Avira AntiVir WebGate / Avira WebGate Suite

User Manual

AVIRA

1 About this Manual

This Chapter contains an overview of the structure and content of this manual.

After a short introduction, you can read information about the following issues:

- The Structure of the Manual – Page 5
- Signs and Symbols – Page 5
- Abbreviations – Page 6

1.1 Introduction

We have enclosed in this manual all the information you need about Avira AntiVir WebGate and it will guide you step by step through installation, configuration and operation of the software.

The appendix contains a Glossary, which explains the basic terms.

The RELEASE_NOTES file included in the product kit presents additional current information about Avira AntiVir WebGate.

For further information and assistance, please refer to our Website, to the Hotline of our Technical Support and to our regular Newsletter (Service – Page 86).

Your Avira Team

1.2 The Structure of the Manual

The manual of your AntiVir software consists in a number of Chapters, bringing you the following information:

Chapter	Contents
1 About this Manual	The structure of the manual, signs and symbols
2 Product Information	General information about Avira AntiVir WebGate software, its modules, features, system requirements and licensing
3 Installation	Instructions to install Avira AntiVir WebGate on your system
4 Configuration	Directions for optimum setting of Avira AntiVir WebGate on your system
5 Operation	Working with Avira AntiVir WebGate; Reactions when detecting viruses and unwanted programs
6 Updates	Running manual or automatic updates
7 Service	Avira Operations GmbH & Co. KG Support and Service
8 Appendix	Glossary of technical terms and abbreviations Golden Rules for Protection against Viruses

1.3 Signs and Symbols

The following characters and symbols are used in this manual:

Symbol	Meaning
✓	placed before a condition which must be fulfilled prior to performing an action.
▶	placed before a step which has to be completed.
↳	placed before an event resulting directly from the previous action.
	placed before an alert warning of critical data loss or hardware damage.
	placed before a particularly important piece of information, for example, relating to steps being carried out.
	denotes a tip facilitating the understanding and operation of the Avira AntiVir WebGate.

For improved legibility and clear marking, the following types of emphasis will also

be used in the text:

Emphasis in text	Explanation
Ctrl+Alt	Key or key combination
/usr/lib/AntiVir/webgate/avupdate-webgate	Path and filename
`ls /usr/lib/AntiVir/webgate`	User entries
Choose component **Select all**	Elements of the software interface such as menu items, window titles and buttons in dialog windows
http://www.avira.com	URLs
Signs and Symbols – Page 5	Cross-reference within the document

1.4 Abbreviations

The manual uses the following abbreviations:

Abbreviation	Meaning
ACL	Access Control List
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
SMTP	Simple Mail Transfer Protocol
SNEWS	Secure News Server
SSL	Secure Sockets Layer
VDF	Virus Definition File

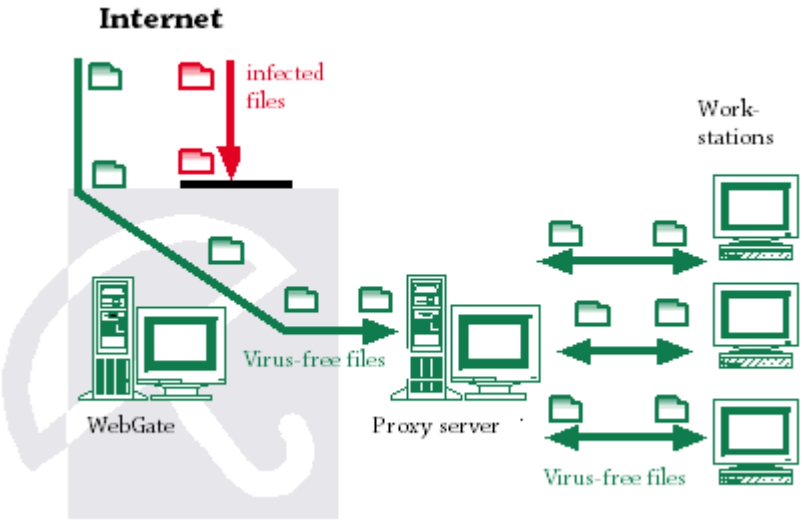
2 Product Information

Internet connection is an underestimated invasion doorway for malware on your computer. If you transfer unfiltered data from the Internet on your system, you can spread all types of malware throughout the entire network.

Avira AntiVir WebGate is a reliable protection for your computer, by scanning, filtering and if necessary blocking access to all files from the Internet.

Furthermore, Avira AntiVir WebGate also scans the entire outgoing traffic.

Usually company computers access the Internet indirectly, via a proxy server. Avira AntiVir WebGate co-operates with the proxy server and completes it in an ideal way.



Right from the beginning, two really important hints:

Losing valuable files usually has dramatic consequences. Not even the best antivirus software can fully protect you against file loss.

▶ Ensure regular backups for your files.

An antivirus program can be reliable and effective only if kept up-to-date.

▶ Ensure that you maintain your Avira AntiVir WebGate up-to-date, using Automatic Updates. You will learn how to do it in this user guide.

2.1 Features

Avira AntiVir WebGate supports a variety of configuration settings for controlling Internet data transfer. The essential features are:

- Extended access control, for setting rules to allow tunneling for certain types of requests and responses.
- Local URL filtering, using the categories in Avira URL Filtering library
- Online URL filtering, using the categories in Avira Web Access and Content Control library (available in **Avira WebGate Suite**)
- Real-time scanning for viruses/unwanted programs
- Heuristic detection of macroviruses
- Scanning all downloaded files (HTTP and FTP)
- Scanning all outgoing files (e. g. PUT and POST)
- Recognition of all common archive types
- Automatic Internet Update for product, scan engine and VDF
- Configurable notification functions for the administrator (protocol, warnings, reports); sending email warnings (SMTP)
- Self-Integrity Program Check, which ensures the antivirus system is operating correctly
- Access control to WebGate using IP addresses
- ICAP support (enables connection through ICAP interface)

2.2 Licensing Concept

You must have a license to use Avira AntiVir WebGate. You are required to accept the license terms
(see http://www.avira.com/en/license-agreement).

There are 2 license modes for Avira AntiVir WebGate:

- Test version
- Full version

The license depends upon the number of users in the network, which are to be protected by Avira AntiVir WebGate.

The license is given in a license file named hbedv.key . You will receive it by email from Avira Operations GmbH & Co. KG. It contains certain data, such as the programs you will use and the time interval of your license. The same license file may refer to more Avira products.

Test Version

Details about the 30-days Test License can be found on our Website:

http://www.avira.com.

Full Version

The range of Full Version features includes:

- Download of Avira AntiVir WebGate Versions from the Internet
- License file by email, for activating the Test Version to a Full Version
- Complete installation instructions (digital)
- Four weeks Installation Support, starting from acquisition date

- Newsletter Service (per email)
- Internet Update Service for program files and VDF

After installing an AntiVir product, you can read the information on your current license, using the license tool avlinfo:

▶ Change to /usr/lib/AntiVir/webgate and call `./avlinfo`

Use `avlinfo -h` to get information about using this tool.

2.3 Modules and Operating Mode of Avira AntiVir WebGate

Avira AntiVir WebGate security software consists in the following modules:
- AntiVir Engine
- Avira Updater
- WebGate Main Program
- Avira URL Filtering library
- Avira Web Access and Content Control library

AntiVir Engine AntiVir Engine essentially represents the scanning and repairing modules of Avira software.

Avira Updater Avira Updater downloads current updates from the Avira AntiVir web servers and installs them at regular intervals, manually or automatically. It can also send update notifications by email.

You can update Avira AntiVir WebGate entirely or only certain components: signatures, engine, scanner.

WebGate Main Program The Main Program is the actual WebGate function, supervising the HTTP and FTP network access over the Internet. It detects viruses and unwanted programs using the Avira AntiVir Engine.

Avira URL Filtering library Avira AntiVir WebGate uses a local filter to determine if an URL is dangerous, based on a list of known URLs, grouped in three categories: Malware, Phishing, Fraud. To increase your security, Avira URL Filter is enabled in every valid WebGate or WebGate Suite installation.

Avira Web Access and Content Control library AntiVir WebGate allows clients to filter outgoing requests based on URL categories, such as *Violence*, *Gambling*, *Erotic* etc. To determine the categories for a certain URL, the Web Access and Content Control library is used. (This module is only activated with the license for **Avira WebGate Suite**.)

To find out more details about the Web Access and Content Control library, please refer to WebGate's installation directory.

2.3.1 System Requirements

Avira AntiVir WebGate asks for the following minimum system requirements:
- Computer: x386, Sparc
- OS: Linux or Sun Solaris

- CPU: 32-bit or 64-bit UNIX
  Running AntiVir software on 64-bit UNIX systems, requires the ability to execute 32-bit binaries. For instructions about checking and eventually enabling this behavior, please refer to the documentation of your UNIX system.
- HD: 10 GB (recommended 50+GB) space on configured TemporaryDir for downloading and scanning large files and 1 GB temporary space needed for unpacking archives
- RAM: 512 MB (recommended 2GB)

The versions for Linux and Solaris use similar installation and application processes (normally only a few file names are different, depending on the target system).

Officially supported distributions for Avira AntiVir WebGate and for Avira WebGate Suite:

- Red Hat Enterprise Linux (RHEL) Server 5.8
- Red Hat Enterprise Linux (RHEL) Server 6.2
- Novell SUSE Linux Enterprise Server (SLES) 11 SP2
- Novell SUSE Linux Enterprise Server (SLES) 10 SP4
- Debian GNU/Linux 5.0
- Debian GNU/Linux 6.0
- Ubuntu Server 10.04 LTS
- Ubuntu Server 11.10
- Ubuntu Server 12.04 LTS
- Sun Solaris 9 (SPARC)*
- Sun Solaris 10 (SPARC)

* supported until 2012-12-31

3 Installation

You can find the current version of Avira AntiVir WebGate on our Website: http://www.avira.com/en/support-download-avira-antivir-webgate.

Avira AntiVir WebGate is supplied as packed archive. This archive contains the AntiVir Engine and VDF files, the Avira Updater, the WebGate Main Program and the optional SMC plug-in.

You are guided through the installation process, step-by-step. This Chapter is composed of the following Sections:

Choosing the WebGate Computer

Getting the Installation Files

Licensing

Installing Avira AntiVirWebGate

Reinstalling and uninstalling AntiVir

3.1 Choosing the WebGate Computer

Depending on network and hardware configuration, there are more possibilities for choosing an Avira AntiVir WebGate computer, as a “guard” between the user’s client and the Internet.

A connection to the proxy server is especially needed, for ensuring a controlled Internet access.

Avira AntiVir WebGate is adjusted first in terms of network configuration (Configuration – Page 18). At the time of the installation, it must be decided on which computer WebGate will be installed.

Caution: If you have also installed Avira AntiVir UNIX Server or Avira AntiVir Professional (UNIX) and you use the Graphical User Interface to configure and operate these products, please note that the GUI is not compatible with the current versions (starting with version 3) of Avira AntiVir UNIX MailGate and Avira AntiVir UNIX WebGate.

3.2 Getting the Installation Files

Downloading the Installation Files from the Internet

Download the current version file from our Website
http://www.avira.com/en/support-download-avira-antivir-webgate
on your local computer. The file name is
antivir-webgate-prof.tgz.

Save the file in a */tmp* folder on the computer, on which you want to run WebGate.

Unpacking Program Files

Go to the temporary directory:

```
cd /tmp
```

Unpack the AntiVir archive:

```
tar -xzvf antivir-webgate-prof-<version>tar.gz
```

in the temporary directory will then appear antivir-webgate-prof-<version> .

3.3 Licensing

You must have a license for AntiVir WebGate, in order to use the program (see Licensing Concept). The license comes in a file named hbedv.key.

This license file contains information regarding the range and period of the license.

Purchasing the License

You can request a 30-day Test License for Avira AntiVir WebGate from our website (www.avira.com).

You will receive the license file by email.

You can easily acquire Avira AntiVir WebGate using our Online Shop (for details, visit http://www.avira.com).

Copying the License File

Copy the license file hbedv.key in the installation directory on your system: /tmp/antivir-webgate-prof-<version>.

3.4 Installing Avira AntiVir WebGate

Avira AntiVir WebGate installation is performed automatically using an installation script. This script performs the following tasks:

- Checks integrity of the installation files
- Checks for the required permissions for installation
- Checks for existing installed versions of AntiVir products on the computer
- Copies the program files and overwrites the existing obsolete files
- Copies the configuration files. Existing AntiVir configuration files are kept
- Installs Avira Updater
- Optionally: installs the plug-in for SMC
- Optionally: configures the automatic start of Avira AntiVir WebGate and Avira Updater

For the first installation, you must follow these steps:

Preparing Installation – Page 13

Installing Avira AntiVir WebGate – Page 13

Preparing Installation

Login as **root**. Otherwise you don't have the required authorization for the installation and the script returns an error message.

Caution: To run Avira Antivir WebGate on a client with active firewall, WebGate needs the following open ports:
`localhost tcp: 50358` (only for SMC user) and `udp port 51973` (if `DBSupport` is set to `YES`)

Go to the directory where you have unpacked Avira AntiVir WebGate:

```
cd /tmp/antivir-webgate-prof-<version>
```

Installing Avira AntiVir WebGate

Note: Depending on the AntiVir products you have already installed on your computer, the installation procedure may vary.

Type:

```
./install
```

Confirm the License Agreement.

The installation script starts. First, the AntiVir Core Components are installed:

```
Do you agree to the license terms? [n] y

creating /usr/lib/AntiVir/webgate ... done
copying LICENSE to /usr/lib/AntiVir/webgate/LICENSE-webgate ... done
1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying uninstall to /usr/lib/AntiVir/webgate... done
copying uninstall_smcplugin.sh to /usr/lib/AntiVir/webgate ... done
```

After you type the path to the key file, the installer continues with updates configuration:

```
Enter the path to your key file: [] /root/Desktop/HBEDV.KEY
copying /root/Desktop/HBEDV.KEY to /usr/lib/AntiVir/webgate/hbedv.key ... done
installation of AntiVir Core Components (Engine, Savapi and Avupdate) complete

2) Configuring updates
An internet updater is available...
...

Would you like to create a link in /usr/sbin for avupdate-webgate ? [y]
```

Type **Y**.

Then the script can create a cron task for automatic Scanner updates:

```
linking /usr/sbin/avupdate-webgate to /usr/lib/AntiVir/webgate/avupdate-webgate ... done

Would you like to setup Scanner update as cron task ? [y]
```

Type **Y**, if you want to create these cron tasks.

Then eventually select the interval to check for updates:

```
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
```

Type **Enter**, if you want to check for updates every 2 hours,
or type **d**, if daily.

Then the script asks, if you want to check for product updates once a week:

```
creating Scanner update cronjob ... done

Would you like to check for WebGate updates once a week ? [n]
```

Type **Y**, if you want to create this task.

The next step of the installation process is installing the main program:

```
creating WebGate update cronjob ... done

setup internet updater complete

3) installing main program
copying doc/antivir_webgate_en.pdf to /usr/lib/AntiVir/webgate ... done
copying bin/linux_glibc22/avwebgate.bin to /usr/libAntiVir/webgate... done
```

The program is installed. Then you are asked if you want to create a link to avwebgate and if the Updater should be automatically activated at system start:

```
Would you like to create a link in /usr/sbin for avwebgate ? [y]
linking /usr/sbin/avwebgate to /usr/lib/AntiVir/webgate/avwebgate ... done

Please specify if boot scripts should be set up.
Set up boot scripts [y]:
```

Confirm with **Enter**. You can change these settings later.

The automatic system start is configured:

```
setting up boot script ... done
installation of main program complete
```

Then you are asked if you want to install WebGate with the optional plug-in for AntiVir Security Management Center.

```
4) activate SMC support
If you are going to use AVIRA Security Management Center (SMC)
to manage this software remotely you need this

Would you like to activate SMC support? [y]
```

If you are using Avira SMC:

Type **Y** or confirm with **Enter**.

The plug-in is installed and the installation process completed:

```
Installation of the following features complete:
    AntiVir Core Components (Engine, Savapi and Avupdate)
    AVIRA Internet Updater
    AVIRA WebGate
    AntiVir SMC plugin
```

Finally, you can start Avira AntiVir WebGate:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

Modified binaries will not run.
For example, if binaries are prelinked: Either disable prelinking or add /usr/lib/AntiVir/webgate as an excluded prelink path in /etc/prelink.conf.

***Warning**: Starting with version 3.0.0, a new scanner backend is used. Old scanner specific configuration options, that are not known to WebGate, must be moved from*
/etc/avira/avwebgate.conf
to the scanner specific configuration file
/etc/avira/avwebgate-scanner.conf.

***Caution**: It is highly recommended that you perform an update after installation, to*

ensure up-to-date protection. This can be done by running:

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=WebGate
```

For more details on updating, *Updates – Page 85.*

3.5 Reinstalling and uninstalling AntiVir

You can re-launch the installation script anytime. There are more situations possible:

- Installing a new version (upgrade). The installation script checks the previous version and installs the necessary new components. The configuration settings already made are not overwritten, but inherited (Configuration – Page 18).
- Later installation of some components.
- Activating or deactivating the automatic start of Avira AntiVir WebGate or Avira Updater.

Reinstalling Avira AntiVir WebGate

The procedure is the same in all cases listed above:

Go to the temporary directory where you have unpacked AntiVir WebGate:

```
cd /tmp/antivir-webgate-prof-<version>
```

Type:

```
./install
```

The installation script runs as described above (see InstallingAvira AntiVir WebGate).

Make the necessary changes during installation.

Avira AntiVir WebGate is installed, with the desired settings.

Uninstalling AntiVir

If you want to uninstall Avira Antivir WebGate, you can use the *uninstall* script, located in your installation directory. The syntax is:

```
uninstall [--product=productname] [--no-interactive]
[--inf=inf file] [--force] [--skip] [--version] [--help]
```

where `productname` is `Webgate`.

Open the directory in which you have installed Avira Antivir WebGate:

```
cd /usr/lib/AntiVir/webgate
```

Type:

```
./uninstall --product=Webgate
```

The script starts uninstalling the product, asking you step by step, if you want to keep backups for the license file, for the configuration files and logfiles; it can also remove the cronjobs you made for WebGate and Scanner.

Answer the questions with **y** or **n** and press **Enter**.

AntiVir WebGate is removed from your system.

4 Configuration

You can configure Avira AntiVir WebGate for optimum performance. The most common settings are suggested in this Chapter. You can modify these settings anytime, to adjust WebGate to your requirements.

You will be guided step by step through the configuration process:

- In Monitoring HTTP Traffic – Page 18 you can read about the different possibilities for WebGate's network setting.
- Monitoring FTP Traffic – Page 22 is a description of integrating WebGate as FTP proxy.
- Integration over ICAP Interface – Page 23 presents the integration of WebGate over ICAP interface.
- In Configuration Files – Page 25 we describe the parameter entries for Product, Scanner, Updater and Access Control List.2
- In Templates Configuration – Page 45 you find out how to customize various notification web pages and emails generated by WebGate.

4.1 Monitoring HTTP Traffic

WebGate can scan the entire incoming and outgoing HTTP traffic for viruses and unwanted programs. It can even scan the web-based FTP transfers (FTP over HTTP). WebGate works with the existing proxy servers and supplements them, but it can also be set as stand-alone HTTP proxy.

Depending on the network and configuration, there are more possibilities for setting Avira AntiVir WebGate as "guard" between the Client computer and the Internet. In all these cases, the user does not have direct connection to the Internet, but through WebGate.

There are three different configurations:

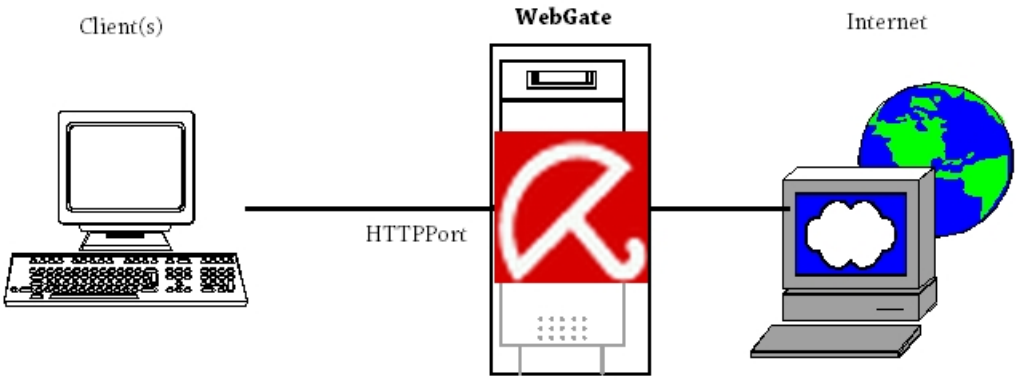
- WebGate without Proxy Server (Network Configuration 0) – Page 18
- WebGate between Client and Proxy Server (Network Configuration 1) – Page 19
- WebGate between Proxy Server and Internet (Network Configuration 2) – Page 21

If you set ports under 1024 during configuration, you have to run WebGate as root.

WebGate without Proxy Server (Network Configuration 0)

If there is no proxy server, WebGate stands between Clients and the Internet. It can be installed directly on Clients or on another computer.

WebGate directs the Clients' enquiries to the Internet and scans the answer from the Internet. The access to infected files from a Website is blocked and only not infected files are forwarded to the Client. From the Client's point of view, WebGate is functioning as a proxy server.



▶ Make the following settings in avwebgate.conf (example):

```
HTTPPort 8080
```

▶ Configure the browser according to the Clients.

If WebGate is installed on the actual Client, we recommend the following settings in avwebgate.conf*:*
`HTTPPort 127.0.0.1:8080`.

▶ For **HTTP Proxy** enter the IP address `127.0.0.1` or `localhost`.

The real settings can differ from those given in the example, but for a correct configuration, the settings in avwebgate.conf *must be compatible with the Client's browser configuration.*

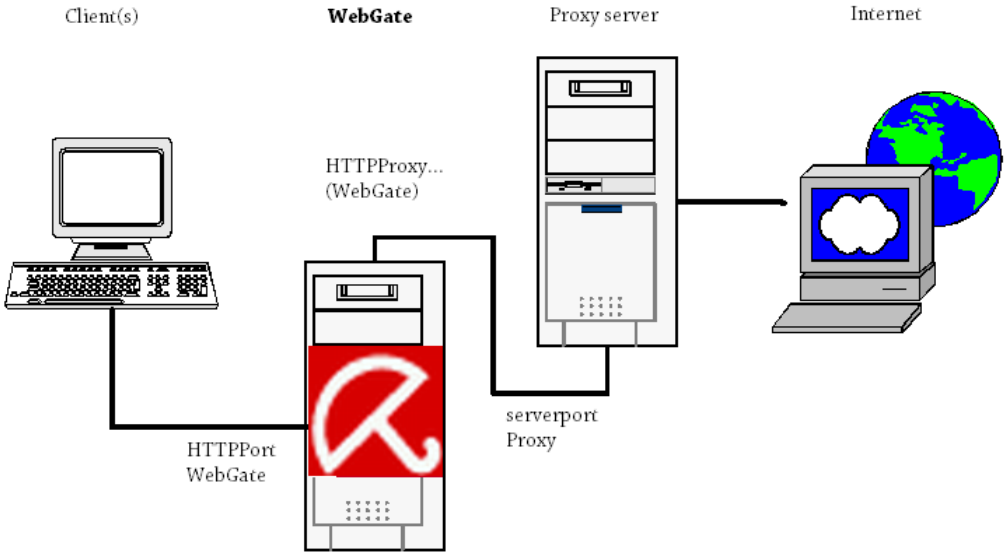
WebGate between Client and Proxy Server (Network Configuration 1)

In this configuration, the other proxy server can be attacked by malicious software. If you want complete protection for your proxy server (normally), network configuration 2 is recommended. See *WebGate between Proxy Server and Internet (Network Configuration 2) – Page 21.*

This configuration is suitable when the proxy is connected to other servers and the Clients need to be protected from infection. WebGate can be installed directly on the proxy server or on another computer.

WebGate directs the Client's inquiries through the proxy server to the Internet and scans the answers from the Internet, which are received through the proxy server. The access to infected files from a Website is blocked and only not infected files are

directed to the Clients.



If WebGate and the proxy server are installed on the same computer:
*It is usually easier to adapt the settings of the proxy server and to inherit the initial settings of the WebGate. In this way, you do not need to make any changes on the Clients.*This example assumes the following proxy server configuration:

```
host proxy.mycompany.com
serverport 3128
```

So, the proxy server communicates with the Clients over port 3128.

- ▶ Install WebGate on the machine proxy.mycompany.com.
- ▶ Make the following settings in avwebgate.conf (example):

  ```
  HTTPPort 3128
  ```

  ↳ Now, the Clients will communicate through WebGate for HTTP and FTP inquiries, not directly through the original proxy server. The browser settings on the Client computers must not be changed.

- ▶ Enter the following values in avwebgate.conf (example):

  ```
  HTTPProxyServer 127.0.0.1
  HTTPProxyPort 8080
  ```

  ↳ WebGate forwards the HTTP and FTP inquiries to localhost port 8080.

- ▶ Change the port of the original proxy server according to the value of `HTTPProxyPort` (in avwebgate.conf), so that it can contact WebGate. For example:

  ```
  serverport 8080
  ```

If WebGate is installed on the actual proxy server:

- ▶ Make sure that WebGate does not respond on the same server port, as is the case in the example above.

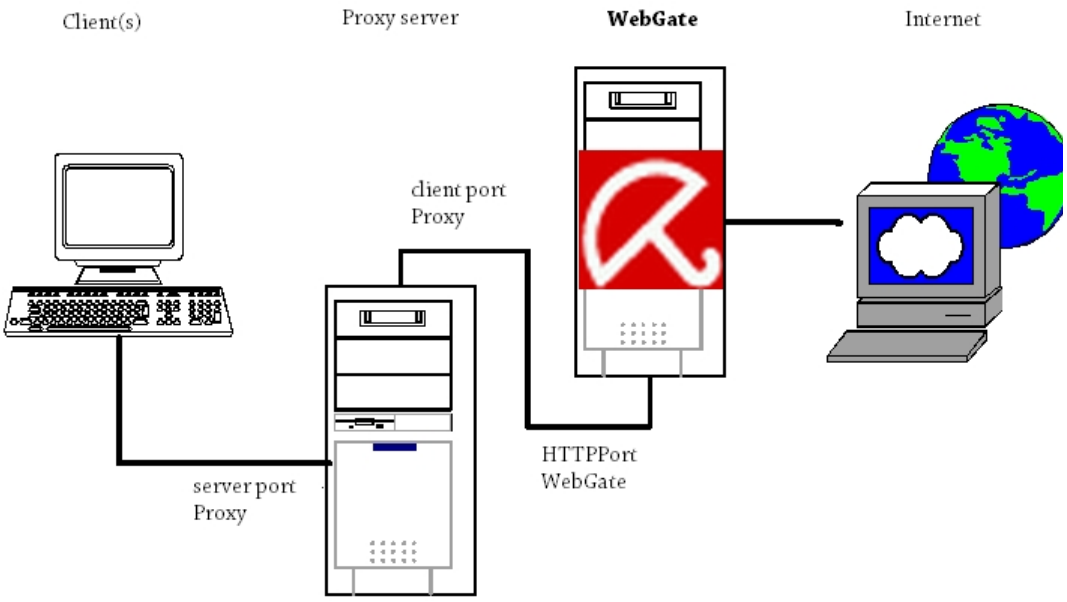
It is also possible to install WebGate on a computer, other than the proxy server. The settings must be done accordingly.

In this network configuration, a Client could also be a proxy server (for example, by installing WebGate between two proxies).

WebGate between Proxy Server and Internet (Network Configuration 2)

If you already use a proxy server, it is better to install WebGate between the proxy and the Internet. In this way malicious software is intercepted by the proxy server. WebGate can be installed directly on the proxy server machine or on another one.

WebGate directs the Clients' inquiries through the proxy towards the Internet and scans the answers from the Internet. The access to infected files from a Website is blocked and only uninfected ones are forwarded to the Clients, through the proxy server.



The example assumes the following configuration of the proxy server:

```
host proxy.mycompany.com
serverport 3128
```

So the proxy server responds on port 3128.

- Make the following settings in avwebgate.conf (example):

```
HTTPPort 8080
```

- Configure the other proxy server, so that it does not directly serve inquiries to the Internet, but directs them to WebGate (e. g. port 8080). This port must correspond to the value of `HTTPPort` in avwebgate.conf .

– *Example for a Squid proxy server:*
In this configuration, you must first start WebGate and then the proxy server. Squid proxy has to direct all inquiries to WebGate (parent proxy), so you have to configure the Squid configuration file squid.conf as follows:

```
cache_peer proxy.mycompany.com parent 8080 0 no-query
no-digest default

acl all src all

never_direct allow all
```

If WebGate is installed on the proxy server machine:

▶ Make sure that WebGate and the proxy server do not respond on the same server ports, such as is the case in the above example.

When a Client asks for data, which can be found on the proxy server's cache, it will receive its data directly from there. These data will not be scanned, until the cache is emptied. It bears a risk, because a new virus might "penetrate" and it could be forwarded to Clients, even if they have updated VDFs.

If you modify the proxy server's port, you have to adapt the settings of the Clients' browsers, which access the proxy.
It is usually easier to keep the proxy settings and to adapt the WebGate settings, just like in the above example.

4.2 Monitoring FTP Traffic

WebGate can also be set as **real** FTP proxy, so that it can scan the files transferred through an FTP Client and even block them. It scans both downloads and uploads.

▶ In avwebgate.conf set the port for the WebGate to communicate with the FTP Clients:

```
FTPPort 2121
```

Now, the FTP Clients can communicate to FTP servers, through WebGate, which means that the Clients have no direct connection to the FTP servers, but to WebGate. In order for WebGate to make a substitute connection to FTP servers, you need to specify the address and the name of the FTP servers. WebGate must receive this information from FTP Clients at login with the USER command:

```
USER <username>@<host>[:<port>]
```

Compared to making a direct connection to FTP server, the connection through WebGate also needs, apart from the user name at login, the host name – separated with the @ character from the user name – or the IP address (optionally with port) of the FTP server.

Example This example illustrates the login procedure, when using a standard Unix FTP

Client:

Assumption: WebGate runs on a machine with the IP address `192.168.0.1` and receives inquiries from FTP Clients on port 2121. You should establish a connection to a remote FTP server with the IP address `10.0.0.1`, the user name "foo" and the password "bar".

```
$ ftp 192.168.0.1 2121
Connected to 192.168.0.1.
220 AntiVir WebGate FTP proxy. Login with <user-
name>@<host>[:<port>]
Name (192.168.0.1:user): foo@10.0.0.1
331 Password required for foo.
Password: bar
230 User foo logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

On login, the FTP Client should be used just as before, i. e. when it was not using WebGate. WebGate acts as proxy between FTP Client and FTP server and scans the transferred data.

Many FTP Clients allow FTP proxy configuration. This enables a certain transparency of WebGate towards the user, i. e. the user senses no difference at login, when using the FTP Client with or without proxy.

Optionally, WebGate allows a parent FTP proxy. For example, it can be set in avwebgate.conf as follows:

```
FTPProxyServer 127.0.0.1
FTPProxyPort 21
```

In this case, WebGate does not communicate directly to the FTP server, but with the indicated parent FTP proxy. Thus, more FTP servers can operate consecutively.

In order to avoid Client timeouts during the transfer of larger files, WebGate sends Keepalive messages to the Client. The time interval is the value of `RefreshInterval` or – if this is 0 – the value of `KeepaliveInterval`. The ClientTimeout range is between 0 and 600.

Furthermore, WebGate sends "NOOP" commands to the server within the established `KeepaliveInterval`, so that it also maintains the connection to the server during sending and receiving larger files to or from the Client.

4.3 Integration over ICAP Interface

If there is a caching server with ICAP support in the network, WebGate can be

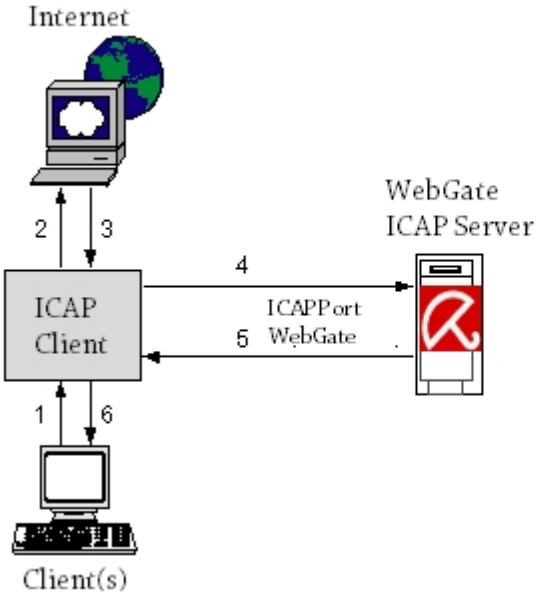
integrated with the ICAP interface. WebGate can still scan and block incoming (RESPMOD) and outgoing (REQMOD) files.

▶ In avwebgate.conf you must set the port, through which WebGate will communicate with the ICAP Client:

```
ICAPPort 1344
```

Scanning Incoming Data Traffic (Response Modification)

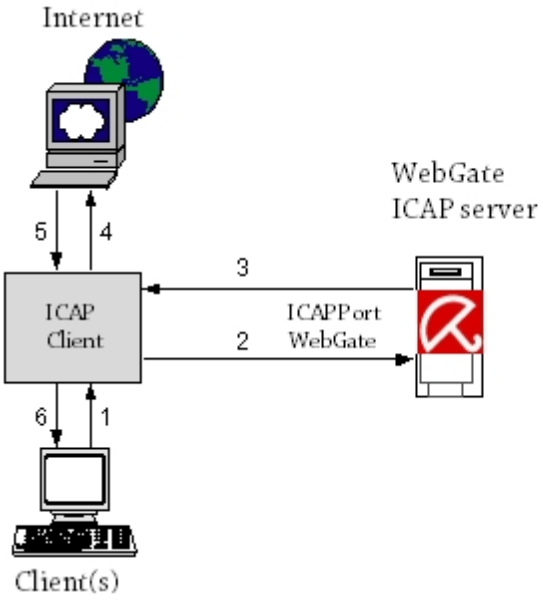
The ICAP Client sends an HTTP response for WebGate to scan (ICAP server). If the data is not infected, it is returned to the ICAP Client and from there forwarded to the Client. If the answer is blocked (e. g. in case of a virus detection), WebGate generates an HTML page, based on the corresponding HTML template, and sends this to the ICAP Client. The page is then forwarded to the Client instead of the original answer from the server.



Scanning Outgoing Data Traffic (Request Modification)

The ICAP Client sends an HTTP request to WebGate (ICAP-Server) for scanning. If the data is not infected, it is returned to the ICAP Client and from there it is sent to the destination server. If the request is blocked (i. e. in case of a virus detection), WebGate generates an HTML page, based on the corresponding HTML template, and sends this to the ICAP Client. In this case, the original request is not sent to

the server anymore.



You can find further details about ICAP server integration in the ICAP Client documentation.

4.4 Configuration Files

This part describes the contents of Avira AntiVir WebGate configuration files:

- /etc/avira/avwebgate.conf - Product configuration
- /etc/avira/avwebgate-scanner.conf - Scanner configuration
- /etc/avira/avupdate-webgate.conf - Updater configuration

The program is provided with default values, which are important for many procedures. Some options can be deactivated with a # at the beginning of the line (commented) or can be set with default values. These can be activated by removing the # character or by changing the values.

4.4.1 Product Configuration in avwebgate.conf

This section provides a short description of the entries in /etc/avira/avwebgate.conf. The settings affect only Avira AntiVir WebGate's behavior and no other Avira AntiVir programs. They partly depend on the basic configuration, on which WebGate has to run (see Monitoring HTTP Traffic – Page 18).

Proxy Settings

Contains settings that control the ports WebGate listens to and what type of connections are accepted. With no configured options WebGate will only listen to HTTP connections.

HTTPPort

Port for scanning HTTP connections:
This sets the port on which WebGate responds to HTTP requests from Client or proxy computers. There are various setups needed, according to the configuration (see Monitoring HTTP Traffic – Page 18).
The default is:

```
HTTPPort [host_ip_or_name:]8080
```

*We recommend **not to** allow access to WebGate from outside your network. WebGate should be therefore connected only to the internal network interface. If you have installed WebGate as parent proxy on the same computer as your existing proxy server, we recommend for example, the following settings:*

```
HTTPPort 127.0.0.1:8080.
```

If neither hostname nor IP address are specified, the port is linked to all interfaces.

FTPPort

Port for scanning FTP connections:
WebGate can also monitor **real** FTP connections. Unlike "FTP over HTTP", WebGate communicates with the Client over FTP. This entry sets the port on which WebGate responds to Client computers or to the FTP proxy server for FTP connections.

Example:

```
FTPPort [hostname_or_ip:]2121
```

Default:

```
NONE
```

ICAPPort

Port for ICAP support:
WebGate can be integrated with the ICAP interface (as ICAP server). This entry sets the communication port between WebGate and the ICAP Clients.

Example:

```
ICAPPort [hostname_or_ip:]1344
```

Default:

```
NONE
```

Max Connections

Maximum number of connections allowed:
The maximum number of simultaneous connections allowed to run through WebGate. The value sets the limit for the number of connections or threads allowed simultaneously.

Range: minimum 0, maximum 15000

Example:

```
MaxConnections 1000
```

Default:

```
MaxConnections 1024
```

If set to `0` WebGate will not limit the number of simultaneous connections.

Connection Settings

HTTPProxy

Settings for HTTP proxy server:
These settings work only for Network Configuration 1. For the installation before a proxy server, WebGate needs the following information:

- `HTTPProxyServer`: Name or IP address of the proxy server
- `HTTPProxyPort`: The port for the proxy server (range is between 0 and 65535)
- `HTTPProxyUsername`, `HTTPProxyPassword`: Login and password for proxy server, if needed

Example:

```
HTTPProxyServer [hostname|ip]
HTTPProxyPort 3128
HTTPProxyUsername username
HTTPProxyPassword password
```

Default:

```
NONE
```

FTPProxy

Settings for FTP proxy server:
If WebGate serves as FTP proxy (see `FTPPort` option, range is between 0 and 65535), you can set a parent proxy for FTP connections.

Range: minimum 0, maximum 65535

Example:

```
FTPProxyPort 2121
```

Default:

```
FTPProxyPort 21
```

Environment settings

User
Group

Switching to users and groups:
After starting, WebGate can switch to other user and group, for running its process. WebGate should not run as root. Enter the user and group IDs, which WebGate should assume after start (and thus turning in the root permissions).

Default:

```
User nobody
Group antivir
```

WebGate must first start as root. If you want to change this parameter, you must specify the values for `User` *and* `Group` *in the file* /etc/avira/avwebgate.conf. *as well as in /etc/avira/avwebgate-scanner.conf*

ScannerListen
Address

Scanner Location:
WebGate no longer starts the SAVAPI daemon. Instead it connects to a running instance using a UNIX socket.

Default:

```
ScannerListenAddress /var/run/avwebgate/scanner
```

If you modify this parameter, you must also change the value for `ListenAddress` *in* /etc/avira/avwebgate-scanner.conf. *See* *Scanner Configuration in avwebgate-scanner.conf – Page 39*

Temporary Dir

Temporary directory:
You can change the name of the temporary directory. The standard is `/tmp`. This directory contains for example, the files during scanning.

Default:

```
TemporaryDir /tmp
 (/var/tmp for Solaris binaries)
```

CacheDir

Cache directory:
This directory contains RTPS and Webprotector cache files.

Example:

```
CacheDir /home/cache
```

Default:

```
CacheDir /var/cache/webgate
```

EmailTo

Email messages:
Avira AntiVir WebGate is able to send emails with additional information (for example about the relevant file), if it detects a virus or unwanted program. There is no default value. In order to send emails, you must enter a recipient address.

Example:

```
EmailTo root@localhost
```

Default:

```
NONE
```

Logging Settings

Syslog Facility

Syslog facility:
WebGate sends notifications to syslog daemon for all important operations. You can specify the facility for these messages.

Example:

```
SyslogFacility home
```

Default:

```
SyslogFacility user
```

The detail level of these messages depends on the settings for `LogLevel`.

LogFile

Path and name of the logfile:
All important WebGate operations are logged through a syslog daemon. You could specify an additional logfile, by entering the full path.

Example:

```
LogFile /var/log/avwebgate.log
```

Default:

```
NONE
```

LogLevel

Level for log notes:
This option defines the logging level for WebGate notifications (possible values: 0 to 7). The higher the level, the more information is logged. The values correspond to Unix standard levels used in syslog:

- 0: no messages
- 1: alerts
- 2: alerts and errors
- 3: alerts, errors and warnings
- 4: alerts, errors and warnings
- 5: alerts, errors and warnings
- 6: alerts, errors, warnings and infos
- 7: alerts, errors, warnings, infos and debug messages

Range: minimum 0, maximum 7

Example:

```
LogLevel 3
```

Default:

```
LogLevel 4
```

DebugLevel

Debug output:
This is the level of detail for debug output (LogLevel 7).

Range: minimum 0, maximum 7

Example:

```
DebugLevel 3
```

Default:

```
DebugLevel 4
```

HTTP Connection Settings

AllowHTTPS Tunnel

Allow HTTPS tunnel:
WebGate allows tunneling for SSL connections (HTTPS). As the data is encrypted, it is not scanned. WebGate does not interfere with the transaction, it just forwards the data. Due to this fact, it can not verify if the protocol being spoken is really HTTP on top of SSL. For this reason, it allows only connections to ports 443 (HTTPS) and 563 (SNEWS).

Syntax:

```
AllowHTTPSTunnel "YES|NO"
```

Default:

```
AllowHTTPSTunnel NO
```

*The data transferred through the HTTPS tunnel will **not** be scanned by WebGate.*

AllowedHTTP ConnectPorts

Tunneling SSL-encrypted connections:
If you want to allow HTTPS connections to non-standard ports, you can do so by adding the desired ports to this list. Each port will be separated by a comma or a whitespace.

Default:

```
AllowedHTTPConnectPorts 443, 563
```

AddX ForwardedFor Header

Header analysis:
In case of a proxy chain network, a downstream proxy server can make no analysis based on the Client's IP address, because it sees all requests as coming from the same address: from the proxy upstream. So the proxy knows only the address of its direct communication partners' and not the address of the computer issuing the request.

If the `AddXForwardedForHeader` option is active, WebGate adds a header field (X-Forwarded-For) to the HTTP request or adds the IP address of the Client it received the request from. In this way WebGate can forward the Client IP address to the downstream proxy servers. These are then able to analyze the header field and to use the included indirect data for example, for access control mechanisms or for logging purposes.

This option could also enable the use of ACLs for a Squid proxy, which is configured by WebGate as parent proxy. The parent proxy must certainly hold the necessary functionality for header analysis.

Syntax:

```
AddXForwardedForHeader "YES|NO"
```

Default:

```
AddXForwardedForHeader NO
```

RemoveX ForwardedFor Header

Header analysis:
This option removes the X-Forwarded-For Header from a request received by WebGate.

Syntax:

```
RemoveXForwardedForHeader "YES|NO"
```

Default:

```
RemoveXForwardedForHeader NO
```

AddViaHeader

Header analysis:
This option adds a Via Header when WebGate is used in ICAP mode.

Syntax:

```
AddViaHeader "YES|NO"
```

Default:

```
AddViaHeader NO
```

AddIcapDate Header

Header analysis
This option adds a Date header when WebGate is used in ICAP mode. By default WebGate does not send a Date header when replying to an ICAP request. To enable sending the Date header with each reply, this option should be set to "YES".

Syntax:

```
AddIcapDateHeader "YES|NO"
```

Default:

```
AddIcapDateHeader NO
```

Example:

```
AddIcapDateHeader YES
```

Timeout Prevention Settings

Contains setting that control how WebGate tries to keeps the connection to the client opened while processing the request.

Refresh/ Redirect/ Keepalive Interval

Avoiding Client-timeouts by large downloads:
Some browsers and proxies send an error message, if no data is received after a certain interval (timeout). WebGate may come to such timeout messages, because of delays during large downloads and scanning.

In order to avoid timeouts, WebGate offers the following possibilities. The entries are given in seconds.

- If the Client is a browser, WebGate sends an HTML progress page, which is updated at regular intervals.

Refresh Interval

Refresh Interval

Range: minimum 0, maximum 3600

Example:

```
RefreshInterval 1800
```

Default:

```
RefreshInterval 0
```

- If the option `RefreshInterval` is deactivated or the Client is not a browser, (temporary) HTTP redirects are sent to the Client. Thus, the Client is cyclically redirected to a dynamic-generated URL, intercepted by WebGate in order to avoid the timeout.

Redirect Interval

Redirect Interval

Range: minimum 0, maximum 3600

Example:

```
RedirectInterval 1800
```

Default:

```
RedirectInterval 0
```

- The above method does not work for all Clients. When encountering problems, use the `KeepaliveInterval` option, to make WebGate send messages to the Client at certain intervals. The value must be smaller than the one set in the Client or proxy server.

Keepalive Interval

Keepalive Interval

Range: minimum 0, maximum 3600

Example:

```
KeepaliveInterval 60
```

Default:

```
KeepaliveInterval 30
```

- WebGate sends extended header data to the Client at the specified interval. In order to maintain the connection WebGate will send no-operation commands to the server during sending or receiving larger files to or from the Client within the specified `KeepaliveInterval`.

KeepaliveMode

Keepalive Mode

Syntax:

```
KeepaliveMode "trickle|header"
```

Example:

```
KeepaliveMode trickle
```

Default:

```
KeepaliveMode header
```

- If you encounter client timeout problems, because the timeout methods described above are not appropriate in your environment or do not work properly, you may enable data trickling by setting `KeepaliveMode` in avwebgate.conf to `trickle`. If this method is used, WebGate sends small pieces of the data at the specified `KeepaliveInterval`, until the download and scan is complete. Once the file is downloaded and scanned, the remainder of the file will be immediately transferred to the client (if clean). If the default value `header` is set, WebGate will use the above mentioned Refresh, Redirect and Keepalive intervals.

.

It is NOT recommended to enable data trickling unless you are experiencing problems using the other timeout prevention methods. Be aware of the risks and limitations before you enable this feature. By enabling the trickle option the data will be sent in small segments to the client. This holds the risk of an infection, eventhough WebGate scans everything that is sent to the client. Since the trickle interval controls the sending of data at a pre-set rate and s specific size, the download speed shown to the client is not related to the actual download speed.

Scan and Filter Settings

ArchiveScan

Scanning archives:
By default, all files in archives are unpacked on access and scanned, according to the settings for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

It is recommended **not** to deactivate these options.

Syntax:

```
ArchiveScan "YES|NO"
```

Default:

```
ArchiveScan YES
```

ArchiveMax Size

Maximum size of archived files:
This option limits the scanning process to the files with unpacked size smaller than `ArchiveMaxSize` (in Bytes). The null value means no limit.

Syntax:

```
ArchiveMaxSize "integer|K|M|G"
```

Example:

```
ArchiveMaxSize 1G
```

Default:

```
ArchiveMaxSize 2G
```

ArchiveMax Recursion

Maximum recursion level:
When scanning recursive archives, the level of the recursion can be limited. The null value means all archives are completely unpacked, regardless of their recursion level.

Range: minimum 0, maximum 1000

Syntax:

```
ArchiveMaxRecursion "integer"
```

Example:

```
ArchiveMaxRecursion 10
```

Default:

```
ArchiveMaxRecursion 20
```

ArchiveMaxRatio

Maximum compression rate for archives:
This option limits the scanning to archives which do not exceed a certain compression level. It ensures protection against so-called "Mail bombs", which occupy unexpectedly large amount of memory when decompressed. The null value means all archives are completely decompressed, regardless of their compression rate.

Range: minimum 0, maximum 1000

Example:

```
ArchiveMaxRatio 100
```

Default:

```
ArchiveMaxRatio 150
```

BlockSuspiciousArchive

Blocking suspicious archives:
When activated, this option blocks archives which exceed one of the limits set for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

If this option is deactivated, all archives are forwarded, regardless of the settings for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

Syntax:

```
BlockSuspiciousArchive “YES|NO”
```

Default:

```
BlockSuspiciousArchive YES
```

BlockEncryptedArchive

Blocking password-protected archives:
If this option is activated, WebGate blocks password-protected archives.

Syntax:

```
BlockEncryptedArchive "YES|NO"
```

Default:

```
BlockEncryptedArchive NO
```

BlockPartialArchive

Block partial archives:

If enabled, multi-volume archives will be blocked.

Syntax:

```
BlockPartialArchive "YES|NO"
```

Default:

```
BlockPartialArchive NO
```

BlockArchiveBomb

Block archive bombs:

If enabled, WebGate blocks files detected as possible archive bombs.

Syntax:

```
BlockArchiveBomb "YES|NO"
```

Default:

```
BlockArchiveBomb YES
```

This option is not affected by `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

Block Unsupported Archive

Block emails with unsupported archives

Emails with archives which the scanner does not support are blocked.

Syntax:

```
BlockUnsupportedArchive "YES|NO"
```

Default:

```
BlockUnsupportedArchive YES
```

Block Extensions

Blocking certain file extensions:
WebGate can block files that have certain extensions. It will also apply for file names in archives.

Syntax:

```
BlockExtensions "ext1;ext2;ext3"
```

Example:

```
BlockExtensions exe;scr;pif
```

Default:

```
NONE
```

Block Categories

URL filtering:
First, the **access control (ACL) rules** are evaluated, which means a rule allowing tunneling for a request will not be blocked by URL filters. Connections that are not tunneled would still pass through the URL filter module, similar to the scanning behavior.

Then, the **Avira URL Filtering library** (LocalFilter) applies. The library tries to determine if an URL is dangerous based on a list of known URLs. A category is returned for each dangerous URL: Malware (60), Phishing (61), Fraud (63). If this category is found in the `BlockCategories` configuration option, the request is denied. The Avira URL Filtering library is available with every valid WebGate or WebGate Suite license.

If the Avira URL Filtering library does not find any match for the URL or the category is not blocked in the configuration file, the **Avira Web Access and Content Control library** (OnlineFilter) is used. It filters requests based on URL categories. This feature is only available with the Avira AntiVir WebGate Suite.

The categories can be specified as single categories or as category ranges. You can specify ranges with a '-' between two category numbers. (4.9 URL filtering).

Example:

```
BlockCategories 0-2 12 14 61
```

Default:

```
NONE
```

Move Concerning FilesTo

Quarantine directory:
By default, blocked files are deleted. But you can specify a quarantine directory to store them.

Syntax:

```
MoveConcerningFilesTo "path"
```

For example:

```
MoveConcerningFilesTo /home/quarantine
```

Default:

```
NONE
```

Heuristics Level

Win32-Heuristics:
Sets the detection level of Win32-Heuristics. available values are `0` (off), `1` (low), `2` (medium) and `3` (high).

Range: minimum 0, maximum 3

Syntax:

```
HeuristicsLevel "0|1|2|3"
```

Example:

```
HeuristicsLevel 1
```

Default:

```
HeuristicsLevel 2
```

Heuristics Macro

Macrovirus Heuristics:
Activates the heuristics for macroviruses in documents. This option is activated by default.

Syntax:

```
HeuristicsMacro "YES|NO"
```

Default:

```
HeuristicsMacro YES
```

Detect...

Detection of other types of unwanted programs:
Besides viruses, there are some other types of harmful or unwanted software. You can activate their detection using the following options:

```
DetectADSPY YES
DetectAPPL NO
DetectBDC YES
DetectDIAL YES
DetectGAME NO
DetectHEUR-DBLEXT YES
DetectJOKE NO
DetectPCK NO
DetectPHISH YES
```

```
DetectSPR NO
```

If you want to enable detection for all the categories above, you can uncomment the following parameter. Note that this will enable detection for all the unwanted programs, overwriting their individual values.

Syntax:

```
DetectAllTypes "YES|NO"
```

Default:

```
DetectAllTypes YES
```

SMC Settings

GUI...

SSL parameters for secure communication with Avira SMC
The following options must be activated, for a secure communication with SMC:

GuiSupport

GuiSupport
This option enables the use of the Console of the Avira Security Management Center (SMC) to manage WebGate remotely.

Syntax:

```
GuiSupport "YES|NO"
```

Default:

```
GuiSupport NO
```

GuiCAFile

GuiCAFile
Specifies the path to the certificate authority file to be used in SMC communication.

Syntax:

```
GuiCAFile "path"
```

Example:

```
GuiCAFile  /usr/lib/AntiVir/webgate/gui/cert/
cacert.pem
```

Default:

```
NONE
```

GuiCertFile

GuiCertFile
Specifies the path to the certificate file to be used in SMC communication and database logging.

Syntax:

```
GuiCertFile "path"
```

Example:

```
GuiCertFile /usr/lib/AntiVir/webgate//gui/cert/
server.pem
```

Default:

```
NONE
```

GuiCertPass

GuiCertPass
Specifies the password for the certificate file.

Syntax:

```
GuiCertPass "string"
```

Example:

```
GuiCertPass antivir_default
```

Default:

```
NONE
```

Please refer to WebGate's installation directory, for more details about advanced configuration options.

GuiHostname

GUI hostname
The GuiHostname is used by the command `avwg_stats` as an interface to listen to connections from SMC.

Syntax:

```
GuiHostname host
```

Default:

```
GuiHostname 127.0.0.1 or localhost
```

Access Control Settings

Forbidden UserAgents

Denying access to specific user agents:
You can specify one or more user agent strings that will be denied access. The main purpose is to avoid unnecessary traffic generated by clients issuing range requests (such as Microsoft's BITS "Background Intelligent Transfer Service") or streaming services (such as Apple's iTunes). Range requests and data streaming are only permitted if specified in AclConfigFile (see below).

Example:

```
ForbiddenUserAgents BITS iTunes
```

Default:

```
NONE
```

AclConfigFile

Access control scheme:
WebGate can also support more complex rules by implementing a Squid-like access control scheme. To use the access control scheme you must create a new configuration file containing the rules describing the desired behavior and have `AclConfigFile` contain the path to it.

Syntax:

```
AclConfigFile /etc/avira/avwebgate.acl
```

Default:

```
NONE
```

4.4.2 Scanner Configuration in avwebgate-scanner.conf

A new configuration file has been introduced, starting with WebGate v.3: /etc/avira/avwebgate-scanner.conf. It contains configuration options specific to the new scanner backend. Usually, you don't have to change the options in this file, but there might be a few exceptions.

User, Group

User, Group:
If you change one of these options, you have to make sure that the files avwebgate-scanner.conf and avwebgate.conf contain the same values for these options and that all directories and files are still accessible to this user. If you make any changes to this option please be aware to change the file avwg_stats.lck appropriately.

Default:

```
User nobody
Group antivir
```

Please note that User/Group are not supported by SMC. Changing these options will prevent SMC communication.

In /etc/avira/avwebgate-scanner.conf:

- Change the owner/group of the path given with `ListenAddress` (NOTE: the option consists of a path and a socket file. Don't forget to stop WebGate before making any changes. If the socket file exists, delete it and only change the owner/group of the directory.)

When changing the user and/or group here, you must also change the options `User` *and* `Group` *in WebGate's configuration file (*/etc/avira/avwebgate.conf*).*

- Adapt the option `SocketPermissions` to the new user/group. See below.

In /etc/avira/avwebgate.conf:

- Change the option `User/Group`

Socket Permissions

SocketPermission
The owner and permissions of the scanner backend's socket.

Example:

```
SocketPermissions 0600
```

ListenAddress

ListenAddress
`ListenAddress` (in avwebgate-scanner.conf) and `ScannerListenAddress` (in avwebgate.conf) specify how the scanner backend can be reached. Both options must point to the same path (the string "unix:" must not be used with the option

ScannerListenAddress):

```
ListenAddress unix:/var/run/avwebgate/scanner
ScannerListenAddress /var/run/avwebgate/scanner
```

CreateSocketDir

CreateSocketDir
If this option is enabled and the provided socket file path does not exist, SAVAPI Service will create the parent directory of the socket file at startup.

Example:

```
CreateSocketDir 1
```

Default:

```
CreateSocketDir 1
```

If the option CreateSocketDir does not exist in the scanner configuration file, the parent directory of the socket file will not be created at startup.

PoolScanners

PoolScanners
The number of AntiVir scanners set in the pool.

Example:

```
PoolScanners 70
```

Default:

```
PoolScanners 105
```

Pool Connections

PoolConnections:
The maximum number of simultaneous connections WebGate allows to the scanner pool.

Example:

```
PoolConnections 70
```

Default:

```
PoolConnections 192
```

PidDir

PidDir
Specifies the SAVAPI service PID file location. Only absolute paths are accepted. If you enter relative paths, SAVAPI will exist with an error.

Example:

```
PidDir /var/temp/webgate
```

Default:

```
PidDir /var/temp
```

LogFileName

LogFileName:
Path to the scanner's logfile.

Example:

```
LogFileName /var/log/avwebgate-scanner.log
```

Default:

```
LogFileName NONE
```

SyslogFacility

SyslogFacility:
The facility that is used, when logging to syslog.

Example:

```
SyslogFacility home
```

Default:

```
SyslogFacility user
```

ReportLevel

ReportLevel:
The scanner can be set to log on different levels:

- 0 - Log errors
- 1 - Log errors and alerts
- 2 - Log errors, alerts, warnings and info
- 3 - Log errors, alerts, warnings, info and debug messages

"alerts" means information about potential malicious code.

Example:

```
ReportLevel 1
```

Default:

```
ReportLevel 0
```

4.4.3 Updater Configuration in avupdate-webgate.conf

Updates ensure that AntiVir WebGate components (WebGate, scanner, VDF and engine), which provide security against viruses or unwanted programs, are always kept up to date.

With Avira Updater you can update Avira software on your computers, using Avira update servers. To configure the update process, use the options in /etc/avira/avupdate-webgate.conf described below. All parameters from avupdate-webgate.conf can be passed to the Updater via command line.

For example:

- parameter in avupdate-webgate.conf:

```
temp-dir=/tmp
```

- command line:

```
/usr/lib/AntiVir/webgate/avupdate-webgate.bin --temp-
dir=/tmp
```

internet-srvs

internet-svrs:
The list of Internet update servers.

```
internet-srvs=http://professional.avira-update.com,
http://professional.avira-update.net
```

master-file

master-file:

Specifies the master.idx file.

```
master-file=/idx/master.idx
```

install-dir **Installation directory:**
Specifies the installation directory for updated product files.

```
install-dir=/usr/lib/AntiVir
```

temp-dir **Temporary Direetcory:**
Temporary directory for downloading update files.

```
temp-dir=/tmp/avira_update/webgate
```

Setting update email reports

All reports on AntiVir updates are sent to the email address given in avupdate-webgate.conf:

mailer **Emails:**

Emails can be sent via `smtp` engine or using `sendmail`:

```
mailer=mutt
```

smtp... **SMTP connection:**

Authentication for smtp connection. Activate the `auth-method` option and then provide the smtp server, port, user and password.

```
auth-method=password
smtp-user=<your_username>
smtp-password=<your_password>
smtp-server=<servername>
smtp-port=25
```

notify-when **Notifications:**

There are three situations to set for email notifications:

- 0 - no email notifications are sent,
- 1 - email notifications are sent in case of "successful update", "unsuccessful update", or "up to date".
- 2 - email notification only in case of "unsuccessful update".
- 3 - email notification only in case of "successful update" (default).

Example:

```
notify-when=1
```

Default:

```
notify-when=3
```

email-to **Email recipients:**

The recipient of notification emails.

Example:

```
email-to root@localhost
```

Default:

```
email-to root@localhost
```

Connection settings for updates

proxy...

Proxy settings:

If the machine uses a HTTP proxy server, proxy configuration settings must be specified in order to make Internet updates.

```
proxy-host=
proxy-port=
proxy-username=
proxy-password=
```

Default:

```
NONE
```

user-agent

User agent:

Specifies the user agent string (`--user-agent`), which is reported to the http server.

Default:

```
@AUVI@1.0;<product_name>-UpdateCP/<updater version>
(<license types>;<products>; <language>; AVE <engine
version>; VDF <VDF version>; <operating system name>;
<operating system details>; <country>; <serial>; <li-
cense serials>; <operating system language>; )
```

By default, the `<product_name>` is `AntiVir`. If the --product-name-file option is specified or if the default productname.dat file exists, `<product name>` is replaced with the content of the respective file.

Examples:

- If the `--product-name-file` option is not specified:

  ```
  @AUVI@1.0;AntiVir-UpdateCP/2.0.3.6 (SAVXE;
  SAVAPILINUX_GLIBC24_X86_64-EN; EN; AVE 8.2.10.52; VDF
  7.11.28.140; LINUXX86_64 2.6.38-13-GENERIC; DISTRO RE-
  LEASE SQUEEZE/SID GLIBC 2.13;EN_US.UTF-8;
  A182365FA39EE0327E3A4918B0358475; 2100133080-ASRTE-
  0000001; EN_US.UTF-8; )
  ```

- If the default productname.dat file apllies:

  ```
  @AUVI@1.0;WEBGATE3.3-UpdateCP/2.0.3.6 (SAVXE;
  SAVAPILINUX_GLIBC24_X86_64-EN; EN; AVE 8.2.10.52; VDF
  7.11.28.140; LINUXX86_64 2.6.38-13-GENERIC; DISTRO RE-
  LEASE SQUEEZE/SID GLIBC 2.13;EN_US.UTF-8;
  A182365FA39EE0327E3A4918B0358475; 2100133080-ASRTE-
  0000001; EN_US.UTF-8; )
  ```

product-name-file

Product-name-file:

Specifies the file in which the product name is stored (for example `WEBGATE3.3`). The file path is relative to the update binary location. The product name is added to the `<product_name>` field in the `--user-agent` string.

The file must be readable and it must contain the product name, as ASCII printable string, without whitespaces and with a maximum length of 64 characters. Otherwise, an error message is displayed and the update process stops.

If no `product-name-file` is specified and if the default productname.dat file does not exist, no changes are made to the user-agent string.

The default value: productname.dat containing the following text: `WEBGATE3.3`

Example:

```
avupdate.bin --product-name-file=my_product_name.dat
```

Logfile settings

log

Logfile

Specify a full path with a filename to which AntiVir Updater will write its log messages.

```
log= /var/log/avupdate-webgate.log
```

log-append

Append logfile

By default, the logfile is overwritten. You can use this option to append the logfile.

```
log-append
```

Setting intranet updates

If you prefer to use an intranet update instead of the default Internet one, you have to configure some parameters in avupdate-webgate.conf or you have to provide them in the command line:

```
intranet-srvs
```

With the Avira Internet Update Manager (IUM) you can automatically download updates for a large number of your Avira products from the internet. The individual client computers in your network do not have to download updates from the internet themselves, but easily through your intranet. For more information, please refer to the Avira IUM user manual (http://www.avira.com/).

Specifies a comma separated list of Avira IUM servers

```
product-root
```

Specifies the root of the update on the IUM server (set to `/update`)

```
intranet
```

Specifies that the update will be made from the intranet rather than from the Internet.

Example:

```
intranet-svrs=http://iumserver:7080
product-root=/update
intranet
```

Setting fallback update servers

If you like to set up fallback update servers, for example in case the intranet servers do not work appropriately and you like to update from Internet servers, you can do a setup by adding the option `peak-handling-srvs` in the configuration file or in the command line. The option has the same syntax as `intranet-srvs`.

Example:

```
peak-handling-srvs=http://profpeak.avira-update.com
```

Integration into Avira Security Management Center (SMC)

In order to configure updates via Avira Security Management Center (SMC), it is necessary to add the update plug-in package to the SMC repository. Once added, a new product "Avira Updater" will be available for installation on machines administered by the SMC.

The "Avira Updater" product allows updates to be configured for all products installed on computers administered by the SMC. For more details, please refer to the SMC documentation.

If you have changed the options for User/Group the communication with Avira SMC will not work.

4.4.4 Access Control Configuration in avwebgate.acl

WebGate implements an access control scheme that is a subset of Squid's.

This feature enables you to set up rules to allow tunneling for certain types of requests and responses. This is useful for supporting streaming Internet content or user agents, that require using HTTP range requests.

The access control scheme is saved in a separate file, specified with the parameter `AclConfigFile` in /etc/avira/avwebgate.conf

Several examples are included in /etc/avira/avwebgate.acl.example.

4.5 Templates Configuration

If you have a valid license file, you may customize various notification web pages and emails generated by Avira AntiVir WebGate. WebGate will send these for example, in case of detecting viruses or unwanted programs: *alert, blocked, error* or

progress template.

These templates are usually created and saved in /usr/lib/AntiVir/webgate/templates. You may also set another directory, using the following entry in /etc/avira/avwebgate.conf:

Syntax:

```
/usr/lib/AntiVir/webgate/avwebgate.bin
  --dump-config|grep -i Template
```

Default:

```
TemplateDir templates
```

Example:

```
TemplateDir /home/templates
```

You can use different keywords for editing template files.

Following is a description of the available templates.

HTML Templates

Template	Meaning
alert.html	Displayed when an alert is found by AntiVir WebGate.
blocked.html	Displayed when AntiVir WebGate has blocked a suspicious file (using various block-settings in avwebgate.conf)
error.html	Displayed if an error occurred while processing the user's request
progress_downloading.html	Displayed while a file is being downloaded (this template is used only when the refresh method for timeout prevention is used)
progress_scanning.html	Displayed while a file is being scanned (this template is used only when the refresh method for timeout prevention is used)
progress_complete.html	Displayed after a file has been downloaded and scanned (this template is used only when the refresh method for timeout prevention is used)
progress_aborted.html	Displayed if the user has aborted the download (this template is used only when the refresh method for timeout prevention is used)
ws_blocked.html	Displayed if the page was part of a category blocked by the user

Email Templates

Template	Meaning
alert.mail	Used when an alert is found by AntiVir WebGate.
blocked.mail	Used when AntiVir WebGate has blocked a suspicious file (using various block-settings in avwebgate.conf)

In order for WebGate to be able to send email messages, an MTA must be configured. WebGate can use either `mail` *or* `sendmail`*. WebGate searches for* `/usr/sbin/sendmail`*,* `/usr/lib/sendmail` *or* `/usr/local/bin/main`*,* `/bin/mail`*,* `/usr/bin/mail`*.*

Template Keywords

Keywords are specified with enclosed "%" characters (for example, %ALERT%). Not all keywords are relevant for all templates (for example, ALERT has no relevancefor progress templates).

A = available for alert templates
B = available for blocked templates
E = available for error templates
P = available for progress templates
W = available for Avira Web Access and Content Control templates

Keyword	Description	Availability
ALERT	Complete alert message	A
ALERT_DESC	Description of alert	A
ALERT_TYPE	Type of alert	A
BLOCKED_REASON	Reason for blocking file	B
CLIENT_IP	IP address of client	A,B
DATA_DIRECTION	"Request" or "response"	A,B
DATA_PERCENT_RECEIVED	Percent of file being downloaded	P
DATA_RECEIVED	Number of bytes of file being downloaded	P

Keyword	Description	Availability
DATA_SIZE	Number of total expected bytes of file being downloaded	P
DETERMINED_CLIENT_ADDRESS	Address of originating client	A,B
DETERMINED_SERVER_ADDRESS	Address of destination server	A,B
ENGINE_VERSION	Version of AntiVir engine	A,B,E
ERROR_CODE	HTTP response code used for the response	E
ERROR_DESC	A short description in text form of the error	E
ERROR_REASON	Description of the HTTP status code	E
PRODUCT_NAME	"AntiVir WebGate"	A,B,E,P,W
PRODUCT_VERSION	Version of WebGate	A,B,E,P,W
PROGRESS_STATUS	"Downloading", "scanning", etc.	P
PROGRESS_URL	URL to abort download (when downloading), URL to get file (when complete)	P
PROXY_HOST	Hostname of machine where WebGate is running	P
QUARANTINE_FILE	Filename of quarantined file	A,B
REFRESH_URL	URL to refresh the progress page	P
REQUESTED_FILE	Filename of file being downloaded	A,B,E,P
REQUESTED_URL	Full URL of file being downloaded	A,B,E,P,W

Keyword	Description	Availability
REQUEST_METHOD	"GET", "POST", etc.	A,B,E
RESPONSE_STATUS	HTTP response code from server	A,B,E
MATCHED_CATEGORIES	All the blocked categories that the requested URL matched	W
MATCHED_CATEGORIES_LI	Al the blocked categories that the requested URL matched represented as a html list. The template designer must surround it with the list directives	W
SERVER_IP	IP address of server	A,B
VDF_VERSION	Version of AntiVir VDF file	A,B,E

4.6 Client Timeout Prevention

WebGate always needs the complete file for scanning. Therefore, the entire file is downloaded before it is scanned and forwarded to the requesting client. Especially when downloading and scanning a large file or if the connection to the Internet is slow, this can cause a significant delay during which the client does not receive feedback. Thus the client application cannot provide a download progress to the user and may even encounter timeout issues.

In order to avoid these problems, WebGate provides different methods for preventing client timeouts: `refresh`, `redirect` and `keepalive`.

The timeout prevention method is chosen dynamically based on the type of client and/or the WebGate configuration settings. WebGate first checks if the refresh method would be appropriate. If not, WebGate checks if the redirect method would be appropriate. If not, WebGate checks if the keepalive method would be appropriate. If none of the timeout methods is appropriate, then WebGate will not attempt any form of timeout prevention.

4.6.1 Refresh method

The refresh method is used for clients identified as browser. WebGate sends HTML pages containing the current progress status that will be refreshed at a specified interval (`RefreshInterval`). After downloading and scanning the file, the user

can get the file from WebGate by clicking on the link provided with the last progress message. If the file is blocked, an HTML page with an alert message is generated from the appropriate template and is sent to the client.

4.6.2 Redirect

If the refresh method is not used (because it is disabled or the client is a non-browser) HTTP redirect messages can be sent to the client at the specified interval (RedirectInterval). The client is redirected to a dynamically generated URL, that can be identified by WebGate and uniquely associated with the appropriate download. Note that this method does not work with every client. If you set the value for this interval too low, you will receive a redirect loop error from most browsers.

4.6.3 Keepalive method

If the refresh and redirect methods are not used (because they are disabled or they are not appropriate), the keepalive method is used.

Here, WebGate sends extended header data (X-WebGate-Status) at the specified interval to the client (KeepaliveInterval). The extended header data is ignored by the client but may be sufficient to reset the timeout. This timeout method may not work, if a proxy is installed between WebGate and the clients.

Data trickling

If you encounter client timeout problems, because the timeout methods described above are not appropriate in your environment or don't work properly, you may enable data trickling by setting "KeepaliveMode" in avwebgate.conf to "trickle". If this method is used, WebGate sends small pieces of the data at the specified "KeepaliveInterval" until the download and scan is complete. Once the file is downloaded and scanned, the remainder of the file will be transferred to the client very fast (if clean).

Although data trickling should work in any environment with every client, it is not an optimal solution. There are some important points that you should keep in mind if you intend to enable data trickling:

- Because small parts of the data are sent to the client before the file is downloaded and scanned completely, there is an unlikely (but not to be ignored) risk that the data trickled to the client contains a virus (or part of a virus). Indeed, WebGate scans the already received part of the file before starting trickling, but the scan result may be misleading because the files were still incomplete at the time of scanning.
- The download speed shown by the client is the speed at which trickle data are received by the client and does not reflect the actual traffic flow at which WebGate is receiving the file.
- Also the estimated time calculated by the client will be vastly overestimated.
- If the first part of the file has been trickled and a virus is found, there is no chance to send the client a notification (e.g. alert HTML page). WebGate

merely terminates the connection to the client. This may result in leaving small incomplete (mostly unusable) files on the client machine that should be deleted by the user.

It is not recommended to enable data trickling unless you are experiencing problems using the other timeout prevention methods. Be aware of the risks and limitations before you enable this feature.

4.7 Advanced Options

The following options can be used to fine-tune WebGate. Normally, you do not need to change any of these settings, but they may sometimes be useful for special configurations and environments:

4.7.1 Proxy Settings

DNSHelpers

DNSHelpers

Range: minimum 0, maximum 64

Example:

```
DNSHelpers 10
```

Default:

```
DNSHelpers 8
```

The number of DNS helper processes created at startup. Allows concurrent DNS lookups, thus enhancing the performance. The maximum allowed valued is 64.

ClientTimeout

ClientTimeout

Range: minimum 0, maximum 600

Example:

```
ClientTimeout 120
```

Default:

```
 ClientTimeout 60
```

Number of seconds to wait for a request from the client until a timeout occurs and the session is aborted.

ServerTimeout

ServerTimeout

Range: minimum 0, maximum 600

Example:

```
ServerTimeout 240
```

Default:

```
ServerTimeout 120
```

Number of seconds to wait for a request from the server until a timeout occurs and the session is aborted.

OpenMax

OpenMax

Range: minimum 0, maximum 2147483647

Example:

```
OpenMax 1000
```

Default:

```
OpenMax 0
```

Specify the maximum number of opened files for the WebGate process. With the default value `0`, WebGate will not change any existing system values.

WorkerPoolSize

WorkerPoolSize

Range: minimum 0, maximum 20000

Example:

```
WorkerPoolSize 100
```

Default:

```
WorkerPoolSize 0
```

The number of threads in the thread pool. By default the thread pool is disabled, and a new thread is created with each request. By setting the value greater than 0 you enable the thread pool.

ScannerPool Size

ScannerPoolSize

Range: minimum 0, maximum 250

Example:

```
ScannerPoolSize 70
```

Default:

```
ScannerPoolSize 100
```

The number of persistent connections to the scanner. If set to 0, then the persistent connections pool is disabled, and a new connection to the scanner is created with each request. The persistent connections pool maintains a number of open connections to the scanner to speed up the scanning process by eliminating the need to create and close a connection for each request.

This is strongly related to the PoolScanners option in avwebgate-scanner.conf which determines how many connections the scanners accepts.

WebGate will attempt to create the configured number of connections.

If PoolScanners is smaller, or not all the scanner connections are available (another process is using some of them), then as many connections as possible are created.

4.7.2 Database Support

WebGate support logging statistics to a database. For details on how to set up the database and other requirements, see Database Setup Requirements.

The database consists of two tables, called `alerts` and `counter`.
`Alerts` contains information about WebGate's alerts. Depending on the settings of the `LogCleanRequests` parameter, the `alerts` table may also contain information about all requests.

`Counter` contains WebGate specific statistics for a quick look-up.

Alerts logged

- status (scan flags, ACL blocked, the filter that blocked the request or clean and tunneled if this is the case)
- url
- alert_url
- alert name
- action (blocked, allowed, tunneled, quarantined, deleted)
- source
- category (received from WebProtector, WebCat and RTSP)
- engine
- date
- vdf

Counters logged

- number of files blocked because of extension
- number of files blocked because of suspicious behavior: processing errors, partial, unsupported, encrypted archives, limits reached (max size, max recursions etc)
- number of infected files
- number of clean files
- number of scanned files
- total of bytes received

Options

DBSupport **DBSupport**

If you enable this option, WebGate enters statistics in a database. The database consists of two tables: `alerts` and `counter`. To set up DBSupport make sure that GUISupport is activated too and the "GUI..." on page 37 certificate options are configured appropriately.

Syntax:

```
DBSupport "YES|NO"
```

Default:

```
DBSupport NO
```

DBodbcIni

DBodbcIni

If you have enabled the `DBSupport` option, the ODBC driver manager uses the specified odbc.ini file. Default setting: the installed ODBC driver manager decides which odbc.ini file to load.

Syntax:

```
DBodbcIni "string"
```

Example:

```
DBodbcIni /path/to/odbc.ini
DBodbcIni /etc/avira/avwebgate-odbc.ini
```

DBodbcLib

DBodbcLib

If you have enabled the `DBSupport` option WebGate loads the library specified here and uses it as the ODBC driver manager. Default setting: one of the following files is loaded in sequence from the default library path: libodbc.so.1, libodbc.so, libiodbc.so.

Syntax:

```
DBodbcLib "string"
```

Example:

```
DBodbcLib /path/to/odbc-library
```

DBodbcData Source

DBodbcDataSource

If you have enabled the `DBSupport` option, the specified database is connected as the source.

Syntax:

```
DBodbcDataSource "string"
```

Default:

```
DBodbcDataSource WebGate
```

DBUpdate Delay

DBUpdateDelay

If you have enabled the `DBSupport` option, the statistics are recorded in the database at regular intervals. You can enter the interval in seconds (s), minutes (m) or hours (h). If you set the value to `0`, the default interval of 1 hour is used. Default: to the whole hour.

Syntax:

```
DBUpdateDelay "timespan"
```

Default:

```
DBUpdateDelay 1h
```

DBLogClean Requests

DBLogCleanRequests

If you have enabled the DBSupport option, requests considered as clean by WebGate are not added to the database by default. This option allows you to

change the default setting.

Syntax:

```
DBLogCleanRequest "YES|NO"
```

Example:

```
DBLogCleanRequests YES
```

Default:

```
DBLogCleanRequests NO
```

Database Setup Requirements

This is a list of version numbers of MySQL servers, MySQL ODBC drivers and ODBC driver managers which should be compatible:

MySQL 5.0.70
MySQL ODBC driver 3.51.11
iODBC 3.52.4

Setup

Before you enable database support, you have to install an ODBC driver manager and set it up. There are two driver managers available:

iODBC - www.iodbc.org (recommended)
unixODBC - www.unixodbc.org

Below is a description on how to install and set up ODBC on Debian 5.0 (please consult the distribution or driver manager manual on how to install and set up ODBC if you use another operating systems).

***Warning**: WebGate is a 32-bit binary and can't use a 64-bit shared object. This means it will not be able to use a 64-bit ODBC driver manager.*

For 64-bit machines you should make sure that the ODBC connector is a 32-bit shared object. For details about how to set up database support in WebGate on a 64-bit machine, see the file README.db-support-SLES10-SP2-64bit.

This file contains an example setup for ODBC on SuSE Linux Enterprise 10 SP2.

1. Set up the database

If you haven't already set up a user with access rights to the database, you should set one up now.
Please consult your database's manual for information on how to add a user to your database and grant the user access.

See the file /usr/lib/AntiVir/webgate/create-db.sql for details on the database layout. The database layout is the script to create a MySQL database.

You can use this script to create the database (example for MySQL, with the server

running on the specified host):

```
# mysql -u <db user> -p -h <your sql server host name>
< create-db.sql
```

Enter password.

2. Install iODBC

You should choose a thread safe library. Please consult the distribution manual to check if your ODBC library was built with thread support.

```
# apt-get install libiodbc2
```

3. Install the corresponding database driver for your database

You should choose a thread safe driver. Please consult the distribution manual to check if your ODBC driver is thread safe.

Example for MySQL ODBC driver:

```
# apt-get install libmyodbc
```

4. Set up odbc.ini (see 5. for an example odbc.ini)

There are different ways to perform the setup:

- Create and/or edit /etc/odbc.ini
  or
- Copy /etc/avira/avwebgate-odbc.ini to /etc/odbc.ini and edit it
  or
- Edit /etc/avira/avwebgate-odbc.ini and set the configuration option "DBodbcIni" in /etc/avira/avwebgate.conf to "/etc/avira/avwebgate-odbc.ini"

If you want to configure the odbc.ini path from the Avira Security Management Center (SMC) please notice that it is not possible to define the file via the SMC GUI. You may copy the path manually to the client, for example with the help of SCP or WinSCP or you may use the file copy function of the SMC. Please make sure that the file has the appropriate write permission. You can set the permission manually via SSH or you may use the chmod-workaround: /bin/chmod a+w/usr/lib/AntiVir/agent/webgate-odbc.ini.

When you configure the DB support by editing the avwebgate-odbc.ini file, please be aware of the accuracy of your entries. There should be no blanks in front of the option names, otherwise you receive an error message.

If you don't specify "DBodbcIni" in /etc/avira/avwebgate.conf, the library decides where to search for the odbc.ini.

The library might also use a different odbc.ini file if the specified file exists but is not readable/writable by the user WebGate is running as.

5. Sample odbc.ini

This is an example of a minimal odbc.ini file.

Please consult the documentation of your database driver for details on the available options.

[WebGate]
Driver = /usr/lib/odbc/libmyodbc.so
Server = hostname.of.my.sql.server
User = username
Password = password
Database = webgate

[WebGate]: The DSN used by WebGate
Driver: This is the path to the driver's library
Server: Database server
User: Username for accessing the database
Password: Username's password
Database: Name of the database to use

6. Enable database support in avwebgate.conf

Set "DBSupport" to `YES` in /etc/avira/avwebgate.conf.

7. Test your ODBC setup

You can use the tool avwg_stats to check database connectivity. The utility avwg_stats is started by WebGate when DBSupport and GuiSupport is enabled. First of all avwg_stats parses the configuration file (/etc/avira/avwebgate.conf) for validation. It is used by WebGate to log to the database and it is used by the SMC to get information from WebGate. The client uses avwg_stats to interrogate the database.

```
/usr/lib/AntiVir/webgate/gui/bin/avwg_stats -S
```

If successful, the tool will print the following:

```
$ /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -S
Using these settings:
ODBC ini:     <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source:  WebGate

Preparing connection ...
=> OK
Connecting ...
=> OK
Disconnecting ...
=> OK

Successfully verified database connectivity!
```

... and something similar if errors occur (example for MySQL, the error message may vary depending on the error type):

```
Using these settings:
ODBC ini:     <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source:  WebGate

Preparing connection ...
=> OK
Connecting ...
Failed to connect to ODBC data source (error code: -2)
([MySQL][ODBC 3.51 Driver]Lost connection to MySQL server at 'reading
initial communication packet', system error: 111)
```

Print CSV list

WebGate is able to print the tables' contents as a CSV (comma separated value) list. By default only the `alerts` table is printed. You can choose another table using the command line option `-t`.

The first line of the resulting list contains the column names. All other lines are the

table's rows. The results are not sorted.

Example:

Print the "alerts" table:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv
```

Print the "counter" table:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv
-t counter
```

CSV separator:

Specify a field separator using one character:

```
-o csv:"s"
```

You must quote the separator for it not to be interpreted by the shell.

Example:

Print the "alerts" table and separate by ";":

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o
csv:";"
```

Time ranges:

You can limit the result to only list rows within a specific time range:

```
-R "YYYY-MM-DD HH:MM:SS/YYYY-MM-DD HH:MM:SS"
```

Example:

Print the "alerts" table limited to a specific time range:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv -
R "2011-04-13 00:00:00/2011-04-13 15:35:43"
```

This will list all alerts which were logged between 2011-04-13 00:00:00 and 2011-04-13 15:35:43

`Alerts` table description

When a mail is blocked, information about the alert(s) is immediately written to the database.

Column	Description
id	This column is an auto-incremented number.
reason	The reason why the request was blocked. The following reasons exist: *Alert* - scanner found malware *Suspicious* - scanner detected a suspicious file *Error* - an error occurred during the scan *Incomplete* - not completely scanned *Encrypted* - scanner found an encrypted file *Extension* - file extension was blocked *Archive bomb* -scanner found an archive bomb *ACL* - request blocked by ACL rules *Online filter* - request blocked by Online filter *Local filter* - request blocked by local filter *RTPS filter* - request blocked by RTPS filter *Clean* - request was allowed *Tunneled* - request was tunneled (not scanned) *Unsupported* - scanner found an unsupported archive ***Note**: other reasons may appear in this column in the future after product updates.*
alertname	Depends on reason: *Alert* - the name of the alert *All other reasons* - A detailed description of the reason
alerttype	additional information on the alert: *Alert* - adware, backdoor, trash, dialer, heuristic, joke, program, riskware, trojan, virus, worm *(**Note**: other categories may appear in this column. The categories depend on the scanner and may change, or new ones may become available after a scanner update).* *All other reasons* - short description of the alertname

Column	Description
filename	The requested URL received by WebGate.
action	The action taken: deleted, quarantined, allowed, blocked, tunneled.
source	The IP of the client that made the request
category	The categories returned by `WebProtector`, `RTPS` and `UrlCheck`, if the option `BlockCategories` is enabled.
alerturl	An URL with more information about the alert (in case an alert was found). E.g.: for the Eicar test file the URL http://www.avira.com/en/threats?q=Eicar%2DTest%2DSignature is added.
missed	Due to internal buffer limits, it may be that not every alert can be written to the database. If this happens, the column "missed" contains the count of alert information which could not be written to the database.
product	Contains the product's name "WebGate".
vdf	Version information of the VDF which was used for scanning.
engine	Version information of the engine which was used for scanning.
hostname	The value of "MyHostName" (/etc/avira/avwebgate.conf). If "MyHostName" is not set, the value returned from `gethostname`(). If `gethostname`() fails, "localhost".
ou	The active organization unit, as reported by PolicyManager.

`Counter` table description

The rows in the counter table are written periodically. The default setting is every completed hour.

You can change the delay between entries using the configuration option `DBUpdateDelay` in /etc/avira/avwebgate.conf.

Example:

```
DBUpdateDelay 30m
```

Write information to the database every 30 minutes
Possible units are: no unit/s=seconds, m=minutes, h=hours

Column	Description
id	This column is an auto-incremented number.
accepted	Total count of scanned files.
clean	Count of clean files.
alerts	Count of malware found.
acl	Count of blocked files by ACLs.
total_size	Total size of traffic.
errors	Count of requests which caused an error while processing.
incomplete	Count of requests which could not be scanned completely.
unsupported	Count of requests which contained an unsupported compression method.
encrypted	Count of requests with encrypted attachments.
extension	Count of files whose names contained a forbidden extension.
limits	Count of files which reached an archive limit while processing.
url_filter	Count of blocked files by URL filters (RTPS, WebCat, WebProtector).
product	The product's name "WebGate".
hostname	The value of "MyHostName" (/etc/avira/avwebgate.conf). If "MyHostName" is not set, the value returned from `gethostname`(). If `gethostname`() fails, "localhost".

Tunneled connections are not listed in the `counter` *table.*

4.7.3 HTTP Connection Settings

AllowHTTP Connect

AllowHTTPConnect

Syntax:

```
AllowHTTPConnect "YES|NO"
```

Default:

```
AllowHTTPConnect NO
```

Allows WebGate to establish a tunnel connection to any port allowed for HTTP if a CONNECT method request is received.

Use this option with caution. WebGate does not check the data transferred over the tunnel connection! Use `AllowHTTPSTunnel` instead if you want to limit the allowed connections to the ports 443 (HTTPS) and 563 (SNEWS).

ProgressAuto Send

ProgressAutoSend

Syntax:

```
ProgressAutoSend "YES|NO"
```

Default:

```
ProgressAutoSend NO
```

After showing the download progress (as refreshing HTML pages), send the downloaded file automatically to the client once the download has finished (may not work with every client).

Progress Filesize Threshold

ProgressFilesizeThreshold

Example:

```
ProgressFilesizeThreshold 1K
```

Default:

```
ProgressFilesizeThreshold 20MB
```

If files larger than the specified value are downloaded, progress messages are sent to the client independent of its content type or file extension. A value of 0 means that the file size doesn't affect the decision regarding which timeout prevention method is used.

ProgressHold Time

ProgressHoldTime

Range: minimum 0, maximum 36000

Example:

```
ProgressHoldTime 2400
```

Default:

```
ProgressHoldTime 1800
```

Number of seconds to wait for a refresh or redirect request from the client, once the download has finished after showing download progress. If no request is received within the specified time, the file is discarded.

ProgressHold TimeAfter GetFile

ProgressHoldTimeAfterGetFile

Range: minimum 0, maximum 7200

Example:

```
ProgressHoldTimeAfterGetFile 1200
```

Default:

```
ProgressHoldTimeAfterGetFile 0
```

Number of seconds to wait for subsequent requests from the client, after the downloaded file was requested from WebGate at least once, using the "Get file..."

link provided with the final progress page. This allows a client to retrieve the temporarily cached file multiple times. If no request is received within the specified time, the file is deleted. By default, a file is immediately deleted after it is sent once to the client.
For Squid (version < 2.5.STABLE9) this should be set to something greater than 0, since Squid retries a request three times if a 403 response is submitted, but after the first request WebGate deletes the requested page.

ProgressHost

ProgressHost

Example:

```
ProgressHost home.security:port
```

Default:

```
ProgressHost Avira.WebGate:80
```

The hostname used for the progress URL. You may specify a real name or address if you encounter problems with DNS lookups performed by the browser or proxy for example. The port must be specified.

RefreshDelay

RefreshDelay

Range: minimum 0, maximum 600

Example:

```
RefreshDelay 60
```

Default:

```
RefreshDelay 3
```

Specifies the delay time in seconds before the first progress message is sent to the client. This is used for slow loading pages, to stop WebGate from displaying the refresh screen. If the value is set lower than RefreshInterval, the value for RefreshInterval is used.

RefreshSkipFile Extensions

RefreshSkipFileExtensions

Example:

```
RefreshSkipFileExtensions xml, htm
```

Default:

```
RefreshSkipFileExtensions htm, html, shtml, css, gif,
jpg, jpeg, png, swf, flv
```

Disable sending of refresh messages when downloading large files with one of the specified extensions.

Refresh Timeout

RefreshTimeout

Range: minimum 0, maximum 3600

Example:

```
RefreshTimeout 60
```

Default:

```
RefreshTimeout 30
```

If there is no refresh or redirect request received within the specified timeout interval in seconds (plus refresh/ redirect time), the download is aborted automatically.

CheckHTTPS Handshake

CheckHTTPSHandshake

Syntax:

```
CheckHTTPSHandshake "YES|NO"
```

Default:

```
CheckHTTPSHandshake YES
```

By default WebGate tries to determine if a CONNECT request is followed by an actual HTTPS handshake. If this is not desired, `CheckHTTPSHandshake` should be set to `NO`.

UseActiveFTP

UseActiveFTP

Syntax:

```
UseActiveFTP "YES|NO"
```

Default:

```
UseActiveFTP NO
```

When "FTP over HTTP" is used, the FTP connection from WebGate to the FTP server is made using passive mode. However, if for some reason passive connections are not desired, the user can set UseActiveFTP to 1 and enable the use of active mode. This option has effect only if "HTTP over FTP" is used (ie: using a browser to view the files on an FTP server). If WebGate is used as FTP proxy, active/passive mode is set by the FTP client used.

AllowActive FTPPorts

AllowActiveFTPPorts

Example:

```
AllowActiveFTPPorts 33323
```

Default:

```
AllowActiveFTPPorts 0
```

Normally, if active FTP connections are made in FTP over HTTP mode, the port the server is asked to connect to is chosen at random. WebGate also allows the user to specify a list of ports it tries to bind to, instead of a random one. One or more single ports (e.g 15673 60754) or port ranges can be specified.
Ranges are specified with a '-' between two port numbers (e.g. 1025-65535). Note that there are no whitespaces allowed between the two port numbers and the dash when specifying a range.

If the list contains port numbers under 1024, WebGate must be run as root by setting User and Group in avwebgate.conf to root. This presents a security risk and should be

avoided.

4.7.4 FTP Connection Settings

FTPDefault Server

FTPDefaultServer

Example:

```
FTPDefaultServer ftp.example.com:21
```

Default:

```
NONE
```

Specifies an FTP server to which WebGate will connect by default when running as FTP proxy. May be useful to protect a single FTP server "transparently".

FTPProxy Username

FTPProxyUsername

Example:

```
FTPProxyUsername user@example
```

Default:

```
NONE
```

FTPProxy Password

FTPProxyPassword

Example:

```
FTPProxyPassword password
```

Default:

```
NONE
```

FTPProxyUsername and FTPProxyPassword are set when WebGate uses a FTP parent proxy.

4.7.5 ICAP Connection Settings

ICAPError ResponseOn Blocked

ICAPErrorResponseOnBlocked

Syntax:

```
ICAPErrorResponseOnBlocked "YES|NO"
```

Default:

```
ICAPErrorResponseOnBlocked NO
```

Changes the ICAP response sent to the ICAP client, if a file is blocked. By default, WebGate sends an ICAP 200 response with an encapsulated HTTP 403 response including an HTML page generated from the appropriate HTML template. If this option is enabled, WebGate sends an ICAP 403 response (without a message-body) to the ICAP client instead.

4.7.6 Timeout Prevention Settings

The timeout prevention method is chosen dynamically, based on the type of client and the WebGate configuration settings. All settings specify how often repetitively a method is used. Valid time multipliers are:

- `s` for seconds (by default a value with no multiplier is considered in seconds)

- `m` for minutes

- `h` for hours

KeepaliveDelay

KeepaliveDelay

Range: minimum 0, maximum 600

Example:

```
KeepaliveDelay 60
```

Default:

```
KeepaliveDelay 0
```

This option applies only if the KeepaliveMode is set to `trickle`. In order to minimize the security risks incorporated by this feature, the `KeepaliveInterval` should not be set to a small value (<30). But sometimes it may be desirable to receive the first bytes shortly after starting the download (e.g. to trigger the "Save As ..." dialog box). This option specifies the delay time in seconds before trickling data starts.

KeepaliveMode

KeepaliveMode

Syntax:

```
KeepaliveMode "trickle|header"
```

Default:

```
KeepaliveMode header
```

In order to prevent client timeouts while downloading and scanning large files, WebGate by default sends extended header data (X-WebGate-Status) to the client at the specified `KeepaliveInterval`. By setting this option to `trickle` you can enable data trickling. If enabled, WebGate sends small parts of the file to the client until the whole file is downloaded and scanned.

Use this option with caution. By using this feature it is theoretically possible for a virus to get through! Be aware of the risks and limitations if you intend to enable data trickling (see 4.6 Client Timeout Prevention).

TrickleDataSize

TrickleDataSize

Example:

```
TrickleDataSize 2
```

Default:

```
TrickleDataSize 1
```

Size for the packets WebGate sends to the client when using trickling. By default the size is specified in bytes. An optional quantifier can be used to change this. K, M and G can be used for Kilobytes, Megabytes and Gigabytes.

For example 1K will be equivalent to 1024 with no quantifier given.

Reserve DataSize

ReserveDataSize

Example:

```
ReserveDataSize 1
```

Default:

```
ReserveDataSize 1024
```

Size of the total data WebGate has to receive before trickling it to the client. By default the size is specified in bytes. An optional quantifier can be used to change this. K, M and G can be used for Kilobytes, Megabytes and Gigabytes. For example 1K will be equivalent to 1024 with no quantifier given.

Please keep in mind that `TrickleDataSize` must be lower than `ReserveDataSize`.

4.7.7 Scan and Filter Settings

BlockOnError

BlockOnError

Syntax:

```
BlockOnError "YES|NO"
```

Default:

```
BlockOnError YES
```

Block files that cause processing errors when scanning them.

Block Unsupported Archive

BlockUnsupportedArchive

Syntax:

```
BlockUnsupportedArchive "YES|NO"
```

Default:

```
BlockUnsupportedArchive YES
```

Block archives that can not be handled by the scanner.

WSInitServer

WSInitServer

Example:

```
WSInitServer debian.home.com:80
```

Default:

```
WSInitServer cobion.avira.com:80
```

This is the server used for the initialization of the Avira Web Access and Content

Control library. For this option to take effect a valid WebGate Suite license must be installed. Normally there is no need to change this.

LocalFilter **LocalFilter**

Syntax:

```
LocalFilter "YES|NO"
```

Default:

```
LocalFilter YES
```

Controls the usage of local URL filter implemented by Avira URL Filtering library. This filter is enabled by default with every WebGate or WebGate Suite license. By setting this to `NO` the filter will be disabled.

OnlineFilter **OnlineFilter**

Syntax:

```
OnlineFilter "YES|NO"
```

Default:

```
OnlineFilter YES
```

Controls the usage of Avira Web Access and Content Control Library. This is enabled by default with every WebGate Suite license. By setting this to `NO` the Avira Web Access and Content Control Library will be disabled.

4.7.8 SNMP Settings

SNMP Recipient **SNMPRecipient**

Example:

```
SNMPRecipient snmp.example.com
```

Default:

```
NONE
```

The host that listens for SNMP traps sent by WebGate. If this value is disabled, no SNMP traps are sent.

SNMPSender **SNMPSender**

Example:

```
SNMPSender 192.0.0.1
```

Default:

```
SNMPSender 127.0.0.1
```

Set up sender for SNMP traps. This option can be used to define which IP address is specified as the sender address in SNMP traps. If a hostname is specified, this will be used to determine the IP address being used by means of DNS-lookup.

SNMP Community

SNMPCommunity

Example:

```
SNMPCommunity CompanyName
```

Default:

```
SNMPCommunity Avira
```

The community string used when sending SNMP traps. A SNMP host can receive traps from WebGate only if it has the same community string or has no community string set.

4.8 Client Configuration

Once WebGate is running, web browsers will need to set WebGate as HTTP/FTP proxy (Network Configuration 0 and Network Configuration 1).

If you already have an HTTP/FTP proxy in your network and WebGate is installed behind the proxy (Network Configuration 2), then you will need to change your proxy's settings instead of the web browser's (see 4.12 Proxy Configuration).

4.9 URL filtering

WebGate allows clients to filter outgoing requests. The filtering is done in two stages.

The Avira URL Filtering library is used. The library tries to determine if an URL is dangerous based on a list of known URLs. A category is returned for each dangerous URL: Malware, Phishing and Fraud. If this category is found in the BlockCategories option in the configuration file the request is denied. The Avira URL Filtering library is available with every valid WebGate or WebGate Suite license.

If the Avira URL Filtering library finds no match for the URL or the category is not blocked in the configuration file, the Avira Web Access and Content Control library is used. This filters requests based on the categories the URL falls into.

This feature is only available with the Avira AntiVir WebGate Suite. The library requires a key file used for encrypting traffic. Each kit contains a key file which can be found in /usr/lib/AntiVir/webgate/wskeyfile.

URL filtering is done after the access control rules are evaluated, so an URL tunneled using these rules will not be blocked regardless of the category it falls into.

Both the Avira URL Filtering library and the Avira Web Access and Content Control library will only block a page based on the URL. If a request is made to an IP address (eg: http://209.85.135.103/) it will not be blocked by the library.

The categories WebGate will block are specified as a list of numbers using the BlockCategories in the configuration file.

The list containing all the available categories and their corresponding numeric value is:

Numeric Value	Category
0	Pornography
1	Erotic / Sex
2	Swimwear / Lingerie
3	Shopping
4	Auctions / Classified Ads
5	Governmental Organizations
6	Non-Governmental Organizations
7	Cities / Regions / Countries
8	Education
9	Political Parties
10	Religion
11	Sects
12	Illegal Activities
13	Computer Crime
14	Political Extreme / Hate / Discrimination
15	Warez / Hacking / Illegal Software
16	Violence / Extreme
17	Gambling / Lottery
18	Computer Games
19	Toys
20	Cinema / Television
21	Recreational Facilities / Amusement / Theme Parks
22	Art / Museums / Memorials / Monuments
23	Music
24	Literature / Books
25	Humor / Comics
26	General News / Newspapers / Magazines
27	Web Mail
28	Chat
29	Newsgroups / Bulletin Boards / Blogs
30	Mobile Telephony
31	Digital Postcards

Numeric Value	Category
32	Search Engines / Web Catalogs / Portals
33	Software / Hardware / Distributors
34	Communication Services
35	IT Security / IT Information
36	Website Translation
37	Anonymous Proxies
38	Illegal Drugs
39	Alcohol
40	Tobacco
41	Self-Help / Addiction
42	Dating / Relationships
43	Restaurants / Bar
44	Travel
45	Fashion / Cosmetics / Jewelry
46	Sports
47	Building / Residence / Architecture / Furniture
48	Nature / Environment / Animals
49	Personal Homepages
50	Job Search
51	Investment Brokers / Stocks
52	Financial Services / Investment / Insurance
53	Banking / Home Banking
54	Vehicles / Transportation
55	Weapons / Military
56	Health
57	Abortion
59	Spam URLs
60	Malware
61	Phishing URLs
62	Instant Messaging
63	Fraud
66	General Business
73	Banner Advertisements
76	Social Networking
77	Business Networking
78	Social Media
79	Web Storage

4.10 SNMP Traps

WebGate may be configured so that the administrator is informed about internal errors and malware alerts via SNMP traps. A specification of these traps is available in the MIB files.

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID).

WebGate provides two MIB files to describe the various SNMP traps WebGate can send:

```
AVIRA-MIB.txt
AVIRA-WEBGATE-V0-MIB.txt
```

By default, the MIB files are copied in the /usr/lib/AntiVir/webgate/data folder. You can either copy these files in your default SNMP Agent mibs folder or you can configure the SNMP Agent to search for MIB files in the above location.
Please check your SNMP Agent documentation for instructions on how to do this.

wgtUp

wgtUp

WebGate is started.

wgtDown

wgtDown

WebGate is stopped.

wgtAlert

wgtAlert

The scanner found malware.

wgtSuspicious

wgtSuspicious

The scanner couldn't finish the scan which causes WebGate to treat the request as suspicious. Parameters: the reason for the suspicion and the URL of the request.

wgtMalware Scanner Unreach

wgtMalwareScannerUnreach

WebGate could not connect to the malware scanner.

wgtMatched CategoryBy OnlineFilter

wgtMatchedCategoryByOnlineFilter

WebGate has matched the request against a configured category with the online filter.Parameters: the category name and the URL of the mathched category.

This feature is available only with a WebGate Suite license.

wgtMatchedCategoryByRTPSFilter

wgtMatchedCategoryByRTPSFilter

WebGate has matched the request against a configured category with the RTPS filter. Parameters: the category name and the URL of the matched category.

This feature is available only with a WebGate RTPS license.

wgtMatchedCategoryByLocalFilter

wgtMatchedCategoryByLocalFilter

WebGate has matched the request against a configured category with the offline filter Parameters: the category name and the URL of the mathched category.

wgtLicenseExpiredOrInvalid

wgtLicenseExpiredOrInvalid

The WebGate's license has expired or is invalid.

wgtLicenseWillExpireSoon

wgtLicenseWillExpireSoon

The license will expire in less than 30 days. Parameters: the number of days the license will still be valid.

4.11 WebGate Access Control

WebGate implements a Squid-like access control scheme. The access control scheme is within a separate file, specified in the configuration file /etc/avira/avwebgate.conf. Each line in this configuration file is limited to 4096 characters. WebGate offers a subset of Squid's to ensure access control. You also may run a Squid proxy server together with Webgate.

Like Squid, WebGate's access control scheme has two components: ACL elements and access lists.

4.11.1 ACL elements

ACL elements

ACL elements

An ACL element has the following format:

```
acl <name> <type> <rule>
```

Each ACL element has a unique name. If multiple elements have identical names an error will be reported.

The element `all` matches any request or reply and is implicitly defined by WebGate. You cannot redefine it.

WebGate uses the following types of ACL elements

browser

Syntax:

```
acl <name> browser [-i] <regexp>
```

Enables filtering of connections based on the User-Agent. The `[-i]` flag generates a case insensitive `regexp` evaluation. If a regular expression starts with `-i` followed by space, it has to be escaped by `\-i`.

src

Syntax:

```
acl <name> src <ip/netmask>
acl <name> src <ip1-ip2/netmask>
```

Enables filtering of connections based on the IP address. You can specify a single IP or a range of IP addresses. When filtering several addresses the logical `OR` is used.

Example:

```
acl <name> src <ip1/netmask ip2/netmask ip3/netmask>
```

The ACL element considers a match if at least one IP address matches.

port

Syntax:

```
acl <name> port <number>
acl <name> port <range>
```

Enables filtering of connections based on the destination port. You can specify a single port or a range of ports. When filtering several ports the logical `OR` is used.

dstdomain

Syntax:

```
acl <name> dstdomain <domain>
acl <name> dstdomain "<file>"
```

Enables filtering of connections based on the destination domain. When filtering several domains the logical `OR` is used.

Example:

```
acl antivir dstdomain .antivir.de
```

The ACL element matches `*.antivir.de`
You can define domains in a separate file by separating them by blanks or by writing the domains on separate lines. To include a file you have to start and end the path with quotes.

dstdomain_regexp

Syntax:

```
acl <name> dstdomain_regexp [-i] <regexp>
acl <name> dstdomain_regexp -f "/path"
```

Enables filtering of connections based on the destination domain, but for matching regular expressions are used.
You can use the `-f` switch for reading a list of regular expressions from a file. The path towards a file must be marked by quotes. Each line in the file represents a regular expression and must have the format: `[-i] <regexp>`.

dsturi

Syntax:

```
acl URIS dsturi -f "path_to_list"
acl URI <uri>
```

Example:

```
acl URIS dsturi -f "/etc/avira/list_of_uris.txt"
acl URI dsturi http://web.address.com
```

Enables the filtering of connections based on the full destination of URIs/URLs. When filtering several URIs/URLs the logical `OR` is used. The path towards a file must be marked by quotes. Each line in the file represents an URI.

dsturi_regexp

Syntax:

```
acl URIS dsturi_regexp [-i] <regular expression>
acl URIS dsturi_regexp [-i] -f "path_to_list"
```

Example:

```
acl URIS dsturi_regexp -i -f "list_of_regex.txt"
```

Enables filtering of connections based on the full destination of URIs/URLs, but for matching regular expressions are used. You can use the `-f` switch for reading a list of regular expressions from a file. The path towards a file must be marked by quotes. Each line in the file represents a regular expression and must have the format: `[-i] <regexp>`.

req_mime_type

Syntax:

```
acl <name> req_mime_type <regular expression>
```

Enables searching for <regexp> in the request mime type header. You can use this element for detecting file uploads or HTTP tunneling requests.

rep_mime_type

Syntax:

```
acl name rep_mime_type regexp
```

Enables searching for <regexp> in the reply mime type header. You can use this element for detecting file downloads. When using http_access rules this element is invalid.

set

Syntax:

```
acl <name> set <option> <value>
```

Enables setting of an option to be used for request or reply. Inside http_access or http_reply_access list this element always evaluates to `true`. If the request matches the appropriate access list the element sets the desired option. You can set the following options:

`TrickleDataSize, ReserveDataSize, KeepAliveMode, RefreshInterval, RedirectInterval and KeepAliveInterval`

If you specify both `ReserveDataSize` and `TrickleDataSize` in the rule definition `http_access` or `http_reply_access` `ReserveDataSize` must be used before `TrickleDataSize`.

When a timeout prevention is set using the ACL elements, it overwrites all other specified in the configuration file.

4.11.2 Access lists

Access lists

Access lists

WebGate supports two of the Squid's access lists: `http_access` and `http_reply_access`. The rule for an access list consists of the rule type, the desired action and a list of ACL elements.

http_access

Syntax:

```
http_access <allow|scan|deny|tunnel> <acl_name>
```

Enables filtering requests based on ACL matches. If several ACL names are given, the logical `AND` is used. The default is to allow the connection but scan the data if no rule matches ("allow" rule). To deny all requests except the above specified ones, you have to add a "http_access deny all" rule.

http_reply_access

Syntax:

```
http_reply_access <allow|scan|deny|tunnel> <acl_name>
```

Enables filtering of server responses based on ACL matches. You can set the following actions:

allow

The request is allowed and passed to the subsequent modules (URL filtering and

scanning).

scan

The request is allowed and passed directly to the scanning module. URL filters have no effect.

deny

The request is blocked by WebGate.

tunnel

The data will be forwarded, WebGate will not interfere with this transaction.

Because the data will not be scanned, the tunnel-action should be used with caution.

4.12 Proxy Configuration

If WebGate is installed "behind" a proxy server (Network Configuration 2) or between two proxies, then you need to configure the proxy to forward all requests to WebGate (ie. to use WebGate as parent proxy).

4.12.1 Squid as Proxy

The following example shows the configuration of the squid proxy server:

To instruct squid to forward ALL requests to Avira AntiVir WebGate, the following entries are necessary in the config file squid.conf:

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl all src all
never_direct allow ALL
```

<WebGateHost> and <WebGatePort> must be replaced by the corresponding values.

Because the data transferred over SSL-tunnel connections (established using the HTTP CONNECT method) ARE NOT SCANNED by WebGate, you may want to configure the proxy to bypass WebGate for these connections, in case the proxy is also used for HTTPS. This can be done with the following configuration (squid.conf):

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl SSL method CONNECT
acl all src all
always_direct allow SSL
never_direct allow ALL
```

Another way is to tell squid explicitly to forward "only" HTTP and FTP requests to WebGate and to bypass WebGate for all other types (squid.conf):

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl SCAN_ACL proto HTTP
acl SCAN_ACL proto FTP
cache_peer_access <WebGateHost> allow SCAN_ACL
cache_peer_access <WebGateHost> deny !SCAN_ACL
never_direct allow SCAN_ACL
```

If WebGate is used as parent proxy, you need to start WebGate before the proxy is started.

4.12.2 Using Squid-ICAP

WebGate can also be used in ICAP mode with Squid ICAP. Since ICAP does not provide any form of timeout prevention, using WebGate this way might be impractical in many situations.
The integrated ICAP support is available in Squid 3.0 or later. It is also possible to patch Squid 2.6 and 2.7.
To enable WebGate to work with Squid-icap the following entries are necessary in squid(3).conf:

```
icap_enable on
icap_service service_1 reqmod_precache  0 icap://
[WEBGATE_HOST]:1344/reqmod
icap_service service_2 respmod_precache 0 icap://
[WEBGATE_HOST]:1344/respmod

adaption_service_set class_1 service_1
adaption_service_set class_2 service_2

adaption_access class_1 allow all
adaption_access class_2 allow all
```

If you are using Squid 3.0 or earlier you need to change the following parameters:
adaption_service_set -> icap_class
adaption_access -> icap_class

4.12.3 Apache as Proxy

If you want to use WebGate in conjunction with an apache proxy (`mod_proxy`) you can configure WebGate as a remote proxy as follows (httpd.conf):

```
ProxyRequests On
ProxyRemote http http://<WebGateHost>:<WebGatePort>
ProxyRemote ftp http://<WebGateHost>:<WebGatePort>
```

<WebGateHost> and <WebGatePort> must be replaced by the corresponding values.

5 Operation

After concluding installation and configuration and Avira AntiVir WebGate is running, WebGate guarantees continuous monitoring of your system. During operation you might have to make occasional changes in settings, as described in Configuration – Page 18.

This Chapter is divided in the following parts:

- Starting and Stopping Avira AntiVir WebGate manually – Page 80, describing the start and stop procedure of WebGate from the console.
- In Procedures when Detecting Viruses or Unwanted Programs – Page 83 you can learn what you should do, in case of an infection in your network.

5.1 Starting and Stopping Avira AntiVir WebGate manually

*You must log in as **root** or you must have the required permissions, in order to start or stop Avira AntiVir WebGate.*

If you have installed WebGate as described in Installing Avira AntiVir WebGate – Page 13, it will start automatically by system start.

Starting Avira AntiVir WebGate

▶ Type:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

↳ The program starts with the following message:

```
Starting AVIRA AntiVir WebGate ...
Starting: savapi
Starting: avwebgate.bin
```

If during installation you have set WebGate to start automatically, then you will not have to worry about this.

This is the recommended way of starting WebGate.

If you want to use different parameters for the avwebgate.bin binary, you can do that by changing the DAEMONPARAMS variable from the avwebgate script.

Command line parameters

avwebgate.bin -C <file>	Specifies an alternate configuration file (Default is: /etc/avira/avwebgate.conf)
-N	Starts WebGate without daemonizing
-D	Sets the DebugLevel (0-7)
-V, --version	Shows the WebGate version number

--filter-version	Shows version information about the used scanner and filters
--status	Shows if WebGate is running as configured
--dump-config	Shows the currently active configuration values
--help	Shows the list of options with their description

Without a working license key, WebGate will not start.

To acquire an evaluation key, please send email to:
sales@avira.com

While downloading "large" files, browsers will not see any progress if the refresh method for preventing timeouts is disabled (default). This is because WebGate first downloads the entire file and scans it before any part of the data are sent to the client.

After scanning, the whole file is sent to the client very fast (LAN).

Stopping Avira AntiVir WebGate

▶ Type:

```
/usr/lib/AntiVir/webgate/avwebgate stop
```

↳ The program ends with the following message:

```
Stopping AVIRA AntiVir WebGate ...
Stopping: avwebgate.bin
Stopping: savapi
```

Restarting AntiVir WebGate

This is used, for example, after making changes in configuration scripts.

▶ Type:

```
/usr/lib/AntiVir/webgate/avwebgate restart
```

↳ The program restarts after showing the following message:

```
Stopping AVIRA AntiVir WebGate ...
Stopping: avwebgate.bin
Stopping: savapi
Starting AVIRA AntiVir WebGate ...
Starting: savapi
Starting: avwebgate.bin
```

Checking AntiVir WebGate status

▶ Type:

```
/usr/lib/AntiVir/webgate/avwebgate status
```

↳ The program shows information on the WebGate daemons:

```
Status: avwebgate.bin running
Status: savapi running
```

5.2 Testing Avira AntiVir WebGate

After completing the installation and configuration, you can test the functionality of AntiVir WebGate using a test virus. This will not cause any damage, but it will force the security program to react when the computer is scanned.

Testing Avira AntiVir WebGate with a Test-Virus

▶ Start WebGate:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

▶ Type the following URL in your Web browser http://www.eicar.org.

▶ Read the information about the test virus eicar.com.

▶ Download the test virus on your computer.

↳ Avira AntiVir WebGate will block the access to the file and issues a warning in the browser:

▶ Check the logfile for detailed notifications about the detection.

5.3 Procedures when Detecting Viruses or Unwanted Programs

If correctly configured, Avira AntiVir WebGate is set to deal automatically with all the tasks on your computer:

- The infected file is repaired or at least deleted.
- If it could not be repaired, the access to the file is blocked and, according to the configuration, the file is renamed or moved. This eliminates the risk of infection.

You should however follow these guidelines:

▶ Try to detect the way the infection "sneaked" on your system.

▶ Perform targeted scanning on the data storage that might be infected.

▶ Inform your team, superiors or partners.

▶ Inform your system administrator and security provider.

Submitting Infected Files to Avira Operations GmbH & Co. KG

▶ Please send us the malware or suspicious files that our product does not yet recognize or remove. Send us the virus or file packed (gzip, WinZIP, PKZip, Arj) in the attachment of an email to virus@antivir.de.

When packing, use the password `virus`. *This way, the file will not be deleted by virus scanners on email gateway.*

6 Updates

With Avira Updater you can update Avira software on your computers, using Avira update servers. The program can be configured either by editing the configuration file (Updater Configuration in avupdate-webgate.conf – Page 41), or by using parameters in the command line.

It is recommended to run the Updater as **root**. If the Updater does not run as **root**, it does not have the necessary rights to restart Avira AntiVir WebGate daemons, so the restart has to be made manually, as **root**.

Advantage: any running processes of Avira AntiVir WebGate daemons (such as Scanner, Engine, WebGate) are automatically updated with the current antivirus files, without interrupting the running scan processes. It is thus ensured that all files are scanned.

6.1 Internet Updates

Manually

If you want to update Avira AntiVir WebGate or some of its components:

▶ Use the command:

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=webgate
```

As `[product]`, you can use:

- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `WebGate` - complete update (WebGate, scanner, engine and vdf files).

If you just want to check for a new Avira AntiVir WebGate version without updating AntiVir WebGate:

▶ Use the command:

```
/usr/lib/AntiVir/webgate/avupdate-webgate --check
--product=webgate
```

Automatic updates with cron daemon

Regular updates are made using cron daemon.

The settings for automatic updates in /etc/crontab have already been made when you installed Avira AntiVir WebGate with the install script, the answer for installing AntiVir Updater and starting it automatically was `yes`.

You can find further information on cron daemon in your UNIX documentation.

To make or change the settings for automatic updates in crontab manually:

▶ Add or edit the entry in /etc/cron.d/avira_updater, similar to the example below.

Example: for an hourly update at *:23, enter the following command:

```
23 * * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=[product]
```

As `[product]`, you can use:

- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `WebGate` - complete update (WebGate, scanner, engine and vdf files).

▶ Start the update process to test the settings:

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=[product]
```

where `[product]` takes the same values as above.

↳ If successful, a report will appear in the logfile /var/log/avupdate-webgate.log

7 Service

7.1 FAQs

7.1.1 How to watch for SNMP traps on Debian 5

1.) Install the snmpd package:

```
$ apt-get install snmpd
```

2.) Copy the MIB files from the Avira AntiVir WebGate package to a folder:

```
$ cp antivir-webgate-prof-<Version>/etc/AVIRA-*-MIB.txt
/usr/share/snmp/mibs
```

3.) Configure snmpd in such way that the WebGate MIB files are read:

```
$ echo "+mibs AVIRA-MIB" >> /etc/snmp/snmp.conf
$ echo "+mibs AVIRA-WEBGATE-V0-MIB" >> /etc/snmp/
snmp.conf
```

4.) Configure snmpd by editing /etc/snmp/snmptrapd.conf.

First we need to tell it to accept WebGate's SNMP traps:

```
$ echo "authCommunity log,execute,net SNMP_COMMUNITY" >>
/etc/snmp/snmptrapd.conf
```

Replace SNMP_COMMUNITY by the value of the SNMPCommunity config option (defaults to `Avira`).

Next we can ask snmptrapd to execute a custom program everytime a given SNMP trap is received.

For example, we might use the following line

```
traphandle AVIRA-WEBGATE-V0-MIB::wgtAlert /usr/local/
bin/webgate_alert
```

to make snmptrapd run `/usr/local/bin/webgate_alert` everytime the wgtAlert trap is received.

For example, `/usr/local/bin/webgate_alert` might look like this:

```
#!/bin/bash

name=
url=

while read oid val
do
  if [ "$oid" = "AVIRA-WEBGATE-V0-MIB::wgtMalwareName.0" ]
  then
    name=$val
  fi

  if [ "$oid" = "AVIRA-WEBGATE-V0-MIB::wgtRequestURL.0" ]
  then
    url=$val
  fi
done

echo "WebGate found $name when accessing $url"
```

5.) Run the following:

```
$ snmptrapd -f -c /etc/snmp/snmptrapd.conf -M /usr/share/snmp/
mibs -m AVIRA-MIB:AVIRA-WEBGATE-V0-MIB
```

and wait for AntiVir WebGate to send the wgtAlert trap (you could try to send the Eicar test virus through AntiVir WebGate to trigger this). You should then see the following output in the terminal where you started `snmptrapd`:

```
WebGate found "Eicar-Test-Signature ; virus ; Contains
code of the Eicar-Test_Signature virus" when accessing
"http://www.eicar.org/download/eicar.com"
```

7.2 Support

Support Service

Our website http://www.avira.com contains all the necessary information on our extensive support service.

The expertise and experience of our developers is available to you. The experts from Avira answer your questions and help you with difficult technical problems.

During the first 14 days after you have purchased a license, you can use our **AntiVir Installation Support** by phone, email or by online form.

For further information on the support for your product, please refer to:
http://www.avira.com/en/support-for-business

FAQ

Before you contact our Hotline, we recommend that you visit our section for Frequently Asked Questions at:
http://www.avira.com/en/support-for-business-faq

Message Board	There is also a message board in which you can participate for free: http://forum.avira.com Please use the Search option, your questions may already have been answered for another user and posted on the board.
Email Support	Support via email can be obtained at http://www.avira.com.

7.3 Online Shop

Would you like to buy our products per mouse-click?

You can visit Avira Online Shop at http://www.avira.com and buy, upgrade or extend AntiVir licenses fast and safely. The Online Shop guides you step-by-step through the orders menu. A **multi language Customer Care Center** explains to you the ordering process, the payment transaction and the delivery. Resellers can order by invoice and use a reseller panel.

7.4 Contact

Address
Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Germany

Internet
You can find further information about us and our products by visiting http://www.avira.com.

8 Appendix

8.1 Glossary

Item	Meaning
Backdoor (BDC)	A backdoor is a program infiltrated in order to steal data from the computer, without the user's knowledge. This program is manipulated by third-parties using a remote backdoor-control software, over the Internet or network. AntiVir detects backdoor-control programs.
cron (daemon)	A daemon which starts other programs on specified times.
Daemon	A background process for administration on Unix systems. On average, there are about a dozen daemons running on a computer. These processes usually start up and shut down with the computer.
Dialer	Paid dialing program. When installed on your computer, this program builds a Premium Rate Number Internet connection, charging you at higher rates. This can lead to huge phone bills. AntiVir detects Dialers.
Engine	The scanning module of AntiVir software.
Heuristic	The systematic process of solving a problem using general and specific rules drawn from previous experience. The solution is however not guaranteed. AntiVir uses a heuristic process for detecting unknown macro viruses. When typical virus-like functions are found, the respective macro is classified as "suspicious".
IUM	Avira Internet Update Manager. The individual client computers in your network do not have to download updates from the internet themselves, but easily through your intranet.
Kernel	The base component of a Unix operating system, which performs elementary functions (e.g. memory and process administration)
Logfile	also: Report file. A file containing reports generated by the program at run-time, when a certain event occurs.
Malware	Generic term for "foreign bodies" of any type. These can be interferences such as viruses or other software, which the user generally considers as unwanted (see also Unwanted Programs).
Quarantine directory	The directory where infected files are stored, to block the user's access to them.
root	The user with unlimited access rights (such as system administrator on Windows)
SAVAPI	Secure AntiVirus Application Programming Interface

Item	Meaning
Signature	A bytes-combination used for recognizing a virus or unwanted program.
Script	A text file containing commands to be executed by the system. (similar to batch files in DOS)
SMC	Avira Security Management Center
SMP (Symmetric Multi Processing)	Unix SMP: Unix version for computers with parallel processors.
SMTP	Simple Mail Transfer Protocol: protocol for email transport on the Internet.
syslog daemon	A daemon used by programs for logging various information. These reports are written in different logfiles. The syslog daemon configuration is in /etc/syslog.conf.
Unwanted programs	The name for programs that do not directly harm the computer, but are not desired by the user or administrator. These can be backdoors, dialers, jokes and games. AntiVir detects various types of unwanted programs.
VDF (Virus Definition File)	A file with known signatures for viruses and unwanted programs. In many cases it is enough for an Update to load the most recent version of this file.

8.2 Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at http://www.avira.com .

8.3 Golden Rules for Protection Against Viruses

- Always keep boot floppy-disks, for your network server and for your workstations.
- Always remove floppy-disks from the drive after finishing the work. Even if they have no executable programs, disks can contain program code in the boot sector and these can serve to carry boot sector viruses.
- Regularly backup your files.
- Limit program exchange: particularly with other networks, mailboxes, Internet and acquaintances.
- Scan new programs before installation and the disk after this. If the program is archived, you can detect a virus only after unpacking and during installation.

If there are other users connected to your computer, you should set the following rules for protection against viruses:

- Use a test computer for controlling downloads of new software, demo versions or virus suspicious media (floppies, CD-R, CD-RW, removable drives).
- Disconnect the test computer from the network!
- Appoint a person responsible with virus infection operations and establish all steps for virus elimination.
- Organize an emergency plan as a precaution for avoiding damage due to destruction, robbery, failure or loss/change due to incompatibility. You can replace programs and storage devices, but not your vital business data.
- Set up a plan for data protection and recovery.
- Your network must be correctly configured and the access rights must be wisely assigned. This is a good protection against viruses.

Issued Q3-2012

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile: +49 7542-500 3000
www.avira.com