Use Shrew Soft VPN Client to Connect with IPSec VPN Server on RV130 and RV130W

Objective

IPSec VPN (Virtual Private Network) enables you to securely obtain remote resources by establishing an encrypted tunnel across the Internet.

The RV130 and RV130W work as IPSec VPN servers, and support the Shrew Soft VPN client.

Make sure to download the latest release of the client software.

- Shrew Soft (https://www.shrew.net/download/vpn)

Note: To be able to successfully setup and configure the Shrew Soft VPN client with an IPSec VPN server, you need to first configure the IPSec VPN server. For information about how to do this, refer to the article *Configuration of an IPSec VPN Server on RV130 and RV130W.*

The objective of this document is to show you how to use the Shrew Soft VPN client to connect with an IPSec VPN Server on the RV130 and RV130W.
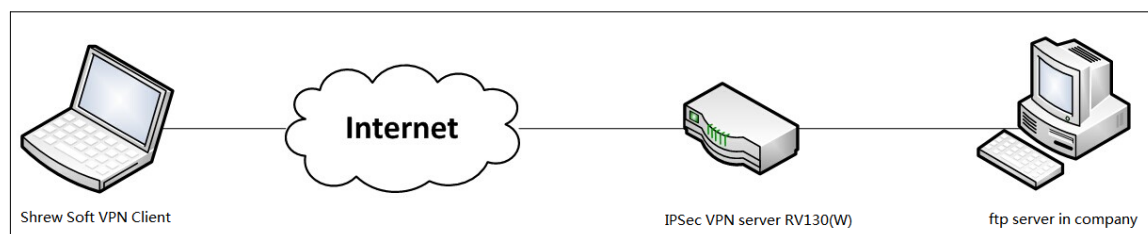
Applicable Devices

- RV130W Wireless-N VPN Firewall

- RV130 VPN Firewall

System Requirements

- 32 or 64-bit systems

- Windows 2000, XP, Vista or Windows 7/8

Topology

A top level topology is shown below illustrating the devices involved in a Shrewsoft client to site configuration.

A more detailed flowchart illustrating the role of DNS servers in a small business network environment is shown below.

Home Office

Main Office

Public Network

Router

VPN Gateway

Home DNS
Server

Remote DNS
Server
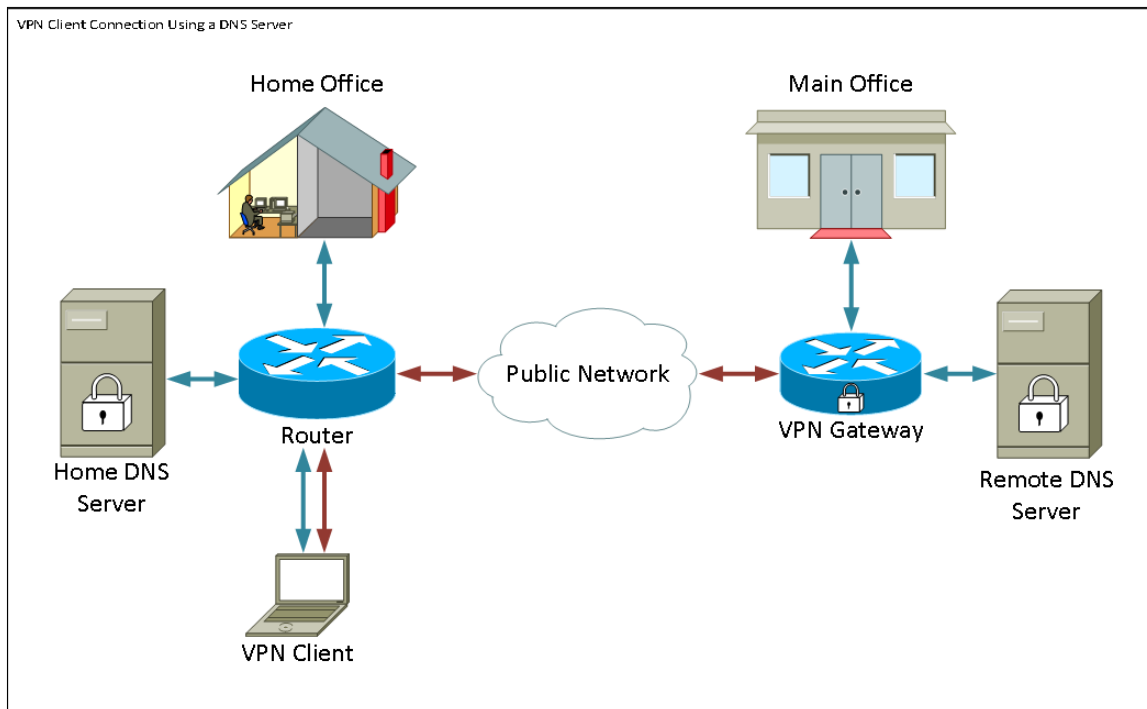
VPN Client

Software Version

- 1.0.1.3

Setup Shrew Soft VPN Client

IPSec VPN Setup and User Configuration

Step 1. Log in to the web configuration utility and choose **VPN > IPSec VPN Server > Setup**. The *Setup* page opens.

Step 2. Verify that the IPSec VPN Server for the RV130 is properly configured. If the IPSec VPN Server is not configured or misconfigured, refer to *Configuration of an IPSec VPN Server on RV130 and RV130W* and click **Save**.

Setup

✅ Configuration settings have been saved successfully

Server Enable:	☑	
NAT Traversal:	Disabled	[Edit]

Phase 1 Configuration

Pre-Shared Key:	Testkey
Exchange Mode:	Main ▼
Encryption Algorithm:	DES ▼
Authentication Algorithm:	MD5 ▼
DH Group:	Group1 (768 bit) ▼
IKE SA Life Time:	3600 Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:	Subnet ▼
IP Address:	192.168.1.0 (Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES ▼
Authentication Algorithm:	MD5 ▼
PFS Key Group:	☑ Enable
DH Group:	Group 1(768 bit) ▼

[Save] [Cancel]

Note: The above settings are an example of an RV130/RV130W IPSec VPN Server configuration. The settings are based on the document, *Configuration of an IPSec VPN Server on RV130 and RV130W,* and will be referred to in subsequent steps.
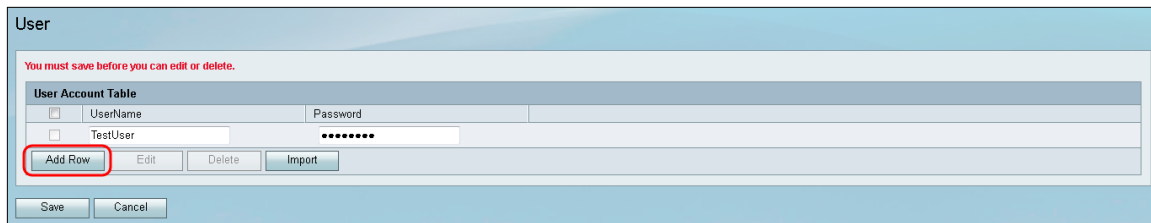
Step 3. Navigate to **VPN > IPSec VPN Server > User**. The *User* page appears.

User

User Account Table

☐	UserName	Password	
☐	No data to display		

[Add Row] [Edit] [Delete] [Import]
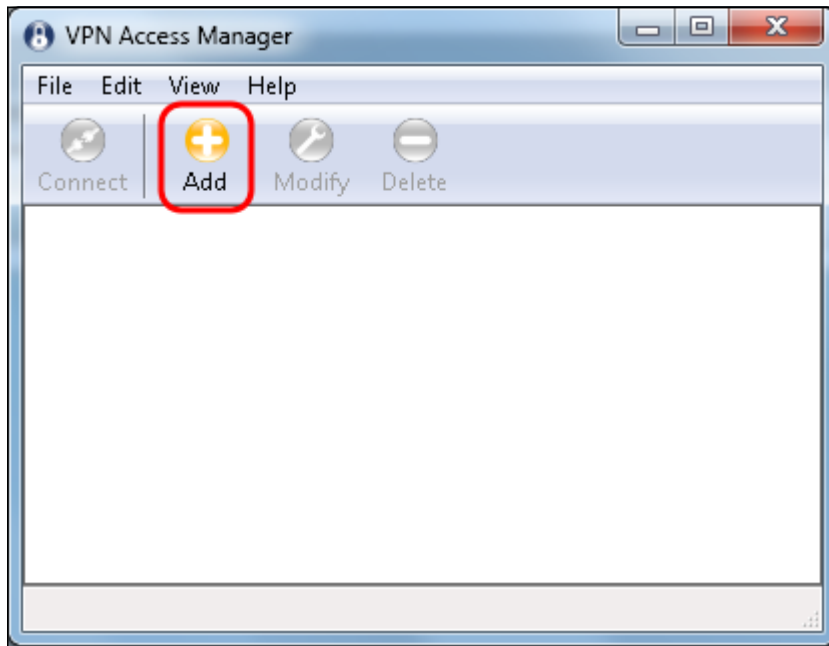
[Save] [Cancel]

Step 4. Click **Add Row** to add user accounts, used to authenticate the VPN clients (Extended Authentication), and enter the desired Username and Password in the fields provided.
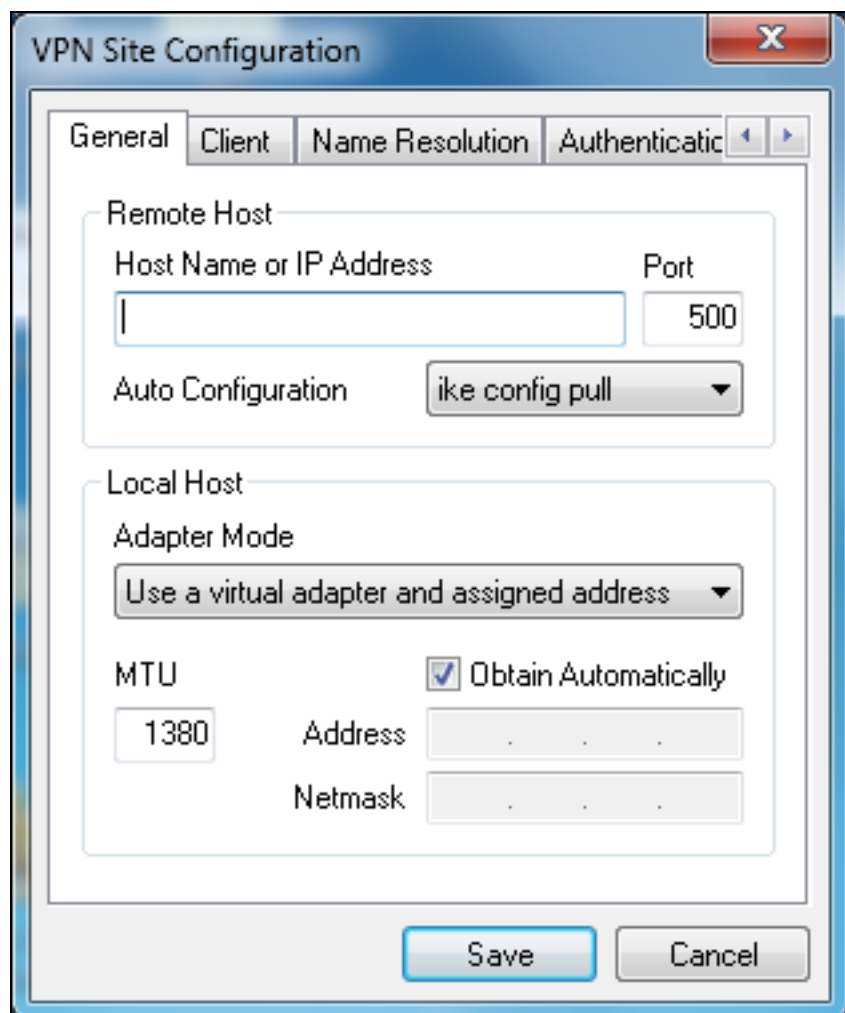
Step 5. Click **Save** to save the settings.
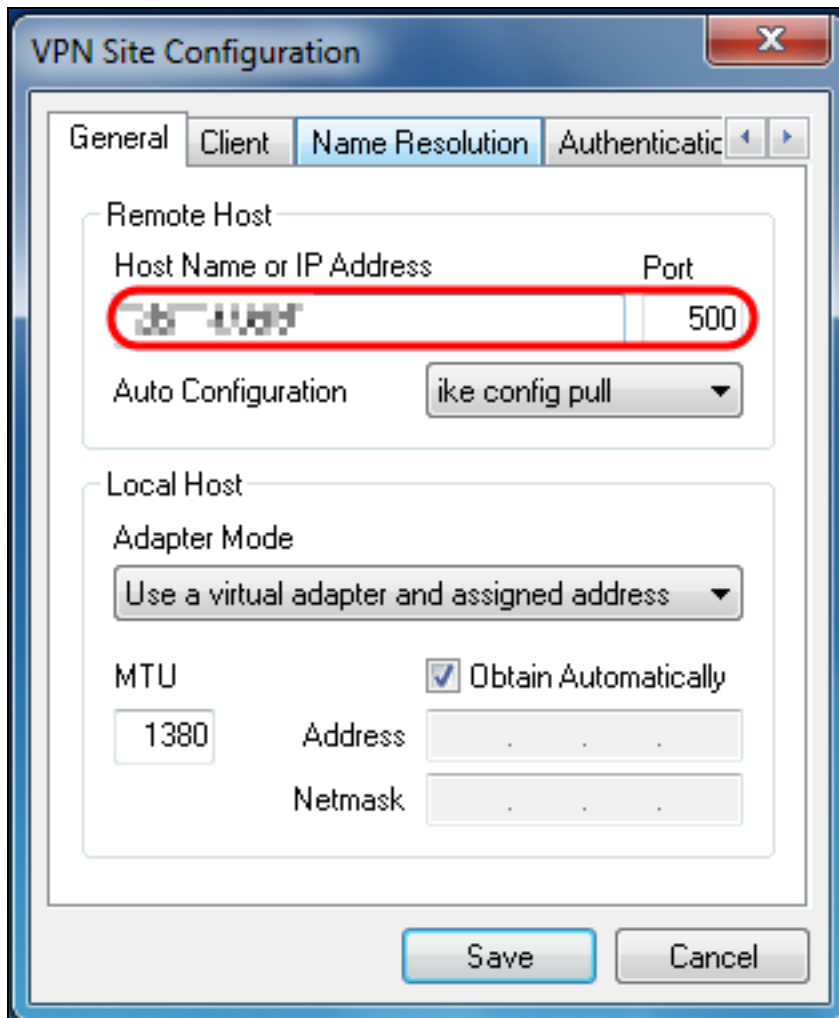
VPN Client Configuration

Step 1. Open Shrew VPN Access Manager and click **Add** to add a profile.


The *VPN Site Configuration* window appears.

Step 2. In the *Remote Host* section under the *General* tab, enter the public Host Name or IP Address of the network you are trying to connect to.

Note: Ensure that the Port number is set to the default value of 500. For the VPN to work, the tunnel uses UDP port 500 which should be set to allow ISAKMP traffic to be forwarded at the firewall.

Step 3. In the *Auto Configuration* drop-down list, choose **disabled**.
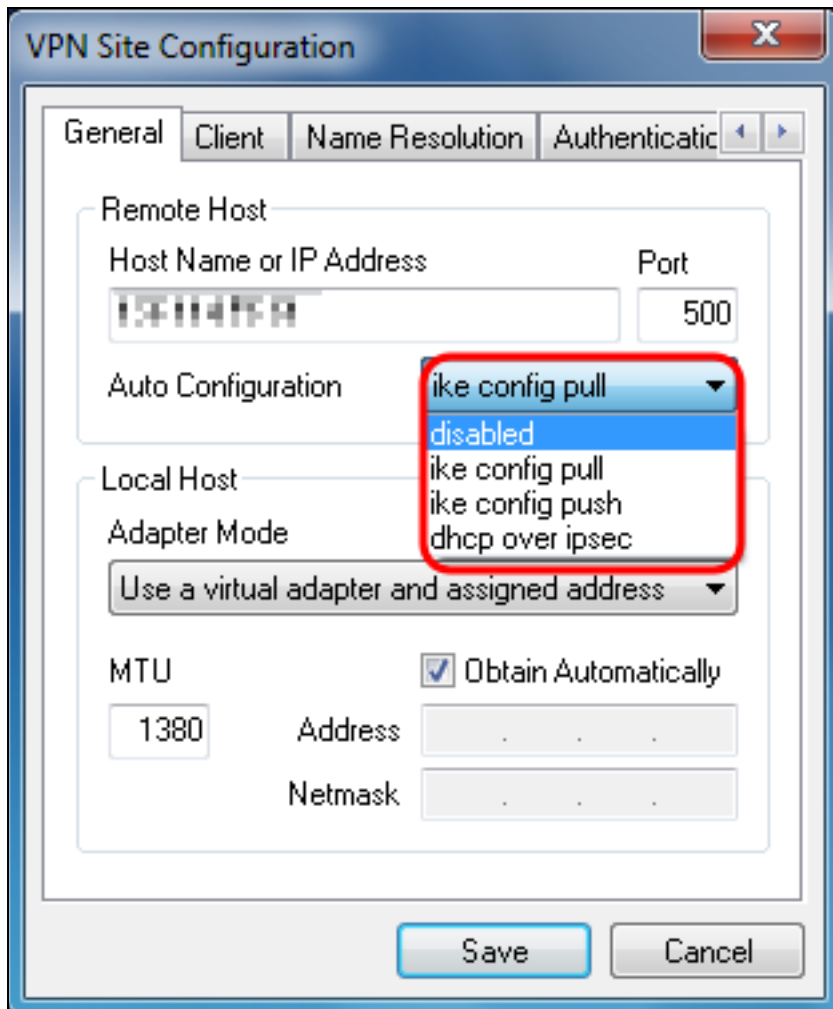
The available options are defined as follows:

• Disabled — 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.

Step 4. In the *Local Host* section, choose **Use an existing adapter and current address** in the *Adapter Mode* drop-down list.
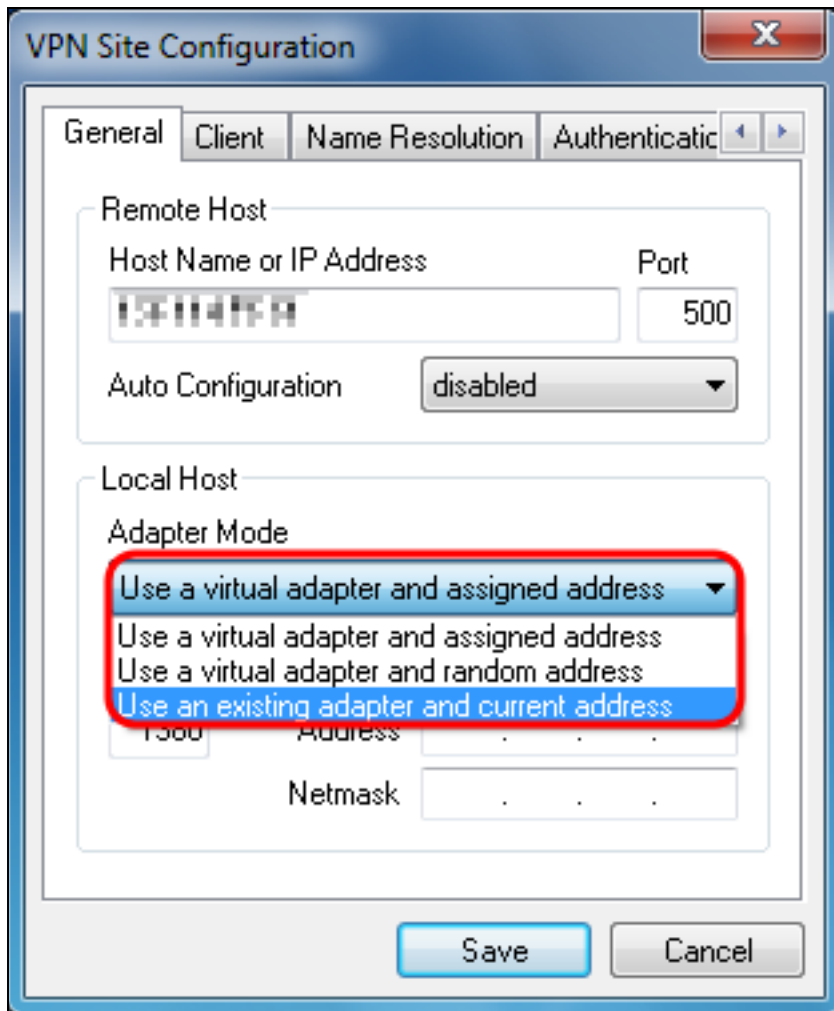
The available options are defined as follows:

• Use a virtual adapter and assigned address — Allows the client to use a virtual adapter with a specified address as the source for its IPsec communications.

• Use a virtual adapter and random address — Allows the client to use a virtual adapter with a random address as the source for its IPsec communications.

• Use an existing adapter and current address — Allows the client to only use its existing, physical adapter with its current address as the source for its IPsec communications.

Step 5. Click on the *Client* tab. In the *NAT Traversal* drop-down list, select the same setting you configured on the RV130/RV130W for NAT Traversal in the article *Configuration of an IPSec VPN Server on RV130 and RV130W.*
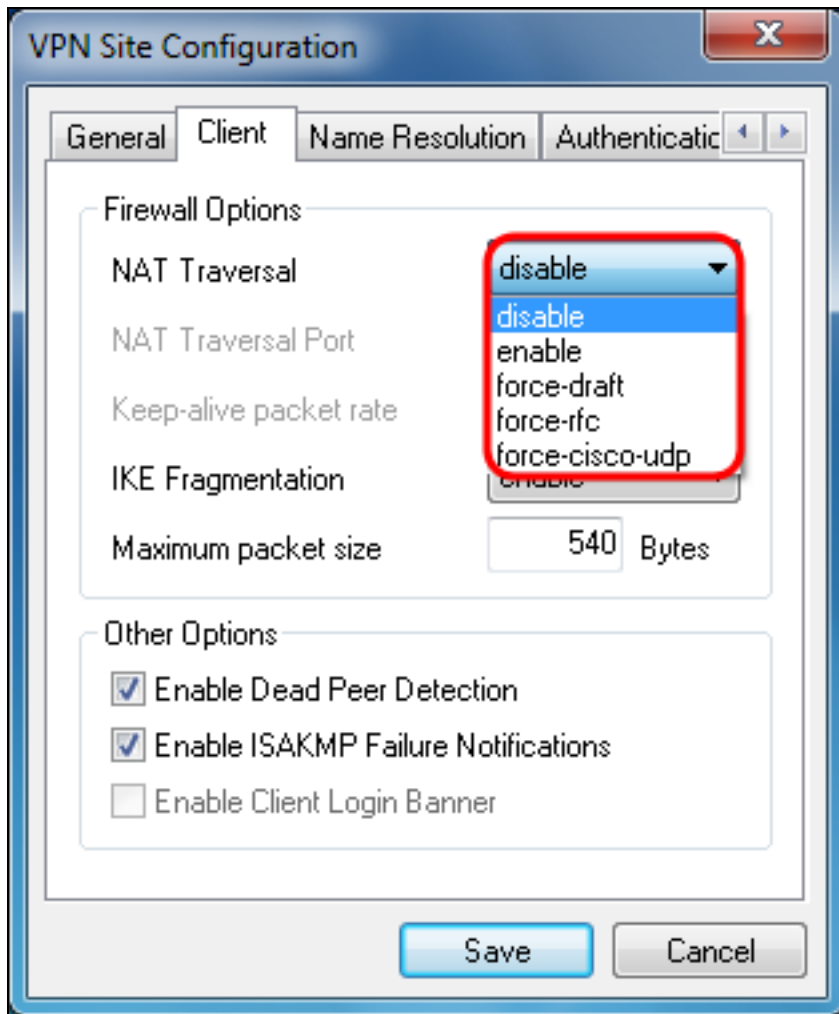
The available Network Address Translation Traversal (NATT) menu options are defined as follows:

• Disable — The NATT protocol extensions will not be used.

• Enable — The NATT protocol extensions will only be used if the VPN Gateway indicates support during negotiations and NAT is detected.

• Force-Draft — The Draft version of the NATT protocol extensions will be used regardless of whether or not the VPN Gateway indicates support during negotiations or NAT is detected.

• Force-RFC — The RFC version of the NATT protocol will be used regardless of whether or not the VPN Gateway indicates support during negotiations or NAT is detected.

• Force-Cisco-UDP — Force UDP encapsulation for VPN clients without NAT.

Step 6. Click on the *Name Resolution* tab, and check the **Enable DNS** check box if you want to enable DNS. If specific DNS settings are not required for your site configuration, uncheck the **Enable DNS** check box.
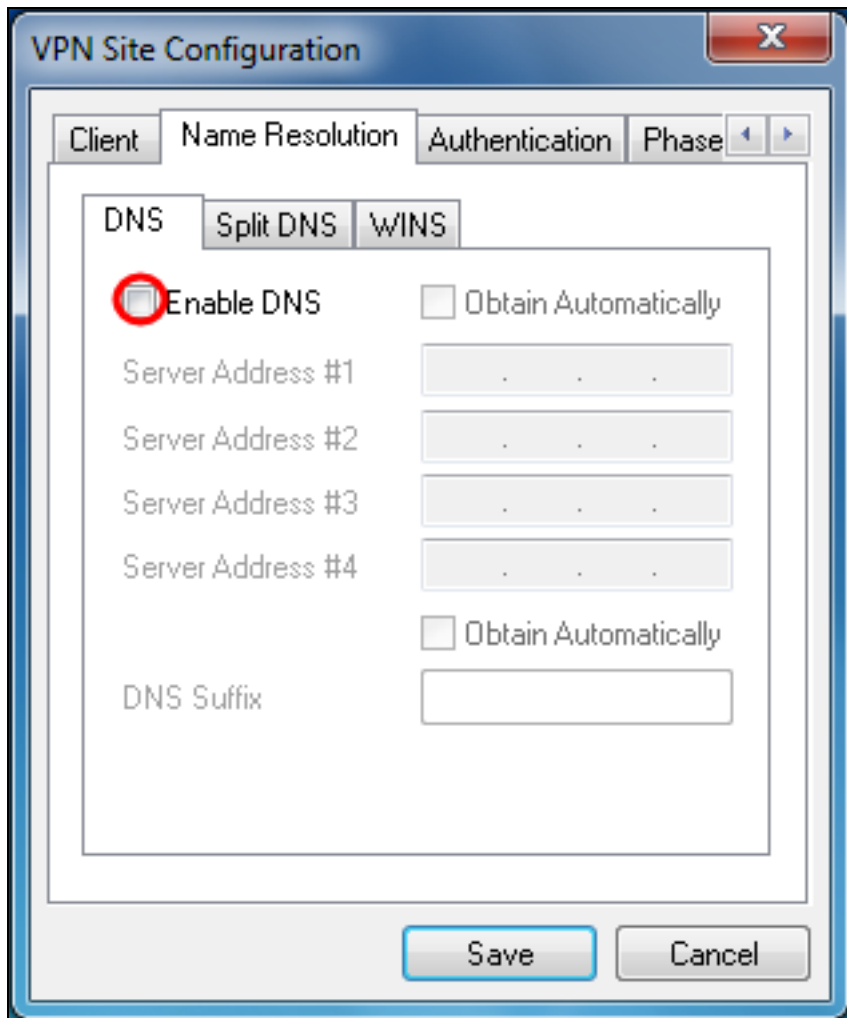
Step 7. (Optional) If your remote gateway is configured to support the Configuration Exchange, the gateway is able to provide DNS settings automatically. If not, verify that the **Obtain Automatically** check box is unchecked and manually enter a valid DNS Server Address.
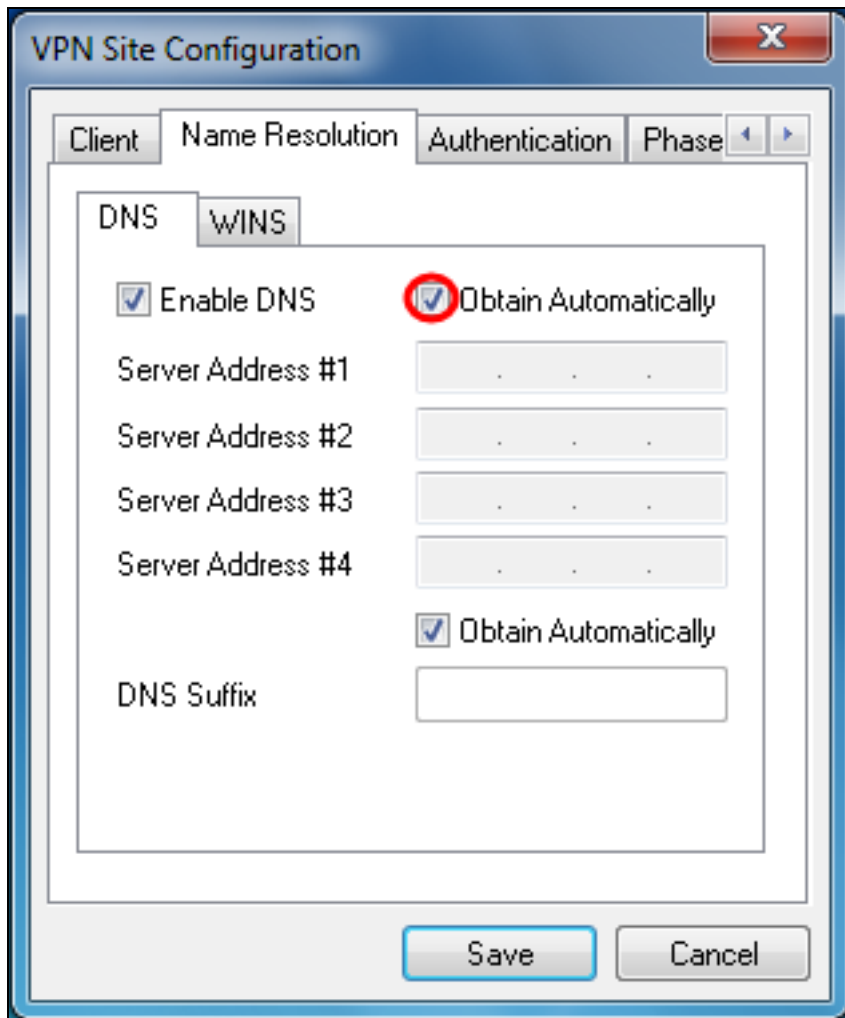
Step 8. (Optional) Click on the *Name Resolution* tab, check the **Enable WINS** check box if you want to enable the Windows Internet Name Server (WINS). If your remote gateway is configured to support the Configuration Exchange, the gateway is able to provide WINS settings automatically. If not, verify that the **Obtain Automatically** check box is unchecked and manually enter a valid WINS Server Address.
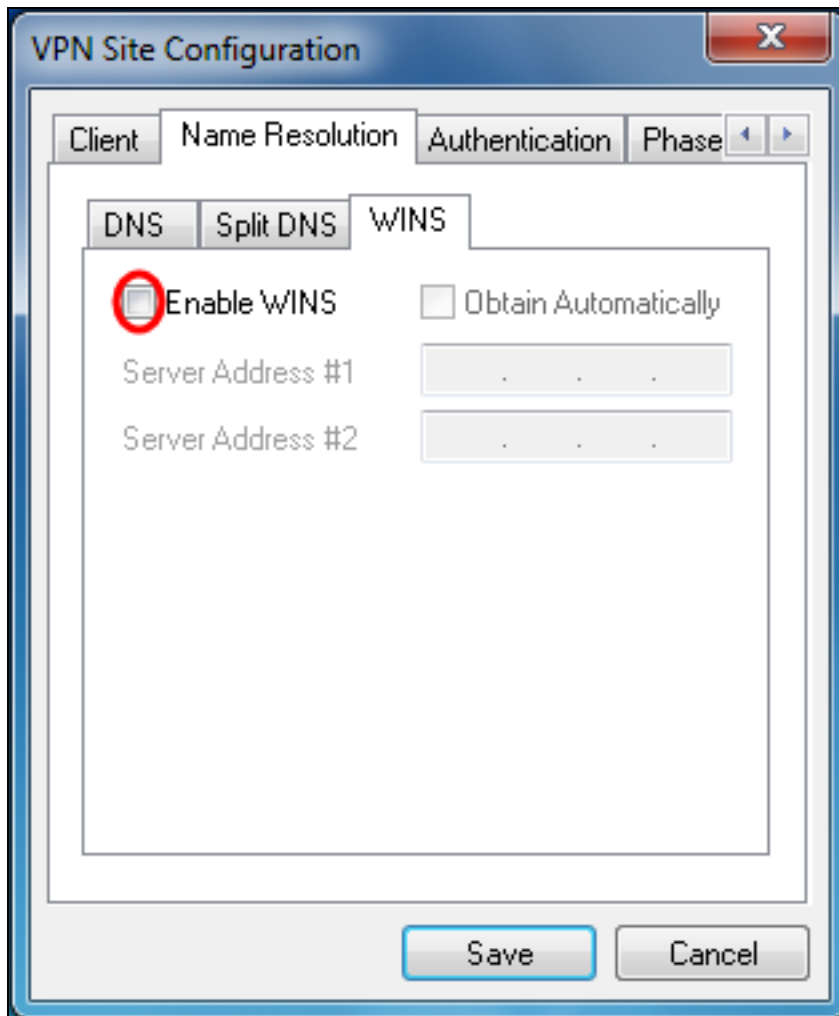
Note: By providing WINS configuration information, a client will be able to resolve WINS names using a server located in the remote private network. This is useful when attempting to access remote windows network resources using a Uniform Naming Convention path name. The WINS server would typically belong to a Windows Domain Controller or a Samba Server.

Step 9. Click on the *Authentication* tab, and select **Mutual PSK + XAuth** in the *Authentication Method* drop-down list.
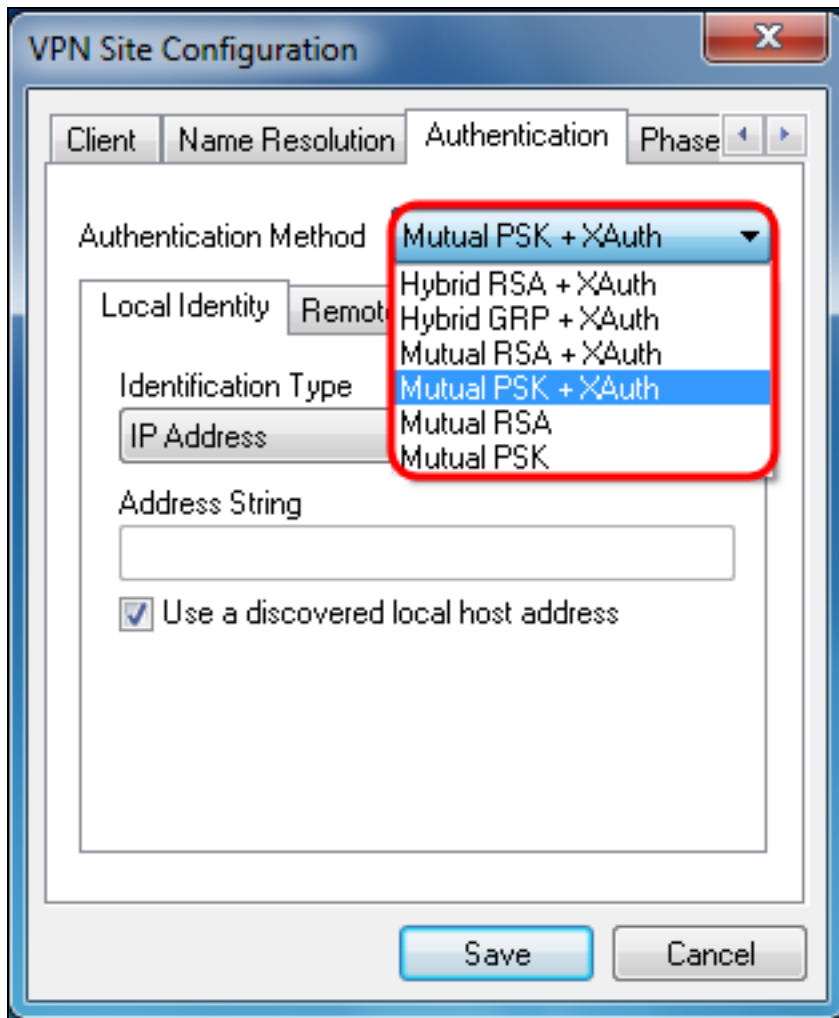
The available options are defined as follows:

• 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.

Step 10. In the *Authentication* section, click on the *Credentials* sub-tab and enter the same pre-shared key you configured on the *IPsec VPN Server Setup* page in the *Pre Shared Key* field.
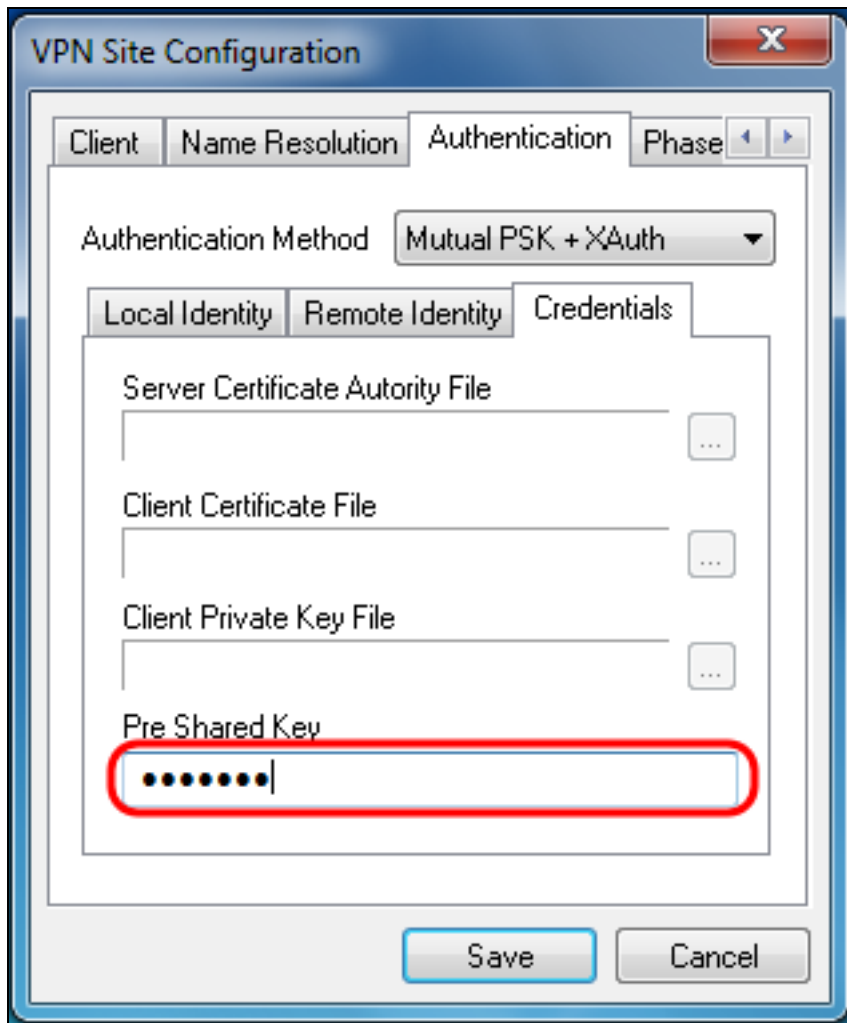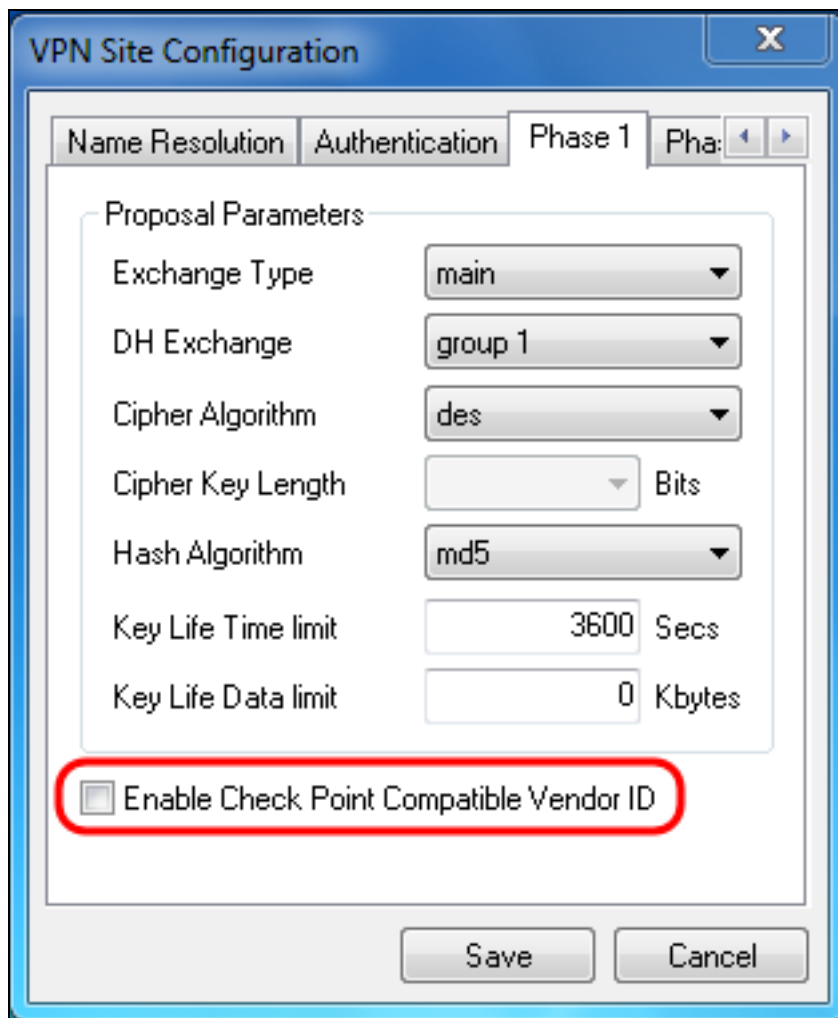
Step 11. Click on the *Phase 1* tab. Configure the following parameters to have the same settings that you configured for the RV130/RV130W in Step 2 of the *IPSec VPN Server User Configuration* section of this document.
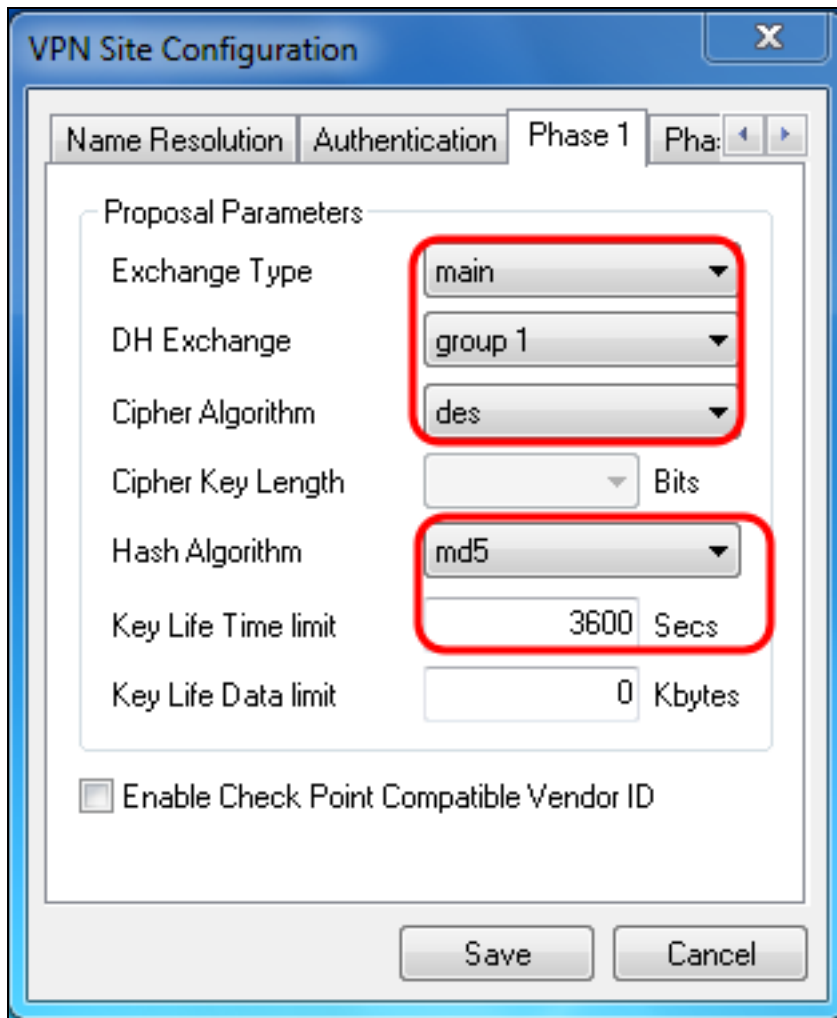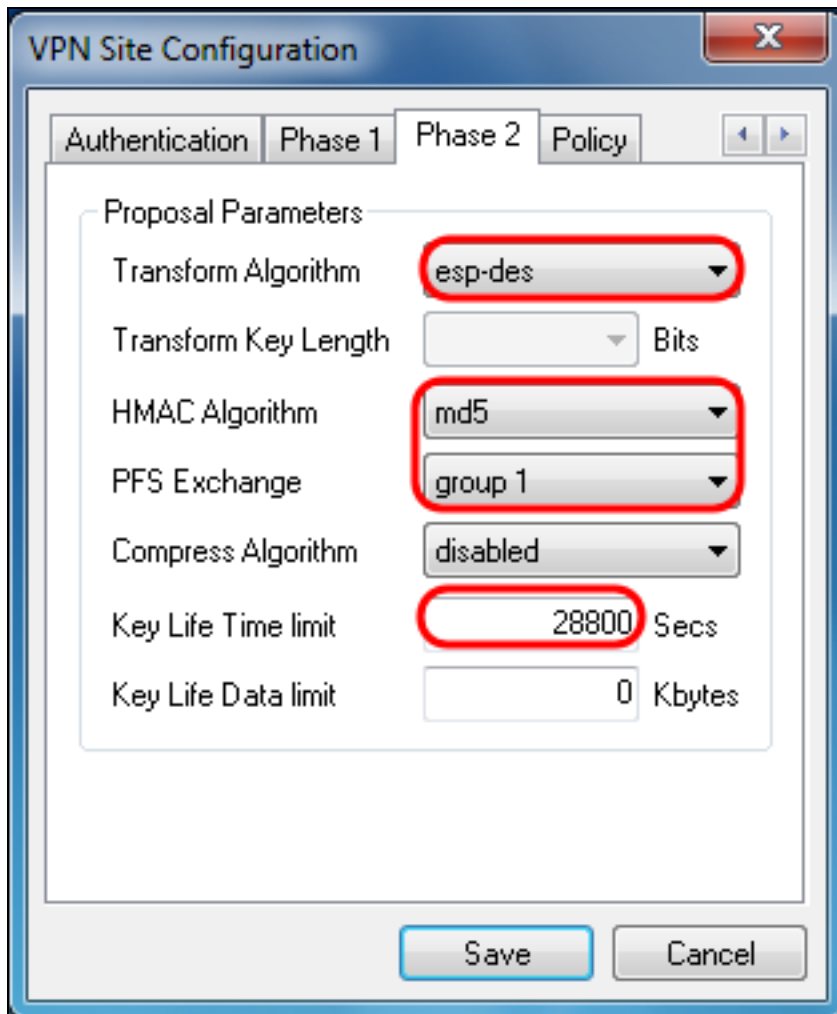
The parameters in Shrew Soft should match the RV130/RV130W configurations in Phase 1 as follows:

- "Exchange Type" should match "Exchange Mode".

- "DH Exchange" should match "DH Group".

- "Cipher Algorithm" should match "Encryption Algorithm".

- "Hash Algorithm" should match "Authentication Algorithm".

Step 12. (Optional) If your gateway offers a Cisco compatible vendor ID during phase1 negotiations, check the **Enable Check Point Compatible Vendor ID** check box. If the gateway does not, or you are unsure, leave the check box unchecked.

Step 13. Click on the *Phase 2* tab. Configure the following parameters to have the same settings that you configured for the RV130/RV130W in Step 2 of the *IPSec VPN Server User Configuration* section of this document.

The parameters in Shrew Soft should match the RV130/RV130W configurations in Phase 2 as follows:

- "Transform Algorithm" should match "Encryption Algorithm".

- "HMAC Algorithm" should match "Authentication Algorithm".

- PFS Exchange" should match "DH Group" if PFS Key Group is enabled on the RV130/RV130W. Otherwise, select **disabled**.

- "Key Life Time limit" should match "IPSec SA Lifetime".

Step 14. Click on the *Policy* tab and select **require** in the *Policy Generation Level* drop-down list. The *Policy Generation Level* option modifies the level in which IPsec Policies are generated. The different levels provided in the drop-down list map to IPSec SA negotiation behaviors implemented by different vendor implementations.
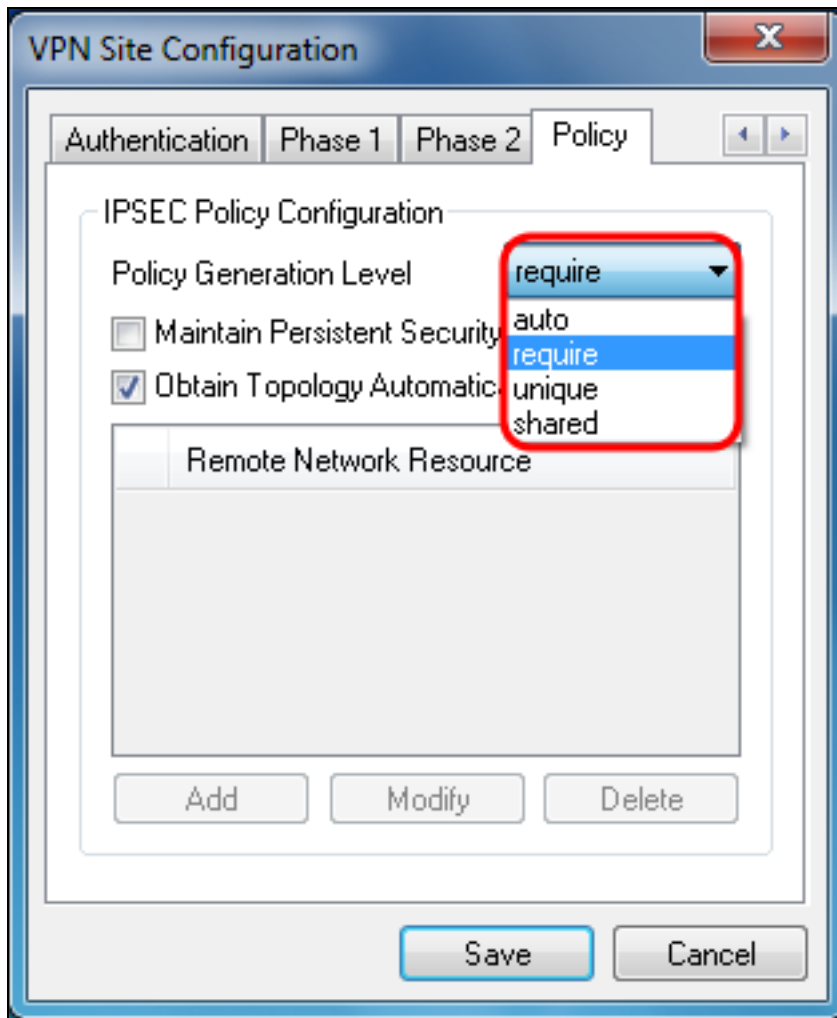
The available options are defined as follows:

 • Auto — The client will automatically determine the appropriate IPSec Policy Level.

 • Require — The client will not negotiate a unique Security Association (SA) for each policy. Policies are generated using the local public address as the local policy ID and the Remote Network Resources as the remote policy ID. The phase2 proposal will use the policy IDs during negotiation.

 • Unique — The client will negotiate a unique SA for each policy.

 • Shared – Policies are generated at the require level. The phase 2 proposal will use the local policy ID as the local ID and Any (0.0.0.0/0) as the remote ID during negotiation.

Step 15. Uncheck the **Obtain Topology Automatically or Tunnel All** check box. This option modifies the way security policies are configured for the connection. When disabled, Manual configuration must be performed. When enabled, Automatic configuration is performed.
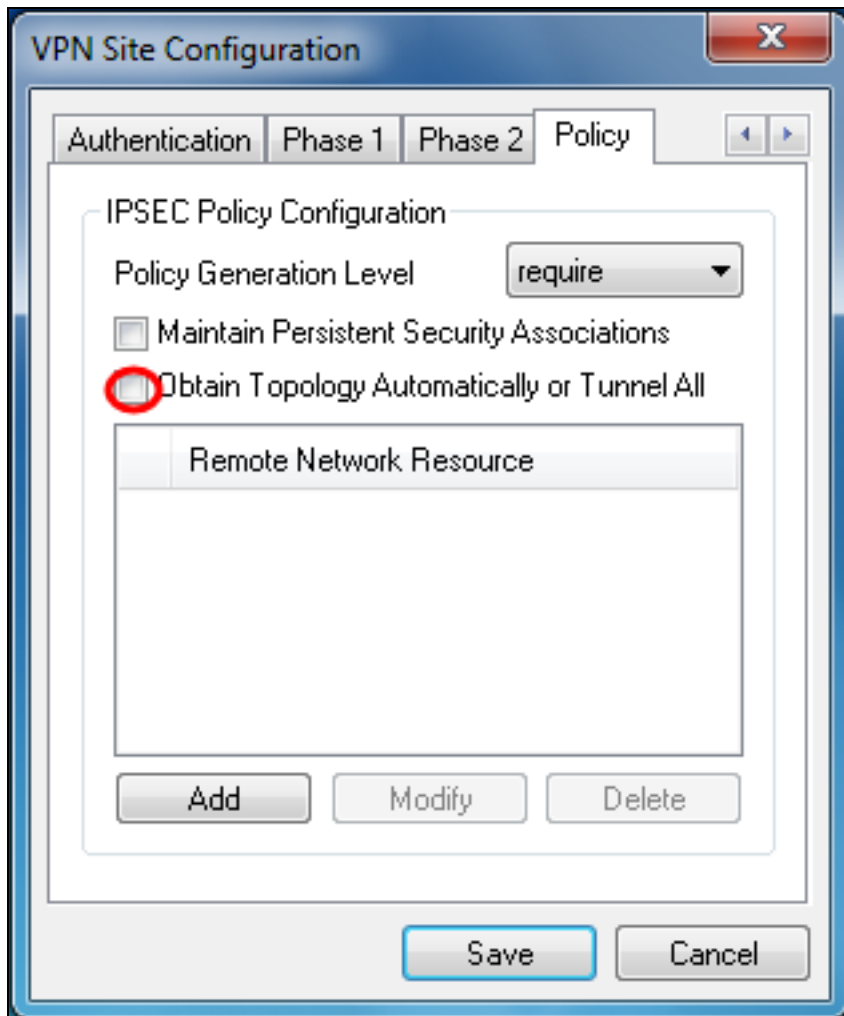
Step 16. Click **Add** in order to add the Remote Network Resource you want to connect to. Remote network resources include remote desktop access, departmental resources, network drives, and secured electronic mail.
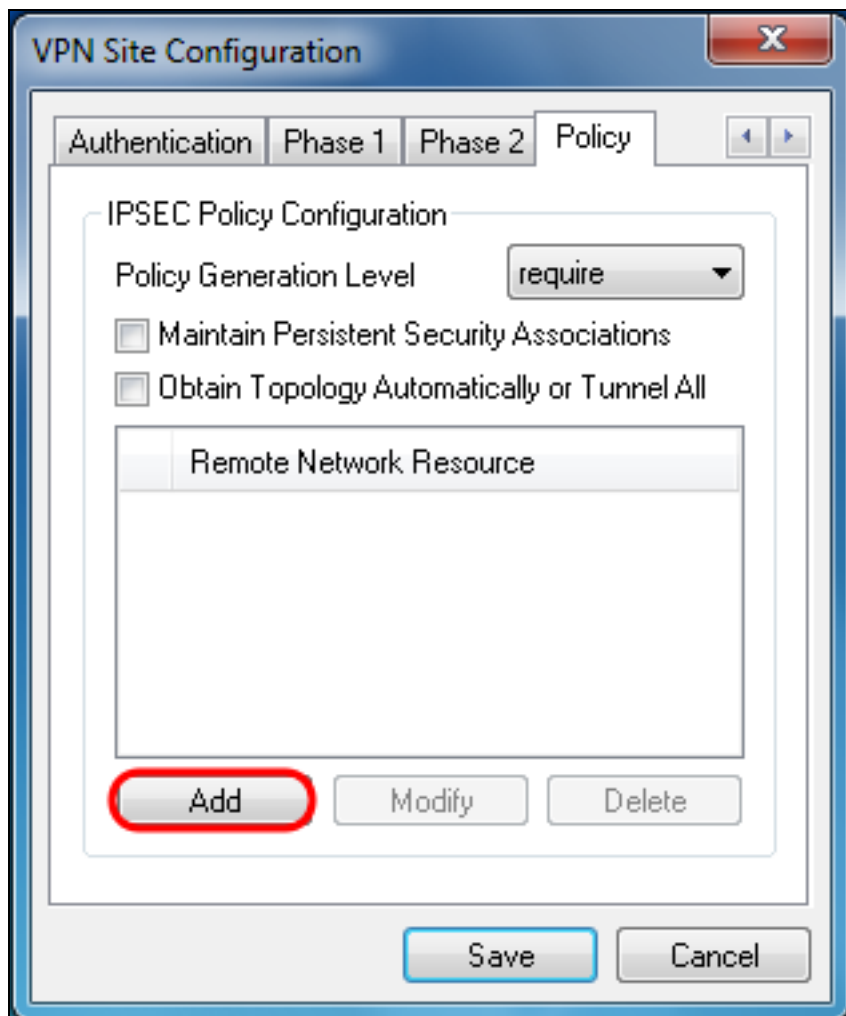
The *Topology Entry* window appears:
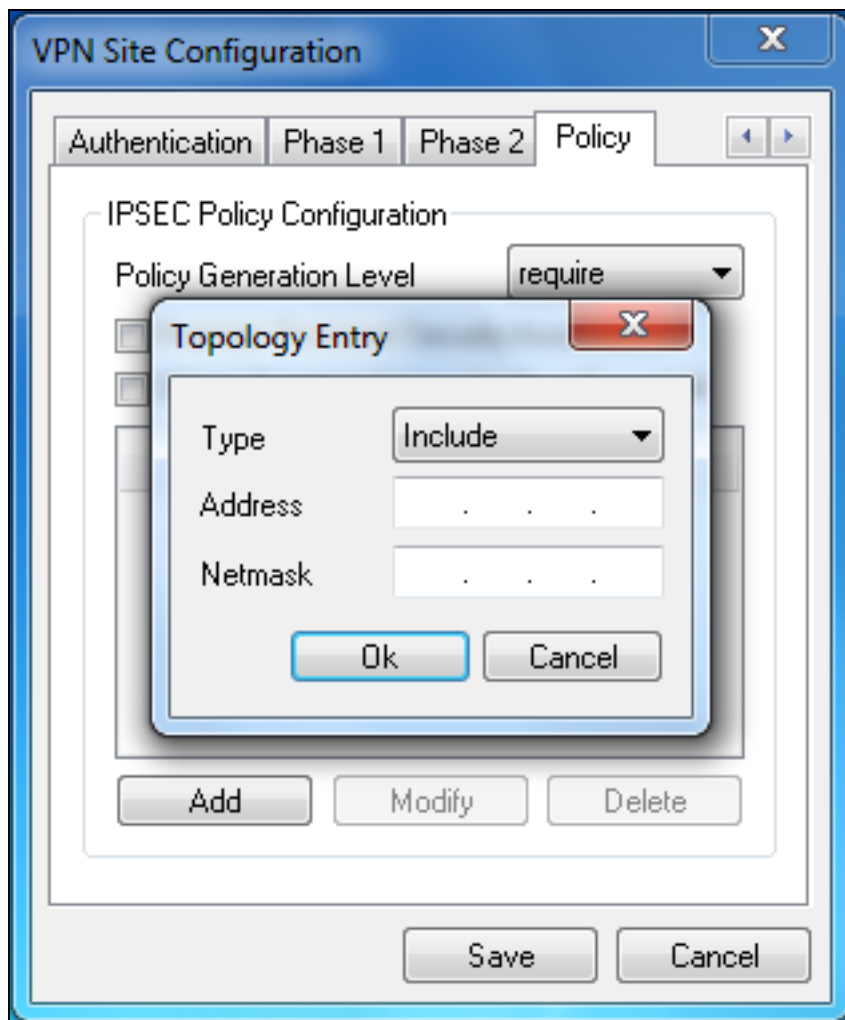
Step 17. In the *Address* field, enter the subnet ID of the RV130/RV130W. The address should match the *IP Address* field in Step 2 of the *IPSec VPN Server Setup and User Configuration* section of this document.
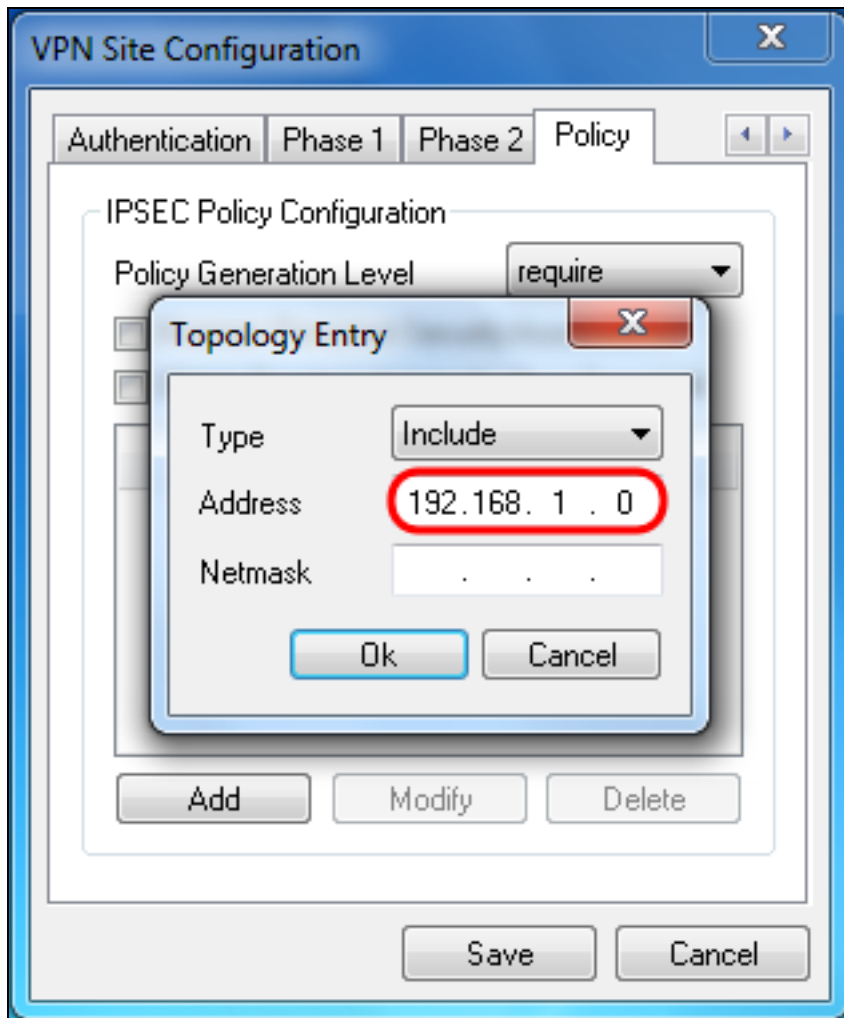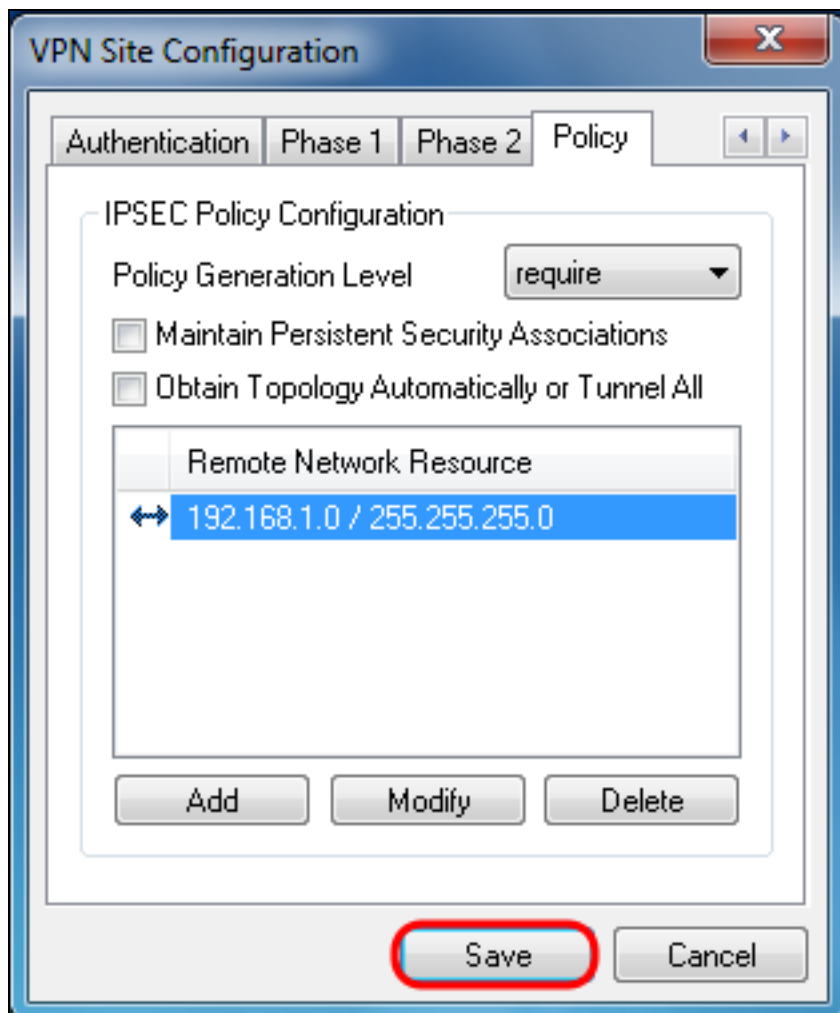
Step 18. In the *Netmask* field, enter the subnet mask for the RV130/RV130W's local network. The netmask should match the *Subnet Mask* field in Step 2 of the *IPSec VPN Server User Configuration* section of this document.
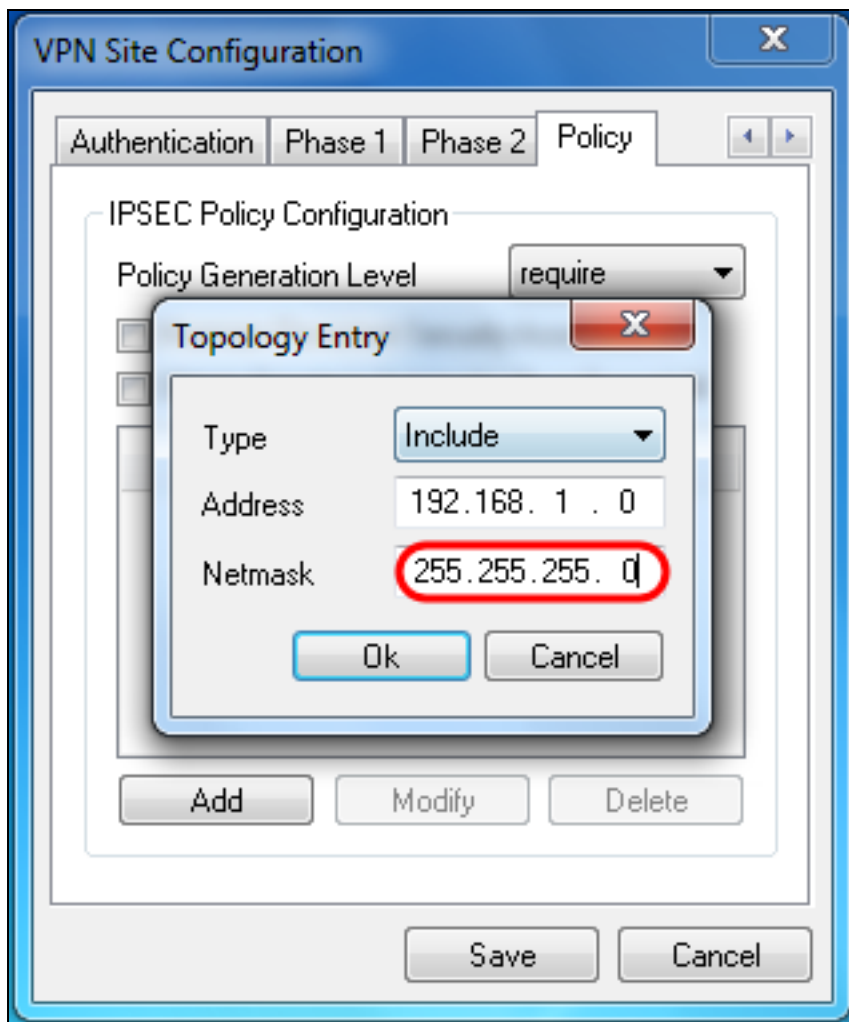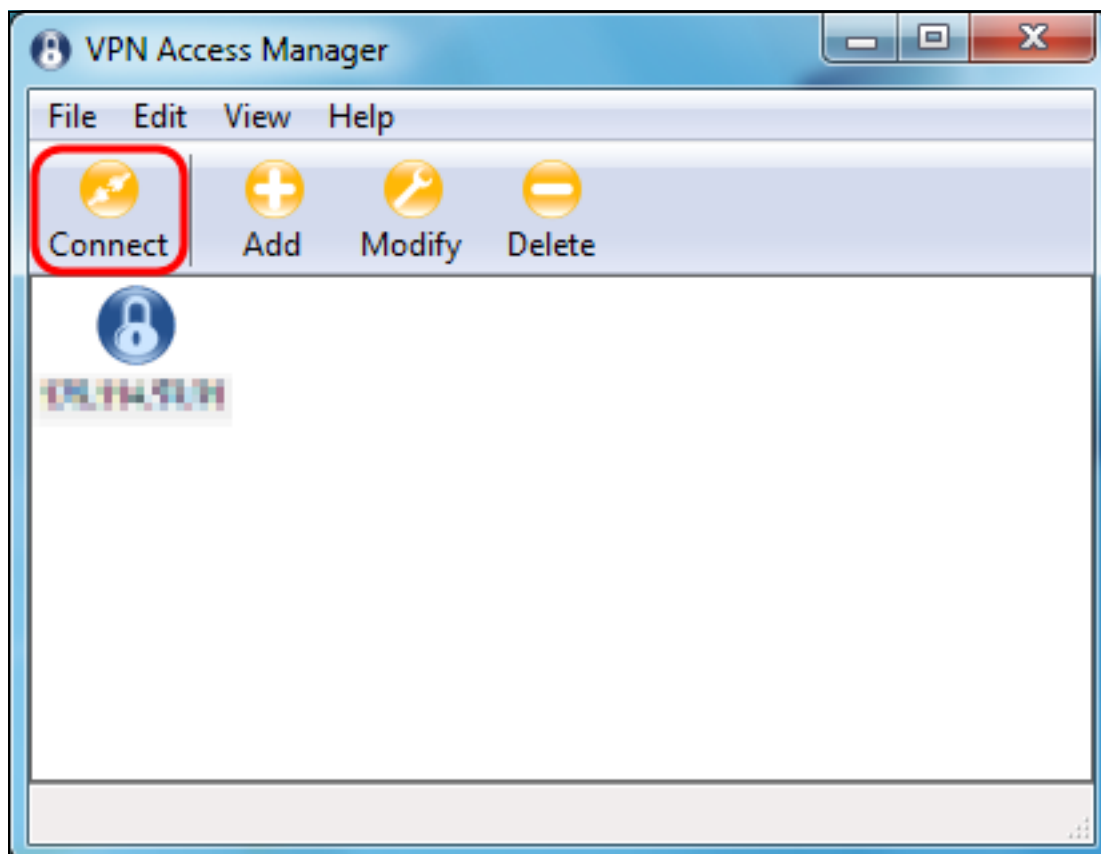
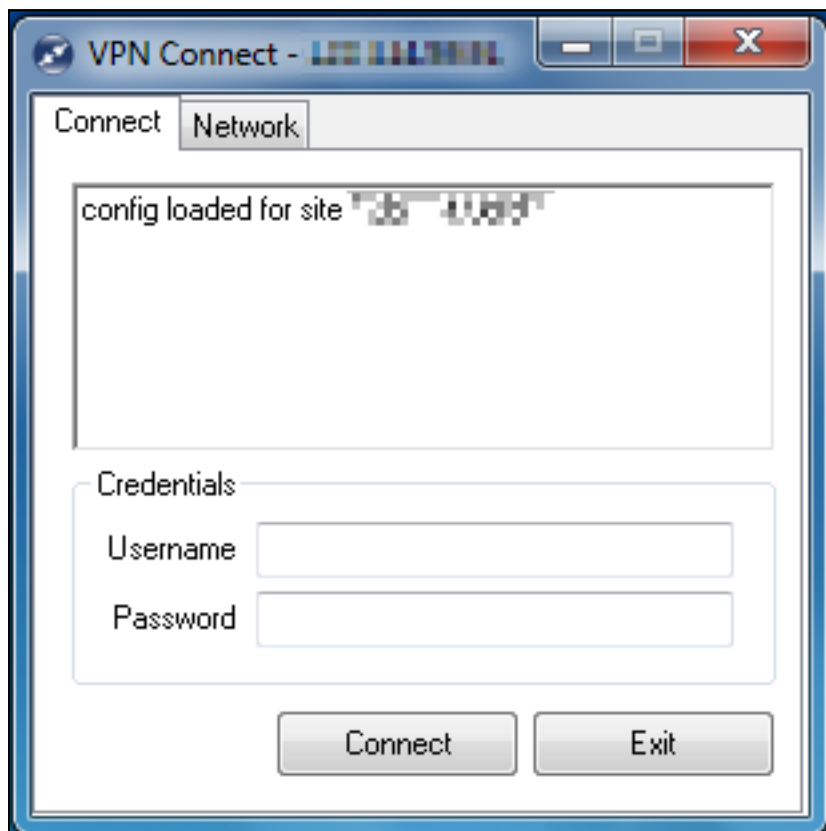Step 19. Click **Ok** to finish adding the Remote Network Resource.
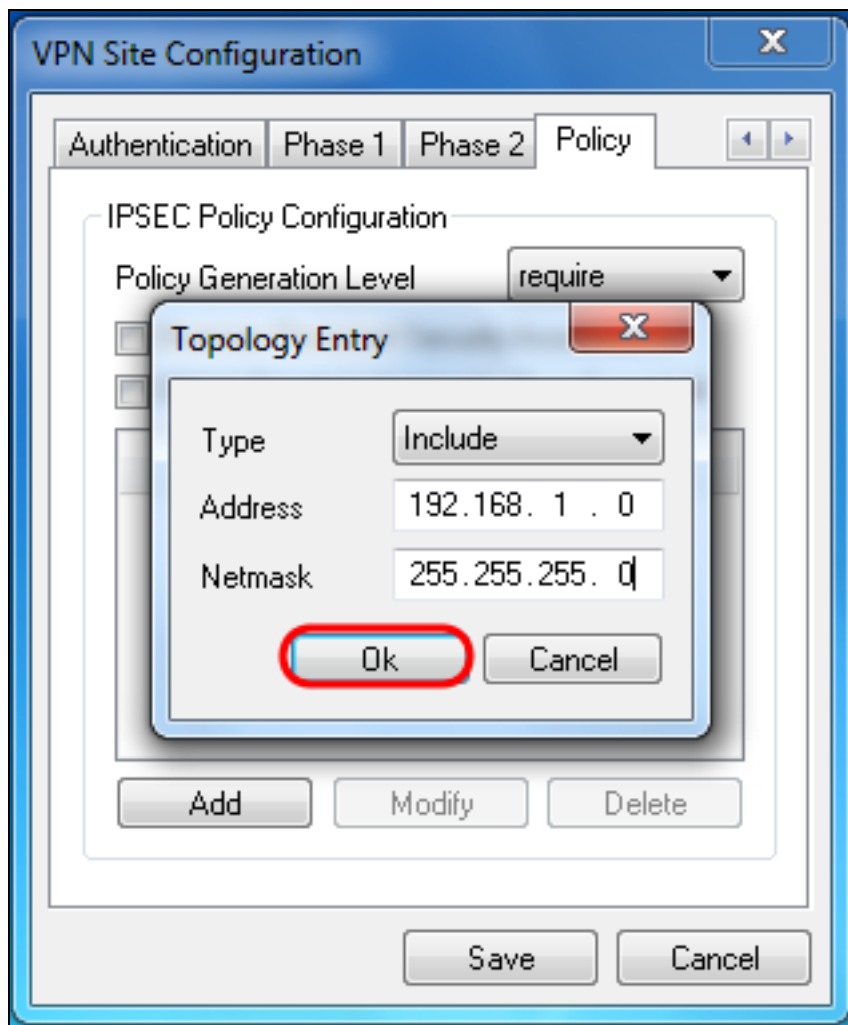
Step 20. Click **Save** to save your configurations for connecting to the VPN Site.

Step 21. Return to the *VPN Access Manager* window to select the VPN Site you configured, and click the **Connect** button.
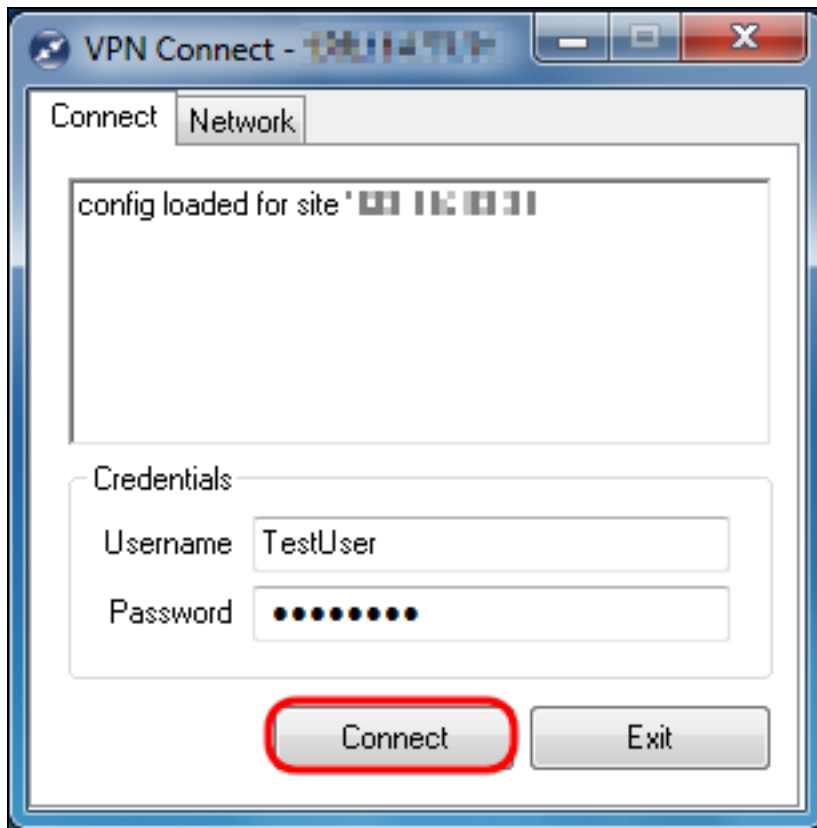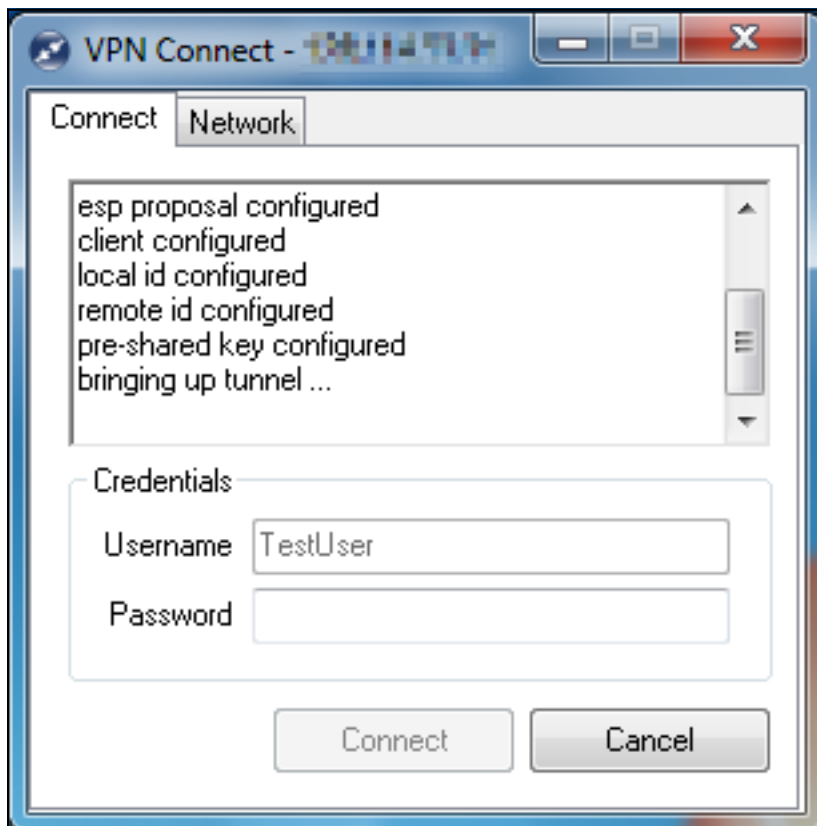
The *VPN Connect* window appears.

Step 22. In the *Credentials* section, enter the username and password of the account you set up in Step 4 of the *IPSec VPN Server User Configuration* section of this document.
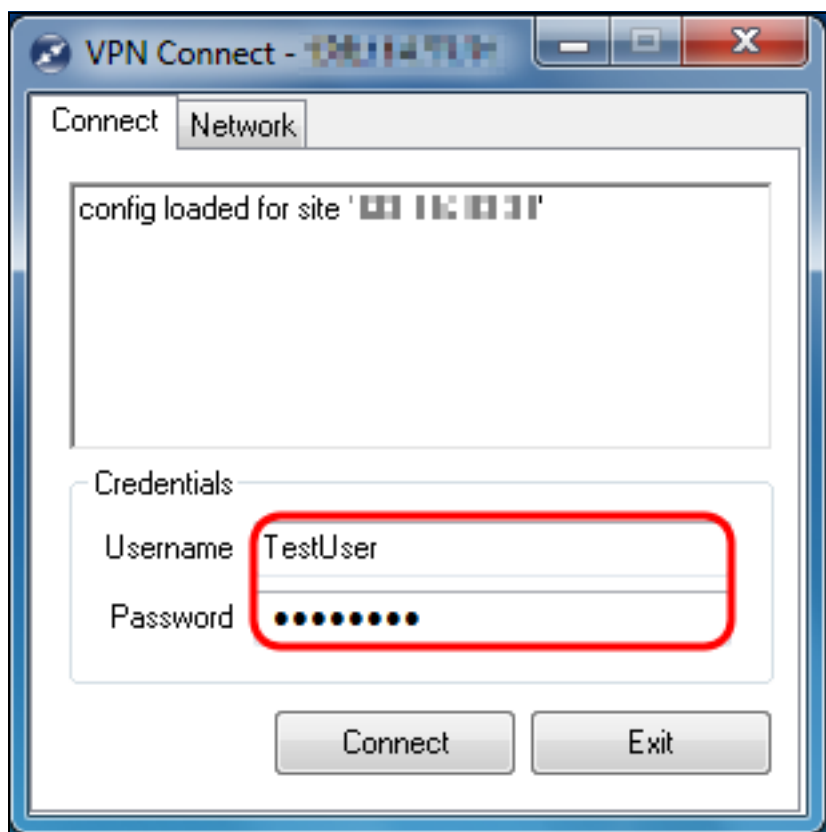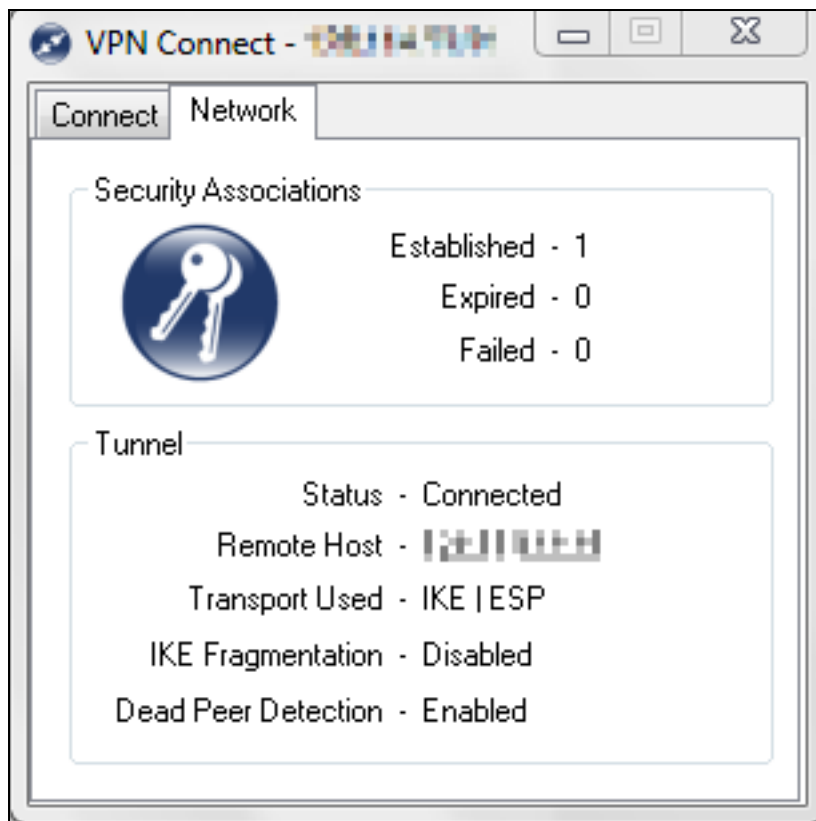

Step 23. Click **Connect** to VPN into the RV130/RV130W.

The IPSec VPN tunnel is established and the VPN client can access the resource behind the RV130/RV130W LAN.

View a video related to this article...

Click here to view other Tech Talks from Cisco