AnyConnect Samsung Knox VPN MDM Integration Guide

Contents

AnyConnect implements the Samsung Knox VPN framework and is compatible with the Knox VPN SDK. It's recommended to use Knox version 2.2 and above with AnyConnect. All operations from IKnoxVpnService are supported. For detailed description of each operation, please see the IKnoxVpnService documentation published by Samsung.

Knox VPN JSON Profile

As required by the Knox VPN framework, each VPN configuration is created using a JSON object. This object has provides three main sections of the configuration:

1. General attributes - "profile_attribute"
2. Vendor (AnyConnect) specific attributes - "vendor"
3. Knox specific profile attributes - "knox"

Supported profile_attribut Fields

- profileName - Unique name for the connection entry to appear in the connection list of the AnyConnect home screen and the Description field of the AnyConnect connection entry. We recommend using a maximum of 24 characters to ensure that they fit in the connection list. Use letters, numbers, or symbols on the keyboard displayed on the device when you enter text into a field. The letters are case-sensitive.

- vpn_type - The VPN protocol used for this connection. Valid values are: sslipsec
- vpn_route_type - Valid values are: 0 – System VPN1 – Per-app VPN

For more information regarding the common profile attributes, please see the Samsung KNOX Framework Vendor Integration Guide.

AnyConnect specific configuration is specified via "**AnyConnectVPNConnection**" key inside inside the "vendor" section. Sample:

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

Supported AnyConnectVPNConnection Fields

- host - The domain name, IP address, or Group URL of the ASA with which to connect. AnyConnect inserts the value of this parameter into the Server Address field of the AnyConnect connection entry.

- authentication - (optional) Only applies when vpn_type (in profile_attributes) is set to "ipsec". Specifies the authentication method used for an IPsec VPN connection Valid values are: EAP-AnyConnect (default value)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity - Used only if authentication is set to EAP-GTC, EAP-MD5, or EAP-MSCAPv2. Provides the IKE identity for these authentication methods.

- usergroup (optional) The connection profile (tunnel group) to use when connecting to the specified host. If present, used in conjunction with HostAddress to form a Group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

- certalias (optional)- KeyChain alias of a client certificate that should be imported from Android KeyChain. The user must acknowledge an Android system prompt before the cert could be used by AnyConnect.

- ccmcertalias (optional)- TIMA alias of a client certificate that should be imported from the TIMA certificate store. No user action is necessary for AnyConnect to receive the cert. Please note: this certificate must have been explicitly whitelisted for use by AnyConnect (e.g. using the Knox CertificatePolicy API).

Inline VPN Packet App Metadata

Inline app metadata for VPN packets is an exclusive feature available on Samsung Knox devices. It is enabled by MDM and provides AnyConnect with source application context for enforcing routing and filtering policies. It is required for implementing certain per-app VPN filtering policies from the VPN gateway on Android devices. Policies are defined to target specific application id or groups of apps via wildcarding and is matched against the source application id of each outbound packet.

MDM dashboard should provide administrators with an option to enable inline packet metadata. Alternatively, MDM could hardcode this option to always be enabled for AnyConnect, which will make use of it as per headend policy.

For more information on AnyConnect’s per-app VPN policies, please see the section on "Define a Per App VPN Policy for Android Devices" in the Cisco AnyConnect Secure Mobility Client Administrator Guide.

MDM Configuration

To enable inline packet metadata, set "uidpid_search_enabled" to 1 in the Knox specific attribute for a configuration. Sample:

```
{
```

```
"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
}
}
}
```