AnyConnect Samsung Knox VPN MDM集成指南

目录

AnyConnect实施Samsung Knox VPN框架，并与Knox VPN SDK兼容。建议将Knox版本2.2及更高版本与AnyConnect配合使用。支持来自IKnoxVpnService的所有操作。有关每个操作的详细说明，请参阅三星发布的IKnoxVpnService文档。

Knox VPN JSON配置文件

根据Knox VPN框架的要求，每个VPN配置都使用JSON对象创建。此对象提供了配置的三个主要部分：

1. 常规属性 — "profile_attribute"
2. 供应商(AnyConnect)特定属性 — “供应商”
3. Knox特定配置文件属性 — "knox"

支持的profile_attribute字段

- profileName — 连接条目的唯一名称，显示在AnyConnect主屏幕的连接列表和AnyConnect连接条目的说明字段中。我们建议最多使用24个字符，以确保它们适合连接列表。在字段中输入文本时，使用设备上显示的键盘上的字母、数字或符号。字母区分大小写。

- vpn_type — 用于此连接的VPN协议。有效值为： sslipsec
- vpn_route_type — 有效值为： 0 — 系统VPN1 — 每应用VPN

有关常用配置文件属性的详细信息，请参阅《Samsung KNOX Framework供应商集成指南》。

AnyConnect特定配置通过“供应商”部分内的“**AnyConnectVPNConnection**”键指定。示例：

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

支持的AnyConnectVPNConnection字段

- host — 要连接的ASA的域名、IP地址或组URL。AnyConnect将此参数的值插入AnyConnect连接条目的Server Address字段。

- authentication — （可选）仅在vpn_type（在profile_attributes中）设置为“ipsec”时适用。 指定用于IPsec VPN连接的身份验证方法有效值为：

EAP-AnyConnect（默认值）EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA

- ike-identity — 仅在身份验证设置为EAP-GTC、EAP-MD5或EAP-MSCAPv2时使用。为这些身份验证方法提供IKE身份。

- usergroup（可选）连接到指定主机时要使用的连接配置文件（隧道组）。如果存在，请与HostAddress一起使用，以形成基于组的URL。如果将主协议指定为IPsec，则用户组必须是连接配置文件（隧道组）的确切名称。 对于SSL，用户组是连接配置文件的group-url或group-alias。

- certalias（可选） — 应从Android KeyChain导入的客户端证书的KeyChain别名。用户必须确认Android系统提示，AnyConnect才能使用证书。

- ccmcertalias（可选） — 应从TIMA证书存储导入的客户端证书的TIMA别名。AnyConnect无需用户操作即可接收证书。请注意：此证书必须已明确列入白名单，供AnyConnect使用（例如使用Knox CertificatePolicy API）。

内联VPN数据包应用元数据

VPN数据包的内联应用元数据是Samsung Knox设备上提供的独有功能。它由MDM启用，并为AnyConnect提供源应用情景，以实施路由和过滤策略。在Android设备上从VPN网关实施某些每应用VPN过滤策略时，必须使用此策略。策略通过通配符定义为针对特定应用ID或应用组，并与每个出站数据包的源应用ID匹配。

MDM控制面板应为管理员提供启用内联数据包元数据的选项。或者，MDM可以对此选项进行硬编码，以便始终为AnyConnect启用，AnyConnect将根据头端策略使用此选项。

有关AnyConnect的每应用VPN策略的详细信息，请参阅《Cisco AnyConnect安全移动客户端管理员指南》中的“定义适用于Android设备的每应用VPN策略”部分。

MDM配置

要启用内联数据包元数据，请在Knox特定属性中为配置将“uidpid_search_enabled”设置为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
}
}
}
```