Configuring the Shrew Soft VPN Client for AOS VPN

Introduction

One of the recommended VPN clients for use with AOS devices is the Shrew Soft VPN client. This client is compatible with Windows 2000, Windows XP, Windows Vista, and Unix. It will interoperate correctly with AOS devices, and supports all forms of encryption that AOS devices currently support.

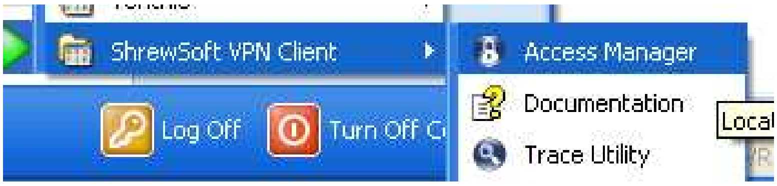
Hardware/Software Requirements

- Please check with Shrew Soft (www.shrew.net) for the requirements of the latest version.
- The AOS device that the client will connect to must be running the Enhanced Feature Pack (EFP) version of AOS.

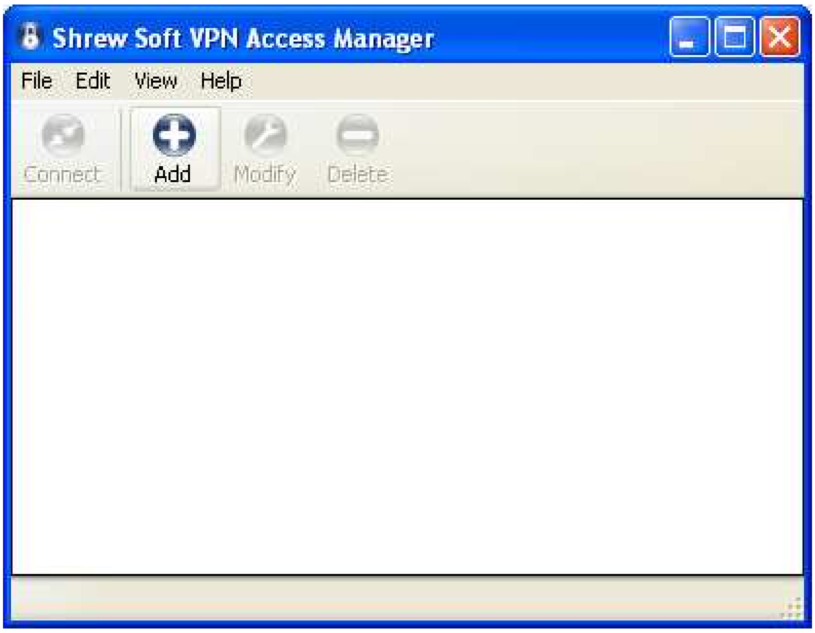
Shrew Soft Client Configuration

Getting Started

After installing the Shrew Soft client, you will need to open the '*Access Manager*', which should have been placed under the '*ShrewSoft VPN Client*' folder in the Start Menu, as shown:



Once open, you will need to add your first connection by clicking the *'Add'* button:

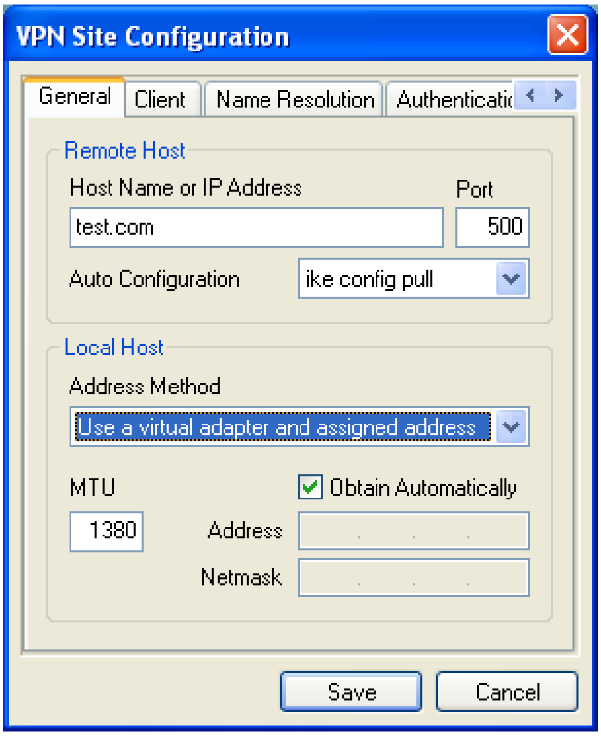


General Tab

Once open, the first tab that needs to be configured is the *'General'* tab. You will need to place the Hostname or IP Address that the client will be connecting to, which should resolve to or be the same as the router's primary Public IP.

(Recommended) If the client will be receiving a virtual IP address from the router, then the rest of the settings can be left at their default settings.

If the client will be hard-coded with an IP address, then Auto-Configuration should be **disabled**, the *'Obtain Automatically'* checkbox should be **unchecked**, and the appropriate IP address and a mask of 255.255.255.255 should be placed in the *'Address'* and *'Netmask'* fields.



Host Name or IP Address: test.com

Port: 500

Auto Configuration: ike config pull

Address Method: Use a virtual adapter and assigned address

MTU: 1380

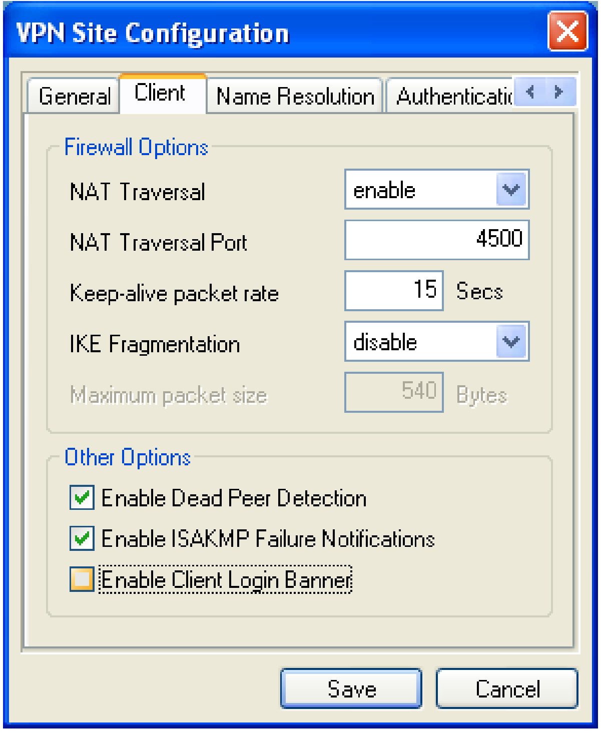
☑ Obtain Automatically

Address: . . .

Netmask: . . .

Client Tab

The next tab to be configured is the *'Client'* tab. In most cases nothing will need to be changed here, but *'IKE Fragmentation'* should be **disabled** and *'Enable Client Login Banner'* should be **unchecked** in all cases.



VPN Site Configuration

Firewall Options

NAT Traversal: enable

NAT Traversal Port: 4500

Keep-alive packet rate: 15 Secs

IKE Fragmentation: disable

Maximum packet size: 540 Bytes

Other Options

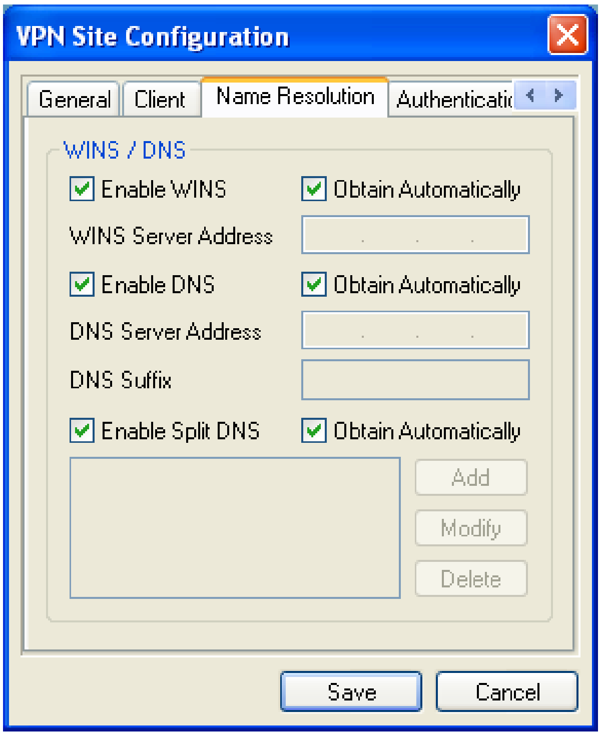
☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

□ Enable Client Login Banner

Name Resolution Tab

The next tab to be configured is the *'Name Resolution'* tab. There is nothing to configure here unless the client is hard-coded with an IP address on the *'General'* tab. **If that is the case**, then the *'Obtain Automatically'* checkboxes would need to be **unchecked**, and the appropriate values entered in. You may need to contact your network administrator for these values.



☑ Enable WINS ☑ Obtain Automatically

WINS Server Address

☑ Enable DNS ☑ Obtain Automatically

DNS Server Address

DNS Suffix

☑ Enable Split DNS ☑ Obtain Automatically

Authentication Tab

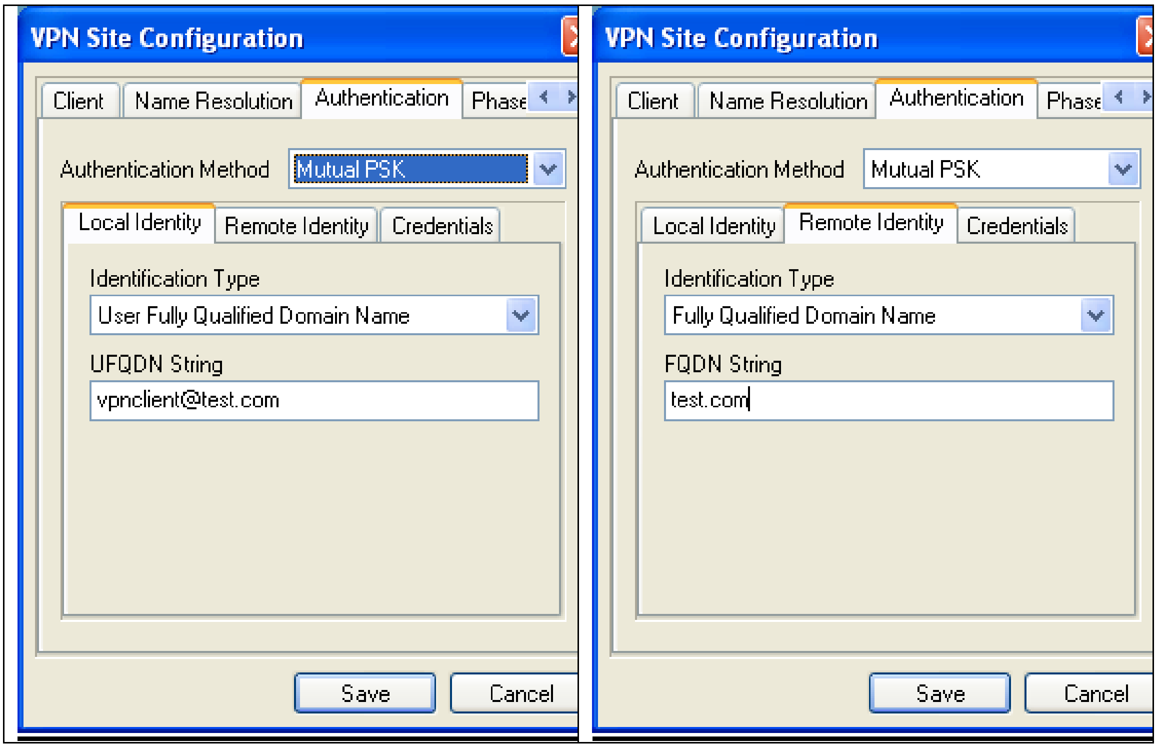
The next tab to be configured is the *'Authentication'* tab. The settings here will depend upon whether you have enabled *'Extended Authentication' (XAUTH)* on the AOS device. This is also where certificates would be setup, but this document will only cover *'Pre-Shared Key' (PSK)* authentication.

If the client **is NOT using XAUTH** (typical), set the *'Authentication Method'* to *'Mutual PSK'*. If the client **is using XAUTH**, set that field to *'Mutual PSK + XAuth'*.

Under the *'Local Identity'* sub-tab, set the *'Identification Type'* to the type set on the AOS device for the client; this will typically be *'Fully Qualified*

Domain Name' (FQDN) or *'User Fully Qualified Domain Name' (User-FQDN, Email Address)*. Then set the string to the correct value the router is expecting.

Under the *'Remote Identity'* sub-tab, set the *'Identification Type'* to what the AOS device will be sending to the client; this will typically be *'FQDN'* or *'IP Address'*. Then set the string to the correct value the AOS device will be sending.



VPN Site Configuration

Authentication Method: Mutual PSK

Identification Type: User Fully Qualified Domain Name

UFQDN String: vpnclient@test.com

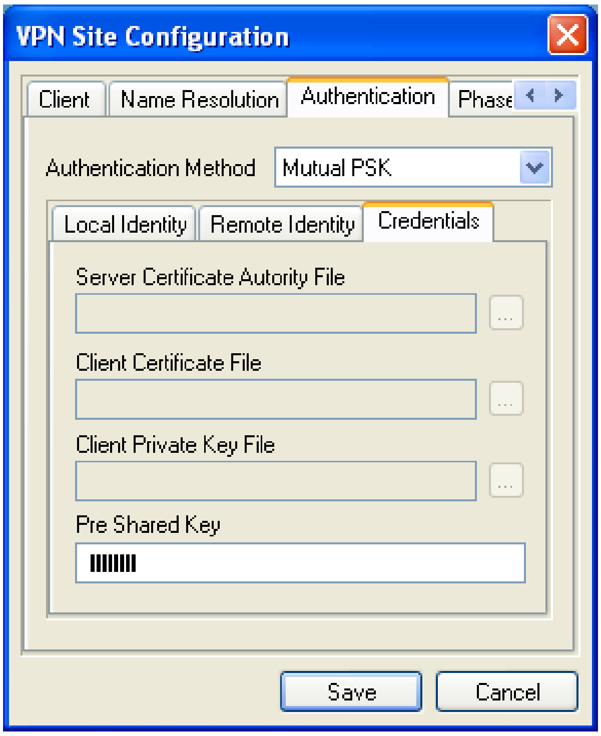
VPN Site Configuration

Authentication Method: Mutual PSK

Identification Type: Fully Qualified Domain Name

FQDN String: test.com

The ‘Credentials’ sub-tab is for inputting the PSK or the certificate *(not covered in this document)*. Enter the appropriate PSK that the AOS device has associated with the identity previously specified.



Authentication Method: Mutual PSK

Server Certificate Autority File

Client Certificate File

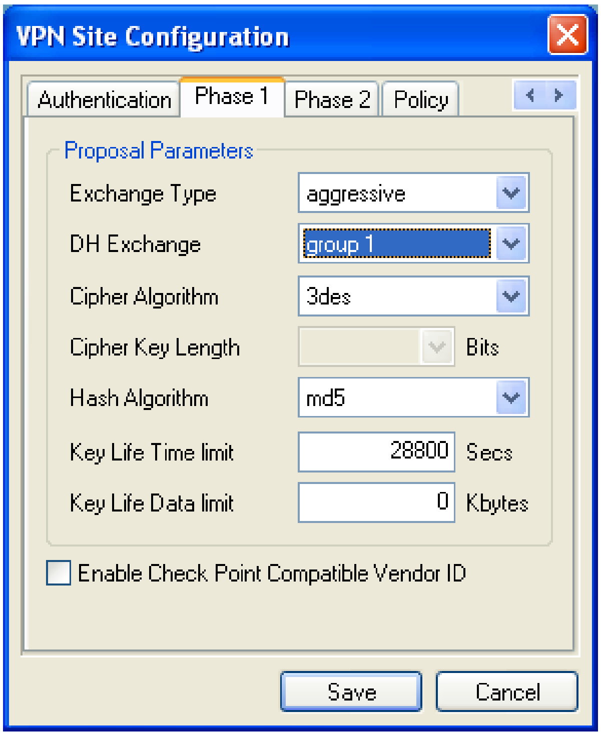
Client Private Key File

Pre Shared Key: ||||||||

Phase 1 Tab

The next tab to be configured is the *'Phase 1'* tab. This tab will reflect the key group, encryption, hashing, and lifetime settings configured for IKE (Phase 1) in the AOS device. VPN clients will typically use *'Aggressive'* mode for the *'Exchange Type'*.

The settings configured during the 'Typical Setup' option of the VPN Wizard in AOS devices are displayed here. AOS devices do not support a Phase 1 Key Life Data limit, so this setting should always be left at zero (0).



Proposal Parameters

Exchange Type: aggressive

DH Exchange: group 1

Cipher Algorithm: 3des

Cipher Key Length: Bits

Hash Algorithm: md5

Key Life Time limit: 28800 Secs

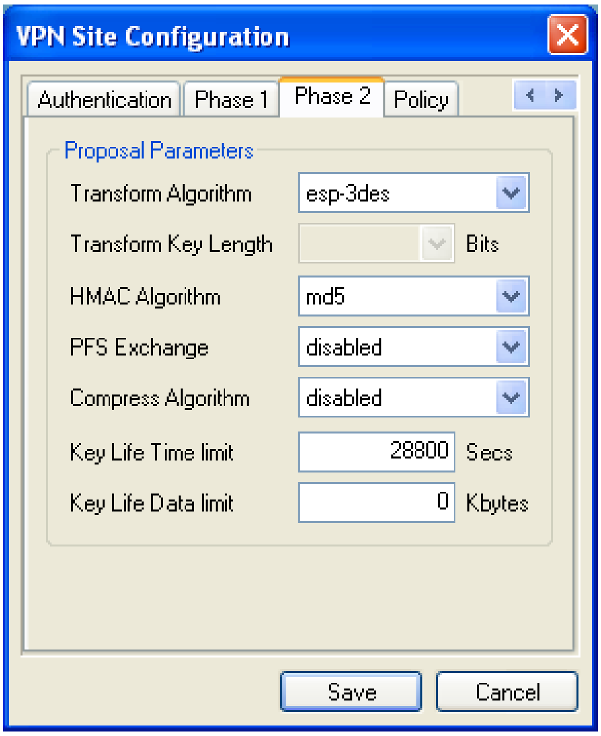
Key Life Data limit: 0 Kbytes

☐ Enable Check Point Compatible Vendor ID

Phase 2 Tab

The next tab to be configured is the *'Phase 2'* tab. This tab will reflect the encryption, hashing, and lifetime settings configured for IPSEC (Phase 2) in the AOS device.

The settings configured during the 'Typical Setup' option of the VPN Wizard in AOS devices are displayed here.



Transform Algorithm: esp-3des

Transform Key Length: Bits

HMAC Algorithm: md5

PFS Exchange: disabled

Compress Algorithm: disabled

Key Life Time limit: 28800 Secs

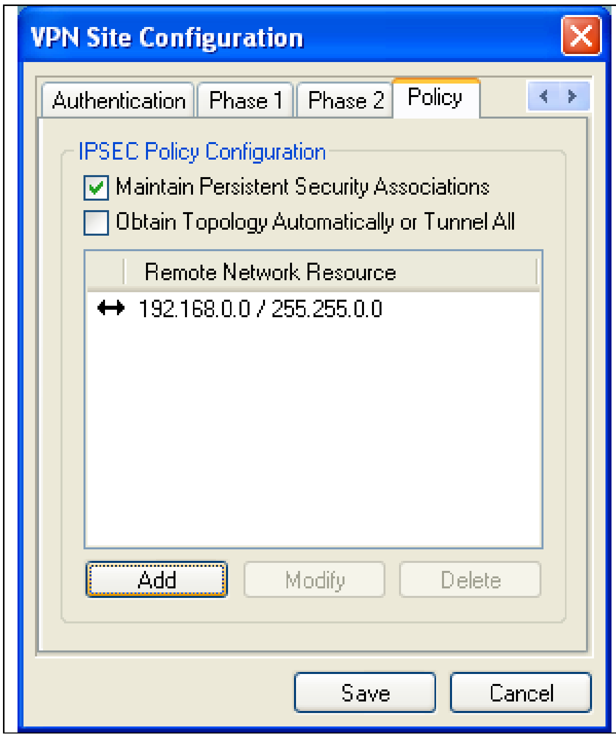
Key Life Data limit: 0 Kbytes

Policy Tab

The final tab to be configured is the *'Policy'* tab. *'Maintain Persistent Security Associations'* should be changed to **checked**. *'Obtain Topology Automatically or Tunnel All'* should be changed to **unchecked**.

The final step is to define the networks behind the AOS device the VPN client will be connecting to. In this example, the VPN client will be allowed to connect with any 192.168 address. The network is added by clicking the *'Add'* button, and defining the appropriate subnet & mask in the popup that appears.

Click *'Save'* when finished.



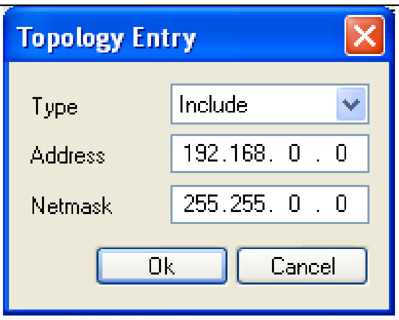
IPSEC Policy Configuration

☑ Maintain Persistent Security Associations

☐ Obtain Topology Automatically or Tunnel All

Remote Network Resource

↔ 192.168.0.0 / 255.255.0.0



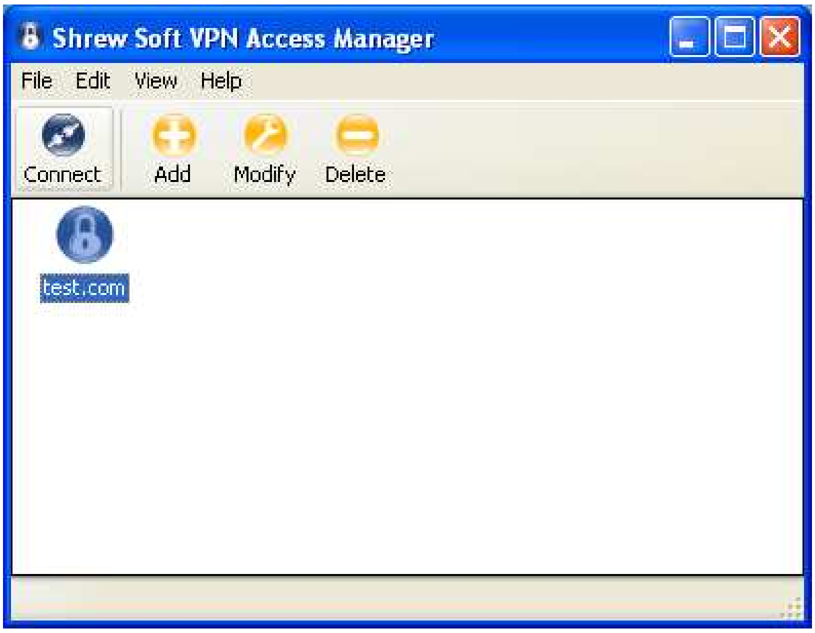
Type: Include

Address: 192.168. 0 . 0

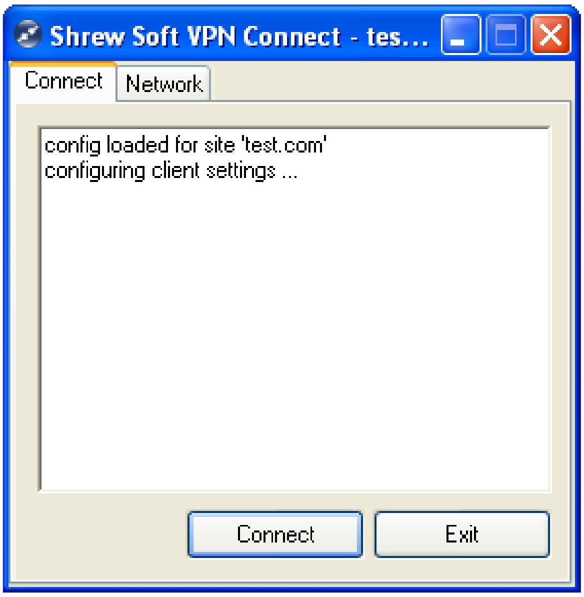
Netmask: 255.255. 0 . 0

Shrew Soft Client Connection

Once the connection has been configured, the program will return you to the Access Manager. You will need to highlight the appropriate connection, and select *'Connect'*.

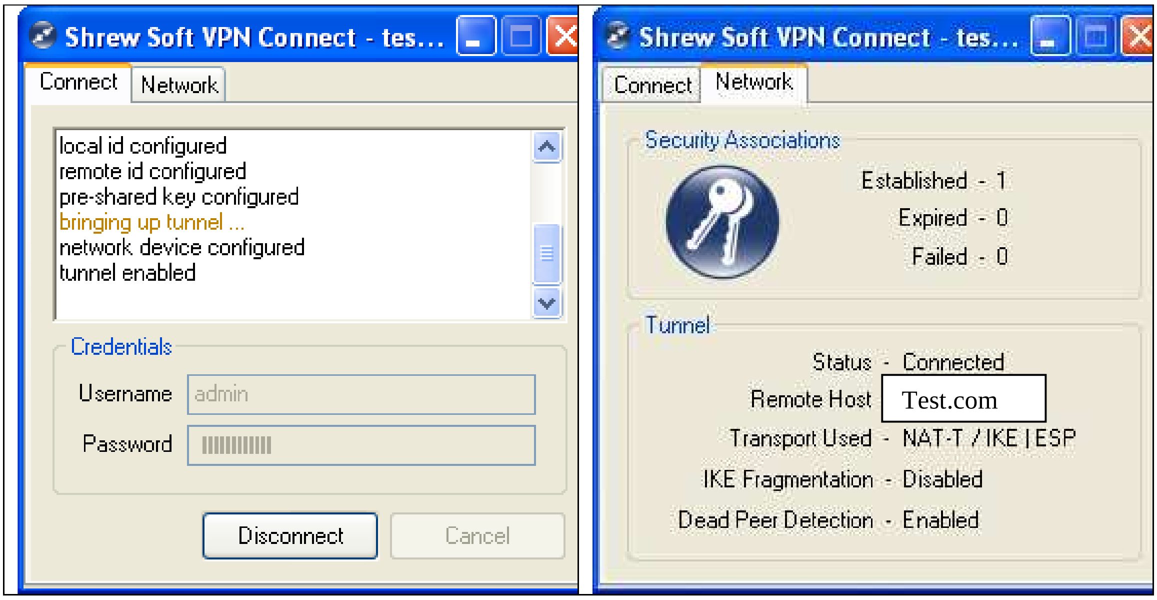


This will open up a new connection window. If you are using XAUTH, there will also be a field to input the username and password your connection requires. Click *'Connect'* when ready.



```
config loaded for site 'test.com'
configuring client settings ...
```

The client will attempt to connect to the AOS device. You can view the step-by-step output of the client on the *'Connect'* tab, or switch to the *'Network'* tab for an overview.



Shrew Soft VPN Connect - tes...
Connect
Network

```
local id configured
remote id configured
pre-shared key configured
bringing up tunnel ...
network device configured
tunnel enabled
```

Credentials

Username: admin

Password: ||||||||||||

Disconnect
Cancel
Shrew Soft VPN Connect - tes...
Connect
Network

Security Associations

Established - 1

Expired - 0

Failed - 0

Tunnel

Status - Connected

Remote Host: Test.com

Transport Used - NAT-T / IKE | ESP

IKE Fragmentation - Disabled

Dead Peer Detection - Enabled

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.