Déployer CSC pour iOS sur des plates-formes MDM supplémentaires

Table des matières

Introduction

Informations générales

Tous les MDM

Cloud MobileIron

Gestion des terminaux Citrix MDM

MDM à faible vitesse

Écoles JAMF

JAMF antérieure à 10.2.0

InTune

Mosyle

En toute sécurité

Introduction

Ce document décrit comment déployer Cisco Security Connector pour iOS sur des plates-formes de gestion d'appareils mobiles supplémentaires.

Informations générales

Le connecteur de sécurité Cisco (CSC) pour iOS est une protection DNS complète Umbrella pour votre iPhone. Avant d'utiliser ce guide pour les déploiements, veuillez lire la documentation de déploiement CSC. Votre périphérique doit être en mode supervisé pour pouvoir utiliser le CSC.

Ce document résume la prise en charge logicielle supplémentaire de la gestion des périphériques mobiles (MDM) pour le CSC. Ces MDM ont été validés par un déploiement réussi, mais ne sont pas encore directement présents sur le tableau de bord.

Pour vérifier qu'un profil existe sur un périphérique iOS :

1. Accédez à Paramètres > Général > Gestion des périphériques > [Nom du profil MDM] > Plus de détails.
2. Vérifiez que le type de profil DNS Proxy est présent avec ces détails :
    - Détails de l'application : `com.cisco.ciscosecurity.app`
    - Détails du bundle fournisseur : `com.cisco.ciscosecurity.ciscoumbrella`

En savoir plus sur les détails du profil iOS à configurer sur le site Apple MDM.

Tous les MDM

Les étapes suivantes s'appliquent au déploiement de tous les MDM et doivent être effectuées en premier :

1. Assurez-vous que votre adresse e-mail d'administrateur est ajoutée au tableau de bord sous l'option « Paramètres » de la page Périphériques mobiles.
2. Téléchargez le fichier `Cisco_Umbrella_Root_CA.cer` à utiliser sur le périphérique iOS. Ce certificat autorise les pages de blocage HTTPS sans erreur. Pour obtenir l'autorité de certification racine :
    1. Accédez à Déploiements > Configuration > Root Certificate.
    2. Sélectionnez Télécharger le certificat.
    3. Enregistrez le téléchargement en tant que fichier `.cer`.

Cloud MobileIron

Actuellement, le téléchargement de MobileIron sur le tableau de bord ne prend en charge que la version sur site. La version Cloud utilise des variables de périphérique différentes de celles du logiciel sur site. Le déploiement est très similaire au déploiement sur site, à quelques exceptions près. MobileIron Core peut nécessiter cette modification, selon la version.

Pour déployer sur MobileIron Cloud :

1. Assurez-vous que votre adresse e-mail d'administrateur est ajoutée au tableau de bord sous l'option « Paramètres » de la page Périphériques mobiles.
2. Téléchargez le profil Mobile Iron depuis le tableau de bord Umbrella.
3. Remplacez ces variables :

Variable générique d'espace réservé	Nouvelle variable
« $DEVICE_SN$ »	${deviceSN}
«$DEVICE_MAC$»*	${deviceWifiMacAddress}

*Cette option est utilisée uniquement pour le composant Clarté du CSC, et non pour le composant Parapluie. Si vous n'utilisez pas Clarity, il n'y a pas de $DEVICE_MAC$ à remplacer.

Gestion des terminaux Citrix MDM

Pour effectuer le déploiement vers Citrix, procédez comme suit dans le tableau de bord :

1. Assurez-vous que votre adresse e-mail d'administrateur est ajoutée au tableau de bord sous l'option « Paramètres » de la page Périphériques mobiles.
2. Téléchargez la configuration MDM générique depuis Umbrella (AMP est configuré de la

même manière).
3. Téléchargez le certificat racine pour Umbrella :
    1. Accédez à Déploiements > Configuration > Root Certificate.
    2. Sélectionnez Télécharger le certificat.
    3. Enregistrez le téléchargement en tant que fichier `.cer`.
4. Modifiez la configuration et remplacez l'espace réservé générique par la variable correcte pour Citrix MDM :

Variable générique d'espace réservé	Nouvelle variable
`Numéro_de_série`	`${device.serialnumber}`
`Adresse_MAC`*	`${device.MAC_ADDRESS}`

*Cette option est utilisée uniquement pour le composant Clarté du CSC, et non pour le composant Parapluie.

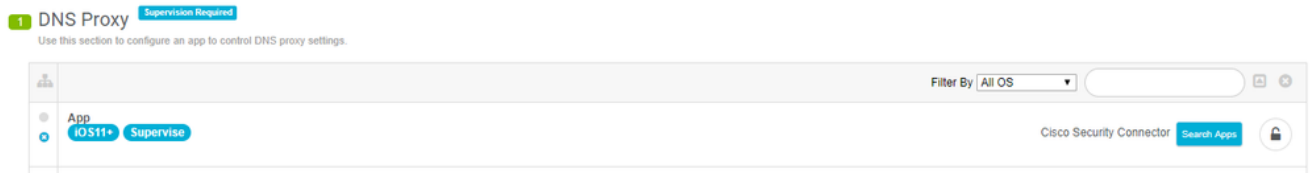
Exécutez ensuite les étapes MDM suivantes :

1. Configurez le MDM pour installer l'application CSC à l'aide d'Apple Business Manager (ABM) (anciennement connu sous le nom de VPP, Volume Purchase Program).
2. Téléchargez la configuration Umbrella et/ou Clarity modifiée dans les étapes de préparation.
3. Suivez les étapes de la documentation Citrix pour importer le profil.
4. Téléchargez le certificat du périphérique pour faire confiance à l'autorité de certification racine Umbrella.
5. Configurez les politiques pour pousser les profils, 1 CA et 1 application CSC vers le ou les périphériques requis.

MDM à faible vitesse

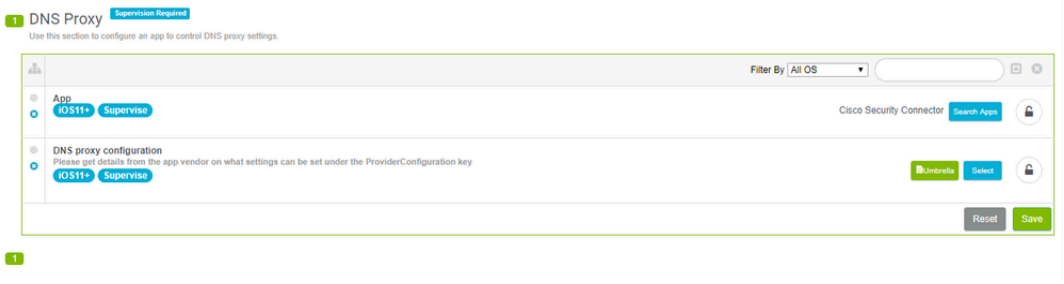
Lightspeed MDM prend en charge la configuration texte du proxy DNS iOS. Pour ce faire, vous pouvez modifier le profil MDM générique.

1. Téléchargez le « fichier mobileconfig générique » et remplacez l'extension de fichier .xml par .txt.
2. Ouvrez le fichier et remplacez la chaîne du numéro de série de l'espace réservé à la ligne 58 par `%serial_number%`
3. Dans Lightspeed, ajoutez Cisco Security Connection au profil de proxy DNS comme indiqué



360019477192

4. Ajoutez le fichier mobileconfig générique modifié à l'option de configuration de proxy DNS sous l'application.



360019477152

5. Enfin, téléchargez l'autorité de certification [racine Cisco](#) depuis Umbrella et déployez-la dans Lightspeed pour garantir des pages de blocage sans certificat.

360019477132

Ces étapes s'appliquent au déploiement de tous les MDM. Veuillez d'abord suivre ces étapes.

Écoles JAMF

Le déploiement de CSC avec les écoles JAMF diffère de JAMF. Commencez par le profil générique et consultez les étapes de la [documentation JAMF](#).

Voici un exemple de configuration de l'emplacement de sélection et de la variable à utiliser pour le numéro de série :

```
        PayloadContent


         AppBundleIdentifier


         com.cisco.ciscosecurity.app
```

```
        PayloadDescription

        Cisco Umbrella

        PayloadDisplayName

        Cisco Umbrella

        PayloadIdentifier

        com.apple.dnsProxy.managed.{pre-filled in the download}

        PayloadType

        com.apple.dnsProxy.managed

        PayloadUUID

        {pre-filled in the download}
```

```
        PayloadVersion


        1


        ProviderBundleIdentifier


        com.cisco.ciscosecurity.app.CiscoUmbrella


        ProviderConfiguration


 disabled


  disabled


  internalDomains
```

```
10.in-addr.arpa

16.172.in-addr.arpa

17.172.in-addr.arpa

18.172.in-addr.arpa

19.172.in-addr.arpa

20.172.in-addr.arpa

21.172.in-addr.arpa

22.172.in-addr.arpa

23.172.in-addr.arpa

24.172.in-addr.arpa
```

```
        25.172.in-addr.arpa


        26.172.in-addr.arpa


        27.172.in-addr.arpa


        28.172.in-addr.arpa


        29.172.in-addr.arpa


        30.172.in-addr.arpa


        31.172.in-addr.arpa


        168.192.in-addr.arpa


        local


      logLevel
```

```
        verbose


        orgAdminAddress


        {pre-filled in the download}


        organizationId


        {pre-filled in the download}


        regToken


        {pre-filled in the download}


        serialNumber


        %SerialNumber%
```

```
        PayloadDisplayName

        Cisco Security

        PayloadIdentifier

        com.cisco.ciscosecurity.app.CiscoUmbrella.{pre-filled in the download}

        PayloadRemovalDisallowed

        PayloadType

        Configuration

        PayloadUUID

        {pre-filled in the download}

        PayloadVersion
```

```
1
```

1. Créez un nouveau profil dans JAMF School.
   Pour plus d'informations, reportez-vous à la documentation JAMF sur les profils de périphériques.
2. Utilisez la charge utile du proxy DNS pour configurer ces paramètres :
   1. Dans le champ ID d'ensemble d'applications, entrez `com.cisco.ciscosecurity.app`.
   2. Dans le champ Provider Bundle ID, saisissez `com.cisco.ciscosecurity.app.CiscoUmbrella`.
3. Ajoutez le fichier XML que vous avez créé à l'étape 2 de la documentation JAMF à la configuration du fournisseur.

JAMF antérieure à 10.2.0

Le déploiement du CSC avec JAMF nécessite une modification importante du profil. Suivez ces étapes pour déployer le CSC avec JAMF MDM.

1. Assurez-vous que votre adresse e-mail d'administrateur est ajoutée au tableau de bord sous l'option Paramètres de la page Périphériques mobiles.
2. Ajoutez l'AC racine Umbrella :
   1. Accédez à Déploiements > Configuration > Root Certificate.
   2. Sélectionnez Télécharger le certificat.
   3. Enregistrez le téléchargement en tant que fichier .cer.
   4. Entrez un nom pour le certificat et sélectionnez Upload Certificate.
   5. Téléchargez le fichier .cer et laissez le champ de mot de passe vide.
   6. Appliquez à la portée de vos périphériques pour diffuser ce certificat.
3. Téléchargez le profil générique depuis le tableau de bord Umbrella.
4. Si vous utilisez JAMF Pro v.10.2.0 ou version ultérieure, vous pouvez ignorer cette étape. Vous pouvez importer en l'état en ajoutant les éléments suivants :

```
<key>serialNumber</key>
<string>$SERIALNUMBER</string>
<key>label</key>
<string>$DEVICENAME</string>
```

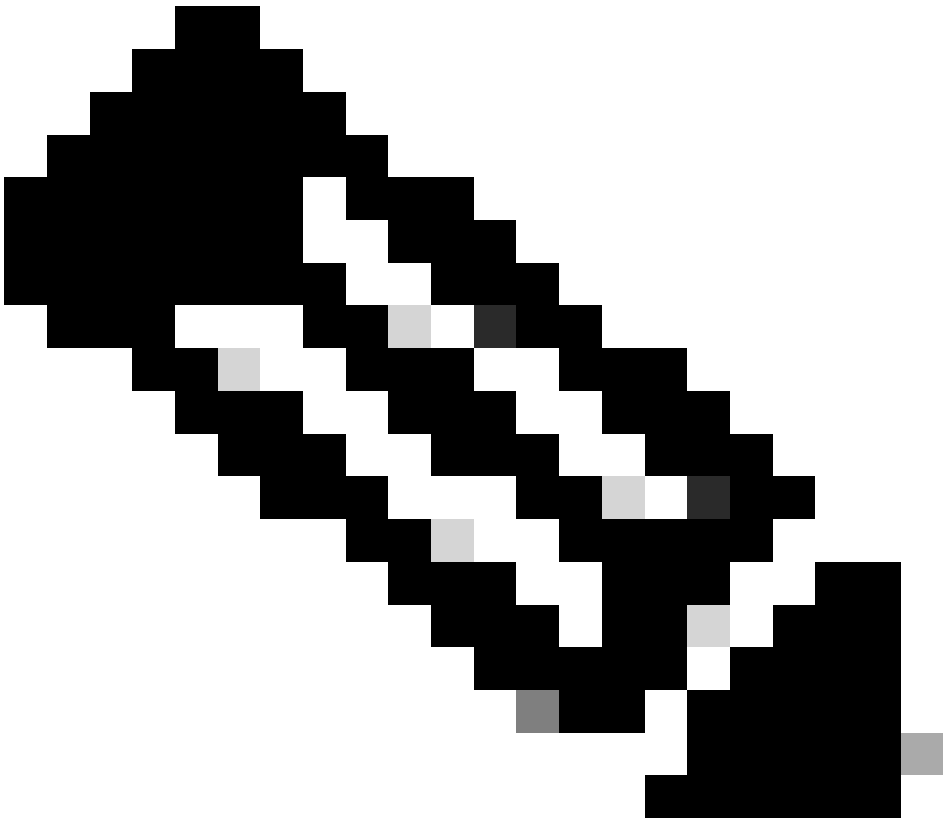
5. Si vous utilisez une version de JAMF antérieure à v.10.2.0, modifiez le profil XML en profondeur, comme indiqué dans cet exemple de profil. Ne copiez pas cet exemple, il ne fonctionne pas tel quel. Utilisez uniquement la configuration de téléchargement générique de

votre tableau de bord.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.d
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>AppBundleIdentifier</key>
<string>com.cisco.ciscosecurity.app</string>
<key>PayloadDescription</key>
<string>Cisco Umbrella</string>
<key>PayloadDisplayName</key>
<string>Cisco Umbrella</string>
<key>PayloadIdentifier</key>
<string>com.apple.dnsProxy.managed.DBE2A157-E134-3E8C-B4FB-23EDF48A0CD1</string>
<key>PayloadType</key>
<string>com.apple.dnsProxy.managed</string>
<key>PayloadUUID</key>
<string>59401AAF-CDBF-4FD7-9250-443A58EAD706</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>ProviderBundleIdentifier</key>
<string>com.cisco.ciscosecurity.app.CiscoUmbrella</string>
<key>ProviderConfiguration</key>
<dict>
<key>disabled</key>
<false/>
<key>internalDomains</key>
<array>
<string>10.in-addr.arpa</string>
<string>16.172.in-addr.arpa</string>
<string>17.172.in-addr.arpa</string>
<string>18.172.in-addr.arpa</string>
<string>19.172.in-addr.arpa</string>
<string>20.172.in-addr.arpa</string>
<string>21.172.in-addr.arpa</string>
<string>22.172.in-addr.arpa</string>
<string>23.172.in-addr.arpa</string>
<string>24.172.in-addr.arpa</string>
<string>25.172.in-addr.arpa</string>
<string>26.172.in-addr.arpa</string>
<string>27.172.in-addr.arpa</string>
<string>28.172.in-addr.arpa</string>
<string>29.172.in-addr.arpa</string>
<string>30.172.in-addr.arpa</string>
<string>31.172.in-addr.arpa</string>
<string>168.192.in-addr.arpa</string>
<string>local</string>
<string>cisco.com</string>
</array>
<key>logLevel</key>
<string>{pre-filled in the download}</string>
<key>orgAdminAddress</key>
<string>{pre-filled in the download}</string>
<key>organizationId</key>
<string>{pre-filled in the download}</string>
<key>regToken</key>
```

```
<string>{pre-filled in the download}</string>
<key>serialNumber</key>
<string>$SERIALNUMBER</string>
<key>label</key>
<string>$DEVICENAME</string>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Cisco Security</string>
<key>PayloadIdentifier</key>
<string>com.cisco.ciscosecurity.app.CiscoUmbrella.{pre-filled in the download}</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>{pre-filled in the download}</string>
<key>PayloadVersion</key>
<integer>{pre-filled in the download}</integer>
</dict>
</plist>
```

6. Importer dans JAMF :
    1. Dans la fenêtre de configuration principale de MDM, cliquez sur New pour créer un nouveau profil.



Remarque : Il doit s'agir d'un profil distinct et ne doit pas être utilisé avec le profil de certificat créé. Pour que l'application fonctionne, ces deux profils doivent être poussés séparément vers l'appareil.

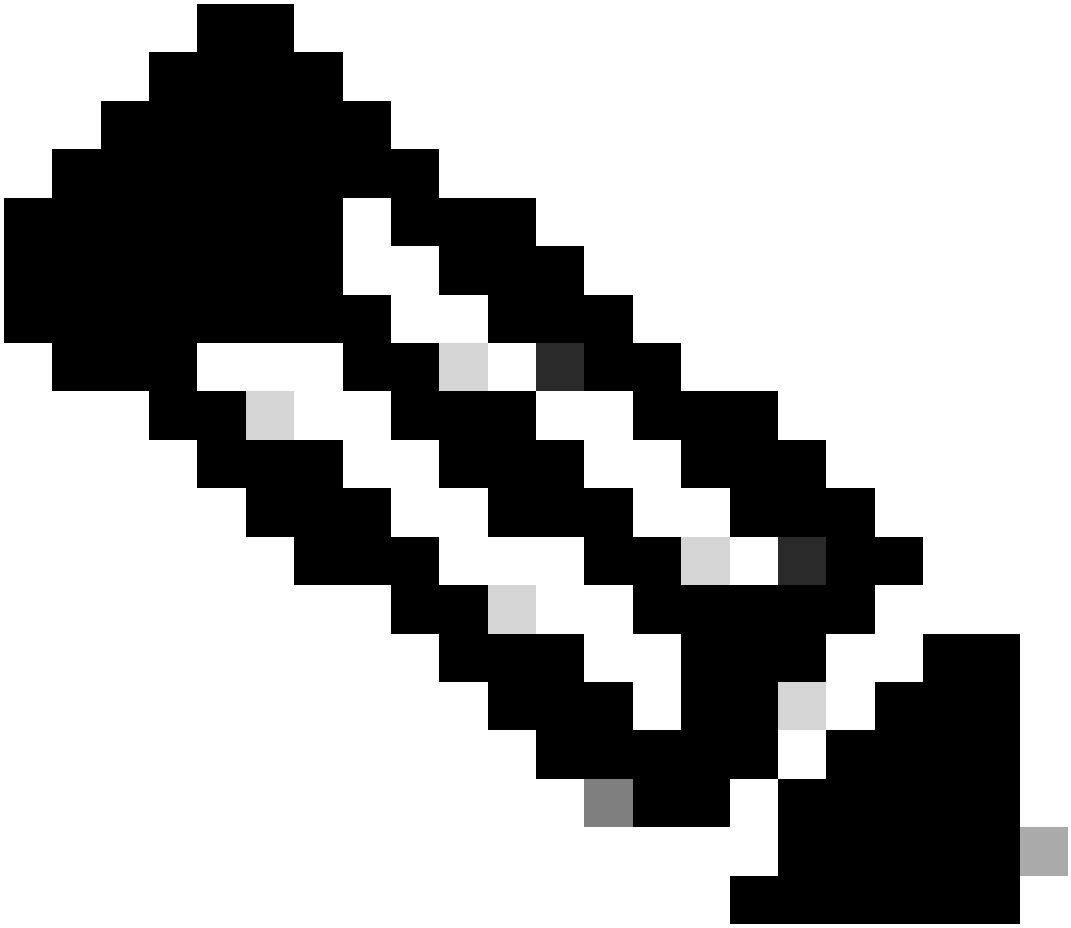
2. Attribuez un nom au profil et accédez au proxy DNS.
3. Sous le proxy DNS, cliquez sur Configure.
4. Définissez la configuration du proxy sur les détails du parapluie :

    1. Dans le champ ID d'ensemble d'applications, entrez `com.cisco.ciscosecurity.app`.
    2. Dans le champ Provider Bundle ID, saisissez `com.cisco.ciscosecurity.app.CiscoUmbrella`.
    3. Coller le contenu XML modifié à partir d'Umbrella dans la configuration du fournisseur Section XML.

5. Cliquez sur Scope et appliquez-le à la portée appropriée des périphériques.

InTune

InTune est directement ajouté au tableau de bord Umbrella. Consultez la documentation d'Umbrella InTune pour plus d'informations.



> Remarque : Clarity est un produit de Cisco AMP for Endpoints. Si vous ne disposez pas d'une licence pour ce produit, ignorez la partie relative à la configuration.

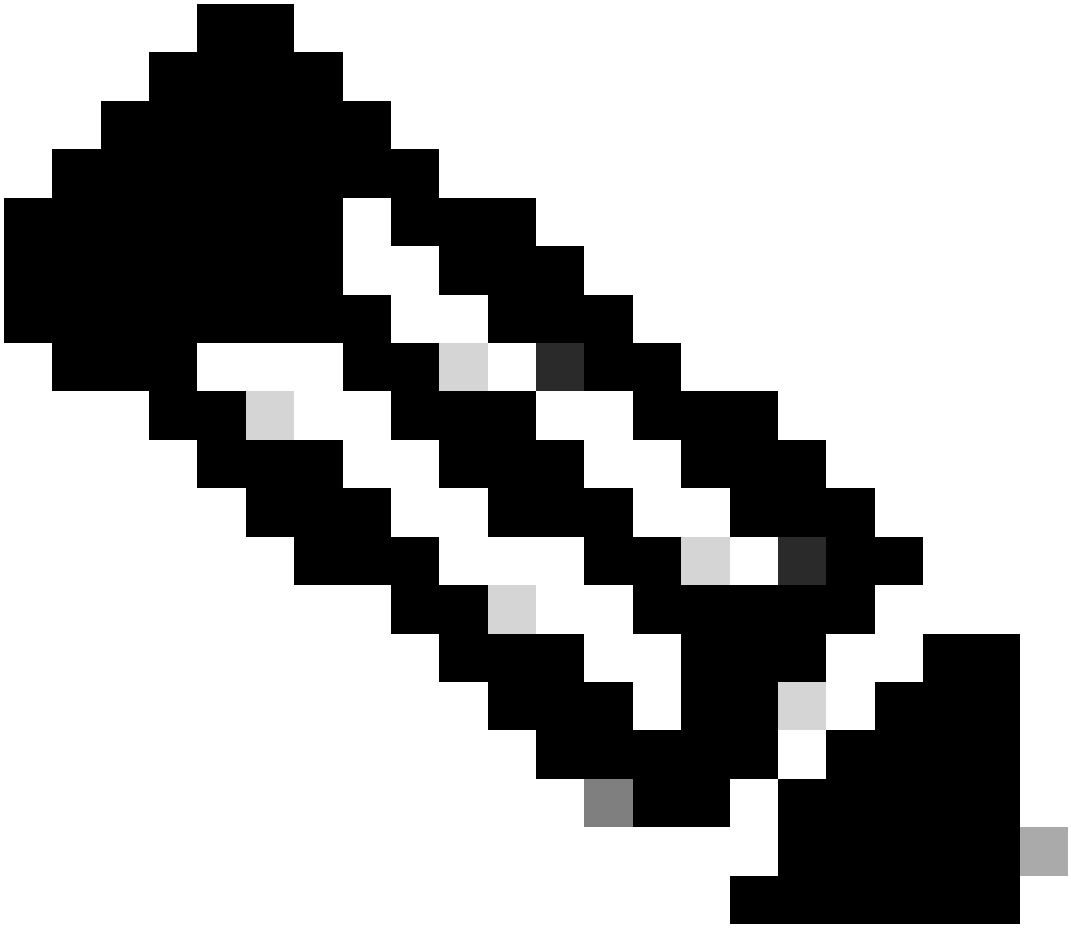
Mosyle

La prise en charge de Mosyle se présente sous la forme de la configuration du proxy DNS :

- Dans le champ ID d'ensemble d'applications, entrez `com.cisco.ciscosecurity.app`.
- Dans le champ Provider Bundle ID, saisissez `com.cisco.ciscosecurity.app.CiscoUmbrella`.

Ajoutez le contenu du fichier XML `<key>ProviderConfiguration</key>` au champ Mosyle Provider Configuration :

```
<dict>
<key>anonymizationLevel</key>
<integer>0</integer>
***
<key>serialNumber</key>
<string>%SerialNumber%</string>
</dict>
```



Remarque : Les paramètres nécessitent que les périphériques soient étendus pour recevoir la configuration, et les étendues ne sont pas ajoutées par défaut.

En toute sécurité

Configurez en toute sécurité sur la page de profil du proxy DNS :

- Dans le champ ID d'offre groupée d'applications, entrez `com.cisco.ciscosecurity.app`

- Dans le champ Provider Bundle ID , saisissez `com.cisco.ciscosecurity.app.CiscoUmbrella`

Pour configurer le fichier `.plist`, procédez comme suit :

1. Commencez par le modèle de configuration commune iOS et modifiez le fichier dans une `.plist` avec seulement les commentaires `<dict>` à `</dict>` à l'intérieur de `<key>ProviderConfiguration</key>`.
2. Remplacez la clé `serialNumber` par la variable `$serialnumber`, telle que définie par Securly.
3. Le contenu du fichier `.plist` peut être très similaire à cet exemple. Téléchargez ceci dans la configuration du proxy DNS :

```
anonymizationLevel

0

disabled

internalDomains

 10.in-addr.arpa

 16.172.in-addr.arpa
```

17.172.in-addr.arpa

18.172.in-addr.arpa

19.172.in-addr.arpa

20.172.in-addr.arpa

21.172.in-addr.arpa

22.172.in-addr.arpa

23.172.in-addr.arpa

24.172.in-addr.arpa

25.172.in-addr.arpa

26.172.in-addr.arpa

27.172.in-addr.arpa

28.172.in-addr.arpa

29.172.in-addr.arpa

30.172.in-addr.arpa

31.172.in-addr.arpa

168.192.in-addr.arpa

local

logLevel

{pre-filled in the download}

orgAdminAddress

{pre-filled in the download}

organizationId

{pre-filled in the download}

regToken

{pre-filled in the download}

serialNumber

$serialnumber

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.