Guía de integración de MDM de VPN Knox de AnyConnect Samsung

Contenido

AnyConnect implementa el marco de VPN Samsung Knox y es compatible con el Knox VPN SDK. Se recomienda utilizar Knox versión 2.2 o posterior con AnyConnect. Se admiten todas las operaciones de IKnoxVpnService. Para obtener una descripción detallada de cada operación, consulte la documentación de IKnoxVpnService publicada por Samsung.

Perfil JSON de VPN Knox

Como requiere el marco de trabajo VPN de Knox, cada configuración VPN se crea mediante un objeto JSON. Este objeto proporciona tres secciones principales de la configuración:

1. Atributos generales - "profile_attribute"
2. Atributos específicos del proveedor (AnyConnect): "proveedor"
3. Atributos de perfil específicos de Knox - "knox"

Campos de Profile_attribut admitidos

- profileName: nombre único para que la entrada de conexión aparezca en la lista de conexiones de la pantalla de inicio de AnyConnect y en el campo Description de la entrada de conexión de AnyConnect. Se recomienda utilizar un máximo de 24 caracteres para asegurarse de que encajan en la lista de conexiones. Utilice letras, números o símbolos en el teclado mostrado en el dispositivo cuando introduzca texto en un campo. Las letras distinguen entre mayúsculas y minúsculas.

- vpn_type: el protocolo VPN utilizado para esta conexión. Los valores válidos son: sslipsec
- vpn_route_type - Los valores válidos son: 0 - VPN del sistema1 - VPN por aplicación

Para obtener más información sobre los atributos de perfil comunes, consulte la Guía de integración de proveedores de Samsung KNOX Framework.

La configuración específica de AnyConnect se especifica mediante la clave "**AnyConnectVPNConnection**" dentro de la sección "proveedor". Ejemplo:

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

Campos de conexión AnyConnectVPNC admitidos

- host: el nombre de dominio, la dirección IP o la URL de grupo del ASA con el que conectarse. AnyConnect inserta el valor de este parámetro en el campo Dirección de servidor de la entrada de conexión de AnyConnect.

- authentication - (opcional) Sólo se aplica cuando vpn_type (in profile_attribute) se establece en "ipsec". Especifica el método de autenticación utilizado para una conexión VPN IPsec Los valores válidos son:
  EAP-AnyConnect (valor predeterminado)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity: se utiliza sólo si la autenticación está configurada en EAP-GTC, EAP-MD5 o EAP-MSCAPv2. Proporciona la identidad IKE para estos métodos de autenticación.

- usergroup (opcional) Perfil de conexión (grupo de túnel) que se utiliza al conectarse al host especificado. Si está presente, se utiliza junto con HostAddress para formar una dirección URL basada en grupo. Si especifica el protocolo principal como IPSec, el grupo de usuarios debe ser el nombre exacto del perfil de conexión (grupo de túnel). Para SSL, el grupo de usuarios es la url de grupo o el alias de grupo del perfil de conexión.

- certalias (opcional): alias KeyChain de un certificado de cliente que se debe importar de Android KeyChain. El usuario debe aceptar un mensaje del sistema Android antes de que AnyConnect pueda utilizar el certificado.

- ccmcertalias (opcional): alias TIMA de un certificado de cliente que se debe importar del almacén de certificados TIMA. No es necesario que el usuario realice ninguna acción para que AnyConnect reciba el certificado. Tenga en cuenta lo siguiente: este certificado se debe haber incluido explícitamente en la lista blanca para que lo utilice AnyConnect (por ejemplo, mediante la API de Knox CertificatePolicy).

Metadatos de aplicaciones de paquetes VPN en línea

Los metadatos de la aplicación en línea para los paquetes VPN es una función exclusiva disponible en los dispositivos Samsung Knox. MDM lo habilita y proporciona AnyConnect con el contexto de la aplicación de origen para aplicar políticas de enrutamiento y filtrado. Se requiere para implementar ciertas políticas de filtrado VPN por aplicación desde el gateway VPN en los dispositivos Android. Las políticas se definen para el ID de aplicación específico o los grupos de aplicaciones a través del comodín y se comparan con el id de aplicación de origen de cada paquete saliente.

El panel MDM debe proporcionar a los administradores una opción para habilitar los metadatos de paquetes en línea. Como alternativa, MDM podría codificar esta opción para que siempre esté habilitada para AnyConnect, que la utilizará según la política de cabecera.

Para obtener más información sobre las políticas de VPN por aplicación de AnyConnect, consulte la sección "Definición de una política de VPN por aplicación para dispositivos Android" en la Guía del administrador de Cisco AnyConnect Secure Mobility Client.

Configuración de MDM

Para habilitar los metadatos del paquete en línea, establezca "uidpid_search_enabled" en 1 en el atributo específico de Knox para una configuración. Ejemplo:

```
{
"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
}
}
}
```