Guideline for setting up a functional VPN

Why do I want a VPN ?

VPN by definition creates a private, trusted network across an untrusted medium. It allows you to connect offices and people from around the world together, using a public network (The Internet) to share data and software. The real advantage comes from the application thereof.

It allows a system administrator to be on the network from a remote point.

Employees can access the network from anywhere in the world where they can get an internet connection. This includes working from home.

It allows for small networks between friends for playing multiplayer LAN games.

In any scenario where you need to connect two PCs/networks together without the ability to string cables between them, a VPN can provide the solution for you.
This document covers a few basic configurations that the WinGate VPN can be used for. Essentially, however, the basic principle for every kind of setup remains the same – you are connecting two networks together using the Internet. The use of the client is the only differentiation along with some small setup adjustments that need to be made to cater for the different scenarios.

A **single office** with **remote**, mobile users.

This scenario is typically used for giving home users access to a company LAN. It can also be applied to employees travelling and needing access to the company LAN. For a guide on configuring this type of setup, please refer to this section.

Connecting **two offices** together.

This scenario is typically used for creating a larger LAN between two or more offices. It creates a transparent, single LAN that allows users from any office to share files and data. For a guide on configuring this type of setup, please refer to this section.

Connecting **two offices** together with **remote**, mobile users.

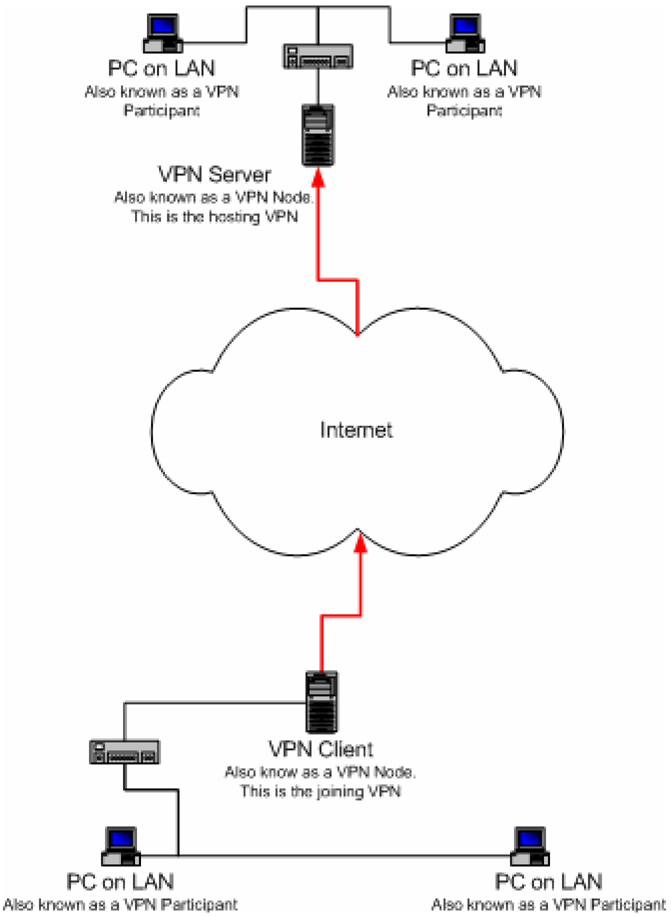
This scenario becomes a blend between the previous two setups. For a guide on configuring this type of setup, please refer to this section.

This document only deals with the configuration of the WinGate VPN. Internal issues, such as setup of your local area network, providing authentication and the handling of domain controllers and such are beyond the scope of this document.

Terminology

For the purpose of this guide, we'll use the following terminology:

VPN Server	The machine hosting the VPN
VPN Client	The machine joining the VPN
VPN Node	A VPN Server or VPN Client
VPN Participant	A machine on the subnet behind the VPN Server or Client


PC on LAN
Also known as a VPN Participant
PC on LAN
Also known as a VPN Participant
VPN Server
Also known as a VPN Node. This is the hosting VPN
Internet
VPN Client
Also know as a VPN Node. This is the joining VPN
PC on LAN
Also known as a VPN Participant
PC on LAN
Also known as a VPN Participant

How does licensing for VPN work?

Licensing is based on the number of VPN Participants on each VPN Node.

If you are connecting three Remote Clients to one Office, with each Remote Client consisting of a laptop and the Office consisting of the VPN Server with 10 PCs on the LAN behind it, you will need:

1 x WinGate VPN 1 LAN-user for each Remote Client
1 x WinGate VPN 12 LAN-user for the Office

If you are connecting two Offices together, one with 10 PCs on the LAN behind it and the other with 4 PCs on the LAN behind it you will need:

1 x WinGate VPN 12 LAN-user for the larger office
1 x WinGate VPN 6 LAN-user for the smaller office

Single Office with Remote Clients

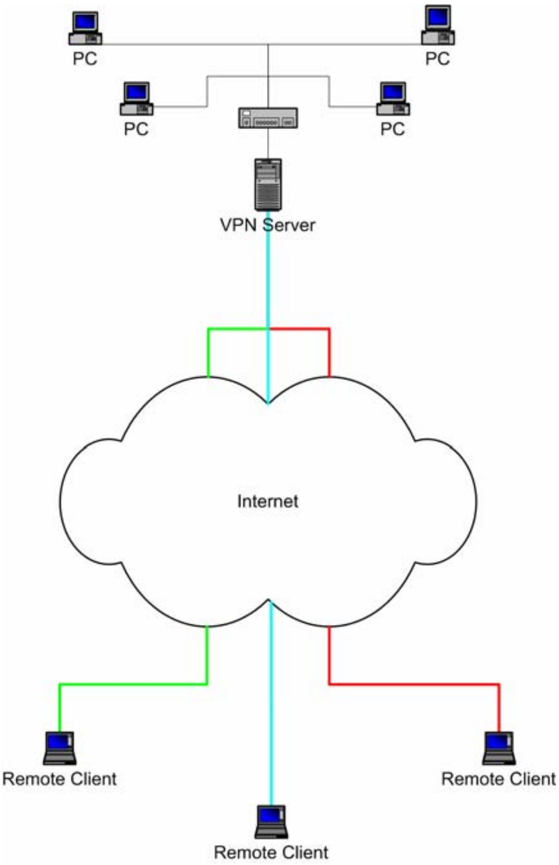
First, setup the VPN server. The VPN Server becomes the access point into your private network, to which your remote users will connect. It should ideally be on a machine that has a permanent Internet connection and preferably a static IP address. If a static IP address is not available, using a third party name to IP provider will definitely ease the configuration of connections in to the VPN. This section guides you through the setup of the VPN Server.

There are some additional considerations for this type of server setup.

1. The first is with machines on the LAN other than the VPN Server. To be able to access these machines you will need to perform some special configuration for each of them. Please refer to this section for more information on how to do this.

2. If you wish to share all machines on the VPN Server's LAN you will need to set its Local Participation mode to "Local Network".

3. Additionally, you will have to ensure that your users have appropriate Operating System Level permissions to access the resources you are sharing with them.



When the VPN Server has been configured you must distribute the exported configuration file to the VPN Clients and must configure each of them in turn. This section guides you through the setup of each VPN Client.

There are some additional considerations for the client setups.

1. If the remote client is on a network of its own rather than being a standalone PC, you will have to ensure that each remote client is on a distinct subnet.

2. If the remote client is on a network of its own and you wish to allow access to all the machines on the LAN you will need to set its Local Participation mode to "Local Network".

3. Depending on how free your remote clients are with their data, you might want to instruct them to allow or deny tunnels between other remote clients.

4. For the remote client to office link you will probably want the remote client to control when to connect or disconnect from the VPN, which means specifying the VPN link should be established manually. Specifying that the VPN client should reconnect is a good idea.

The remote clients will then, after having established an Internet connection, connect to your VPN.

Two offices

You need to choose which office will become the VPN Server. Normally, one that matches the recommendations for static IP or permanent Internet connection is most appropriate.

As before, you configure the VPN server first. The VPN Server becomes the access point into your private network, to which your second office will connect.

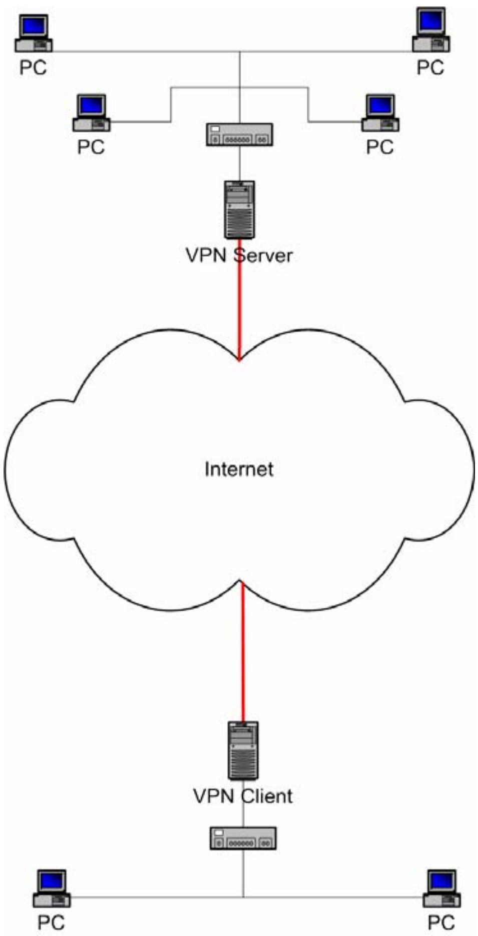
This section guides you through the setup of the VPN Server. Once you have the Server configured you send its exported configuration to the other office. At the other office you configure the VPN Client to join the remote network. This section guides you through the setup of the VPN Client.

There are some additional considerations for this type of setup.

1. The first is with machines on the LAN other than the VPN Nodes. To be able to access these machines you will need to perform some special configuration for each of them. Please refer to this section for more information on how to do this.

2. If you wish to share all machines on the VPN Node's LAN you will need to set its Local Participation mode to "Local Network".

3. Additionally, you will have to ensure that your users have appropriate Operating System Level permissions to access the resources you are sharing with them.



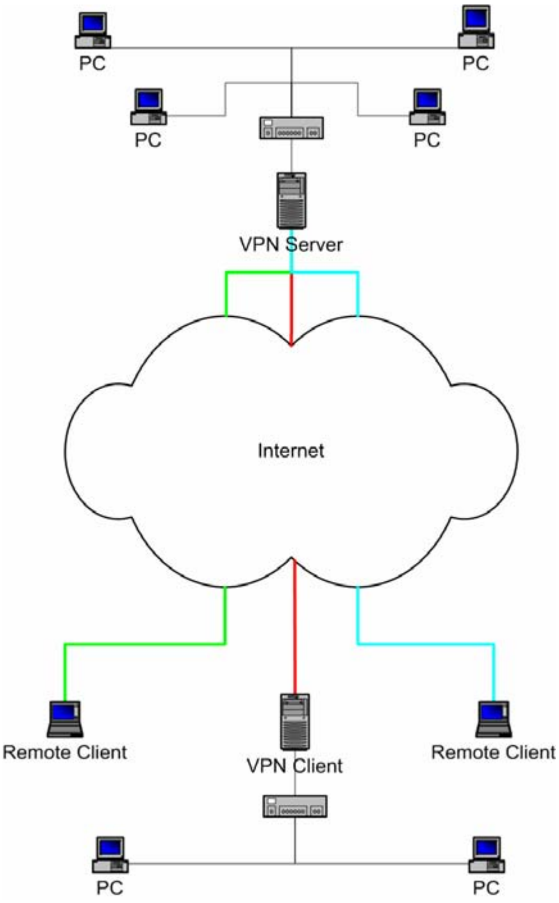
4. If you wish to allow either end of the VPN to connect you will need to configure a VPN Server at each office. You would then send the appropriate exported configuration to the other office and import it to create the appropriate VPN Client.

5. In several cases these offices are behind NAT devices. Refer to this section for potential problems with NAT devices.

6. For the office-to-office link you will probably want a permanently established connection, which means specifying the VPN link should be established when WinGate starts and that it should automatically re-connect.

Two offices with remote clients

This setup follows the same logical setup as the previous examples. Make the determination about which Office will become the VPN Server as discussed before and install the software. Once you have configured the VPN you can export its configuration. You will find detailed steps for configuring a VPN here.



The exported configuration file can then be sent to the other office where you will import it to create a VPN Client. Details on configuring a VPN Client can be found here.

You must send the configuration file to each remote client that wishes to join the VPN. They will each need to install the software and import the configuration in the same fashion that the office VPN Client had to.

There are some additional considerations for this type of setup.

1. The first is with machines on the LAN other than the VPN Nodes. To be able to access these machines you will need to perform some special configuration for each of them. Please refer to this section for more information on how to do this.

2. If you wish to share all machines on the VPN Node's LAN you will need to set its Local Participation mode to "Local Network".

3. Additionally, you will have to ensure that your users have appropriate Operating System Level permissions to access the resources you are sharing with them.

4. If you wish to allow either end of the VPN to connect you will need to configure a VPN Server at each office. You would then send the appropriate exported configuration to the other office and import it to create the appropriate VPN Client.

5. In several cases these offices are behind NAT devices. Refer to this section for potential problems with NAT devices.

6. If the remote client is on a network of its own rather than being a standalone PC, you will have to ensure that each remote client is on a distinct subnet.

7. If the remote client is on a network of its own and you wish to allow access to all the machines on the LAN you will need to set its Local Participation mode to "Local Network".

8. Depending on how free your remote clients are with their data, you might want to instruct them to allow or deny tunnels between other remote clients.

9. For the office-to-office link you will probably want a permanently established connection, which means specifying the VPN link should be established when

WinGate starts and that it should automatically re-connect.

10. For the remote client to office link you will probably want the remote client to control when to connect or disconnect from the VPN, which means specifying the VPN link should be established manually. Specifying that the VPN client should reconnect is a good idea.

What do I install / configure on the Server?

Your server must have Internet access and be able to receive incoming connections from the Internet. In some cases this might involve configuring a hardware device so it will allow the connection through to the VPN Server. If you suspect you have such a device, read this section for more information on any additional configuration that might be required.

You must first install the appropriate software. This can be WinGate (With a VPN license) or WinGate VPN. Once you have it installed and the machine has rebooted, you need to configure your VPN.

If you are using WinGate, read this section for a step-by-step guide on configuring a VPN.

If you are using WinGate VPN, read this section for a step-by-step guide on configuring a VPN.

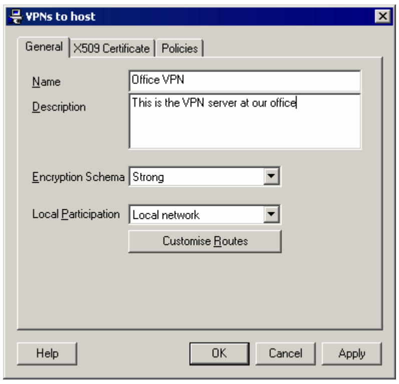
I am using WinGate

If you are using WinGate to share your Internet Connection you will need to add your VPN license to WinGate. For more information on VPN licenses, click here.

1. Open **GateKeeper** by double clicking the WinGate Engine Monitor in the taskbar.

2. On the **System** tab, double click the VPN Service to access the VPN configuration. This will take you to the VPN configuration dialog.

3. On the **VPNs to Host** tab, click the **Add** button to add a new VPN configuration. This will take you to the VPNs to Host configuration dialog.



VPNs to host

Name: Office VPN
Description: This is the VPN server at our office
Encryption Schema: Strong
Local Participation: Local network

4. On the **General** tab, enter the following values:

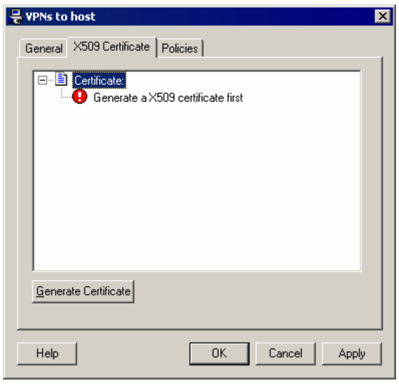
   4.1. Name – an easy to remember name for your VPN. The name of your network or location is a good choice.

   4.2. Local Participation – this determines how the VPN will share your network.

No Participation	This network does not participate in the VPN
Local Machine	Only this PC participates in the VPN
Local Network	This PC and all other PCs on the LAN participates

   4.3. Encryption – leave this at “Strong”

5. On the **X509** tab, generate the certificate that is associated with this VPN by clicking Generate. This will take you to the X509 Certificate Generation Wizard.



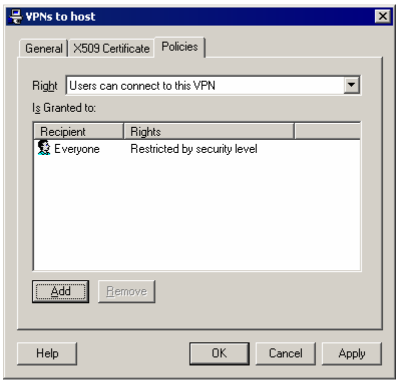
VPNs to host

Certificate:
Generate a X509 certificate first

   5.1. On the **encryption** tab, leave everything at default values. You have to enter and confirm an appropriate passphrase. Use something that contains a mixture of letters and numbers. You do not need to remember this value.

5.2. On the **certificate** detail tab, fill in as many values as possible. No values are required, but your certificates are more detailed with more information entered.

5.3. **Confirm** your details and click **OK**. The certificate will not be generated immediately. This is done when you click **OK** to accept the VPN configuration.


VPNs to host

Right: Users can connect to this VPN

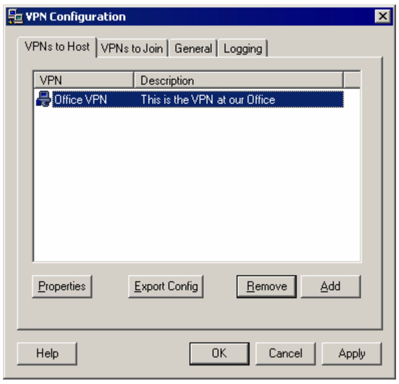
Is Granted to:

Recipient	Rights
Everyone	Restricted by security level

6. On the **Policies** tab, determine which users are allowed to connect to this VPN. This is for establishing the control channel connection between the Server and it's clients. It does not apply to normal, network operation across the VPN.

7. Once you have configured everything, you can click **OK** to accept the VPN configuration. It will now generate the certificate. You should receive an informational system log message to indicate that this has been completed.

8. Once the message has been returned, you can export the information your clients will need to connect to the VPN. You do this by selecting the VPN and clicking the **Export Config** button. This will take you to the Export Config wizard.


VPN Configuration

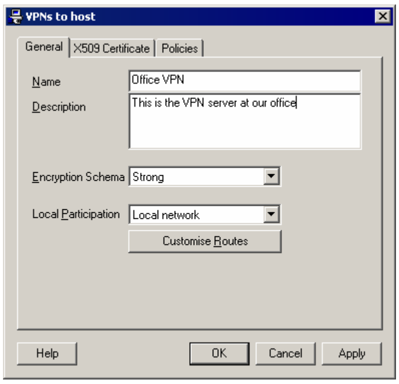
VPN	Description
Office VPN	This is the VPN at our Office

9. Here you enter the name or IP address that is used to find your VPN on the Internet. If you are using a dynamic IP to host-name system or have a DNS name associated with your PC, use that name. Otherwise, you need to enter your IP address here. When you click **OK**, it will prompt you to save the information. Save this file to a location where you can easily access it. You will need that file for the client configuration.

I am using WinGate VPN

1. Open **GateKeeper** by double clicking the VPN Monitor in the taskbar.

2. On the **VPN** tab, click the **Add a new VPN** button under the VPNs to Host section to add a new VPN configuration. This will take you to the VPNs to Host configuration dialog.


VPNs to host

General | X509 Certificate | Policies

Name: Office VPN

Description: This is the VPN server at our office

Encryption Schema: Strong

Local Participation: Local network

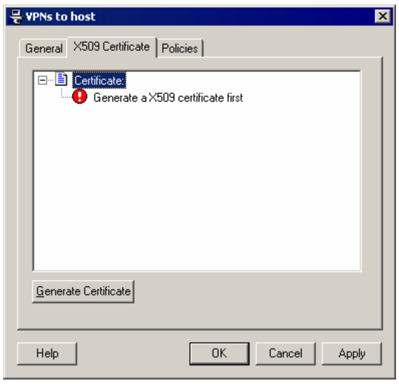
3. On the **General** tab, enter the following values:

3.1. Name – an easy to remember name for your VPN. The name of your network or location is a good choice.

3.2. Local Participation – this determines how the VPN will share your network.

No Participation	This network does not participate in the VPN
Local Machine	Only this PC participates in the VPN
Local Network	This PC and all other PCs on the LAN participates

3.3. Encryption – leave this at “Strong”


VPNs to host

General | X509 Certificate | Policies

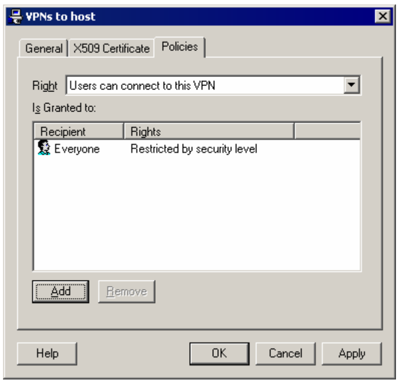
Certificate:
Generate a X509 certificate first

4. On the **X509** tab, generate the certificate that is associated with this VPN by clicking Generate. This will take you to the X509 Certificate Generation Wizard.

4.1. On the **encryption** tab, leave everything at default values. You have to enter and confirm an appropriate passphrase. Use something that contains a mixture of letters and numbers. You do not need to remember this value.

4.2. On the **certificate** detail tab, fill in as many values as possible. No values are required, but your certificates are more detailed with more information entered.

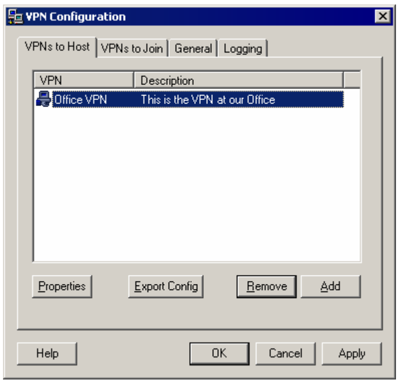
4.3. **Confirm** your details and click **OK**. The certificate will not be generated immediately. This is done when you click **OK** to accept the VPN configuration.



5. On the **Policies** tab, determine which users are allowed to connect to this VPN. This is for establishing the control channel connection between the Server and it's clients. It does not apply to normal, network operation across the VPN.

6. Once you have configured everything, you can click **OK** to accept the VPN configuration. It will now generate the certificate. You should receive an informational system log message to indicate that this has been completed.

7. Once the message has been returned, you can export the information your clients will need to connect to the VPN. You do this by selecting the VPN and clicking the **Export Config** button. This will take you to the Export Config wizard.



8. Here you enter the name or IP address that is used to find your VPN on the Internet. If you are using a dynamic IP to host-name system or have a DNS name associated with your PC, use that name. Otherwise, you need to enter your IP address here. When you click **OK**, it will prompt you to save the information. Save this file to a location where you can easily access it. You will need that file for the client configuration.

What do I install / configure on the VPN client?

Your client must have Internet access and be able to make outgoing connections to the Internet using TCP and UDP. It must also be able to receive incoming traffic from the Internet on a UDP port. In some cases this might involve configuring a hardware device so it will allow the connection through to the VPN Node. If you suspect you have such a device, read this section for more information on any additional configuration that might be required.

Once you have ensured that Internet access is possible you must install the appropriate software. This can be WinGate (With a VPN license) or WinGate VPN. Once you have it installed and the machine has rebooted, you need to configure your VPN.

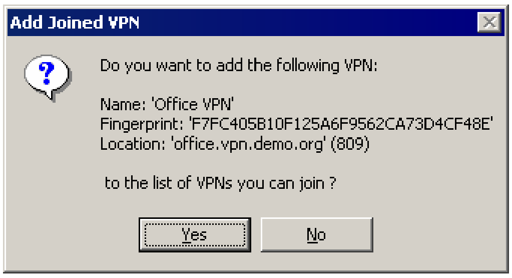
If you are using WinGate, read this section for a step-by-step guide on configuring a VPN.

If you are using WinGate VPN, read this section for a step-by-step guide on configuring a VPN.

I am using WinGate

If you are using WinGate to share your Internet Connection you will need to add your VPN license to WinGate. For more information on VPN licenses, click here.

1. Double click the **VPN Configuration file** you received from the VPN Servers Administrator.



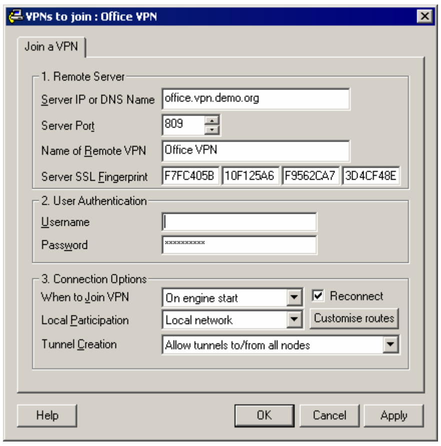
Add Joined VPN

Do you want to add the following VPN:

Name: 'Office VPN'
Fingerprint: 'F7FC405B10F125A6F9562CA73D4CF48E'
Location: 'office.vpn.demo.org' (809)

to the list of VPNs you can join ?

2. **GateKeeper** will automatically launch and ask if you want to add the configuration for this VPN to your system. Click “Yes” to add the configuration. This will take you to the VPN configuration dialog.



VPNs to join : Office VPN

Join a VPN

1. Remote Server
Server IP or DNS Name: office.vpn.demo.org
Server Port: 809
Name of Remote VPN: Office VPN
Server SSL Fingerprint: F7FC405B 10F125A6 F9562CA7 3D4CF48E

2. User Authentication
Username:
Password: **********

3. Connection Options
When to Join VPN: On engine start
☑ Reconnect
Local Participation: Local network
Tunnel Creation: Allow tunnels to/from all nodes

3. Most values will already be filled in for you. It is a good idea to double-check each value though, to ensure that it is correct. In the **Remote Server** section, check the following values:

   3.1. Server IP or DNS Name – this is the name or IP that you will access the server with. This must be visible from the Internet.

   3.2. Server Port – this is the configured port on which your VPN Server is listening on. The default is port 809 (TCP).

   3.3. Name of Remote VPN – An easy to remember name for your VPN. This name must match the name assigned to the VPN by the Administrator.[1]

   3.4. Server SSL Fingerprint – this is a value generated by the server and is used by the remote client to validate that we are talking to the correct VPN Server.

[1] Do not confuse the VPN name with the VPN address (DNS name)

4. In the **User Authentication** section, enter the following values:

4.1. Username – this is the name of a WinGate User that has been granted access through the policies to access the WinGate VPN.

4.2. Password – this is the password for the WinGate User configured above.

These values are NEVER transmitted with the configuration – you will need to contact the host of the VPN Server to find out which values you should use.

5. In the **Connection Options** section, check the following values:

5.1. When to Join VPN – this determines when WinGate VPN will attempt to connect to the remote VPN.

On Engine Start	Connect once the WinGate Engine has started
Manually	The user establishes the connection in GateKeeper
Disabled	This VPN cannot be connected

5.2. Reconnect – this option reconnects the VPN if the Internet or VPN connection is lost.

5.3. Local Participation – this determines how the VPN will share your network.

No Participation	This network does not participate in the VPN
Local Machine	Only this PC participates in the VPN
Local Network	This PC and all other PCs on the LAN participates

5.4. Tunnel Creation – this determines which nodes this VPN will allow to establish tunnels with it.

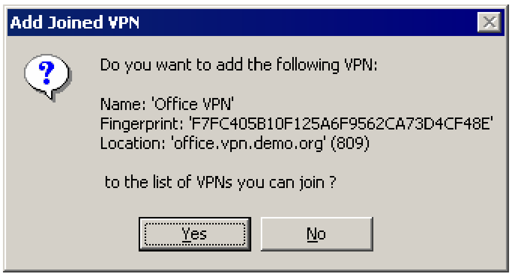
To/from all Nodes	All clients connecting to the server can establish a data tunnel with this node and potentially access any resources this VPN publishes. This is in addition to the data tunnel with the VPN server
Only with Master	This option will not allow other clients connecting to the same server to establish tunnels with this client. The tunnel to the server is still established normally.

6. Once you have verified all the settings you can click “Ok” to close the dialog. This will return you to the main GateKeeper interface, from where you can connect the VPN if required.

I am using WinGate VPN

To be able to configure this VPN you will need the exported configuration file from the VPN Server. This configuration file helps you verify the identity of the VPN Server.

7. Double click the **VPN Configuration file** you received from the VPN Servers Administrator.



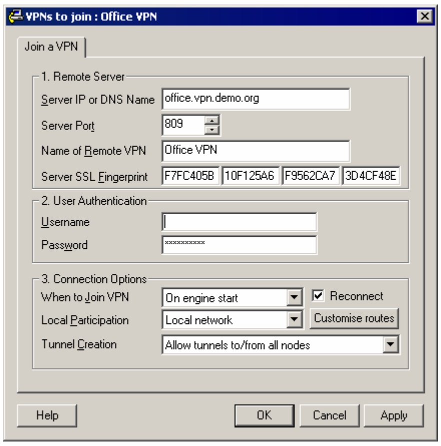
Add Joined VPN

Do you want to add the following VPN:

Name: 'Office VPN'
Fingerprint: 'F7FC405B10F125A6F9562CA73D4CF48E'
Location: 'office.vpn.demo.org' (809)

to the list of VPNs you can join ?

8. **GateKeeper** will automatically launch and ask if you want to add the configuration for this VPN to your system. Click “Yes” to add the configuration. This will take you to the VPN configuration dialog.



VPNs to join : Office VPN

Join a VPN

1. Remote Server
Server IP or DNS Name: office.vpn.demo.org
Server Port: 809
Name of Remote VPN: Office VPN
Server SSL Fingerprint: F7FC405B 10F125A6 F9562CA7 3D4CF48E

2. User Authentication
Username:
Password: **********

3. Connection Options
When to Join VPN: On engine start
☑ Reconnect
Local Participation: Local network
Tunnel Creation: Allow tunnels to/from all nodes

9. Most values will already be filled in for you. It is a good idea to double-check each value though, to ensure that it is correct. In the **Remote Server** section, check the following values:

   9.1. Server IP or DNS Name – this is the name or IP that you will access the server with. This must be visible from the Internet.

   9.2. Server Port – this is the configured port on which your VPN Server is listening on. The default is port 809 (TCP).

   9.3. Name of Remote VPN – An easy to remember name for your VPN. This name must match the name assigned to the VPN by the Administrator.[2]

   9.4. Server SSL Fingerprint – this is a value generated by the server and is used by the remote client to validate that we are talking to the correct VPN Server.

[2] Do not confuse the VPN name with the VPN address (DNS name)

10. In the **User Authentication** section, enter the following values:

10.1. Username – this is the name of a WinGate User that has been granted access through the policies to access the WinGate VPN.

10.2. Password – this is the password for the WinGate User configured above.

These values are NEVER transmitted with the configuration – you will need to contact the host of the VPN Server to find out which values you should use.

11. In the **Connection Options** section, check the following values:

11.1. When to Join VPN – this determines when WinGate VPN will attempt to connect to the remote VPN.

On Engine Start	Connect once the WinGate Engine has started
Manually	The user establishes the connection in GateKeeper
Disabled	This VPN cannot be connected

11.2. Reconnect – this option reconnects the VPN if the Internet or VPN connection is lost.

11.3. Local Participation – this determines how the VPN will share your network.

No Participation	This network does not participate in the VPN
Local Machine	Only this PC participates in the VPN
Local Network	This PC and all other PCs on the LAN participates

11.4. Tunnel Creation – this determines which nodes this VPN will allow to establish tunnels with it.

To/from all Nodes	All clients connecting to the server can establish a data tunnel with this node and potentially access any resources this VPN publishes. This is in addition to the data tunnel with the VPN server
Only with Master	This option will not allow other clients connecting to the same server to establish tunnels with this client. The tunnel to the server is still established normally.

12. Once you have verified all the settings you can click “Ok” to close the dialog. This will return you to the main GateKeeper interface, from where you can connect the VPN if required.

General Troubleshooting

The basic troubleshooting steps are:

Determine if you can establish a connection to the VPN Server. This step requires an active Internet connection and a running VPN Server. Your VPN Server must be able to receive connections on the VPN Port (Default 809) from the Internet.

If the connection can be successfully established, the two VPN Nodes can exchange control information. This is the control connection and uses TCP. The next step is to verify that the routes are not showing up as “Disabled” or “In conflict”.

This problem is most common in scenarios where different VPN nodes are on the same subnet. If the VPN Server has a subnet of 192.168.0.*** and the VPN Client has a subnet of 192.168.0.*** neither end will be able to determine where to send a packet for a machine with the IP address 192.168.0.10, as it could be on either end.

If no routes are showing up with errors you should verify the tunnel. Do this by attempting to ping the internal IP address of the VPN Server from the VPN Client and vice versa. If the ping succeeds the data channel is operational. If it fails however, there could be a problem with an intermediary NAT device. Refer to this section for more information on correct port forwarding.

If the ping is successful, but your VPN participants are still showing up as not accessible, your problem is either with browsing or with the setup of the client machines. Network machines on your VPN Server or Client network must believe they can get to the machines on the other network. This means that either they use their default route to get to these machines, or they must have specific routes configured. Otherwise they will refuse to send a packet back even if they receive one. Refer to this section for possible solutions for client PCs.

I have a NAT device that provides Internet connectivity

If you have a NAT device or firewall it could potentially interfere with the VPN Data Channel. The VPN Data Channel uses the UDP transport protocol to transfer networking information from one network to the other. This is a connectionless protocol, which generally means that firewalls, etc. must be explicitly instructed to either allow the traffic or route the traffic to a specific VPN Server.

By default, WinGate VPN uses port 809 for the Data Channel. You can find the configured port number in the WinGate VPN Configuration, on the **General** tab.

I can see all the shares, but cannot browse or open any files

On some types of connection, there is a reduction in the MTU (Maximum Transmission Unit, which is a measure of the largest packet payload that may be sent over a network interface or point to point link). For instance PPPoE connections reduce the MTU by 8 bytes. The standard MTU for Ethernet is 1500 bytes, which means you can have up to 1500 bytes of payload over Ethernet. The Ethernet frame itself has a 14-byte header, so the actual maximum packet size (as opposed to the MTU) is 1514. WinGate VPN reduces the MTU as well, since the encryption and tunnelling require approx 50 - 60 bytes per packet.

If there are MTU issues, you can find that large (maximum size) packets can be lost. This produces strange effects such as:

Able to connect to a network share, prompted for a password, etc. but unable to browse large directories or transfer files.
Network drive mappings are disconnected and are generally unreliable.

Using Ping, you can send packets of different sizes. WinGate VPN fragments packets (if allowed) when it transfers them across the VPN. Therefore you should be able to send large ping packets successfully across the VPN if everything is working properly. If not, then once you get to a certain size, they will stop working.

To send a packet of a certain size, use the -l switch on the ping command. e.g.

```
ping 192.168.1.1 -l 1422
```

This will send a ping packet with a 1422 byte ICMP payload. It is important to note that the actual packet size of the ping packet is 28 bytes larger than this since the IP plus ICMP headers use 26 bytes. Therefore the example above will send a packet of 1450 bytes (not including the Ethernet header). The Ethernet header is not counted because this is stripped off and not transmitted over the VPN.

By working out the ping size that works vs the size that doesn't you can calculate what the effective MTU really is. For dialup connections and some network interfaces, it is then possible to modify the MTU so that your client machines will no longer send packets that are too big.

I am having problems accessing computers

Network browsing via Network Neighbourhood is a client-server process. The browse client (Network Neighbourhood) must be able to communicate with a browse server (Commonly called a master browser) or any machine that maintains a browse list, such as a a domain controller or an Active Directory server.

If this machine is located behind the VPN Node, you will have to ensure that it can respond to the appropriate browse requests. Refer to this section for information on making machines accessible across the VPN.

I cannot access any machines behind the hosted OR joined

If you cannot access any of the machines they will show up as “Not Accessible” in GateKeeper. The first step in working out where this problem is would be to verify that you have configured that machine to be aware of the VPN.

The Qbik VPN is a routing based solution. For it to function, both ends of the VPN and all participants in the VPN must be aware of how to access the remote networks.

There are three possible ways to do this.

Default Gateway

In the standard, operating system TCP/IP configuration screen, you set the default gateway of the VPN participant to be the appropriate VPN Node (Host or Joiner). This forces all network traffic that the VPN participant does not know how to route through to the VPN Node, who will then route the appropriate traffic to the remote network.

RIP Listener

WinGate VPN can broadcast route updates as it becomes aware of new VPNs becoming available. If you install a RIP v 2 compatible listener on the VPN participant it will receive these RIP broadcasts and be able to route traffic destined for the remote subnet to the VPN Node.

If the VPN Node is not your Internet Gateway it is possible that your Internet Gateway will support RIP v 2. (Most DSL/NAT boxes have a RIP v 2 Listener built in) If this is the case, you can turn it on for the gateway.

Static Route

By adding a static route you can explicitly tell each participant how to route to the remote subnet. For example, the LAN on the VPN Server uses the IP Range of 192.168.1.***. The VPN Server is 192.168.1.13. The LAN the VPN Joiner uses the IP Range of 192.168.4.***.

If you want to add a static route on a participant behind the VPN Joiner you would specify:

```
route add 192.168.4.0 MASK 255.255.255.0 192.168.1.13
```

This route will send all traffic destined for any machine on the 192.168.4.*** subnet to the VPN Server for processing.

Nothing on my remote client is visible across the VPN

It is important to note that if you are on a single interface machine (Dial-up modem, Cable modem or similar) without a network card you will need to enable File and Printer Sharing on the interface that provides you with Internet access.

Enabling this allows the networking subsystem to start which in turn allows you to browse and share files across a network.

The WinGate Firewall will prevent unauthorised access to your computer. If you do not have File and Printer Sharing enabled on at least one of your interfaces the appropriate network sub-systems that allow access to files, printers and browsing thereof will not be running and you will be unable to access any of those services.

Can I use a MAC or Linux based machine for WinGate VPN?

A MAC or Linux machine can be a VPN Participant, but not a VPN Node. Use the setup guide here to ensure that the participant can see the network.

Common tests

```
ping <machine name>

D:\>ping blade

Pinging blade [192.168.4.99] with 32 bytes of data:

Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.4.99:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

This will send a ping packet to the appropriate machine after resolving the name into an IP address. This tests that the name and the ip address can be resolved across the VPN.

```
ping <ip address>
D:\>ping 192.168.4.99

Pinging 192.168.4.99 with 32 bytes of data:

Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128
Reply from 192.168.4.99: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.4.99:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

This will send a ping packet to the appropriate machine. This tests that the IP address can be reached across the VPN.

```
nbtstat –a <ip address>
D:\>nbtstat -a blade

192.168.4.190:
Node IpAddress: [192.168.4.190] Scope Id: []

        NetBIOS Remote Machine Name Table

     Name            Type        Status
   ---------------------------------------------
   BLADE          <00>  UNIQUE      Registered
   BLADE          <20>  UNIQUE      Registered
   WORKGROUP  <00>  GROUP       Registered
   BLADE          <03>  UNIQUE      Registered

   MAC Address = xx-xx-xx-xx-xx-xx
```

This will send a nbtstat query to the appropriate machine. If you get a response it indicates that the VPN Data Channel is established and that you can reach the remote machine.

\\<ip address>
This will browse to a machine using its IP address. You can enter this command on any Explorer Address bar, or from the Start menus RUN command.

\\<machine name>
This will browse to a machine using its name. You can enter this command on any Explorer Address bar, or from the Start menus RUN command.