Configuratie van RV042, RV042G en RV082 VPN-routers voor Windows

Doel

Een Virtual Private Network (VPN) is een methode voor externe gebruikers om virtueel verbinding met een privaat netwerk via het internet te maken. Een client-naar-gateway VPN verbindt de desktop of laptop van een gebruiker met een externe netwerk met behulp van VPN-clientsoftware. De verbinding van client tot Gateway VPN is nuttig voor externe werknemers die zich veilig aan het kantoornetwerk willen verbinden. De client van VPN tonen is software die op een ver host-apparaat is geconfigureerd dat eenvoudige en beveiligde VPN-connectiviteit biedt.

Het doel van dit document is om u te tonen hoe u de globale VPN-client voor een computer kunt configureren die verbonden is met een RV042, RV042G of RV082 VPN-router.

N.B.: Dit document gaat ervan uit dat u al de Windows VPN-client op de Windows-computer hebt gedownload. Anders moet u een client-naar-gateway VPN-verbinding configureren voordat u het VPN-venster kunt configureren. Om meer te weten te komen over het configureren van client naar gateway VPN, raadpleegt u *Een afstandsbediening van toegangstunnelheid (client naar gateway) voor VPN-clients op RV042-, RV042G- en RV082 VPN-routers*.

Toepasselijke apparaten

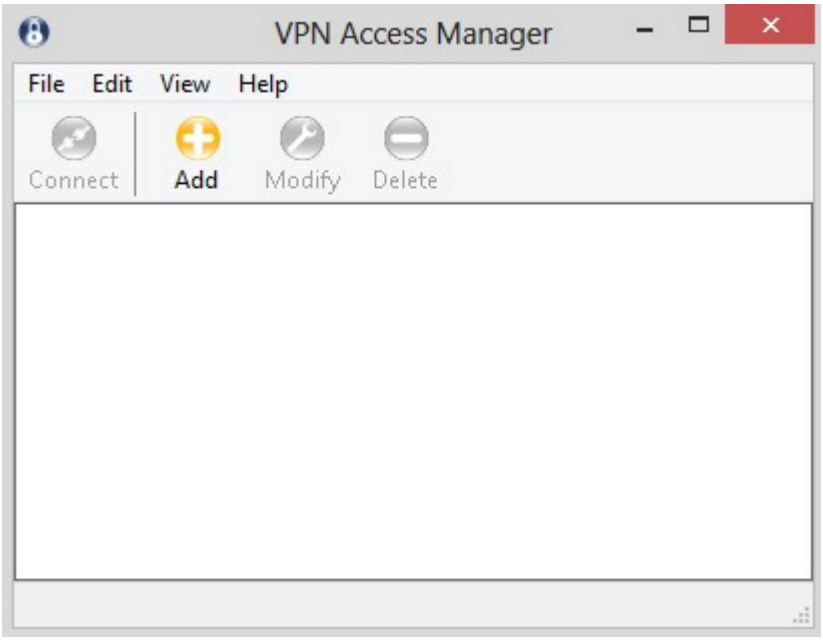
- RV042
- RV042G
- RV082

Softwareversie

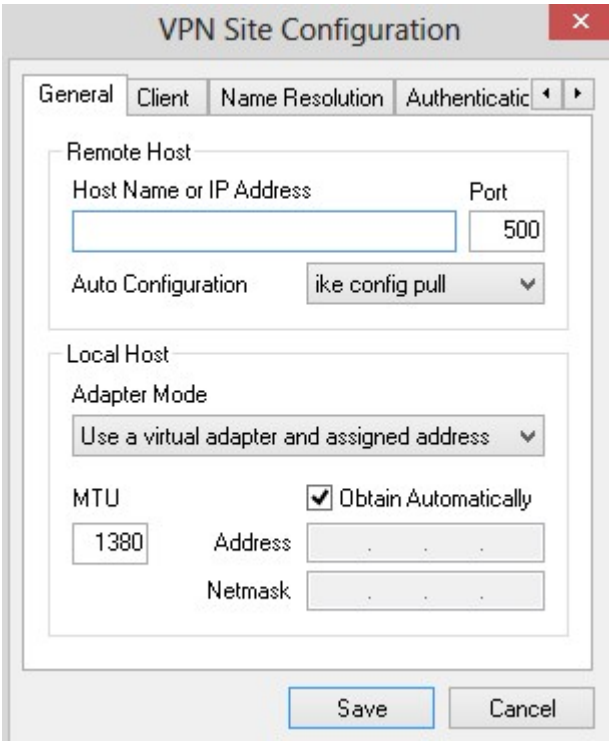
- v4.2.2.08

Configuratie van VPN-clientverbinding tonen op Windows

Stap 1. Klik op het **VPN-clientprogramma** tonen op de computer en open het. Het venster *Shrew Soft VPN Access Manager* wordt geopend:

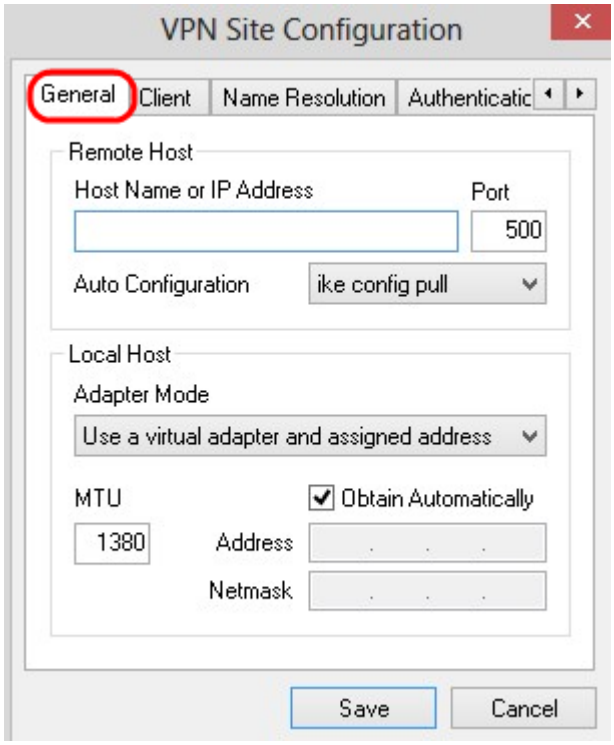


Stap 2. Klik op **Add**. Het venster *VPN Site Configuration* verschijnt:



Algemene configuratie

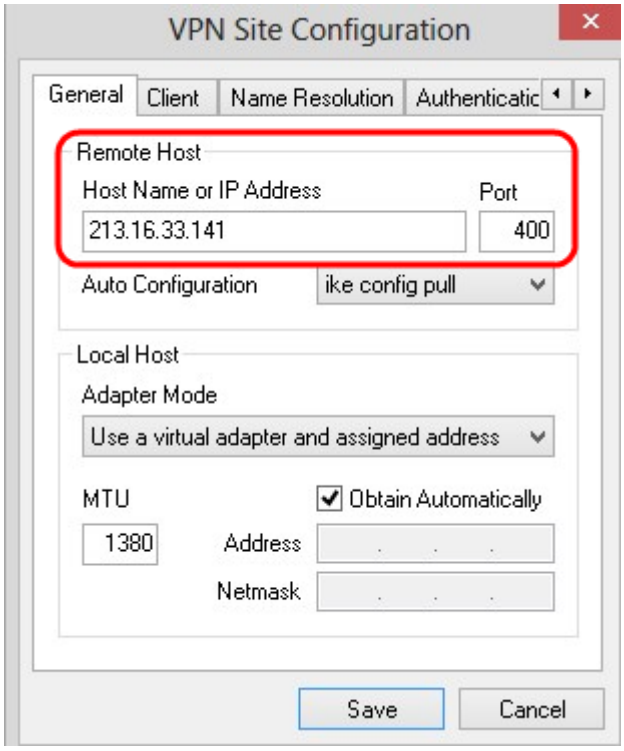
Stap 1. Klik op het tabblad **Algemeen**.



Opmerking: Het *algemene* gedeelte wordt gebruikt om de Remote en Local Host IP-adressen te configureren. Deze worden gebruikt om de netwerkparameters te definiëren voor de client-naar-gateway-verbinding.

Stap 2. In het veld *Host Name of IP Address*, specificeert u het externe IP-adres van de host, dat het IP-adres van het geconfigureerde WAN is.

Stap 3. Voer in het veld *Port* het nummer in van de poort die voor de verbinding moet worden gebruikt. Het poortnummer dat in het voorbeeld wordt gebruikt, is 400.



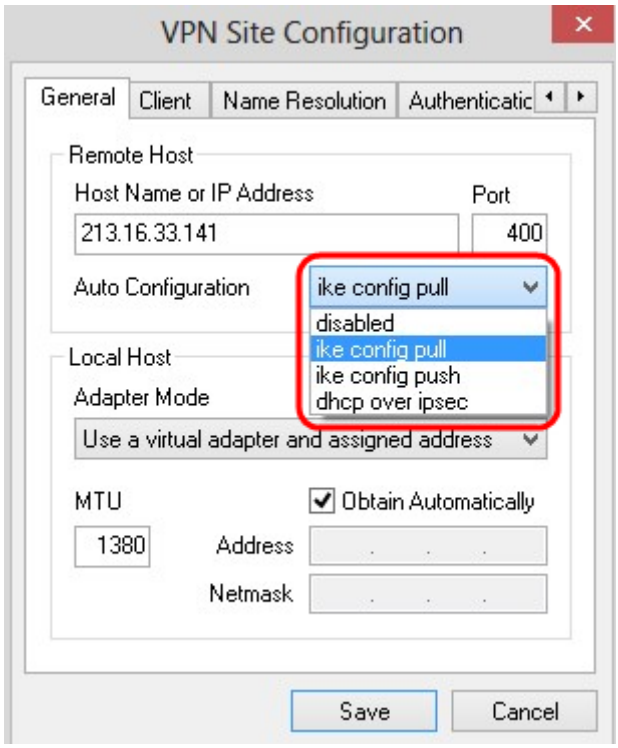
Stap 4. Kies in de vervolgkeuzelijst *Auto Configuration* de gewenste configuratie.

- Uitgeschakeld — Met de optie uitgeschakeld worden alle automatische clientconfiguraties uitgeschakeld.

- IKE Config - Hiermee kunt u verzoeken van een computer door de client instellen. Met ondersteuning van de meerdere methode van de computer, retourneert het verzoek een lijst met instellingen die worden ondersteund door de client.

- IKE Config Push - biedt een computer de mogelijkheid om instellingen aan de client aan te bieden tijdens het configuratie. Met ondersteuning van de drukmethode door de computer, retourneert het verzoek een lijst met instellingen die worden ondersteund door de client.

- DHCP over IPSec — geeft de client de mogelijkheid om instellingen van de computer via DHCP via IPSec aan te vragen.

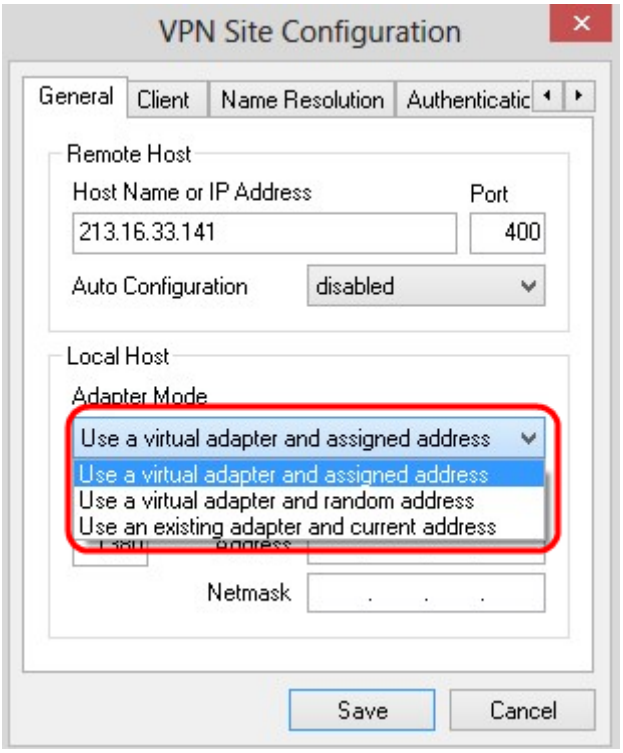


Stap 5. Kies in de vervolgkeuzelijst Adapter-*modus* de gewenste adaptermodus voor lokale host op basis van de automatische configuratie.

- Gebruik een virtuele adapter en toegewezen adres — Hiermee kunt u een virtuele adapter met een bepaald adres gebruiken.

- Gebruik een virtuele adapter en een willekeurig adres: hiermee kan de client een virtuele adapter gebruiken met willekeurig adres.

- Gebruik een bestaande adapter en huidig adres — Gebruik een bestaande adapter en het bijbehorende adres. Er hoeft geen aanvullende informatie te worden ingevoerd.

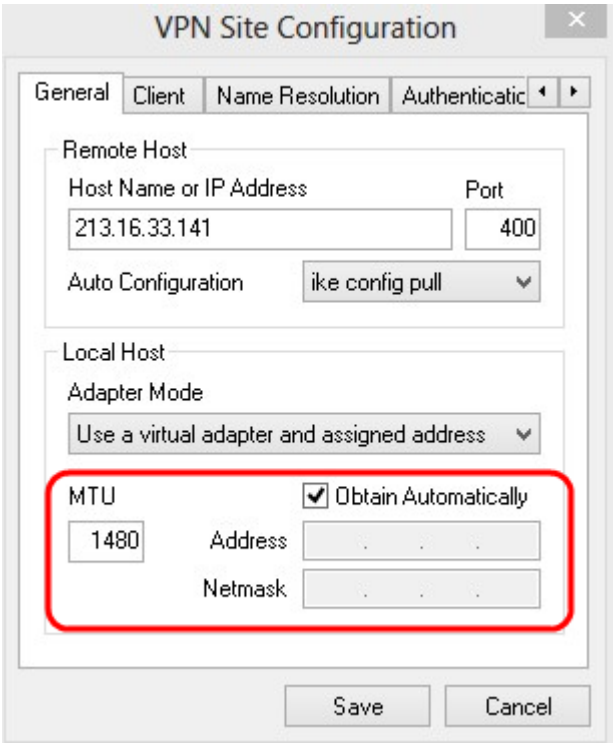


Stap 6. Voer de maximale transmissie-eenheid (MTU) in het veld *MTU in* als u **een virtuele adapter gebruikt en** het **toegewezen adres in de** vervolgkeuzelijst Adapter-modus in Stap 5 **hebt** toegewezen. De maximale transmissie-eenheid helpt IP-fragmentatieproblemen op te lossen. De standaardwaarde is 1380.

Stap 7. (Optioneel) Om het adres en het subnetmasker automatisch via DHCP-server te ontvangen, schakelt u het vakje **Automatisch** verkrijgen in. Deze optie is niet voor alle configuraties beschikbaar.

Stap 8. Voer het IP-adres van de externe client in het *veld Adres in* als u **in Stap 5** hebt gekozen voor **Gebruik een virtuele adapter en toegewezen adres** in de vervolgkeuzelijst Adapter-modus.

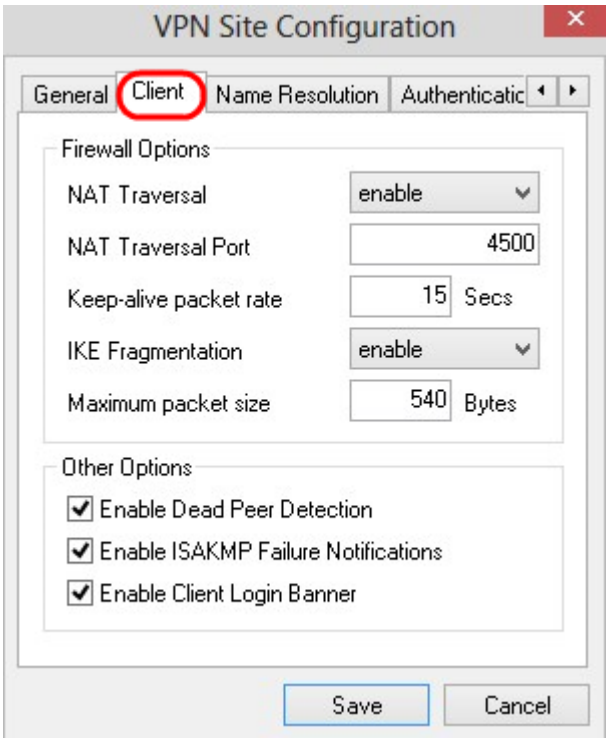
Stap 9. Voer Subnetmasker van het IP-adres van de externe client in het veld *Netmasker* in als u **FineReader-adapter** hebt **gebruikt en** het **toegewezen adres in de** vervolgkeuzelijst Adapter-modus in Stap 5 hebt **gekozen**.



Stap 10. Klik op **Opslaan** om de instellingen op te slaan.

Clientconfiguratie

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



N.B.: In het gedeelte *Client* kunt u de firewallopties configureren, detectie van dodelijke peers en foutmeldingen in ISAKMP (Internet Security Association en Key Management Protocol). De instellingen definiëren welke configuratieopties handmatig zijn ingesteld en die automatisch worden verkregen.

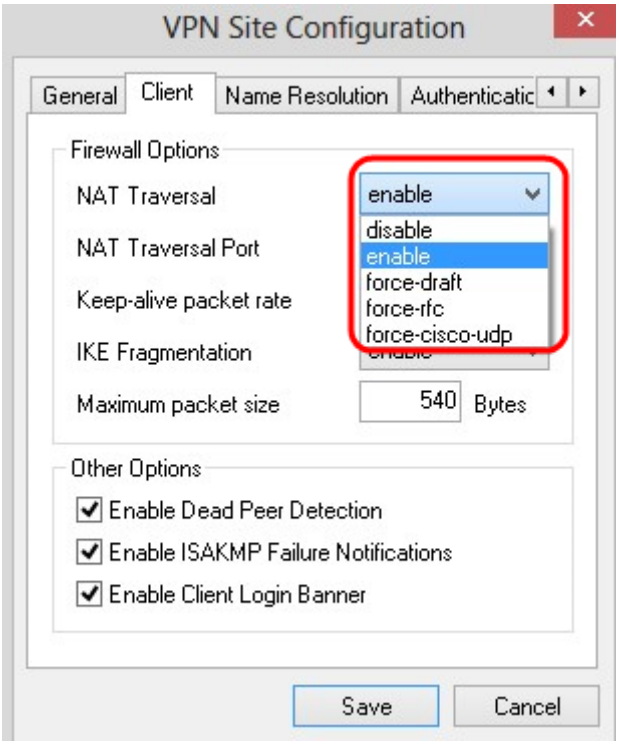
Stap 2. Kies de juiste NAT-optie (Netwerkadresomzetting) in de vervolgkeuzelijst *NAT-traject*.

- Uitschakelen — NAT-protocol is uitgeschakeld.

- Schakel — IKE-fragmentatie wordt alleen gebruikt als de gateway ondersteuning door onderhandelingen aangeeft.

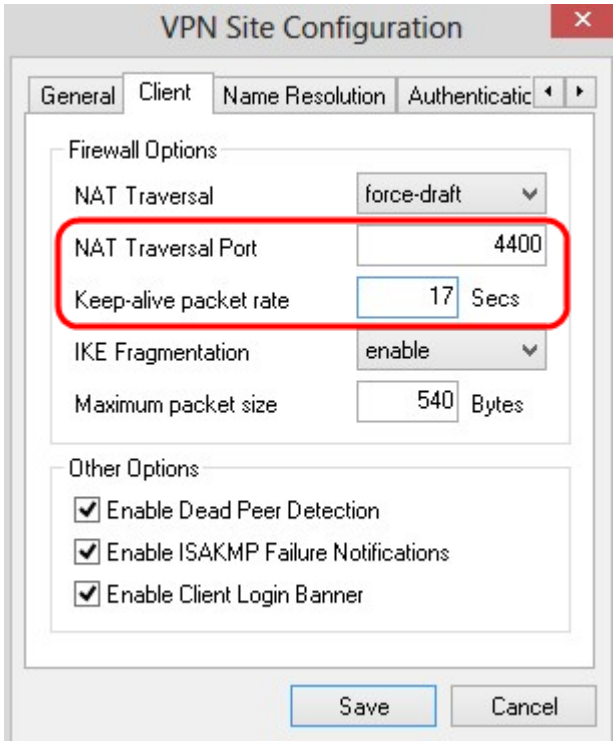
- Ontwerp forceren — De ontwerpversie van het NAT-protocol. Het wordt gebruikt als de gateway ondersteuning aangeeft door onderhandelingen of de detectie van de NAT.

- Forceer RFC — De RFC-versie van het NAT-protocol. Het wordt gebruikt als de gateway ondersteuning aangeeft door onderhandelingen of de detectie van de NAT.



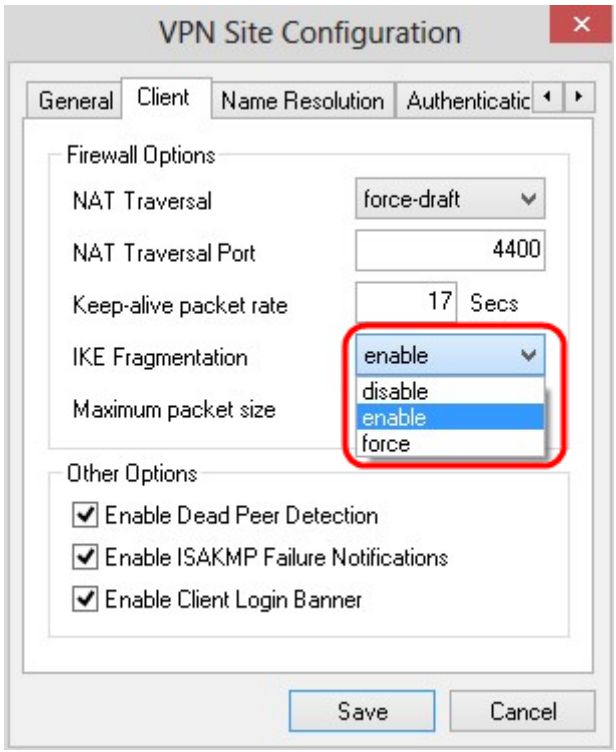
Stap 3. Voer de UDP-poort voor de NAT in het veld *NAT*-transversale poort in. De standaardwaarde is 4500.

Stap 4. In het veld *Levend pakkettarief* houdt u een waarde in voor de pakketpakketten die u wilt behouden. De waarde wordt in seconden gemeten. De standaardwaarde is 30 seconden.



Stap 5. Kies in de vervolgkeuzelijst *IKE Fragmentation* de juiste optie.

- Uitschakelen — IKE-fragmentatie wordt niet gebruikt.
- Schakel — IKE-fragmentatie wordt alleen gebruikt als de gateway ondersteuning door onderhandelingen aangeeft.
- Macht — IKE-fragmentatie wordt gebruikt ongeacht aanwijzingen of detectie.



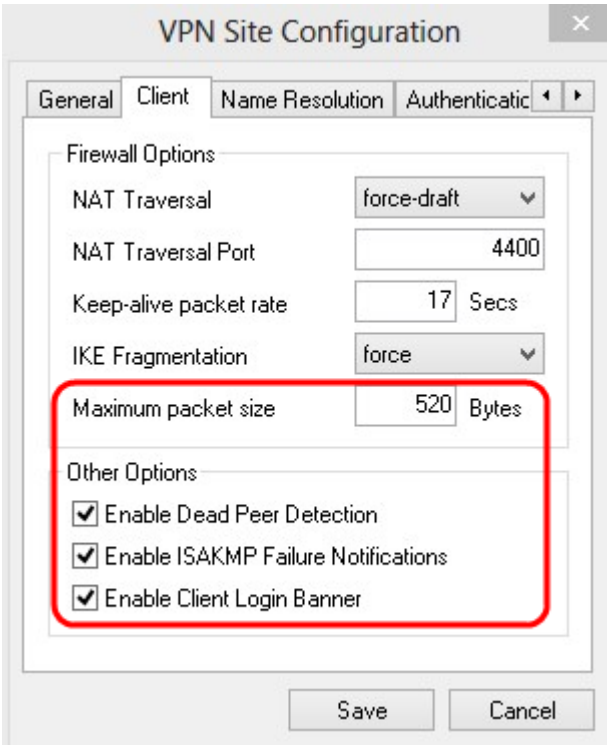
Stap 6. Voer de maximale pakketgrootte in het veld *maximale pakketgrootte* in bytes. Als de pakketgrootte groter is dan de maximale pakketgrootte, wordt de IKE fragmentatie uitgevoerd. De standaardwaarde is 540 bytes.

Stap 7. (Optioneel) Om de computer en de client in staat te stellen te detecteren wanneer de

andere niet langer kan reageren, schakelt u het vakje **Dead Peer Detectie inschakelen in**.

Stap 8. (Optioneel) Als u meldingen van fouten door de VPN-client wilt verzenden, controleert u het vakje **Automation-Meldingen voor ISAKMP-fouten inschakelen**.

Stap 9. (optioneel) Om een logbanner van de client te tonen wanneer de verbinding met de poort is aangegaan, schakelt u het aanvinkvakje **client inschakelen in**.



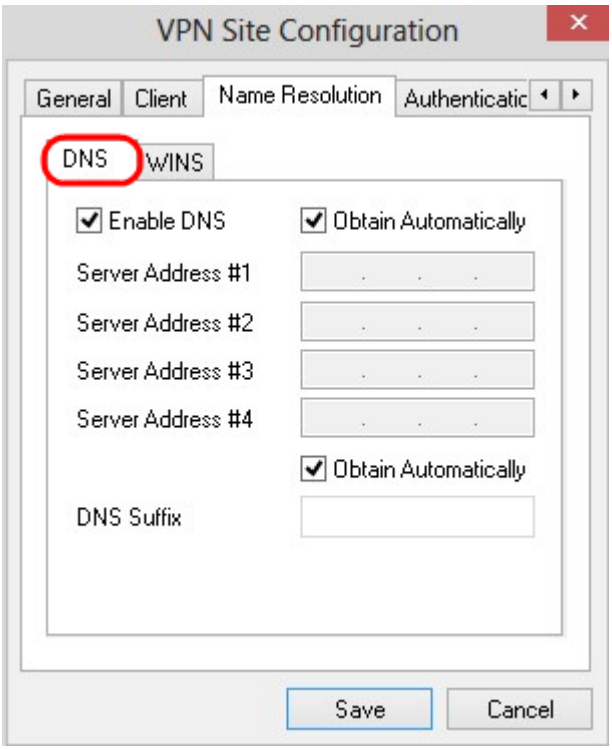
Stap 10. Klik op **Opslaan** om de instellingen op te slaan.

Configuratie van naamresolutie

Stap 1. Klik op het tabblad **Naam resolutie**.

Opmerking: Het gedeelte *Name Solutions* wordt gebruikt om de instellingen DNS (Domain Name System) en WIN (Windows Internet Name Service) te configureren.

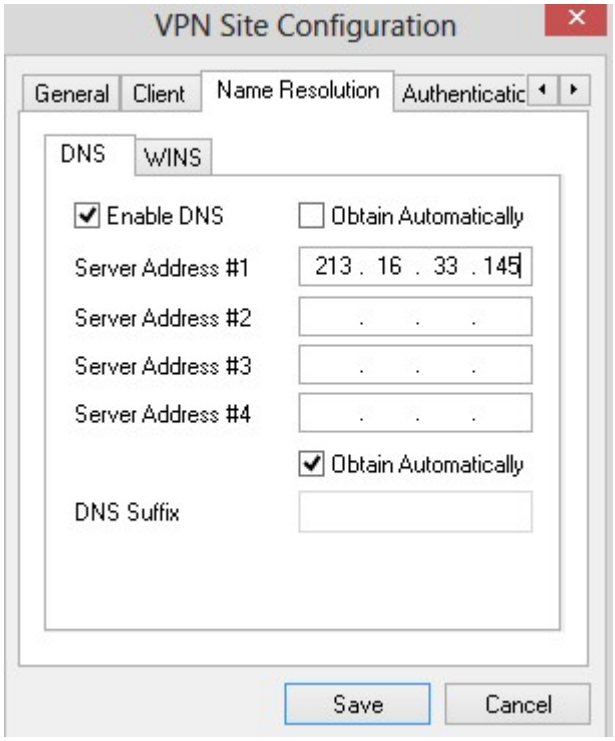
Stap 2. Klik op het tabblad **DNS**.



Stap 3. Controleer **DNS**-systeem **inschakelen** om het Domain Name System (DNS)-systeem in te schakelen.

Stap 4. (Optioneel) Controleer het vakje **Automatisch** aanvinken om het DNS-serveradres automatisch te verkrijgen. Als u deze optie kiest, slaat u over naar Stap 6.

Stap 5. Voer het DNS-serveradres in het veld *Server Address #1 in*. Als er een andere DNS-server is, voert u het adres van deze servers in de resterende velden *voor serveradres in*.



Stap 6. (Optioneel) Controleer het vakje **Automatisch** aanvinken om het achtervoegsel van de DNS-server automatisch te verkrijgen. Als u deze optie kiest, slaat u over naar Stap 8.

Stap 7. Voer het achtervoegsel van de DNS-server in het veld *DNS*-achtervoegsel in.

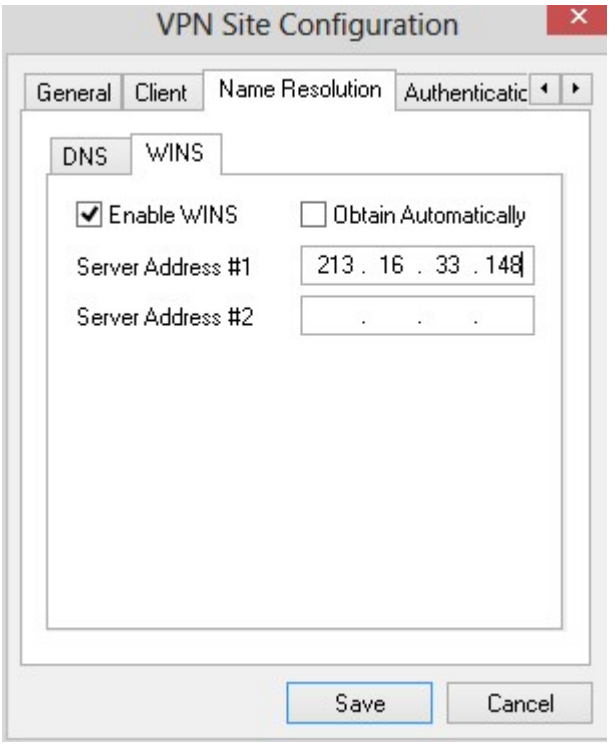
Stap 8. Klik op **Opslaan** om de instellingen op te slaan.

Stap 9. Klik op het tabblad **WINS**.

Stap 10. Controleer **WINS in** om Windows Internet Name Server (WINS) in te schakelen.

Stap 1. (Optioneel) Controleer het vakje **Automatisch** aanschaffen om het DNS-serveradres automatisch te verkrijgen. Als u deze optie kiest, slaat u over naar Stap 13.

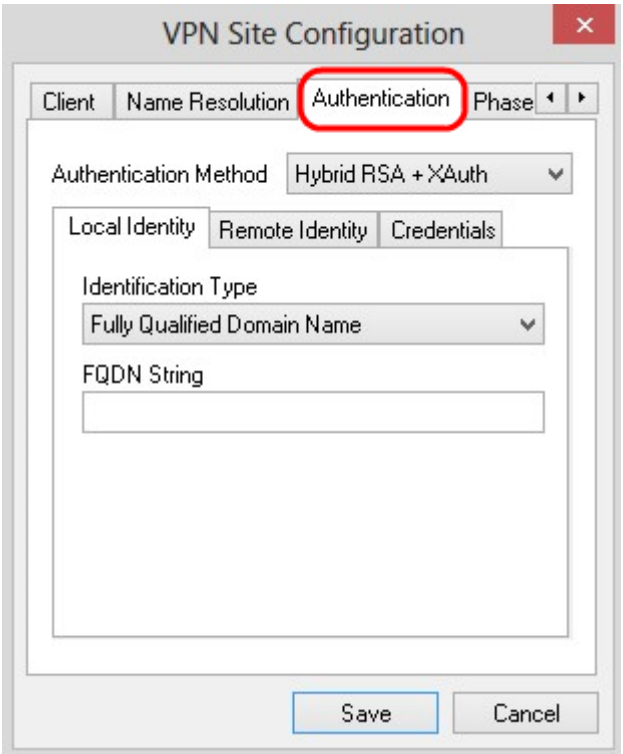
Stap 12. Voer het adres van de WINS-server in het veld *Server Address #1* in. Als er andere DNS-servers zijn, voert u het adres van deze servers in de resterende velden *voor serveradres in*.



Stap 13. Klik op **Opslaan** om de instellingen op te slaan.

Verificatie

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



Opmerking: In het gedeelte *Verificatie* kunt u de parameters voor de client configureren om de verificatie aan te pakken wanneer er een ISAKMP SA wordt gestart.

Stap 2. Kies de juiste methode voor de verificatie in de vervolgkeuzelijst *Verificatiemethode*.

- Hybride RSA + XAuth — De klantenkrediet is niet nodig. De client zal de gateway echt maken. De aanmeldingsgegevens worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of van een sleutelbestandstype.

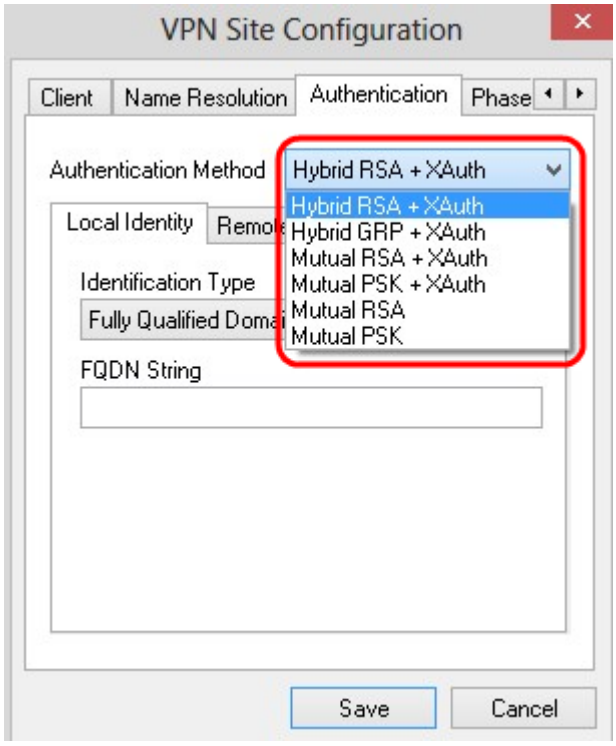
- Hybride GRP + XAuth — De clientcreditering is niet nodig. De client zal de gateway echt maken. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificatenbestand en een gedeeld geheime string zijn.

- Wederzijdse RSA + XAuth — Cliënt en gateway hebben beide nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificaatbestanden of het sleuteltype zijn.

- Wederom PSK + XAuth — Clientgegevens en toegangspoort zijn beide nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van een gedeeld geheim strijkje zijn.

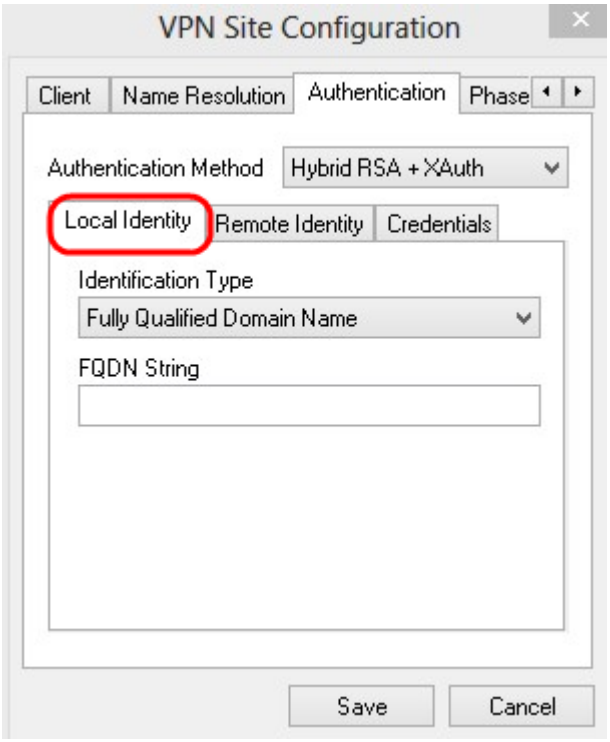
- Wederom RSA — Cliënt en gateway hebben beide geloofsbrieven nodig om te authentiseren. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificaatbestanden of het sleuteltype zijn.

- Wederom PSK — Cliënt en poort hebben beide geloofsbrieven nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van een gedeeld geheim strijkje zijn.



Configuratie lokale identiteit

Stap 1. Klik op het tabblad **Local Identity**.



Opmerking: Lokale identiteit stelt de ID in die naar de gateway wordt verzonden ter verificatie. In het gedeelte *Local Identity* wordt het Identificatietype en FQDN (Full Qualified Domain Name) String geconfigureerd om te bepalen hoe de ID wordt verzonden.

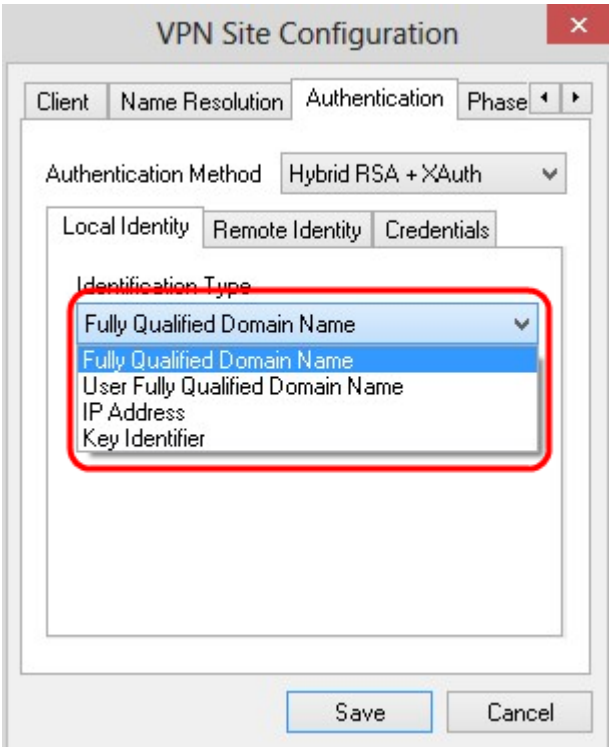
Stap 2. Kies de juiste identificatieoptie in de vervolgkeuzelijst *Identificatietype*. Niet alle opties zijn beschikbaar voor alle authenticatiemodi.

- Volledig gekwalificeerde Domeinnaam — De client-identificatie van de lokale identiteit is gebaseerd op een volledig gekwalificeerde Domeinnaam. Als u deze optie kiest, volgt u Stap 3 en slaat u vervolgens over naar Stap 7.

- Gebruiker Volledig gekwalificeerde Domeinnaam - De client-identificatie van de lokale identiteit is gebaseerd op de volledig gekwalificeerde Domeinnaam van de gebruiker. Als u deze optie kiest, volgt u Stap 4 en slaat u vervolgens over naar Stap 7.

- IP-adres — Clientidentificatie van de lokale identiteit is gebaseerd op IP-adres. Als u controleert **Gebruik een ontdekt lokaal host-adres**, wordt het IP-adres automatisch herkend. Als u deze optie kiest, volgt u Stap 5 en slaat u vervolgens over naar Stap 7.

- Identificatiecode van de cliënt — Identificatie van de lokale cliënt wordt bepaald op basis van een identificator. Als u deze optie kiest, volgt u Stap 6 en Stap 7.



Stap 3. Voer de volledig gekwalificeerde domeinnaam in als DNS-string in het veld *FQDN-string*.

Stap 4. Voer de volledig gekwalificeerde domeinnaam van de gebruiker in als DNS-string in het veld *UFQDN-string*.

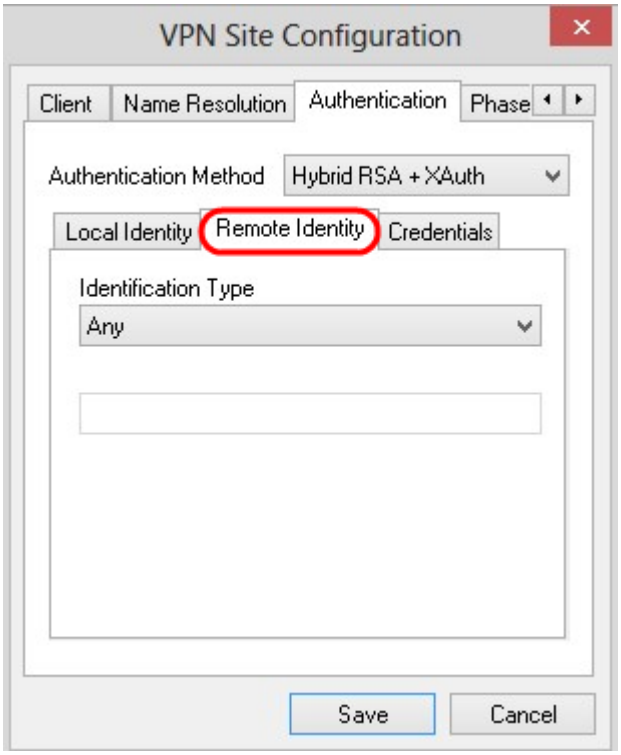
Stap 5. Voer het IP-adres in het veld *UFQD*-string in.

Stap 6. Voer de belangrijkste identificator in om de lokale client in de *Key ID String* te identificeren.

Stap 8. Klik op **Opslaan** om de instellingen op te slaan.

Configuratie van externe identiteit

Stap 1. Klik op het tabblad **Remote Identity**.



Opmerking: Remote Identity verifieert de ID vanuit de gateway. In het gedeelte *Externe Identiteit* wordt het Identificatietype ingesteld om te bepalen hoe de ID wordt geverifieerd.

Stap 2. Kies de juiste identificatieoptie in de vervolgkeuzelijst *Identificatietype*.

- Alle — De externe client kan alle waarde of ID accepteren om echt te maken.

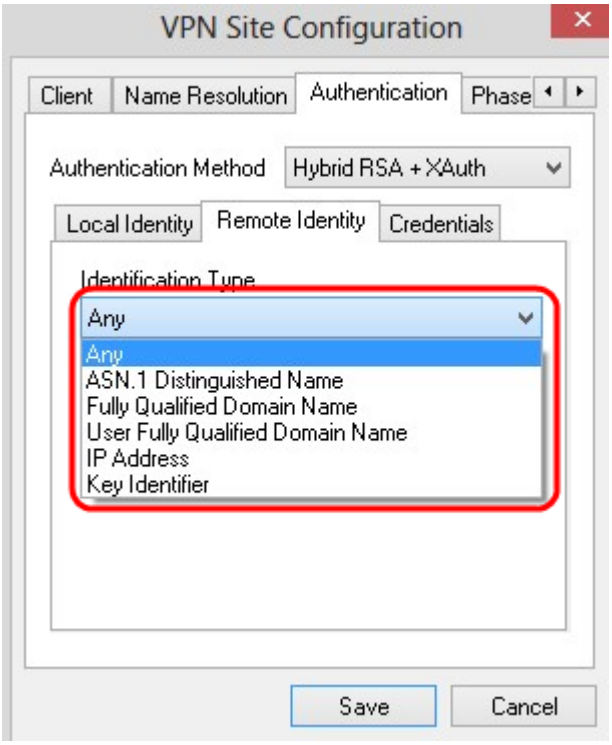
- ASN.1 Naam — De externe client wordt automatisch geïdentificeerd uit een PEM- of PKCS12-certificaatbestand. U kunt deze optie alleen kiezen als u in Stap 2 van de sectie *Verificatie* een RSA-authenticatiemethode kiest. Controleer de **onderwerping in het ontvangen certificaat maar vergelijk deze niet met een** vinkvakje **voor de specifieke waarde** om het certificaat automatisch te ontvangen. Als u deze optie kiest, volgt u Stap 3 en slaat u vervolgens over naar Stap 8.

- Volledig gekwalificeerde Domeinnaam — De clientidentificatie van de externe identiteit is gebaseerd op de volledig gekwalificeerde Domeinnaam. U kunt deze optie alleen kiezen als u in Stap 2 van de sectie *Verificatie* een PSK-verificatiemethode kiest. Als u deze optie kiest, volgt u Stap 4 en slaat u vervolgens over naar Stap 8.

- Gebruiker Volledig gekwalificeerde Domeinnaam - De client-identificatie van de externe identiteit is gebaseerd op een volledig gekwalificeerde Domeinnaam van de gebruiker. U kunt deze optie alleen kiezen als u in Stap 2 van de sectie *Verificatie* een PSK-verificatiemethode kiest. Als u deze optie kiest, volgt u Stap 5 en slaat u vervolgens over naar Stap 8.

- IP-adres — Clientidentificatie van de externe identiteit is gebaseerd op IP-adres. Als u controleert **Gebruik een ontdekt lokaal host-adres**, wordt het IP-adres automatisch herkend. Als u deze optie kiest, volgt u Stap 6 en slaat u vervolgens over naar Stap 8.

- Belangrijkste identificator — De client-identificatie van de externe cliënt is gebaseerd op een sleutelidentificatiecode. Als u deze optie kiest, volgt u Stap 7 en Stap 8.



Stap 3. Voer de string ASN.1 in het veld *ASN.1 DN-string in*.

Stap 4. Voer de volledig gekwalificeerde domeinnaam in als een DNS-string in het veld *FQDN-string*.

Stap 5. Voer de volledig gekwalificeerde domeinnaam van de gebruiker in als DNS-string in het veld *UFQDN-string*.

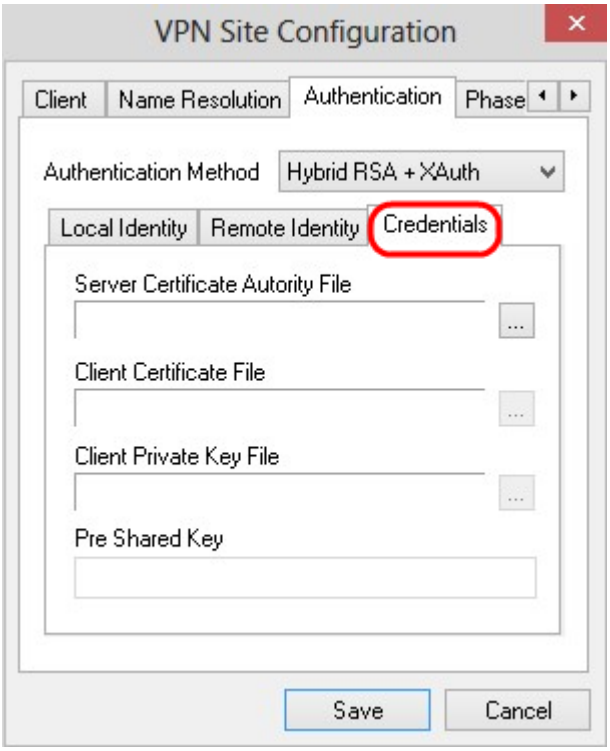
Stap 6. Voer het IP-adres in het veld *UFQD-string in*.

Stap 7. Voer de belangrijkste identificator in om de lokale client in het veld *Key ID String* te identificeren.

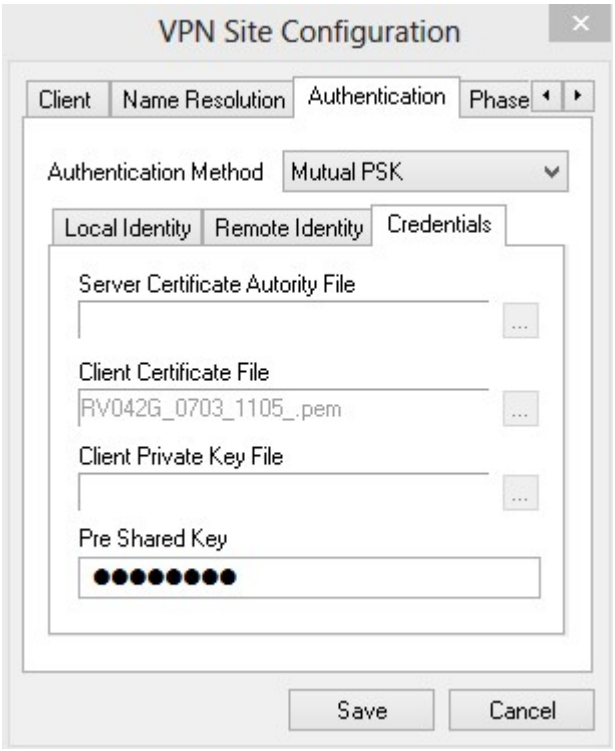
Stap 8. Klik op **Opslaan** om de instellingen op te slaan.

Credentials configuratie

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



Opmerking: In het gedeelte *Credentials* is de voorgedeelde sleutel ingesteld.



Stap 2. Klik op het **bestand** met servercertificaat om het bestand te kiezen. pictogram naast het veld *Server certificaatinstantie* en kies het pad waar u het servercertificaatbestand op uw pc hebt opgeslagen.

Stap 3. Klik op het **...** pictogram naast het veld *Clientcertificaat* en kies het pad waar u het clientcertificaatbestand op uw pc hebt opgeslagen.

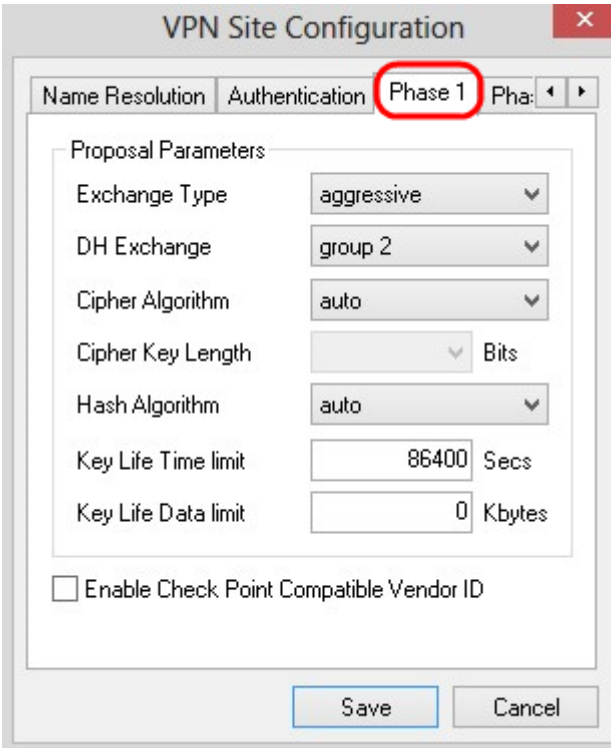
Stap 4. Klik op het **bestand** om het client-private sleutelbestand te kiezen. pictogram naast het veld *Clientbestand* en kies het pad waar u het clientbestand voor privé-toets in uw pc hebt opgeslagen.

Stap 5. Voer de vooraf gedeelde toets in het veld *PreShared Key in*. Dit moet dezelfde toets zijn die u gebruikt tijdens de configuratie van de tunnel.

Stap 6. Klik op **Save** om de instellingen op te slaan.

Configuratie fase 1

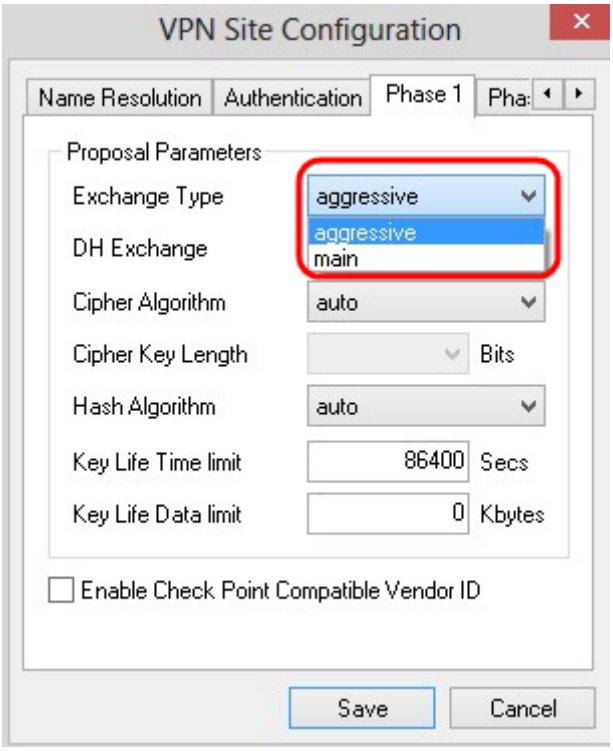
Stap 1. Klik op het tabblad **Phase 1**.



Opmerking: In het gedeelte *Fase 1* kunt u de parameters zo configureren dat een ISAKMP SA met de client gateway kan worden ingesteld.

Stap 2. Kies het juiste type voor sleuteluitwisseling in de vervolgkeuzelijst *Wisseltype*.

- Hoofdscherm — De identiteit van de peers is beveiligd.
- Aggressief: De identiteit van de peers is niet vastgemaakt.



Stap 3. In de vervolgkeuzelijst *DH Exchange* kiest u de juiste groep die tijdens de configuratie van de VPN-verbinding is geselecteerd.

Stap 4. Kies in de vervolgkeuzelijst *algoritme* kopiëren de juiste optie die tijdens de configuratie van de VPN-verbinding is geselecteerd.

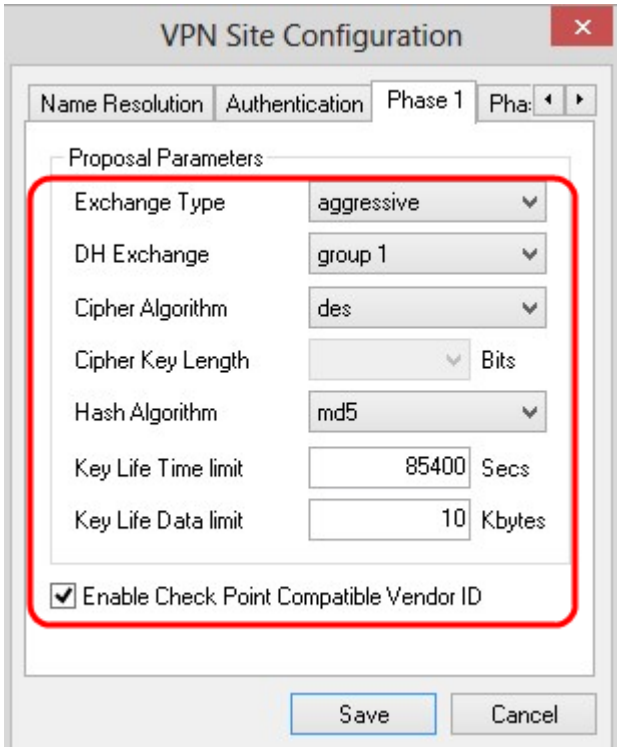
Stap 5. Kies in de vervolgkeuzelijst *Toetslengte* van het *scherm* de optie die overeenkomt met de lengte van de sleuteloptie die is geselecteerd tijdens uw configuratie van de VPN-verbinding.

Stap 6. Kies in de vervolgkeuzelijst *Hash Algorithm*, de optie die tijdens de configuratie van de VPN-verbinding is geselecteerd.

Stap 7. Voer in het veld *Key Life Time*-grenswaarde in de waarde die tijdens de configuratie van de VPN-verbinding is gebruikt.

Stap 8. Voer in het veld *Key Life Data* limit in de waarde in kilobytes om te beschermen. De standaardwaarde is 0 en schakelt de functie uit.

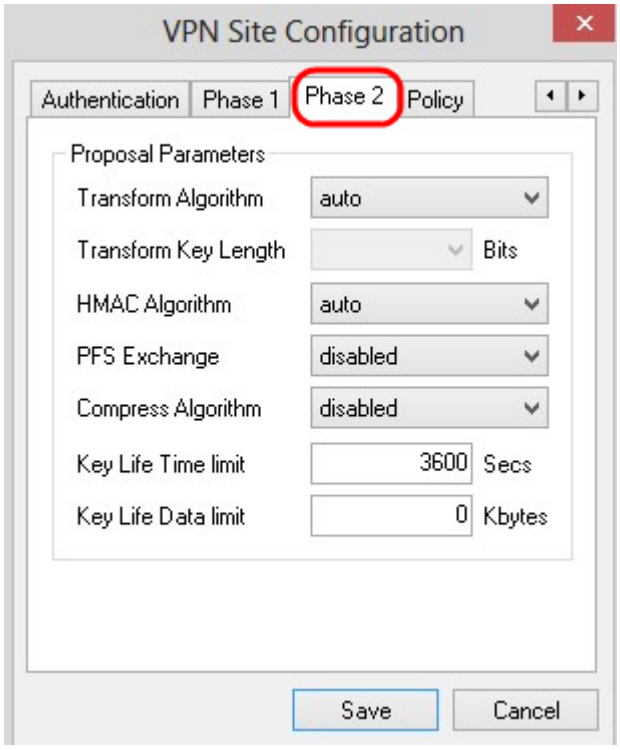
Stap 9. (optioneel) Controleer het vakje **aangevinkt met compatibele verkoper en ID**.



Stap 10. Klik op **Opslaan** om de instellingen op te slaan.

Configuratie fase 2

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



Opmerking: In het gedeelte *Fase 2* kunt u de parameters zo configureren dat een IPsec SA met de externe client gateway kan worden ingesteld.

Stap 2. Kies in de vervolgkeuzelijst *Algoritme* omzetten de optie die is geselecteerd tijdens de configuratie van de VPN-verbinding.

Stap 3. Kies in de vervolgkeuzelijst *Toetslengte omzetten* de optie die overeenkomt met de

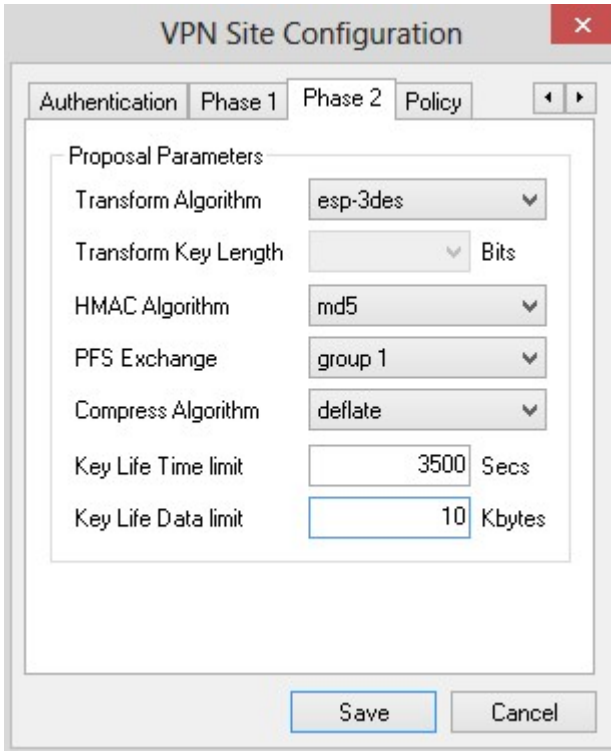
sleutellengte van de optie die is geselecteerd tijdens de configuratie van de VPN-verbinding.

Stap 4. Kies in de vervolgkeuzelijst *HMAC-algoritme* de optie die tijdens de configuratie van de VPN-verbinding is geselecteerd.

Stap 5. In de vervolgkeuzelijst *PFS Exchange* kiest u de optie die tijdens de configuratie van de VPN-verbinding is geselecteerd.

Stap 6. Voer in het veld *Key Life Time-limiet* in de waarde die wordt gebruikt tijdens de configuratie van de VPN-verbinding.

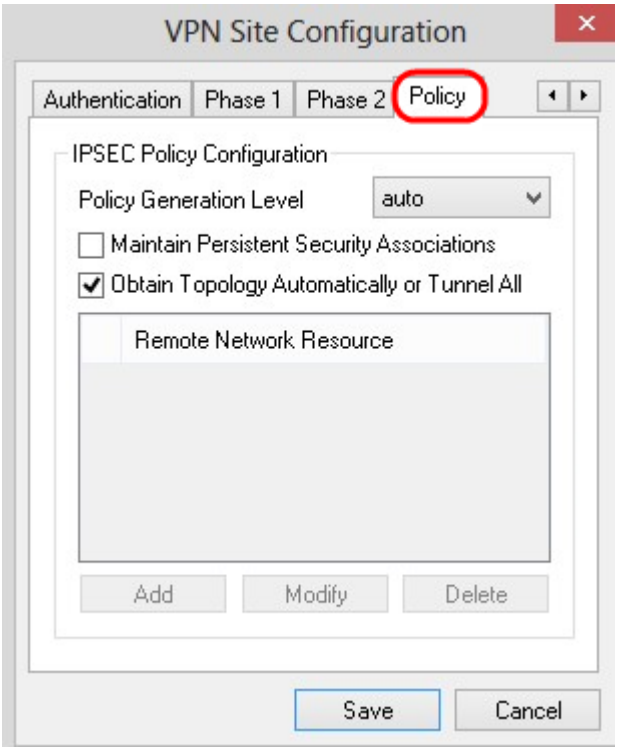
Stap 7. Voer in het veld *Key Life Data limit* in de waarde in kilobytes om te beschermen. De standaardwaarde is 0 en schakelt de functie uit.



Stap 8. Klik op **Opslaan** om de instellingen op te slaan.

Beleidsconfiguratie

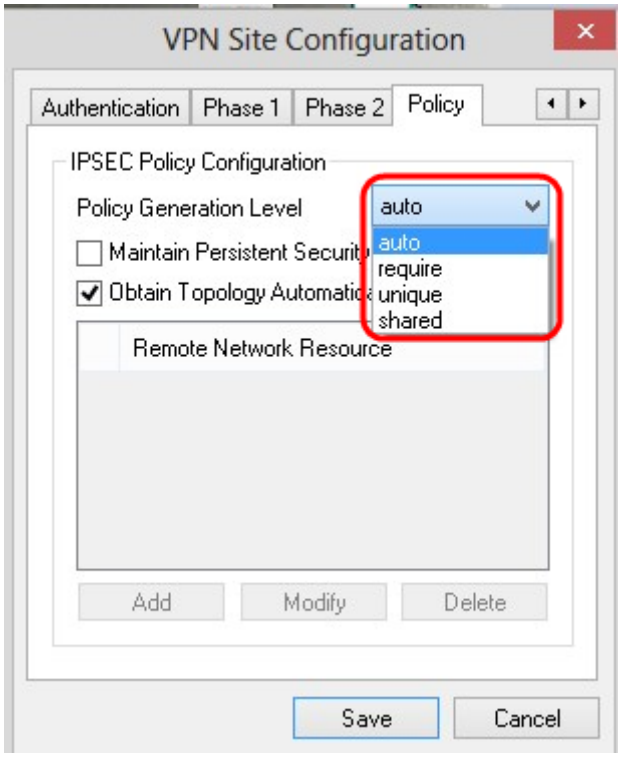
Stap 1.Klik op het tabblad **Beleid**.



Opmerking: In de sectie *Beleidsbeleid* is het IPSEC-beleid gedefinieerd. Dit is vereist voor de client om met de host te communiceren voor de configuratie van de site.

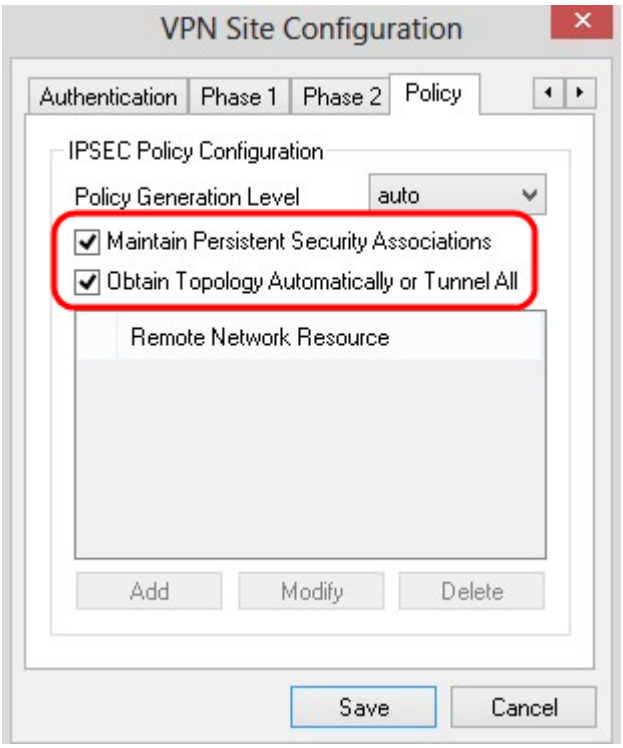
Stap 2. Kies in de vervolgkeuzelijst *Niveau* van *Beleidsgeneratie* de juiste optie.

- Auto — Het gewenste IPsec-beleidsniveau wordt automatisch bepaald.
- Vereiste — Er wordt niet onderhandeld over een unieke veiligheidsassociatie voor elk beleid.
- Uniek — Er wordt onderhandeld over een unieke veiligheidsinstantie voor elk beleid.
- Gedeeld — Het juiste beleid wordt op het vereiste niveau ontwikkeld.

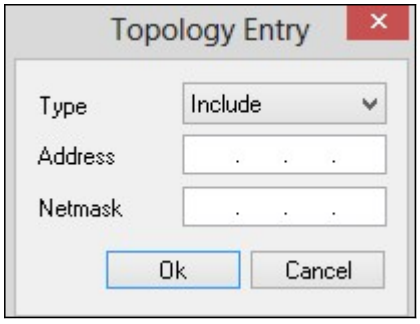


Stap 3. (Optioneel) Om de IPSec-onderhandelingen te wijzigen, controleert u het vakje **Onderhouden persistente security associaties**. Als dit mogelijk is, wordt voor elk beleid direct na het aansluiten onderhandeld. Indien gehandicapt, wordt er op behoefte onderhandeld.

Stap 4. (Optioneel) Om een automatisch meegeleverde lijst met netwerken van het apparaat te ontvangen, of om alle pakketten standaard naar de RV0XX te verzenden, **dient** u **automatisch** de **betreffende topologie of het** vakje **Tunnel All te** controleren. Als dit niet is gebeurd, moet de configuratie handmatig worden uitgevoerd. Als dit item is ingeschakeld, slaat u de optie Stap 10 over.

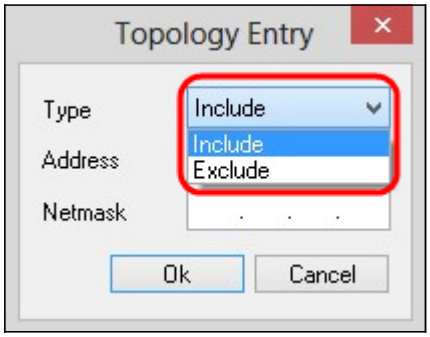


Stap 5. Klik op **Add** om een onderwerp in de tabel toe te voegen. Het venster *Topologie*-ingang verschijnt.



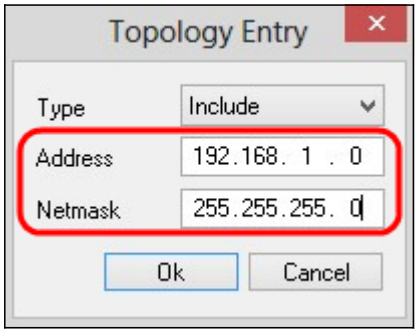
Stap 6. Kies in de vervolgkeuzelijst *Type* de juiste optie.

- Inclusief — Het netwerk is bereikbaar via een VPN-gateway.
- Uitsluiten - Het netwerk is toegankelijk via een lokale connectiviteit.

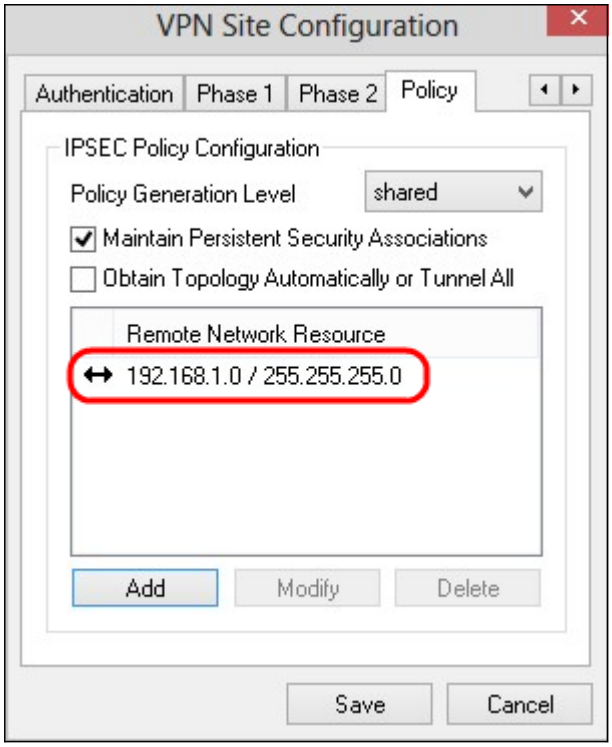


Stap 7. Voer in het veld *Adres* het IP-adres in van de RV0XX.

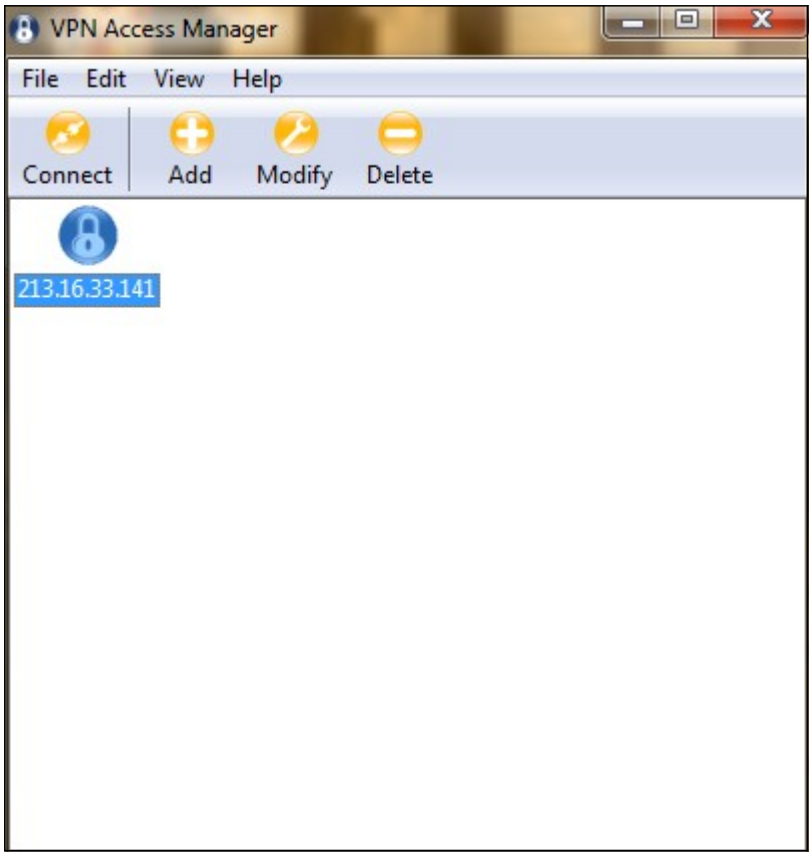
Stap 8. In het veld *Netmasker* voert u het subnetmasker van het apparaat in.



Stap 9. Klik op **OK**. Het IP-adres en het subnetmaskeradres van de RV0XX worden weergegeven in de lijst met externe netwerkbronnen.



Stap 10. Klik op **Save**, wat de gebruiker naar het *VPN Access Manager*-venster retourneert waar de nieuwe VPN-verbinding wordt weergegeven.

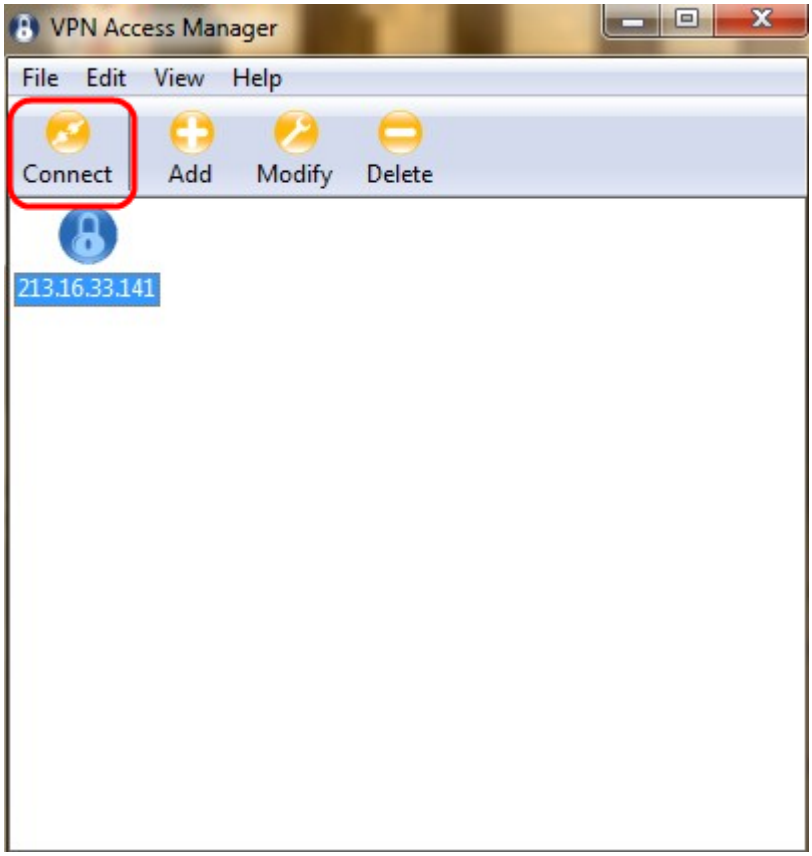


Connect

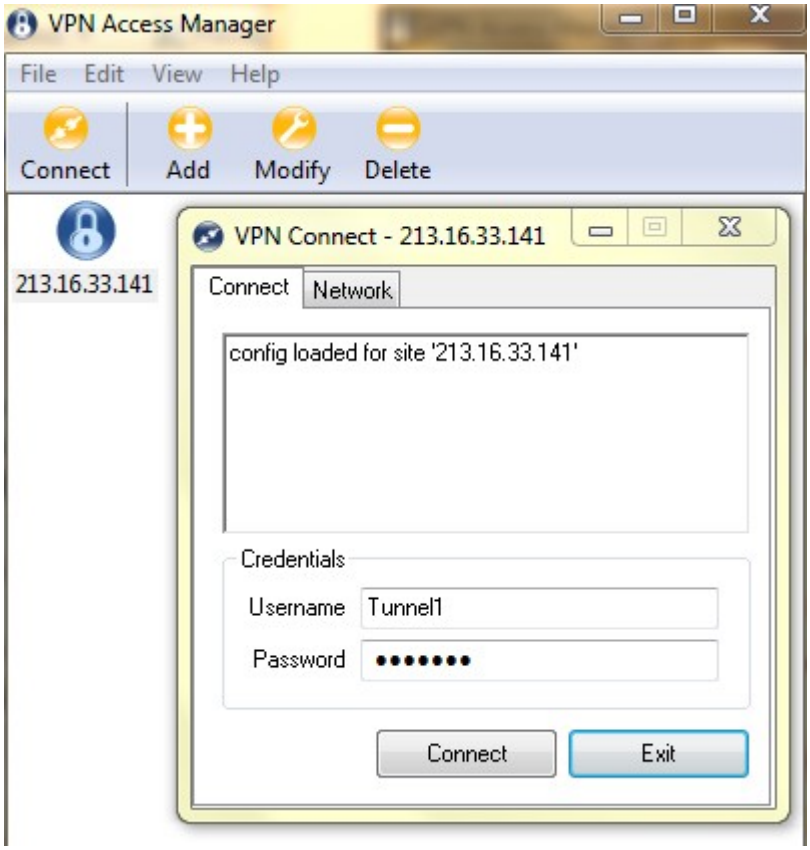
In dit gedeelte wordt uitgelegd hoe u de VPN-verbinding kunt instellen nadat alle instellingen zijn geconfigureerd. De vereiste logininformatie is hetzelfde als de VPN-clienttoegang die op het apparaat is ingesteld.

Stap 1. Klik op de gewenste VPN-verbinding.

Stap 2. Klik op **Connect.**



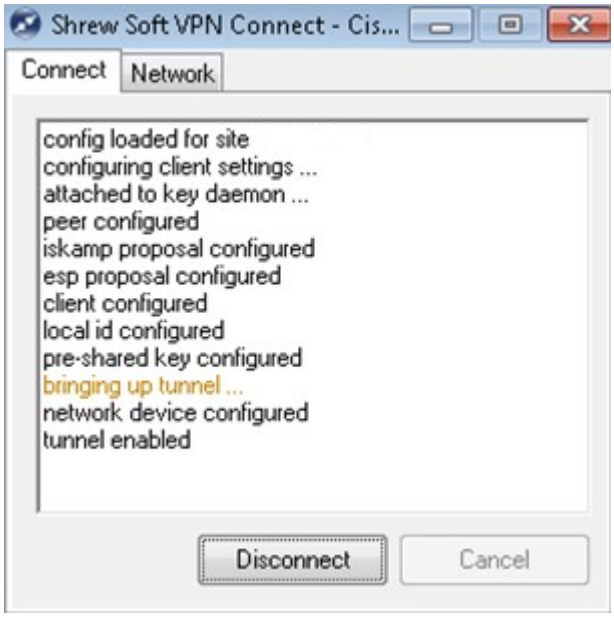
Het *VPN Connect*-venster verschijnt:



Stap 3. Voer de gebruikersnaam voor VPN in het veld *Gebruikersnaam* in.

Stap 4. Voer het wachtwoord in voor de VPN-gebruikersaccount in het veld *Wachtwoord*.

Stap 5. Klik op **Connect**. Het *venster Shrew Soft VPN Connect* verschijnt:



Stap 6. (optioneel) Klik om de verbinding uit te schakelen op **afsluiten**.

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.