AnyConnect Samsung Knox VPN MDM-Integrationsanleitung

Inhalt

AnyConnect implementiert das VPN-Framework von Samsung Knox und ist mit dem Knox VPN SDK kompatibel. Es wird empfohlen, mit AnyConnect die Knox-Version 2.2 und höher zu verwenden. Alle Vorgänge von IKnoxVpnService werden unterstützt. Eine detaillierte Beschreibung der einzelnen Vorgänge finden Sie in der IKnoxVpnService-Dokumentation von Samsung.

Knox VPN JSON-Profil

Wie im Knox VPN-Framework erforderlich, wird jede VPN-Konfiguration mit einem JSON-Objekt erstellt. Dieses Objekt enthält drei Hauptabschnitte der Konfiguration:

1. Allgemeine Attribute - "profile_attribute"
2. Herstellerspezifische (AnyConnect) Attribute - "Anbieter"
3. Knox-spezifische Profilattribute - "knox"

Unterstützte profile_attribut-Felder

- profileName - Ein eindeutiger Name für den Verbindungseintrag, der in der Verbindungsliste des AnyConnect-Hauptbildschirms und im Feld Description (Beschreibung) des AnyConnect-Verbindungseintrags angezeigt wird. Es wird empfohlen, maximal 24 Zeichen zu verwenden, um sicherzustellen, dass diese in die Verbindungsliste aufgenommen werden. Verwenden Sie Buchstaben, Zahlen oder Symbole auf der Tastatur, die auf dem Gerät angezeigt wird, wenn Sie Text in ein Feld eingeben. Bei den Buchstaben wird die Groß- und Kleinschreibung beachtet.

- vpn_type - Das für diese Verbindung verwendete VPN-Protokoll. Gültige Werte sind: SSLIPS
- vpn_route_type - Gültige Werte sind: 0 - System-VPN1 - anwendungsbasiertes VPN

Weitere Informationen zu den allgemeinen Profilattributen finden Sie im Integrationsleitfaden für Samsung KNOX Framework-Anbieter.

Die AnyConnect-spezifische Konfiguration wird im Abschnitt "Anbieter" über den Schlüssel **"AnyConnectVPNCConnection"** festgelegt. Beispiel:

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

```
}
}
```

Unterstützte AnyConnectVPNConnectionsfelder

- host: Der Domänenname, die IP-Adresse oder die Gruppen-URL der ASA, mit der eine Verbindung hergestellt werden soll. AnyConnect fügt den Wert dieses Parameters in das Feld Server Address des AnyConnect-Verbindungseintrags ein.

- authentication - (optional) Gilt nur, wenn vpn_type (in profile_attribute) auf "ipsec" festgelegt ist. Gibt die für eine IPsec-VPN-Verbindung verwendete Authentifizierungsmethode an. Gültige Werte sind:
  EAP-AnyConnect (Standardwert)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity - Wird nur verwendet, wenn die Authentifizierung auf EAP-GTC, EAP-MD5 oder EAP-MSCAPv2 festgelegt ist. Stellt die IKE-Identität für diese Authentifizierungsmethoden bereit.

- usergroup (optional) Das Verbindungsprofil (Tunnelgruppe), das bei der Verbindung mit dem angegebenen Host verwendet wird. Verwenden Sie ggf. zusammen mit HostAddress eine gruppenbasierte URL. Wenn Sie das primäre Protokoll als IPsec angeben, muss die Benutzergruppe der genaue Name des Verbindungsprofils (Tunnelgruppe) sein. Bei SSL ist die Benutzergruppe die Gruppen-URL oder Gruppen-Alias des Verbindungsprofils.

- certalias (optional) - KeyChain-Alias für ein Clientzertifikat, das aus der Android KeyChain importiert werden soll. Der Benutzer muss eine Android-Systemaufforderung bestätigen, bevor das Zertifikat von AnyConnect verwendet werden kann.

- cccertalias (optional) - TIMA-Alias für ein Client-Zertifikat, das aus dem TIMA-Zertifikatsspeicher importiert werden soll. Für den Empfang der Zertifizierung durch AnyConnect ist keine Benutzeraktion erforderlich. Hinweis: Dieses Zertifikat muss explizit für die Verwendung durch AnyConnect Whitelist (z. B. über die Knox CertificatePolicy API) gezeichnet worden sein.

Inline-VPN-Paketanwendungsmetadaten

Inline-App-Metadaten für VPN-Pakete sind eine exklusive Funktion, die auf Samsung Knox-Geräten verfügbar ist. Er wird vom MDM aktiviert und stellt AnyConnect mit dem Kontext der Quellanwendung zum Durchsetzen von Routing- und Filterrichtlinien zur Verfügung. Sie ist für die Implementierung bestimmter anwendungsspezifischer VPN-Filterungsrichtlinien vom VPN-Gateway auf Android-Geräten erforderlich. Die Richtlinien werden für die Ziel-Anwendungs-ID oder Gruppen von Anwendungen über Platzhalter definiert und mit der Quell-Anwendungs-ID jedes ausgehenden Pakets abgeglichen.

Das MDM-Dashboard sollte Administratoren eine Option zum Aktivieren von Inline-Paketmetadaten bieten. Alternativ kann MDM diese Option hardcodieren, sodass sie immer für AnyConnect aktiviert ist. Diese Option wird gemäß Headend-Richtlinie verwendet.

Weitere Informationen zu VPN-Richtlinien für AnyConnect pro Anwendung finden Sie im Abschnitt "Definieren einer VPN-Richtlinie pro Anwendung für Android-Geräte" im Administratorleitfaden für den Cisco AnyConnect Secure Mobility Client.

MDM-Konfiguration

Um Inline-Paketmetadaten zu aktivieren, legen Sie im Knox-spezifischen Attribut für eine Konfiguration "uidpid_search_enabled" auf 1 fest. Beispiel:

```
{
"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
}
}
}
```