Configuration of Shrew VPN Client on RV042, RV042G and RV082 VPN Routers through Windows

Objective

A Virtual Private Network (VPN) is a method for remote users to virtually connect to a private network over the Internet. A Client to Gateway VPN connects the desktop or laptop of a user to a remote network using VPN client software. Client to Gateway VPN connections are useful for remote employees who want to securely connect to the office network remotely. Shrew VPN Client is software configured on a remote host device that provides easy and secure VPN connectivity.

The objective of this document is to show you how to configure Shrew VPN Client for a computer that connects to a RV042, RV042G or RV082 VPN Router.

Note: This document assumes you have already downloaded the Shrew VPN Client on the Windows computer. Otherwise you need to configure a Client to Gateway VPN connection before you can start to configure the Shrew VPN. To know more on how to configure Client to Gateway VPN, refer to *Set Up a Remote Access Tunnel (Client to Gateway) for VPN Clients on RV042, RV042G and RV082 VPN Routers*.

Applicable Devices

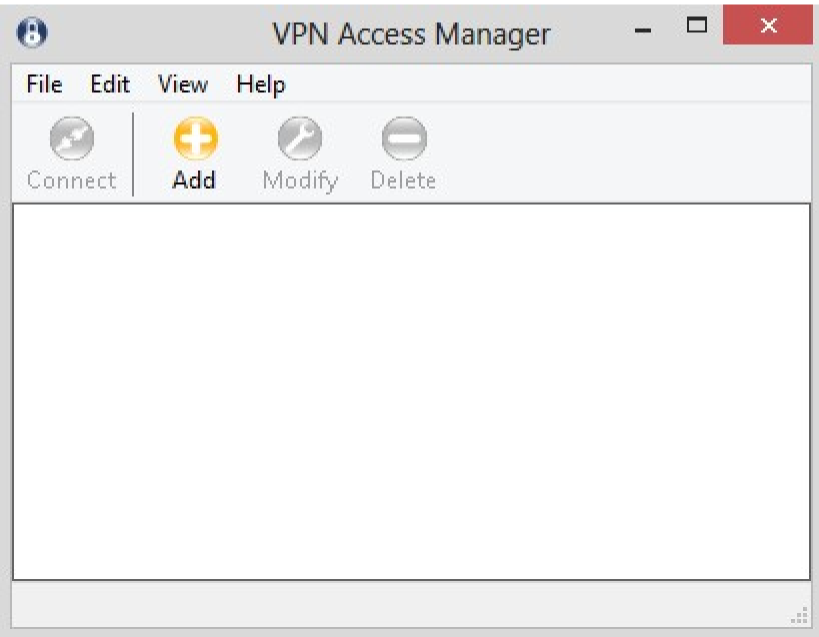
- RV042
- RV042G
- RV082

Software Version

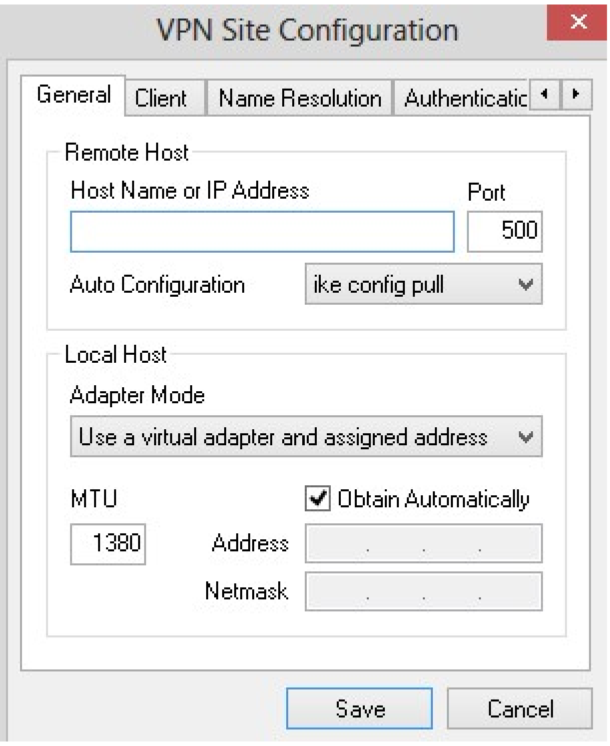
- v4.2.2.08

Configure the Shrew VPN Client Connection on Windows

Step 1. Click the **Shrew VPN Client program** on the computer and open it. The *Shrew Soft VPN Access Manager* window opens:



Step 2. Click **Add**. The *VPN Site Configuration* window appears:



Remote Host

Host Name or IP Address

Port 500

Auto Configuration: ike config pull

Local Host

Adapter Mode: Use a virtual adapter and assigned address

MTU 1380

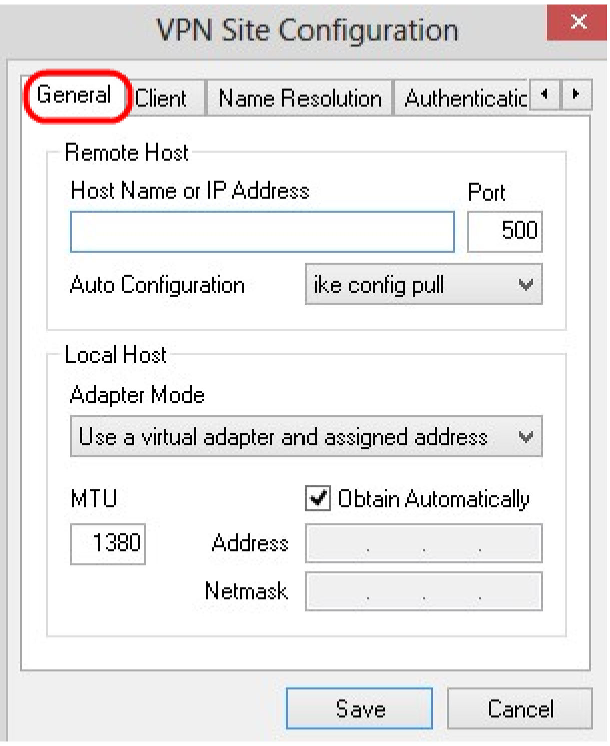
☑ Obtain Automatically

Address

Netmask

General Configuration

Step 1. Click the **General** tab.



Remote Host

Host Name or IP Address

Port 500

Auto Configuration ike config pull

Local Host

Adapter Mode

Use a virtual adapter and assigned address

MTU 1380

☑ Obtain Automatically

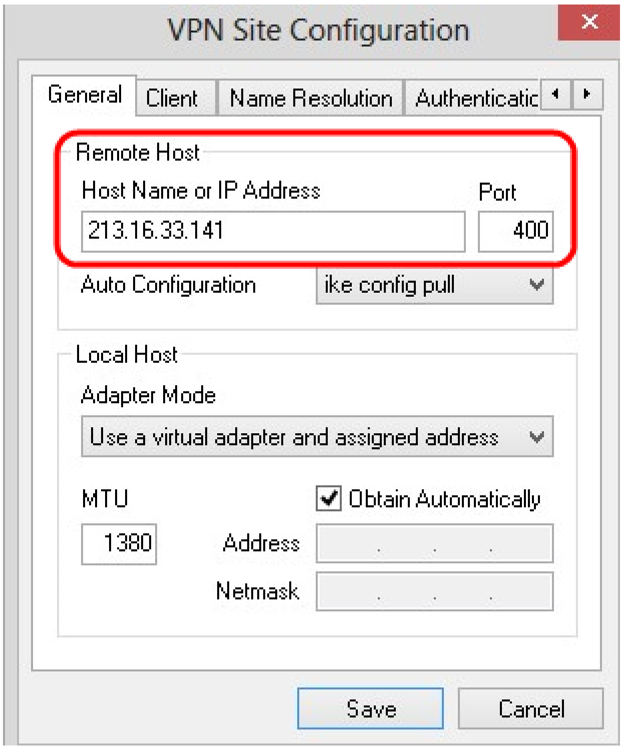
Address . . .

Netmask . . .

Note: The *General* section is used to configure the Remote and Local Host IP addresses. These are used to define the network parameters for the Client to Gateway connection.

Step 2. In the *Host Name or IP Address* field, enter the remote host IP address, which is the IP address of the configured WAN.

Step 3. In the *Port* field, enter the number of the port to be used for the connection. The port number used in the pictured example is 400.



Remote Host

Host Name or IP Address 213.16.33.141

Port 400

Auto Configuration ike config pull

Local Host

Adapter Mode

Use a virtual adapter and assigned address

MTU 1380

☑ Obtain Automatically

Address . . .

Netmask . . .

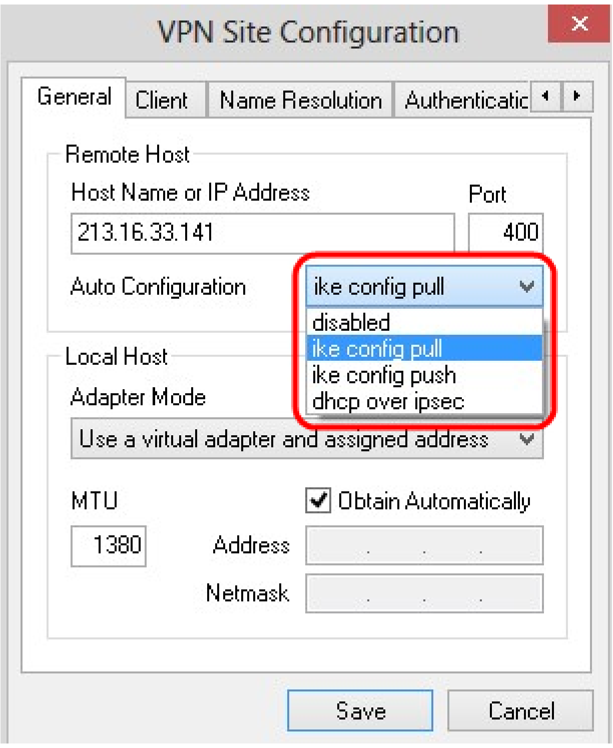
Step 4. From the *Auto Configuration* drop-down list, choose the desired configuration.

- Disabled — The disabled option disables any automatic client configurations.
- IKE Config Pull — Allows setting requests from a computer by the client. With the support

of the Pull method by the computer, the request returns a list of settings that are supported by the client.

- IKE Config Push — Gives a computer the opportunity to offer settings to the client through the configuration process. With the support of the Push method by the computer, the request returns a list of settings that are supported by the client.

- DHCP Over IPSec — Gives the client the opportunity to request settings from the computer through DHCP over IPSec.



VPN Site Configuration

Remote Host

Host Name or IP Address 213.16.33.141

Port 400

Auto Configuration ike config pull

Local Host

Adapter Mode Use a virtual adapter and assigned address

MTU 1380

☑ Obtain Automatically

Address . . .

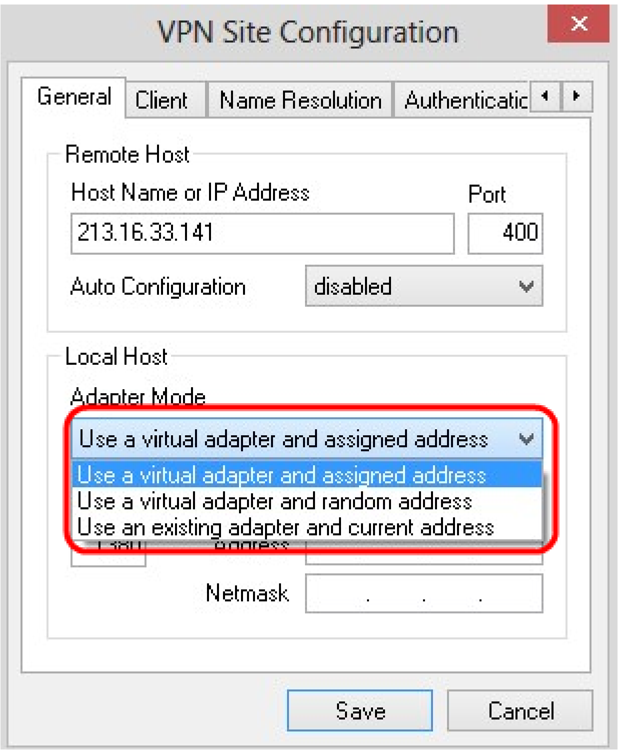
Netmask . . .

Step 5. From the *Adapter Mode* drop-down list, choose the desired adapter mode for local host based on the Auto Configuration.

- Use a Virtual Adapter and Assigned Address — Allows the client to use a virtual adapter with a specified address.

- Use a Virtual Adapter and Random Address — Allows the client to use a virtual adapter with random address.

- Use an Existing Adapter and Current Address — Uses an existing adapter and its address. No additional information needs to be entered.


VPN Site Configuration
General
Client
Name Resolution
Authenticatic
Remote Host
Local Host
Use a virtual adapter and assigned address
Use a virtual adapter and random address
Use an existing adapter and current address
Save
Cancel

Host Name or IP Address: 213.16.33.141

Port: 400

Auto Configuration: disabled

Adapter Mode: Use a virtual adapter and assigned address

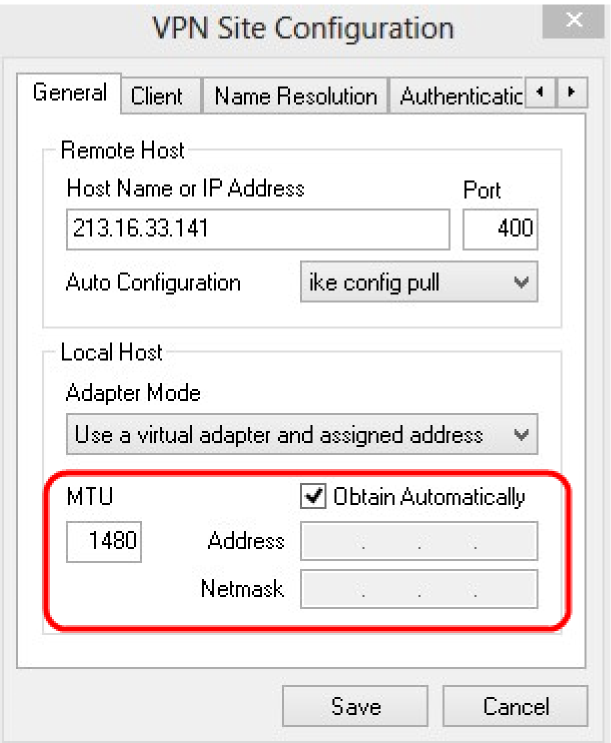
Netmask: . . .

Step 6. Enter the maximum transmission unit (MTU) in the *MTU* field if you chose **Use a Virtual Adapter and Assigned Address** from the *Adapter Mode* drop-down list in Step 5. The maximum transmission unit helps to resolve IP fragmentation problems. The default value is 1380.

Step 7. (Optional) To get the Address and Subnet Mask automatically through DHCP server, check the **Obtain Automatically** check box. This option is not available for all configurations.

Step 8. Enter the IP address of the remote client in the *Address field* if you chose **Use a Virtual Adapter and Assigned Address** from the ***Adapter Mode*** drop-down list in Step 5.

Step 9. Enter Subnet Mask of the IP address of the remote client in the *Netmask* field if you chose **Use a Virtual Adapter and Assigned Address** from the *Adapter Mode* drop-down list in Step 5.



VPN Site Configuration

General | Client | Name Resolution | Authenticatic

Remote Host

Host Name or IP Address: 213.16.33.141

Port: 400

Auto Configuration: ike config pull

Local Host

Adapter Mode: Use a virtual adapter and assigned address

MTU: 1480

☑ Obtain Automatically

Address: . . .

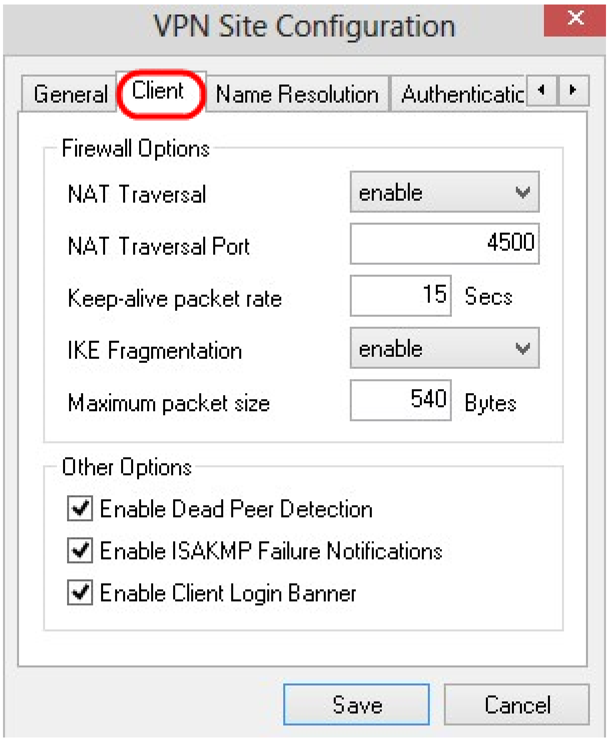
Netmask: . . .

Save | Cancel

Step 10. Click **Save** to save the settings.

Client Configuration

Step 1. Click the **Client** tab.



VPN Site Configuration

General | Client | Name Resolution | Authenticatic

Firewall Options

NAT Traversal: enable

NAT Traversal Port: 4500

Keep-alive packet rate: 15 Secs

IKE Fragmentation: enable

Maximum packet size: 540 Bytes

Other Options

☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

☑ Enable Client Login Banner

Save | Cancel

Note: In the *Client* section, you can configure the Firewall options, Dead Peer Detection, and ISAKMP (Internet Security Association and Key Management Protocol) Failure Notifications. The settings define which configuration options are manually configured and which are automatically obtained.

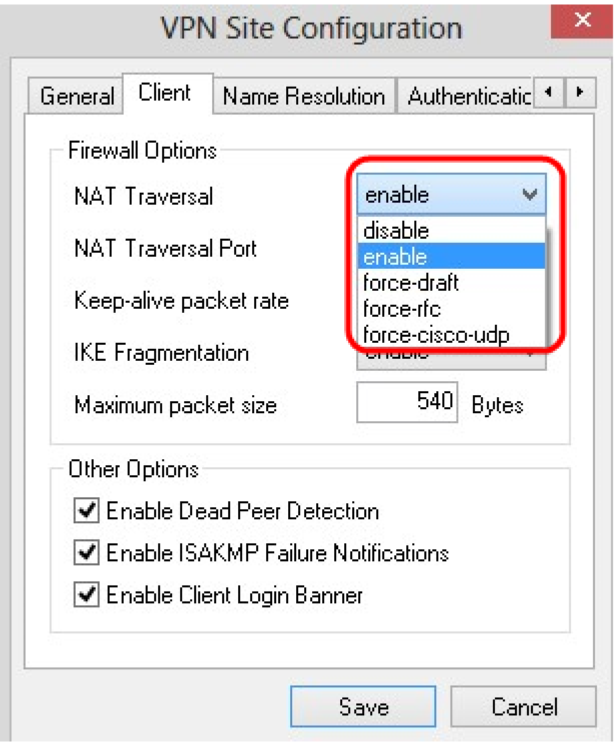
Step 2. Choose the appropriate NAT (Network Address Translation) traversal option from the *NAT Traversal* drop-down list.

- Disable — NAT protocol is disabled.

- Enable — IKE fragmentation is only used if the gateway indicates support through negotiations.

- Force Draft — The draft version of the NAT protocol. It is used if the gateway indicates support through the negotiation or the detection of the NAT.

- Force RFC — The RFC version of the NAT protocol. It is used if the gateway indicates support through the negotiation or the detection of the NAT.



Firewall Options

NAT Traversal: enable

NAT Traversal Port

Keep-alive packet rate

IKE Fragmentation: enable

Maximum packet size: 540 Bytes

Other Options

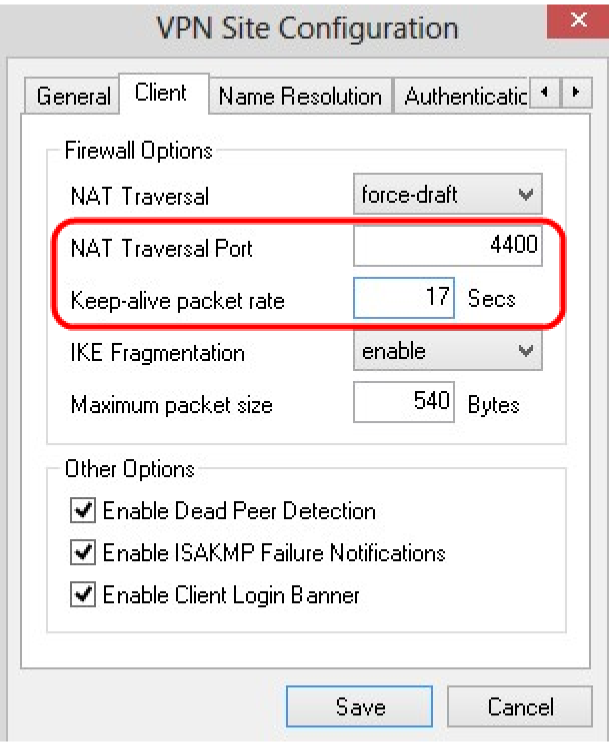
☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

☑ Enable Client Login Banner

Step 3. Enter the UDP port for the NAT in the *NAT Traversal Port* field. The default value is 4500.

Step 4. In the *Keep-alive packet rate* field, enter a value for the rate keep-alive packets are sent. The value is measured in seconds. The default value is 30 seconds.



Firewall Options

NAT Traversal: force-draft

NAT Traversal Port: 4400

Keep-alive packet rate: 17 Secs

IKE Fragmentation: enable

Maximum packet size: 540 Bytes

Other Options

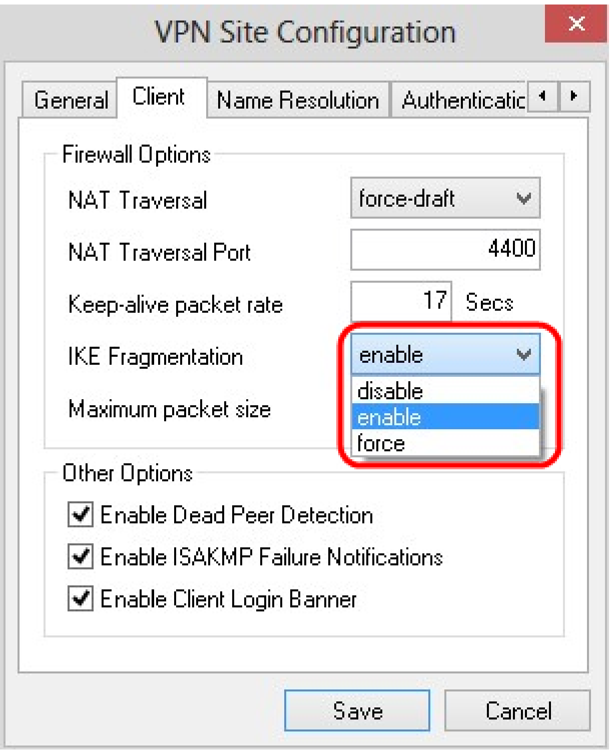
☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

☑ Enable Client Login Banner

Step 5. In the *IKE Fragmentation* drop-down list, choose the appropriate option.

- Disable — IKE fragmentation is not used.
- Enable — IKE fragmentation is only used if the gateway indicates support through negotiations.
- Force — IKE fragmentation is used regardless of indications or detection.



Firewall Options

NAT Traversal: force-draft

NAT Traversal Port: 4400

Keep-alive packet rate: 17 Secs

IKE Fragmentation: enable

Maximum packet size

Other Options

☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

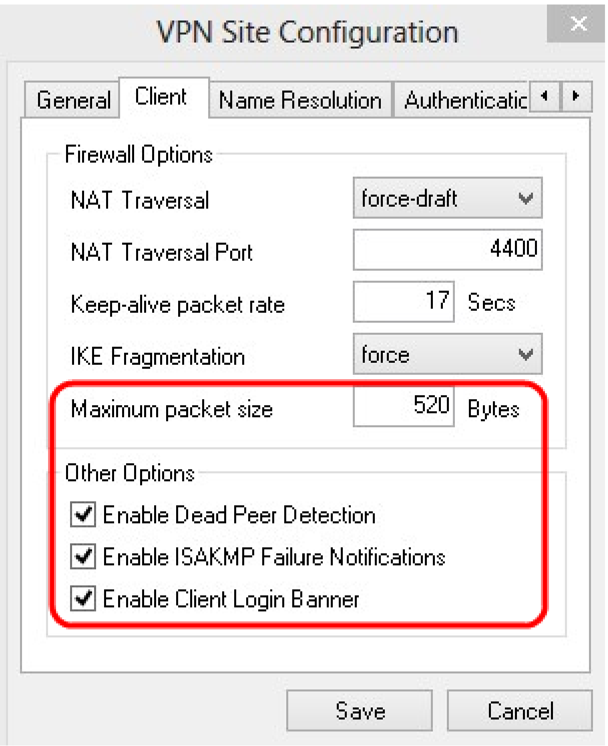
☑ Enable Client Login Banner

Step 6. Enter the maximum packet size in the *Maximum packet size* field in Bytes. If the packet size is larger than the maximum packet size, IKE fragmentation is performed. The default value is 540 Bytes.

Step 7. (Optional) To allow the computer and client to detect when the other is no longer able to respond, check the **Enable Dead Peer Detection** check box.

Step 8. (Optional) To send failure notifications by the VPN client, check the **Enable ISAKMP Failure Notifications** check box.

Step 9. (Optional) To show a login banner by the client when the connection is established with the gateway, check the **Enable Client Login** check box.



VPN Site Configuration

Firewall Options

NAT Traversal: force-draft

NAT Traversal Port: 4400

Keep-alive packet rate: 17 Secs

IKE Fragmentation: force

Maximum packet size: 520 Bytes

Other Options

☑ Enable Dead Peer Detection

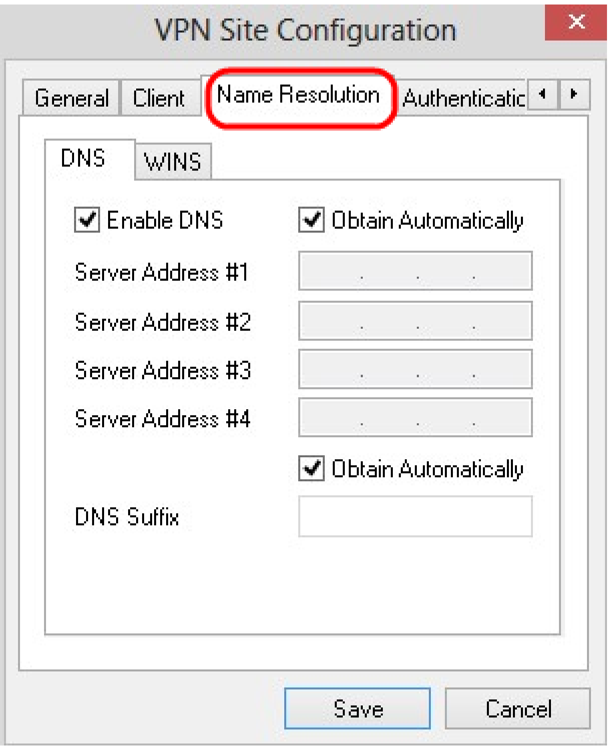
☑ Enable ISAKMP Failure Notifications

☑ Enable Client Login Banner

Step 10. Click **Save** to save the settings.

Name Resolution Configuration

Step 1. Click the **Name Resolution** tab.



☑ Enable DNS ☑ Obtain Automatically

Server Address #1

Server Address #2

Server Address #3

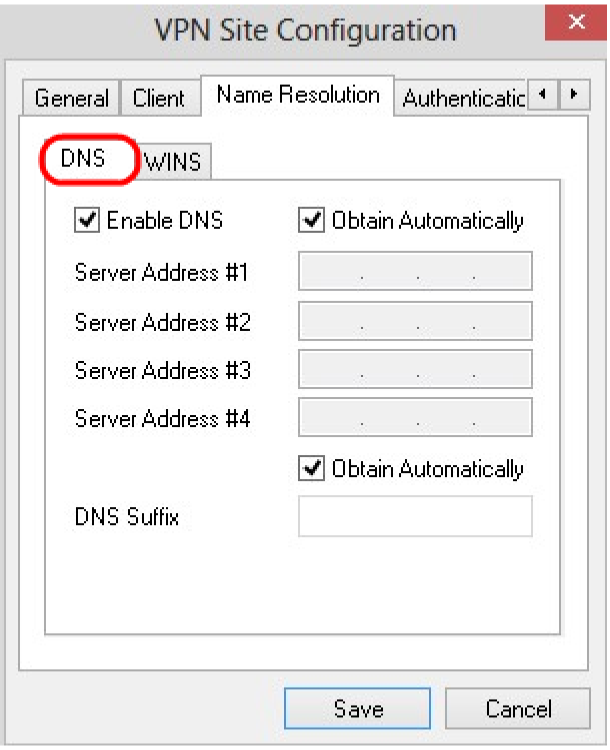
Server Address #4

☑ Obtain Automatically

DNS Suffix

Note: The *Name Resolution* section is used to configure DNS (Domain Name System) and WIN (Windows Internet Name Service) settings.

Step 2. Click the **DNS** tab.



☑ Enable DNS ☑ Obtain Automatically

Server Address #1

Server Address #2

Server Address #3

Server Address #4

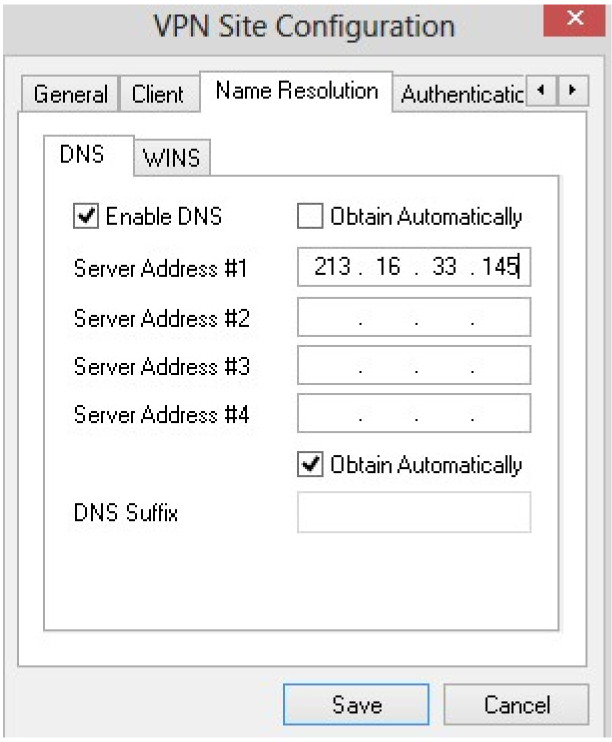
☑ Obtain Automatically

DNS Suffix

Step 3. Check **Enable DNS** to enable Domain Name System (DNS).

Step 4. (Optional) To get the DNS server address automatically, check the **Obtain Automatically** check box. If you choose this option, skip to Step 6.

Step 5. Enter the DNS server address in the *Server Address #1* field. If there is another DNS server, enter the address of those servers in the remaining *Server Address* fields.



VPN Site Configuration

☑ Enable DNS ☐ Obtain Automatically

Server Address #1 213 . 16 . 33 . 145

Server Address #2 . . .

Server Address #3 . . .

Server Address #4 . . .

☑ Obtain Automatically

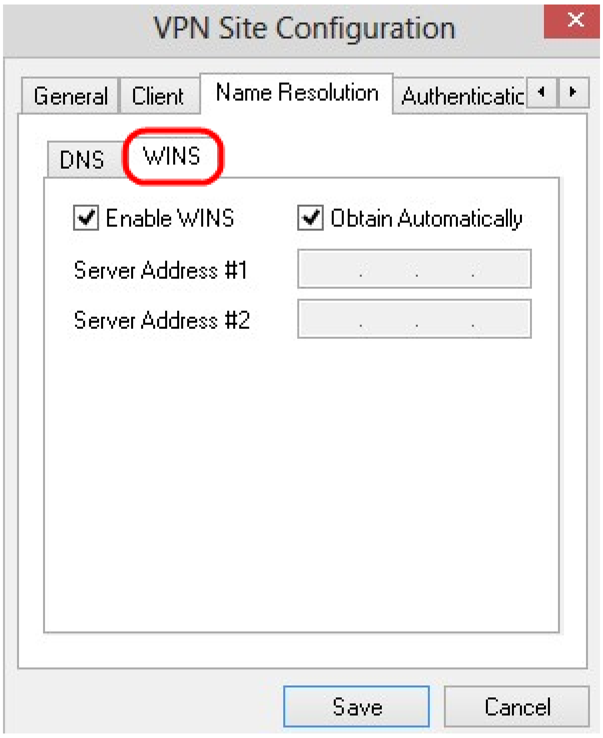
DNS Suffix

Step 6. (Optional) To get the suffix of the DNS server automatically, check the **Obtain Automatically** check box. If you choose this option, skip to Step 8.

Step 7. Enter the suffix of the DNS server in the *DNS Suffix* field.

Step 8. Click **Save** to save the settings.

Step 9. Click the **WINS** tab.



VPN Site Configuration

☑ Enable WINS ☑ Obtain Automatically

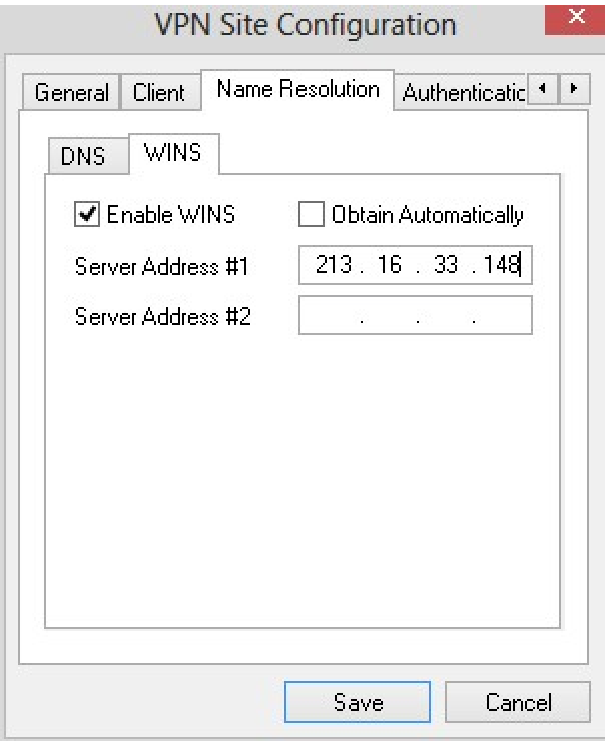
Server Address #1 . . .

Server Address #2 . . .

Step 10. Check **Enable WINS** to enable Windows Internet Name Server (WINS).

Step 11. (Optional) To get the DNS server address automatically, check the **Obtain Automatically** check box. If you choose this option, skip to Step 13.

Step 12. Enter the address of the WINS server in the *Server Address #1* field. If there are other DNS servers, enter the address of those servers in the remaining *Server Address* fields.



☑ Enable WINS ☐ Obtain Automatically

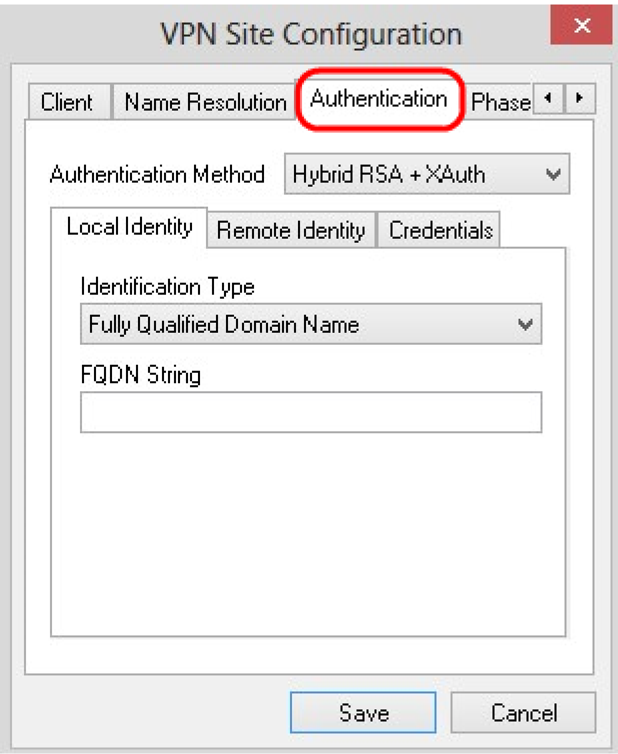
Server Address #1: 213 . 16 . 33 . 148

Server Address #2: . . .

Step 13. Click **Save** to save the settings.

Authentication

Step 1. Click the **Authentication** tab.



Authentication Method: Hybrid RSA + XAuth

Identification Type: Fully Qualified Domain Name

FQDN String:

Note: In the *Authentication* section, you can configure the parameters for the client to handle authentication when it attempts to establish an ISAKMP SA.

Step 2. Choose the appropriate method of authentication from the *Authentication Method* drop-down list.

- Hybrid RSA + XAuth — The client credential is not needed. The client will authenticate the gateway. The credentials will be in the form of PEM or PKCS12 certificate files or key files type.

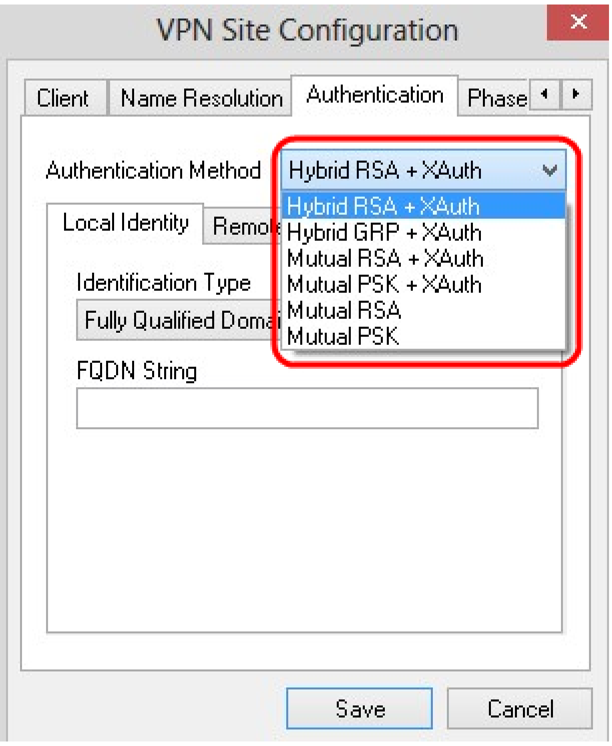
- Hybrid GRP + XAuth — The client credential is not needed. The client will authenticate the gateway. The credentials will be in the form of PEM or PKCS12 certificate file and a shared secret string.

- Mutual RSA + XAuth — Client and gateway both need credentials to authenticate. The credentials will be in the form of PEM or PKCS12 certificate files or key type.

- Mutual PSK + XAuth — Client and gateway both need credentials to authenticate. The credentials will be in the form of a shared secret string.

- Mutual RSA — Client and gateway both need credentials to authenticate. The credentials will be in the form of PEM or PKCS12 certificate files or key type.

- Mutual PSK — Client and gateway both need credentials to authenticate. The credentials will be in the form of a shared secret string.

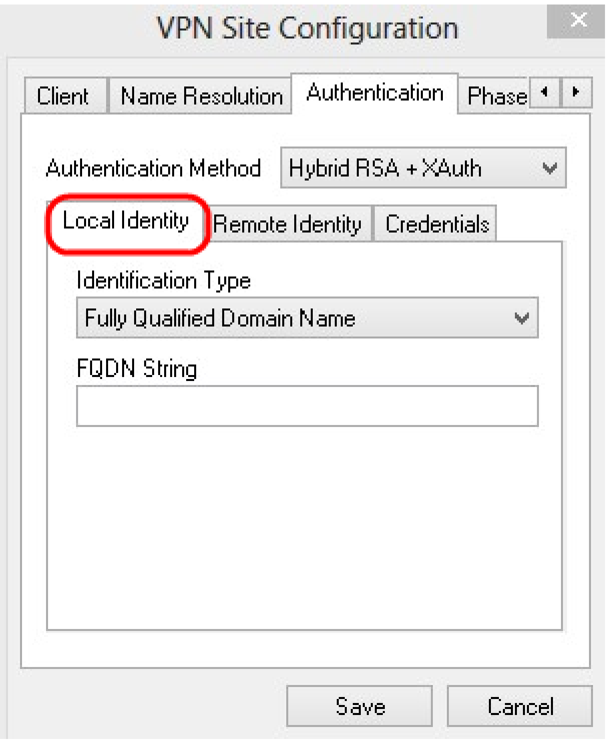

Authentication Method: Hybrid RSA + XAuth

Identification Type: Fully Qualified Domai

FQDN String:

Local Identity Configuration

Step 1. Click the **Local Identity** tab.



Note: Local Identity sets the ID that is sent to the Gateway for verification. In the *Local Identity* section, the Identification Type and FQDN (Fully Qualified Domain Name) String is configured to determine how the ID is sent.

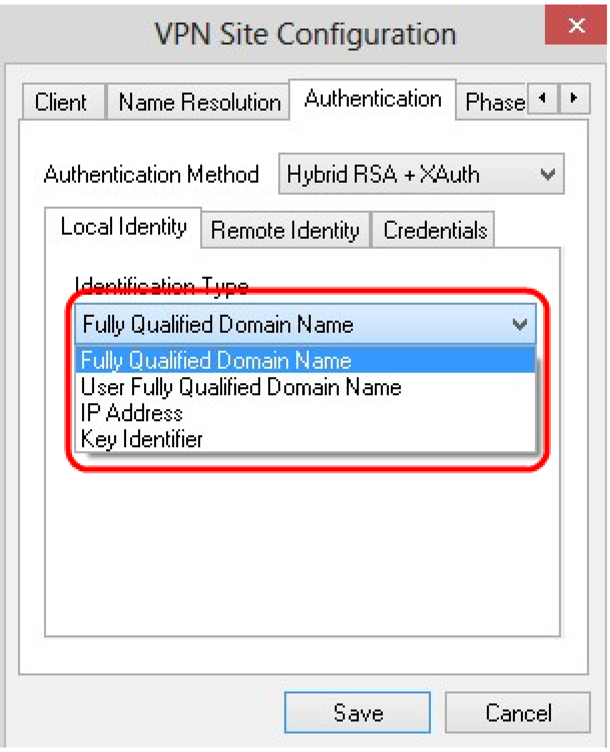
Step 2. Choose the appropriate identification option from the *Identification Type* drop-down list. Not all options are available for all authentication modes.

- Fully Qualified Domain Name — The client identification of the local identity is based on a Fully Qualified Domain Name. If you choose this option, follow Step 3 and then skip to Step 7.

- User Fully Qualified Domain Name — Client identification of the local identity is based on User Fully Qualified Domain Name. If you choose this option, follow Step 4 and then skip to Step 7.

- IP Address — Client identification of the local identity is based on IP address. If you check **Use a discovered local host address**, the IP address is discovered automatically. If you choose this option, follow Step 5 and then skip to Step 7.

- Key Identifier — Client identification of the local client is identified based on a key identifier. If you choose this option, follow Step 6 and Step 7.



Authentication Method: Hybrid RSA + XAuth

Identification Type: Fully Qualified Domain Name

Step 3. Enter the fully qualified domain name as DNS string in the *FQDN String* field.

Step 4. Enter the user fully qualified domain name as DNS string in the *UFQDN String* field.

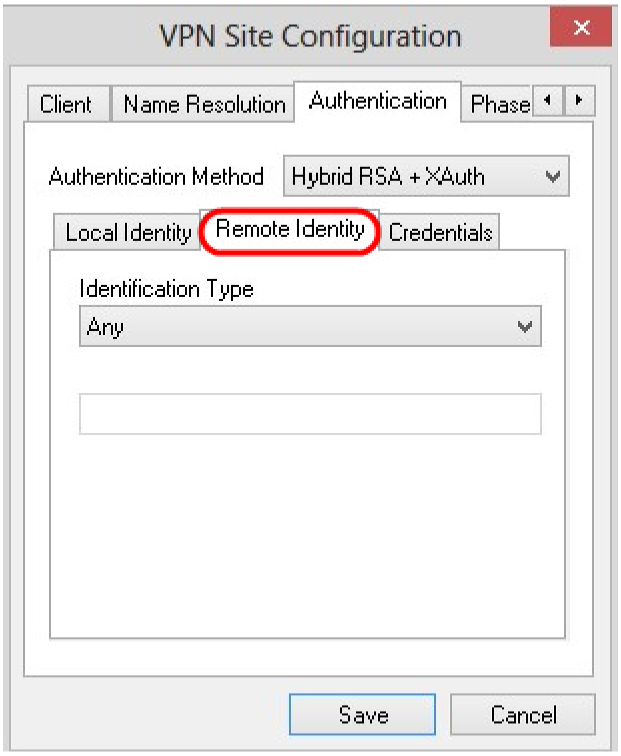
Step 5. Enter the IP address in the *UFQDN String* field.

Step 6. Enter the key identifier to identify the local client in the *Key ID String*.

Step 7. Click **Save** to save the settings.

Remote Identity Configuration

Step 1. Click the **Remote Identity** tab.



VPN Site Configuration

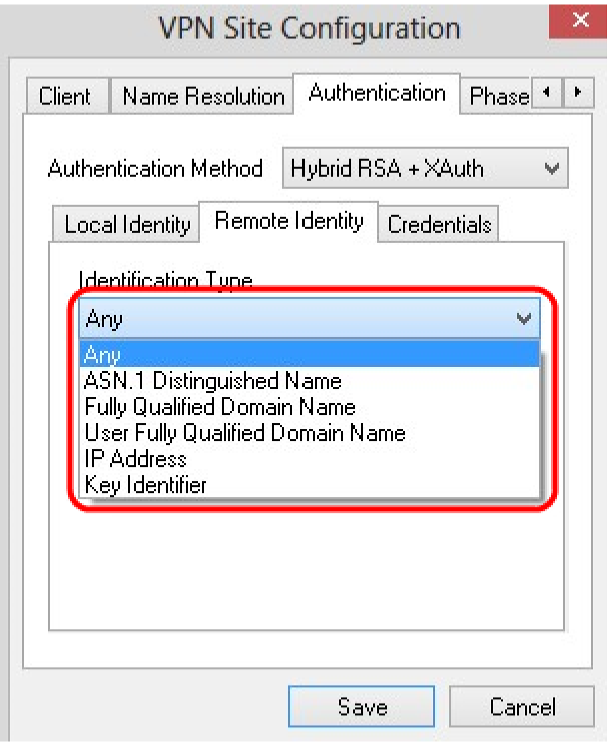
Authentication Method: Hybrid RSA + XAuth

Identification Type: Any

Note: Remote Identity verifies the ID from the Gateway. In the *Remote Identity* section, the Identification Type is configured to determine how the ID is verified.

Step 2. Choose the appropriate identification option from the *Identification Type* drop-down list.

- Any — The remote client can accept any value or ID to authenticate.
- ASN.1 Distinguished Name — The remote client is identified automatically from a PEM or PKCS12 certificate file. You are only able to choose this option if you choose an RSA authentication method in Step 2 of the *Authentication* section. Check the **Use the subject in the received certificate but don't compare it with a specific value** check box to automatically receive the certificate. If you choose this option, follow Step 3 and then skip to Step 8.
- Fully Qualified Domain Name — Client identification of the remote identity is based on Fully Qualified Domain Name. You are only able to choose this option if you choose a PSK authentication method in Step 2 of the *Authentication* section. If you choose this option, follow Step 4 and then skip to Step 8.
- User Fully Qualified Domain Name — Client identification of the remote identity is based on User Fully Qualified Domain Name. You are only able to choose this option if you choose a PSK authentication method in Step 2 of the *Authentication* section. If you choose this option, follow Step 5 and then skip to Step 8.
- IP Address — Client identification of the remote identity is based on IP address. If you check **Use a discovered local host address**, the IP address is discovered automatically. If you choose this option, follow Step 6 and then skip to Step 8.
- Key Identifier — Client identification of the remote client is identify is based on a key identifier. If you choose this option, follow Step 7 and Step 8.



Step 3. Enter the ASN.1 DN string in the *ASN.1 DN String* field.

Step 4. Enter the fully qualified domain name as a DNS string in the *FQDN String* field.

Step 5. Enter the user fully qualified domain name as DNS string in the *UFQDN String* field.

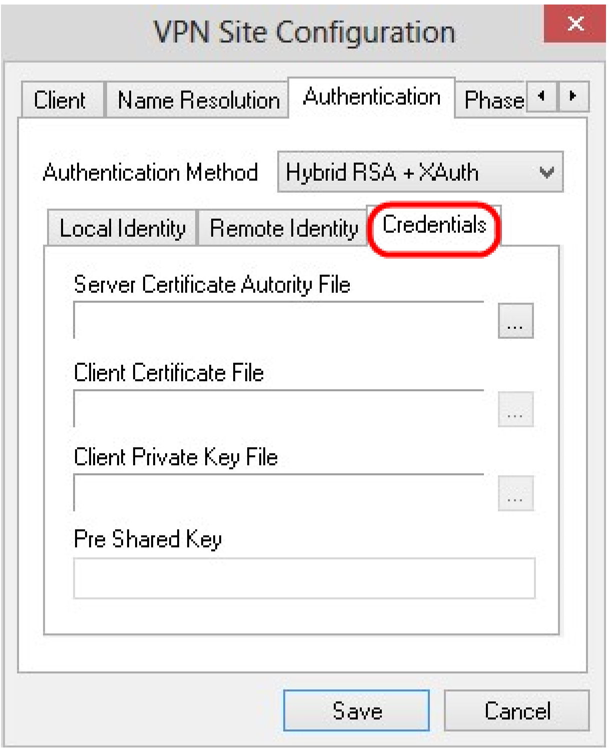
Step 6. Enter the IP address in the *UFQDN String* field.

Step 7. Enter the key identifier to identify the local client in the *Key ID String* field.

Step 8. Click **Save** to save the settings.

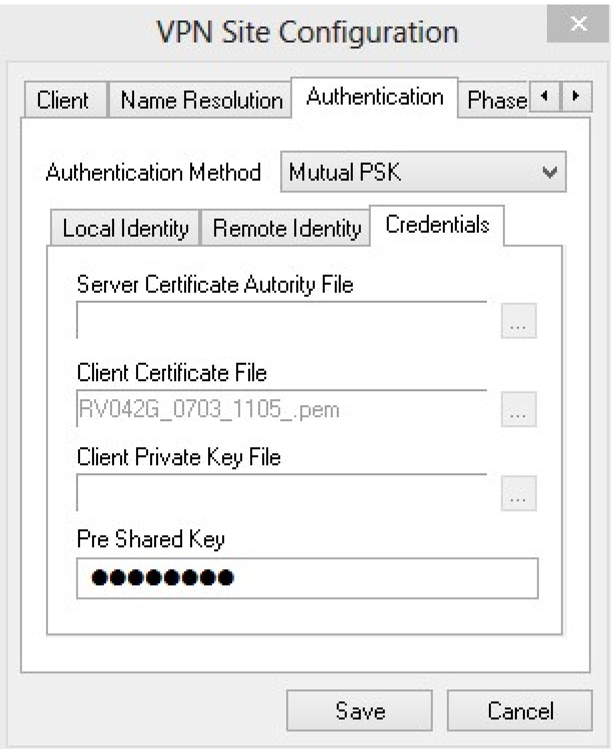
Credentials Configuration

Step 1. Click the **Credentials** tab.



Authentication Method: Hybrid RSA + XAuth

Note: In the *Credentials* section, the Pre Shared Key is configured.



Authentication Method: Mutual PSK

Client Certificate File: RV042G_0703_1105_.pem

Pre Shared Key: ●●●●●●●●●

Step 2. To choose the Server Certificate File, click the **...** icon next to the the *Server Certificate Authority File* field and choose the path where you saved the Server Certificate File on your PC.

Step 3. To choose the Client Certificate File, click the **...** icon next to the *Client Certificate File* field and choose the path where you saved the Client Certificate File on your PC.

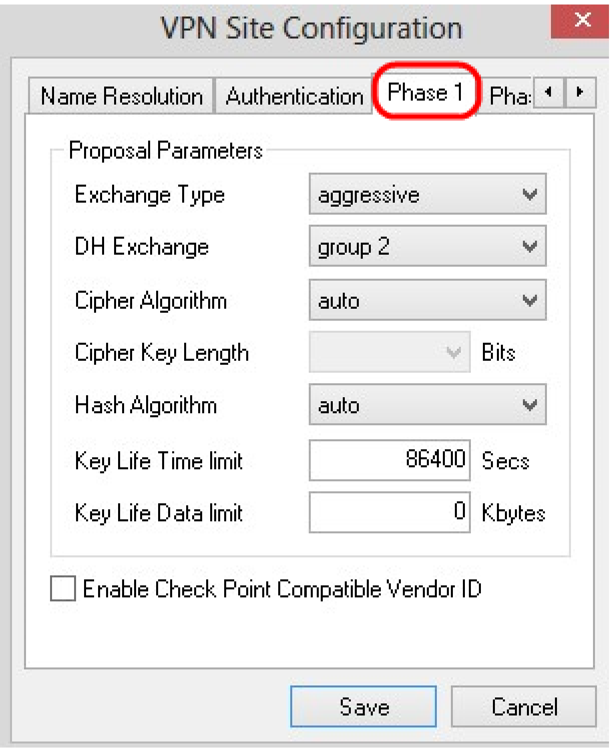
Step 4. To choose the Client Private Key File, click the **...** icon next to the *Client Private Key File* field and choose the path where you saved the Client Private Key File in your PC.

Step 5. Enter the preshared key in the *PreShared Key* field. This should be the same key that you use during the configuration of the tunnel.

Step 6. Click **Save** to save the settings.

Phase 1 Configuration

Step 1. Click the **Phase 1** tab.



Proposal Parameters

Exchange Type: aggressive

DH Exchange: group 2

Cipher Algorithm: auto

Cipher Key Length: Bits

Hash Algorithm: auto

Key Life Time limit: 86400 Secs

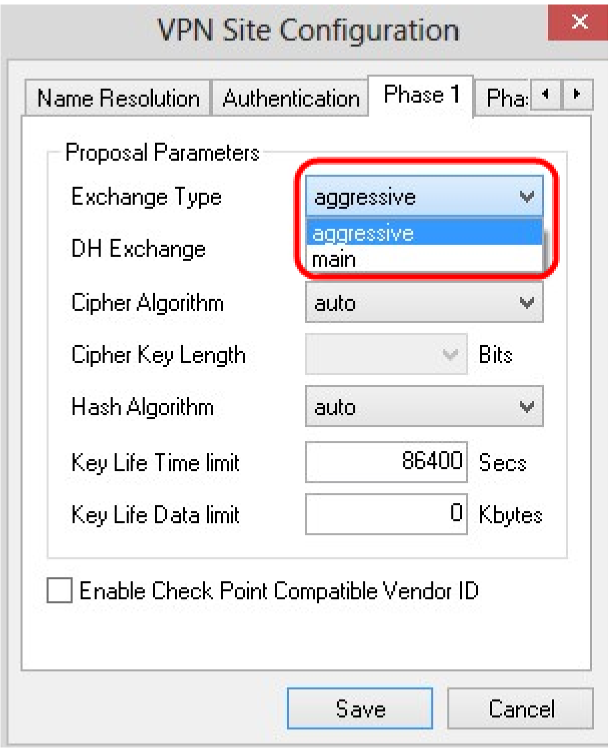
Key Life Data limit: 0 Kbytes

□ Enable Check Point Compatible Vendor ID

Note: In the *Phase 1* section, you can configure the parameters such that an ISAKMP SA with the client gateway can be established.

Step 2. Choose the appropriate key exchange type from the *Exchange Type* drop-down list.

- Main — The identity of the peers are secured.
- Aggressive — The identity of the peers are not secured.



Proposal Parameters

Exchange Type: aggressive

DH Exchange

Cipher Algorithm: auto

Cipher Key Length: Bits

Hash Algorithm: auto

Key Life Time limit: 86400 Secs

Key Life Data limit: 0 Kbytes

□ Enable Check Point Compatible Vendor ID

Step 3. In the *DH Exchange* drop-down list, choose the appropriate group that was chosen during the configuration of the VPN Connection.

Step 4. In the *Cipher Algorithm* drop-down list, choose the appropriate option that was chosen during the configuration of the VPN Connection.

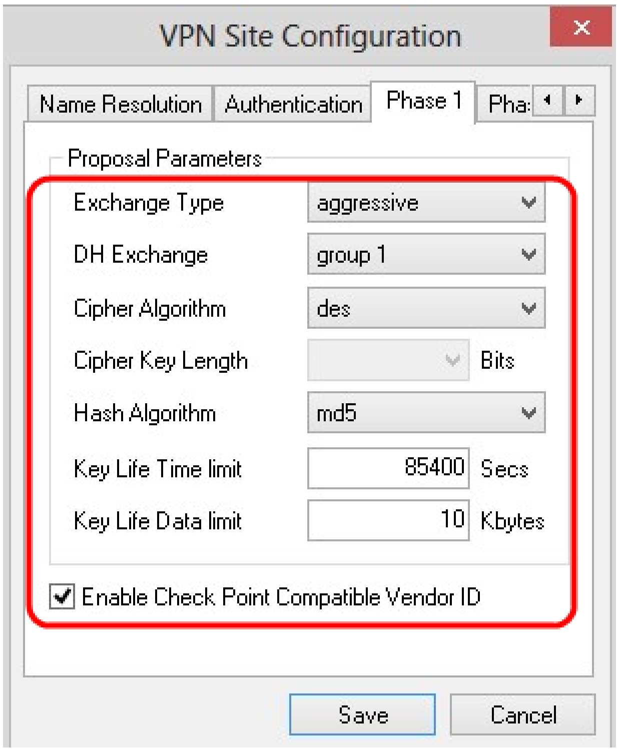
Step 5. In the *Cipher Key Length* drop-down list, choose the option that matches the key length of the option that was chosen during your configuration of the VPN Connection.

Step 6. In the *Hash Algorithm* drop-down list, choose the option that was chosen during your configuration of the VPN Connection.

Step 7. In the *Key Life Time* limit field, enter the value used during your configuration of the VPN Connection.

Step 8. In the *Key Life Data* limit field, enter the value in kilobytes to protect. The default value is 0 which turns off the feature.

Step 9. (Optional) Check the **Enable Check Point Compatible Vendor ID** check box.



Proposal Parameters

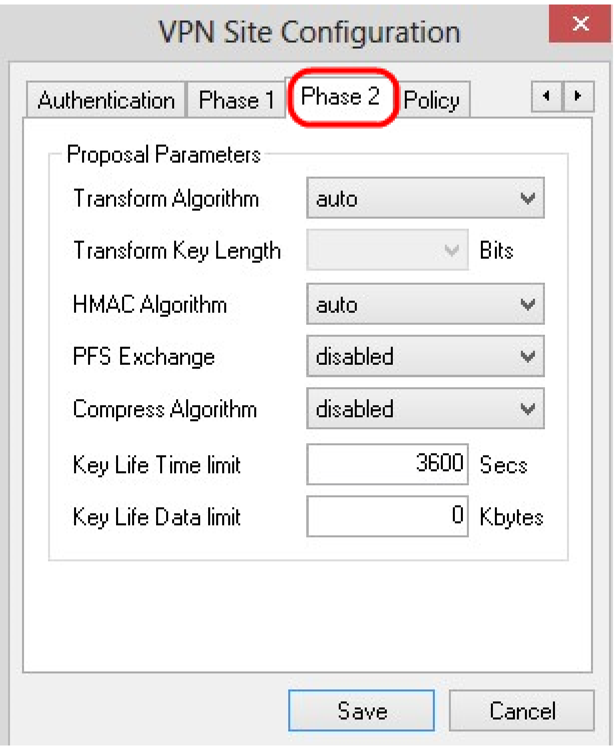
Exchange Type	aggressive	
DH Exchange	group 1	
Cipher Algorithm	des	
Cipher Key Length		Bits
Hash Algorithm	md5	
Key Life Time limit	85400	Secs
Key Life Data limit	10	Kbytes

☑ Enable Check Point Compatible Vendor ID

Step 10. Click **Save** to save the settings.

Phase 2 Configuration

Step 1. Click the **Phase 2** tab.



Proposal Parameters

Transform Algorithm	auto	
Transform Key Length		Bits
HMAC Algorithm	auto	
PFS Exchange	disabled	
Compress Algorithm	disabled	
Key Life Time limit	3600	Secs
Key Life Data limit	0	Kbytes

Note: In the *Phase 2* section, you can configure the parameters such that an IPsec SA with the remote client gateway can be established.

Step 2. In the *Transform Algorithm* drop-down list, choose the option that was chosen during the configuration of the VPN connection.

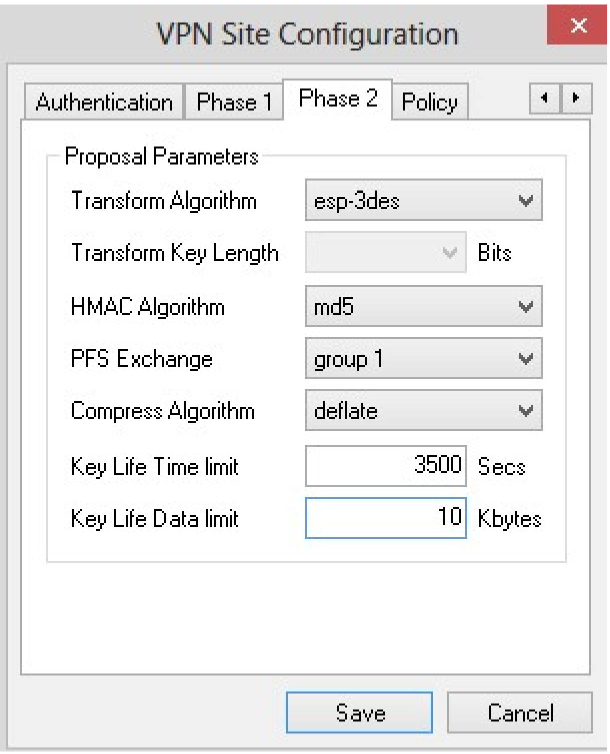
Step 3. In the *Transform Key Length* drop-down list, choose the option that matches the key length of the option that was chosen during the configuration of the VPN connection.

Step 4. In the *HMAC Algorithm* drop-down list, choose the option that was chosen during the configuration of the VPN connection.

Step 5. In the *PFS Exchange* drop-down list, choose the option that was chosen during the configuration of the VPN connection.

Step 6. In the *Key Life Time limit* field, enter the value used during the configuration of the VPN connection.

Step 7. In the *Key Life Data limit* field, enter the value in kilobytes to protect. The default value is 0 which turns off the feature.



Proposal Parameters

Transform Algorithm esp-3des

Transform Key Length Bits

HMAC Algorithm md5

PFS Exchange group 1

Compress Algorithm deflate

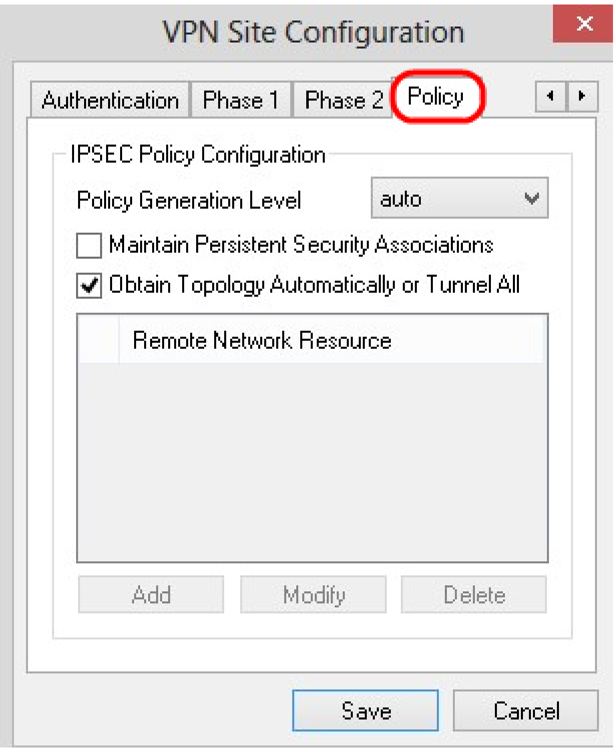
Key Life Time limit 3500 Secs

Key Life Data limit 10 Kbytes

Step 8. Click **Save** to save the settings.

Policy Configuration

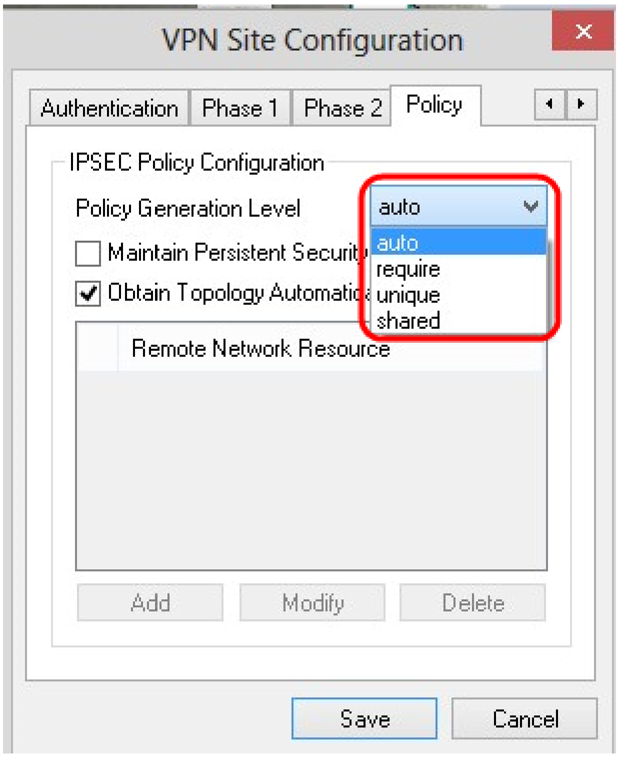
Step 1.Click the **Policy** tab.



Note: In the *Policy* section, the IPSEC Policy is defined, which is required for the client to communicate with the host for the site configuration.

Step 2. In the *Policy Generation Level* drop-down list, choose the appropriate option.

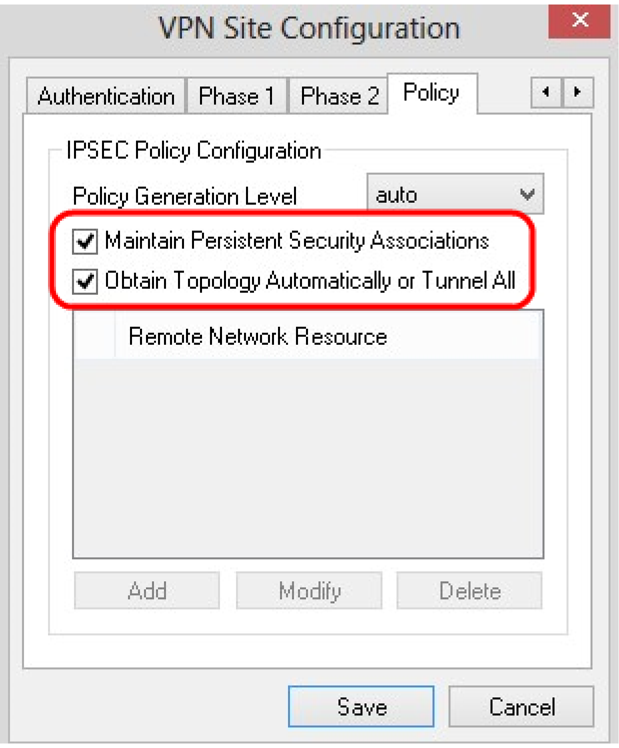
- Auto — The necessary IPsec Policy level is automatically determined.
- Require — A unique security association for each policy is not negotiated.
- Unique — A unique security association for each policy is negotiated.
- Shared — The appropriate policy is generated at the necessary level.



Step 3. (Optional) To change the IPSec negotiations, check the **Maintain Persistent**

Security Associations check box. If enabled, negotiation is made for each policy directly after connected. If disabled, negotiation is made on a need basis.

Step 4. (Optional) To receive an automatically provided list of networks from the device, or to send all packets to the RV0XX by default, check the **Obtain Topology Automatically or Tunnel All** check box. If unchecked, the configuration must be performed manually. If this is checked, skip to Step 10.

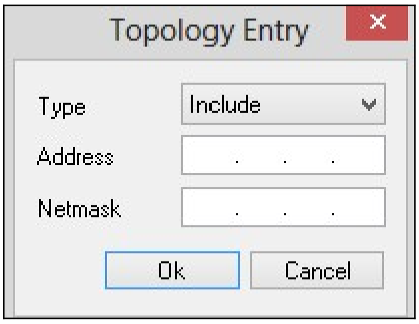


Policy Generation Level: auto

☑ Maintain Persistent Security Associations

☑ Obtain Topology Automatically or Tunnel All

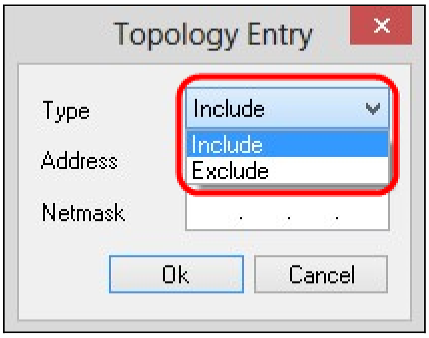
Step 5. Click **Add** to add a Topology entry into the table. The *Topology Entry* window appears.



Type: Include

Step 6. In the *Type* drop-down list, choose the appropriate option.

- Include — The network is accessed through a VPN gateway.
- Exclude — The network is accessed through local connectivity.


Topology Entry

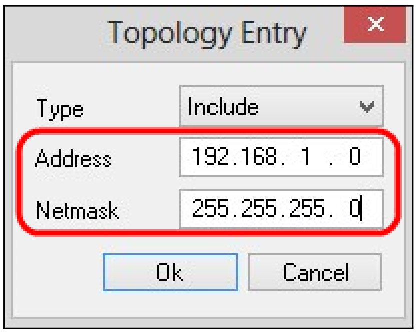
Type: Include

Address

Netmask

Step 7. In the *Address* field, enter the IP address of the RV0XX.

Step 8. In the *Netmask* field, enter the subnet mask address of the device.

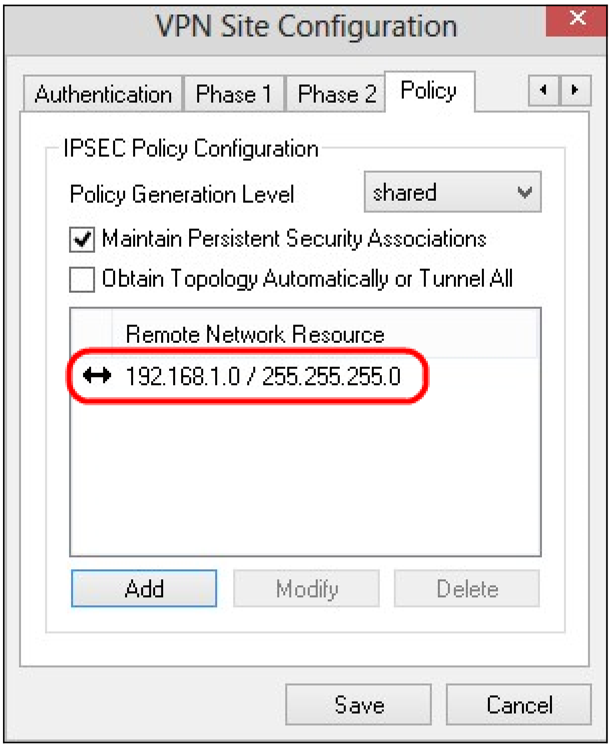

Topology Entry

Type: Include

Address: 192.168.1.0

Netmask: 255.255.255.0

Step 9. Click **OK**. The IP address and the subnet mask address of the RV0XX are displayed in the Remote Network Resource list.


VPN Site Configuration

IPSEC Policy Configuration

Policy Generation Level: shared

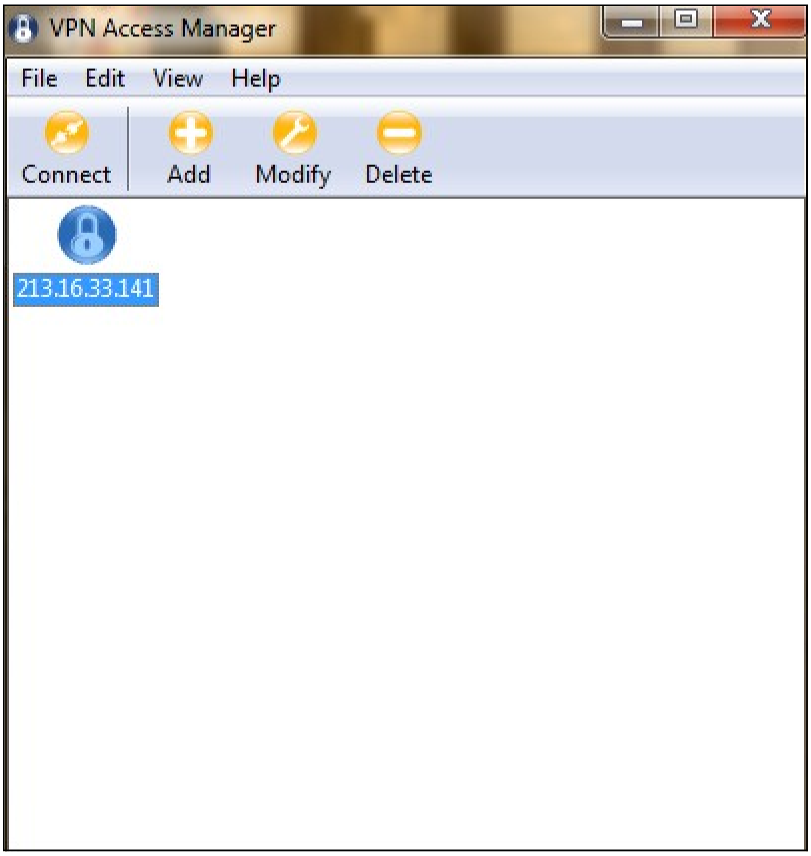
☑ Maintain Persistent Security Associations

□ Obtain Topology Automatically or Tunnel All

Remote Network Resource

↔ 192.168.1.0 / 255.255.255.0

Step 10. Click **Save**, which returns the user to the *VPN Access Manager* window where the new VPN connection is displayed.

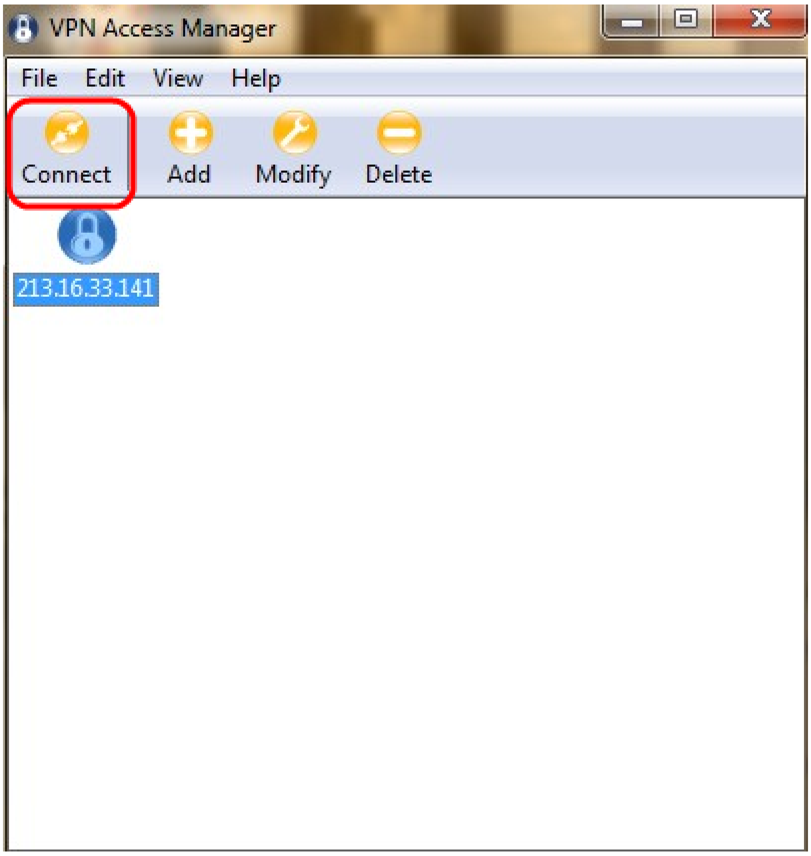


Connect

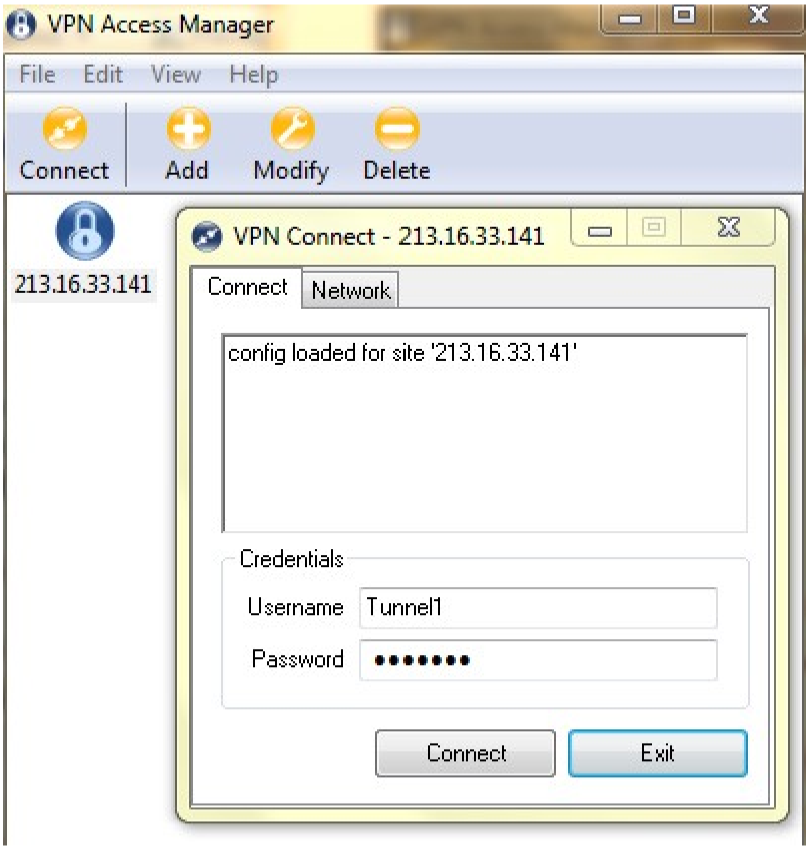
This section explains how to setup the VPN connection after all the settings are configured. The required log in information is the same as the VPN Client Access configured on the device.

Step 1. Click the desired VPN connection.

Step 2. Click **Connect.**



The *VPN Connect* window appears:



```
config loaded for site '213.16.33.141'
```

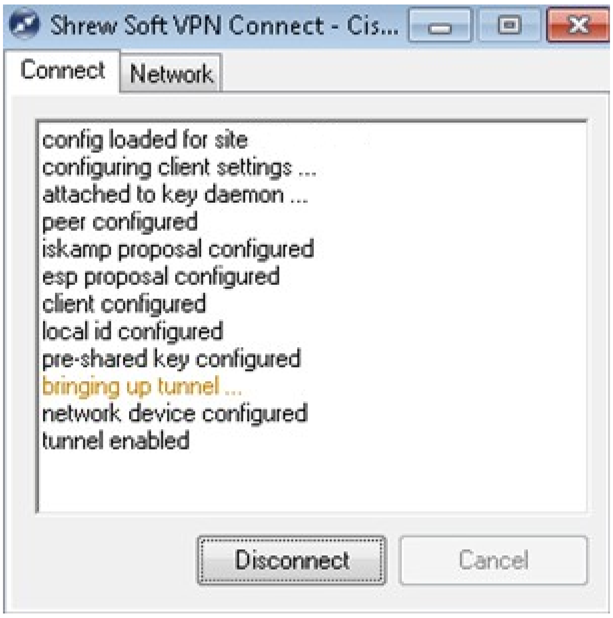
Username: Tunnel1

Password: •••••••

Step 3. Enter the username for the VPN in the *Username* field.

Step 4. Enter the password for the VPN user account in the *Password* field.

Step 5. Click **Connect**. The *Shrew Soft VPN Connect* window appears:



```
config loaded for site
configuring client settings ...
attached to key daemon ...
peer configured
iskamp proposal configured
esp proposal configured
client configured
local id configured
pre-shared key configured
bringing up tunnel ...
network device configured
tunnel enabled
```

Step 6. (Optional) To disable the connection, click **Disconnect**.