Comprendre le déploiement automatisé avec le profil de regroupement (Windows)

Table des matières

Introduction

Aperçu

Créer le package de prédéploiement

- Création du package de déploiement

Hébergement du package

Déployer le package

- commandes MSI

Propriétés MSI supplémentaires pendant l'installation

- Activer le verrouillage
- Masquer les programmes et les fonctionnalités

Déploiement du profil Umbrella (post-installation)

Désactivation de la fonctionnalité VPN (post-installation)

Déployer l'autorité de certification racine Cisco

Introduction

Ce document décrit le didacticiel de déploiement automatisé avec le profil Umbrella intégré dans Cisco Secure Client (Windows).

Aperçu

Le déploiement du Cisco Secure Client (CSC) (anciennement AnyConnect) avec le module Umbrella implique les composants suivants :

- Installation du module VPN principal CSC
- Installation du module de sécurité d'itinérance Umbrella
- Installation du profil Umbrella (OrgInfo.json)
- Installation du module DART (Diagnostic and Reporting Tool) (facultatif)

Cet article fournit un didacticiel sur l'installation de ces composants par programme (sous Windows). Le profil Umbrella est intégré dans le package d'installation et peut être installé à partir de dossiers partagés.

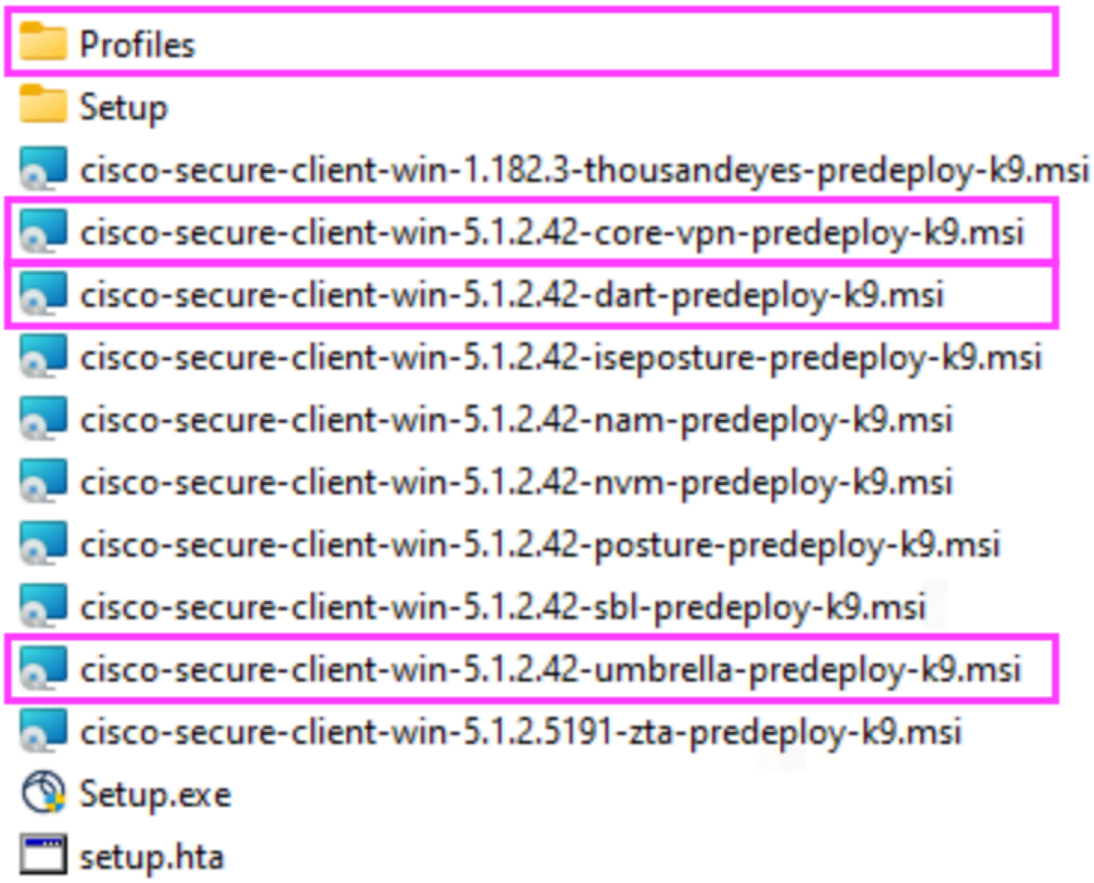
Créer le package de prédéploiement

Ces étapes permettent de déployer le module Umbrella. Notez que la fonctionnalité VPN Cisco est complètement désactivée. Cependant, le module VPN principal doit toujours être installé car il est

utilisé pour l'interception sous-jacente du trafic DNS.

Création du package de déploiement

1. Téléchargez le profil du module de sécurité d'itinérance Umbrella depuis votre tableau de bord Umbrella. Déploiements > Ordinateurs itinérants > Clients itinérants.
   - Le nom de fichier téléchargé du profil de module est Orginfo.json
2. Téléchargez le package de « prédéploiement » du module Umbrella Roaming Security pour Windows à partir de l'un des emplacements suivants :
   - :software.cisco.com
   - Notes de version Umbrella
3. Extrayez le client AnyConnect téléchargé et recherchez le numéro de version. Notez les noms de fichiers et les numéros de version dans le package extrait



27073502800788

4. Ajoutez votre fichier OrgInfo.json dans le dossier "Profiles\Umbrella"* dans le même répertoire que le programme d'installation. Cette étape est essentielle pour que le module Cisco Umbrella s'enregistre automatiquement après l'installation. La structure du dossier doit ressembler à ceci :
<#root>

```
cisco-secure-client-win-X.X.XXXXX-core-vpn-predeploy-k9.msicisco-secure-client-win-win-X.X.X
```

\Profiles\umbrella\OrgInfo.json

Créez le sous-dossier \Profiles\Umbrella à côté de vos fichiers MSI s'il n'existe pas déjà.

Hébergement du package

Le package doit être distribué aux utilisateurs finaux avec le sous-dossier « Profiles\Umbrella ». Cela peut se faire de la manière suivante :

- Un dossier réseau partagé
- Logiciel de gestion des terminaux prenant en charge la composition de packages d'installation multifichiers

Déployer le package

Les fichiers MSI peuvent désormais être simplement déployés à l'aide d'un logiciel de gestion des terminaux ou avec « msiexec ».

commandes MSI

<#root>

msiexec /package cisco-secure-client-win-

X.X.XXXXX

-core-vpn-predeploy-k9.msi

PRE_DEPLOY_DISABLE_VPN=1

/norestart /passive /lvx* vpninstall.log
msiexec /package cisco-secure-client-win-

X.X.XXXXX

-umbrella-predeploy-k9.msi

PRE_DEPLOY_DISABLE_VPN=1

/norestart /passive /lvx* umbrellainstall.log
msiexec /package cisco-secure-client-win-

X.X.XXXXX

-dart-predeploy-k9.msi /norestart /passive /lvx* dartinstall.log

IMPORTANT : Remplacez X.X.XXXXX par les numéros de version corrects correspondant à vos noms de fichiers MSI.

Assurez-vous que l'option PRE_DEPLOY_DISABLE_VPN=1 est ajoutée aux arguments d'installation pour désactiver la fonctionnalité VPN. Vous pouvez également omettre cet argument pour activer la fonctionnalité VPN.

Propriétés MSI supplémentaires pendant l'installation

Les packages d'installation Cisco prennent en charge plusieurs propriétés MSI qui peuvent être modifiées pendant l'installation. Les propriétés couramment utilisées pour Cisco Umbrella sont les suivantes :

- LOCKDOWN = Comme décrit, empêche la désactivation manuelle du service
- ARPSYSTEMCOMPONENT = Masque le programme dans la liste « Programmes et fonctionnalités » de Windows

Pour définir ces paramètres lors de l'installation, suivez les mêmes étapes, mais passez les propriétés supplémentaires à la commande msiexec :

Activer le verrouillage

<#root>

```
msiexec /package <MSI> /passive
```

LOCKDOWN=1

```
 /lvx*
```

Masquer les programmes et les fonctionnalités

<#root>

```
msiexec /package <MSI> /passive
```

ARPSYSTEMCOMPONENT=1

```
 /lvx*
```

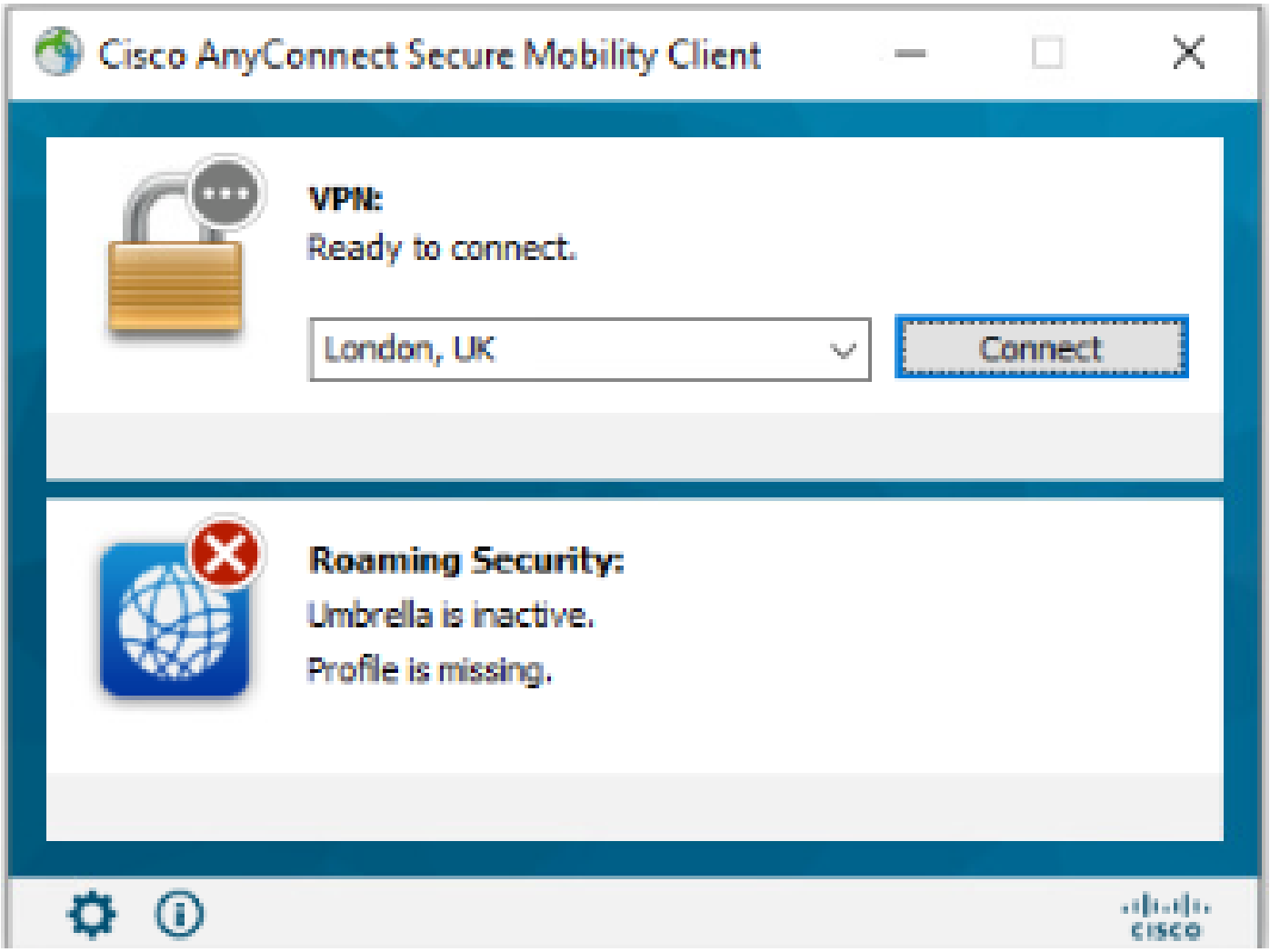
Vous pouvez également configurer ces paramètres MSI en fournissant des fichiers de transformation d'installation personnalisés (fichiers .mst). Pour plus d'informations, consultez Configurer le verrouillage AnyConnect.

Déploiement du profil Umbrella (post-installation)

L'erreur courante « Profile is missing » indique que le module Cisco Umbrella est installé, mais que le profil (OrgInfo.json) ne l'est pas. Cela signifie que le module Cisco Umbrella ne peut pas

s'enregistrer auprès de Cisco Umbrella ou activer la protection.

Notez que ce problème ne se produit pas si le profil a été correctement incorporé dans le package d'installation.



4435402655892

S'il n'est pas possible d'incorporer le profil dans le package d'installation, il peut être copié séparément sur le point d'extrémité à l'aide d'une tâche ou d'un script d'installation. Le profil doit être déployé à cet emplacement :

```
%PROGRAMDATA%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
```

Le script PowerShell montre un exemple de création du fichier OrgInfo.json par programme en tant que tâche de post-installation. Remplacez les espaces réservés ORG_ID, FINGERPRINT et USER_ID par les valeurs appropriées de votre profil.

```
$org_file = "%PROGRAMDATA%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json"
$data=@"
```

```
{
    "organizationId" : "ORG_ID",
    "fingerprint" : "FINGERPRINT",
    "userId" : "USER_ID"
}
"@

if(-not(Test-Path -Path $org_file))
{

$data > $org_file
}
```

Désactivation de la fonctionnalité VPN (post-installation)

Si la fonctionnalité VPN n'a pas été désactivée pendant le déploiement, il est possible de la désactiver ultérieurement en déployant un profil VPN spécial sur le périphérique. Voir https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows

Déployer l'autorité de certification racine Cisco

Pour les pages de blocage sans erreur et la navigation HTTPS, il est nécessaire de faire confiance à l'autorité de certification Cisco Umbrella Root pour chaque terminal. Reportez-vous à votre logiciel de gestion des terminaux pour obtenir des détails sur le déploiement centralisé d'une autorité de certification.

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.