Bereitstellung einer schnellen VPN-Alternative für Mac OS auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Es gibt keine Quick VPN-Version, die für Mac OS geeignet ist. Es gibt jedoch eine wachsende Anzahl von Benutzern, die eine Quick VPN-Alternative für Mac OS bereitstellen möchten. In diesem Artikel wird IP Securitas als Alternative für ein Quick VPN verwendet.

Hinweis: Sie müssen die IP Securitas herunterladen und auf Ihrem MAC-Betriebssystem installieren, bevor Sie mit der Konfiguration beginnen. Sie können es über den folgenden Link herunterladen:

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

In diesem Artikel wird erläutert, wie Sie eine QuickVPN-Alternative für Mac OS auf RV016-, RV042-, RV042G- und RV082-VPN-Routern bereitstellen.

Unterstützte Geräte

RV016
â€¢RV042
ãƒ» RV042G
RV082

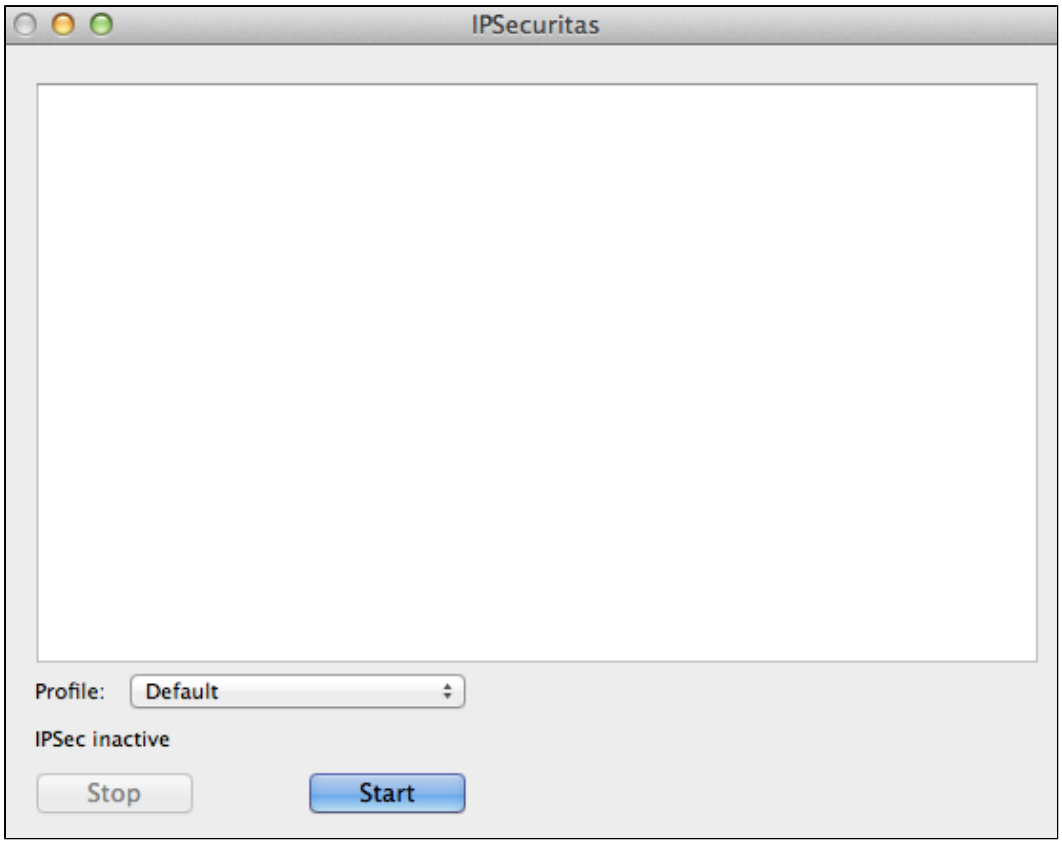
Software-Version

ãƒ» v4.2.2.08

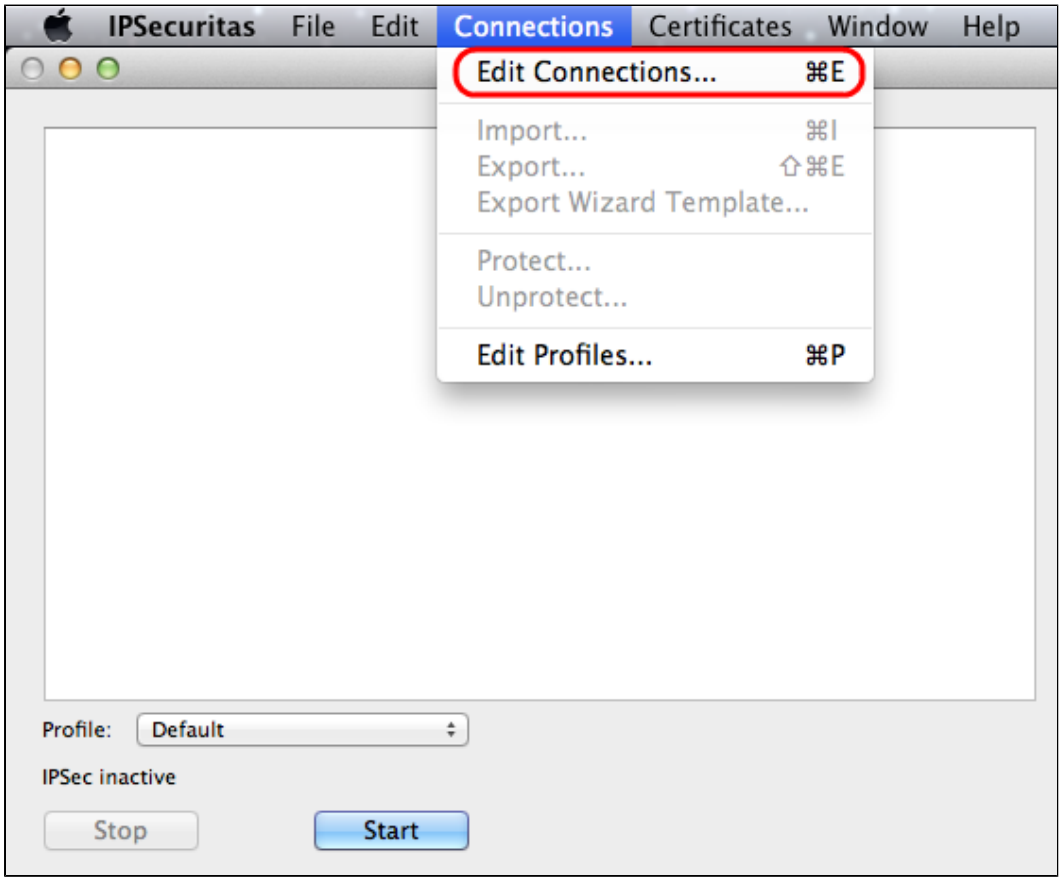
Bereitstellung einer schnellen VPN-Alternative für Mac OS

Hinweis: Die Konfiguration des Geräts zwischen VPN-Client und Gateway muss zuerst durchgeführt werden. Weitere Informationen zum Konfigurieren des VPN-Clients für das Gateway finden Sie unter *Richten Sie einen Remote-Zugriffstunnel (Client to Gateway) für VPN-Clients auf RV016-, RV042-, RV042G- und RV082-VPN-Routern ein.*

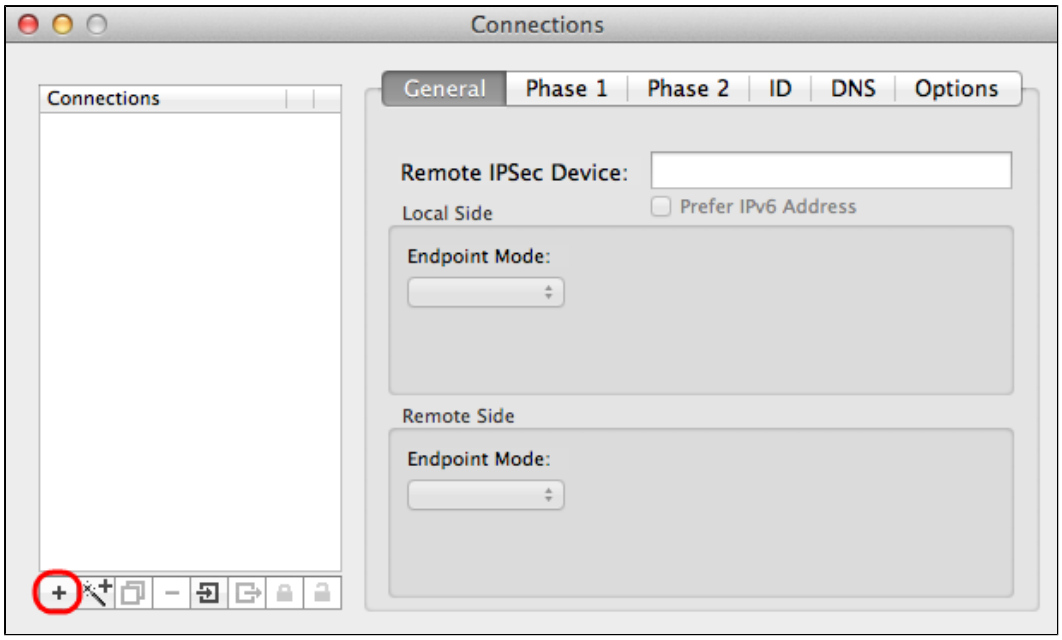
Schritt 1: Führen Sie die IP Securitas unter Mac OS aus. Das Fenster *IPSecuritas* wird angezeigt:



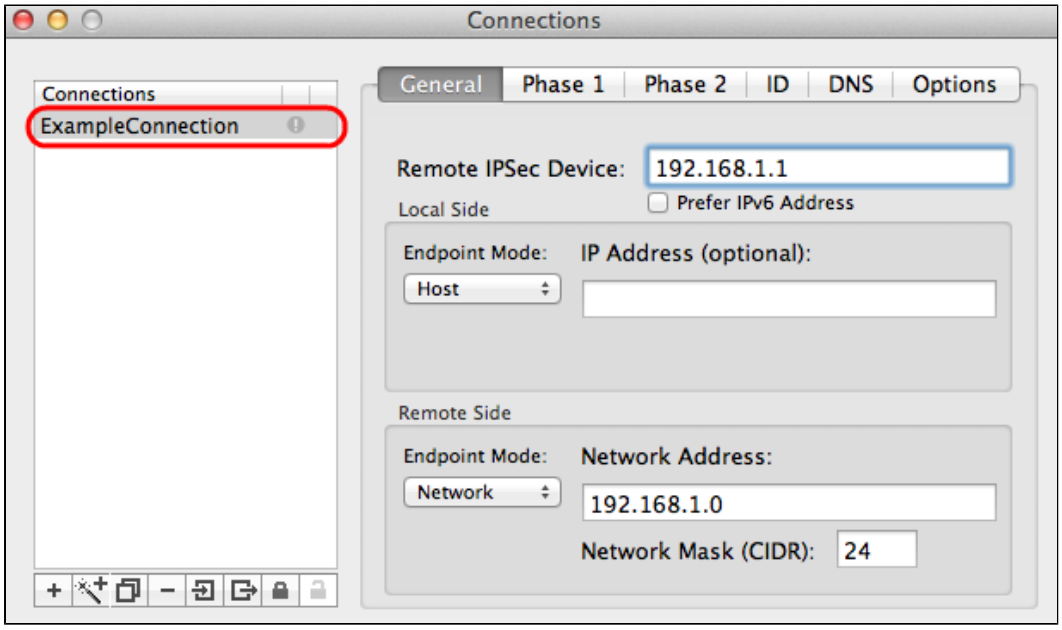
Schritt 2: Klicken Sie auf **Start**.



Schritt 3: Wählen Sie in der Menüleiste **Verbindungen > Verbindungen bearbeiten**. Das Fenster *Verbindungen* wird angezeigt.

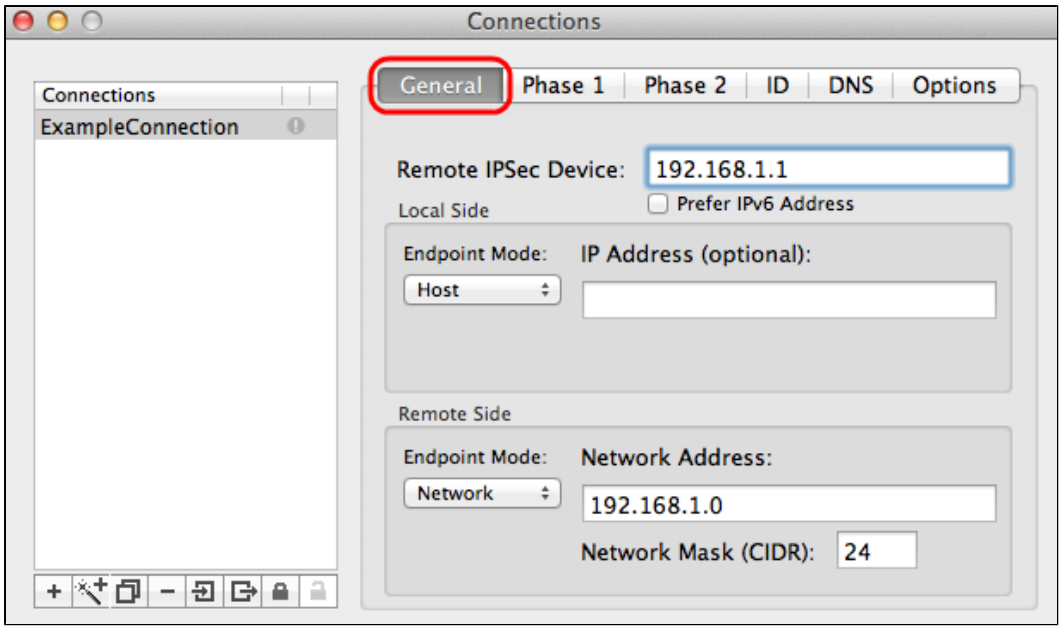


Schritt 4: Klicken Sie auf das Symbol +, um eine neue Verbindung hinzuzufügen.



Schritt 5: Geben Sie unter "Verbindungen" einen Namen für die neue Verbindung ein.

Allgemein



Schritt 1: Klicken Sie auf die Registerkarte **Allgemein**.

Schritt 2: Geben Sie die IP-Adresse des Remote-Routers in das Feld Remote IPSec-Gerät ein.

Hinweis: Sie müssen die lokale Seite nicht konfigurieren, da diese Konfiguration für den Remote-Client vorgesehen ist. Sie müssen nur den Remote-Modus konfigurieren.

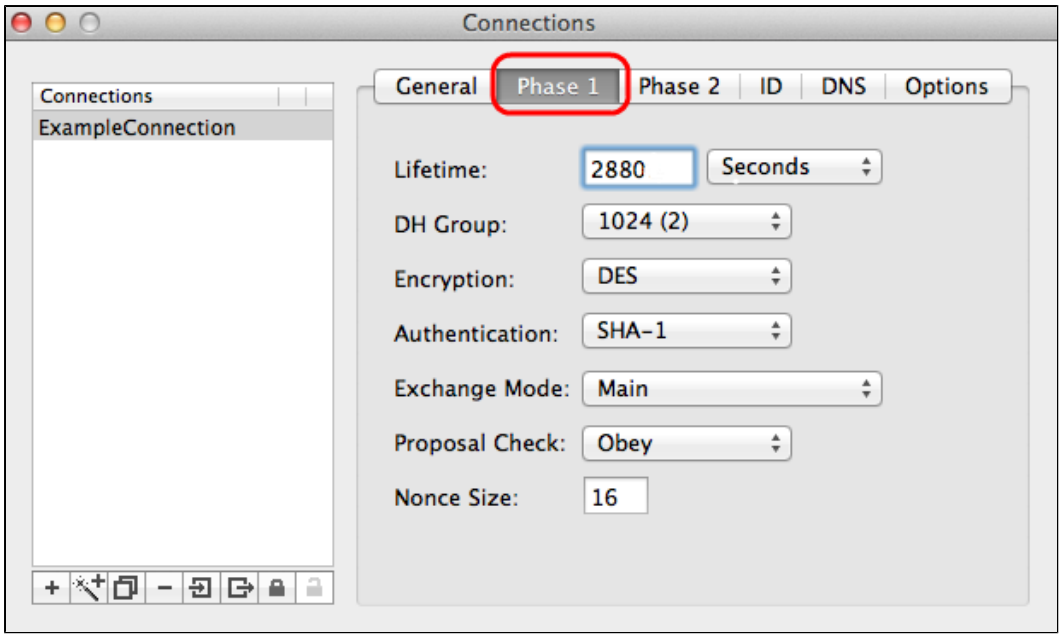
Schritt 3: Wählen Sie im Bereich Remote Side (Remote-Seite) **Network (Netzwerk)** aus der Dropdown-Liste Endpoint Mode (Endpunktmodus) aus.

Schritt 4: Geben Sie die Subnetzmaske in das Feld Network Mask (CIDR) (Netzwerkmaske (CIDR)) ein.

Schritt 5: Geben Sie die Remote-Netzwerkadresse in das Feld Netzwerkadresse ein.

Phase 1

Phase 1 ist die Simplex-SA (Logical Security Association) zwischen den beiden Tunnelenden, die eine sichere authentifizierte Kommunikation unterstützt.



Schritt 1: Klicken Sie auf die Registerkarte **Phase 1**.

Schritt 2: Geben Sie die Lebensdauer, die Sie während der Konfiguration des Tunnels eingegeben haben, in das Feld Lebensdauer ein. Wenn die Zeit abläuft, wird automatisch ein neuer Schlüssel ausgehandelt. Die Schlüsselverwendungsdauer kann zwischen 1081 und 86400 Sekunden liegen. Der Standardwert für Phase 1 beträgt 28800 Sekunden.

Schritt 3: Wählen Sie in der Dropdown-Liste "Lifetime" (Lebensdauer) die entsprechende Zeiteinheit aus. Der Standardwert ist Sekunden.

Schritt 4: Wählen Sie die gleiche DH-Gruppe aus der Dropdown-Liste aus, die Sie für die Konfiguration des Tunnels eingegeben haben. Die Diffie-Hellman-Gruppe (DH) wird für den Schlüsselaustausch verwendet.

Schritt 5: Wählen Sie aus der Dropdown-Liste Verschlüsselung den Verschlüsselungstyp aus, den Sie für die Konfiguration des Tunnels eingegeben haben. Die Verschlüsselungsmethode legt die Länge des Schlüssels fest, der zum Verschlüsseln/Entschlüsseln von ESP-Paketen (Encapsulating Security Payload) verwendet wird.

Schritt 6: Wählen Sie aus der Dropdown-Liste "Authentifizierung" die Authentifizierungsmethode aus, die Sie für die Konfiguration des Tunnels eingegeben haben. Der Authentifizierungstyp bestimmt die Methode zur Authentifizierung von ESP-Paketen.

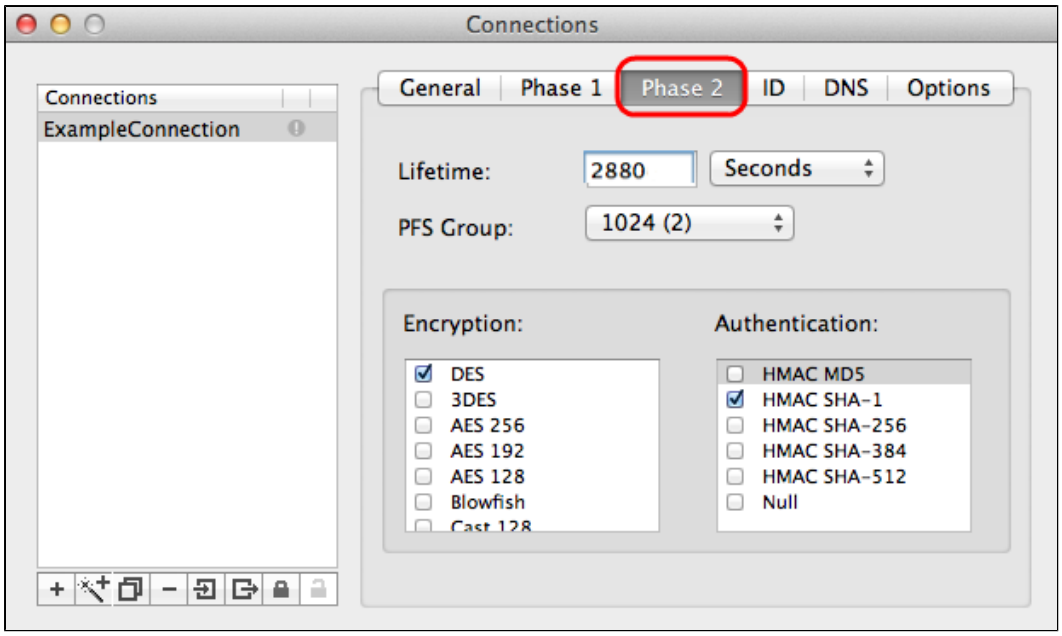
Schritt 7. Wählen Sie in der Dropdown-Liste "Exchange Mode" (Austauschmodus) den entsprechenden Austauschmodus aus.

ãƒ» Main (Hauptmodus): Stellt den Austauschmodus für alle Gateway-Typen außer FQDN (Full Qualified Domain Name) dar.

ãƒ» Aggressive (Aggressiv): Stellt den Austauschmodus für ein FQDN-Gateway (Full Qualified Domain Name) dar.

Phase 2

Phase 2 ist die Sicherheitszuordnung zur Bestimmung der Sicherheit des Datenpakets während des Durchlaufs der Datenpakete durch die beiden Endpunkte.



Schritt 1: Klicken Sie auf die Registerkarte **Phase 2**.

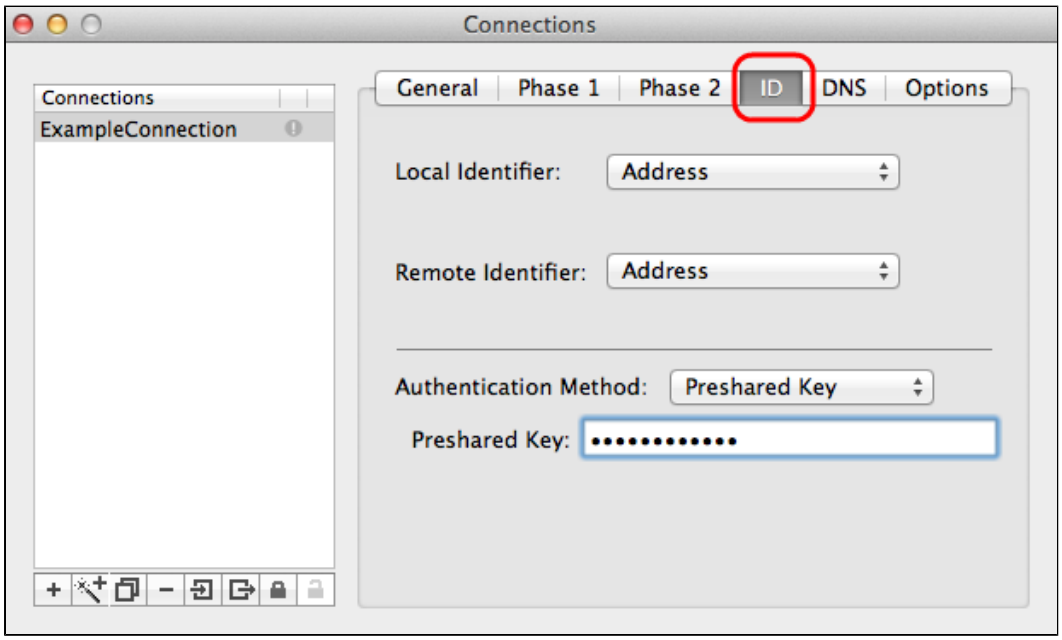
Schritt 2: Geben Sie die gleiche Lebensdauer in das Feld "Lifetime" (Lebensdauer) ein, die Sie für die Konfiguration des Tunnels eingegeben haben, sowie Phase 1.

Schritt 3: Wählen Sie in der Dropdown-Liste "Lifetime" (Lebensdauer) dieselbe Zeiteinheit aus, die Sie für die Konfiguration des Tunnels und für Phase 1 eingegeben haben.

Schritt 4: Wählen Sie dieselbe DH-Gruppe aus der Dropdown-Liste Perfect Forwarding Secrecy (PFS) Group (Perfektes Weiterleitungsgeheimnis) aus, die Sie für die Konfiguration des Tunnels eingegeben haben.

Schritt 5: Deaktivieren Sie alle nicht verwendeten Verschlüsselungs- und Authentifizierungsmethoden. Überprüfen Sie nur die auf der Registerkarte für Phase 1 definierten Optionen.

ID



Schritt 1: Klicken Sie auf die Registerkarte **ID**.

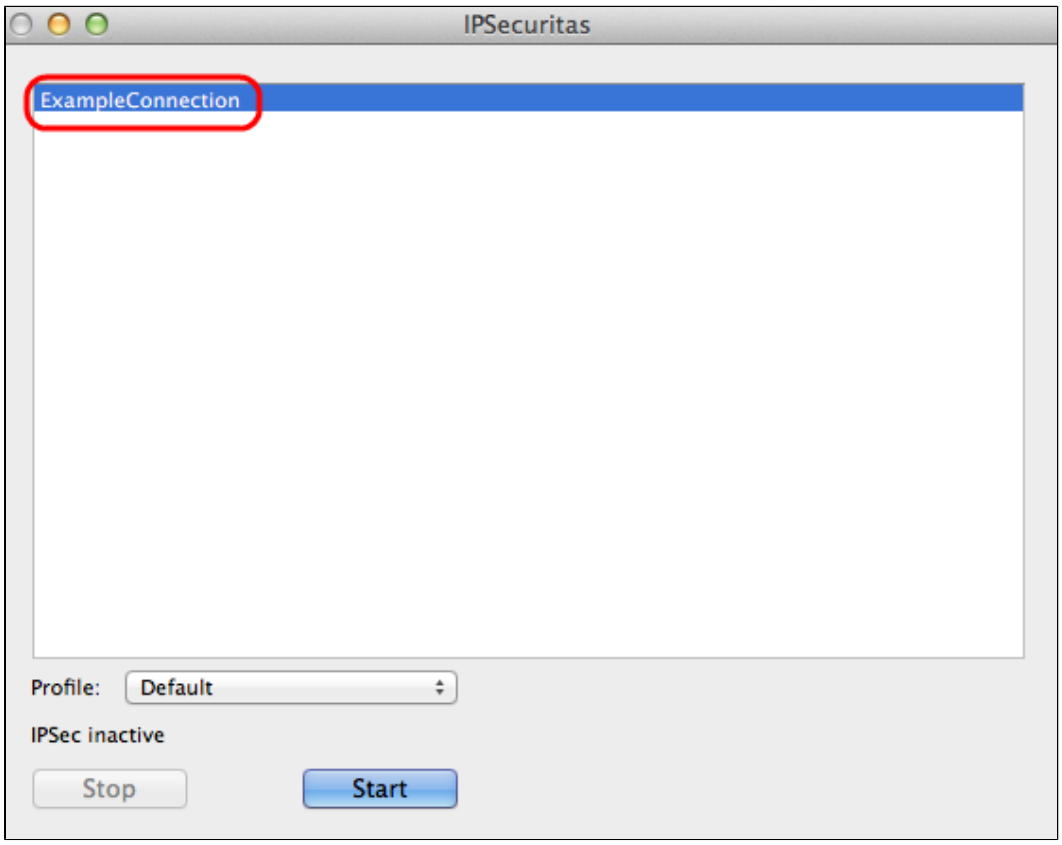
Schritt 2: Wählen Sie in der Dropdown-Liste Local Identifier (Lokale Kennung) die gleiche Methode für die lokale Kennung wie der Tunnel aus. Geben Sie ggf. den entsprechenden Wert entsprechend dem Typ der lokalen ID ein.

Schritt 3: Wählen Sie in der Dropdown-Liste Remote Identifier (Remote-Kennung) die gleiche Methode zur Remote-Kennung wie der Tunnel aus. Geben Sie ggf. den entsprechenden Wert für den Remote-Identifizierungstyp ein.

Schritt 4: Wählen Sie in der Dropdown-Liste "Authentifizierungsmethode" die gleiche Authentifizierungsmethode wie der Tunnel aus. Geben Sie ggf. den entsprechenden Authentifizierungswert entsprechend dem Authentifizierungstyp ein.

Schritt 5: Klicken Sie auf das Symbol **x** (roter Kreis), um das Verbindungsfenster zu schließen. Dadurch werden die Einstellungen automatisch gespeichert. Das Fenster *IPSecuritas* wird angezeigt.

Verbindung



Schritt 1: Klicken Sie im Fenster *IPSecuritas* auf **Start**. Der Benutzer wird dann mit dem VPN verbunden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.