

VPN setup in Windows 10

The Cisco VPN client does not work in Windows 10. You can use a VPN client made by ShrewSoft instead.



Download the latest version by visiting <https://www.shrew.net/download/vpn> and selecting the Installer option at the top of the table. The OS Support does not mention Windows 10, but it will work.

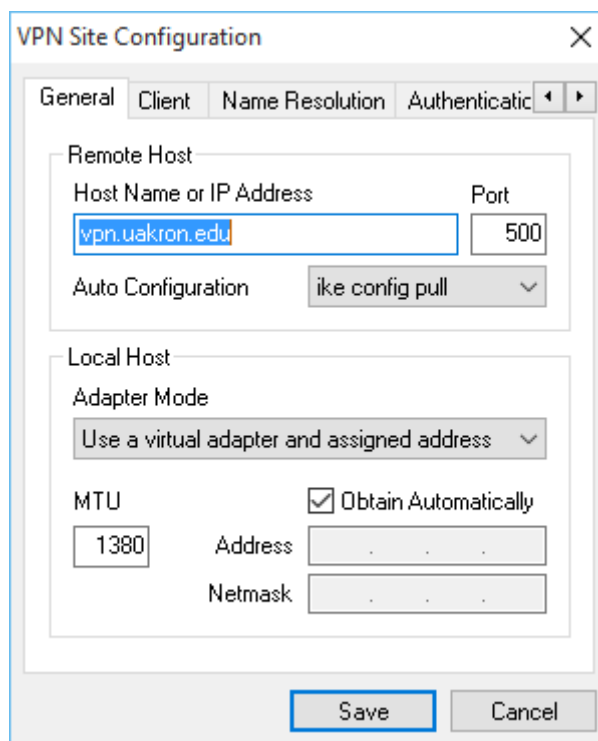
Downloads

STABLE RELEASE					
Date	Build	OS Support	Download	Changelog	
Jul 01 2013	2.2.2-release	Windows 2K/XP/Vista/7/8	- Installer	client	
Jun 05 2013	2.2.1-release	Windows 2K/XP/Vista/7/8	- Installer	client ike	
Apr 24 2013	2.2.0-release	Windows 2K/XP/Vista/7/8	- Installer	client ike	

Once installed, you can find the software as the “VPN Access Manger” under “ShrewSoft VPN Client” in the Start menu if a shortcut was not created on the desktop during install. Open the software and click the Add button.

Fill out the various tabs as follows –

1. General: Add host name – **vpn.uakron.edu**



VPN Site Configuration

General Client Name Resolution Authenticatic

Remote Host

Host Name or IP Address Port

vpn.uakron.edu 500

Auto Configuration ike config pull

Local Host

Adapter Mode

Use a virtual adapter and assigned address

MTU Obtain Automatically

1380 Address . . .

Netmask . . .

Save Cancel

2. **Client:** No change

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section includes: NAT Traversal (enable), NAT Traversal Port (4500), Keep-alive packet rate (15 Secs), IKE Fragmentation (enable), and Maximum packet size (540 Bytes). The 'Other Options' section includes: Enable Dead Peer Detection (checked), Enable ISAKMP Failure Notifications (checked), and Enable Client Login Banner (checked). 'Save' and 'Cancel' buttons are at the bottom.

3. **Name Resolution:** No Change

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Name Resolution' tab selected. The 'DNS' sub-tab is active. It includes: Enable DNS (checked), Obtain Automatically (checked), four Server Address fields (all empty), and DNS Suffix (empty). There is also an 'Obtain Automatically' checkbox for the DNS Suffix section. 'Save' and 'Cancel' buttons are at the bottom.

4. Authentication

Local Identity Tab

VPN Site Configuration

Client Name Resolution Authentication Phase

Authentication Method Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Identification Type Key Identifier

Key ID String Zipnet

Save Cancel

Change

Authentication Method to
“Mutual PSK + XAuth”

Identification Type to
“Key Identifier”

Key ID String to
“ Zipnet”
(must use capital Z)

Remote Identity Tab

VPN Site Configuration

Authentication Phase 1 Phase 2 Policy

Authentication Method Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Identification Type Any

Save Cancel

No Change

Credentials Tab

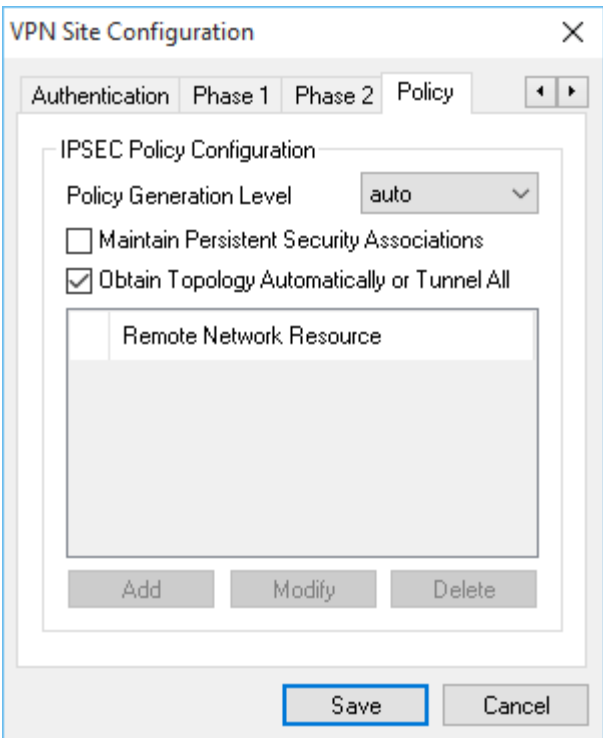
The screenshot shows the 'Credentials Tab' of the 'VPN Site Configuration' dialog. The 'Authentication Method' is set to 'Mutual PSK + XAuth'. Under the 'Credentials' sub-tab, there are fields for 'Server Certificate Authority File', 'Client Certificate File', and 'Client Private Key File', each with a browse button. The 'Pre Shared Key' field contains five black dots. At the bottom, there are 'Save' and 'Cancel' buttons.

Change Pre Shared Key to "zippy"

5. Phase 1, Phase 2, Policy: No Change

The screenshot shows the 'Phase 1' tab of the 'VPN Site Configuration' dialog. The 'Proposal Parameters' section includes: 'Exchange Type' (aggressive), 'DH Exchange' (group 2), 'Cipher Algorithm' (auto), 'Cipher Key Length' (dropdown), 'Hash Algorithm' (auto), 'Key Life Time limit' (86400 Secs), and 'Key Life Data limit' (0 Kbytes). There is an unchecked checkbox for 'Enable Check Point Compatible Vendor ID'. 'Save' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Phase 2' tab of the 'VPN Site Configuration' dialog. The 'Proposal Parameters' section includes: 'Transform Algorithm' (auto), 'Transform Key Length' (dropdown), 'HMAC Algorithm' (auto), 'PFS Exchange' (disabled), 'Compress Algorithm' (disabled), 'Key Life Time limit' (3600 Secs), and 'Key Life Data limit' (0 Kbytes). 'Save' and 'Cancel' buttons are at the bottom.



Click Save and give the connection a name. Double click the connection and enter your uanet credentials to login. You can disconnect from the software window or by right-clicking the ShrewSoft icon in the system tray.