

## Introduction to the WinGate AntiVirus

Welcome to the WinGate AntiVirus!

A plug-in available with WinGate 5.0 and beyond, the Visnetic AntiVirus plugin for WinGate comes complete with a range of configurable options that will help keep your network safe from viruses. It's 'set and forget' software – simply configure the WinGate AntiVirus and let it take care of the rest. All you have to do is keep your virus definitions up-to-date.

The engine powering the WinGate AntiVirus comes from Kaspersky Labs, providers of superior data-security technologies and software.

Kaspersky's market-leading product is the Kaspersky AntiVirus, a product well-known for its rapid ability to identify virus definitions as new virus threats are introduced.

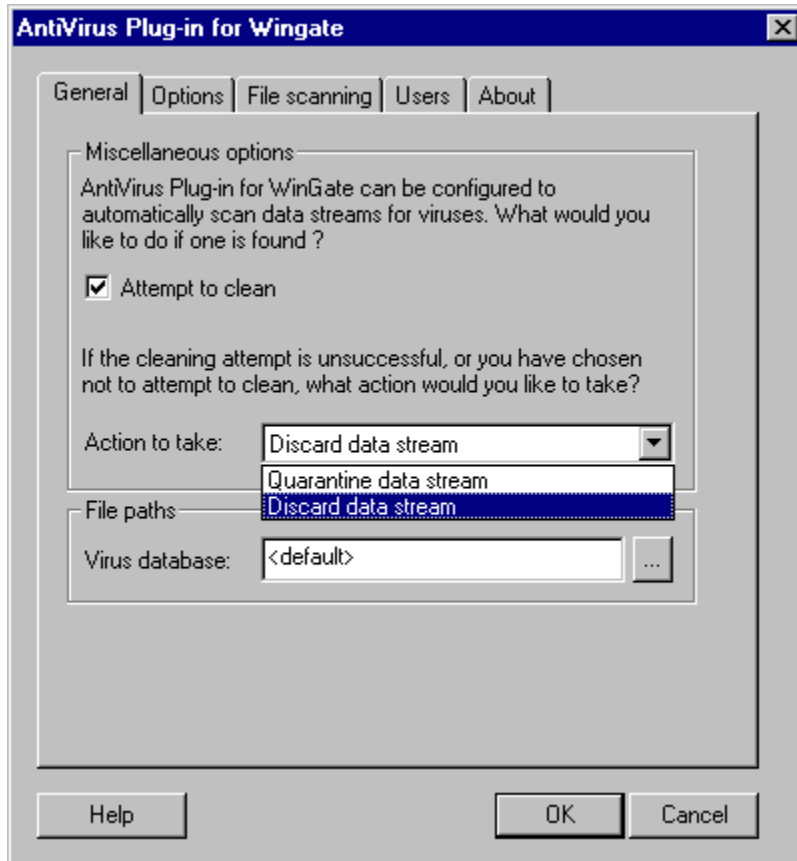
The WinGate AntiVirus plugin is powered by the **Kaspersky Anti-Virus 4.0** engine.

The main features of the WinGate AntiVirus engine are:

- protection against viruses, worms, trojan horses, time bombs, drop dead devices or other malicious code.
- advanced scanning techniques, that identify, quarantine or eradicate infected files on servers, workstations and personal computers.
- full support for all operating systems, including Windows XP.
- a quarantine feature for isolating infected and suspicious objects.
- module-based design allowing for both savings in operating memory and increased stability (whereby possible errors in the anti-virus application operation do not affect system functioning as a whole).
- rapid, daily updating of virus signatures as new viruses are introduced.
- The ability to scan incoming / outgoing data streams from your WinGate server.

## General Tab

Use this tab to select general settings in the WinGate AntiVirus.



### Miscellaneous Options:

**Action to Take-** Your options are:

- Quarantine data stream – this option will force WinGate send the infected file(s) to a quarantine folder on the server.
- Discard data stream – this option will force WinGate to delete the data stream upon discovery of a virus – no quarantine.

Note: Due to the way WinGate AntiVirus scans the data stream when using FTP, the client may still receive up to 75% of each individual file in the stream. WinGate will then notify the user that the download was infected.

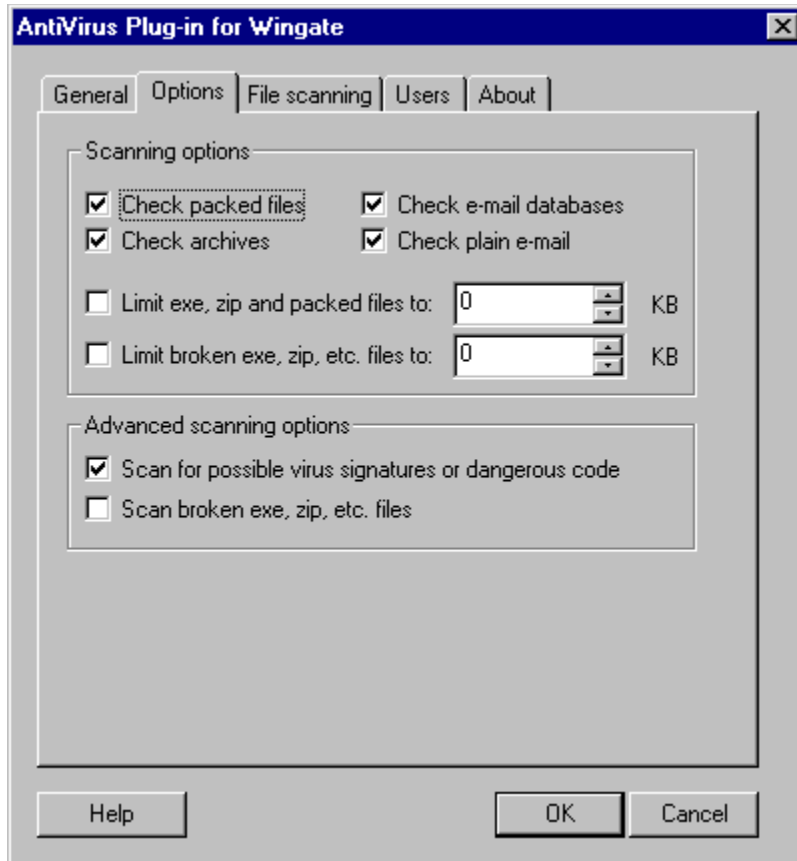
### File Paths:

**Virus database-** This is the location of virus definitions on your machine.

## Options Tab

Use this tab to select more advanced options for the WinGate AntiVirus. If in doubt, we suggest you keep the defaults.

**NB:** This tab will only be available if your version of the Deerfield / Kaspersky antivirus engine is up to date.



### Scanning options:

**Check packed files-** This refers to compressed and self-extracting files, like .exes and .zip files.

**Check archives-** Check this box to include in the scan all files marked as 'Archived'.

**Check email databases-** This refers to any file containing, or relating to, email.

**Check plain email-** This refers to .eml files

**Limit exe, zip and packed files to-** You may not wish to scan files over a certain size. Enter the upper limit here.

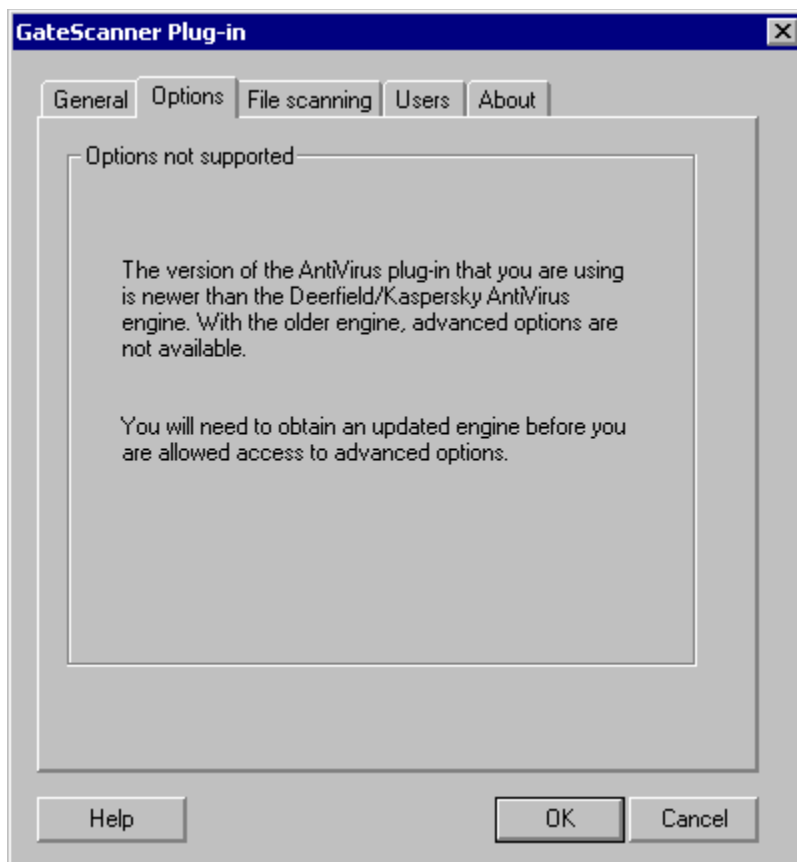
**Limit broken exe, zip etc, files to-** You may not wish to scan broken files over a certain size. Enter the upper limit here.

### Advanced scanning options:

**Scan for possible virus signatures or dangerous code-** This generally refers to VB/Runtime scripts that could contain viruses or other damaging code.

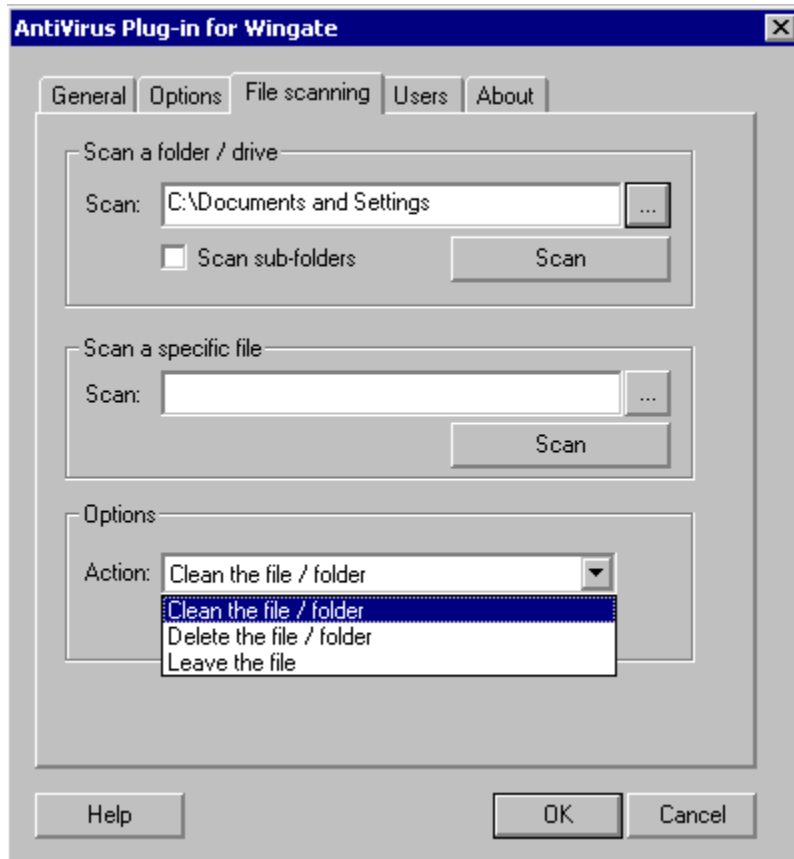
**Scan broken exe, zip, etc. files-** Check this box to include broken files of any kind in your scan.

**Note:** If your version of the Deerfield / Kaspersky AntiVirus Engine is older than the WinGate AntiVirus plug-in, then the following screen will display –



## File Scanning Tab

Use this tab for selecting particular drives, folders and files to scan on an ad hoc basis. This tab does not however, set overall configuration preferences - use the General and Options tabs for this.



### Scan a Folder / Drive:

**Scan-** Select a particular folder or drive on your machine that you want to scan.

**Scan sub-folders-** Selecting this option will perform the scan on all folders inside the folder you have chosen in the 'Scan' field.

### Scan a Specific File:

**Scan-** Select a particular file on your machine that you want to scan.

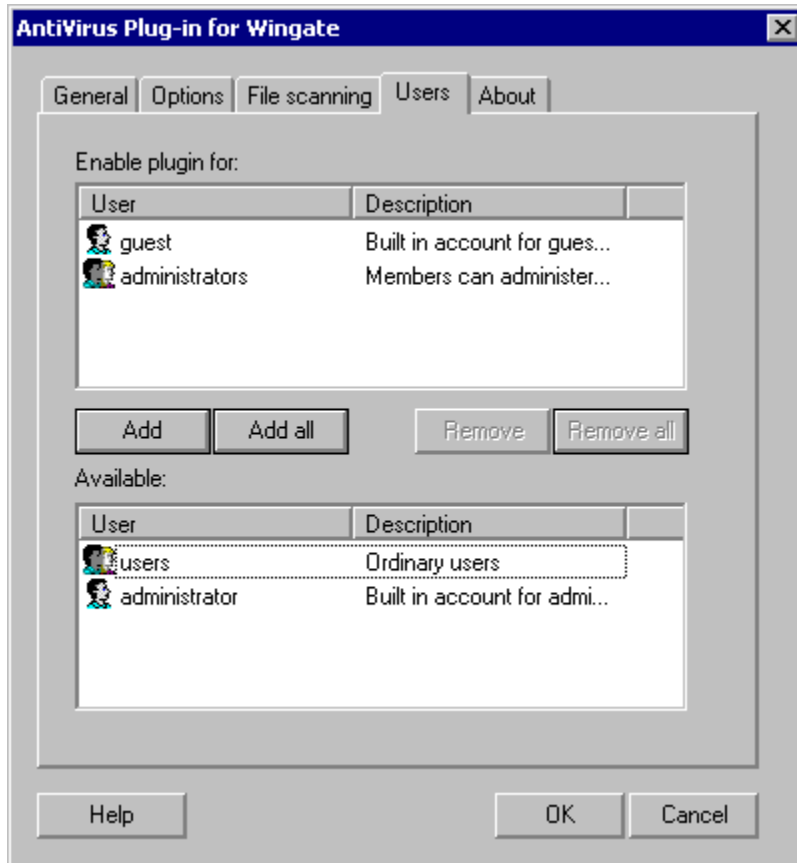
### Options:

**Action-** Select what action you want to perform to the selected file(s). Your options are-

- Clean the file / folder – if unsuccessful, you will be presented with the option of deleting.
- Delete the file / folder – sends the infected files/folders to your Recycle Bin.
- Leave the file – this option neither cleans nor deletes, it simply leaves the file/folder where it was. This is not recommended, as it is potentially dangerous if you forget that the file/folder is infected with a virus.

## Users Tab

This screen allows you to change the users/ user groups for whom GateScanner is enabled or disabled.



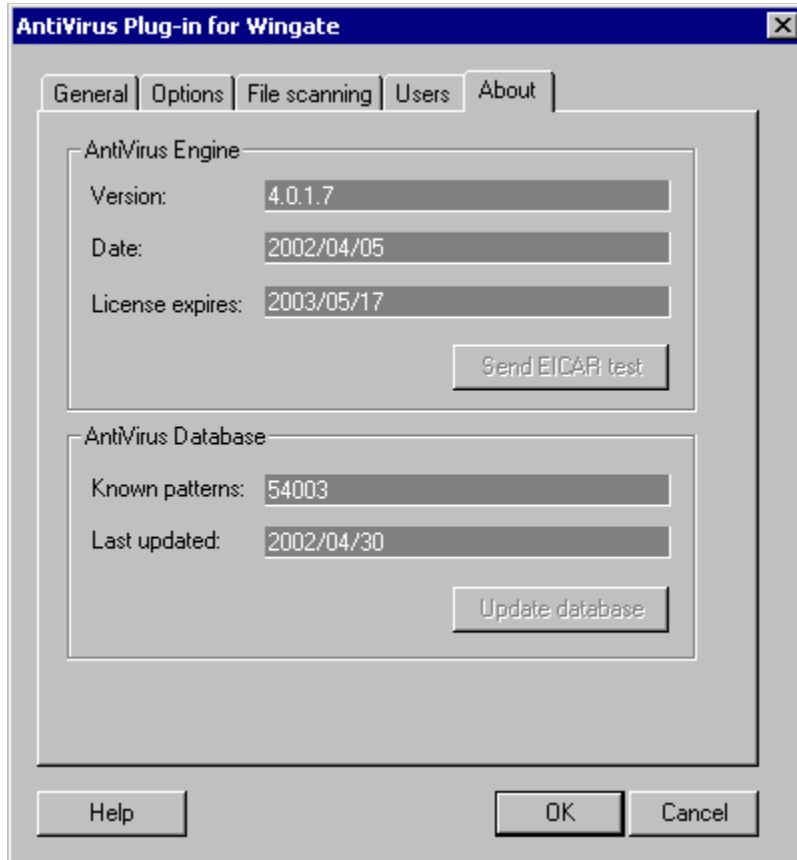
Double-clicking on a user/ group in the 'Available' field, sends that user/ group to the 'Enable plugin for' field, thereby making this particular user/ group subject to the current configuration settings for the GateScanner plugin.

Similarly, double-clicking users/ user groups in the 'Enable plugin for' field sends the user/ user group to the 'Available' field, thereby deselecting the particular user/ group.

You may perform the same functions by simply highlighting the user(s)/ group(s) and clicking 'Add' or 'Remove' as required.

## About Tab

This tab contains information about the Kaspersky Antivirus Engine and Database.



### AntiVirus Engine:

**Version-** This is the version number of the Kaspersky engine you have installed.

**Date-** This denotes the date you installed this version of the Kaspersky engine.

**License Expires-** This expiry date refers to the license provided by the Kaspersky AntiVirus engine. This is distinct from the license you have for the WinGate AntiVirus plugin.

**Send EICAR Test-** Click this button if you want to actively test your AntiVirus program with the EICAR virus – please note that this virus contains no malicious code and cannot damage your system. It will however, test the effectiveness of your virus protection.

### AntiVirus Database:

**Known Patterns-** This number denotes the number of viruses, or virus patterns, that the Kaspersky engine protects your system from.

**Last Updated-** This is the date that you last updated your virus definitions.

**Update Database-** This command fetches the last virus definition update issued, and downloads it to your machine.

