Guia de integração de AnyConnect Samsung Knox VPN MDM

Índice

AnyConnect executa a estrutura de Samsung Knox VPN e é compatível com o Knox VPN SDK. Recomendou usar a versão 2.2 e mais recente de Knox com AnyConnect. Todas as operações de IKnoxVpnService são apoiadas. Para a descrição detalhada de cada operação, veja por favor a documentação de IKnoxVpnService publicada por Samsung.

Perfil de Knox VPN JSON

Segundo as exigências da estrutura de Knox VPN, cada configuração de VPN é criada usando um objeto JSON. Este objeto tem fornece três seções principais da configuração:

1. Atributos do general - “profile_attribute”
2. Atributos do específico do vendedor (AnyConnect) - “vendedor”
3. Atributos específicos do perfil de Knox - “knox”

Campos apoiados do profile_attribut

- profileName - Nome exclusivo para que a entrada de conexão apareça no a lista da conexão da tela home de AnyConnect e o campo de descrição da entrada de conexão de AnyConnect. Nós recomendamos usar um máximo de 24 caráteres para assegurar-se de que caibam na lista da conexão. Use letras, números, ou símbolos no teclado indicado no dispositivo quando você incorpora o texto em um campo. As letras são diferenciando maiúsculas e minúsculas.

- vpn_type - O protocolo VPN usado para esta conexão. Os valores válidos são: SSLipsec
- vpn_route_type - Os valores válidos são: 0 – Sistema VPN1 – Por-APP VPN

Para obter mais informações sobre dos atributos do perfil da terra comum, veja por favor o guia de integração do vendedor da estrutura KNOX de Samsung.

A configuração específica de AnyConnect é especificada através do interior da chave de “**AnyConnectVPNConnection**” para dentro a seção do “vendedor”. Amostra:

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

Campos apoiados de AnyConnectVPNConnection

- host - O Domain Name, o IP address, ou o grupo URL do ASA com que a conectar. AnyConnect introduz o valor deste parâmetro no campo de endereço do servidor da entrada de conexão de AnyConnect.

- autenticação - (opcional) aplica-se somente quando o vpn_type (nos profile_attributes) é ajustado ao “ipsec”. Especifica o método de autenticação usado para valores válidos de uma conexão do IPSec VPN são:
  EAP-AnyConnect (valor padrão)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- IKE-identidade - Usado somente se a autenticação é ajustada ao EAP-GTC, ao EAP-MD5, ou ao EAP-MSCAPv2. Fornece a identidade IKE para estes métodos de autenticação.

- grupo de utilizadores (opcional) o perfil de conexão (grupo de túneis) a usar-se ao conectar ao host especificado. Se presente, usado conjuntamente com o host address para formar uma URL Grupo-baseada. Se você especifica o protocolo preliminar como IPsec, o grupo de usuário deve ser o nome exato do perfil de conexão (grupo de túneis). Para o SSL, o grupo de usuário é a grupo-URL ou o grupo-pseudônimo do perfil de conexão.

- certalias (opcionais) - Pseudônimo de KeyChain de um certificado de cliente que deva ser importado de Android KeyChain. O usuário deveu reconhecer um alerta do sistema de Android antes que o CERT poderia ser usado por AnyConnect.

- ccmcertalias (opcionais) - Pseudônimo TIMA de um certificado de cliente que deva ser importado da loja do certificado TIMA. Nenhuma ação de usuário é necessária para que AnyConnect receba o CERT. Note por favor: este certificado deve explicitamente ter sido whitelisted para o uso de AnyConnect (por exemplo usando o Knox CertificatePolicy API).

Metadata Inline do App do pacote de VPN

Os metadata Inline do app para pacotes de VPN são uma característica exclusiva disponível em dispositivos de Samsung Knox. É permitido pelo MDM e fornece AnyConnect o contexto do aplicativo de fonte reforçando o roteamento e as políticas de filtragem. Exige-se executando determinadas políticas de filtragem por-APP VPN do gateway de VPN em dispositivos de Android. As políticas são definidas para visar a identificação do aplicativo ou grupos específicos de apps através de wildcarding e combinadas contra a identificação do aplicativo de fonte de cada pacote externo.

O painel MDM deve fornecer administradores uma opção para permitir metadata inline do pacote. Alternativamente, o MDM poderia hardcode esta opção sempre ser permitida para AnyConnect, que a utilizará conforme a política do final do cabeçalho.

Para obter mais informações sobre das políticas de VPN por-APP de AnyConnect, veja por favor a seção em “definir a pela política de VPN do App para dispositivos de Android” no guia do administrador do Cliente de mobilidade Cisco AnyConnect Secure.

Configuração MDM

Para permitir metadata inline do pacote, ajuste “uidpid_search_enabled” a 1 no atributo específico de Knox para uma configuração. Amostra:

```
{
"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
}
}
}
```