AnyConnect Samsung Knox VPN MDM 통합 설명서

목차

AnyConnect는 Samsung Knox VPN 프레임워크를 구현하며 Knox VPN SDK와 호환됩니다 .AnyConnect에서는 Knox 버전 2.2 이상을 사용하는 것이 좋습니다.IKnoxVpnService의 모든 작업이 지원됩니다.각 작업에 대한 자세한 내용은 삼성에서 게시한 IKnoxVpnService 문서를 참조하십시오.

Knox VPN JSON 프로필

Knox VPN 프레임워크에 필요한 경우 각 VPN 컨피그레이션은 JSON 개체를 사용하여 생성됩니다 .이 개체에는 구성의 세 가지 기본 섹션이 있습니다.

1. 일반 특성 - "profile_attribute"
2. 공급업체(AnyConnect) 특정 특성 - "공급업체"
3. Knox 특정 프로필 특성 - "knox"

지원되는 profile_attribute 필드

- profileName - AnyConnect 홈 화면의 연결 목록과 AnyConnect 연결 항목의 Description 필드에 표시되는 연결 항목의 고유 이름입니다.연결 목록에 맞도록 최대 24자를 사용하는 것이 좋습니다.필드에 텍스트를 입력할 때 장치에 표시되는 키보드의 문자, 숫자 또는 기호를 사용합니다 .문자는 대/소문자를 구분합니다.

- vpn_type - 이 연결에 사용되는 VPN 프로토콜입니다.유효한 값은 다음과 같습니다. sslipsec
- vpn_route_type - 유효한 값은 다음과 같습니다. 0 - 시스템 VPN1 - 앱당 VPN

공통 프로파일 특성에 대한 자세한 내용은 Samsung KNOX Framework Vendor Integration Guide를 참조하십시오.

AnyConnect 특정 컨피그레이션은 "vendor" 섹션 내부에서 "**AnyConnectVPNConnection**" 키를 통해 지정됩니다.샘플:

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

지원되는 AnyConnectVPNC연결 필드

- host - 연결할 ASA의 도메인 이름, IP 주소 또는 그룹 URL입니다.AnyConnect는 이 매개변수의 값을 AnyConnect 연결 항목의 Server Address 필드에 삽입합니다.

- authentication - (선택 사항) vpn_type(profile_attributes)이 "ipsec"으로 설정된 경우에만 적용됩니다. IPsec VPN 연결에 사용되는 인증 방법을 지정합니다. 유효한 값은 다음과 같습니다. EAP-AnyConnect(기본값)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity - 인증이 EAP-GTC, EAP-MD5 또는 EAP-MSCAPv2로 설정된 경우에만 사용됩니다. 이러한 인증 방법에 대한 IKE ID를 제공합니다.

- usergroup(선택 사항) 지정된 호스트에 연결할 때 사용할 연결 프로파일(터널 그룹)입니다.있는 경우 HostAddress와 함께 사용하여 그룹 기반 URL을 형성합니다.Primary Protocol을 IPsec으로 지정하는 경우 User Group은 연결 프로파일(터널 그룹)의 정확한 이름이어야 합니다. SSL의 경우 사용자 그룹은 연결 프로파일의 group-url 또는 group-alias입니다.

- certalias(선택 사항) - Android KeyChain에서 가져와야 하는 클라이언트 인증서의 KeyChain 별칭입니다.AnyConnect에서 인증서를 사용하려면 사용자가 Android 시스템 프롬프트를 승인해야 합니다.

- ccmcertalias(선택 사항) - TIMA 인증서 저장소에서 가져와야 하는 클라이언트 인증서의 TIMA 별칭AnyConnect에서 인증서를 받는 데 필요한 사용자 작업은 없습니다.참고:이 인증서는 AnyConnect에서 사용할 수 있도록 명시적으로 허용 목록에 추가되어 있어야 합니다(예: Knox CertificatePolicy API 사용).

인라인 VPN 패킷 앱 메타데이터

VPN 패킷용 인라인 앱 메타데이터는 삼성 녹스 디바이스에서 사용할 수 있는 전용 기능입니다.MDM에서 활성화되며 라우팅 및 필터링 정책을 적용하기 위해 소스 애플리케이션 컨텍스트와 AnyConnect를 제공합니다.Android 디바이스의 VPN 게이트웨이에서 특정 앱별 VPN 필터링 정책을 구현하는 데 필요합니다.정책은 와일드카드를 통해 특정 애플리케이션 ID 또는 앱 그룹을 대상으로 지정하도록 정의되며 각 아웃바운드 패킷의 소스 애플리케이션 ID와 일치합니다.

MDM 대시보드는 관리자에게 인라인 패킷 메타데이터를 활성화하는 옵션을 제공해야 합니다.또는 MDM은 항상 AnyConnect에 대해 활성화되도록 이 옵션을 하드코딩할 수 있으며, 이는 헤드엔드 정책에 따라 이를 사용합니다.

AnyConnect의 퍼 앱(per-app) VPN 정책에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client Administrator Guide의 "Define a App VPN Policy for Android Devices" 단원을 참조하십시오.

MDM 컨피그레이션

인라인 패킷 메타데이터를 활성화하려면 구성에 대한 Knox 특정 속성에서 "uidpid_search_enabled"를 1로 설정합니다.샘플:

```
{
"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
}
}
}
```