Configurer CSC avec un module de parapluie pour Kandji RMM (macOS)

Table des matières

Introduction

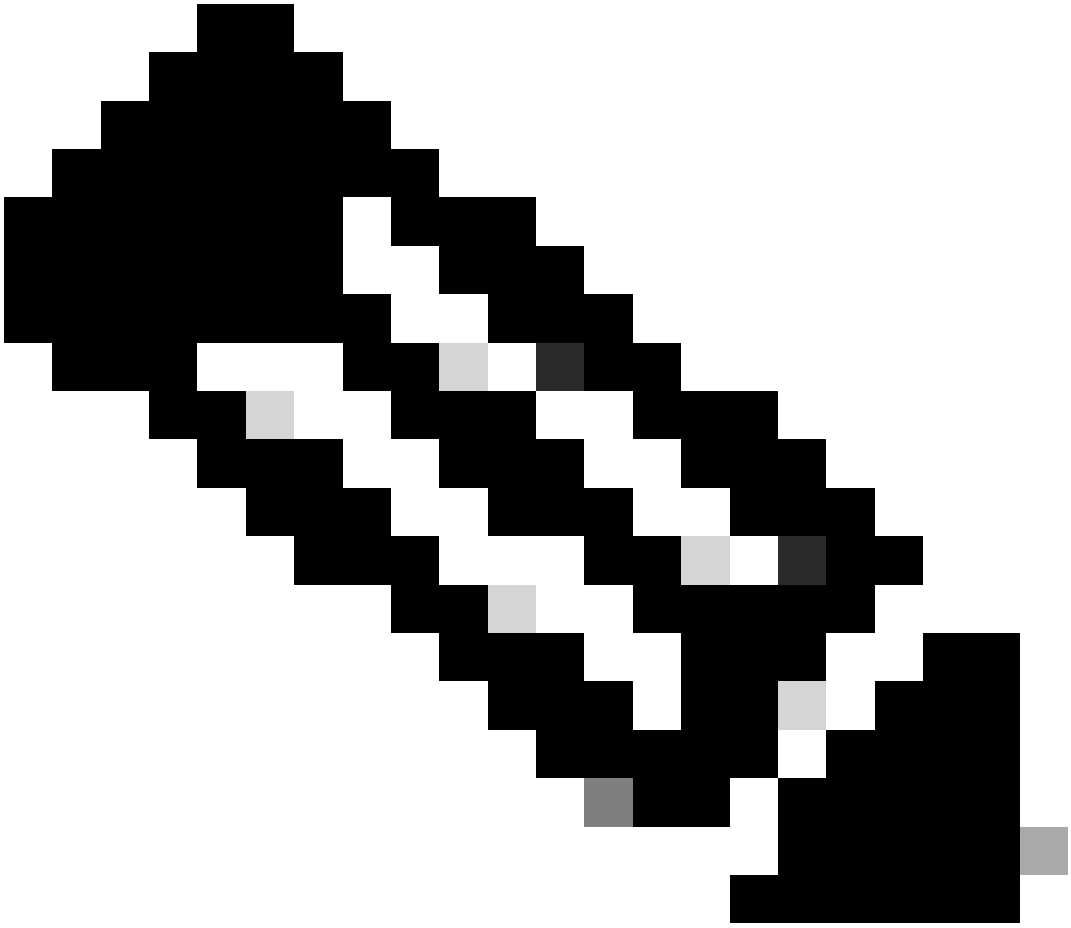
Ce document décrit comment configurer Cisco Secure Client (CSC) avec le module Umbrella pour Kandji RMM (macOS).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au tableau de bord Umbrella.
- Accès au portail Kandji.
- Profil de module Secure Client Umbrella (orginfo.json).
- Package de prédéploiement du client sécurisé pour la version à déployer.



Remarque : Ce guide utilise la méthode de déploiement .zip dans Kandji, ainsi qu'un script de post-installation.

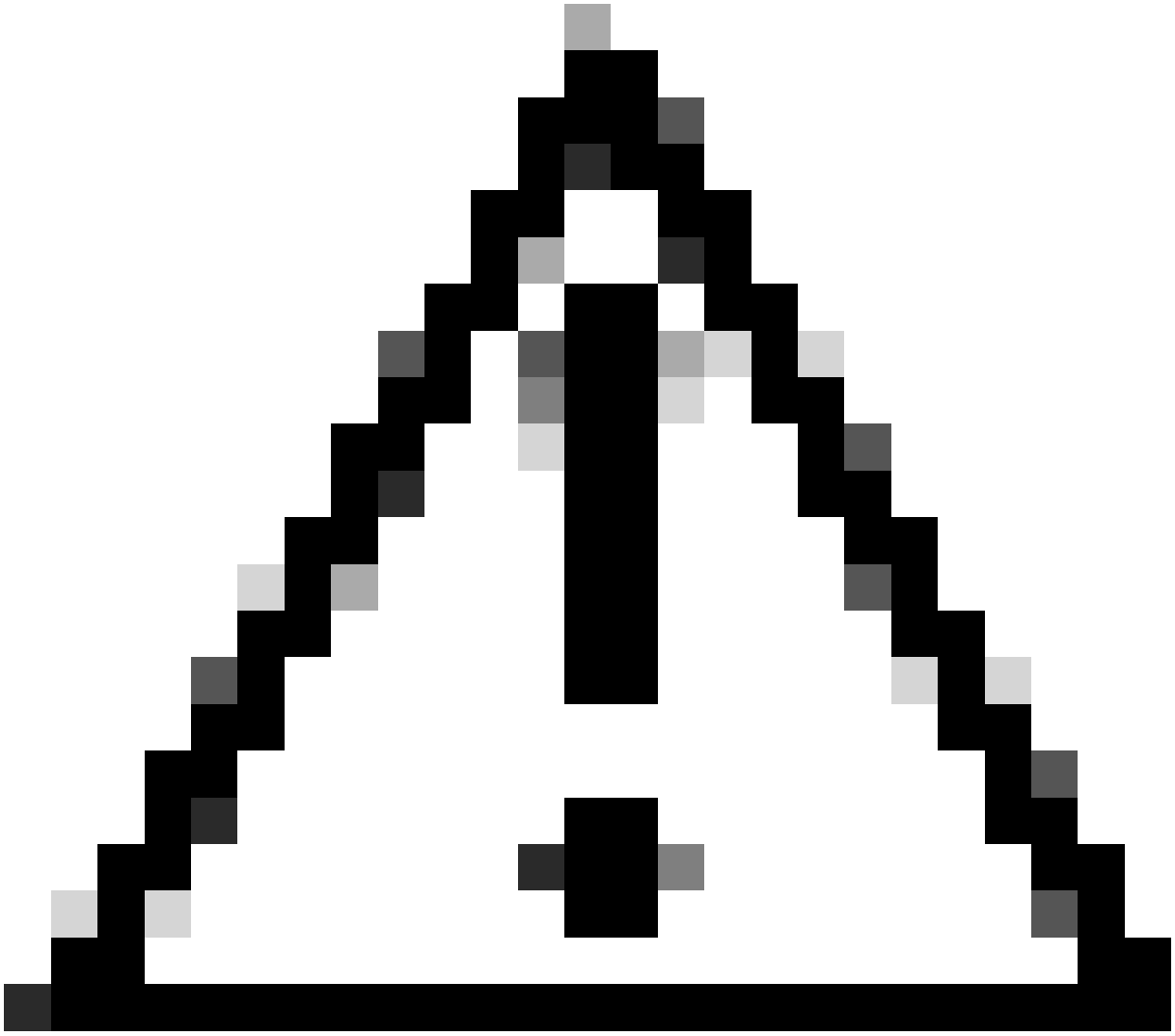
Composants utilisés

Les informations contenues dans ce document sont basées sur le module Cisco Secure Client with Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

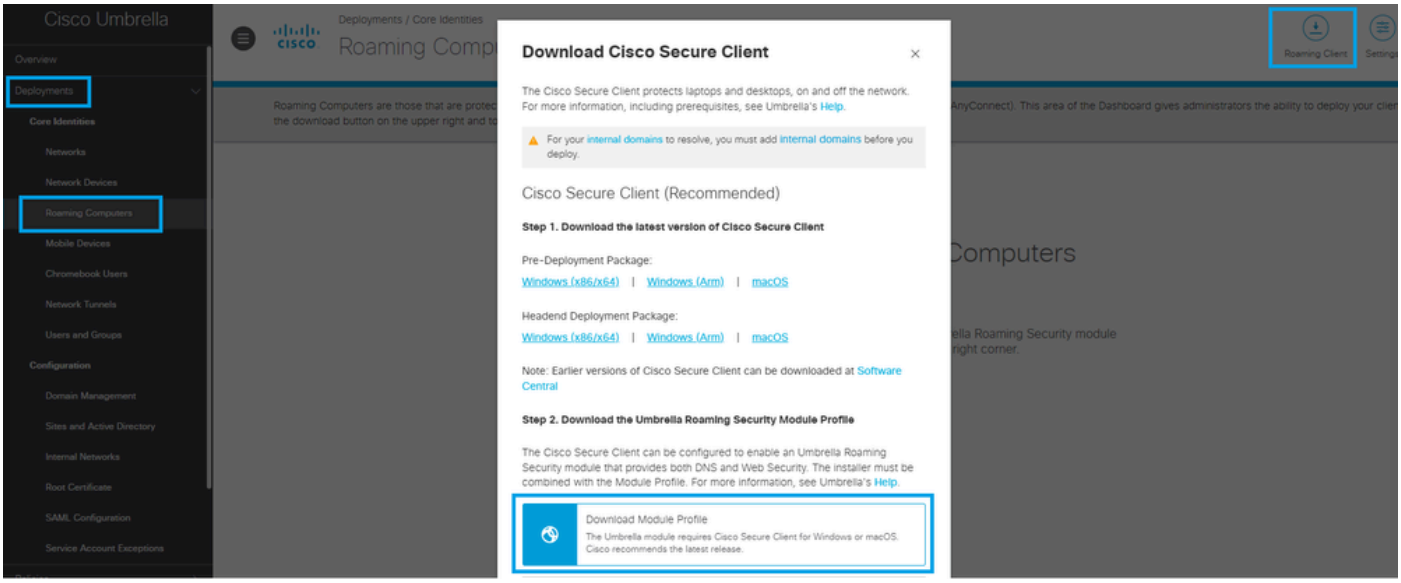
Cet article décrit comment configurer Cisco Secure Client (CSC) avec le module Umbrella pour Kandji RMM (macOS).



Mise en garde : Cet article est fourni en l'état au 3 mars 2025. L'assistance Cisco Umbrella ne garantit pas que ces instructions sont valides après cette date et sujettes à modification en fonction des mises à jour de Kandji.

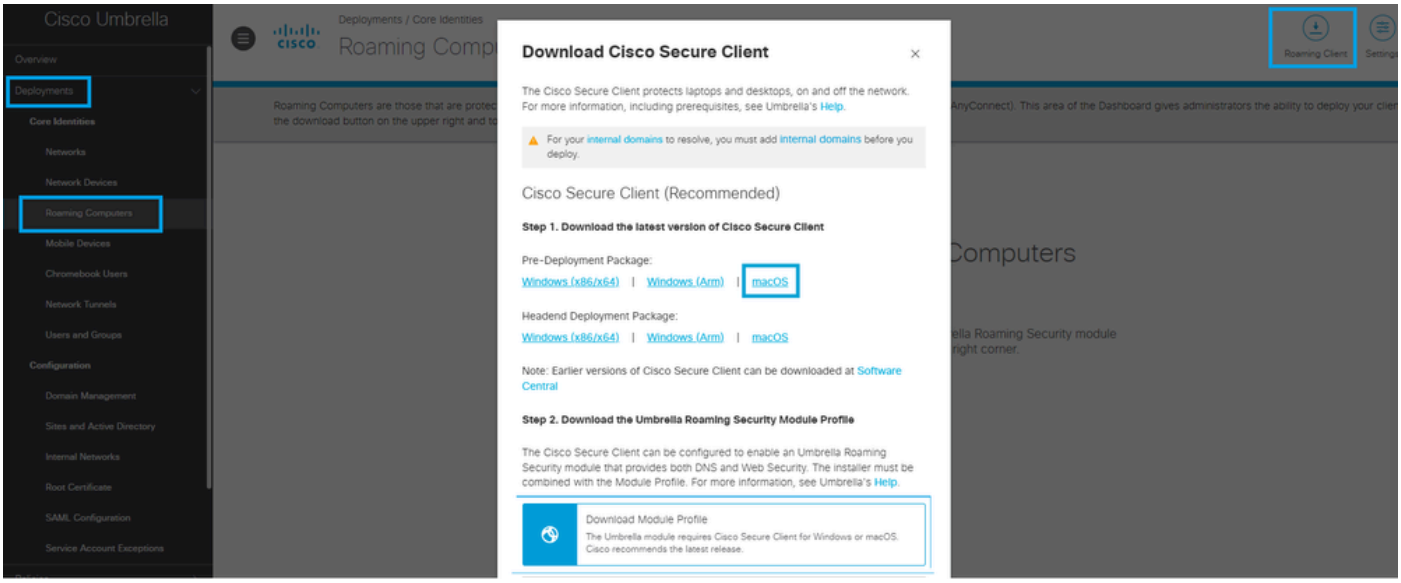
Préparation du programme d'installation .zip

1. Accédez à votre tableau de bord Umbrella et téléchargez le profil de module Secure Client Umbrella (orginfo.json) en accédant à Déploiements > Clients itinérants > Télécharger > Télécharger le profil de module.



34747396643092

2. Vous pouvez également télécharger la dernière version du programme d'installation de macOS en sélectionnant le package de prédéploiement.



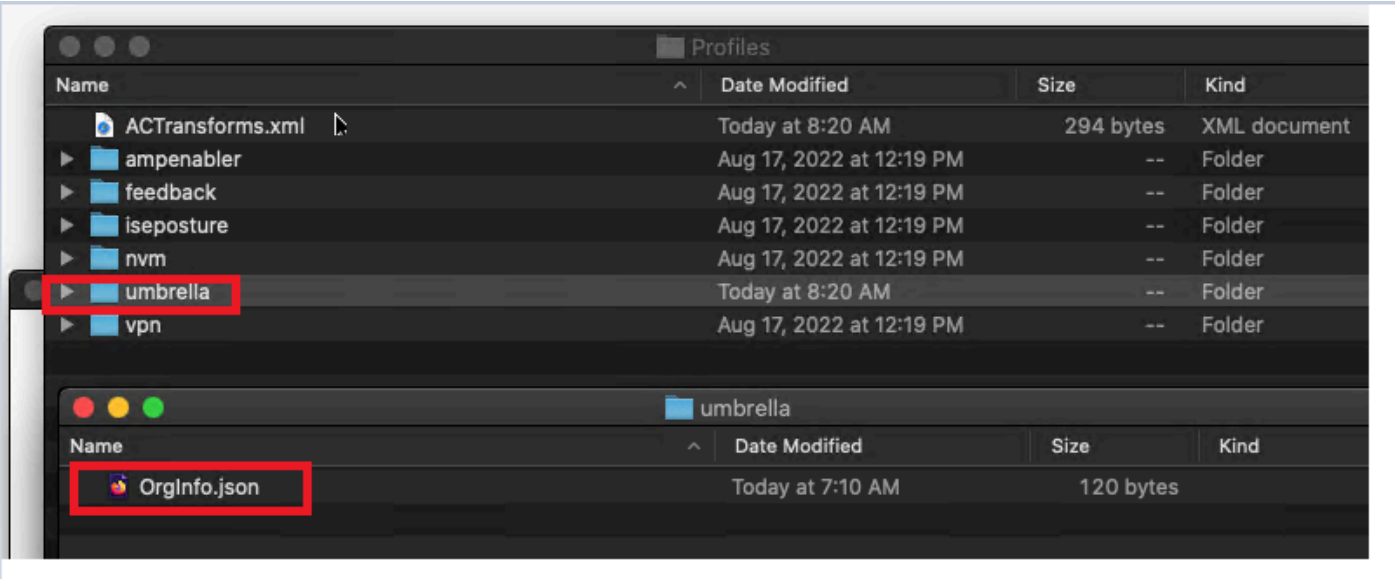
34747396644884

3. Vous pouvez maintenant configurer le fichier .dmg pour le déploiement en remplaçant l'image du programme d'installation par une version accessible en écriture. Pour ce faire, utilisez Disk Utility ou l'application Terminal à l'aide de la commande suivante :

```
hdiutil convert  -format UDRW -o
```

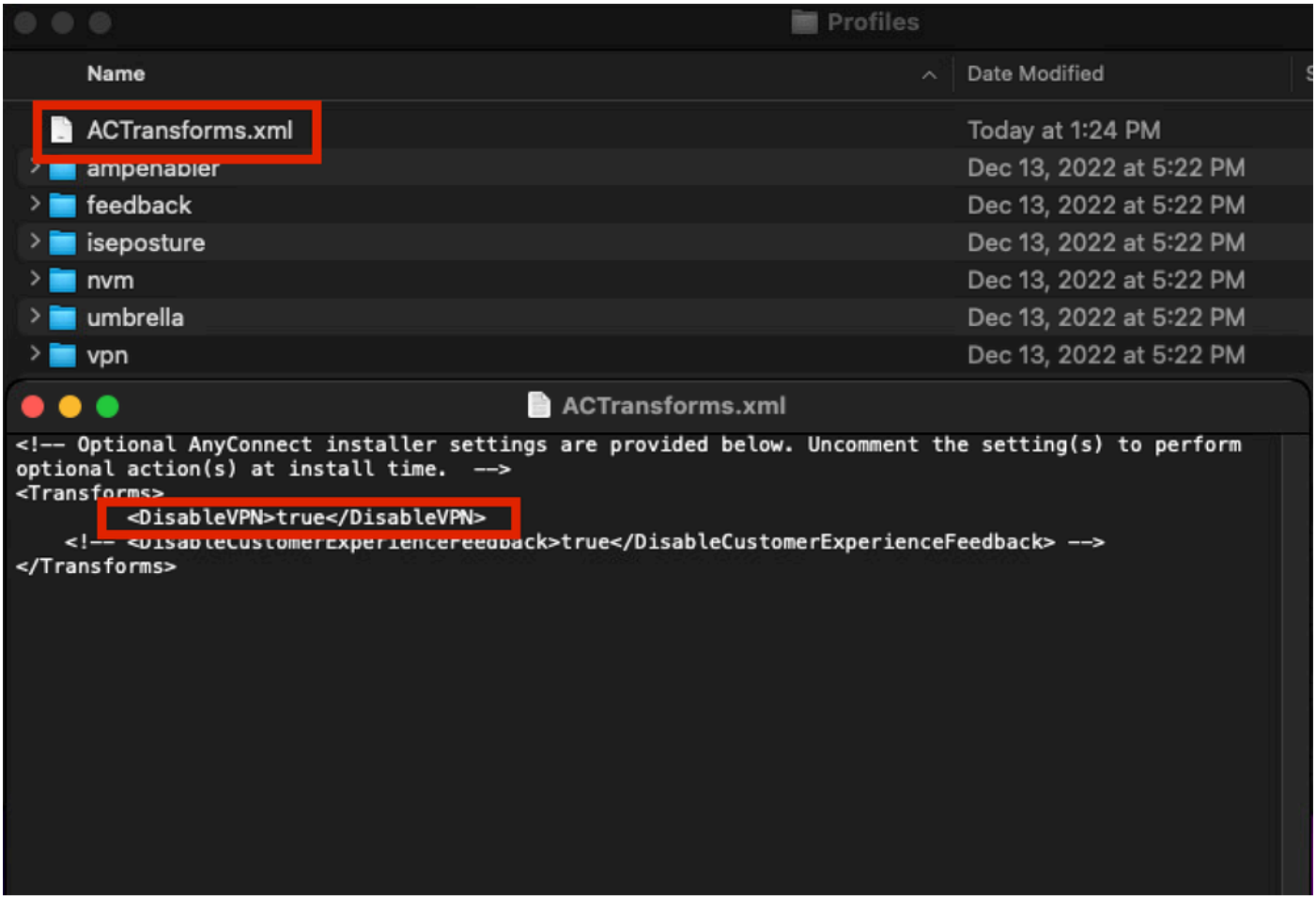
```
user@macOS-          Desktop % hdiutil convert cisco-secure-client-macos-5.0.00556-predeploy-k9.dmg -format UDRW -o cisco-umbrella.dmg
Reading Protective Master Boot Record (MBR : 0)…
Reading GPT Header (Primary GPT Header : 1)…
Reading GPT Partition Data (Primary GPT Table : 2)…
Reading  (Apple_Free : 3)…
Reading disk image (Apple_HFS : 4)…
.....................................................................
Reading  (Apple_Free : 5)…
Reading GPT Partition Data (Backup GPT Table : 6)…
.....................................................................
Reading GPT Header (Backup GPT Header : 7)…
.....................................................................
Elapsed Time: 898.924ms
Speed: 152.4Mbytes/sec
Savings: 0.0%
created: /Users/user/Desktop/cisco-umbrella.dmg
```

4. Ouvrez le fichier .dmg nouvellement converti et accédez au dossier 'Profiles'. Ensuite, dans le dossier Umbrella, placez le fichier OrgInfo.json que vous avez téléchargé à partir de votre tableau de bord.



34747396647444

4.1. Pour masquer éventuellement le module VPN, modifiez le fichier ACTransforms.xml. Mettez à jour l'élément `<DisableVPN>` sur `true` et supprimez les balises de commentaire `<!-` et `->`



34747372903956

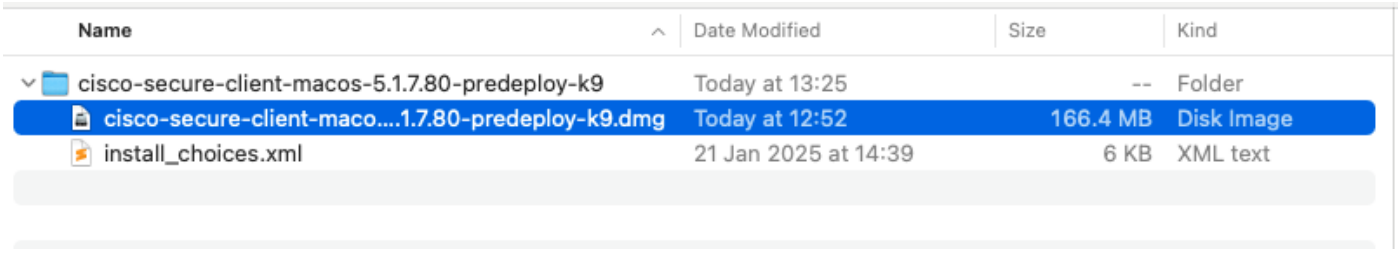
5. Ensuite, créez un nouveau fichier nommé install_choice.xml. Ce fichier peut spécifier les modules que vous souhaitez installer.

Exécutez cette commande pour générer le fichier :

```
installer -pkg /volumes/Cisco\ Secure\ Client\ /Cisco\ Secure\ Client.pkg -showChoiceChangesXML > ~/Dow
```

- Pour ignorer un module, définissez le module avec 0.
- Pour installer un module, définissez le module avec 1.

Ce fichier doit se trouver dans le même dossier que le fichier .dmg modifié. Votre structure de dossiers peut ressembler à cette capture d'écran :



Dans cet exemple, le fichier install_choice.xml inclut les modules Core VPN, Umbrella et DART, chacun défini sur 1, indiquant qu'ils sont inclus dans l'installation du client sécurisé :

```
attributeSetting
```

```
choiceAttribute
```

```
visible
```

```
choiceIdentifier
```

```
choice_anyconnect_vpn
```

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_anyconnect_vpn

attributeSetting

1

choiceAttribute

selected

choiceIdentifier

choice_anyconnect_vpn

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_fireamp

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_fireamp

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_fireamp

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_dart

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_dart

attributeSetting

1

choiceAttribute

selected

choiceIdentifier

choice_dart

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_secure_firewall_posture

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_secure_firewall_posture

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_secure_firewall_posture

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_iseposture

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_iseposture

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_iseposture

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_nvm

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_nvm

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_nvm

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_secure_umbrella

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_secure_umbrella

attributeSetting

1

choiceAttribute

selected

choiceIdentifier

choice_secure_umbrella

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_thousandeyes

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_thousandeyes

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_thousandeyes

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_duo

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_duo

attributeSetting

0

choiceAttribute

selected

choiceIdentifier

choice_duo

attributeSetting

choiceAttribute

visible

choiceIdentifier

choice_zta

attributeSetting

choiceAttribute

enabled

choiceIdentifier

choice_zta

attributeSetting

0

choiceAttribute

selected

```
        choiceIdentifier




        choice_zta
```

6. Vous pouvez maintenant remplacer l'image du programme d'installation par une version en lecture seule à l'aide de Disk Utility ou de l'application Terminal :

```
hdiutil convert <source dmg> -format UDRO -o <output dmg>
```

7. L'étape finale de la préparation de l'installation Umbrella consiste à convertir le dossier d'installation en fichier .zip, prêt à être téléchargé sur le tableau de bord Kandji.

Modifications du tableau de bord Kanji

1. Pour macOS 13 (et versions ultérieures) et Secure Client 5.1, l'agent VPN nécessite l'approbation de l'utilisateur avant d'être lancé par le système d'exploitation. Pour automatiser ce processus d'approbation ou empêcher les utilisateurs de désactiver les éléments de connexion appartenant au client sécurisé, vous devez déployer un profil MDM avec des attributs configurés pour les éléments de connexion gérés.

- Préfixe d'identificateur de bundle : com.cisco.secureclient
- Identifiant de l'équipe : DE8Y96K9QP

Vous pouvez les créer à l'aide du guide Kandji Configure the Login & Background Items Library Item, qui utilise l'identificateur d'ensemble : com.cisco.secureclient.

2. Le client sécurisé Cisco utilise une extension de système réseau sur macOS 11 (et versions ultérieures), regroupée dans une application nommée « Client sécurisé Cisco - Filtre de socket ». Ensuite, vous devez demander à Kandji d'installer ceci en utilisant les identifiants fournis ici :

- Identifiant de l'équipe : DE8Y96K9QP
- Identifiant du bundle : com.cisco.anyconnect.macos.acsockext
- Type d'extension système : ExtensionRéseau

Ces identificateurs peuvent être configurés à l'aide du guide Kandji : Extensions système - Présentation et guide

3. Le client sécurisé Cisco doit être déployé en tant qu'application personnalisée, ce qui peut être fait à l'aide du guide Kandji : Déploiement d'applications personnalisées

Lorsque vous atteignez l'étape Add & Configure, effectuez les ajustements suivants pour le déploiement :

- Choisir le type de package : Choisir un fichier ZIP
- Télécharger le programme d'installation : Téléchargez le fichier .zip configuré précédemment à l'étape 7.
    - Si vous choisissez un type de fichier .zip, vous pouvez disposer d'un champ supplémentaire pour définir un emplacement de décompression. (L'emplacement par défaut est /var/tmp/)
- Script post-installation : Fournissez un script à exécuter après l'exécution du package.
    - Mettez à jour `<Filename.zip>` avec le nom utilisé à l'étape 7.
    - Mettez à jour `<Nom du dossier>` utilisé pour contenir le fichier .dmg et le fichier install_choice.xml
    - Mettez à jour `<Output dmg file.dmg>` avec le nom déclaré à l'étape 5 précédente.

Exemple de script

```
#!/bin/bash

# Optional extract the ZIP file. (Kandji extracts to /var/tmp by default)
#unzip "/var/tmp/Cisco Secure Client 5-1-7-80.zip" -d /var/tmp/

# Mount the DMG.
hdiutil attach "/var/tmp/<Folder Name>/<Output dmg file.dmg>"

# Run the installer with our xml choices file.
installer -pkg "/Volumes/Cisco Secure Client 5.1.7.80/Cisco Secure Client.pkg" -applyChoiceChangesXML "

# Check installer exit code.
if [ $? -ne 0 ]; then
echo "Error: Installation failed."
# Add any necessary cleanup or rollback actions here
exit 1
fi

# Unmount the DMG.
hdiutil detach "Cisco Secure Client 5.1.7.80"

# Remove the temp files & folders.
rm -rf /var/tmp/<Folder Name>
rm -f /var/tmp/<Filename.zip>

exit 0
```

Si vous rencontrez des problèmes de déploiement liés au déploiement du client sécurisé Cisco,

vous pouvez contacter l'équipe Cisco TAC.

Pour les problèmes de déploiement liés au module Umbrella, veuillez enregistrer un ticket d'assistance auprès de l'assistance Cisco Umbrella.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.