



# Déploiement nouveau MacOS

Connecter le Mac au réseau KACE jusqu'à indication contraire. S'il s'agit d'un laptop, utiliser l'adaptateur commandé avec le poste pour la connexion au réseau. A défaut, utiliser un adaptateur commun au bureau du pôle micro.

Pour un laptop, brancher l'alimentation sur secteur tout au long de la procédure.

## ▼ Définir le nom du poste

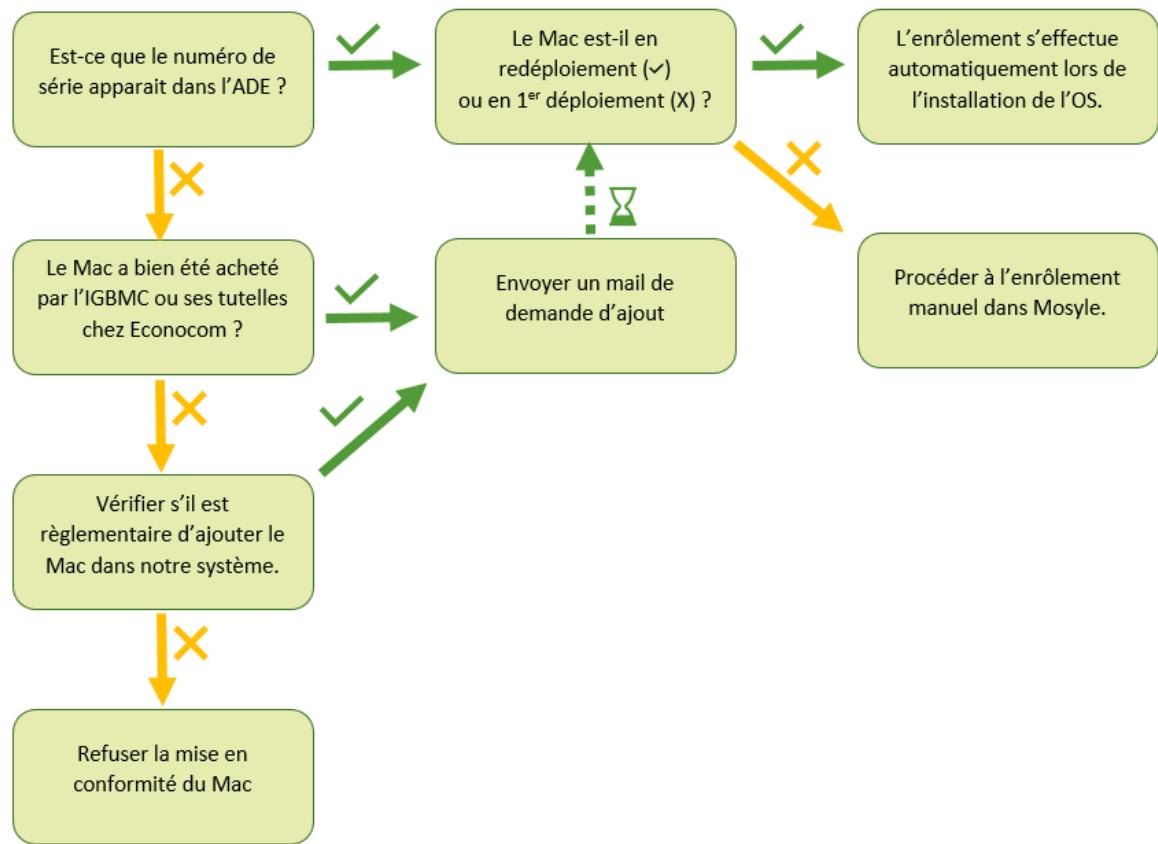
Suivre la procédure suivante :

Règle de nommage des postes de travail

Ce nom doit être **ajouté dans le titre du ticket** de suivi du redéploiement.

## ▼ Vérifier l'enregistrement dans l'ADE et Mosyle

Schéma décisionnel :



Les étapes de la procédure sont détaillées sur cette page :

#### Intégration d'un Mac dans Mosyle

### ▼ Installer l'OS

Le Mac est livré avec un OS préinstallé.

A noter : il est **impossible** d'installer un OS antérieur à celui avec lequel le Mac est livré.

### ▼ Paramétrages à l'ouverture

A la fin de l'installation du système d'exploitation :

- De manière générale, refuser la localisation du poste et le partage de données pour l'amélioration.
- Le fuseau horaire doit être défini manuellement (et non en fonction de la localisation du poste, qu'il faut refuser) et impérativement sur "Paris, Madrid".
- Définir la langue du texte et du clavier : français ou anglais exclusivement.

Sur un MacBook on prendra la langue du clavier impérativement.

Pour un iMac c'est en fonction de l'utilisateur ou du clavier commandé avec le poste.

Le changement de langue et de clavier est bien géré sur Mac, il sera donc possible de faire ce changement pour la session utilisateur ultérieurement.

- Créer le compte d'administration du poste :
  - Login = administrateur (sans majuscule)
  - Mot de passe spécifique au compte à récupérer dans le fichier Keepass "liste-mdp".
  - Pas d'indice de mot de passe.

## ▼ Rechercher les mises-à-jour

Dès que la session administrateur est ouverte, rechercher si des mises à jour sont disponibles pour le système choisi.

- **Pour un système MacOS 12 Monterey et antérieurs :**

Aller dans les "Paramètres Système" (via l'icone grise en roue dentée dans le Dock, ou via le Menu Pomme), puis ouvrir la rubrique "Mise à jour de logiciels".

- **Pour un système MacOS 13 Ventura et ultérieurs :**

Aller dans les "Réglages Système" (via l'icone grise en roue dentée dans le Dock, ou via le Menu Pomme), ouvrir la rubrique "Général", puis "Mise à jour de logiciels".

Si un OS supérieur mais non-supporté par le Service informatique est proposé, chercher un lien vers "autres mises à jour" pour accéder aux mises à jour du système en place.

Les mises à jour de l'OS et de Safari sont à installer.

Une fois les mises à jour installées, redémarrer le poste.

## ▼ Mise en conformité

### ▼ Définition en local du nom choisi pour le poste

Ouvrir le Terminal : Menu Aller > Utilitaires > Terminal

Exécuter les commandes suivantes : **Toutes les lettres doivent être en majuscule.**

```
sudo scutil --set ComputerName $nomdumac  
sudo scutil --set LocalHostName $nomdumac  
sudo scutil --set HostName $nomdumac
```

Puis redémarrer.

▼ (hors procédure)

Exécuter le script de nommage avec cette commande :

```
sudo sh stock/MAC/Scripts/ajout-nom_ordinateur.sh
```

Lorsque le script le demande, entrer le nom choisi pour le Mac dans l'étape précédente "Définir le nom du poste". **Toutes les lettres doivent être en majuscule.**

Enfin, lorsque le script demande s'il faut redémarrer, entrer "Y" et valider.

▼ **Seulement si le Mac est doté d'une puce Apple Silicon (type M1, M2 ou M3 et M4) : installer Rosetta 2**

Ouvrir le Terminal : Menu Aller > Utilitaires > Terminal

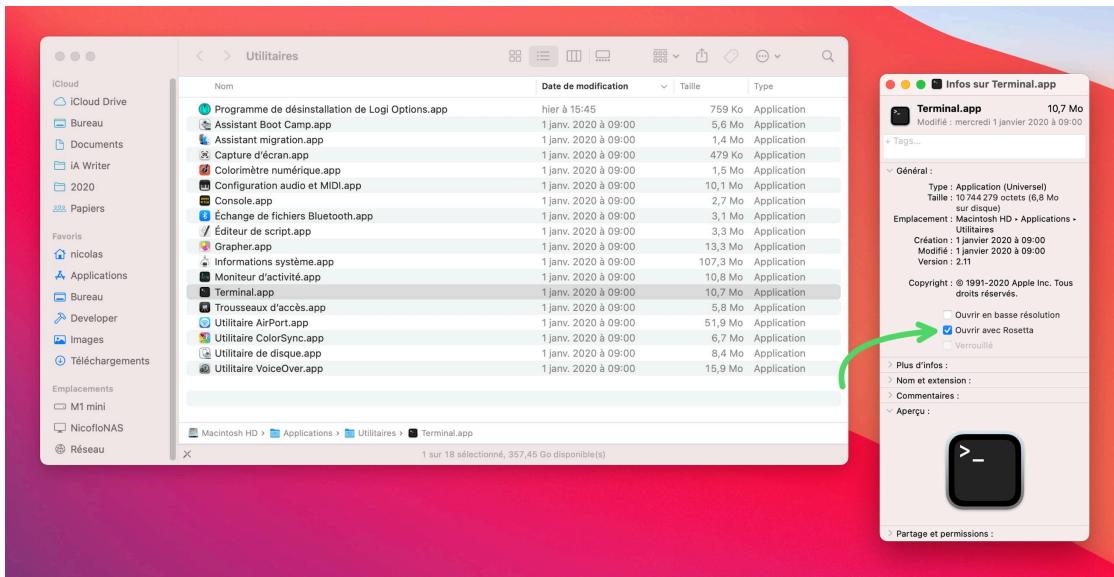
Entrer et valider la commande suivante

```
sudo softwareupdate --install-rosetta
```

Quitter le Terminal : Menu Terminal > Quitter Terminal ; ou par le raccourci clavier : ⌘q

Dans le Finder, sélectionner l'application Terminal, puis ouvrir les informations avec le raccourci ⌘I (ou control-clic pour ouvrir le menu contextuel > Lire les informations).

Dans la fenêtre d'infos, cocher "ouvrir avec Rosetta".



**Attention depuis Sonoma (MacOS 14) il faut recocher "ouvrir avec rosetta" pour le terminal dans chaque session**

## ▼ Monter le lecteur réseau Stock

Ouvrir le Terminal : Menu Aller > Utilitaires > Terminal

Entrer et valider la commande suivante :

```
mkdir stock
```

Cette commande crée un dossier vide à la racine de l'utilisateur administrateur et le nomme "stock". Il sert ensuite de point de montage pour le lecteur réseau "stockage-micro/stock", qu'on monte avec la commande suivante :

```
mount_smbfs "//igbmc;USER@stockage-micro.igbmc.u-strasbg.fr/stock" stock
```

**⚠ Remplacer USER par son login IGBMC.**

## ▼ Scripts de configuration et installation du Pack de base d'applications

Ouvrir le Terminal : Menu Aller > Utilitaires > Terminal

Monter le lecteur réseau Stock (voir plus haut pour les instructions).

Entrer et valider les commandes suivantes :

```
sudo sh stock/MAC/Scripts/0config-catalina.sh
```

```
sudo sh stock/MAC/Scripts/install-imprimante.sh
```

```
sudo sh stock/MAC/Installation_Silencieuse/install-packBASE-sonoma.sh
```

- Choisir ensuite la langue en saisissant **en** ou **fr**
- Le pack de base appelle les scripts d'installation des logiciels suivants : "Java RE" "KACE\_Agent" "HP" "Office2021" "VLC" "Remote\_Desktop-latest".

Ensuite, redémarrer le poste.

## ▼ Mise à jour de la fiche d'inventaire du poste sur KACE K1000

L'agent Kace vient d'être installé : il faut vérifier que le périphérique remonte bien. Dans la fiche d'inventaire, attribuer au poste un emplacement et une date de livraison.

## ▼ S'il s'agit d'un Mac sous MacOS 15 Sequoia

Dans le Terminal en administrateur, entrer et valider la commande suivante :

```
sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist PrivateMACAddressModeSystemSetting -int 1
```

Puis redémarrer.

# ▼ Vérifications

## ▼ Présence de l'Agent Kace, remontée d'inventaire, fiche d'Actif

- Le poste doit remonter dans KACE > Inventaire > Périphériques

Si le poste n'apparaît pas, imposer un inventaire forcé avec cette commande :

```
sudo /Library/Application\ Support/Quest/KACE/bin/runkbot 1 0
```

Attendre 3 à 5 minutes pour que le poste remonte dans la liste des Périphériques.

- Vérifier que l'**emplacement** et la **date de livraison** du poste sont renseignés dans sa fiche d'Actif.
- L'icone de l'Agent Kace doit apparaître en vert dans la Barre de Menus.

Si l'icone est rouge au lieu de verte, ouvrir le menu déroulant et faire redémarrer l'agent.

▼ Si la remontée d'inventaire ne fonctionne pas (pb rencontré sur la dernière version de l'agent 13.2.23 associée à la dernière version de Ventura 13.6.3 sur Mac M2) > Appliquer cette médecine :

#### Essayer de réinstaller l'agent :

- Supprimer l'entrée dans k1000 si elle existe.
- `sudo /Library/Application\ Support/Quest/KACE/bin/AMPTools uninstall all-kuid`
- `sudo reboot`

Réinstaller avec l'agent téléchargé depuis la console k1000 dans Settings > Provisionning > Update Agent Settings.

Essayer un runkbot : `/Library/Application\ Support/Quest/KACE/bin/runkbot 1 0`

Si infructueux : Vérifier que le service konea est en cours d'exécution :

```
ps aux | grep konea
```

Vous devriez avoir un résultat du genre :

```
root      47404  0,0  0,1 410099600  7888 ?? Ss  11:12
0:00.61 /Library/Application Support/Quest/KACE/bin/konea
root      50483  0,0  0,0 408637136  1520 s000 S+  12:
09  0:00.01 grep konea
```

Si le processus konea est manquant, vous pouvez essayer de l'exécuter manuellement avec un `/Library/Application\ Support/Quest/KACE/bin/konea`

Une fois le processus actif essayez de faire un `runkbot 10` pour voir si le poste remonte dans l'inventaire.

Si après redémarrage le service konea ne se lance toujours pas > appliquez la procédure suivante :

Verifiez que le `konea.plist` se trouve au bon emplacement avec les bonnes permissions :

```
sh-3.2$ ls -lah /Library/LaunchDaemons/kon*
rw-r--r-- 1 root wheel 479B May 31 09:12 /Library/LaunchDae
mons/konea.plist
```

Ensuite, demandez au système de charger le démon et de l'exécuter tant que la machine est active, puis vérifiez :

```
sh-3.2$ sudo launchctl load -w /Library/LaunchDaemons/kon
ea.plist
```

```
sh-3.2$ sudo launchctl list | grep konea
```

## ▼ Bonne jonction au domaine IGBMC

Deux vérifications sur ce point :

- L'objet au nom du poste s'est bien créé dans l'ActiveDirectory, il est actif et il se situe dans l'OU Postes > Mac.

La création est automatique, mais il faut laisser au moins 30 minutes après la création de la fiche du poste dans KACE pour que le script crée le nouvel objet ordinateur.

- Le domaine IGBMC apparaît dans :

- **Pour un système MacOS 12 Monterey et antérieurs :**

Préférences Système > Utilisateurs et groupes > Options >  
Compte serveur réseau

- **Pour un système MacOS 13 Ventura et ultérieurs :**

Réglages Système > Utilisateurs et Groupes

Au bas de cette page, dans la rubrique "Serveurs de comptes réseau", IGBMC doit apparaître avec un point vert.

- En remédiation, si l'un et/ou l'autre des points à vérifier n'est pas bon, exécuter cette commande dans le Terminal :

```
sudo sh stock/MAC/Scripts/domain.sh
```

Reprendre ensuite les 2 vérifications et si ce n'est toujours pas résolu, faire la commande suivante **ET** relancer à nouveau le script "domain.sh" comme précédemment.

```
dsconfigad -force -remove -u johndoe -p nopasswordhere
```

## ▼ Applications Microsoft Office

- Lancer l'application Word et ouvrir un document vierge.
- Si un bandeau jaune indique que des mises à jour sont disponibles, cliquer sur le lien affiché.

Appliquer l'ensemble des mises à jour proposées par AutoUpdate, et cocher la case "maintenir les applications à jour sur cet appareil".  
Quitter Word.

Dans le cas où les mises à jour sont en échec de manière répétée :

- Aller sur le site <https://office-reset.com> et télécharger l'utilitaire "Microsoft\_Office\_Reset\_1.9.1.pkg".
- Lancer l'utilitaire, à l'étape "Type d'installation", cocher "Réinitialiser AutoUpdate", et Continuer.
- Une fois que la réinitialisation est terminée, relancer les mises à jour de la suite Office.
- Si un compte Microsoft est demandé à l'ouverture de l'application, quitter toute les applications Office. Ouvrir un Terminal et exécuter cette commande :

```
sudo sh stock/MAC/Installation_silencieuse/Office2021/fix-activation.sh
```

Vérifier que le problème est résolu en ouvrant à nouveau une application Office.

## ▼ Présence active de Cortex

L'icone Cortex est présente dans la Barre des Menus, et en ouvrant la Console dans ce menu déroulant, l'état est "Protected".

Si ce n'est pas le cas :

- Vérifier que Mosyle a bien déployé le profil Cortex, sinon réappliquer le profil.
- Réappliquer l'installation infogérée par Kace :  
serv-k1000 > Distribution > Installations infogérées > RIP - MAC - Cortex >  
ajouter le périphérique dans le champ "périphériques" puis cliquer sur "Exécuter maintenant".

## ▼ Bascule sur le réseau interne

- ▼ Dans le cas d'un iMac disposant d'une carte réseau interne :

Simplement connecter l'appareil sur le réseau normal, et vérifier qu'il ne bascule pas sur le réseau invité (vlan 38), mais **bien sur l'interne (vlan 37)**.

- ▼ Dans le cas d'un MacBook connecté avec l'adaptateur fourni par l'utilisateur :

Récupérer l'adresse MAC de l'adaptateur en allant dans Réglages Système > Réseau > \$Nom de l'adaptateur connecté\$ > Détails > Matériel > Adresse MAC

Copier cette adresse dans un bloc-note, et passer les lettres minuscules en majuscules.

Se connecter sur la page KACE > Gestion des actifs > Actifs, et rechercher l'adresse MAC.

- Si la recherche donne un résultat, l'adaptateur est déjà enregistré. Ouvrir sa fiche d'actif et vérifier que les champs sont correctement complétés.
- Si la recherche ne donne pas de résultat, suivre la procédure d'enregistrement sur cette page :

### KACE - Ajout d'un adaptateur réseau

- ▼ Dans les autres cas :

Garder le poste connecté au réseau KACE (vlan 69) et ouvrir une session avec son compte, puis se connecter sur le wi-fi "IGBMC". Si cette connexion est effective et stable, le test est réussi. Fermer cette session puis supprimer cet utilisateur. L'étape d'ouverture de session de test peut être sautée.

- Pour un système **macOS 15 Sequoia**, il faut désactiver Private Wi-fi Address par script

```
sudo defaults write /Library/Preferences/SystemConfiguration/co  
m.apple.airport.preferences.plist PrivateMACAddressModeSyste  
mSetting -int 1
```

▼ Pistes à vérifier en cas de problème :

Vérifier que l'objet poste n'est pas désactivé dans l'ActiveDirectory, et se trouve dans l'OU Postes > Mac

En ouvrant les propriétés de l'objet, dans l'onglet "Membre de", vérifier si un groupe "NAP-AUTO" figure dans la liste.

Vérifier que l'adresse MAC (de la carte réseau ou de l'adaptateur) n'est pas désactivée dans l'OU Nap.

## ▼ Ouverture d'une session test avec compte du domaine

- Le poste doit être connecté sur le réseau interne (et non sur le vlan69).
- Déconnecter la session administrateur.
- Sur la page d'ouverture de session, choisir "autre", entrer son login et mot de passe IGBMC.
- Si la session s'ouvre, le test est réussi.
- Supprimer ce compte.

## ▼ Supprimer entièrement une session pour un système MacOS 13 Ventura et ultérieurs

- Ouvrir la session administrateur.

- Ouvrir les Réglages Système, rubrique "Utilisateurs et groupes"
- Cliquer sur l'icône "i" sur la ligne du compte à supprimer
- Dans la fenêtre de détail du compte, cliquer sur "supprimer ce compte"
- Saisir les identifiants administrateur
- Dans la fenêtre de confirmation, choisir "supprimer le dossier de départ"

## ▼ Prise en main et contrôle à distance

- Le Mac en cours de préparation doit être connecté au réseau interne (vlan 37).

Le réseau KACE (vlan 69) peut être utilisé s'il n'y a pas de prise réseau sur l'iMac, ou si on ne dispose pas de l'adaptateur lié à la machine dans le cas d'un MacBook.

- A partir d'un mac du service informatique connecté au réseau interne ou au réseau KACE, lancer l'application Partage d'écran (Finder > Applications > Utilitaires > Partage d'écran).
- Cliquer sur l'icône "+"
- Dans la nouvelle fenêtre, entrer le nom du poste. L'adresse IP actuelle du poste visé est aussi une possibilité.
- Dans la nouvelle fenêtre, entrer l'identifiant administrateur et son mot de passe.
- Choisir "Partager le moniteur". Cette option permet d'entrer dans la session de l'utilisateur, on voit donc la même chose que l'utilisateur. L'autre option permet d'ouvrir la session administrateur en parallèle de la session utilisateur, sans interférer directement. Si cette option peut être utile, **il est IMPERATIF de bien déconnecter l'administrateur AVANT de quitter la prise en main à distance** (menu Pomme > fermer la session administrateur). Autrement l'utilisateur est dans l'incapacité d'effectuer une action aussi simple que d'éteindre sa machine par lui-même.
- L'affichage de l'ordinateur distant apparaît dans une fenêtre.

- Vérifier que la prise de contrôle est effective en ouvrant et fermant une fenêtre sur l'ordinateur distant

Si l'action de cliquer ne produit pas d'effet, vérifier d'abord que l'application Partage d'écran n'est pas en mode "lecture seule" : l'icone figurant une souris au centre du bandeau supérieur de l'application Partage d'écran doit être bleue et non grisée.

## ▼ Installation des logiciels

Se limiter au pack de base et aux installations infogérées à jour.

Pour les autres demandes, proposer de reprendre rdv plus tard. Ne créer de nouveau compte adm que sur demande spontanée de l'utilisateur, après approbation de la charte utilisateur-administrateur.

A l'étape du rdv, demander à l'utilisateur de préparer tous les téléchargements dont il a besoin pour que l'intervention soit au plus court.

### ▼ A partir de Mosyle

### ▼ A partir de KACE

Ajouter l'étiquette de déploiement du logiciel dans la fiche KACE du poste.

Appliquer 2 inventaires successivement sur le poste.

Une fois le logiciel installé, retirer l'étiquette de déploiement du logiciel.

### ▼ A partir du Stock (obsolète, préférer les autres moyens, le 05/05/2025)

Installer les logiciels demandés grâce à la commande suivante dans le Terminal :

```
sudo sh stock/MAC/Installation_Silencieuse/Nom_Du_Logiciel/install.  
sh
```

### ▼ Démonter le lecteur réseau Stock

```
diskutil umount stock
```

## ▼ Lorsque le poste est prêt

Informer l'utilisateur, dans le ticket de déploiement, qu'il peut passer récupérer son matériel.

Templates de communication à envoyer à l'utilisateur :

▼ en Francais

Bonjour,

Votre nouveau poste a été déployé avec ce système d'exploitation. Si vous avez le moindre souci avec celui-ci n'hésitez pas à nous contacter via [helpdesk@igbmc.fr](mailto:helpdesk@igbmc.fr).

Vous pouvez récupérer votre poste au service informatique entre 9h et 12h et 13h et 17h sur rendez-vous du lundi au vendredi, excepté les lundis après-midi.

▼ in English

Hi,

Your new computer has been deployed with this operating system. If you have any issue with it, you can contact us via [helpdesk@igbmc.fr](mailto:helpdesk@igbmc.fr).

You can retrieve your computer at IT between 9 am and 12 am and 1 pm and 5 pm on appointment from monday to friday, except in monday afternoon.

Enfin, **changer la catégorie du ticket** vers "poste de travail > Configuration d'un poste de travail > prêt à récupérer".

Déposer le matériel et les accessoires associés, bien étiquetés avec le nom du destinataire et le numéro du ticket, sur le meuble bleu au stock informatique.

## ▼ Ouverture de session avec l'utilisateur final

La première ouverture de session doit être faite au service informatique.

Réaliser avec l'utilisateur les configurations suivantes :

- Sur un laptop, connecter le wifi IGBMC dans la session de l'utilisateur
- Sur un laptop, installer le profil de connexion aux réseaux wi-fi Eduroam et Osiris.

Téléchargement du profil sur cat.eduroam.org

Double-cliquer sur le fichier téléchargé. Ouvrir les Réglages Système > Confidentialité et sécurité > Autres > Profils

Double-cliquer sur la ligne des profils Eduroam et confirmer leur installation.

Passer les 2 invites d'authentification sans les renseigner et attendre la fin de l'installation.

Connecter le wi-fi sur le réseau Eduroam, et demander à l'utilisateur de renseigner ses identifiants Unistra (login seul, sans la partie domaine). Attendre que la connexion soit établie et stable. Si le wi-fi bascule automatiquement vers un autre réseau, c'est qu'il y a eu un problème lors de l'authentification. Parfois, un 2e essai est nécessaire.

Répéter la dernière étape avec le réseau wi-fi Osiris.

- Sur un laptop, connecter le VPN paloalto avec l'utilisateur, vérifier que le message indique que l'équipement est conforme.
- Sur tout les appareils, vérifier avec un redémarrage que l'utilisateur nouvellement créé parvient bien à déverrouiller le disque (démontre que l'utilisateur a le token filevault)
- Sur tout les appareils, si les droits d'admin sont demandés, inscrire le poste dans l'interface (procédure en lien ci-dessous). Vérifier la présence de l'onglet admin on demand dans l'application Self-service. Faire la démonstration du fonctionnement d'admin on-demand avec l'utilisateur.

#### Admin On-Demand

- Sur les appareils dotés d'une puce Apple Silicon : activer Rosetta dans la session de l'utilisateur.