Een snel VPN-alternatief voor Mac OS implementeren op RV016, RV042, RV042G en RV082 VPN-routers

Doel

Er is geen Quick VPN versie geschikt voor Mac OS. Er is echter een groeiend aantal gebruikers die een Quick VPN-alternatief voor Mac OS willen implementeren. In dit artikel wordt IP Security gebruikt als alternatief voor een snelle VPN.

Opmerking: U moet de IP-beveiligingen downloaden en installeren op uw MAC OS voordat u de configuratie start. U kunt het downloaden via de volgende link:

http://www.lobotomo.com/products/IPSecuritas/

In dit artikel wordt uitgelegd hoe u een Quick VPN-alternatief voor Mac OS kunt implementeren op RV016, RV042, RV042G en RV082 VPN-routers.

Toepasselijke apparaten

· RV016
â€¢RV042
· RV042G
· RV082

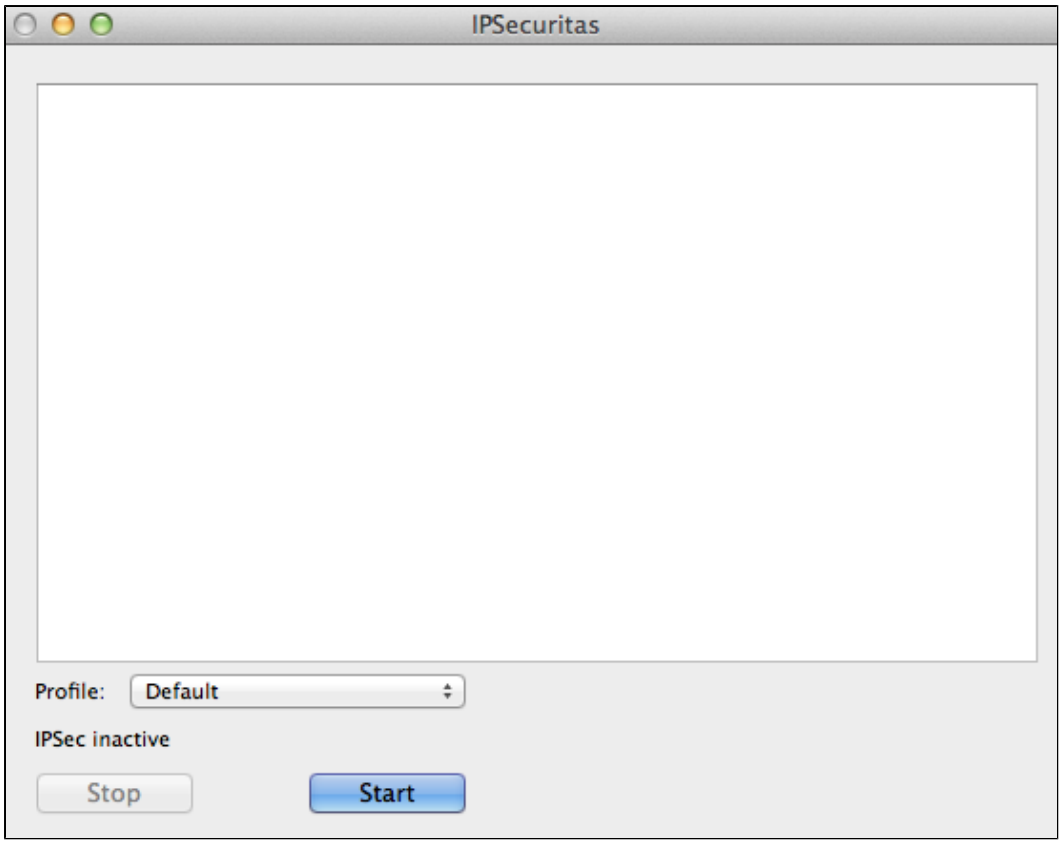
Softwareversie

· v4.2.2.08

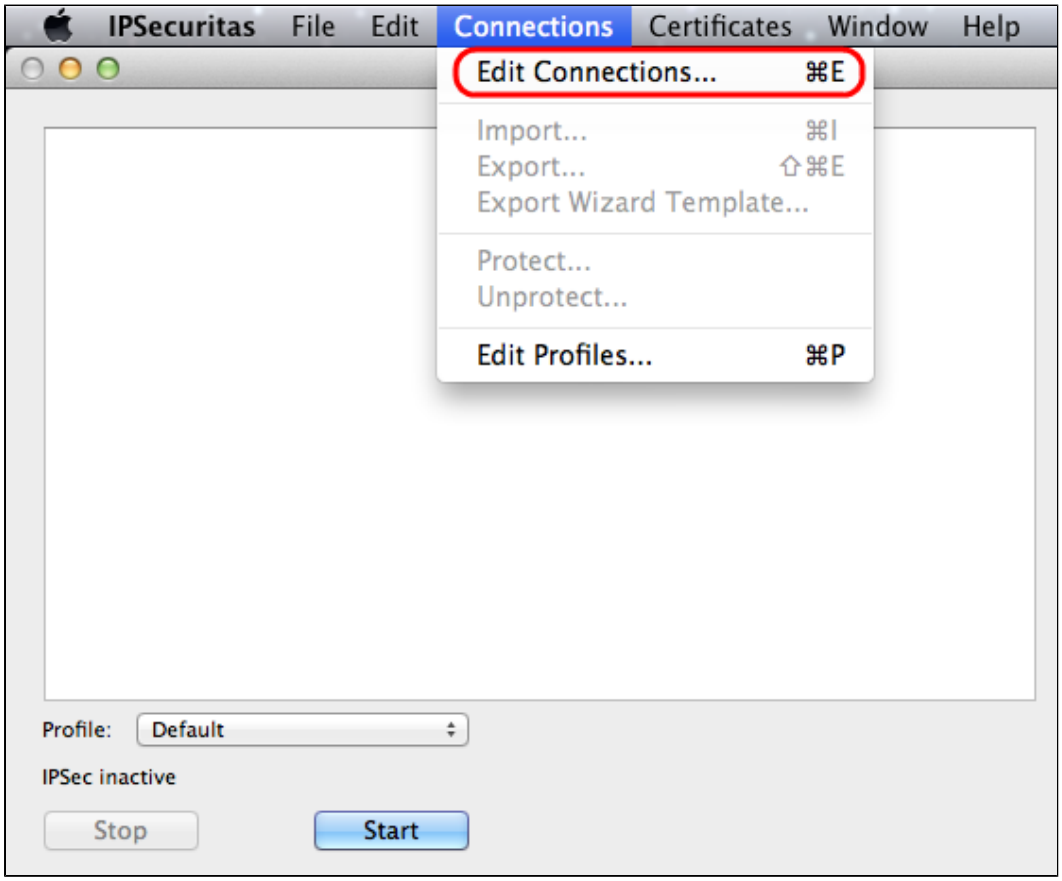
Een Quick VPN-alternatief voor Mac OS implementeren

Opmerking: de configuratie van VPN-client naar gateway van het apparaat moet eerst worden uitgevoerd. Raadpleeg *Een externe toegangstunnel (client naar gateway) instellen voor VPN-clients op RV016, RV042, RV042G en RV082 VPN-routers voor meer informatie over het* configureren van VPN-client voor gateway.

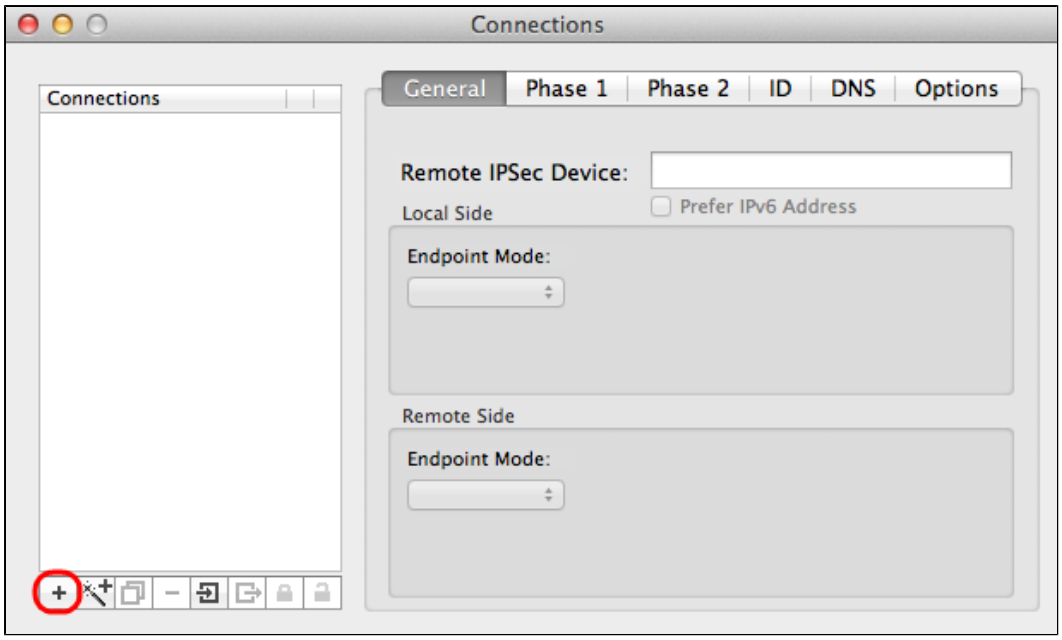
Stap 1. Voer de IP-beveiliging uit op het Mac OS. Het venster *IPSecuritas* verschijnt:



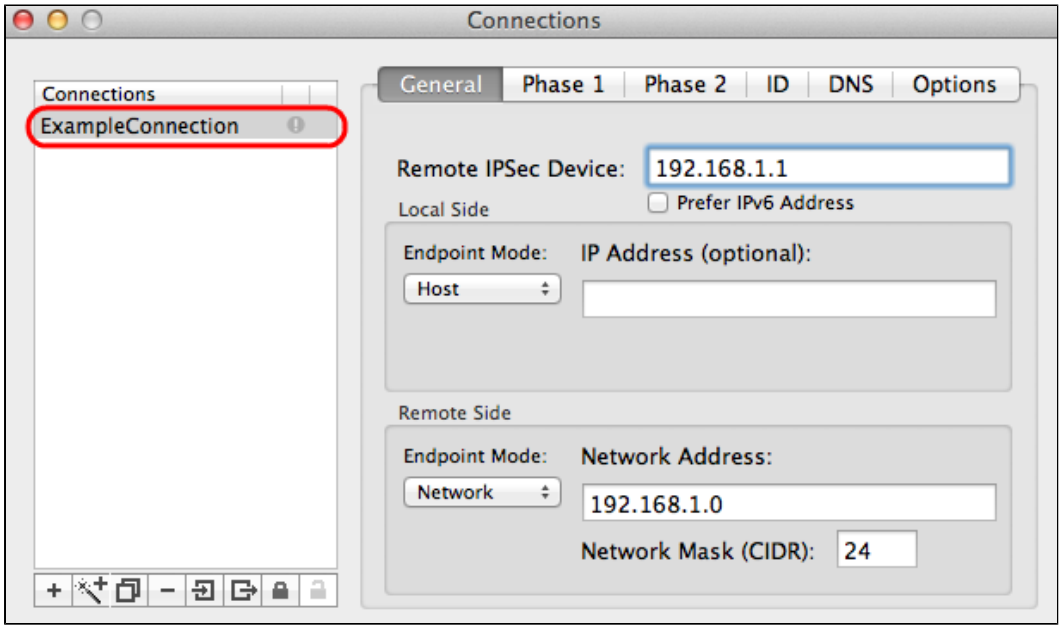
Stap 2. Klik op **Start**.



Stap 3. Kies **Verbindingen > Verbindingen bewerken** op de menubalk. Het venster *Connections* verschijnt.

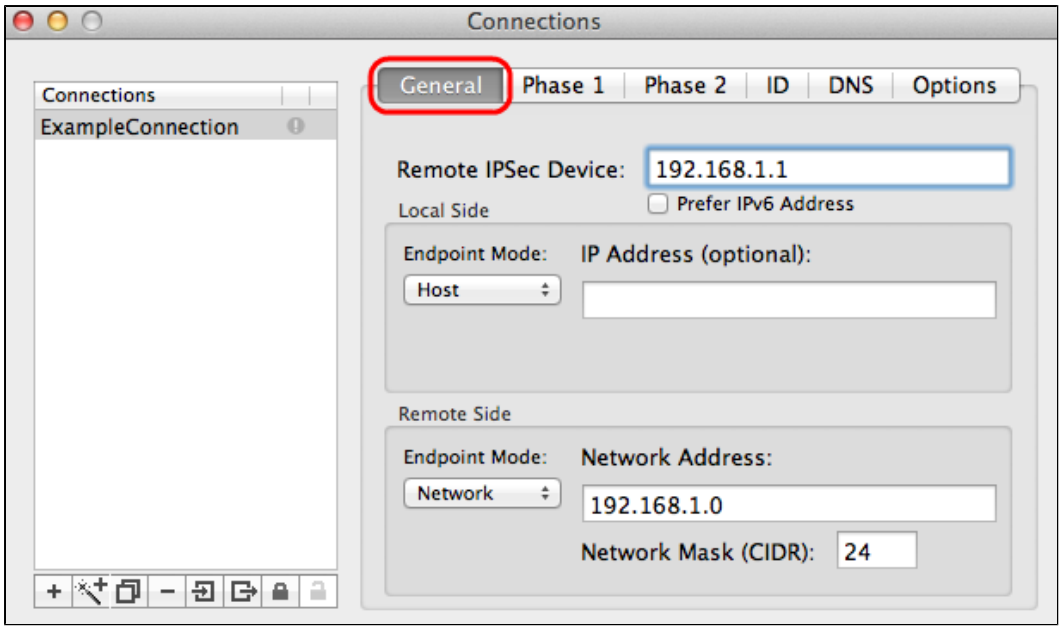


Stap 4. Klik op het + pictogram om een nieuwe verbinding toe te voegen.



Stap 5. Voer een naam in voor de nieuwe verbinding onder verbindingen.

Algemeen



Stap 1. Klik op het tabblad **Algemeen**.

Stap 2. Voer het IP-adres van de externe router in het veld Extern IPSec-apparaat in.

Opmerking: u hoeft Local Side niet te configureren omdat deze configuratie is bedoeld voor een externe client. U hoeft alleen de afstandsbediening te configureren.

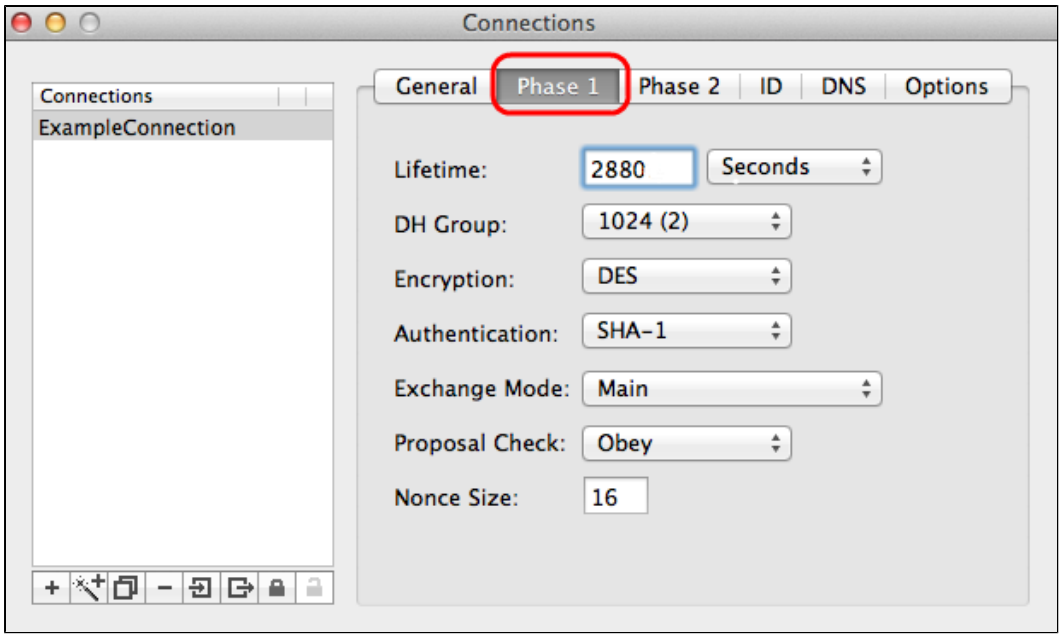
Stap 3. Kies in het gedeelte Remote Side **Network** in de vervolgkeuzelijst Endpoint Mode.

Stap 4. Voer het subnetmasker in in het veld Netwerkmasker (CIDR).

Stap 5. Voer het externe netwerkadres in het veld Netwerkadres in.

Fase 1

Fase 1 is de simplex, logical security associatie (SA) tussen de twee uiteinden van de tunnel om beveiligde geauthenticeerde communicatie te ondersteunen.



Stap 1. Klik op het tabblad **Fase 1**.

Stap 2. Voer de levensduur in die u tijdens de configuratie van de tunnel in het veld Leven hebt ingevoerd. Als de tijd verstrijkt, wordt automatisch opnieuw onderhandeld over een nieuwe sleutel. De belangrijkste levensduur kan variëren van 1081 tot 86400 seconden. De standaardwaarde voor fase 1 is 28800 seconden.

Stap 3. Kies de juiste tijdseenheid voor het Leven uit de vervolgkeuzelijst Leven. De standaardinstelling is seconden.

Stap 4. Kies dezelfde DH-groep die u hebt opgegeven voor de configuratie van de tunnel in de vervolgkeuzelijst DH-groep. De Diffie-Hellman (DH) groep wordt gebruikt voor sleuteluitwisseling.

Stap 5. Kies het coderingstype in de vervolgkeuzelijst Encryptie die u hebt ingevoerd voor de configuratie van de tunnel. De methode Encryption bepaalt de lengte van de sleutel die wordt gebruikt om ESP-pakketten (Encapsulating Security payload) te versleutelen of te decrypteren.

Stap 6. Kies de verificatiemethode die u hebt ingevoerd voor de configuratie van de tunnel uit de vervolgkeuzelijst Verificatie. Het type verificatie bepaalt de methode voor het verifiëren van ESP-pakketten.

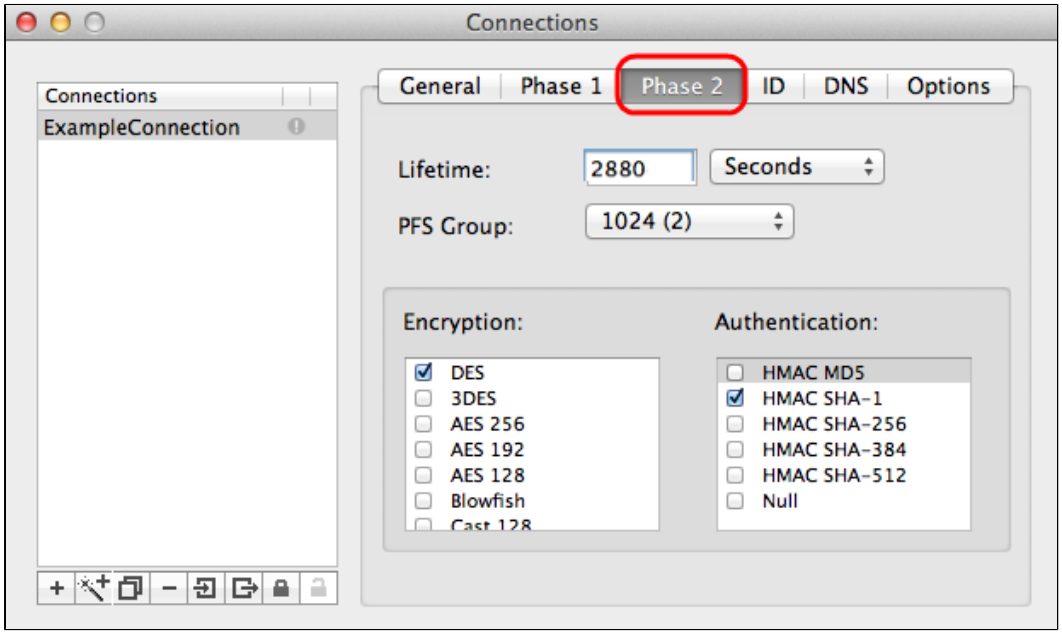
Stap 7. Kies de gewenste uitwisselingsmodus in de vervolgkeuzelijst Exchange Mode.

· Main â€" vertegenwoordigt uitwisselingsmodus voor alle type gateway behalve Full Qualified Domain Name (FQDN).

· Aggressief â€" Vertegenwoordigt de uitwisselingsmodus voor FQDN-gateway (Full Qualified Domain Name).

Fase 2

Fase 2 is de beveiligingskoppeling om de beveiliging van het gegevenspakket tijdens de gegevenspakketten die door de twee eindpunten worden doorgegeven, te bepalen.



Stap 1. Klik op het tabblad **Fase 2**.

Stap 2. Voer hetzelfde leven in in het veld Leven dat u invoert voor de configuratie van de tunnel en

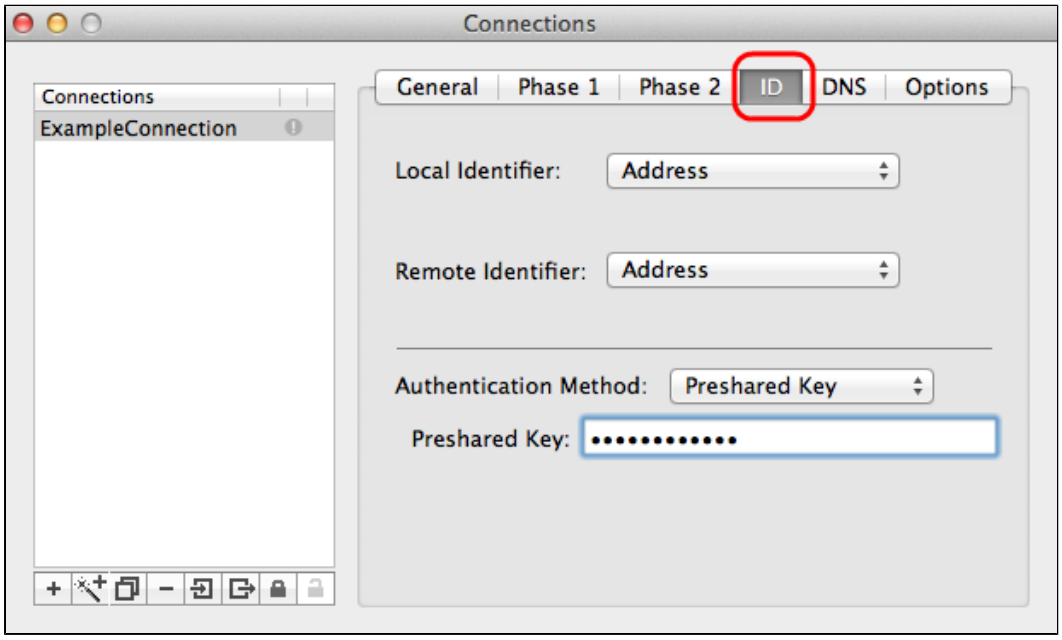
ook fase 1.

Stap 3. Kies dezelfde tijdeenheid van het leven uit de vervolgkeuzelijst Leven die u invoerde voor de configuratie van de tunnel en fase 1.

Stap 4. Kies dezelfde DH-groep uit de vervolgkeuzelijst Perfect Forwarding Secrecy (PFS) Group die u hebt ingevoerd voor de configuratie van de tunnel.

Stap 5. Schakel alle methoden voor ongebruikte versleuteling en verificatie uit. Controleer alleen de waarden die onder het tabblad Fase 1 zijn gedefinieerd.

identiteitsbewijs



Stap 1. Klik op het tabblad **ID**.

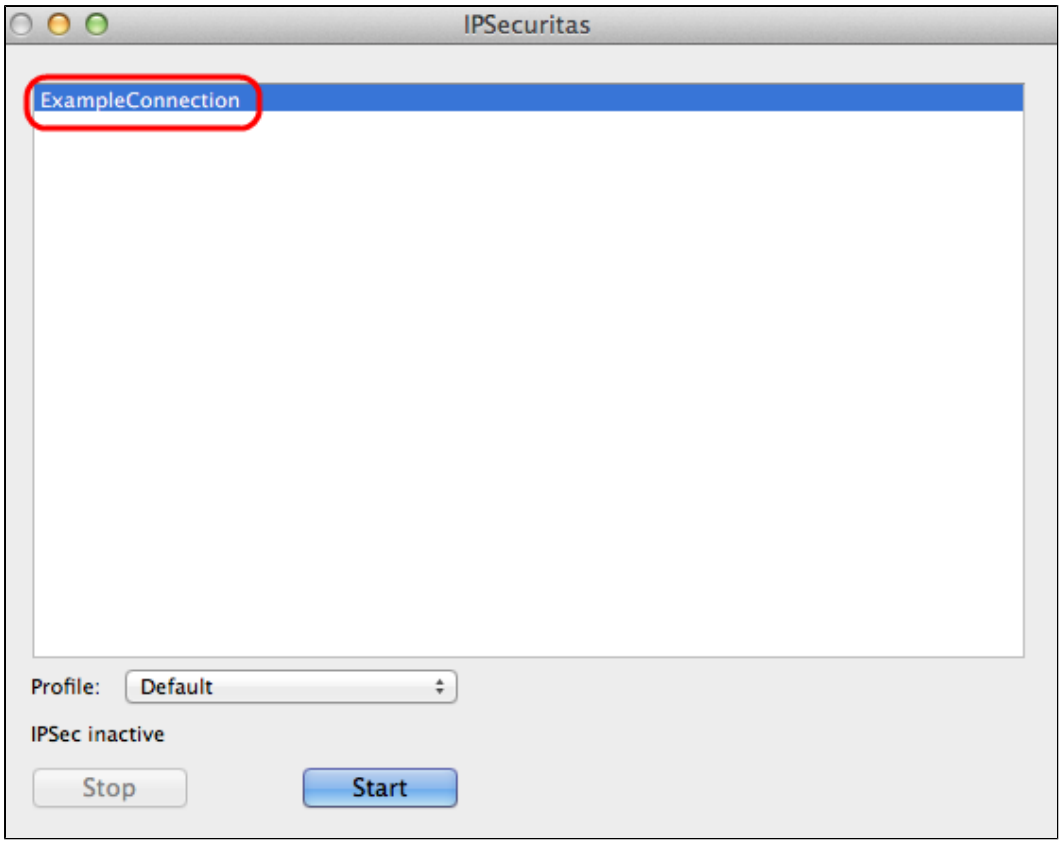
Stap 2. Kies dezelfde methode voor lokale identificatie als de tunnel in de vervolgkeuzelijst Local Identifier. Voer indien nodig de juiste waarde in volgens het type lokale identificatiecode.

Stap 3. Kies dezelfde methode van externe identificatie als de tunnel uit de vervolgkeuzelijst Remote Identifier. Voer indien nodig de juiste waarde in volgens het type identificatiecode op afstand.

Stap 4. Kies dezelfde verificatiemethode als de tunnel in de vervolgkeuzelijst Verificatiemethode. Voer indien nodig de juiste verificatiewaarde in volgens het type verificatiemethode.

Stap 5. Klik op het **x**-pictogram (rode cirkel) om het verbindingsvenster te sluiten. De instellingen worden automatisch opgeslagen. Het venster *IPSecuritas* verschijnt.

Connection



Stap 1. Klik in het venster *IPSecuritas* op **Start**. De gebruiker wordt vervolgens verbonden met toegang tot VPN.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.