AnyConnect Samsung Knox VPN MDM整合指南

目錄

AnyConnect實施Samsung Knox VPN框架並與Knox VPN SDK相容。建議在AnyConnect中使用Knox版本2.2及更高版本。支援來自IKnoxVpnService的所有操作。有關每項操作的詳細說明，請參閱三星發佈的IKnoxVpnService文檔。

Knox VPN JSON配置檔案

根據Knox VPN框架的要求，每個VPN配置均使用JSON對象建立。此對象提供了配置的三個主要部分：

1. 常規屬性 — "profile_attribute"
2. 供應商(AnyConnect)特定屬性 — 「供應商」
3. 諾克斯特定配置檔案屬性 — 「諾克斯」

支援的profile_attribut欄位

- profileName — 在AnyConnect主螢幕的連線清單和AnyConnect連線條目的Description欄位中顯示的連線條目的唯一名稱。我們建議最多使用24個字元，以確保這些字元適合連線清單。在欄位中輸入文本時，使用裝置上顯示的鍵盤上的字母、數字或符號。字母區分大小寫。

- vpn_type — 用於此連線的VPN協定。有效值為： sslipsec
- vpn_route_type -有效值為： 0 — 系統VPN1 — 每應用VPN

有關常見配置檔案屬性的更多資訊，請參閱Samsung KNOX Framework Vendor Integration Guide。

AnyConnect特定配置通過「**vendor**」部分中的「AnyConnectVPNConnection」鍵指定。示例：

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

支援的AnyConnectVPNConnection欄位

- host — 要連線的ASA的域名、IP地址或組URL。AnyConnect將此引數的值插入AnyConnect連線條目的Server Address欄位中。

- authentication — （可選）僅當vpn_type（在profile_attributes中）設定為「ipsec」時適用。

指定用於IPsec VPN連線的身份驗證方法有效值為：
EAP-AnyConnect（預設值）EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA

- ike-identity — 僅當身份驗證設定為EAP-GTC、EAP-MD5或EAP-MSCAPv2時才使用。為這些身份驗證方法提供IKE身份。

- usergroup(可選)連線到指定主機時要使用的連線配置檔案（隧道組）。如果存在，則與HostAddress結合使用以形成基於組的URL。如果將主協定指定為IPsec，則使用者組必須是連線配置檔案（隧道組）的確切名稱。 對於SSL，使用者組是連線配置檔案的group-url或group-alias。

- certalias（可選） — 應從Android KeyChain匯入的客戶端證書的KeyChain別名。使用者必須先確認Android系統提示，AnyConnect才能使用該證書。

- ccmcertalias（可選） — 應從TIMA證書儲存匯入的客戶端證書的TIMA別名。AnyConnect接收證書無需使用者操作。請注意：此證書必須已被明確列入白名單以供AnyConnect使用（例如使用Knox CertificatePolicy API）。

內聯VPN資料包應用後設資料

VPN資料包的內聯應用後設資料是Samsung Knox裝置上可用的專有功能。它由MDM啟用，並為AnyConnect提供源應用程式上下文以實施路由和過濾策略。在Android裝置上，從VPN網關實施某些基於應用的VPN過濾策略時需要該設定。策略通過萬用字元定義為目標特定的應用程式ID或應用程式組，並與每個出站資料包的源應用程式ID進行匹配。

MDM儀表板應向管理員提供啟用內聯資料包後設資料的選項。或者，MDM可以將此選項硬編碼為始終啟用AnyConnect，AnyConnect將根據頭端策略使用該選項。

有關AnyConnect的每應用VPN策略的詳細資訊，請參閱《Cisco AnyConnect安全移動客戶端管理員指南》中「為Android裝置定義每應用VPN策略」一節。

MDM配置

要啟用內聯資料包後設資料，請在配置的Knox特定屬性中將「uidpid_search_enabled」設定為1。示例：

```
{
"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
}
}
}
```