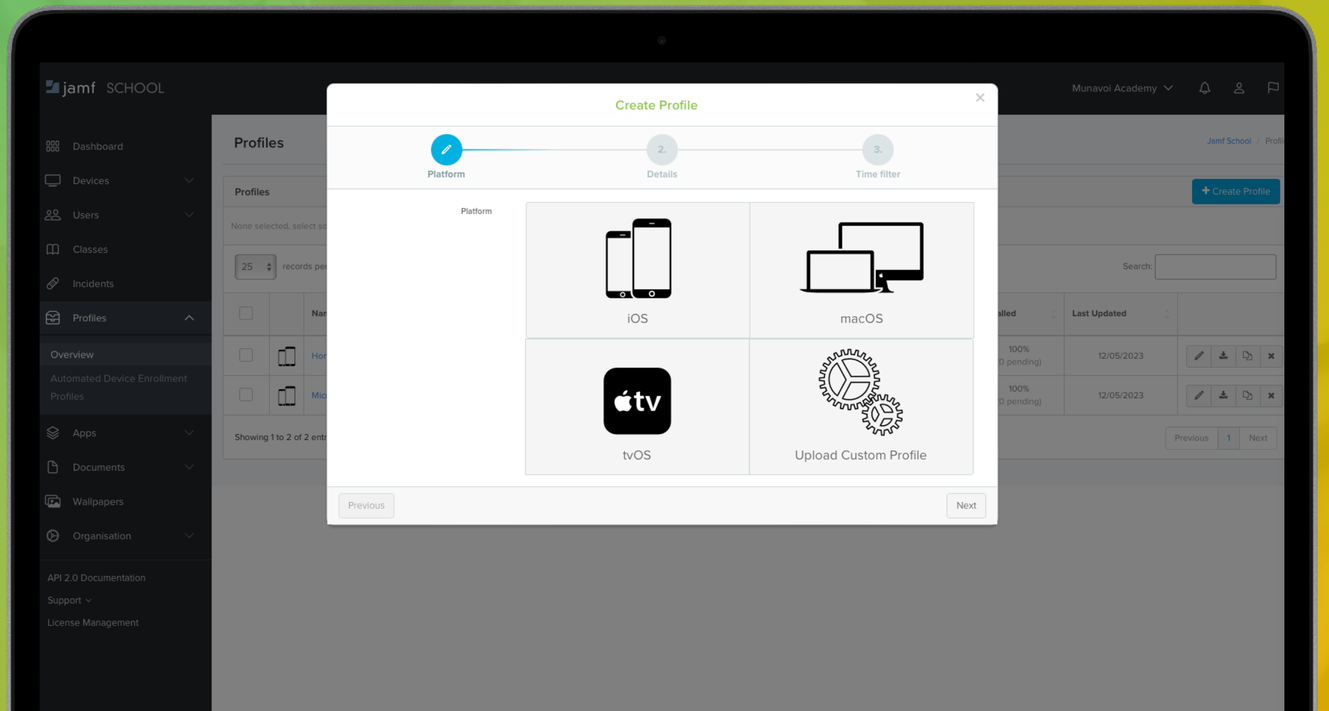
1. **iPadOS** 13 ou plus récent avec une app d’authentification
2. **macOS** 10.15 ou plus récent avec une app d’authentification
3. Un Profil de Configuration pour **l’extension SSO**

Prérequis au déploiement



Configuration

Devenez un héros du SSO en 4 étapes



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>
```

```
<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>
```

1

```
<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>
```

1

2

```
<string>Sso</string>
```

1

```
<key>Type</key>
<string>Redirect</string>
```

2

```
<key>ExtensionIdentifier</key>
<string>com.microsoft.azureauthenticator.ssoextension</string>
```

3

```
<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>
```

```
<string>Sso</string>
```

1

```
<key>Type</key>
<string>Redirect</string>
```

2

```
<key>ExtensionIdentifier</key>
<string>com.microsoft.azureauthenticator.ssoextension</string>
```

3

```
<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>
```

4

L’AUDIENCE EN CE MOMENT :

“Ola ça devient complexe !”

App Extension SSO

Remove

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

App Extension SSO 1

Remove

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

App Extension SSO

1

Remove

Sign-on type: Redirect

2

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

App Extension SSO

1

Remove

Sign-on type: Redirect

2

Extension Identifier: com.microsoft.azureauthenticator.ssoextension

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

3

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

App Extension SSO

1

Remove

Sign-on type: Redirect

2

Extension Identifier: com.microsoft.azureauthenticator.ssoextension

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

3

URLs:

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

+ −

4

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

Les 4 **étapes magiques**

Type de profil = SSO

Un profil nécessite toujours une charge utile (payload).

Sign-on type = Redirect

Méthode d’authentification. Microsoft nécessite l’option “Redirect”.

Extension Identifier = Authentication app bundle ID

Bundle ID de l’app d’authentification, ce paramètre est différent suivant la plateforme.

URLs = Dépendant de votre configuration côté IdP

URLs données par le fournisseur d’identité pour rediriger vers le SSO.

Single Sign-on Extensions

1 payload configured

Remove all | + Add

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/

+ Add

Single Sign-on Extensions

1 payload configured

Remove all | + Add

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

1

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

2

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

3

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.

4

- 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/

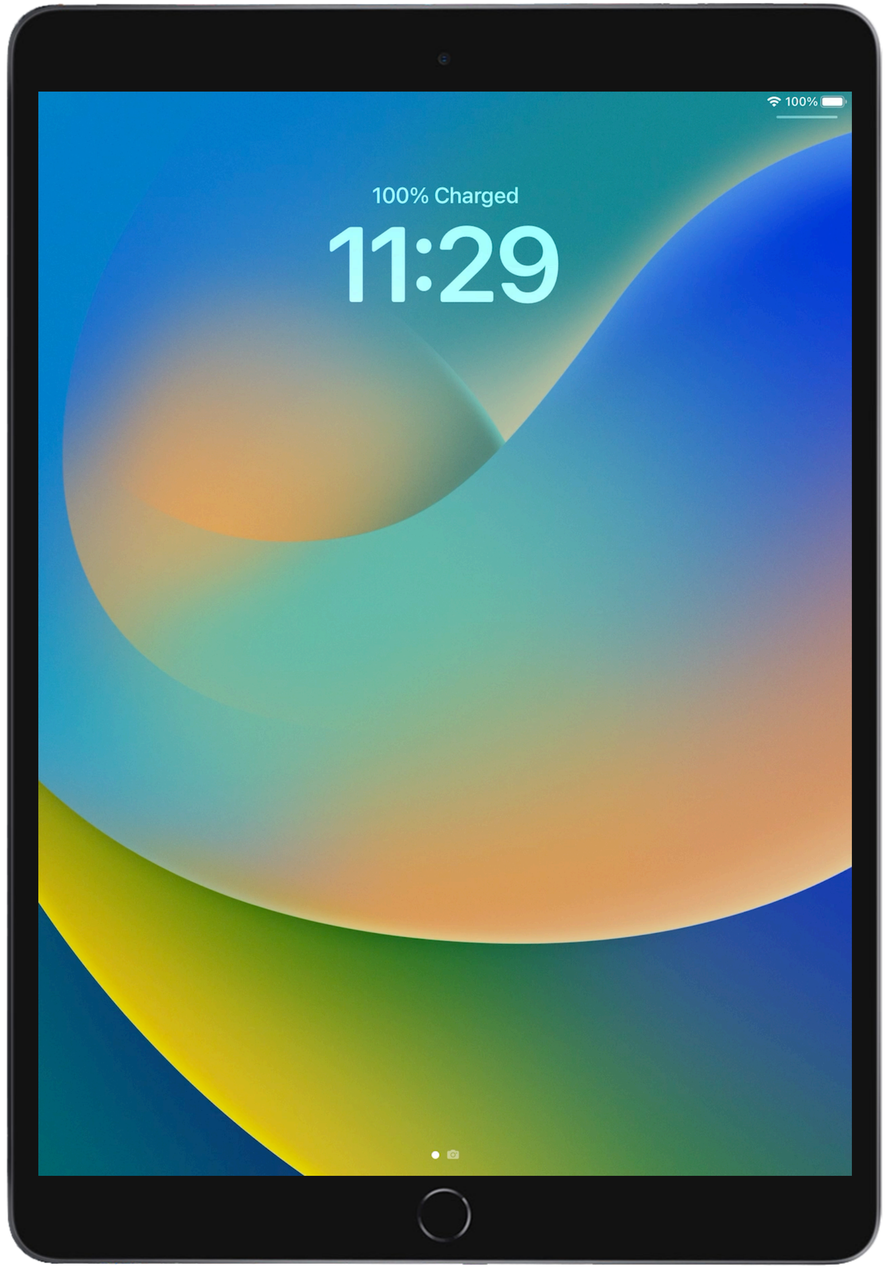
+ Add

L’AUDIENCE EN CE MOMENT :

“OK, mais à quoi ça ressemble côté utilisateur ?”

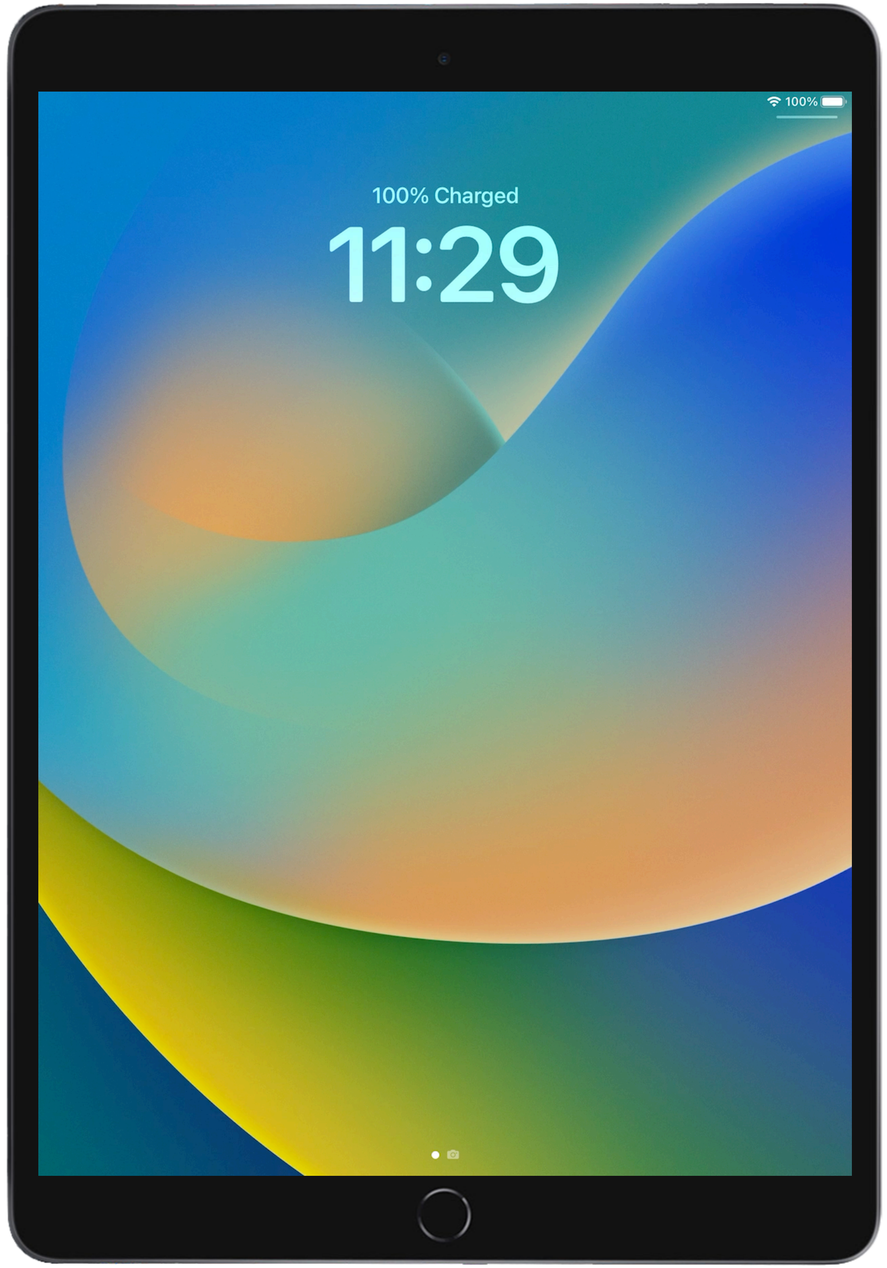
Exemples sur **iPad**

Sans SSO



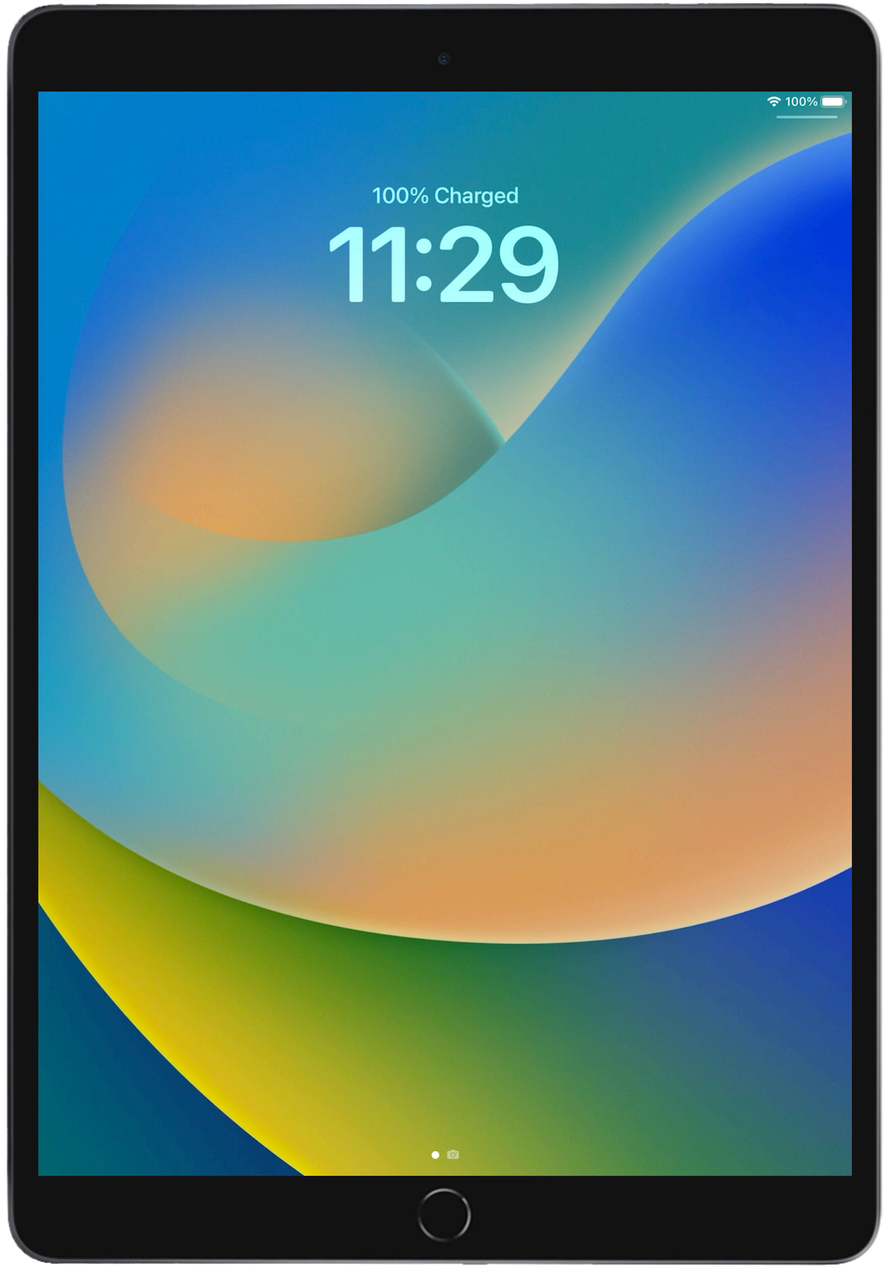
Exemples sur **iPad**

Sans SSO



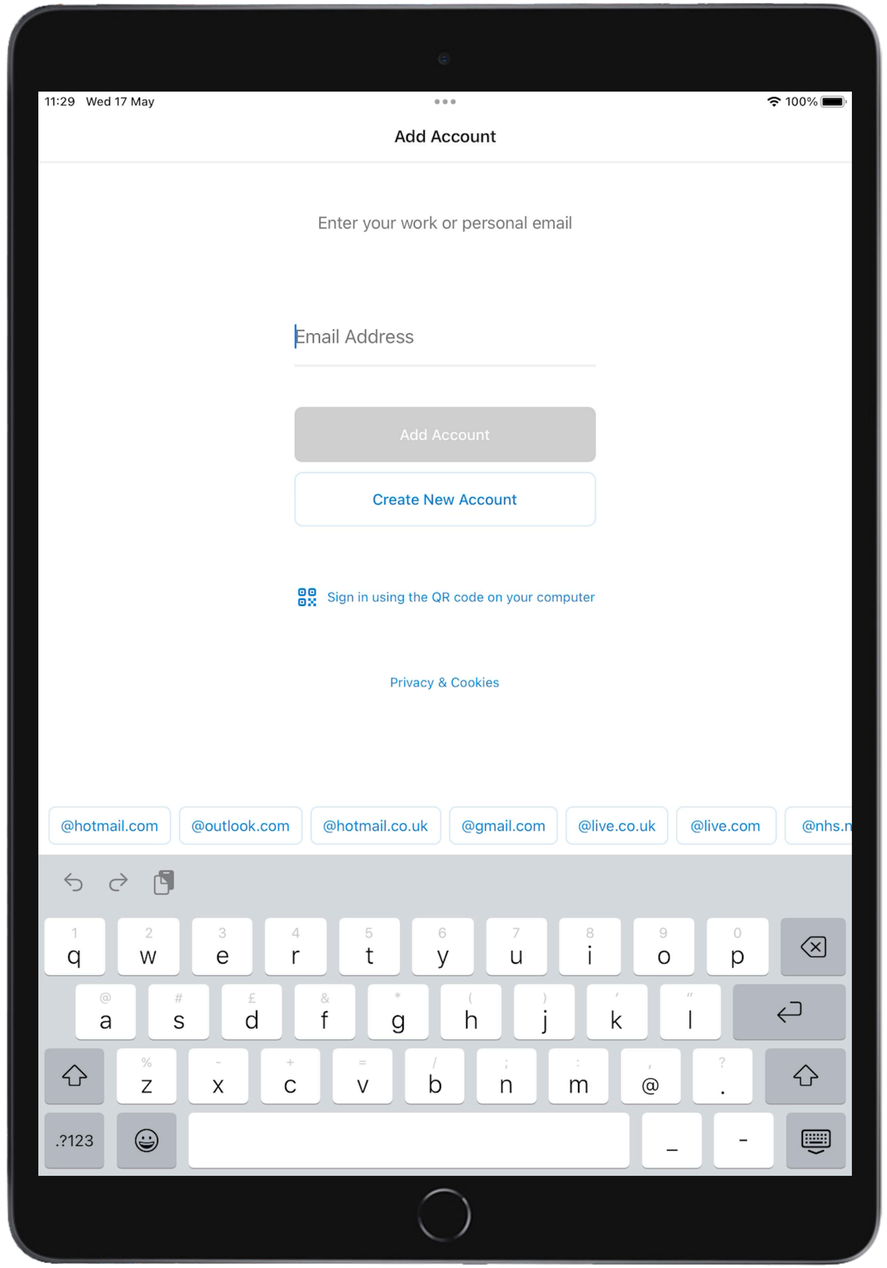
Exemples sur **iPad**

Sans SSO



Exemples sur **iPad**

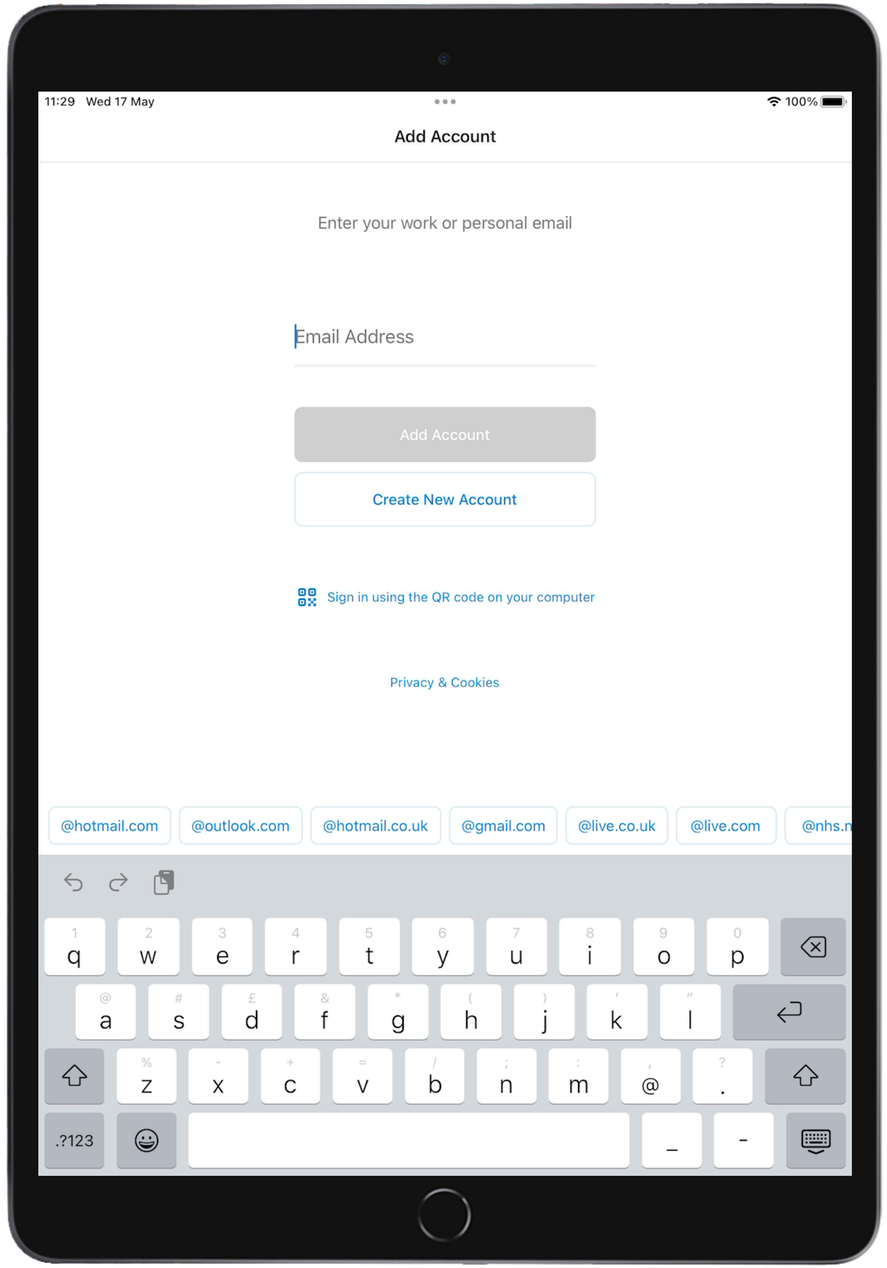
Sans SSO



JAMF NATION LIVE

Exemples sur **iPad**

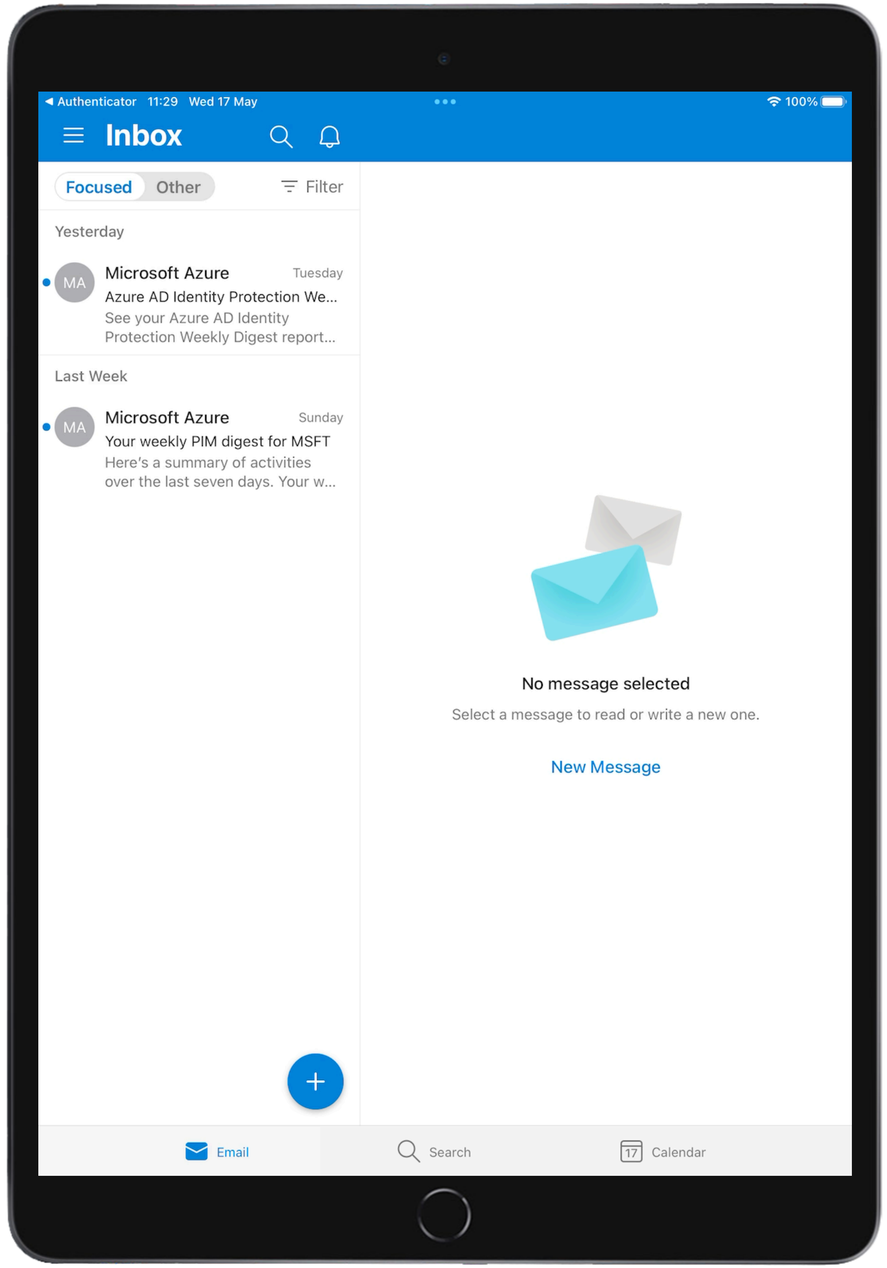
Sans SSO



JAMF NATION LIVE

Exemples sur **iPad**

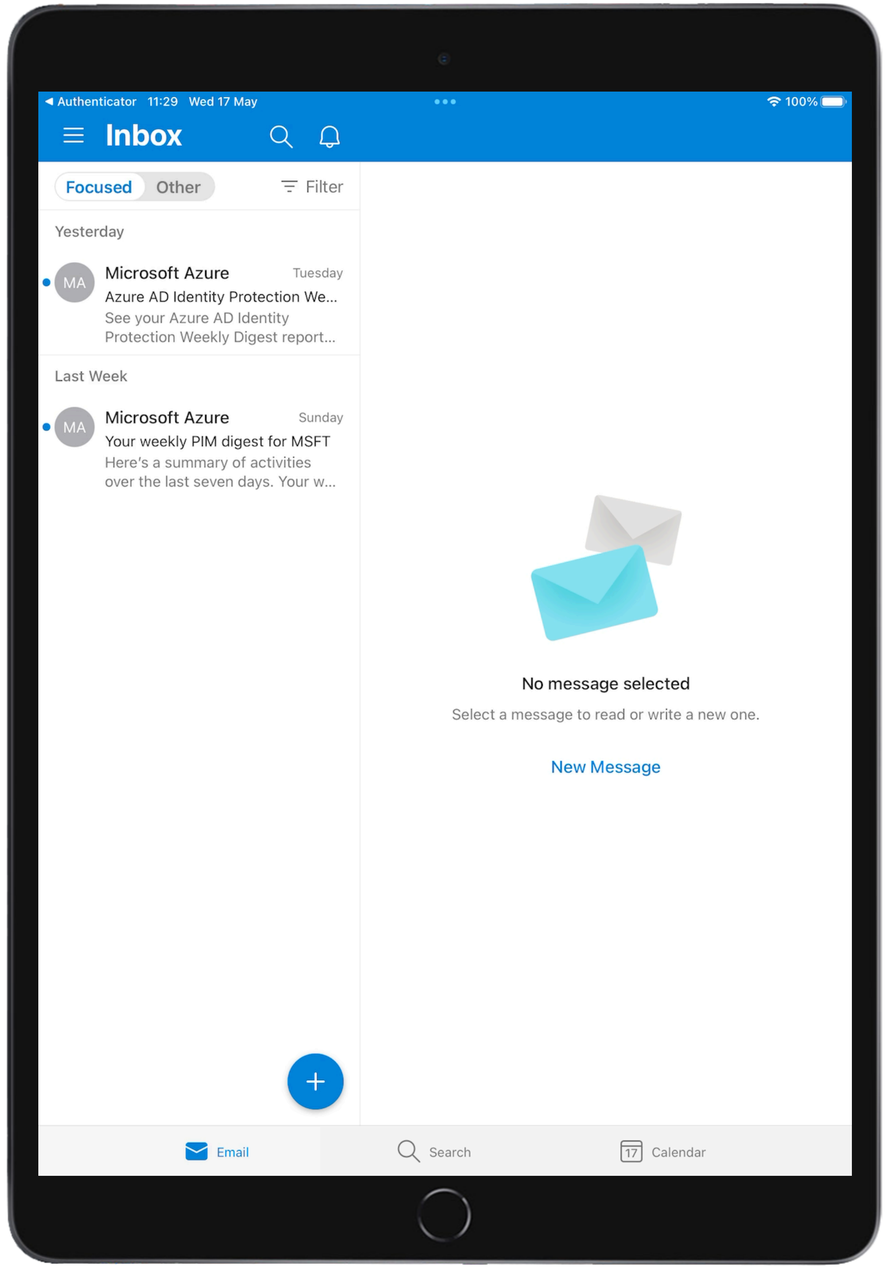
Sans SSO



Exemples sur **iPad**

Sans SSO

Microsoft Outlook ✅
Microsoft Authenticator ✅
portal.office.com ❌



JAMF NATION LIVE

Sans SSO

=

Plusieurs authentification nécessaires

Avec SSO

=

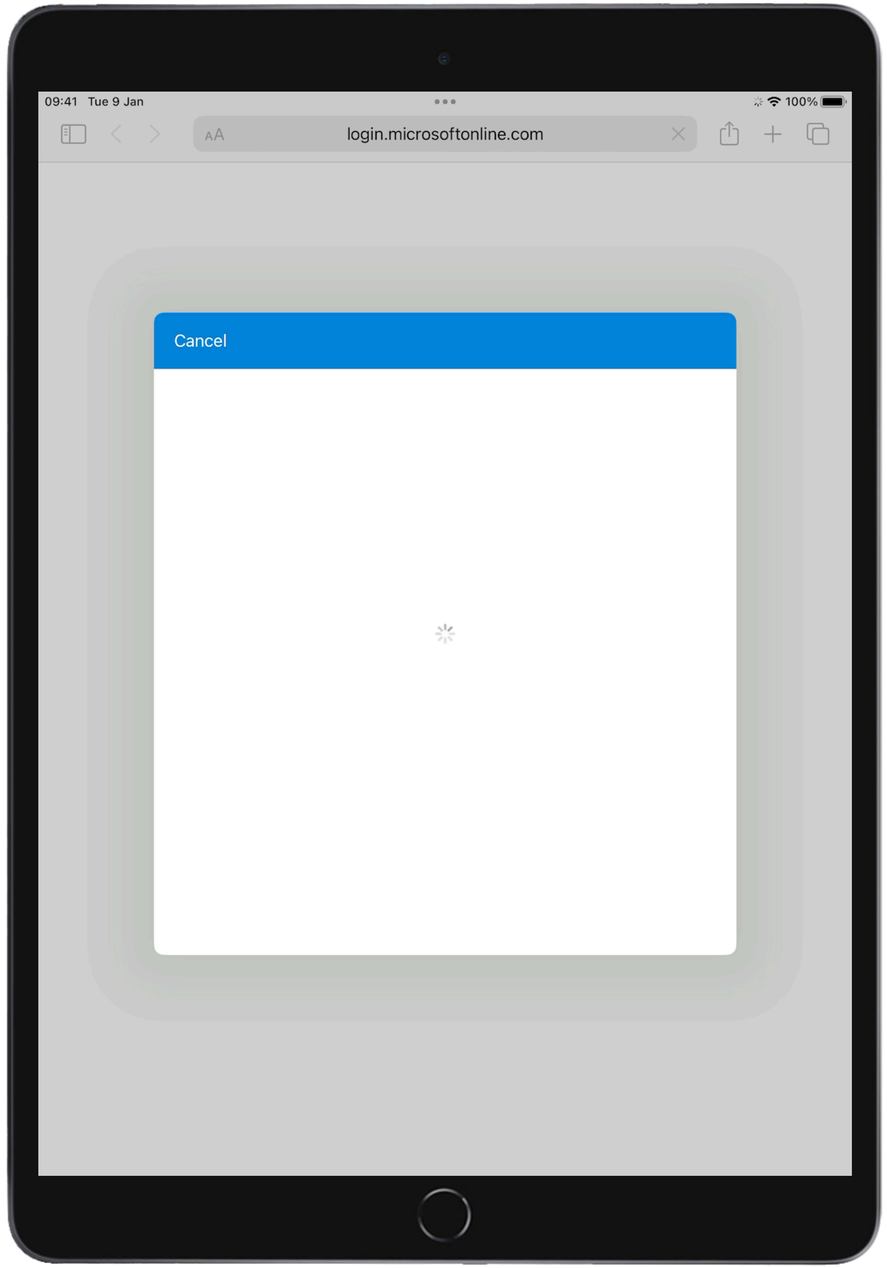
Une seule authentification nécessaire

Exemples sur **iPad**

Avec SSO

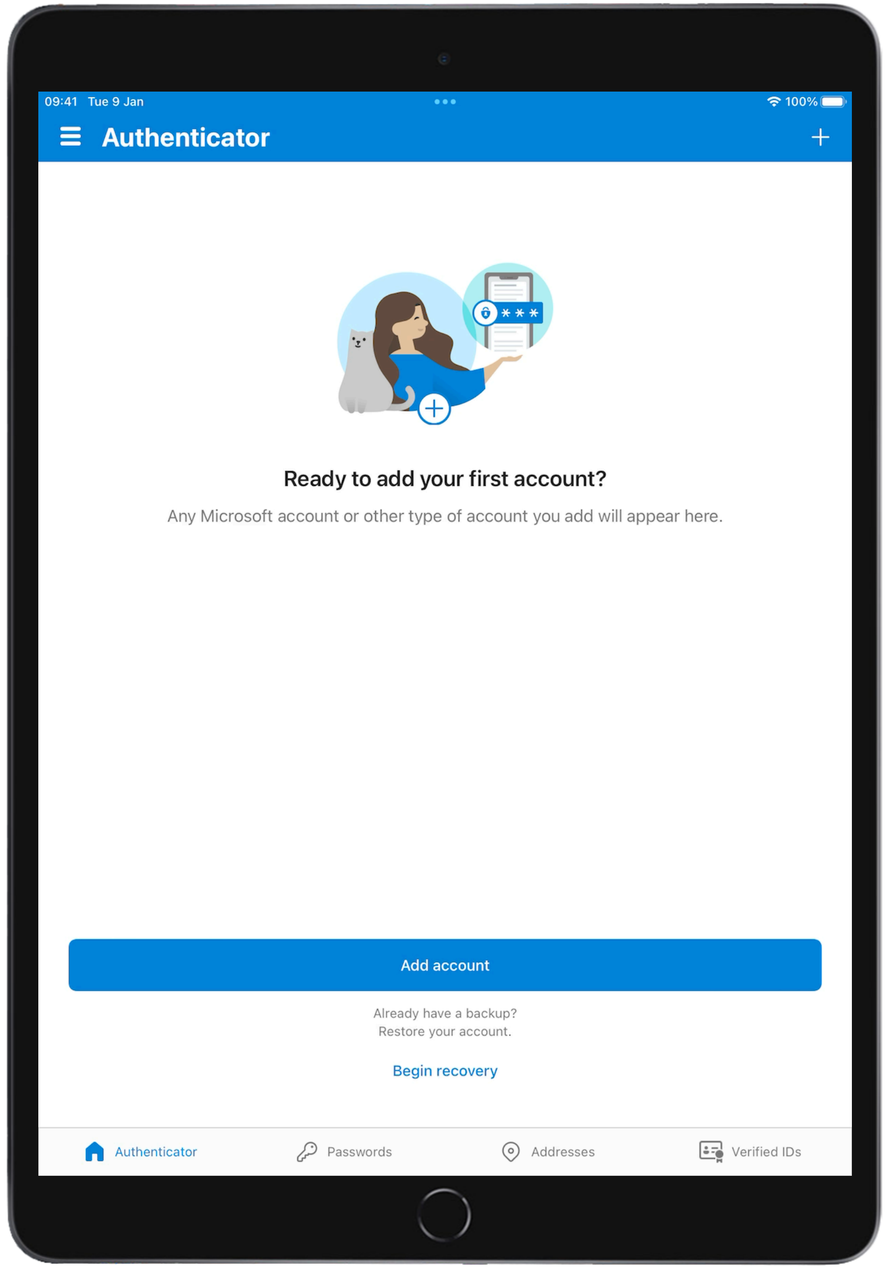
Exemples sur **iPad**

Avec SSO



Exemples sur **iPad**

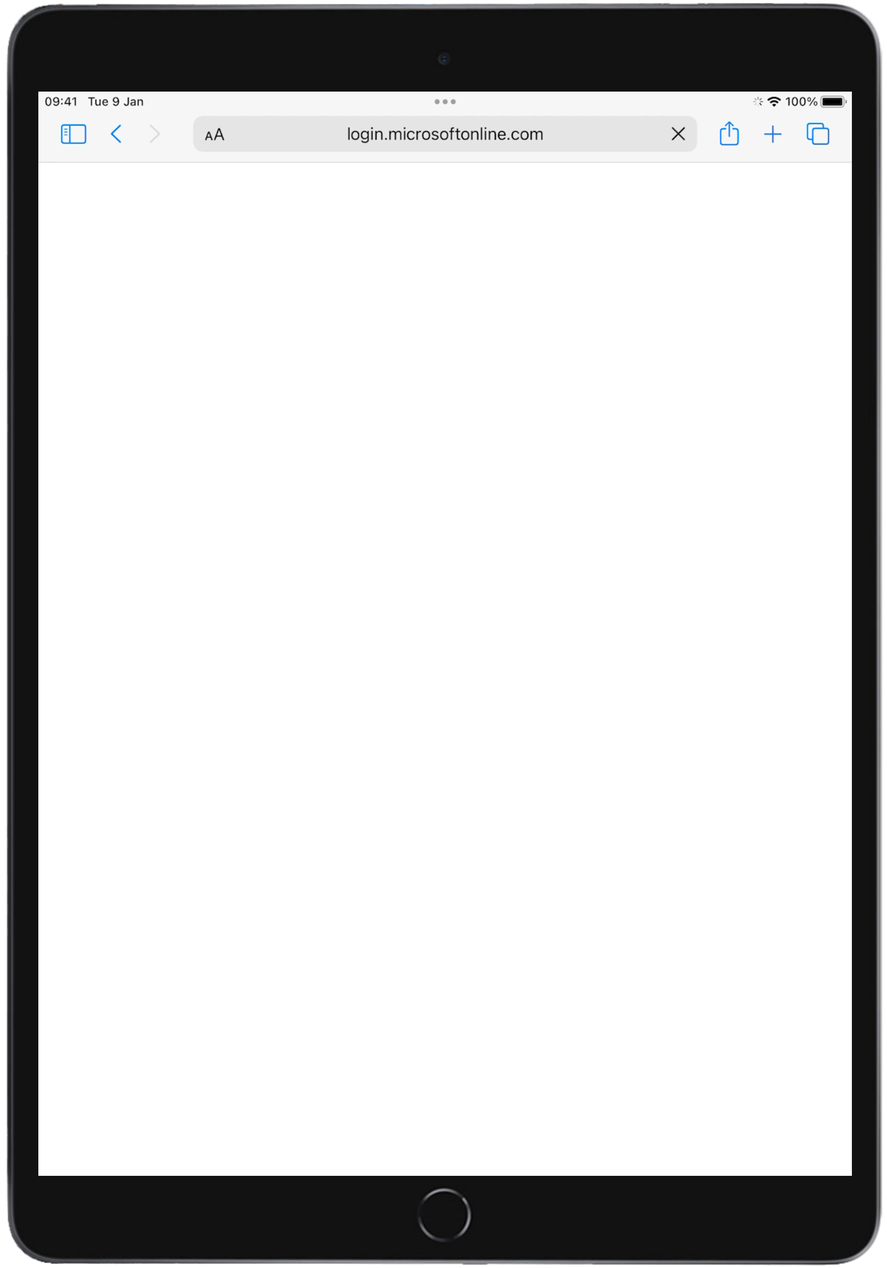
Avec SSO



JAMF NATION LIVE

Exemples sur **iPad**

Avec SSO



Sans SSO

=

Plusieurs authentification nécessaires

Avec SSO

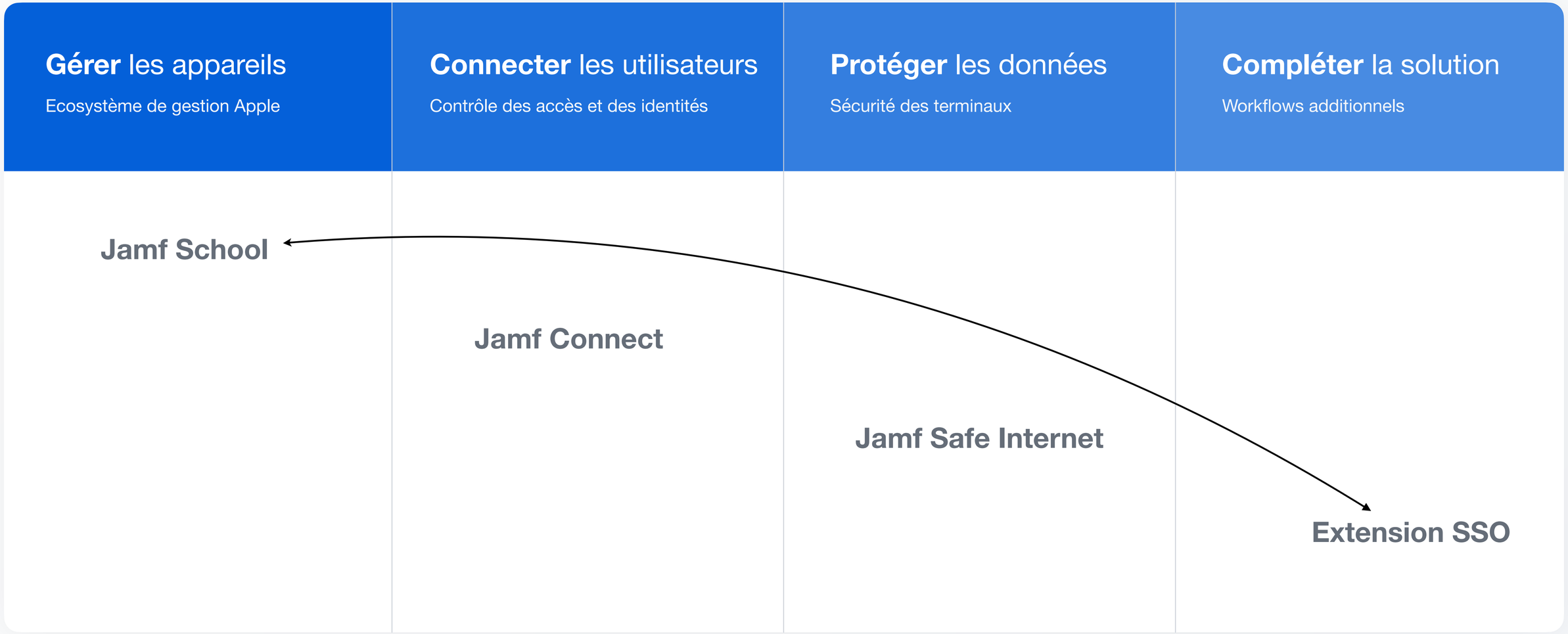
=

Une seule authentification nécessaire

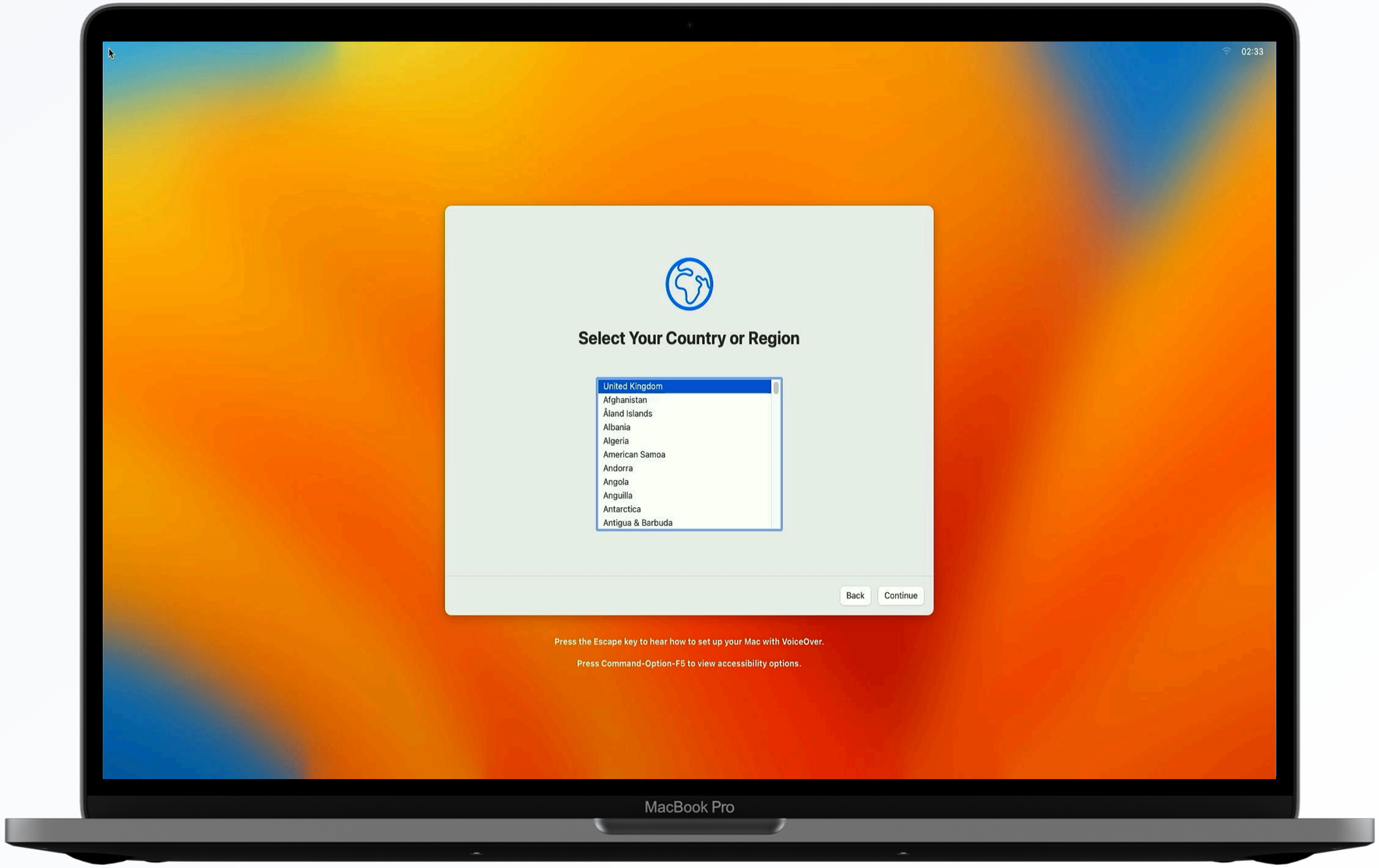
Workflows

Plateforme Jamf

Gérer les appareils	**Connecter** les utilisateurs	**Protéger** les données	**Compléter** la solution
Ecosystème de gestion Apple	Contrôle des accès et des identités	Sécurité des terminaux	Workflows additionnels



Plateforme Jamf

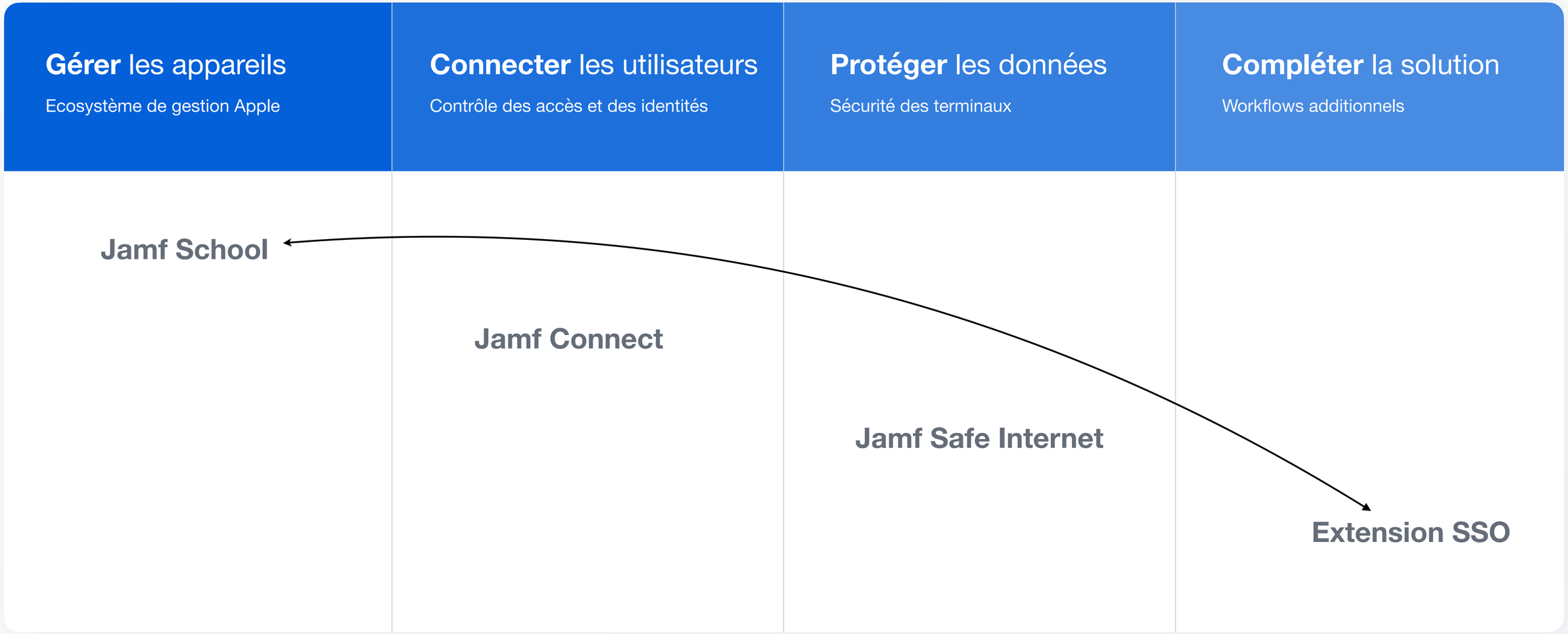


Plateforme Jamf

Plateforme Jamf

Plateforme Jamf

Gérer les appareils	**Connecter** les utilisateurs	**Protéger** les données	**Compléter** la solution
Ecosystème de gestion Apple	Contrôle des accès et des identités	Sécurité des terminaux	Workflows additionnels



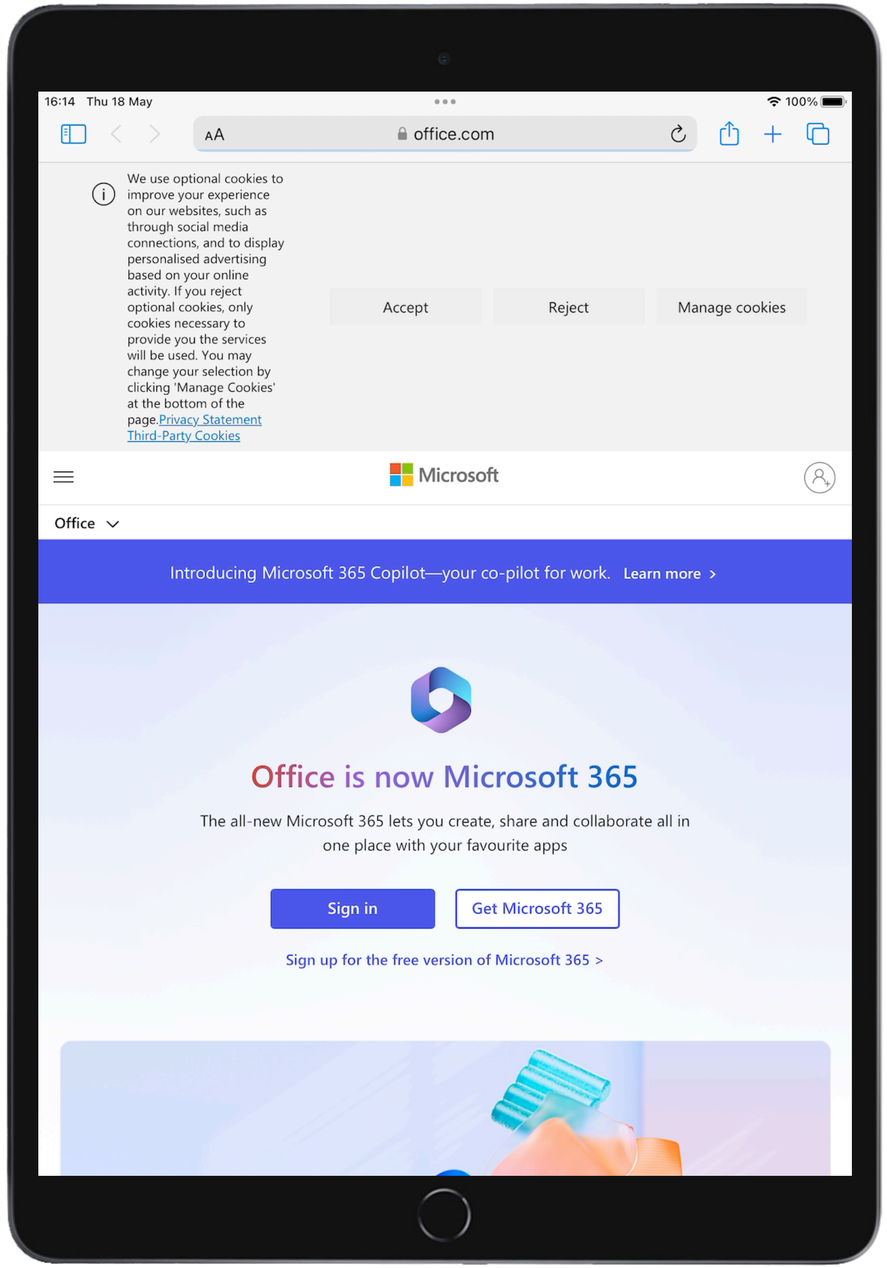
Remarques et Recommandations

“Il y a le bon SSO et le mauvais SSO”

Exemples sur **iPad**

Exemples sur **iPad**

portal.office.com ✅



Exemples sur **iPad**

portal.office.com ✅
Outlook 🤷‍♀️

Exemples sur **iPad**

portal.office.com ✅
Outlook 🤷‍♀️
Word ❌

Dois-t-on se ré-authentifier souvent malgré l'activation du SSO?

Ca dépend !

La configuration par défaut d'Azure Active Directory (Azure AD) pour la fréquence de connexion utilisateur est une fenêtre cumulative de 90 jours.
Demander des informations d'identification aux utilisateurs semble souvent une chose sensée à faire, mais celle-ci peut avoir l'effet inverse que celui prévu : les utilisateurs qui sont habitués à entrer leurs informations d'identification machinalement peuvent involontairement les fournir à une invite de demande d'informations d'identification malveillante.

Microsoft

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

Que ce passe-t-il quand un utilisateur met à jour son mot de passe ?

Il recevra devra se ré-authentifier.

Peut-on exclure une application ou un service de l'architecture SSO ?

Oui, il existe une option pour ça !

Bundle IDs des apps non autorisée à utiliser le SSO.

```
<key>AppBlockList</key>

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

Autoriser toutes les applications gérées à utiliser le SSO.

```
<key>Enable_SSO_On_All_ManagedApps</key>

<integer>1</integer>
```

Bundle IDs des apps autorisée à utiliser le SSO.

```
<key>AppAllowList</key>

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

Super, j’aimerais plus d’infos sur le sujet.

Pas de problèmes !

Articles, Guides et plus encore…

Rappel des 4 étapes magiques

Jamf, Apple & Microsoft ❤️

En résumé

Le **SSO** c’est bien

Sécurisé
Approuvé par l’IT
Unifié à travers les appareils Apple

Le **SSO** c’est simple

4 étapes de déploiement
1 processus d’enrôlement
Disponible dès aujourd'hui

Les **Utilisateurs** apprécient

Simple d’utilisation
S’intègre dans les process existants

Questions?

Merci

JAMF NATION LIVE