Guide d'intégration d'AnyConnect Samsung Knox VPN MDM

Contenu

AnyConnect implémente le cadre de Samsung Knox VPN et est compatible avec Knox VPN SDK. Il a recommandé d'utiliser la version 2.2 et ultérieures de Knox avec AnyConnect. Toutes les exécutions d'IKnoxVpnService sont prises en charge. Pour la description détaillée de chaque exécution, voyez s'il vous plaît la documentation d'IKnoxVpnService éditée par Samsung.

Profil de Knox VPN JSON

Selon les exigences du cadre de Knox VPN, chaque configuration du VPN est créée utilisant un objet JSON. Cet objet a fournit trois sections principales de la configuration :

1. Attributs de général - « profile_attribute »
2. Attributs de particularité de constructeur (AnyConnect) - « constructeur »
3. Attributs spécifiques de profil de Knox - « knox »

Champs pris en charge de profile_attribut

- profileName - Nom unique pour que l'entrée de connexion apparaisse dans la liste de connexion de l'écran d'accueil d'AnyConnect et le champ description de l'entrée de connexion d'AnyConnect. Nous recommandons utilisant un maximum de 24 caractères de nous assurer qu'ils s'adaptent dans la liste de connexion. Utilisez les lettres, les nombres, ou les symboles sur le clavier affiché sur le périphérique quand vous entrez dans le texte dans un champ. Les lettres distinguent les majuscules et minuscules.

- vpn_type - Le protocole VPN utilisé pour cette connexion. Les valeurs valides sont : SSLipsec
- vpn_route_type - Les valeurs valides sont : 0 – Système VPN1 – Par-app VPN

Pour plus d'informations sur les attributs de profil de terrain communal, voyez s'il vous plaît le guide d'intégration de constructeur de cadre KNOX de Samsung.

La configuration spécifique d'AnyConnect est spécifiée par l'intermédiaire de l'intérieur de clé de « **AnyConnectVPNConnection** » à l'intérieur la section de « constructeur ». Échantillon :

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

Champs pris en charge d'AnyConnectVPNConnection

- hôte - L'URL de nom de domaine, d'adresse IP, ou de groupe de l'ASA avec laquelle à connecter. AnyConnect insère la valeur de ce paramètre dans la zone adresse d'adresse du serveur de l'entrée de connexion d'AnyConnect.

- authentification - (facultatif) s'applique seulement quand le vpn_type (dans les profile_attributes) est placé au « ipsec ». Spécifie la méthode d'authentification utilisée pour des valeurs valides d'une connexion VPN d'IPsec sont : Eap-AnyConnect (valeur par défaut)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- IKE-identité - Utilisé seulement si l'authentification est placée à EAP-GTC, à EAP-MD5, ou à EAP-MSCAPv2. Fournit l'identité d'IKE pour ces méthodes d'authentification.

- usergroup (facultatif) le profil de connexion (groupe de tunnel) à l'utiliser en se connectant à l'hôte spécifié. Si présent, utilisé en même temps que le host address pour former un URL basé sur groupe. Si vous spécifiez Protocol primaire comme IPsec, le groupe d'utilisateurs doit être le nom précis du profil de connexion (groupe de tunnel). Pour le SSL, le groupe d'utilisateurs est le groupe-URL ou le groupe-pseudonyme du profil de connexion.

- certalias (facultatifs) - Pseudonyme de trousseau de clés d'un certificat client qui devrait être importé du trousseau de clés d'Android. L'utilisateur doit reconnaître un système invite d'Android avant que le CERT pourrait être utilisé par AnyConnect.

- ccmcertalias (facultatifs) - Pseudonyme TIMA d'un certificat client qui devrait être importé de la mémoire de certificat TIMA. Aucune action de l'utilisateur n'est nécessaire pour qu'AnyConnect reçoive le CERT. Notez s'il vous plaît : ce certificat doit explicitement whitelisted à l'usage d'AnyConnect (par exemple utilisant Knox CertificatePolicy API).

Métadonnées intégrées d'app de paquet VPN

Les métadonnées intégrées d'app pour des paquets VPN est une caractéristique exclusive disponible sur des périphériques de Samsung Knox. Il est activé par MDM et fournit à AnyConnect le contexte d'application source pour imposer le routage et les stratégies de filtrage. On l'exige pour mettre en application certaines stratégies de filtrage du par-app VPN de la passerelle VPN sur des périphériques d'Android. Des stratégies sont définies pour viser l'id d'application ou les groupes spécifiques d'app par l'intermédiaire de wildcarding et sont appariées contre l'id d'application source de chaque paquet sortant.

Le tableau de bord MDM devrait fournir à des administrateurs une option d'activer des métadonnées intégrées de paquet. Alternativement, MDM pourrait coder en dur cette option d'être activé toujours pour AnyConnect, qui se servira de elle selon la stratégie de headend.

Pour plus d'informations sur les règles VPN du par-app d'AnyConnect, voyez s'il vous plaît la section sur « définir a par règle VPN d'app pour des périphériques d'Android » dans le guide de l'administrateur de Client à mobilité sécurisé Cisco AnyConnect.

Configuration MDM

Pour activer des métadonnées intégrées de paquet, placez « uidpid_search_enabled » à 1 dans

l'attribut spécifique de Knox pour une configuration. Échantillon :

```
{
"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
}
}
}
```