AnyConnect Samsung Knox VPN MDM統合ガイド

内容

AnyConnectはSamsung Knox VPNフレームワークを実装し、Knox VPN SDKと互換性があります。Knoxバージョン2.2以降をAnyConnectで使用することを推奨します。IKnoxVpnServiceからのすべての操作がサポートされます。各操作の詳細については、Samsungが公開しているIKnoxVpnServiceのドキュメントを参照してください。

Knox VPN JSONプロファイル

Knox VPNフレームワークの要求に応じて、各VPN設定はJSONオブジェクトを使用して作成されます。このオブジェクトには、設定の3つの主要なセクションがあります。

1. 一般属性：「profile_attribute」
2. ベンダー(AnyConnect)固有の属性：「ベンダー」
3. Knox固有のプロファイル属性：「knox」

サポートされるprofile_attributeフィールド

- profileName:AnyConnectホーム画面の接続リストとAnyConnect接続エントリの[Description]フィールドに表示される接続エントリの一意の名前。接続リストに収まるように、最大24文字を使用することをお勧めします。フィールドにテキストを入力するときに、デバイスに表示されるキーボードの文字、数字、記号を使用します。大文字と小文字は区別されます。

- vpn_type：この接続に使用されるVPNプロトコル。有効な値は次のとおりです。 sslIPSec
- vpn_route_type：有効な値は次のとおりです。 0 – システムVPN1 – アプリケーションごとのVPN

共通プロファイル属性の詳細については、『Samsung KNOX Framework Vendor Integration Guide』を参照してください。

AnyConnect固有の設定は、「ベンダー」セクション内の「AnyConnectVPNConnection」キーで指定します。例：

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

サポートされるAnyConnectVPNConnectionフィールド

- host：接続先のASAのドメイン名、IPアドレス、またはグループURL。AnyConnectは、このパラメータの値をAnyConnect接続エントリの[Server Address]フィールドに挿入します。

- authentication: （オプション）vpn_type (in profile_attributes)が「ipsec」に設定されている場合にのみ適用されます。 IPsec VPN接続に使用する認証方式を指定します。有効な値は次のとおりです。
  EAP-AnyConnect（デフォルト値）EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity：認証がEAP-GTC、EAP-MD5、またはEAP-MSCAPv2に設定されている場合にのみ使用されます。これらの認証方式のIKE IDを提供します。

- usergroup （オプション）指定したホストに接続するときに使用する接続プロファイル（トンネルグループ）。存在する場合は、HostAddressとともに使用してグループベースのURLを形成します。プライマリプロトコルをIPsecとして指定する場合、ユーザグループは接続プロファイル（トンネルグループ）の正確な名前である必要があります。 SSLの場合、ユーザグループは接続プロファイルのグループURLまたはグループエイリアスです。

- certalias（オプション） – Android KeyChainからインポートするクライアント証明書のKeyChainエイリアス。証明書をAnyConnectで使用する前に、ユーザはAndroidシステムプロンプトに同意する必要があります。

- ccmcertalias（オプション）:TIMA証明書ストアからインポートするクライアント証明書のTIMAエイリアス。AnyConnectが証明書を受信するために必要なユーザアクションはありません。注：この証明書は、AnyConnectで使用するために明示的にホワイトリストされている必要があります（たとえば、Knox CertificatePolicy APIを使用）。

インラインVPNパケットアプリケーションメタデータ

VPNパケットのインラインアプリメタデータは、Samsung Knoxデバイスで使用できる専用機能です。これはMDMによって有効にされ、ルーティングポリシーとフィルタリングポリシーを適用するためのソースアプリケーションコンテキストとともにAnyConnectを提供します。これは、AndroidデバイスのVPNゲートウェイから特定のアプリごとのVPNフィルタリングポリシーを実装するために必要です。ポリシーは、ワイルドカードを使用して特定のアプリケーションIDまたはアプリケーションのグループを対象として定義され、各発信パケットの送信元アプリケーションIDと照合されます。

MDMダッシュボードでは、インラインパケットメタデータを有効にするオプションを管理者に提供する必要があります。または、MDMは、このオプションをAnyConnectに対して常に有効にするようにハードコードできます。このオプションは、ヘッドエンドポリシーに従って使用されます。

AnyConnectのアプリごとのVPNポリシーの詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の「Define a Per App VPN Policy for Android Devices」の項を参照してください。

MDMの設定

インラインパケットメタデータを有効にするには、設定のKnox固有属性で「

uidpid_search_enabled」を1に設定します。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
}
}
}
```