# Guide d'intégration MDM AnyConnect Samsung Knox VPN

## Contenu

AnyConnect implémente le framework Samsung Knox VPN et est compatible avec le SDK Knox VPN. Il est recommandé d'utiliser Knox version 2.2 et ultérieure avec AnyConnect. Toutes les opérations de IKnoxVpnService sont prises en charge. Pour une description détaillée de chaque opération, veuillez consulter la documentation IKnoxVpnService publiée par Samsung.

### Profil JSON VPN Knox

Comme l'exige le framework Knox VPN, chaque configuration VPN est créée à l'aide d'un objet JSON. Cet objet comporte trois sections principales de la configuration :

1. Attributs généraux - « profile_attribute »
2. Attributs spécifiques au fournisseur (AnyConnect) - « fournisseur »
3. Attributs de profil spécifiques à Knox - « knox »

### Champs Profile_Attribute pris en charge

- profileName : nom unique de l'entrée de connexion à afficher dans la liste des connexions de l'écran d'accueil AnyConnect et dans le champ Description de l'entrée de connexion AnyConnect. Nous vous recommandons d'utiliser un maximum de 24 caractères pour vous assurer qu'ils s'insèrent dans la liste des connexions. Utilisez des lettres, des chiffres ou des symboles sur le clavier affiché sur le périphérique lorsque vous saisissez du texte dans un champ. Les lettres sont sensibles à la casse.

- vpn_type - Protocole VPN utilisé pour cette connexion. Les valeurs valides sont les suivantes : sslipsec
- vpn_route_type - Les valeurs valides sont : 0 - VPN système1 - VPN par application

Pour plus d'informations sur les attributs de profil courants, reportez-vous au Guide d'intégration des fournisseurs de Samsung KNOX Framework.

La configuration spécifique d'AnyConnect est spécifiée via la clé "**AnyConnectVPNConnection**" dans la section « Fournisseur ». Exemple :

```
{
"KNOX_VPN_PARAMETERS": {
"profile_attribute": {
"profileName": "SSL VPN",
"vpn_type": "ssl",
"vpn_route_type": 0
},
"vendor": {
"AnyConnectVPNConnection": {
"host": "vpn.company.com"
}
}
}
}
```

### Champs AnyConnectVPNConnection pris en charge

- host : nom de domaine, adresse IP ou URL de groupe de l'ASA avec lequel se connecter. AnyConnect insère la valeur de ce paramètre dans le champ Server Address de l'entrée de connexion AnyConnect.

- authentication - (facultatif) Ne s'applique que lorsque vpn_type (dans profile_attribute) est défini sur « ipsec ». Spécifie la méthode d'authentification utilisée pour une connexion VPN IPsec Les valeurs valides sont :
  EAP-AnyConnect (valeur par défaut)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity - Utilisé uniquement si l'authentification est définie sur EAP-GTC, EAP-MD5 ou EAP-MSCAPv2. Fournit l'identité IKE pour ces méthodes d'authentification.

- usergroup (facultatif) Profil de connexion (groupe de tunnels) à utiliser lors de la connexion à l'hôte spécifié. S'il est présent, utilisé conjointement avec HostAddress pour former une URL basée sur un groupe. Si vous spécifiez le protocole principal comme IPsec, le groupe d'utilisateurs doit être le nom exact du profil de connexion (groupe de tunnels). Pour SSL, le groupe d'utilisateurs est l'url de groupe ou l'alias de groupe du profil de connexion.

- certalias (facultatif) : alias KeyChain d'un certificat client qui doit être importé à partir d'Android KeyChain. L'utilisateur doit accuser réception d'une invite système Android avant que le certificat puisse être utilisé par AnyConnect.

- ccmcertalias (facultatif) : alias TIMA d'un certificat client qui doit être importé à partir du magasin de certificats TIMA. Aucune action de l'utilisateur n'est nécessaire pour qu'AnyConnect reçoive le certificat. Remarque : ce certificat doit avoir été explicitement blanchi pour être utilisé par AnyConnect (par exemple en utilisant l'API Knox CertificatePolicy).

### Métadonnées d'application de paquets VPN en ligne

Les métadonnées d'application en ligne pour les paquets VPN sont une fonctionnalité exclusive disponible sur les périphériques Samsung Knox. Il est activé par MDM et fournit à AnyConnect un contexte d'application source pour l'application des politiques de routage et de filtrage. Il est nécessaire pour mettre en oeuvre certaines stratégies de filtrage VPN par application à partir de la passerelle VPN sur les périphériques Android. Les stratégies sont définies pour cibler des ID d'application spécifiques ou des groupes d'applications via un masque générique et sont comparées à l'ID d'application source de chaque paquet sortant.

Le tableau de bord MDM doit fournir aux administrateurs une option pour activer les métadonnées de paquets en ligne. Sinon, MDM pourrait coder cette option de façon à toujours être activée pour AnyConnect, qui l'utilisera en fonction de la stratégie de tête de réseau.

Pour plus d'informations sur les stratégies VPN par application d'AnyConnect, reportez-vous à la section relative à la définition d'une stratégie VPN par application pour les périphériques Android dans le Guide de l'administrateur client Cisco AnyConnect Secure Mobility.

Configuration MDM

Pour activer les métadonnées de paquets en ligne, définissez « uidpid_search_enabled » sur 1 dans l'attribut spécifique de Knox pour une configuration. Exemple :

```
{
"KNOX_VPN_PARAMETERS": {
"profile_attribute": {
"profileName": "ac_knox_profile",
"vpn_type": "ssl",
"vpn_route_type": 1
},
"vendor": {
"AnyConnectVPNConnection": {
"host": "asa.acme.net"
}
},
"knox": {
"uidpid_search_enabled": 1
}
}
}
```