

# Configuration gérée pour AnyConnect pour Android

## Contenu

AnyConnect pour Android prend en charge [les configurations gérées](#), qui peuvent être provisionnées par des applications MDM/EMM. Le schéma est intégré à l'APK d'AnyConnect (dans res/restrictions.xml) et peut être récupéré via [l'API EMM de Google](#). Le schéma inclut une documentation détaillée sur chaque champ et définit un formulaire qui pourrait être rendu par le portail d'administration EMM.

Pour provisionner une seule entrée de configuration VPN, les administrateurs peuvent utiliser les champs `vpn_connection_*`. Pour provisionner plusieurs configurations VPN, les administrateurs peuvent utiliser le champ `vpn_configuration_list`, qui est un BundleArray qui peut contenir une ou plusieurs entrées `vpn_configuration`.

Certaines des clés de configuration managées sont des valeurs dynamiques à jetons qui doivent être renseignées par le logiciel EMM.

### Certificats client de provisionnement

AnyConnect prend en charge le processus standard de provisionnement EMM des certificats clients. `vpn_keychain_cert_alias` doit contenir l'alias Android KeyChain du certificat. Lorsque cette valeur est présente, AnyConnect appelle [KeyChain.selectPrivateKeyAlias](#) pour démarrer l'importation (si l'alias n'a pas déjà été importé). En règle générale, l'utilisateur est invité à approuver la demande par le système d'exploitation. Pour une expérience utilisateur plus transparente, l'application EMM peut implémenter [onChoosePrivateKeyAlias](#) pour éviter d'inviter l'utilisateur.

La plupart des portails EMM permettent à l'administrateur d'entrer une valeur symbolique spéciale pour le champ `vpn_keychain_cert_alias`. Une fois que l'application EMM a importé le certificat dans Android KeyChain, elle utilisera l'alias de certificat réel à la place du jeton spécial.

Note: la valeur de `vpn_keychain_cert_alias` doit correspondre à l'alias KeyChain réel du certificat. Sinon, l'utilisateur peut être invité à plusieurs reprises, car AnyConnect pense que le certificat n'a pas été importé.

Pour récapituler le processus de provisionnement EMM du certificat client :

1. L'application EMM obtient le certificat (par exemple via SCEP) et l'importe dans Android KeyChain.
2. (Recommandé) L'application EMM implémente `DeviceAdminReceiver.onChoosePrivateKeyAlias()` de sorte qu'AnyConnect sera automatiquement approuvé pour utiliser le certificat
3. L'application EMM définit l'alias KeyChain du certificat importé dans le champ `vpn_keychain_cert_alias` de la configuration gérée d'AnyConnect.

### Identificateur de périphérique de provisionnement

AnyConnect prend en charge le provisionnement EMM d'un identificateur de périphérique qui

pourrait être utilisé pour le contrôle d'accès au réseau ou la création de rapports à l'aide du champ de valeur symbolique spécial **vpn\_connection\_device\_id**. Pour plus d'informations sur l'ID de périphérique, reportez-vous à cette [note de zone technique](#).