

Background to Virtual Private Networks

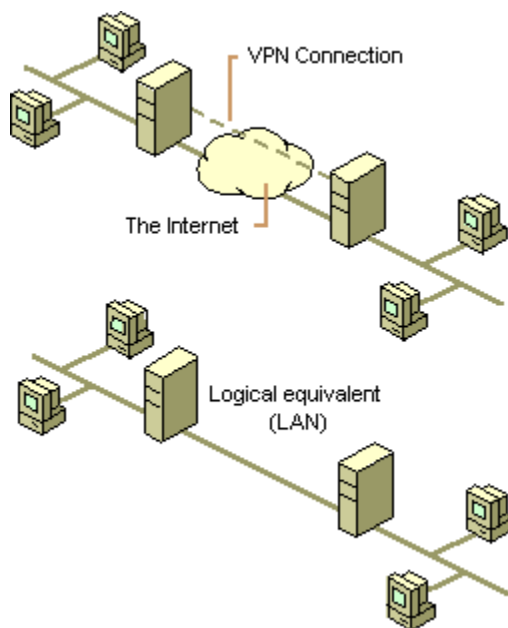
A simple definition of a virtual private network (VPN) is "a private network constructed within a public network infrastructure, such as the global Internet."

Typically, it is used to connect remote clients to the local area network (LAN), or to connect two LANs together.

The private data that travels over the public network, or Internet, is encrypted to preserve security.

The following is a classic example of a VPN. Notice how the 'shared or public network' (e.g. the Internet) allows authorised users in remote locations to connect to the network in the same way that nodes on a LAN can connect to a server.

Click [here](#) for specifics on the WinGate VPN.



Step by Step Guide

The following is a quick step-by-step guide describing the basics of hosting and joining a VPN. Click the links for more detailed screen-based information.

Hosting a VPN

Follow the steps below if you want to **host** a VPN:

1. Download one of the 'host' versions of the VPN product from the WinGate Website You may either do this at the same time as you download WinGate (this option is available on the main WinGate installation wizard) or you may click on the 'VPN' icon on the GateKeeper toolbar to get a trial version of this product.
2. Once installed, double-click 'VPN' on GateKeeper's system tab.
3. Click the [VPNs to Host](#) tab on the VPN Configuration screen.
4. Enter basic details about your VPN in the [General tab](#).
5. Define policy details governing the VPN you're hosting in the [Policies tab](#).
6. Create an individual X509 Certificate for any VPNs you want to host. Click [here](#) to find out more about [security and certificates](#) in the WinGate VPN.
7. [Confirm details](#) of the certificate(s) you have created.
8. You are now free to distribute details of your VPN to those who you wish to join it. This must include your IP address or DNS Name, the port you are using (usually 809), the fingerprint generated by your certificate, and the individual username and password you assign to each user. The best way to do this is by [exporting the configuration](#) in a single file, which clients can then use to enable a successful connection.

Joining a VPN

Follow the steps below if you want to **join** a VPN:

1. Download one of the 'join' versions of the VPN product from the [WinGate website](#). You may either do this at the same time as you download WinGate (this option is available on the main WinGate installation wizard) or you may click on the 'VPN' icon on the GateKeeper toolbar to get a trial version of this product.
2. Once installed, double-click 'VPN' on GateKeeper's system tab.
3. Click the [VPNs to Join](#) tab on the [VPN Configuration](#) screen.
4. Enter connection and authentication details (including server name, port number, username/ password, and fingerprint) about the VPN you are joining in the [VPN to Join](#) screen. You may take a short-cut when entering these details by [importing the configuration](#) (in the form of a single file) from the VPN host.
5. Go to GateKeeper, right click on the VPN and click 'Connect'.
6. You will shortly be able to see all the network machines on your Network Neighborhood – be aware that it may take a couple of minutes for the machines to register here, but you will be able to browse for them immediately using a UNC (Universal Naming Convention) e.g. [\\computername\documents](#) using the 'Run' command on your Start menu.

Operating a Peer-to-Peer VPN

Follow these steps if you want to operate a **Peer-to-Peer** VPN, and click [here](#) for more information on [Peer to Peer VPNs](#).

1. Each peer (we'll call them 'Peer 1' and 'Peer 2') downloads the Peer-to-Peer VPN product from the WinGate Website <http://www.wingate.com> . You may either do this at the same time as you download WinGate (this option is available on the main WinGate installation wizard) or you may click on the 'VPN' icon on the GateKeeper toolbar to get a trial version of this product.
2. Once installed, Peer 1 double-clicks 'VPN' on GateKeeper's system tab.
3. Peer 1 must now create an individual X509 Certificate for the VPN. Click [here](#) to find out more about [security and certificates](#) in the WinGate VPN.
4. [Confirm Details](#) of the certificate.
5. You are now free to distribute details of your VPN to those who you want to join it. This must include your IP address or DNS Name, the port you are using (usually 809), the fingerprint generated by your certificate, and the individual username and password you assign to each user. The best way to do this is by [exporting the configuration](#) in a single

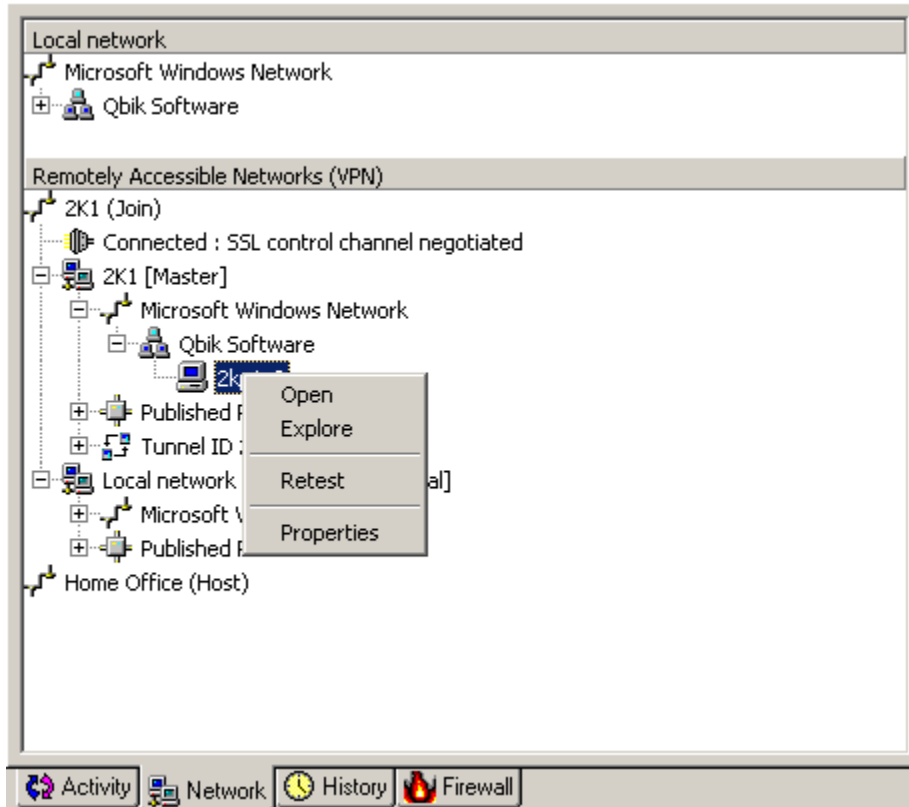
file, which clients can then use to enable a successful connection.

6. Peer 2 may now import these details which (along with using the same license as Peer 1) will enable a successful connection to the VPN.
7. Peer 2 may now create and export his own certificate which Peer 1 can use to connect to the VPN that Peer 2 has initiated, allowing reciprocal connection options.

Note: See the [Troubleshooting](#) section if you encounter system-generated error messages.

VPN Display





The following is a typical example of VPN activity that can be viewed from GateKeeper's Network tab.



This network tab divides the screen between the machine's Local Area Network (LAN) at the top, and the Remotely Accessible Networks which are made available by the VPN. Right-clicking on any particular machine, whether it be local or remote, gives you three options-

1. Open – this opens the local machine
2. Explore – this opens the local machine and connected network
3. Re-test – this retests the specific computer behind the VPN
4. Properties – this allows you to view the properties of the particular machine.

VPN Monitor- The VPN Monitor is an icon in the system tray that displays the status of the VPN. There are four colours:

-  A blue/green icon denotes a connected VPN.
-  A black icon denotes a disconnected VPN.
-  A red icon denotes a stopped WinGate VPN engine.
-  A yellow icon denotes a WinGate VPN engine in the process of starting or stopping.

If you are having problems with your VPN, this is the first place you should look – it appears in the Network tab of the main GateKeeper screen and also in the bottom right hand corner of the system tray e.g. here it is second from the right on this system tray -



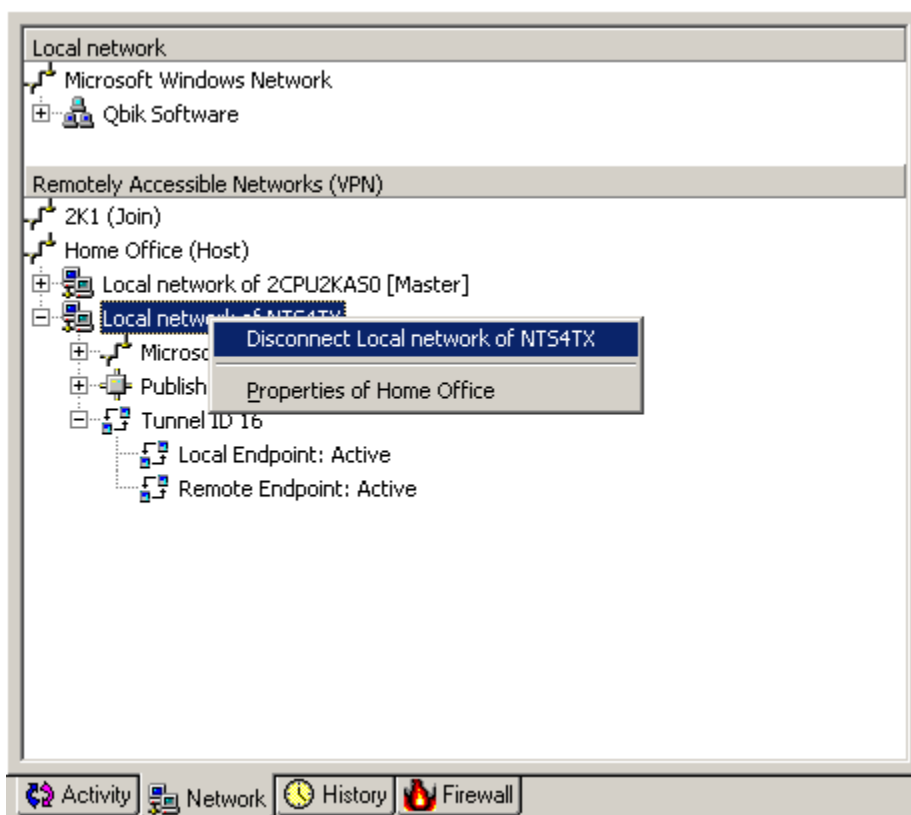
You can mouse over the VPN Monitor for tool tips.

Network Window

The Network Window allows you to see the status of your local area network and any connected VPNs. This Window will appear on WinGate with VPN installations and WinGate VPN installations. From here you can:

- Connect a VPN
- Disconnect a VPN
- Change the properties of a VPN
- Disconnect a node joined to a VPN (Host only)
- Re-test any of the machines accessible through a VPN connection

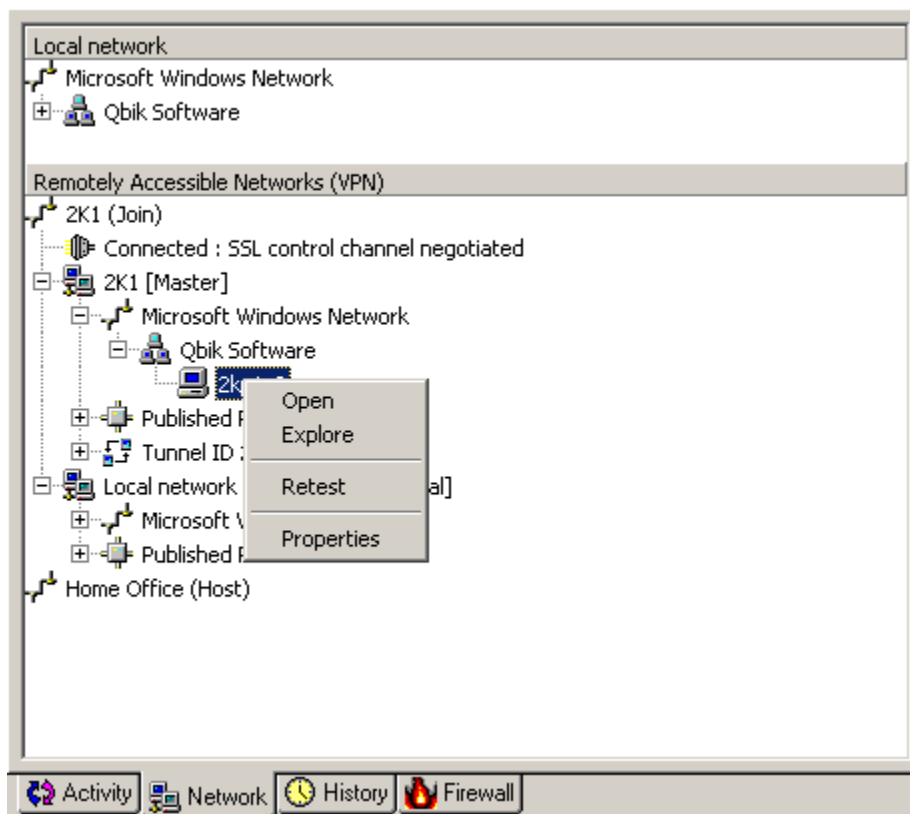
In addition, you can see up to date status information about the network, the VPN and the various tunnels.



This view shows a hosted VPN with the right-click menu for a joined node dropped down. You can right-click on any item for the appropriate context-sensitive menu.

- **Microsoft Windows Network** – details the enumeration of computers behind this VPN. Click [here](#) for more information.
- **Published routes** – shows the routes that are published by this VPN. Click [here](#) for more information.
- **Tunnel** – shows the current status of any tunnels with this node. Click [here](#) for more information.

Any appropriate messages, such as expired certificates, status of the connection or error messages will be displayed underneath the entry as appropriate.



This view shows a joined VPN with the right-click menu for a computer behind the hosted VPN dropped down. You can right-click on any item for the appropriate context-sensitive menu.

Microsoft Windows Network






This portion of the network window shows the current list of machines behind the appropriate node. You can right-click on any machine for more options.

- Open – opens a Windows Explorer view of the machine
- Explore – opens a Windows Explorer view of the machine with the Folders view active
- Retest – retests the machines availability, using WINS
- Properties – opens a dialog that shows details of the machine, such as IP address.

Due to the nature of NETBIOS enumeration, the time it takes for machines to appear in the Network Window is determined by the speed of your link and can vary.

Published Routes





This portion of the network window shows the list of routes that are published by the appropriate node. The routes can be in a variety of states.

-  - Disabled – the route is disabled by user choice
-  - Enabled – the route is active and published
-  - In conflict – the route has been disabled by the host VPN because it conflicts with another route
-  - Ignored / local conflict – the route has been disabled by the local VPN because it conflicts with a local route entry
-  - Forced – the route is not normally published with the local participation selected, but has been published because a user specifically forced it to be published

Note: When forcing a route to be published, please ensure that you are aware of the impact this would have on your routing.

Tunnels

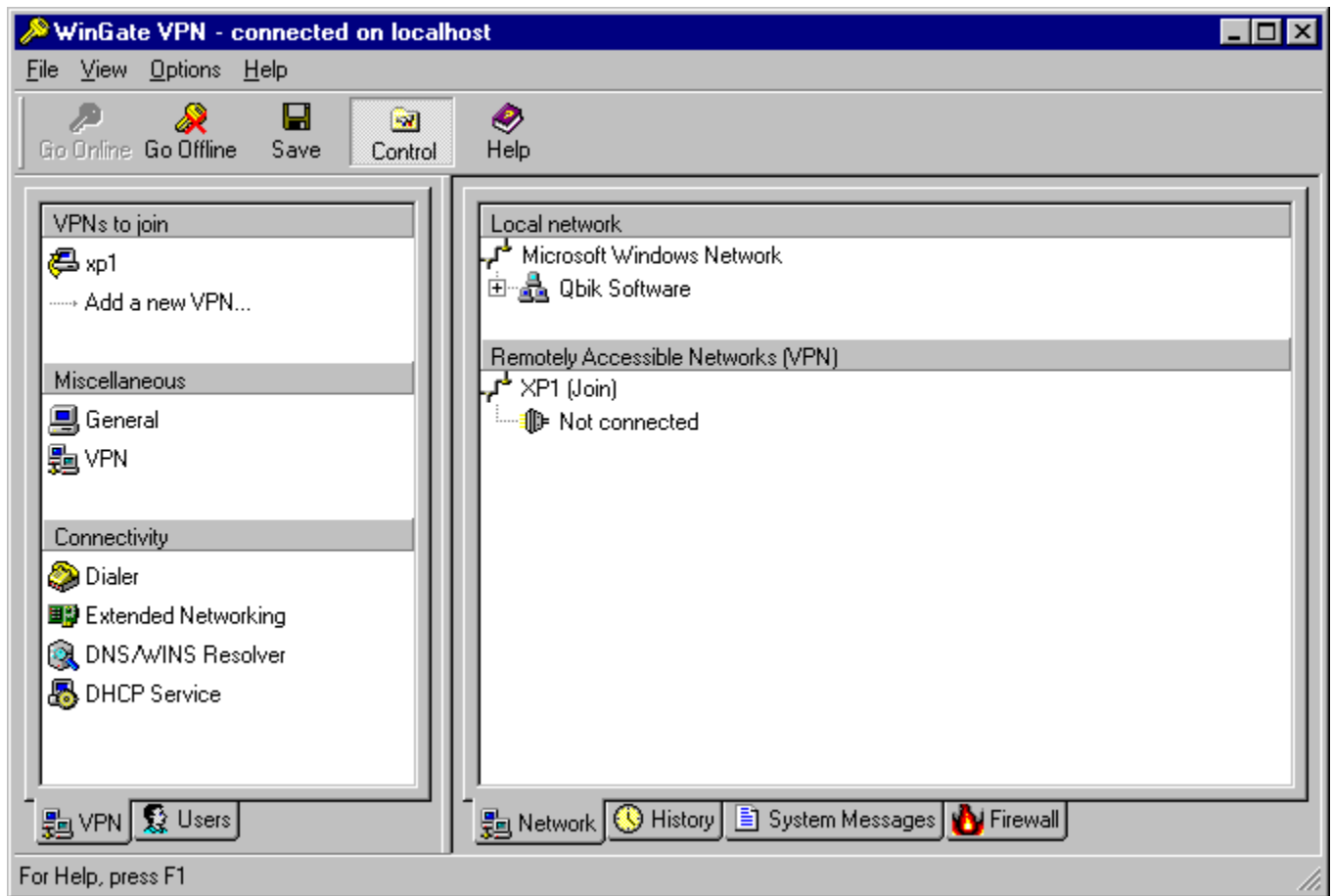
Tunnels are shown with regards to the node they are tunneling to. There are four possible states:

-  - In Stasis – the tunnel has not been requested or created. This normally shows when a node will only accept tunnels to the VPN Host, and not with other nodes.
-  - Pending – the tunnel has been requested but not created. This will change to "Active" or "Error"
-  - Active – the tunnel has been created. If you are experiencing problems with tunneled data, you might need to verify the routing configuration.
-  - Error – the tunnel has not been created. The appropriate error status or error code will be listed.

VPN Only GUI

It is now possible to run a VPN without WinGate – this is known as the ‘VPN Only GUI’. All the operations are the same as in the WinGate Plugin VPN (running as a plugin to WinGate), except that:

- The VPN Only GUI displays more information ‘up front’ than in the WinGate Plugin VPN.
- The VPN Only GUI is very simple to set-up and use – particularly handy for client machines on which there is no need for the entire WinGate program.



The VPN only GUI is designed to be very ‘clickable’.

- Clicking on any menu item under the ‘VPNs hosted’ heading brings up the [VPNs to Host](#) screen.
- Clicking on any menu item under the ‘Miscellaneous’ heading brings up the [VPNs to Host Tab](#) screen.
- Clicking on the Dialer icon brings up the Dialer Properties screen.
- Clicking on the Extended Networking icon brings up the Extended Network Driver screen.

Note:

The DHCP option will be available with all VPN Only GUI installations, apart from Peer 2 Peer and Remote Client licenses. You have full control of the DHCP service as in WinGate.

The WinGate VPN

The WinGate VPN is a full-service Virtual Private Network available with WinGate 5.0 and beyond.

The WinGate VPN needs no additional or dedicated hardware, and the server can run on a variety of platforms. All current Windows versions supported, including:

- Windows NT 4 / 2000 / XP
- Windows ME / 98 / 95

VPN clients can support any operating system that uses TCP/IP – including Mac and Linux machines.

The WinGate VPN uses some WinGate features, but it requires a separate download from the WinGate website <http://www.wingate.com> . You may trial this product for 30 days, free-of-charge.

The WinGate VPN is an easy to use, easy to set-up, affordable solution. Key features of it include:

- a live activity screen showing all current participants.
- support for the routing of any IP based protocol, including TCP, UDP, ICMP and GRE.
- the VPN server node can participate as a network peer or 'neutral' umpire.
- each node can join or host multiple VPNs, and keep the same IP address for each virtual network it belongs to.
- fully-encrypted data tunnels using 128-bit 'Twofish' cypher.
- a firewall to protect the VPN gateway from unwanted external traffic.
- VPN control connections use industry-standard SSL.
- a user interface that is clean and simple to configure – the network window displays real-time updates, so you can keep an eye on current activity.
- ability to connect across NAT gateways.
- the use of industry-standard X509 certificates to ensure node identity and connection security.

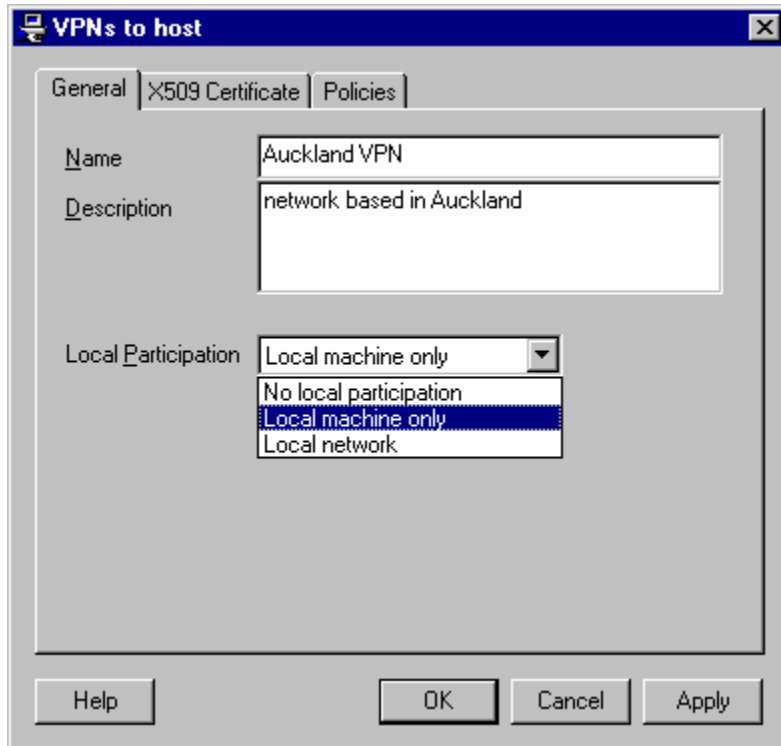
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

<http://www.openssl.org>

Click [here](#) for a [Step by Step Guide](#) on hosting and joining a VPN.

VPNs to Host

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



Name - Enter the 'Name' of the VPN you are setting up. This is the name that nodes must use in order to make the connection. VPN clients attempting to connect to your VPN **must** use this name in order to do so.

Description - This is not a mandatory field.

Local Participation - Choose the access level you want in the 'Local Participation' field. Your options are:

- 'No local participation' (allows remote clients to join the VPN and communicate with each other, but not access the VPN host itself)
- 'Local machine only' (allows remote clients to access the VPN host itself, but not the network connected to it)
- 'Local network' (if you want the remote clients to have full access to the network)

Selecting either the 'Local Machine Only' or 'Local Network' options displays the 'Customise Routes' button.

The image shows a Windows-style dialog box titled "VPNs to host :". It has three tabs: "General", "X509 Certificate", and "Policies". The "General" tab is selected. Inside the dialog, there are two text input fields: "Name" with the text "Auckland VPN" and "Description" with the text "VPN based in Auckland". Below these is a "Local Participation" section with a dropdown menu currently showing "Local network". A button labeled "Customise Routes" is positioned below the dropdown. At the bottom of the dialog are four buttons: "Help", "OK", "Cancel", and "Apply".

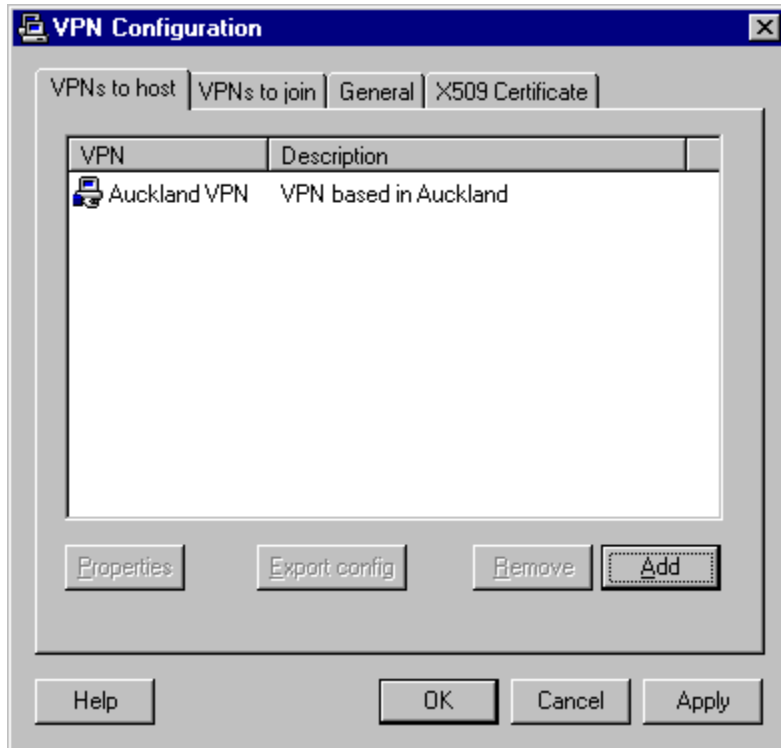
Field	Value
Name	Auckland VPN
Description	VPN based in Auckland
Local Participation	Local network

Buttons: Help, OK, Cancel, Apply

Click [Customise Routes](#) to define customisation options for your network.

VPNs to Host Tab

Click [here](#) for a [Step by Step Guide](#) on hosting and joining a VPN.



The above screen displays all the VPNs hosted on this node.

Export Config - Click 'Export Config' to send the selected VPN's settings to a file. This file may then be distributed to everyone connecting to the VPN. Click [here](#) to learn how to do this.

Add - Click 'Add' to initiate a VPN. This brings up the [VPNs to Host](#) screen.

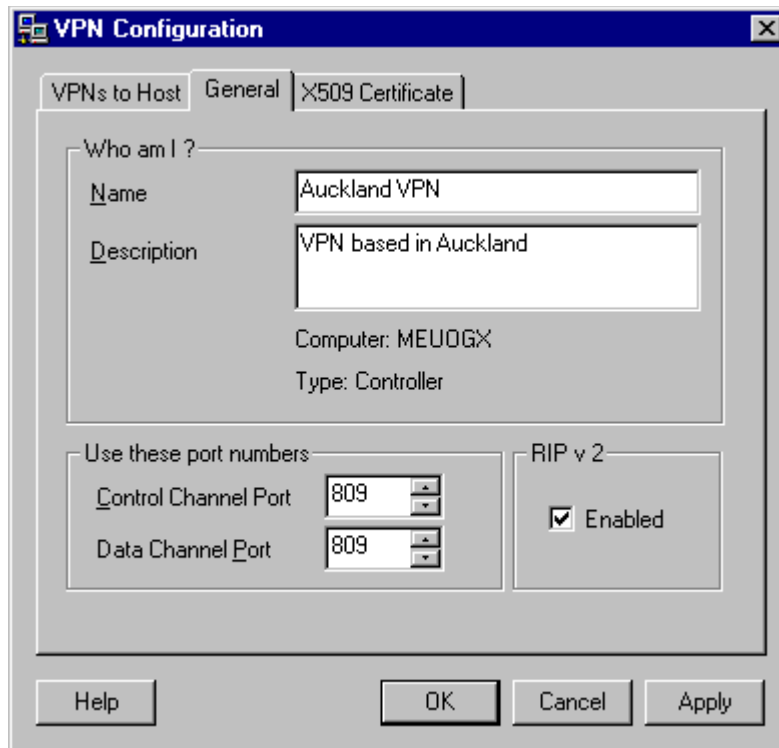
Remove - Click 'Remove' to cease hosting the highlighted VPN.

Apply - Click 'Apply' to implement all changes made to the information in the screen.

General Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

The main purpose of this tab is to identify this node to the VPN server and to define which port numbers to use.



The screenshot shows the 'VPN Configuration' dialog box with the 'General' tab selected. The 'Who am I?' section contains a 'Name' field with 'Auckland VPN' and a 'Description' field with 'VPN based in Auckland'. Below these, it shows 'Computer: MEUOGX' and 'Type: Controller'. The 'Use these port numbers' section has 'Control Channel Port' and 'Data Channel Port' both set to 809. The 'RIP v 2' section has a checked 'Enabled' checkbox. At the bottom are 'Help', 'OK', 'Cancel', and 'Apply' buttons.

Name - Choose a name for your VPN.

Description - Enter anything you like here. Not a mandatory field.

Control Channel Port - This is the port for communication between VPN nodes. The default port is 809.

Data Channel Port - This is the the port that handles network traffic across the VPN. Likewise, default is 809. Every node connected to the VPN must have the same ports selected if they are to participate in any exchange of data.

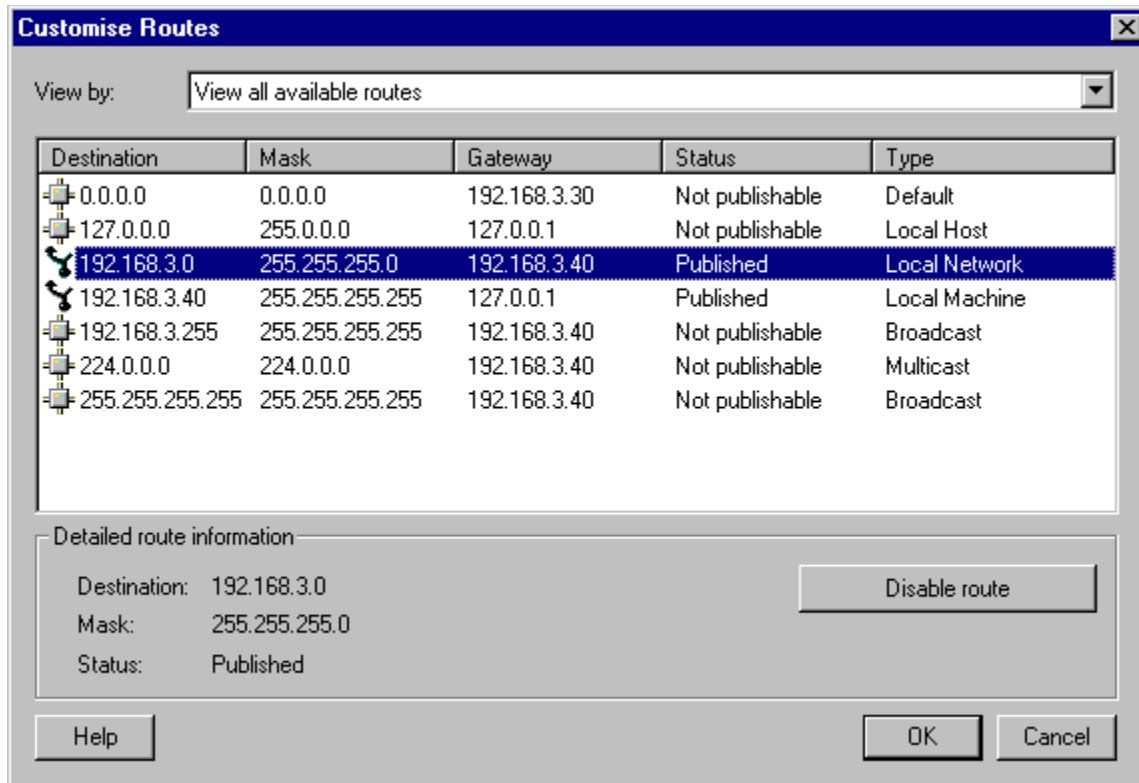
RIP v 2 - Check this box if you want to publish routing information onto your LAN using RIP 2. If your client machines have RIP support activated, they'll become aware that you are the gateway for routes available over the VPN.

Note - RIP (**R**outing **I**nformation **P**rotocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs.

Customise Routes

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

The purpose of this screen is to display all relevant routes available to be used by your VPN.



View by: Options are:

- **View all available routes** - This displays all routes available to be used on your VPN.
- **View routes that will apply to Local Machine Only Access** - This displays all routes available to the one machine connecting to the VPN.
- **View routes that will apply to Local Network Access** - This will display potentially more routes than for Local Machine Only because it will include the necessary routes to allow machines networked to the primary VPN machine to use the VPN.

Detailed Route Information:

Destination - This is the IP address or DNS name of the machine you're trying to connect to through the VPN or locally.

Mask - This denotes the subnet the route is on.

Status - This will either be 'Published', 'Not Publishable' or 'Not Published'.

Published

A route that has a status of "Published" will be used by the WinGate VPN.

Not Published

A route that has a status of "Not Published" can potentially be used by the WinGate VPN, but is not normally published by the local participation mode you have selected. You have the option of forcing this route to be published. Normally, you will not need to publish any of these routes unless you have a specific configuration that demands it.

Not Publishable

A route that has a status of "Not Publishable" cannot be used by the WinGate VPN as core networking relies on it.

Please note that all machines wanting to access the VPN through your hosting / joining VPN must be able to access the remote network through the primary VPN machine. This can be achieved in three ways:

1. By installing the RIP Client on each machine who will participate through the primary VPN machine
2. By ensuring that the primary VPN machine is the default gateway for all the machines that will be accessing the VPN.
3. By manually adding static routes between all machines that will be accessing the VPN and the VPN machine.

You can quickly determine if machines are able to use the VPN by checking their status in the network window.

VPNs to Join

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

Use this tab to enter connection details about the VPN you are joining. (This step may be bypassed if you are importing the configuration of the VPN you are joining – in this case these fields get populated automatically).

VPNs to join : Auckland VPN

Join a VPN

1. Remote Server

Server IP or DNS Name: 202.180.113.234

Server Port: 809

Name of Remote VPN: Auckland VPN

Server SSL Fingerprint: OOHRJRJ NFDSERT UIAWQSD SSEFGGG

2. User Authentication

Username: Administrator

Password: xxxxxxxx

3. Connection Options

When to Join VPN: Manually ☒ Reconnect

Local Participation: Local network Customise routes

Tunnel Creation: Allow tunnels to/from all nodes

Help OK Cancel Apply

Server IP or DNS Name - Enter the name of the VPN server you are joining. This may be an IP address (as above) or a DNS name such as vpn.qbik.com. The name must be resolvable to an IP address, either by DNS server or by a HOSTS file.

Server Port - Enter the port number that will allow you to connect to the host. 809 is the standard port to connect on.

Name of Remote VPN - Enter the name of the VPN host on the server you are connecting to.

Server SSL Fingerprint - This is the code used by the client to correctly identify the host. This should be requested from the VPN administrator, or imported along with the rest of the VPN's configuration .

Username and Password - This will validate and identify you to the host. No connection will be permitted without the correct username and password. **Note:** this is your WinGate username and password, rather than your Windows details.

When to Join VPN - Choose when you want to access the VPN. Your options are:

- 'On engine start' (you will have access to the VPN when the WinGate engine starts)

- 'Manually' (you will have access to the VPN only when you decide to connect to it)
- 'Disabled' (you cannot access the VPN)

Reconnect – Force the VPN to reconnect when it loses the connection. The VPN will attempt to reconnect once per minute unless the host has disconnected it manually or the user has disconnected the VPN manually.

Local Participation - Choose the access level you want in the 'Local Participation' field. Your options are:

- 'No local participation' (allows remote clients to join the VPN and communicate with each other, but not access the VPN host itself)
- 'Local machine only' (allows remote clients to access the VPN host itself, but not the network connected to it)
- 'Local network' (if you want the remote clients to have full access to the network).

Customise Routes - Click the [Customise Routes](#) button to define customisation options for your network.

Tunnel Creation - Your options are:

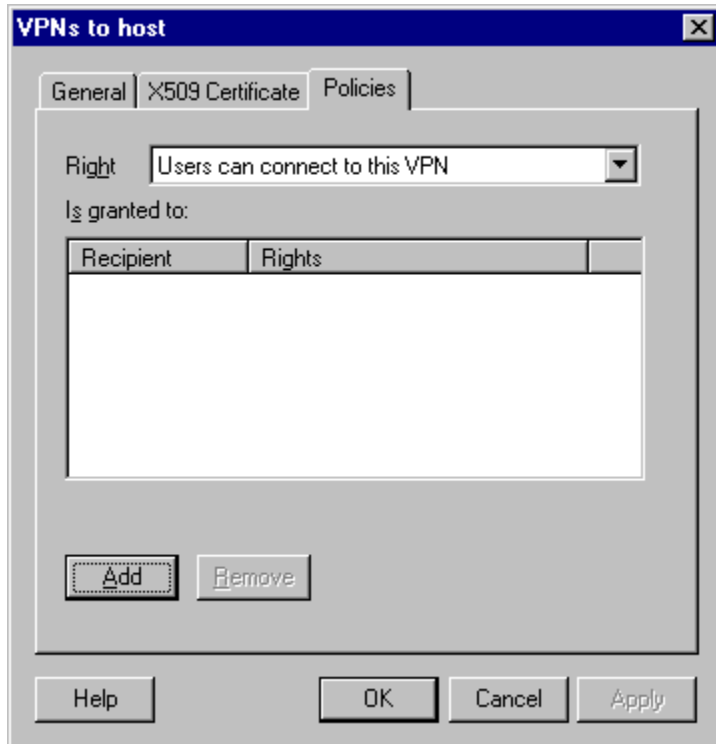
- 'Allow tunnels to/from all nodes'
 - § this allows a tunnel of communication between all participants in the VPN
- 'Allow a tunnel only to the master node'
 - § this allows tunnels of communication only to the host of the VPN and will deny access to/from other nodes attached to the master.

For more information about tunnels, click [here](#).

It is recommended that the first time you connect to a particular VPN, you do so *manually*. This involves right clicking on the VPN you have joined in GateKeeper and selecting 'Connect'.

Policies Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining at VPN.

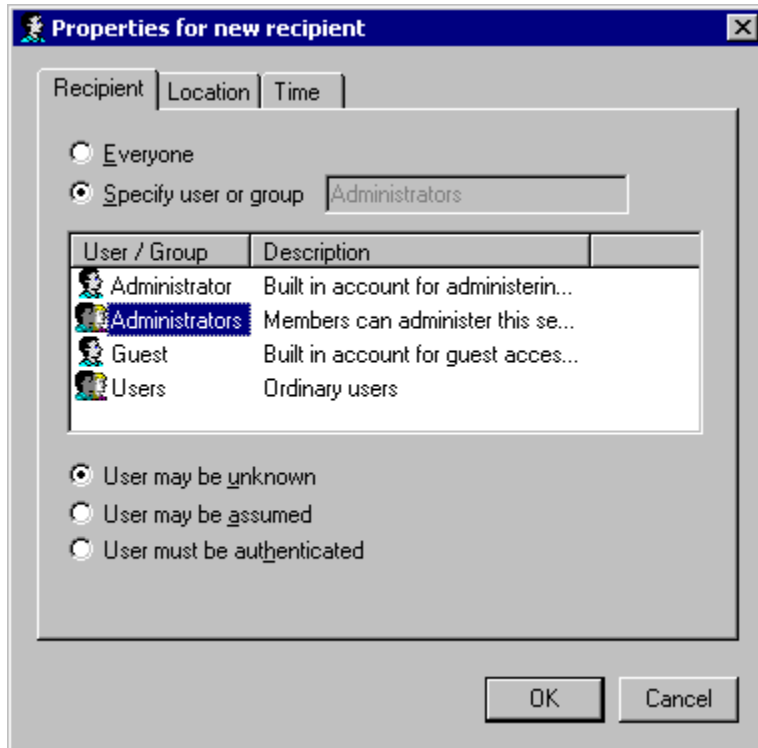


Use the above screen to enter policy details governing who is able to join the VPN you're hosting.

Click the 'Add' button to bring up the [Properties for New Recipient](#) screen.

Properties for New Recipient

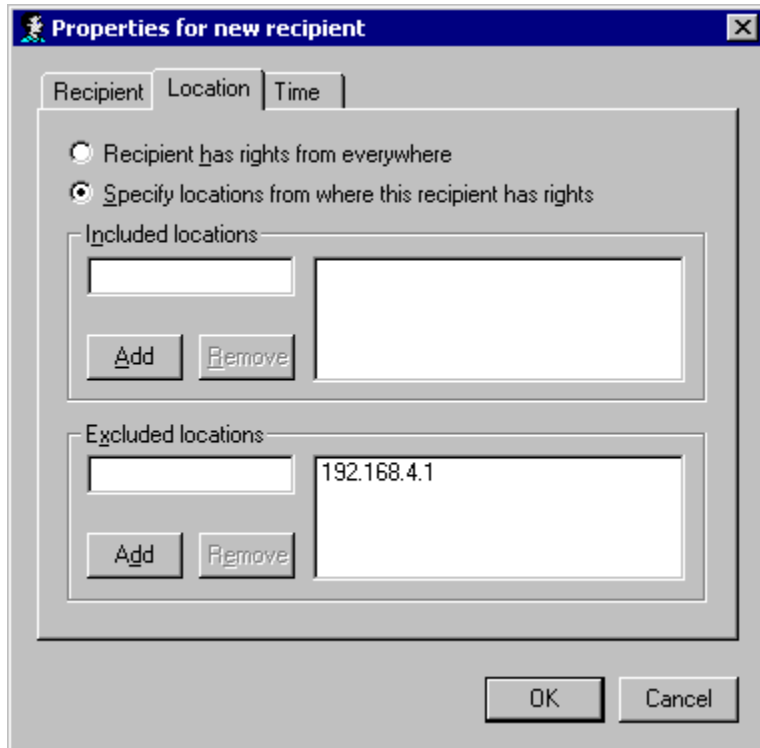
Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



Use the check boxes to specify whether a user or group accessing the VPN may be unknown, assumed or must be authenticated.

Location Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

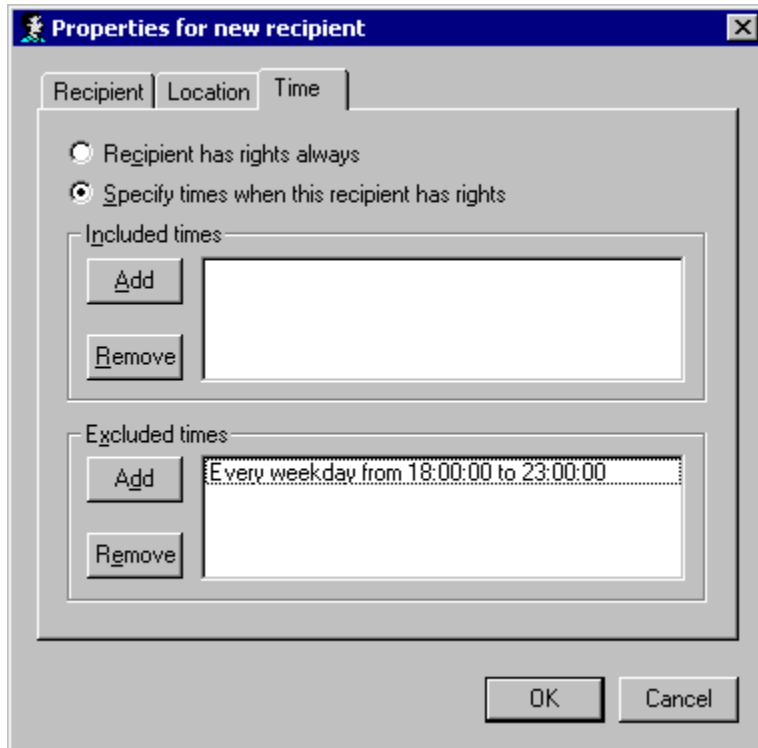


The screenshot shows a Windows-style dialog box titled "Properties for new recipient". It has three tabs: "Recipient", "Location", and "Time". The "Location" tab is currently selected. Inside the dialog, there are two radio buttons: "Recipient has rights from everywhere" (which is unselected) and "Specify locations from where this recipient has rights" (which is selected). Below the radio buttons, there are two sections. The first section is labeled "Included locations" and contains an empty text input field, an "Add" button, and a "Remove" button. The second section is labeled "Excluded locations" and contains an empty text input field and a "Remove" button. To the right of the "Excluded locations" input field, the IP address "192.168.4.1" is listed. At the bottom of the dialog, there are "OK" and "Cancel" buttons.

Click the 'Add' and 'Remove' buttons to specify the locations from which the recipient has access rights. This location must be in the form of an IP address.

Time Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



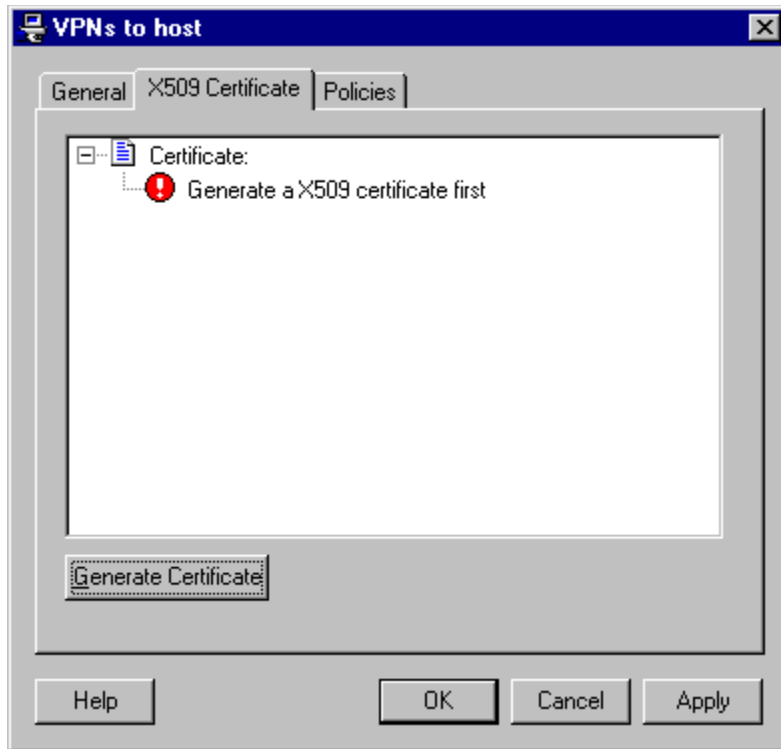
The screenshot shows a Windows-style dialog box titled "Properties for new recipient". It has three tabs: "Recipient", "Location", and "Time", with the "Time" tab currently selected. Inside the dialog, there are two radio buttons: "Recipient has rights always" (which is unselected) and "Specify times when this recipient has rights" (which is selected). Below these, there are two sections: "Included times" and "Excluded times". Each section has an "Add" button and a "Remove" button next to a text input field. The "Included times" field is empty. The "Excluded times" field contains the text "Every weekday from 18:00:00 to 23:00:00". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Click the 'Add' and 'Remove' buttons to specify what times of the day that the recipient has access rights to the VPN.

Security with the WinGate VPN

WinGate VPN authentication is achieved using certificates. Click [here](#) to find out more about certificates.

Clicking the [X509 Certificate](#) tab on the VPN Configuration screen will bring up the following screen. Use this screen to start generating the certificate for your VPN – this will be the standard by which others will identify and authenticate themselves to the host VPN.



Note that this certificate has not yet been generated. You will need to generate one in order to set-up an authentication process for your VPN.

Click [Request Certificate](#) to proceed.

Encryption/Generator Used

Record the details of the private key on this screen.

Key type : RSA

Encryption: 3DES in EDE CBC mode

Options: Use 65537 for the exponent

A smaller exponent results in faster operation, but a weaker key

Size: 1024 bits

Passphrase: xxxxxx

Confirm: xxxxxx

For optimal security you should make your passphrase approximately 128 characters long

< Back Next > Cancel Help

RSA - This is the standard protocol for cryptographic applications. Read about it [here](#).

Encryption - There are three options in this drop-down box. They are:

- DES in CBC Mode (fast but rather weak, susceptible to a brute force attack, particularly with computers becoming more and more powerful)
- 3DES in EDE CBC Mode (the same as the above but done 3 times with 3 different keys – slower but reasonably secure)

Options - An exponent is a quantity representing the power to which some other quantity is raised. Read more about exponents [here](#).

The two options from this drop-down box are:

- Use 65537 for the exponent
- Use 3 for the exponent

Note that there is a trade-off between security and speed. A smaller exponent (in this case 3) means a faster, but less secure, operation.

Size - This refers to the size of the private key, expressed in bits.

Passphrase and Confirm - These fields must match. The passphrase is used to decrypt the private key from persistent storage. The longer the passphrase is, the more securely it will be stored.

Click 'Next' to proceed. The [Details of the Certificate](#) screen will appear.

Details of the Certificate

Use this screen to enter details of the certificate.

Details of the Certificate

Country: New Zealand

State / Province: North Island

Locality (City) : Auckland

Organization: Qbik

Organization Unit:

Common Name:

Email Address: admin@qbik.com

Certificate Expires: 7/ 6/2005

< Back Next > Cancel Help

This is a typical example of the information usually presented in a VPN Certificate. Note that only the two drop-down fields are mandatory.

The 'Country' field defaults to 'Neutral Zone'.

When generating a certificate, the 'Certificate Expires' field defaults to today + 5 years. Sometimes however, you will want a certificate to last a much longer time than this – perhaps as long as 10 years.

The other fields are not compulsory. However, it is not usual to have a certificate without most of the information displayed above. In particular, you will probably want to fill out the following fields:

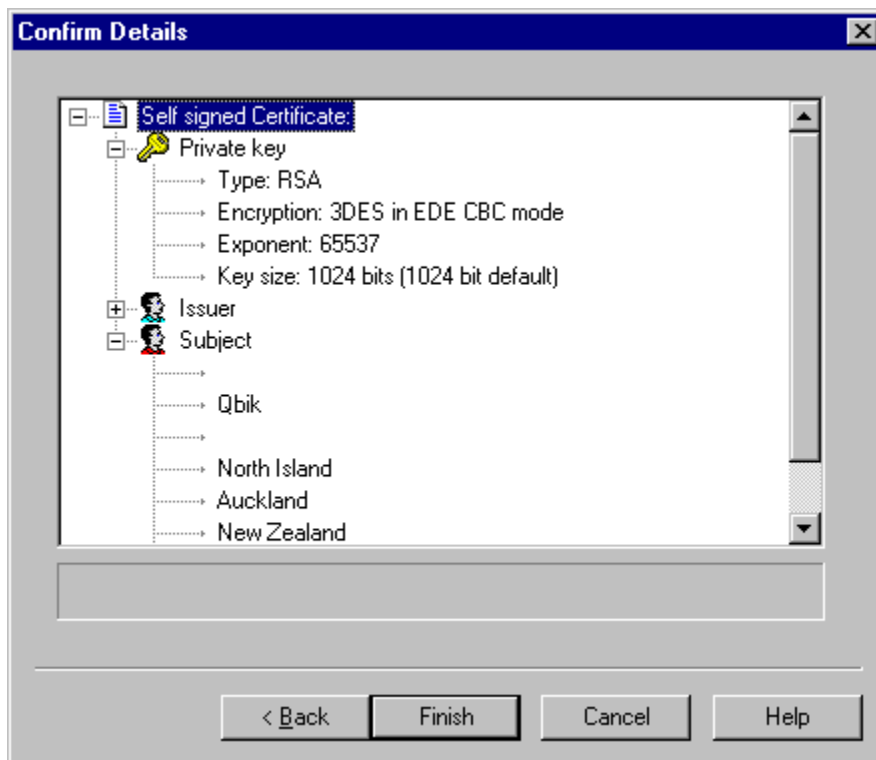
- Organization (for the company who is operating the VPN)
- Organization Unit (for the department within that company)
- Common Name (for the user-friendly name by which others can recognise the VPN)

Click 'Next' to proceed. The [Confirm Details](#) screen will appear.

Confirm Details

Use this screen to view the details of the certificate you are requesting. If all details are correct, click 'Finish'. If not, click 'Back' to go back and amend them.

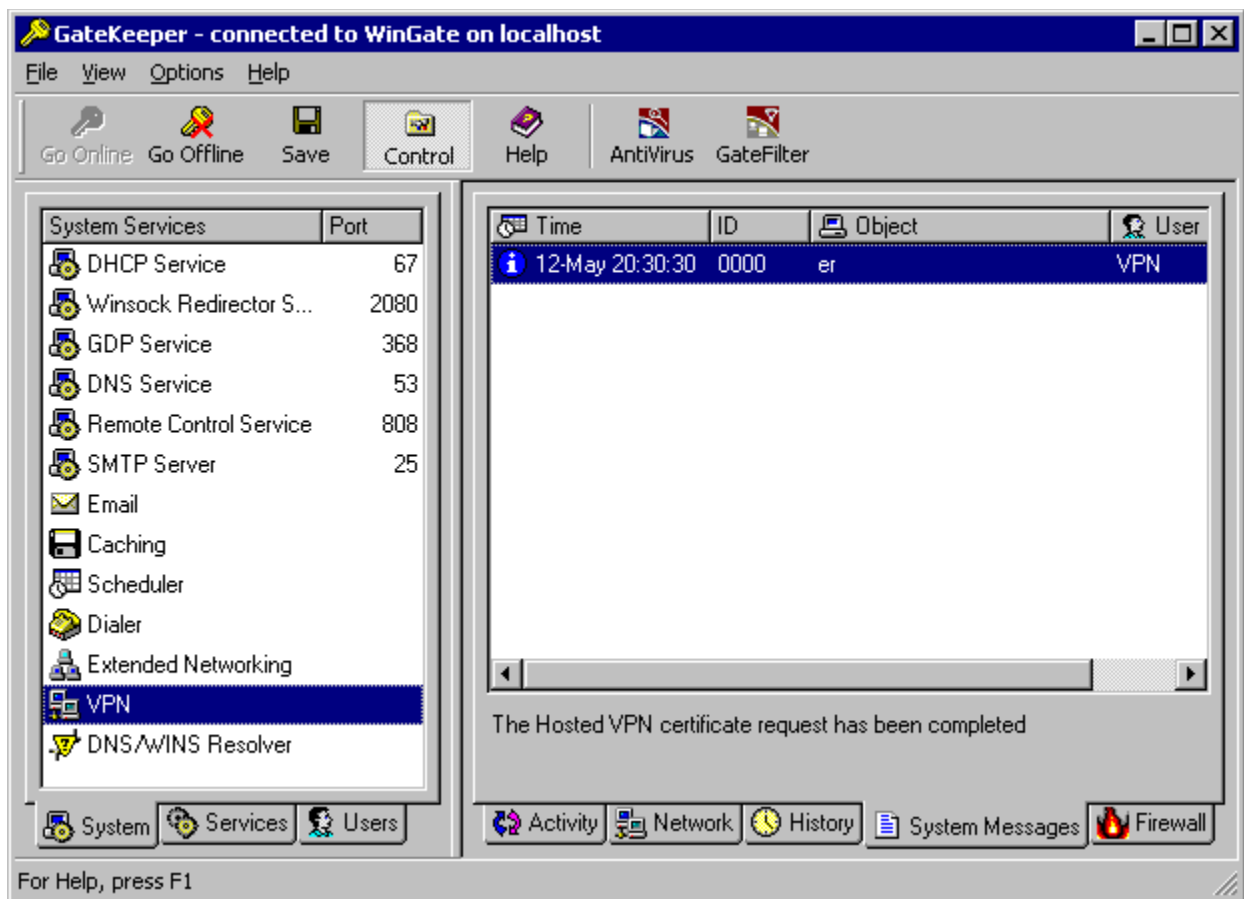
The screen below is an example of the Confirm Details screen with the 'Private Key' menu expanded.



Clicking 'Finish' will take you back to where you started, but with an authenticated certificate e.g.

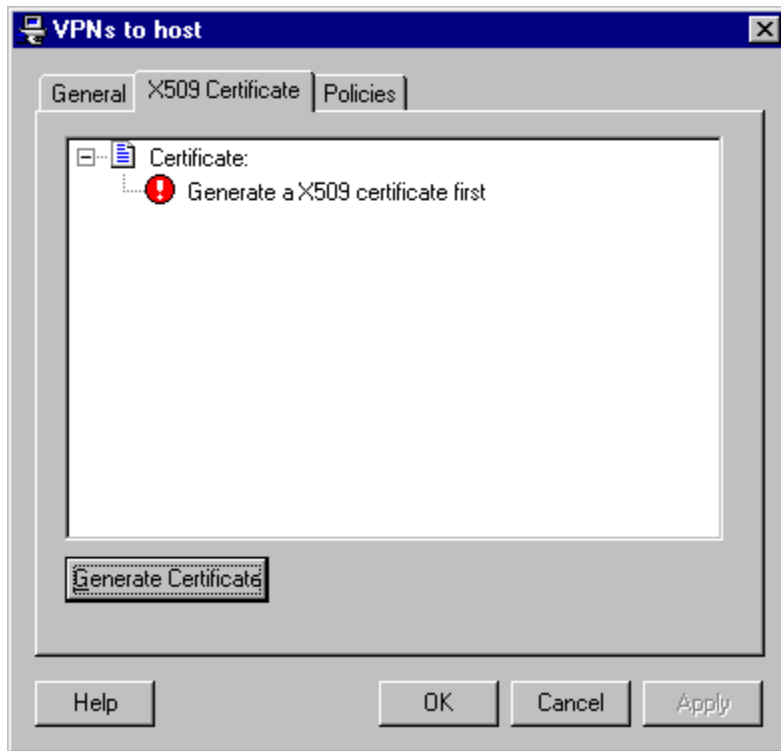


This will also be displayed on the main GateKeeper screen e.g. the text "The Hosted VPN certificate request has been completed" in the screen below-



X509 Certificate

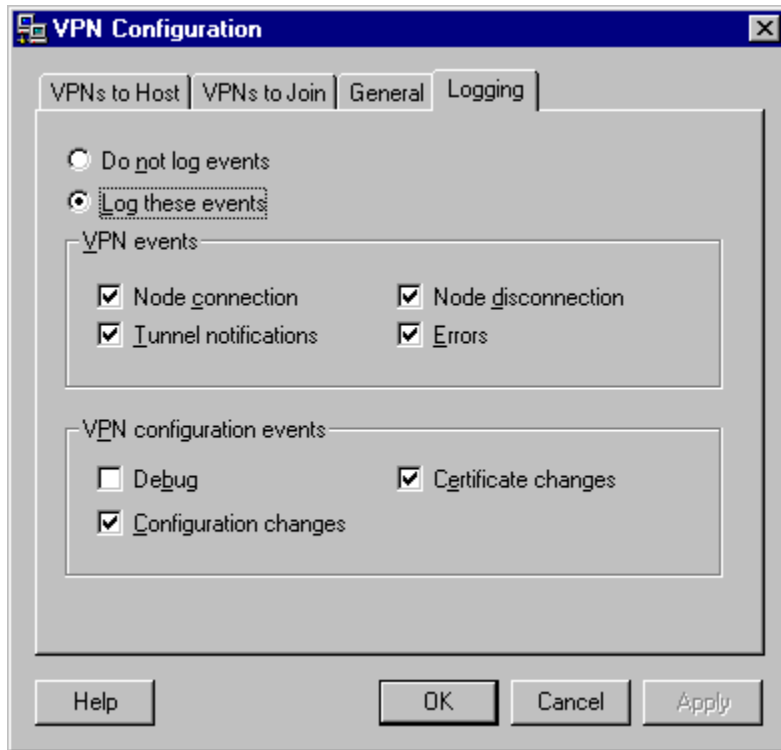
This is the screen where you start to generate the certificate for your VPN. Click 'Generate Certificate' to begin this process. The [Encryption/Generator Used](#) screen will display.



VPN Logging Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

The main purpose of this tab is to help configure the logging options that will be applied to the WinGate VPN.



The screen shows the default settings for the WinGate VPN logging configuration. Please note that these options apply to all the configured VPNs.

Do not log events / log these events - This option allows you to turn logging on (Log these events) or to turn logging off (Do not log events). If you have logging enabled, you can still turn individual events on and off.

Node connection – Any events dealing with the connecting of a node will be logged. This includes connection establishment between the VPN Host and the VPN Client and any other connected nodes and any protocol negotiations.

Node disconnection – Any events dealing with the disconnecting of a node will be logged. This includes disconnecting from the VPN Host, and any participating nodes leaving the VPN.

Certificate changes – Any changes to the certificate of the Hosted VPN is logged

Tunnel notifications – The establishment of a tunnel or any changes to a tunnel will be logged. This includes any tunnel requests that are denied because of a node's local participation or it's allowed tunnel creation.

Configuration changes – Any changes to the VPN configuration, excluding certificate changes, that will affect connectivity are logged.

Errors – Significant errors are logged

Debug – A special logging mode that logs debugging information. This is to assist the support team in tracking down problems.

VPN Troubleshooting

The following is a list of error messages that may be returned from VPN screens or common problems with the VPN setup. Each of these error messages comes with a suggested fix.

The server certificate fingerprint does not validate

Suggested Fix-

The fingerprint is a public identifier of the server. This is your easiest way to authenticate the server's identity. If you receive this error message, it means that:

- a) the fingerprint you entered when configuring the VPN you're joining was incorrectly entered. Check that this value is correct. Please remember, this value is case insensitive. Also, 0 (zero) sometimes looks a lot like O (the letter) – mixing these up is a common mistake. (**Note:** it will never be the letter 'O' – the fingerprint only uses the letters A - F). Or-
- b) the server has changed its certificate. In this case, you should contact the hosted VPN's administrator to obtain a new certificate.

No response to username and password authentication

Suggested Fix-

This message is displayed when the server fails to respond to your login. It does not mean that the TCP/IP connection has been closed, but that some server-side problem prevented it from responding with the appropriate data. There is nothing you can do from your end to remedy this problem. Contact your system administrator.

Invalid username and password

Suggested Fix-

The username and password combination is used after a secure connection has been established and after you've verified the server's fingerprint. If you get this message, it means that either the username, or the password you specified on the VPN to Join screen, are incorrect. This could commonly be caused by typing mistakes.

If you are sure that the values you entered are correct, you should contact the VPN administrator. It could be that your account has not been given access to the VPN, or that your account is not fully enabled.

Connection refused or Connection to remote host timed out

Suggested Fix-

These error messages happen before the SSL connection is established. It means that a TCP/IP connection could not be established by the remote server. First, check that you can connect to the server by some other mechanism (e.g. running the 'ping' or 'tracert' command). If the server is online, a firewall or other problem might be preventing incoming connections. You may need to contact the VPN administrator for more information on this.

Unable to connect using SSL

Suggested Fix-

This message indicates a problem on the server. It means that the server's internal certificate and key-pairs are mismatched, and are generally indicative of some form of tampering. If you see this message, you should contact the VPN administrator and ask them to verify their security set-up. It could also be displayed if there are problems negotiating the details required to instantiate the secure connection.

Socket Error 10049 (Thd 1212) (socket #6E), 0.0.0.0:1242 to :0) (for example)

Error messages that look like this are indicative of a failure in the underlying socket system. The most likely cause of a message like this is a programming fault. You should take note of the exact message and contact your system administrator.

Unable to browse the remote network

This is normally caused by incorrect routing setup. For WinGate VPN to function, the VPN computer must be able to route any network packets between the appropriate client and the remote VPN. There are several alternatives for fixing this problem.

1. Ensure that the default gateway for each of the client computers is set to the WinGate VPN computer. This routes all network traffic through the WinGate VPN computer.

2. Install a RIP version 2 compatible listening program on the client computer(s). WinGate VPN will broadcast all published routes for RIP listeners.
3. Add static routes between the WinGate VPN computer and the appropriate clients.

You will also need to ensure that any intermediate firewalls and routers used by your organization in-between the VPN computer and the Internet have the appropriate holes and routing setup done. If your connection is being translated, you will be able to see this in the [Network Window](#).

Duplicate names detected on network

In the first case, this might be an actual conflict. Please ensure that each end of the VPN connection (And potentially other nodes joining the same VPN) have unique computer names.

If the duplicate name conflict continues to occur, please verify the status of any WINS servers running on the network and ensure that their cache is cleaned of any duplicate machine names. You should also ensure that the NETBIOS protocol is not bound to your external interface unless you absolutely need this.

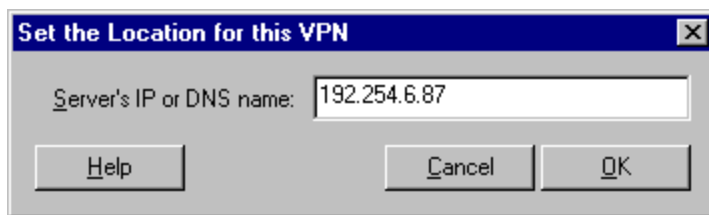
Export Configuration Files

The WinGate VPN allows the exporting and importing of configuration files, to make hosting and joining VPNs much easier.

The following information will be distributed:

- Server name (IP address and port or DNS name and port)
- VPN name
- Fingerprint

If you are hosting a VPN, and want others to join, click the 'Export Config' button on the VPNs to Host tab. This will bring up the 'Set the location for this VPN' window.



As stated on the interface, the location you define in the 'Server' field may be either an IP address or a DNS name.

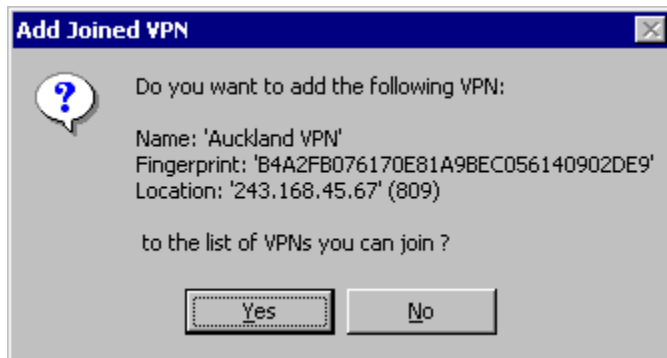
Click OK to open up your windows explorer, where you can save your configuration files. These files may now be distributed to clients, allowing them to join your VPN.

Note: This configuration file will contain no private / sensitive information. You will still have to communicate the username and password to the client by other means.

Import Configuration Files

After you have downloaded configuration files sent to you by the administrator of a host VPN, you may then use these files to join it.

Click 'Import Config' on the VPNs to Join tab to bring up the following dialog-



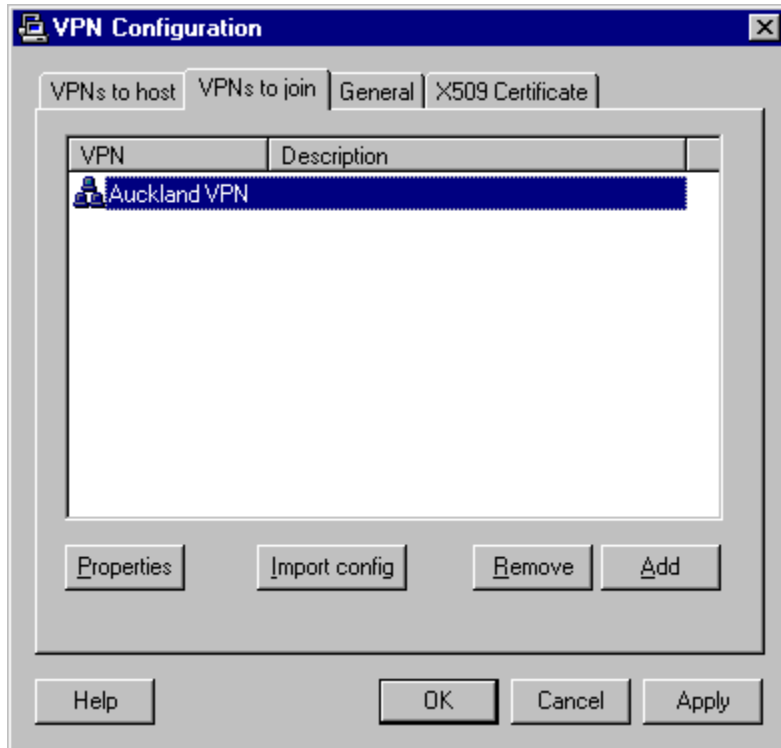
Click 'Yes' to confirm this VPN as one that you can join.

This will open up the [VPNs to Join](#) screen, from which you may proceed to join the VPN.

Note: An alternative way to doing this is opening up the **.vpn** file directly from your Windows explorer. You may open it in a text file (just to view the imported information) or double-click to open the 'VPNs to Join' screen in GateKeeper.

VPNs to Join Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



The above screen displays all the VPNs you are joined to.

Properties - Click on this button to explore details about the highlighted VPN.

Import Config - Click 'Import Config' to import configuration files sent to you from a VPN host administrator. Click [here](#) to learn how to do this.

Add - Click 'Add' to join a new VPN. This brings up the [VPNs to Join](#) screen.

Remove - Click 'Remove' to cease being joined to the highlighted VPN.

Apply - Click 'Apply' to implement all changes made to the information in the screen.

Peer-to-Peer VPNs

The WinGate Peer to Peer VPN is a more informal VPN between two parties which has no predefined hosting or joining, only periodic connections from each endpoint allowing access to shared network resources.

How is it different from a 'normal' VPN?

The Peer-to-Peer VPN offers no 'VPN to Host' or 'VPN to Join' options because, as the name suggests, members of this kind of VPN are considered peers – there is no master-slave relationship here.

Limitations -

- Peer-to-Peer VPN is only available to two parties at any one time.
- When neither member of a VPN has a static IP (i.e. both receive randomly generated IP numbers during each of their dial-up Internet sessions), DNStoGo is necessary to connect to the VPN. You can download a free copy of DNStoGo [here](#).
- If you do not wish to use DNStoGo, you must find some other, more manual method of letting your VPN peer know what your IP is. You can find out your own IP by opening an Internet session and then selecting 'Run' from the Start menu and typing-
 - winipcfg (for Windows 95/98), or
 - ipconfig (for Windows NT, 2000, ME or XP).

Peer-to-Peer General Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

Enter general details about your VPN on this screen.



The screenshot shows a 'VPN Configuration' dialog box with a blue title bar and a close button. It has four tabs: 'General', 'X509 Certificate', 'Policies', and 'Connecting'. The 'General' tab is active. It contains the following fields and buttons:

- VPN Name:** A text box containing 'Mike's VPN'.
- Node name:** A text box containing 'Local network of BOB'.
- Description:** A large text area containing 'A peer to peer VPN'.
- Control channel port:** A spin box set to '809'.
- Data channel port:** A spin box set to '809'.
- Buttons:** 'Import Config' and 'Export config' are located to the right of the port spin boxes. At the bottom of the dialog are 'Help', 'OK', 'Cancel', and 'Apply' buttons.

VPN Name - Enter the 'Name' of the VPN you are setting up. This is the name that nodes must use in order to make the connection. It must match the 'official' name of the host VPN.

Node Name - This is the name of the individual machine as represented on the VPN network.

Description - This is not a mandatory field.

Control Channel Port - This is the port for communication between VPN nodes. The default port is 809.

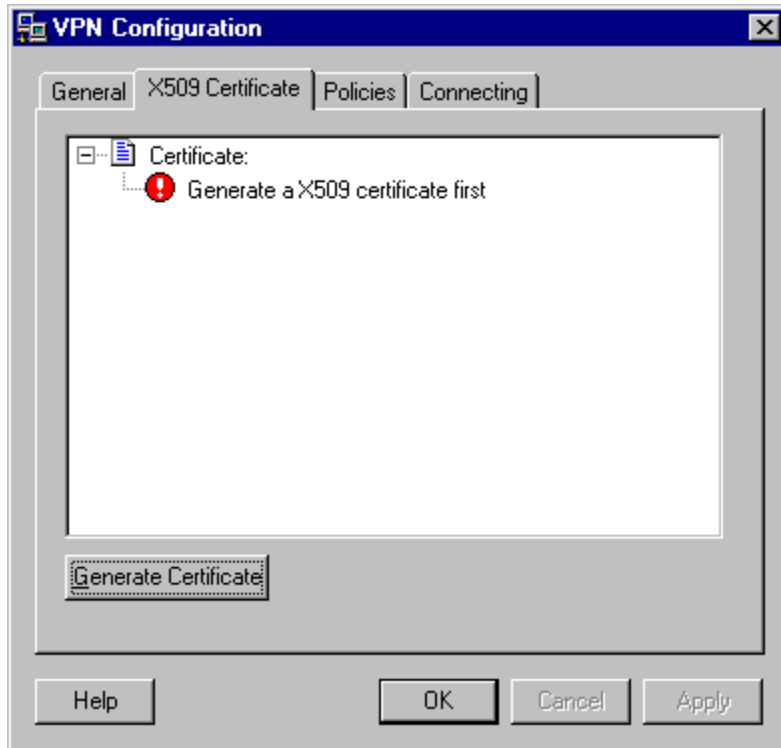
Data Channel Port - This is the port that handles network traffic across the VPN. Likewise, default is 809. Every node connected to the VPN must have the same ports selected if they are to participate in any exchange of data.

Import Config - Click [here](#) to find out how to import configuration files.

Export Config - Click [here](#) to find out how to export configuration files.

Peer-to-Peer X509 Certificate Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



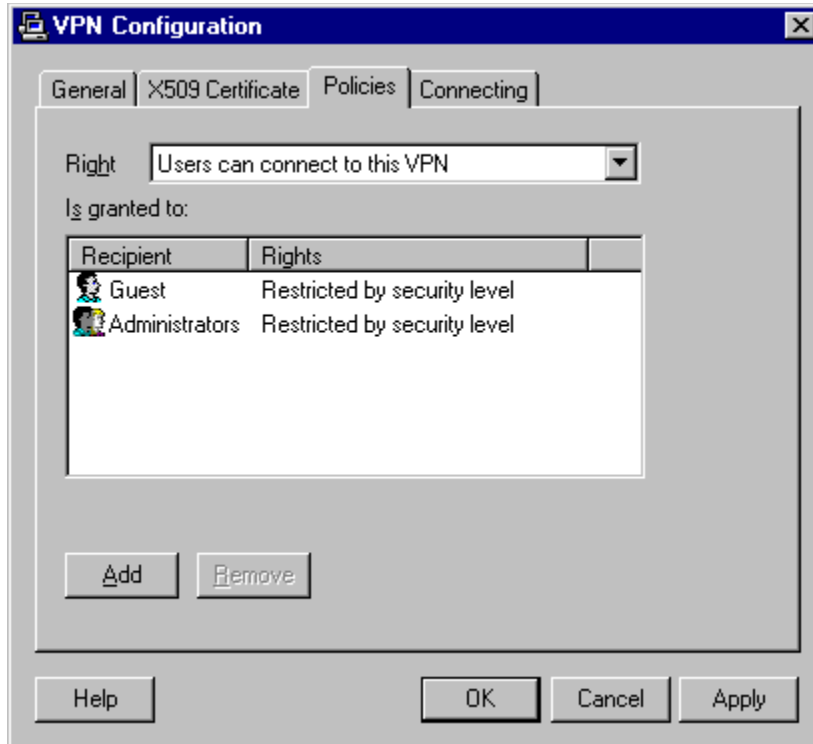
Generate Certificate – Click this button to generate a certificate for your VPN.

Import – Click [here](#) to find out how to import configuration files.

Export – Click [here](#) to find out how to export configuration files.

Peer-to-Peer Policies Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.



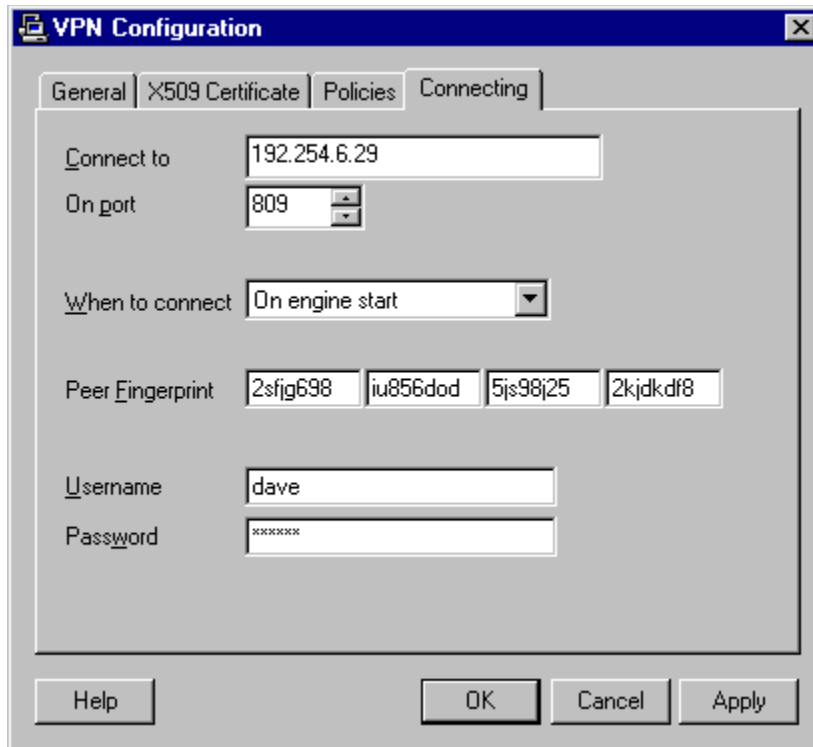
Use the above screen to enter policy details governing who is able to join the VPN you're hosting.

Click the 'Add' button to bring up the [Properties for New Recipient](#) screen.

Peer-to-Peer Connecting Tab

Click [here](#) for a [Step by Step Guide](#) to hosting and joining a VPN.

Use this tab to enter connection details about the VPN you are joining.



The screenshot shows a 'VPN Configuration' dialog box with a blue title bar and a close button. It has four tabs: 'General', 'X509 Certificate', 'Policies', and 'Connecting'. The 'Connecting' tab is selected. The dialog contains the following fields and controls:

- Connect to:** A text box containing the IP address '192.254.6.29'.
- On port:** A spin box set to '809'.
- When to connect:** A dropdown menu currently showing 'On engine start'.
- Peer Fingerprint:** Four text boxes containing the characters '2sfig698', 'iu856dod', '5js98j25', and '2kjdkdf8' respectively.
- Username:** A text box containing the name 'dave'.
- Password:** A text box filled with masked characters (asterisks).

At the bottom of the dialog are four buttons: 'Help', 'OK', 'Cancel', and 'Apply'.

Connect to - Enter the IP number of your VPN peer.

On port - Enter the port number you wish to connect to the VPN on.

When to connect - You have three options as to when to connect to the VPN.

1. On engine start
2. Manually
3. Disabled

Peer Fingerprint - This is the code used by VPN members to identify themselves to one another. This should be requested from the VPN administrator, or imported along with the rest of the VPN's configuration.

Username and Password - This will validate and identify you to your VPN peer. No connection will be permitted without the correct username and password.

Installing VPN Only GUI

This guide is intended for people installing this version of WinGate VPN. It is *strongly recommended* that you read the entire guide before installing WinGate VPN. This is because WinGate VPN may not work unless you install it on the right computers and in the right order. Following the steps below will help you to complete a successful install first time.

We also encourage you to be familiar with our [recommended setup](#) before you begin installing WinGate VPN. This will prevent backtracking later on. Following this you should be ready to install WinGate VPN on your network. Follow these steps carefully to ensure an easy and trouble free install:

- ü [STEP 1](#) **Setting up a working network**
- ü [STEP 2](#) **Setting up the WinGate VPN server**
- ü [STEP 3](#) **Installing or upgrading to this version of WinGate VPN**
- ü [STEP 4](#) **Setting up the VPN**

Refer to the Step by Step guide for more information. This can only be done once you've installed the product.

If you already have a working network, you will find this installation simple. This guide is organized so that you can follow each installation step in the order that you should do it. Once you have completed a step, click on the toolbar button labeled >> to move to the next required step.

Note:

If you purchased a computer that has WinGate VPN installed already, you will not need to follow this install process because WinGate VPN will already be setup to work correctly.

STEP 1: Setting Up A Working Network

You must have a working network before you can install WinGate VPN. This network can be Ethernet, Token-Ring, FDDI, etc. as long as it uses the TCP/IP protocol.

Before beginning to install WinGate VPN, you should [test to see that TCP/IP is working properly](#) by 'pinging' each computer on your network.

à [Click here](#) to return to the install menu.

STEP 2: Setting up the WinGate VPN server

The requirements for installing or upgrading to this version of WinGate VPN are very basic. Note that if you are upgrading from a working version of WinGate VPN then you should not need to alter your existing setup. We recommend that you change the Windows network name for this computer to 'WINGATE VPN' (this is only for ease of identification and is not necessary).

Your **WinGate VPN server** must meet the following basic requirements:

- Windows 95, 98, NT (version 4.0 or later), 2K or XP.
- If running Windows NT, we recommend you have a minimum of [Service Pack 4 installed](#)
- [A direct connection to the Internet](#)
- [TCP/IP installed](#)
- [TCP/IP configured for WinGate VPN](#)
- [WinSock2 installed](#) (only if computer is running Windows 95).

Once the computer meets these requirements, you are ready to begin a clean install of WinGate VPN, or upgrade an existing install to a later version of WinGate VPN. If you already have a working version of WinGate VPN, then we recommend that you *upgrade* to preserve your existing configuration.

à [Click here](#) to return to the install menu.

STEP 3: Installing or upgrading WinGate VPN

Once the WinGate VPN server is ready, you must decide whether to do a clean install, or upgrade an existing copy of WinGate VPN installed on this computer. If you have another version of WinGate VPN working already, we recommend you choose to upgrade (this means you can retain your existing configuration). *If you do not do this you will **lose** any previous configuration.*

- [Begin clean install of this version of WinGate VPN](#)
- [Begin upgrading to this version of WinGate VPN](#)

Please note that WinGate VPN cannot be installed over an existing version of WinGate. If you wish to add VPN functionality to your current WinGate installation, please contact your distributor for the appropriate information.

à [Click here](#) to return to the install menu.

Service Pack Requirements

This version of WinGate VPN requires you to have Service Pack 4 or later installed on your WinGate VPN server computer (this applies to both NT Server 4.0 and NT Workstation 4.0).

See the **WinGate VPN Info** link (view this from the *WinGate VPN program group* under the *Start Menu*) – ‘**downloads**’ section, to learn where you can get the required patch from.

Direct Connection to the Internet

It is essential that the chosen WinGate VPN server have a direct connection to the Internet. It can be a dial-up account held with an ISP, an ISDN line, a T1 leased line or any other method, which provides a computer with direct connectivity to the Internet.

Note that the performance of WinGate VPN will be directly affected by the speed of the Internet connection you are using. Therefore, we recommend that you purchase the best connection that you can afford.

Installing TCP/IP on the WinGate VPN server

Installing TCP/IP is one of the most important requirements for using WinGate VPN. Both the WinGate VPN server and client computers (whether running Windows, MacOS, Unix or Linux) must have this networking protocol installed. It is usually bundled free with your operating system.

Important Note:

- If you have a working Internet modem setup then you already have TCP/IP installed and therefore this step may be skipped
- You may be asked for a disk to install the software from. This will be the CD or disk for your operating system (e.g. a Windows CD).

In Windows 95 or 98

1. Press the **Start** button
2. Select *Settings /Control Panel*
3. Double-click the **Network** icon
4. To install TCP/IP, click the '**Add...**' button
5. Double-click **Protocol**, then select **Microsoft**
6. Select **TCP/IP** and click **OK**.

(** You will be asked to restart your computer **)

In Windows NT4

1. Press the **Start** button
2. Select *Settings / Control Panel*
3. Double-click the **Network icon**
4. To install TCP/IP, choose **protocol**
5. Click **Add**
6. Select **TCP/IP Protocol** and click **OK**.

(** You will be asked to restart your computer **)

In Windows 2000

1. Press the **Start** button
2. Select **Network and Dialup Connections**
3. Double-click the '**Local Area Connection**' icon
4. Click on the '**Install...**' button
5. Select **Microsoft**, then **TCP/IP Protocol**
6. Click **OK**.

(** You will be asked to restart your computer **)

In Windows XP

TCP/IP is installed by default on Windows XP. It cannot be removed.

This step is not required.

à [Click here](#) to return to the install menu.

Configuring TCP/IP for the WinGate VPN server

Because of the way WinGate VPN works, you'll need to assign a special (known as static) IP address to the WinGate VPN server. We strongly recommend **192.168.0.1** and we will refer to that number from here on. If you are not using this number, or any of the defined private addresses allocated by the InterNIC (the governing body that allocates all Internet addresses), then you may run into conflict problems. This should be relatively rare however.

There are five or six sections in this dialog box. We'll deal with each of them in order:

IP Address Select the '**Specify an IP address**' option. Then type in **192.168.0.1** as the IP address. This is a private address that won't exist anywhere on the Internet, so you can let the WinGate VPN server use it for the internal LAN only. Next, fill in the '**Subnet Mask**' text area with **255.255.255.0**

WINS Configuration

Leave this as is.

Gateway Leave this entry blank even if you intend to use the NAT.

Bindings By default, the Client for Microsoft Networks option is checked. Leave it alone.

Advanced No changes are needed from the default.

DNS Configuration

Select the '**Enable DNS**' option. Enter your user name in the Host box. In the Domain, put in the name of your ISP, like abc.com or partyon.com or whatever.

In the DNS Server Search Order section, put in the IP address of your provider's name server and press the '**Add**' button. It should already be there, so don't add it again if it is. To find this number if you have a shell account on your ISP's server, you can log into your provider with a terminal program (telnet) and type 'nslookup'. Your provider's server will return the DNS address. If that doesn't work, you can use 131.107.1.7 and/or 204.95.111.254 (those belong to Microsoft).

In the Domain Suffix Search Order section, type in the domain suffix (usually the same as the domain) and press the Add button.

When you're all done setting these options, press the **OK** button. Then press the **OK** button in the **Network** dialog box. Windows will ask you to reboot. Press '**Yes**' and wait for your computer to restart.

à [Click here](#) to return to the install menu.

Installing WinSock 2

Some versions of Windows 95 will not have WinSock 2 installed (it is standard with 98, NT4 and 2000). You will have to install it before you can install WinGate VPN on this computer. WinSock 2 provides your applications with special network functionality.

You can download the WinSock 2 extension for free from the Microsoft web site (www.microsoft.com) or alternatively from the WinGate website.

<http://www.wingate.com>

à [Click here](#) to return to the install menu.

Clean Install of WinGate VPN

Important Notes About Installation:

- Make sure that your selected WinGate VPN server meets the [requirements outlined here](#)
- WinGate VPN does not require any software to be installed on your client computers. (Computers on your local area network)

To begin a clean install, answer the question below and then follow the instructions carefully.

What did you run on your network prior to this WinGate VPN version?

- **No proxy server or gateway at all**

Run the installer program on your selected WinGate VPN server.

- **Any other version of WinGate VPN**

1. Uninstall the old version. This will effectively lose all of your previous configuration and settings (if you do not want to lose these we recommend you do an upgrade installation). To uninstall, select '**Uninstall WinGate VPN**' from the *WinGate VPN program group* under the *Start menu*
2. Run the install program on your selected WinGate VPN server.

- **Another proxy server product e.g. Microsoft Proxy Server 2.0**

We recommend removing any other proxy server software, as it is likely to conflict with WinGate VPN (i.e. services will attempt to run on the same ports). However, this is not absolutely required – it is possible to run any number of proxy server products on the same computer.

Was the clean install successful?

WinGate VPN runs "invisibly" as a Windows Service. This means it won't appear as an application on your desktop. The file WinGate VPN.exe does the actual work without interfering with the usability of your computer. The big advantage of services is that they run when Windows starts. No user has to be logged in for services to run, and the operating system does not close them down when a user logs off. The operation of services in 95/98 is a little different than NT, but the same basic operation is achieved.

When the installer has *finished*, the following icon should appear in the system tray:



This indicates that the WinGate VPN Engine Service is running and that the install was successful. Icons will have been added to the WinGate VPN group for stopping and starting this service.

à [Click here](#) to return to the install menu.

Upgrading to WinGate VPN

Bug-Fixes & Minor Enhancements

A range of bug fixes and minor enhancements have been addressed in this WinGate VPN release. You are encouraged to browse these changes and updates by selecting the "WinGate VPN Info" link from the *Start Menu* in the *WinGate VPN program group*.

If you already have a version of WinGate VPN installed, the installer will automatically detect an upgrade and select defaults accordingly. An upgrade will replace the original WinGate VPN program and resource files with updated versions, and configure any new features. It will allow you to keep your existing configuration, but will make changes to accommodate the new features.

Important Notes About Installation:

- Make sure that your selected WinGate VPN server meets the [requirements outlined here](#).
- WinGate VPN does not require any software to be installed on your client computers. (Computers on your local area network)

To begin upgrading answer the question below, then follow the instructions carefully.

What did you run on your network previous to this WinGate VPN version?

There is currently no upgrade path provided for WinGate VPN.

Was the upgrade install successful?

WinGate VPN will run "invisibly" as a Windows Service. This means it won't appear as an application on your desktop. The WinGate VPN.exe file does the actual work without interfering with the usability of your computer. The big advantage of services is that they run when Windows starts. No user has to be logged in for services to run, and the operating system does not close them down when a user logs off. The operation of services in 95/98 is a little different than NT, but the same basic operation is achieved.

When the installer has *finished*, the following icon should appear in the system tray:



This indicates that the WinGate VPN Engine Service is running. Icons will have been re-added to the WinGate VPN group for stopping and starting this service. Start GateKeeper and check to see that all of your settings (policies, groups and users, mapped links etc.) have appeared in the upgraded version.

à [Click here](#) to return to the install menu.

Changes made by WinGate VPN Installation

After installing WinGate VPN you may notice that several changes have been made to your 'Network Settings' on the WinGate VPN Server computer. These settings will not change the normal operation of your system and will be completely restored to their original state if you choose to uninstall WinGate VPN.

Note for users of WinGate VPN on Windows NT 4:

The NAT for Windows NT consists of a low-level driver file, qbikhh???.sys. ?? represents the current operating system. These are placed in the 'drivers' directory under Windows\system32.

Note for users of WinGate VPN on Windows 95/98:

If you choose to uninstall WinGate VPN, your network will be restored to its original state.

Test TCP/IP

Ping is a popular utility that is installed as part of the TCP/IP protocol suite. It is used as a quick and easy method of finding out whether or not another computer is online and responding.

When you "ping" another computer's IP address (or by domain name), you are effectively sending out the message "Are you there?" (this consists of four ICMP packets). If the computer is online and able to respond, it will then send a reply consisting of the same four ICMP packets.

If you try and use the ping command and it fails, you can use Event Viewer to check the event log and look for problems reported by *Setup* or the *Internet Protocol (TCP/IP) service*.

Testing TCP/IP on the Local Computer

You can test whether the TCP/IP installed on a computer is working properly by 'pinging' the loopback address on your computer. You do this by typing **ping 127.0.0.1** at the command prompt.

If **ping** fails, verify that the computer was restarted after TCP/IP was installed and configured.

Pinging Across the Network

(a) 'Pinging' the WinGate VPN server

At the command line type (replacing 192.168.0.1 with the IP of your WinGate VPN server):

```
ping 192.168.0.1
```

The response should be:

```
Pinging [192.168.0.1] with 32 bytes of data
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
```

This is a confirmation that TCP/IP is working properly. This result should be the same from any computer on the network. If this is the case, you can then move on to configuring TCP/IP for either the WinGate VPN server or the client computer.

Note:

If you get:

```
Destination host unreachable
```

or:

```
Bad IP
```

then you need to check your TCP/IP settings as outlined previously.

(b) 'Pinging' a Computer on the Internet

Note that this will NOT work for you until you have completed installing WinGate VPN on your network (because WinGate VPN DNS is required to resolve the URL to an IP address).

At the command line type (or any other reliable web site):

```
ping www.cnn.com
```

Any computer on the network except the WinGate VPN server should produce this response, (although the IP may vary)


```
Pinging cnn.com [207.25.71.29] with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

If you have defined a default Gateway, - with an IP address of 192.168.0.4 in this example, the following response should be produced (at this stage, you do not need to know about the default gateway.)

```
Pinging cnn.com [207.25.71.29] with 32 bytes of data
Reply from 192.168.0.4: Destination host unreachable.
Reply from 192.168.0.4: Destination host unreachable.
Reply from 192.168.0.4: Destination host unreachable.
Reply from 192.168.0.4: Destination host unreachable.
```

This means that WinGate VPN DNS is working properly. The DNS has looked-up the name, and returned the corresponding IP address for that name. You will never get response times for an external computer on the Internet (e.g. www.cnn.com) using a client computer behind WinGate VPN.

Uninstalling WinGate VPN

To Uninstall WinGate VPN from Your System:

- Choose the **Uninstall WinGate VPN** icon from the *WinGate VPN group* in the *Start menu* **OR**
- Open *Control pane* *Add-remove software*/'WinGate VPN Server'/Remove.

Selecting Installation Directory

*This topic refers to the installer dialog **Selecting Installation Directory**.*

This directory is where the WinGate VPN executables and resource files will be installed. This should be a local drive on the Wingate VPN server.

The default directory is:

```
C:\Program Files\WinGate VPN
```

The installer will inform you of the amount of free space on your hard disk.

Start Installation

Begin the Installation Process.

This step begins the installation procedure. It will copy the appropriate files onto your computer and make some adjustments to the various system settings (e.g. Windows registry).

If you have chosen to install the **WinGate VPN**, then the WinGate VPN engine service will start once the install is complete and your computer has been rebooted. You should open the help file and read through the VPN sections. This will show you how best to configure the WinGate VPN computer.

Recommended Network Configurations

MS-Windows Systems

If the client is a PC running Microsoft Windows, we recommend one of the following setup options in order of preference:

1. Enable DHCP so your client computers are automatically assigned IP addresses and default gateway settings.
2. Ensure that the client computer has its default gateway set to the primary VPN machine.
3. Install and use the Qbik RIP Client on the client computers.

Non-Windows Systems

If the client is a computer running anything other than Microsoft Windows (like MacOS, Unix or Linux), we recommend the following setup:

1. Enable DHCP so your client computers are automatically assigned IP addresses and default gateway settings.
2. Ensure that the client computer has its default gateway set to the primary VPN machine.

VPN Glossary

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Algorithm

The term algorithm (pronounced Al-go-rith-um) is a procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa Al-Khowarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. Al-Khowarizmi's work is the likely source for the word *algebra* as well.

A computer program can be viewed as an elaborate algorithm. In mathematics and computer science, an algorithm usually means a small procedure that solves a recurrent problem.

B

C

Certificate

The risks associated with physically publishing keys are obvious. The solution is to have a trusted third party, called a Certificate Authority (CA). The CA publishes a directory signed with the CA's private key. In actual practice, rather than signing a directory, what the CA does is sign individual messages which contain both the name of the key owner and his public key. These messages are generally known as certificates, hence the name Certificate Authority. The primary standard for certificates is X509.

Cipher

A cipher is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself. Its origin is the Arabic *sifr*, meaning *empty* or *zero*. In addition to the cryptographic meaning, cipher also means (1) someone insignificant, and (2) a combination of symbolic letters as in an entwined weaving of letters for a monogram.

Some ciphers work by simply realigning the alphabet (for example, A is represented by F, B is represented by G, and so forth) or otherwise manipulating the text in some consistent pattern. However, almost all serious ciphers use both a key (a variable that is combined in some way with the unencrypted text) and an algorithm (a formula for combining the key with the text). A block cipher is one that breaks a message up into chunks and combines a key with each chunk (for example, 64-bits of text). A stream cipher is one that applies a key to each bit, one at a time. Most modern ciphers are block ciphers.

D

Decryption

Decryption is the process of converting [encrypted](#) data back into its original form, so it can be understood.

DES

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

DSA

The **Digital Signature Algorithm** (DSA) is a Federal Information Processing Standard (FIPS) publication of the National Institute of Standards and Technology of the US Department of Commerce. It is a variant of the ElGamal signature mechanism. The DSA

was designed exclusively for signing / verification (and, therefore, also for data integrity), but other algorithms in the ElGamal family can be used for encryption / decryption (and, therefore, key transfer if what is being encrypted and decrypted is a symmetric key). The security of these algorithms is based on the difficulty of computing logarithms in a finite field. The current state of research with respect to discrete logarithms suggests that DSA keys should be at least 1024 bits long to provide adequate security for the medium-to-long term.

E

Encryption

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a "code," can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a *code* is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

Exponent

An exponent is a quantity representing the power to which some other quantity is raised. Exponents do not have to be numbers or constants; they can be variables. They are often positive whole numbers, but they can be negative numbers, fractional numbers, irrational numbers, or complex numbers.

F

Fingerprint

An authentication tool, a fingerprint is a digest of the host's 'root key'. It is used to verify that the user is connecting to the correct network.

G

H

I

ICMP

ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

J

K

L

Logarithm

A logarithm is an exponent used in mathematical calculations to depict the perceived levels of variable quantities such as visible light energy, electromagnetic field strength, and sound intensity.

M

N

Node

In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes.

O

P

Private Key

In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

Public Key

A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encryption messages and digital signature.

The use of combined public and private keys is known as *asymmetric* cryptography. A system for using public keys is called a public key infrastructure (PKI).

Q

R

RSA

The algorithm proposed by Ron **Rivest**, Adi **Shamir** and Len **Adleman** in 1978, known as RSA, is one of the earliest and most versatile of the public-key algorithms. It is suitable for encryption / decryption, for signing / verification (and therefore, for data integrity), and for key establishment (specifically key transfer). It can be used as the basis for a secure pseudo-random number generator as well as for the security in some electronic games. Its security is based on the difficulty of factoring very large integers. The current state of factoring research suggests that RSA keys should be at least 1024 bits long to provide adequate security for the medium-to-long term.

S

SSL

SSL stands for Secure Sockets Layer. It is the standard internet protocol for managing the security of message transmission on the internet. It utilises the RSA public-and-private key encryption system.

T

Tunnel

A tunnel is a particular type of dedicated connection across a network – allowing nodes on physically different networks to connect to each other as if they were on the same network. VPN tunnels tend to operate across static IPs, using the internet like it was a direct wire between two computers.

Twofish

A block cipher, created by Counterpane Systems for submission to the NIST Advanced Encryption Standard (AES) process.

Twofish is designed to be highly secure and highly flexible. It is well suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Numerous implementation trade-offs allow an implementer to balance performance variables like encryption speed, key setup time, code size, RAM, ROM, and gate count.

Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all users.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

V

W

X

X509

The most widely accepted format for public key certificates. Directory authentication in X.509 can be carried out using either secret-key techniques or public-key techniques; the latter is based on public-key certificates.

The X.509 standard is supported by a number of protocols, including PEM, PKCS, S-HTTP, and SSL.

Y

Z

