Introduction to the WinGate Internet Client

WinGate Internet Client

The **WinGate Internet Client** (WGIC) is included with WinGate. When installed on your client computers it works with the WinGate server, allowing your applications to connect 'directly' to the Internet with no further configuration (unlike with proxies). It achieves this with the Winsock Redirection Service, which lets your applications think and act as if it were connected to the Internet itself.

You can access the WGIC from the Windows control panel (displayed below) by clicking *Start/Settings/Control Panel*. When using the WGIC, client computers are provided with the additional control of the WinGate Dialup Monitor (which shows what connections are being used and allows them to be closed).

Where Do I Start?

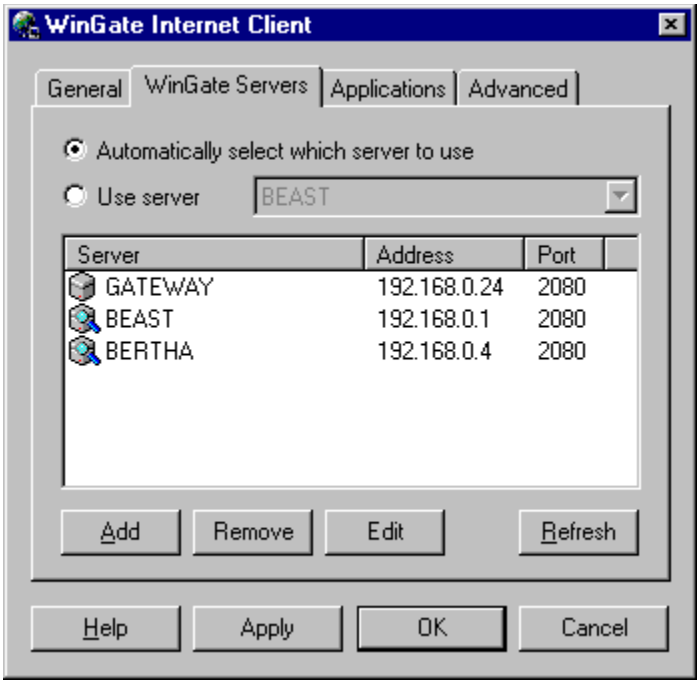
- Check out How To Use WinGate Help to learn about the interactive features of this help file
- Learn about tuning Internet connectivity with the WGIC interface
- Learn about the WinGate Dialup Monitor
- Learn about how WGIC works using the Winsock Redirection Service on the WinGate computer.

Click here to learn more about Qbik and what we do.

General Tab

Click the link to find out how to use WinGate Help

WinGate Servers Tab



Click on this link to find out how to use WinGate Help

The WGIC will automatically find any WinGate servers on your network (so long as they are running). In this dialog, the two WinGate servers **BEAST** and **BERTHA** have been detected running on the network. **GATEWAY** is another server that was not detected for some reason (perhaps it was offline at the time), but has been entered by the user. Notice that it is represented with a different icon than the automatically detected WinGate servers.

Server

This is the Windows network name for the WinGate computer residing on the network.

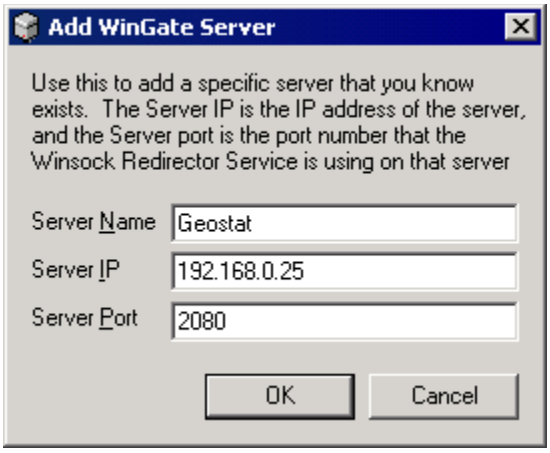
Address

This is the private IP address of the WinGate server.

Port

The port is the TCP port on which the WRP Service is running on the WinGate server. The WGIC uses the WRP Service to provide Internet connectivity through the WinGate computer. The WinGate computer will listen on port 2080 (the default port for WRP) for incoming requests to connect out, or on another port for incoming requests.

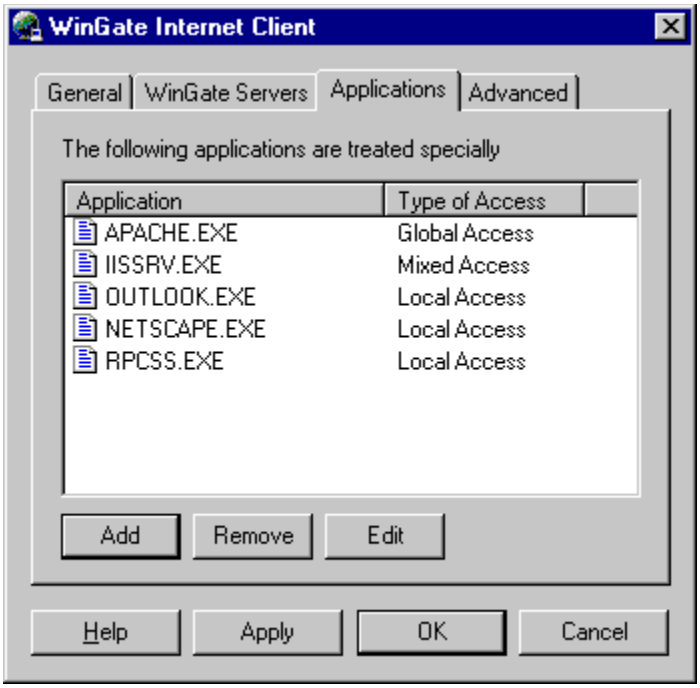
Add WinGate Server



Click on this link to find out how to use WinGate Help

Use this dialog to **Add** or **Edit** the details for a new or existing WinGate server. You would only need to *add* a WinGate server when it is not detected by the WGIC for some reason.
Clicking OK in this instance would cause a new WinGate computer named **GEOSTAT** to be added to the server list (so long as it exists at the address provided).

Applications Tab



Click on this link to find out how to use WinGate Help

Client Applications and the WGIC

Most applications request outgoing connections with other computers somewhere on the Internet (and outside your network) to get some service. These are commonly referred to as **client applications**. For instance, your web browser connects to a computer running a web server on the Internet and asks it to send it back a web page in HTML (that page is specified by the URL). Similarly, when you check your email, you are requesting a POP3 server running somewhere on the Internet to send any mail it is holding for you to your local computer so that you can read it. Client applications will work seamlessly with the WGIC.

Using Local Access Mode

In many cases, you may wish to use the speed and simplicity of WinGate NAT for client applications (those that request outgoing Internet connections only). Any applications that you want to use NAT must be changed to run in *Local Access Mode* on the *Application* tab. You can read more about the advantages and drawbacks of the NAT approach in the NAT section of the main WinGate help file.

Local Access Mode can also be used to disable the WGIC for problematic applications. You can read more about how to do this in the troubleshooting WGIC topic.

Server Application and the WGIC

Some applications 'listen' for incoming connections or data from other computer. These are called **server applications** because they provide a service to the computers that connect to them. However,

for a server application to 'hear' incoming requests from the Internet, it must be bound to a port on a public interface (i.e. a port on the WinGate computer). The WGIC will intercept any requests to 'listen' on a local port and redirect these requests to the WinGate server (this is why you can run into trouble when running the same server application on two client computers using the WGIC).

Using Global Access Mode

A server application can freely 'listen' to port numbers above 1024. For network security reasons, the default configuration for the WGIC will not let any application 'listen' on a port below 1024. If you run a server on a port number below 1024 and you want it to be accessible to computers on the Internet you *must* change it to Global Access Mode on the Application tab. Typically you will need to do this for Web Servers (they usually listen on port 80) and FTP servers (they usually listen on port 21).

Using Mixed Access Mode

Intranet Web Servers and local FTP servers are becoming increasingly common on local networks. Though these are server applications, they do NOT usually accept connections from other computers on the Internet (outside your network). Their job is to service the computers that run on the local network only (e.g. most corporate Intranets contain sensitive information that should not be published to anyone other than employees). You should change these applications to run in Mixed Access Mode on the Application tab. This allows applications to make any outgoing connections with WRP, but will only accept incoming connections from computers on the same network.

Application Scope

You get this dialog by pressing the **Add** or **Edit** buttons from the **Applications tab**. By default, every application will be 'modeless'. This works fine for all client applications that only request connections and data from computers on the Internet. However, as a built-in safety net for server applications the WGIC can step in and change the WGIC mode of an application. You will learn more about this under Mixed Access Mode below.

Local Access Mode

Local Access Mode has become much more significant with the advent of NAT in WinGate 4.0. Applications running in Local Access Mode will be disabled for the WGIC. This is useful if you want them to use the NAT for connectivity, or if they are problematic for the WGIC (read the troubleshooting WGIC topic to find out more on this). Note that the WinGate NAT Service must be installed on the WinGate computer for it to work.

To use WinGate NAT you must tell the WGIC to 'ignore' that application (e.g. in the screen above, Netscape Navigator will not use WRP). This is because the WGIC will intercept any Internet activity (both outgoing and incoming) before the NAT module hears about it. In Local Access Mode, an application will use the NAT (so long as the TCP/IP default gateway setting on the client points to the WinGate computer, and the application is not configured to use proxies). Remember that the NAT only provides connectivity for client applications (not server applications).

à Click here. to learn more about integrating the WGIC with NAT

Mixed Access Mode

Mixed Access Mode is a safe but functional mode for server applications. This allows applications to make any outgoing connections with WRP, but will only allow incoming connections from computers on the same network. It is most appropriate for server applications like Intranet Web or Ftp servers. It is

called ‘mixed’ because it provides an application with a safe mixture of global and local connectivity.

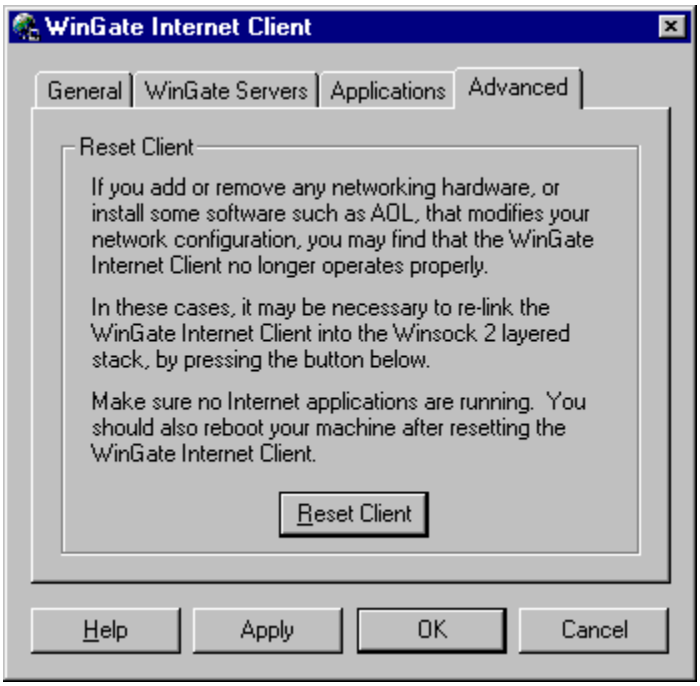
Mixed Access Mode is automatically allocated to any server applications that attempt to ‘listen’ to a system port (anything below 1024). This is a safety mechanism of the WGIC, as it requires you to explicitly set the application to Global Access Mode before it is visible to anyone on the Internet.

Global Access Mode

Global Access Mode is for server applications that must ‘listen’ for connections and service computers on the Internet (beyond your local network). It effectively removes any safety restrictions that the WGIC may impose on the application. Note that using this mode may allow intruders on the Internet to access your application (and hence the service that it provides). Running applications in this mode is a potential security threat to your network so you should make sure you have configured it appropriately.

To learn more about the "**Use non-standard connection sequence**" option click the check box hot spot on the screenshot above (*popup* help will appear).

Advanced Tab



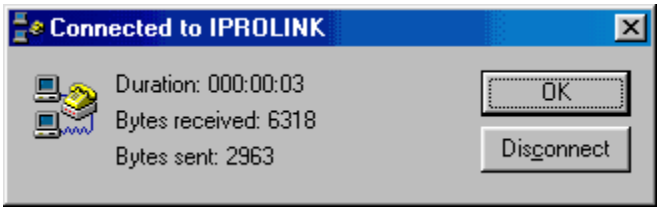
Click on this link to find out how to use WinGate Help

WinGate Dialup Monitor

The **WinGate Dialup Monitor** (WGDM) is a feature of the WinGate Internet Client. It is a small applet that starts up when an Internet connection has been initiated on the WinGate server. It gives users some information about their connection to the Internet, like what they are connected with and the duration, bytes sent and bytes received. It is accessed by double clicking its icon in the system tray shown below (remember it only appears once you have initiated a dial).

There are **two** modes of operation for the WGDM: Modem Internet Connection and Non-Modem Internet Connection.

Modem Internet Connection



In this mode, the WGIC (running on Windows 98) is connecting via a WinGate computer that is connected to the Internet with a modem (dialup account). The time online and data counts are displayed. The **Disconnect** button is only available in this mode and allows the user to terminate the connection when the modem is idle to cut down on unnecessary time online.

Typical User Scenario:

1. The modem on the WinGate machine is offline
2. A user runs a web browser on his/her client computer setup with the WGIC
3. The user types in a URL and presses enter (e.g. www.qbik.com)
4. The WGIC runs the WGDM
5. The WGIC passes the request to the WinGate computer, which begins dialing up an Internet account using the modem
6. Updates are sent through to the WGDM as the modem starts dialing, connects, logs on, then reports ‘Connected to IPROLINK’
7. The web browser receives the data requested (e.g. the Qbik homepage)
8. Updates are sent though to the WGDM on data totals
9. After a few seconds, the WGDM is minimized to the system tray in the task bar
10. The user double clicks on the WGDM icon for details on the connection
11. The user clicks the Disconnect button to hang up the modem as they intend to spend a reasonable amount of time perusing the retrieved web page.

Non-Modem Internet Connection

In this mode, the WGIC (running on Windows 95 or NT) is connecting via a WinGate computer that is connected to the Internet with a non-dialup method (e.g. T1 LAN connection). In both modes the '*Duration*' time refers to the time that the WGIC has had a control connection open with WinGate.

Typical User Scenario:

1. The WinGate computer is permanently connected with a T1 to the Internet
2. A user runs a web browser on his/her client computer that is setup with the WGIC
3. The user types in a URL and presses enter (e.g. www.qbik.com)
4. The WGIC runs the WGDM
5. The WGDM reports 'Connected to WinGate on BEAST'
6. The WGIC passes the request to WinGate
7. Updates are sent to the WGDM on the client computer as the data it requested is received
8. After a few seconds, the WGDM is minimized to the system tray in the task bar
9. The user can double click on the WGDM icon for details on the connection.

Auto Select Server

Tick this box if you want the WGIC to automatically select the best WinGate server to use. You can override this by deselecting the box.

Server list

This is the list of the WinGate servers that the WinGate Internet Client has found, their IP address, port on which the Winsock redirection protocol service is running, and priority. You can use this list to select which server to use if you don’t select the automatic option.

Refresh server list

This button will refresh the list of WinGate servers. Do this if you believe that the contents are out of date.

Apply OK Cancel

Press **Apply** to apply the changes.
Press **OK** to apply and save the changes and exit.
Press **Cancel** to discard changes and exit.

Remove

This will remove the currently selected application entry. Do this if you want to return the application to its default mode.

Enable the WinGate Internet client

This turns the WGIC on and off. Default is on. Turn off to disable the Winsock Redirection Service running on the WinGate computer.

Launch the WinGate Dialup Monitor

Enables/disables the WinGate Dialup Monitor. If you have this option enabled, the WGDM will popup when the dialer is activated on the WinGate computer. It is enabled by default.

Help

Activates this help file.

Browse

This button allows you to browse for the application that you want to set a non-default mode.

Automatically discovered servers

The servers **BEAST** and **BERTHA** were found automatically by the WGIC using GDP. Discovered servers use a different icon to manually added servers.

Use server

Use this option to override the automatic selection of a WinGate server. The drop box contains all discovered and manually added WinGate servers. Select the one you want the client to use.

Note:

It is best to use *Automatic selection* whenever possible. Automatic selection allows the client to select the most appropriate server, and automatically switches to another server if the current server is unavailable.

Remove server

Removes the manually selected WinGate server from the server list

Manually added server

This server was manually added to the server list. You will notice that the icon is different.

Reset Client

This button will reset the client as detailed on the **Advanced** tab.

Local Access Mode application

The WGIC can interfere with *RPCSS.exe* on Windows NT (a system process). For this reason it is set to **Local Access Mode** so that it is ignored by the WGIC, and therefore will no longer cause any trouble (e.g. system locking up).

Local Access Mode application

Both Netscape (web browser) and Outlook (email client) have been set to **Local Access Mode**. This is so that both applications will be ignored by the WGIC and therefore will use WinGate NAT for Internet connectivity.

Mixed Access Mode application

The Microsoft Internet Information Server (a web server) has been set to **Mixed Access Mode**. This is because it is used to server the company Intranet (and therefore will only be servicing computers on the local network – not from the Internet).

Global Access Mode application

The Apache Web Server is set to **Global Access Mode** because it serves the company E-Commerce Web Site. Since this site must be accessible to the general public (to allow them to purchase products), it is permitted to service computers on the Internet. In this case, the WGIC will allow this server application to bind to a visible system port on the WinGate computer.

Non-Standard Connection Sequence

You should enable this check box when you are having problems with a particular application. It is an "if all else fails" option and should never be required under normal circumstances (it is will only be useful for a very small number of applications that make calls to Winsock in a *non-standard* way).

Installing the WinGate Internet Client

Check the Requirements for the WGIC

You should check that any client computer satisfies the following requirements before installing the WinGate Internet Client. In all cases, you should setup the WinGate server and make sure that the Winsock Redirection Service is enabled and running *before* you begin installing the WGIC.

The requirements for installing the WGIC are as follows:

- Running Windows 95, 98, NT4, 2000 or WP
- The computer is **NOT** running the WinGate server
- If running Windows 95 then WinSock 2 must be installed
- TCP/IP protocol installed and working properly.

Run the WGIC Installer Program

Once your computer satisfies these basic requirements, you can install the WGIC:

1. Run the installer program (wingate.exe) on your client computer (this is the same installer you used for the WinGate server)
2. The installer should detect the WinGate server on the network and default to the client install. If it does not you can select to install the WinGate Internet Client
3. Read the instructions provided by the installer at each step (taking time to read help for further explanation).

Like the WinGate engine, the WinGate Internet Client runs as a **Windows Service**. This means that it will always run in the background, whether you are logged in or not. You can run the WGIC applet for further configuration from the *Windows Control Panel* (click *Start/Settings/Control Panel*).

Configuring Applications to Use the WGIC

Once the installer has finished, your applications will connect to the Internet with **no** further configuration (the Winsock Redirection Service must be running on the WinGate server). The WGIC will seamlessly provide all *outgoing* and *incoming* access to and from the Internet.

If you were using proxies before you installed the WGIC then you should remove any old proxy settings because your applications should be configured to connect 'directly' to the Internet (rather than through proxies). If you do not remove these settings, your applications will still work but they will be using the WinGate proxies, not the WGIC

If you want to use WinGate NAT from the same computer then additional configuration of the client will be required. This is minimal and you can click here to find out how to integrate the NAT with the WGIC.

Uninstalling WinGate Internet Client

To Uninstall the WGIC from Your System:

- Choose the '**WinGate Internet Client Uninstall**' option from the *WinGate Internet Client group* under the *Star*t menu **OR**
- Open *Control panel/Add-Remove Software /'WinGate Internet Client'/ Remove*

Remember that any applications configured to connect 'directly' to the Internet will no longer work from this computer (once you have uninstalled the WGIC).

Troubleshooting WGIC

Occasionally, the WGIC can cause problems with WinSock applications on the client computer (it will lock up or start running very slowly). If this happens, you must tell the WGIC to ignore the problematic application by setting it to run in *Local Access Mode*.

Find out which application is causing the problem

If you are not running Windows NT, this can be difficult. You will have to determine yourself what application is making WinSock requests, which are triggering the WGIC.

If you are running Windows NT this involves running the **Task Manager**:

1. In Windows NT hit **Ctrl+Alt+Del** and view the **Processes** tab
2. Click on the CPU column header (this will order the active processes by the amount of CPU they are using)
3. Problematic applications will frequently appear at the top of the list, as they will be using excessive amounts of CPU time (note that System Idle Process should always be high as this is basically unused CPU).

Set problematic applications to run in Local Access Mode

Once you know what application/process the WGIC is interfering with, you should tell the WGIC to 'ignore' it by setting it to run in *Local Access Mode*. This will solve the problem because the WGIC will no longer respond to the applications that WinSock requests (to connect to another computer using TCP/IP).

à Click here to see how to set an application to run in Local Access Mode.

Installing WinSock 2

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

You can download the WinSock 2 extension free of charge from the Microsoft web site (www.microsoft.com).

Installing TCP/IP on the Client Computers

Ensure that the WinGate engine is running on the network *before* you configure the client computers (the engine will start automatically following a successful install).

TCP/IP may already be installed. If this is the case, you may not need to install it again but you can test to see that it is working properly. If you later have problems with TCP/IP, remove and reinstall the protocol using the steps below.

Note:

- If you have a working Internet modem setup then you already have TCP/IP installed
- 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 98 or ME…

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

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

In Windows NT 4…

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 hit **OK**

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

In Windows 2000 / XP…

1. Press the **Start** button
2. Select *Network and Dialup Connections*
3. Double-click on 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 **)

You should repeat this process for each computer that you want to share the Internet with using WinGate. Once you have done this, we recommend you test your installation of TCP/IP

Test TCP/IP

Once you have installed TCP/IP on each computer, they should all be able 'ping' the WinGate server. We will explain this shortly. **Ping** is a very useful utility that is installed with the TCP/IP protocol. When you ping another computer's IP address, you are sending out the message "Are you there?" to that particular computer. If everything is working properly then the pinged computer will send you a reply to confirm that they exist.

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 (yourself). 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 Server

At the command line type (replacing 192.168.0.1 with the IP of your WinGate 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 then you can move on to configuring TCP/IP for either the WinGate 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 on your network (because WinGate 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 server should produce this response(note that 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.
```

If you get this type of answer, then WinGate 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.

Integrating WGIC With NAT

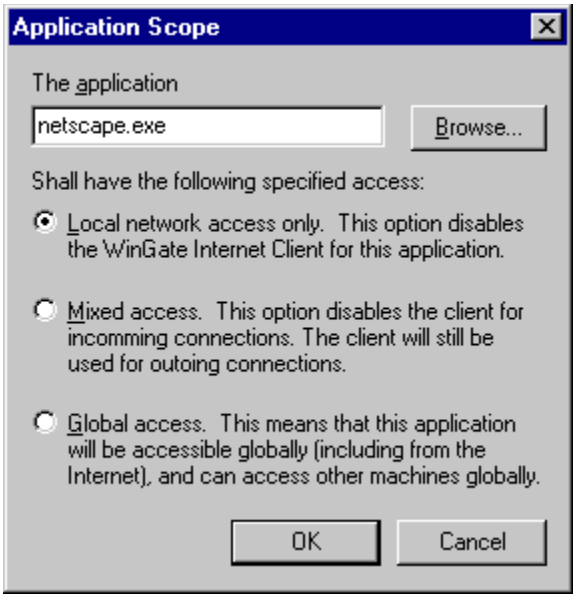
This section tells you how to integrate the WinGate Internet Client with WinGate NAT. We recommend integrating these two methods to satisfy virtually any requirement for Internet connectivity.

Using NAT with the WGIC:

This combination allows users to maximize their ability to share an Internet connection (both *outgoing* with NAT and *incoming* with WGIC), while giving you a high level of control over any applications you choose to administer more carefully using the WGIC.

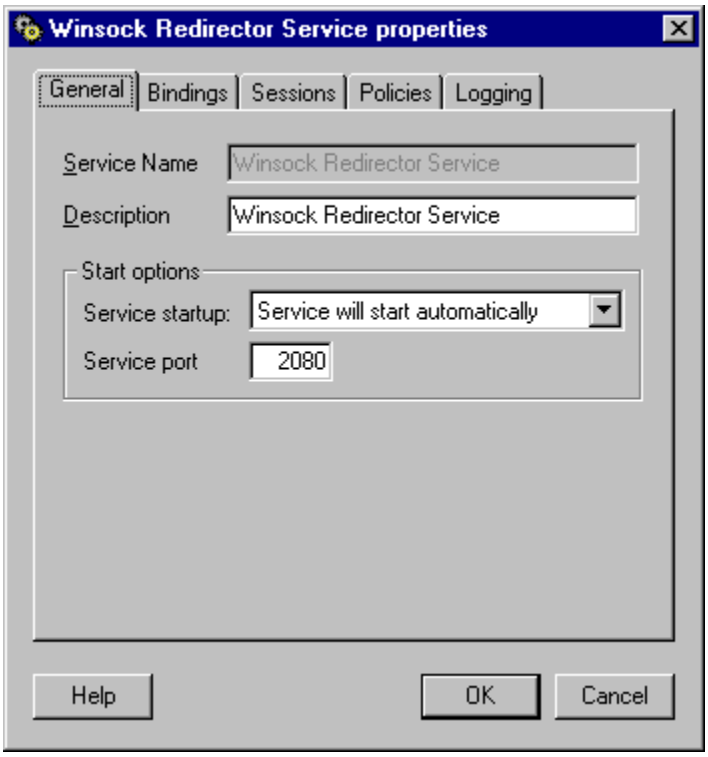
Once the WGIC is installed, it will provide the default connectivity for every client application trying to connect to the Internet from that computer. To use the NAT, you must configure the WGIC to *ignore* a particular application. Follow these steps to use NAT and the WGIC on the same client computer:

1. Make sure your '**Default gateway**' points to the WinGate server (this is done automatically if DHCP is enabled)
2. Make sure that your Windows applications are configured to connect directly to the Internet
3. Install the WGIC on the client computer (it will handle all access to the Internet unless you to explicitly tell it to ignore a particular application)
4. Go to the *control panel* and open the applet named '**WinGate Internet Client**'
5. Select the '**Application**' tab and click the '**Add**' button
6. Select an application that you want to use the NAT e.g. Netscape.exe (if you do not know the name of an applications .exe, click on the '**Browse**' button and look for that application on the local drive)
7. Select '**Local Network Access**' and the selected application will be ignored by the WGIC (in the screenshot below the user is configuring Netscape to use the NAT)



8. Repeat this process for each Internet application that you want the WGIC to ignore (and therefore use the NAT)
9. Click on the '**Apply**' button, and then click '**OK**'.

Winsock Redirection Protocol Service



The **WRP Service** runs on the WinGate server and implements the **WRP** (Winsock Redirection Protocol). WRP allows your Internet applications to run as if they are directly connected to the Internet. Once the WinGate Internet Client (**WGIC**) is installed on your client computers, no Internet software configuration is needed. Previous versions of WinGate required each application to be configured manually for proxy operation. This is no longer required, although any proxy-configured software will still work.

The WRP gives all your applications the benefit of being directly connected to the Internet, while enjoying the benefits of a proxy server and the security of a firewall.

WRP allows your client applications to:

- Make TCP connections (e.g. WWW browsing)
- Accept TCP connections (e.g. like a WWW server)
- Send UDP data (EG Streaming applications like Real Audio)
- Accept UDP data (EG like a RA server).

How does it work?

WRP works like this: an Internet application on the client computer attempts to make a connection to a computer on the Internet. The WinGate WRP client detects this and determines what kind of request it is. If it is a connection to a computer on the same network, the client lets the application make the

connection directly. If the client tries to connect to a computer on the Internet, (i.e. it is not on the same network) then the WRP client 'catches' the connection and sends it to the WinGate WRP service. WinGate then makes the connection as if it was the client computer, and because it is directly connected to the Internet, it succeeds.

What needs setting up?

In a word, nothing! Let's look at the configurations normally required and how this is overcome with WinGate.

Configuring TCP/IP

With WinGate DHCP, you don't need to configure TCP/IP. Just install it, and it works. All your computers are automatically given IP numbers.

Configuring applications

Applications no longer need any configuration to use the Internet. WinGate Internet Client takes care of this.

The WRP service is fully configurable, however its default configuration is designed to be optimal for most situations. A great feature of WRP is that you no longer need to have different proxies for different services. WRP is a new connection method that allows connections to be handled natively instead of at an application level. While you can still have separate proxies, you only need them if you want specific control over those services. Most people will only need WRP, DHCP, DNS and RCS servers.

à WRP FAQ

WRP Application Modes

When the WinGate Internet Client recognizes that an application is trying to bind to a system port number (port number less than 1024), it assumes that the application is a server-style application (i.e. it waits and listens for incoming connections from other computers).

WinGate looks at the name of the application, and it saves this information with a mode parameter. When you open the control panel applet, the name and details will be listed, and you can modify the selected mode. Internet applications that run on a computer with the WinGate Internet Client installed have a mode associated with the way they are allowed to operate.

Local Access Mode:

When an application is set to run in *Local Access Mode,* it is ignored by the WGIC. This means that no outgoing or incoming requests for Internet connections will be redirected by the WGIC. *This mode is of key importance when using NAT together with the WGIC on a single computer*. Any applications that you want to use NAT for outgoing connectivity must be set to run in **Local Access Mode**.

Mixed Access Mode:

This mode allows the applications to make outward connections using WRP, but will not allow incoming connections from the Internet via WRP. Only computers on your local network will be able to connect to this application. All applications will be set to run *Mixed Access Mode* by default.

Global Access Mode:

Applications set to run in *Global Access Mode* will have full connection ability. They can accept incoming connections and can make outgoing connections using WRP. For your server application to be externally accessible, it will need to operate in this mode.

WRP Compatibility

Applications that make only outgoing connections (called client applications) are fully supported by WinGate WRP. This covers the bulk of client applications: web browsers, email, FTP etc.

Any application that accepts incoming connections (called server applications) on a fixed port will be limited to running one copy per WinGate installation. This is because WRP causes the corresponding port on the WinGate server to be bound and "listen".

Conflict arises when a second application attempts to associate/bind to the same port. This can be overcome on the network by changing the port on which the server listens, or using a mapped link in WinGate and disabling the WinGate client. Any application that listens to a predefined port is in this situation. If the port can be changed, then conflict is avoided.

See also:

Note for Application developers

Notes for Winsock Application Developers

This topic contains some suggested guidelines for developers of WinSock 2 applications. By following these guidelines, developers will help to ensure that any software they write will interact with the WinGate Winsock Redirection Protocol (WRP).

1. Avoid at all costs implementing protocols where the client explicitly tells the server what its IP address or port is for any connection or transfer of data back to the client. This is for the following reasons:

    a) A client cannot be expected to even know it's real IP address on a NAT system, and there may not even be a mechanism to discover it

    b) The server can always use **getpeername()** to find out where the client is communicating from, so transmitting the information is often redundant (and can be misleading).

2. Avoid at all costs using fixed port numbers in the client application. If the client needs to accept a connection, or receive data on a port number, this number should be allocated by the operating system (by calling **bind()** with a port number of zero), and the resultant port number transmitted to the other end. Take care also when doing this, as it may break some NAT systems. The best way is to have any connections required initiated by the client.

3. Consider that any computer can be multi-homed. So, calling **gethostbyname()** on the result of **gethostname()** and using the first returned IP address will break many applications. If you must know your IP address, obtain it in terms of the interface on the local computer that will see the other host that is the other interested party in the communication. You can do this by either:

    a) If you have a TCP connection open to the other party, call **getsockname()** on that socket to retrieve your IP address

    b) Else, if you have no connection, make a dummy connection to a known service on the other party, and then call **getsockname()** on the connected socket

    c) Or if you cannot know about any specific service to connect to, bind a dummy socket to each known interface, and try a connection to the other party on a random port. The connection will fail quickly with **WSAENETUNREACHABLE** if you are trying the wrong interface. You will get either a successful connection, or a failure of connection refused you are on the right interface

    d) Or use SNMP to enumerate the route table on your computer, and work out the interface IP from that

    e) Or use Winsock 2 calls to determine the correct interface.

Additional Notes:

- When using WRP and the WinGate Internet Client, or a socks client and server, ALL client computers will immediately become multi-homed. For this reason guideline three becomes particularly important.
- Some circuit-level proxies hook calls to getsockname() and getpeername(), and provide the interface on the server. Some do not. WRP/WGIC does.

WRP FAQ

What is WRP?

Winsock Redirection Protocol is a specification for Winsock request redirection. It enables client computers to gain access to the Internet without proxies or a direct connection.

What is the WRP service?

Winsock Redirection Protocol Service is the server in WinGate that provides WRP access. Like an FTP server provides FTP.

What is the WGIC?

The WinGate Internet Client is the service that lets your client computers use the WRP SERVICE on the WinGate server. It is invisible, but configurable through its control panel icon.

What are the advantages of using WRP?

Firstly, it is very easy to use. No more client configuration is required; once installed, the WinGate client does everything for you. WinGate configuration is simple too. Most people only need 5 services, instead of about 15!

Second, WRP is fast. Once installed, there is no more time wasted getting applications working.

What are the disadvantages?

As all connections are made from the WinGate server, on the ports requested by the client application, port conflicts may occur. See the section on Current compatibility.

Do I need to know lots about networking?

No. That is the bonus of the WinGate WRP Service. In fact you don't even need to know that it is running. Once installed, the WinGate Internet Client will do all of the work for you.

How do I install WRP?

You must have the WRP Service installed on the WinGate server (it is an ordinary WinGate System Service that is installed by default). Installing the WinGate Internet Client on client computers enables them to use this service. To see how to install the WinGate Internet Client read the installation section of this help file.

I have run the install, I can't see the WinGate Internet Client?

Don't worry, this is correct. The WGIC runs as a service similar to the way a mouse driver works: It's always ready, but you can't see it. It requires no configuration, but there is an icon added to the control panel.

Can I be sure my network is secure if I use WRP?

Yes. WRP Service is carefully designed to give you maximum security. The WRP Service will only work for the computers on your own LAN. If you accidentally run a server on a client computer, it will not be accessible to the Internet unless you explicitly allow this.

How do I configure WRP to block ALL applications except the ones I choose?

Using the '**ban client application**' setting (added in version 3.05 and later) you can achieve this.

Try changing the WRP Policies to:

1. Default rights are ignored
2. Add "**Everyone**" with ban list "**Not client application name is empty**". These two entries ban all applications for everyone. So:
3. Add "**Everyone**" with ban list "**Not client application name equals X**" (e.g. where X is TELNET.EXE)
4. Add "Everyone" with ban list "**Not client application name equals Y**" (e.g. where Y is NETSCAPE.EXE).

Now they can run the client with apps X and Y but no others. This provides centralized control over what applications WRP will and will not re-direct.

However, this is not a completely bulletproof solution (which is why we've never pursued such a scheme). Bear in mind that a rogue user can subvert this by changing the name of the .EXE you chose to ban (i.e. you ban netscape.exe but allow telnet.exe. Renaming the netscape.exe file as telnet.exe allows the user to evade this policy.

Is it easy to use?

Very easy. WRP is designed to run without any user intervention required.

Why should I use WRP?

WRP saves you time and money configuring your network. WRP is great for network administrators, as client applications now require no setup to use a firewall.

Will it work with my old applications?

Yes. The WRP client will allow any TCP or UDP application to run as if it was directly connected to the Internet.

Is it forwards compatible?

Yes. WRP will allow any TCP or UDP application to run as if it was directly connected to the Internet.

How do I set up applications to use it?

You don't! WRP works without any application configuration. No more proxy settings, no more mapped links or hosts files.

Can I have several versions of WinGate running?

Yes. Each WRP client can handle multiple WinGate engines on your network. The most appropriate WinGate will be used. If one WinGate is too busy, the client will use another.

What is GDP?

Generic Discovery Protocol. This protocol is an IANA registered Internet standard, with an assigned system port number: 368. GDP is used for finding or discovering Gateway computers on a network.

Is WRP a standard?

Yes. WRP uses GDP to discover WinGate installations. WRP is a protocol specification for Winsock redirection. Both WRP and GDP specifications were created and developed by Qbik New Zealand Ltd.

How compatible it is with my computers?

It is 100% compatible with any PC running Windows 95, 98, NT4, or higher.

What if I have Macintoshes on my network? What about other types of computers?

The WRP client is only available for Windows 95 98 and NT. Other PCs will have to use the WinGate Proxies or NAT Service (NAT was introduced in WinGate 4.0).

Will the people on my network need training?

No. No training is required because WRP is transparent, the computer user does not need to know anything about WRP or how they are getting Internet access.

Can I run multiple WRP Services on my network?

Yes. Each WRP client can handle multiple WinGate engines on your network. The most appropriate WinGate server will be used. If one WinGate is busy, the client will use another (unless you specify otherwise).

Will it work with Intranet servers?

Yes. WRP does not affect connections to computers on your own LAN.

What does this mean for Internet software authors?

WRP is good news. Proxy support is no longer required. All TCP and UDP client and server applications will work. No firewall configuration will be needed to use the Internet.

Information

You can view the following general information from these links:

- WinGate FAQ
- WinGate Licensing
- Contact information
- About Qbik New Zealand
- How to use WinGate Help effectively

WinGate FAQ

For those of you who don't know what the FAQ is, here is our first question:

What is the FAQ?

An FAQ is a list of Frequently Asked Questions. The WinGate FAQ contains questions that often arise for new and existing users of WinGate. If the Manual hasn't answered your questions or solved your problem, then the FAQ is the next place to look.

Where is the FAQ?

The WinGate FAQ and Knowledge base is now located online at

http://www.wingate.com/support/

Open a browser and enter the address above.

Licensing in WinGate

The WinGate license you enter will determine **two** important things:

- Whether WinGate will run in Plus, Pro or Enterprise version mode
- How many users WinGate will allow to share the Internet connection at once.

The way WinGate Licenses work has changed a little in WinGate. We have made it easier for you to evaluate WinGate's Plus, Pro and Enterprise versions with a free 30-day trial licence.

I would like to trial WinGate for FREE before making a purchase?

When installing WinGate users may select a **FREE 30-Day Trial WinGate Pro License**. Users are no longer required to *apply* for a trial key and may start using the software immediately.

This enables you to run a full-featured version of WinGate on your network with any license and any number of users for 30 days.

After 30 days (from the day it is first installed) this trial key will expire. At this point you can purchase a license to continue using our product (while retaining all of your existing setup) – no re-installation is required.

I would like to purchase a license for WinGate?

Choosing a suitable number of licenses. This is entirely dependent on the size of your network, and how frequently your users will be using the Internet once they have access. If your users will be permanently connected the Internet all of the time then they will require a separate license each. On the other hand, if they use it intermittently and at different times of the day then you can probably share a poll of licenses between them (WinGate will share these on a first-in-first-serve basis).

You can purchase the following licenses for each version of WinGate:

Number of Users	Plus	Pro	Enterprise
3	√	√	
6	√	√	
12	√	√	
25		√	
50		√	
Unlimited			√

Note that bandwidth (performance of the connection) is NOT related to the license count. Some people use the license count as an easy way to make sure that each user is receiving a sufficient amount of bandwidth. WinGate limits computers, but not bandwidth per computer. If you are having bandwidth problems, it may be because one or more users are using a large proportion of the available bandwidth for some activities.

How Does WinGate Count Licenses?

WinGate licenses are based on the number of computers connected to the Internet with WinGate at any one time. When a computer attempts to connect to the Internet, WinGate records it's unique private IP address and counts this as one connected user. The number of connected users permitted by WinGate will depend on the size of the license that you purchase. WinGate will accept connections from (and hence provide Internet access to) only the licensed number of computers at any one time. However, bear in mind that the Wingate server will always count as the first license.

Note About License Counts:

You should note that this license count includes computers connecting from anywhere, not just your LAN, so if you are allowing access to Internet users (e.g. access to a web server running on the local network) then you need to allow for these users as well. However, the license count **excludes** DHCP clients. This means **any** licensed version of WinGate will provide full DHCP to any number of clients.

Contact Information

You can get ***technical support*** from the dealer from whom you purchased WinGate. For purchasing, if you have obtained a trial key for WinGate, you should purchase your license from the dealer who provided your license.

All other contact for WinGate is handled by the Authors, ***Qbik New Zealand Ltd.*** at the following URL:
http://www.wingate.com

Sales inquiries may be made to sales@wingate.com
Other inquiries may be made to info@wingate.com

Documentation for WinGate is being revised and improved continuously. Please visit the WinGate web site occasionally for updated documentation and other information.
A full list of WinGate dealers, searchable by country is available at the following URL:
http://www.wingate.com/resellers

About Qbik New Zealand Limited

WinGate is owned and developed by **Qbik New Zealand Limited** - a software development company specializing in innovative Internet software solutions. Our main office is in Auckland, New Zealand. You can find out more about Qbik and our other products on our web site at: **http://www.qbik.com**

For any online WinGate support, you should see the following web site (for sales and any other general inquiries refer to the Contact information): **http://www.wingate.com**

For sales, support, and general inquiries, see the Contact Information.

Development	**QA**	**Website**
Adrien de Croy	Neil Gooden	Ryan Johnson
Tim Warren	Erwin Woodcock	
Gene Soudlenkov		
Scott Woods		
Pascal Janse van Vuuren		
Zan Oliphant		

Thanks also go to the many WinGate beta testers and supporters for giving their time and energy towards making WinGate the product that we are most proud of.

How To Use WinGate Help

Using the F1 Key to Load Context-Specific Help

This help has been designed to teach you about WinGate in an interactive way. While using GateKeeper or the WinGate Internet Client, you can press the **F1** key (the standard Help shortcut key) at any time to load **context-specific help**.

This means that the help loaded will apply to the screen that you are currently in. For example, pressing F1 while editing the DHCP Service properties will load help on configuring DHCP.

Using Hot Spots to Move Through Help

Most of the screen shots of GateKeeper that appear in help are loaded with **hotspots**. Hotspots allow you to click on areas of the interface in help as if you were using the real interface (e.g. menus, buttons, tabs and anything else you want to find out about). Some hotspots will jump you to the appropriate place in help, while others will simply pop-up a description of the item. The advantage is that you can explore the features of WinGate in a natural way, while reading about each feature as you go.

You can practice using hotspots on the dialog below, or return to the previous screen by clicking on the **BACK** button. Notice how the mouse pointer will change when it runs over a hot spot – this will help you find the hot spots in other screens.

How To Use WinGate Help

Using the F1 Key to Load Context-Specific Help

This help has been designed to teach you about WinGate in an interactive way. While using GateKeeper or the WinGate Internet Client you can press the **F1** key (the standard Help shortcut key) at any time to load ***context-specific help***.

This means that the help loaded will apply to the screen that you are currently in. For example, pressing F1 while editing the DHCP Service properties will load help on configuring DHCP.

Using Hot Spots to Move Through Help

Most of the screen shots of GateKeeper that appear in help are loaded with **hotspots**. Hotspots allow you to click on areas of the interface in help as if you were using the real interface (e.g. menus, buttons, tabs and anything else you want to find out about). Some hotspots will jump you to the appropriate place in help, while others will simply pop-up a description of the item. The advantage is that you can explore the features of WinGate in a natural way, while reading about each feature as you go.

You can practice using hotspots on the dialog below, or return to the previous screen by clicking on the **BACK** button. Notice how the mouse pointer will change when it runs over a hot spot – this will help you find the hot spots in other screens.

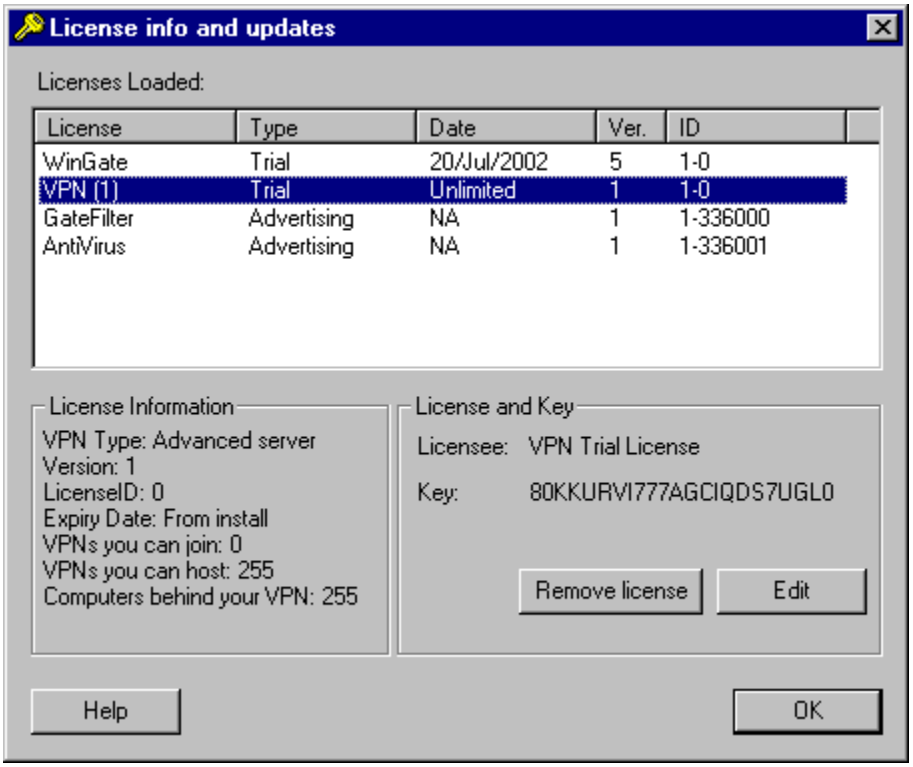
Feature Unavailable with this License

This feature is unavailable because you have not yet upgraded to the latest version of WinGate (this feature is part of the latest version). Though we'd love to keep giving you more for free, we have to make money somewhere.

Go to http://wingate.com/pricing to review your new or upgrade license options.

License Information

Use this window to review, add, and amend licensing information.



Clicking on the 'New' button pops up a new window, allowing you to input 'Licensee' and 'Key' information into this dialog.

Highlighting a license does three things:

1. It displays useful information in the 'License Information' field.
2. It turns the 'New' button into an 'Edit' button (allowing you to amend license information).
3. It makes the 'Remove License' button functional.

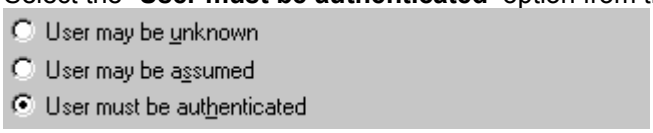
User Authentication With The WGIC

You can require users to **securely authenticate** themselves through the WinGate Internet Client (WGIC login dialog displayed above). This is configured in the *WRP Service policies* using GateKeeper (if it was on the WGIC then users could simply turn it off/on at their leisure).

Requiring users to authenticate for WRP has the following advantages:

- Prevents *unauthorized* users gaining Internet access from unattended computers
- Prevents users installing their own *unauthorized* copy of the WinGate Internet Client
- Provides improved control and logging of individual users.

1. In GateKeeper open the *properties for the WRP Service* and click on the *policies* tab
2. Double-click on the **policy recipients** (typically this will be "Everyone")
3. Select the '**User must be authenticated**' option from the radio button group:

4. Now click **OK** and make sure that you have configured the '*Default rights (System Policies):*' combo box appropriately (typically this will be **"are ignored")**.

   à Click here to learn more about integrating Service Policies (apply per-service) and System Policies (apply to all services).

Now all client computers will be presented with the WGIC logon dialog the *first* time an application attempts to use WinGate WRP.

Security Concepts in WinGate

WinGate has been designed to provide a very high level of security, and to allow great flexibility of accounting for use of the Internet. There are a number of major concepts in the way that the security features of WinGate govern its actions. These center on the following WinGate security objects:

Users

A user is someone or something that is obtaining service from WinGate. To keep track of all the users in WinGate, there is a **User Database**, and the **User Authentication Service** (UAS - which is a key component of the **Remote Control Service**) handles the authentication of users when this is required. User records in the database have a number of associated privileges and track data about the user's use of WinGate.

Computers

A computer in WinGate is a record of a physical machine that is connected to WinGate. Computers are tracked according to their private IP numbers, which should be assigned uniquely on your local network. Each computer is associated with a **Confidence Level** that corresponds with how confident WinGate is about the identity of the user on that computer (by default a computer will be 'unknown').

The 3 Confidence Levels are:

Unknown — WinGate has no prior information about the user

Assumed — WinGate makes an assumption about who the user is, based upon the IP number of the machine connected or the network name of the computer (this is set up under 'Locations' in GateKeeper). In addition, users can make use of insecure authentication in Telnet or Socks Proxy Service to achieve an assumed level of authentication. These methods are not recommended as they are not encrypted, and therefore not secure.

Authenticated — WinGate knows who the user is because they have been properly authenticated.

Note that with WinGate the terms 'Logged In' and 'Authenticated' are used synonymously.

WinGate Security Policies

Policies in WinGate can be implemented at both the system level and on a service-by-service basis. You can create a mix of policies at both levels to enforce the level of security required for your network.

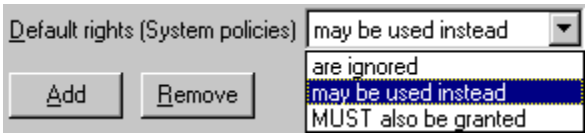
System Policies (All-Services)

System Policies are the *primary* way for implementing security and control with WinGate. Policies can now be defined per service, per user, per group as well as per time of day, and can be restricted on a per request basis. These are the overall restrictions that apply to all services (unless these are overridden at

the service policy level).

Service Policies (Per-Service)

Service Policies are the *secondary* way for implementing security and control with WinGate. These rules are evaluated only for the service that they are applied to. However, it is important to integrate the policies that apply for services (Service Policies) with those policies that apply to everything (System Policies). You do this by specifying one of the options below when you define rights for a service.



"are ignored" – this means System Policies do not apply for this service (in which case you must be careful when creating these rules as they will be the *only* security for that service)

"may be used instead" – this means that something permitted by the Service Policies may be restricted by the System Policies. This option implements two-levels of security so it can be considered reasonably secure.

"MUST also be granted" – this is the greatest level of security as both policies must explicitly grant rights for a user. Of course, it is also the least flexible of these three approaches.

Consider the Following Scenario for Controlling WRP:

You want to set up a minimal set of security policies and restrictions that will apply for all WinGate services (and hence all types of Internet access from your LAN). You implement these policies at the **System Level**. However, because the WinGate Internet Client will connect "any" Internet applications that demand it, you want to implement far tighter control over the WRP Service. You implement these tighter policies at the **Service Level**, selecting System Level policies '*are ignored*' in the WRP service properties.

Custom Groups and Users

With WinGate Pro and WinGate Enterprise you can create custom groups or users. This allows you to create different levels of security that can be applied to 'groups' of users. This is time saving and is an effective way of managing security on your network.

{ewl RoboEx32.dll, WinHelp2000, }