Fonctionnalités prises en charge par le client de mobilité sécurisée Cisco AnyConnect pour les périphériques Android

Objectif

Le client Cisco AnyConnect Secure Mobility, également appelé client VPN Cisco AnyConnect, est une application logicielle pour la connexion à un réseau privé virtuel (VPN) qui fonctionne sur différents systèmes d'exploitation et configurations matérielles. Cette application logicielle permet aux ressources distantes d'un autre réseau de devenir accessibles comme si l'utilisateur était directement connecté au réseau, mais de manière sécurisée. Le client Cisco AnyConnect Secure Mobility offre une nouvelle façon innovante de protéger les utilisateurs mobiles sur des plates-formes informatiques ou de smartphones, offrant une expérience plus transparente et toujours protégée pour les utilisateurs finaux et une application complète des politiques pour un administrateur informatique.

L'objectif de ce document est de présenter la matrice des fonctionnalités du client Cisco AnyConnect Secure Mobility pour les périphériques Android.

Version du logiciel

- 4.4

Matrice des fonctionnalités d'Android AnyConnect

Déploiement et configuration

Installer ou mettre à niveau à partir du magasin d'applications	Oui
Prise en charge du profil VPN Cisco (importation manuelle)	Oui
Prise en charge du profil VPN Cisco (importation lors de la connexion)	Oui
Entrées de connexion configurées pour la gestion des appareils mobiles (MDM)	Oui
Entrées de connexion configurées par l'utilisateur	Oui

Tunnellisation

Sécurité de la couche	Oui

transport (TLS)	
TLS de datagramme (DTLS)	Oui
Internet Protocol Security Internet Key Exchange version 2 Network Address Translator Traversal (IPsec IKEv2 NAT-T)	Oui
IKEv2 - ESP (Encapsulating Security Payload) brut	Non
Suite B (IPsec uniquement)	Oui
Compression TLS	Oui
Détection des homologues morts	Oui
keepalive de tunnel	Oui
Plusieurs interfaces réseau actives	Non
Tunnellisation par application (nécessite une licence Plus ou Apex et ASA 9.4.2 ou ultérieure)	Oui, Android 5.0+ ou Samsung Knox
Tunnel complet (le système d'exploitation peut faire des exceptions sur certains trafics, tels que le trafic vers le magasin d'applications)	Oui
Tunnel fractionné (y compris fractionné)	Oui
Réseau local (LAN) (à l'exclusion des zones séparées)	Non
Système DNS (Split-Domain Name System)	Oui, fonctionnera avec l'inclusion fractionnée.
Reconnexion automatique / Itinérance réseau	Oui, quelle que soit la spécification de profil Auto Reconnect, AnyConnect Mobile tente toujours de maintenir le VPN lorsque les utilisateurs se déplacent entre les réseaux 3G et Wi-Fi.
VPN à la demande (déclenché par la destination)	Non
VPN à la demande (déclenché par l'application)	Non
Retouche	Oui
Transport public IPv4	Oui
Transport public IPv6	Oui, nécessite Android 5.0 ou version ultérieure

Tunnel IPv4 sur IPv4	Oui
Tunnel IPv6 sur IPv4	Oui
Domaine par défaut	Oui
Configuration du serveur DNS	Oui
Prise en charge de proxy côté privé	Non, les proxy Wi-Fi sont désactivés lorsque le VPN est établi.
Exceptions de proxy	Non
Prise en charge du proxy côté public	Non
Bannière de pré-connexion	Oui
Bannière post-connexion	Oui
Préservation des points de code de services différenciés (DSCP)	Oui

Connexion et déconnexion

Équilibrage de charge VPN	Oui
Liste des serveurs de sauvegarde	Oui
Sélection optimale de la passerelle	Non

Authentification

Authentification du certificat client	Oui
Protocole OCSP (Online Certificate Status Protocol)	Oui
Gestion manuelle des certificats d'utilisateur	Oui
Gestion manuelle des certificats de serveur	Oui
Protocole d'inscription de certificat simple Inscription existante (SCEP) Veuillez confirmer pour votre plate-forme.	Oui
Inscription au proxy SCEP Veuillez confirmer pour votre plate-forme.	Oui
Sélection automatique des certificats	Oui
Sélection manuelle du certificat	Oui
Prise en charge des cartes à puce	Non

Nom d'utilisateur et mot de passe	Oui
Jeton ou défi	Oui
Authentification double	Oui
URL (Uniform Resource Locator) de groupe (spécifié dans l'adresse du serveur)	Oui
Sélection de groupe (liste déroulante)	Oui
Préremplissage des informations d'identification à partir du certificat utilisateur	Oui
Enregistrer le mot de passe	Non

Interface utilisateur

Interface utilisateur graphique autonome	Oui
Interface utilisateur du système d'exploitation natif	Non
Gestionnaire API (Application Program Interface) / URI (Uniform Resource Identifier) (voir Gestion URI)	Oui
Personnalisation de l'interface utilisateur	Non
Localisation de l'interface utilisateur	Oui, l'application contient des langues préemballées.
Préférences utilisateur	Oui
widgets d'écran d'accueil pour un accès VPN en un clic	Oui
Icône d'état spécifique à AnyConnect	Facultatif

Position mobile

Numéro de série ou vérification d'ID unique	Oui
OS et version AnyConnect partagés avec tête de réseau	Oui

Gestion URI

Ajouter une entrée de connexion	O

	ui
Connexion à un VPN	Oui
Préremplissage des informations d'identification lors de la connexion	Oui
Déconnecter VPN	Oui
Importer le certificat	Oui
Importer les données de localisation	Oui
Importer le langage de balisage extensible Profil client (XML)	Oui
Contrôle externe (utilisateur) des commandes URI	Oui

Rapports et dépannage

Statistiques	Oui
Journalisation / Informations de diagnostic (DART)	Oui

Certifications

FIPS 140-2 niveau 1	Oui

Pour plus d'informations sur les licences AnyConnect sur les routeurs de la gamme RV340, consultez l'article Licence AnyConnect pour les routeurs de la gamme RV340.