# Avira Internet Security FireWall

# HowTo





# **Table of Contents**

1. Basic knowledge about the Firewall	3
2. Explanation of the terms	3
3. Configuration Possibilities	5
3.1. Security Level	5
3.1.1 Block all	6
3.1.2 Custom	6
3.1.3 High	7
3.1.4 Medium	/
2.2 Configuration	/7
3.2 Configuration	/ 8
3.2.2 Application rules	
3.2.3 Trusted vendors	
3.2.4 Settings	
3.2.5 Pop-up settings	21
4. General information about "Child Protection	". 24
4.1 Enable "Safe Browsing" in "Child Protection"	25
4.2 User selection	25
4.3 Roles	26
4.3.1 Properties of the role	27
5. Changing the update intervals	29
5.1 Changing an update job	30
5.2 Product update	30
5.3 Restart settings	32

# *<b>AVIRA*

# 1. Basic knowledge about the Firewall

A firewall works with network protocols like e.g. TCP, UDP, IT, etc.

A simple example for building up a connection is also called a handshake procedure. This example shows how a communication is established between two computers in the Internet.

- Computer A sends a package with the information that it wants to build up a connection with computer B
- Computer B answers that it is ready
- Computer A confirms the answer of Computer B
- The connection between Computer A and B is now established and the exchange of data can begin.

# 2. Explanation of the terms

# ТСР

The Transmission Control Protocol (TCP) is an agreement (or protocol) about the way data is being exchanged between computers.

# UDP

The User Datagram Protocol (UDP) is a minimal connectionless network protocol. So-called ports are used to send the data with UDP to the right program on the target computer. Therefore, the port number of the service that contains the data is sent as well. Additionally, UPD offers an integrity check by sending a check sum. This makes the detection of an incomplete transmission possible.

# Flooding

Flooding describes the overflow in a network that is caused by packages. Flooding can paralyze the data transmission in a network (or of a single computer) as the computer or the network is overflowed by a mass of requests and cannot react anymore. You can compare that to a traffic jam on a freeway.

# Ports

A port can be compared to a house number. The difference is that a house, in this case a computer, can have several numbers. A port is a part of an address which assigns the arriving package to an application.



### Example

Port 110 is responsible for the service POP3 and guarantees the access to the email server. Special applications use port numbers that are firmly assigned by the IANA and generally known. Usually the ports are numbered from 0 to 1023 and are called Well Known Ports. Producers of applications can register ports for their own protocols if necessary, similar to domain names.

The registration of the ports offers the advantage that an application can be identified according to the port number, but only if the application uses the IANA registered port. The rest of the ports from port number 49152 to 65535 are so called Dynamic and/or Private Ports. For further information please click here.

#### Port scan

Port scans are executed in order to spy out free ports on the computer. If a computer provides a server service to others, it opens either a TCP/IP or UDP port or both or several ports. A web server has to open the port 80. A port scan finds out which ports are opened on the computer.

#### IP

In order to get connected to a computer the Internet Protocol (IP) identifies it with a definite IP address. In case you send a letter to a friend you have to write the street and the city on it. The IP address has the same function.

#### **Host File**

Sometimes the host file is used to block known web servers by entering the local host (127.0.0.1), so that all requests are sent to the own system. The specialty of this method is that the blockage is valid in the whole system and is not limited to the browser as web filters are. Furthermore you can use these filters against some malware programs if they are trying to get commands from already known servers.

#### URL

Uniform Resource Locators (URL) are a kind of Uniform Resource Identifiers (URIs). URLs identify and locate a resource via the used network protocol (e.g. HTTP or FTP) and the location of the resource within the computer networks.

As URLs are the first and most frequent kind of URIs the terms are often used as synonyms. In colloquial language URL is frequently used as a synonym for Internet addresses like e.g. www.avira.com.

#### Slide-Up

A slide-up is a small window that appears slowly on the top right or down right of your screen and disappears after an interaction or after some time.

# *CAVIRA*

# **3.**Configuration Possibilities

# 3.1. Security Level

First, you have to decide which security level you want to use. A security level that is too high might cause a malfunction of some system features. Using a security level that is to low, you run the risk that not all accesses to your computer are blocked.

In general it can be said: If the PC is not connected with a local network and no network-compatible device (e.g. network printer) is located near the PC, the security level can be set to "High". This means the computer is invisible in the network.

Furthermore, connections from outside are blocked and flooding as well as port scans are prevented.

This is the default setting after the installation of the Avira Internet Security.

In case the PC is located in a network environment or the PC should have access to network devices like e.g. network printer, the security level should be set on "Medium". The "High" level might block the network printer or not recognize it as the firewall does not know that a printer is available.

Please proceed as follows:

🔁 Avira Internet Security			
File View Extras Update Hel	p		
<i>C</i> AVIRA	Avira Internet Security		
Status PC PROTECTION Q System Scanner Realtime Protection	Your computer is secure All services are working correctly		
Backup	PC Protection		Internet Protection
<ul> <li>FireWall</li> <li>Web Protection</li> </ul>	Realtime Protection	¢	FireWall
Mail Protection	♀ Scan system	Ф	Web Protection
Social Networks	Last scan: Not performed		
🙀 Safe Browsing	③ Execute backup	¢	Mail Protection
MOBILE PROTECTION	Last backup: Not performed		
Android Security	🖓 Start update	¢	
ADMINISTRATION	Last update: 9/13/2012		Safe Browsing
😓 Quarantine			Game Mode
🛗 Scheduler			
Reports	Your product is activated until: 12/31/20	12	
Events	*J Renew		Need the help of a security expert?
			Sist Avira Experts Market

Start the Avira Control Center

# *<b>AVIRA*

You can start it by a left double click on the umbrella symbol. The tray icon is located in the task bar, down right next to the system time.

• Open the register "FireWall"

< Avira Internet Security			
File View Extras Update	Help		
<b>Ravira</b>	Avira Internet Se	curity	
🧭 Status	ale .		Configuration
PC PROTECTION			
Q System Scanner	Security level		
🖵 Realtime Protection	- Block all	Medium security lev	vel
③ Backup		Suspicious TCP and	UDP packets are discarded.
INTERNET PROTECTION	Custom	Flooding and Portso	cans are prevented.
🛕 FireWall		Allow external net	for access to shared resources.
Web Protection	e High		
Mail Protection	. Medium		
CHILD PROTECTION			
🧐 Social Networks	Low		
🙀 Safe Browsing			
MOBILE PROTECTION	Transfer		
Android Security	4.89 kB/s		
ADMINISTRATION			
😓 Quarantine		<b>16.</b> 41 -	
📋 Scheduler			
🗐 Reports		Download	Upload
Events	Current	0 B/s	0 B/s
	Total	77.73 MB	1.69 MB

The register is opened by a left mouse click on the register "FireWall". The register "FireWall" is located on the left side of the Control Center below the menu "INTER-NET PROTECTION".

• Adaption of the Security Level of the Firewall

By clicking and keeping hold of the security level controller you can adapt the security level. The possible levels are "Low", "Medium", "High", "Custom" and "Block all". You can find a description of the levels directly on the right side of the controller.

Please choose the level "Medium", in case any problems with network printers, removable hard disk or similar network connections should occur.

# 3.1.1 Block all

All network connections are blocked.

### 3.1.2 Custom

With this option you can set user defined rules.



# 3.1.3 High

The computer is invisible in the network and the connections coming from outside are blocked. Flooding and port scan are prevented.

## 3.1.4 Medium

In comparison to the firewall setting "High", the computer is visible in the network and receives TCP and UDP requests. These requests are rejected. TCP and UDP packages which are received unexpectedly will not be processed and accepted. Flooding and port scan will be prevented.

Problems with the network can occur using the level "Medium", too. In this case you should change the level to "Low".

The preset level is more distinctive in the security level "Medium". This means that with "Medium" some TCP and UDP package requests are recognized and forwarded automatically. Others are rejected.

### 3.1.5 Low

The level "Low" offers you the protection of the Avira Firewall, too. Flooding and port scan will not be prevented, only detected. These are the most frequent methods for finding vulnerabilities on your computer.

In case these settings are not enough for you or you have to activate different ports for an application, you can find more configurations in chapter 3.2 Configuration.

# 3.2 Configuration

Click with the right mouse button on the tray icon in the task bar and choose the item "Configure Avira Internet Security". You also have the possibility to start the configuration by opening the Avira Control Center. Thereafter, press F8 or click on *Extras* > *Configuration*.

In the configuration on the left pane double-click on "Internet protection" and then on "FireWall". Activate the *Expert mode* in order to have access to all possible settings. Here you can configure the following settings:

- Adapter rules
- Application rules
- Trusted vendors
- Settings
- Popup settings



Avira Internet Security		_ <b>_</b> ×
<b>RAVIRA</b>	Avira Internet Security	
1 Expert mode	Internet Protection > FireWall > Adapter rules	? Help
PC Protection		
Internet Protection	E- Local Area Connection 2 (Active)	
<ul> <li>FireWall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> </ul>	ICMP protocol     TCP Port Scan     Up Port Scan     Outgoing Rules     Outgoing Rules	
Mail Protection	Add rule Remove rule Rule up Rule down	Rename rule
<ul> <li>Child Protection</li> <li>General</li> </ul>	Description	•
	Default values QK Cancel Apply	

## 3.2.1 Adapter rules

Each hardware entity that is simulated by a software or each hardware entity (e.g. a network interface card) is seen as an adapter (e.g. Miniport, Bridge Connection, etc.)

The Avira FireWall shows the adapter rules for all adapters that exist on your computer and have a driver installed.

A predefined adapter rule is dependent on the security level. You can change the security level via the Avira Control Center as it is described in chapter 3.1 or change the adapter rules as you like. After you have changed the adapter rules the controller of the firewall is set on the security level "Custom".

### **Incoming Rules**

Incoming rules help to control the incoming data traffic with the Avira FireWall.

### Example

• You want to add the IP address 10.40.30.20.

# *CAVIRA*

If you click on "Add rule", a window opens with different predefined rules. There you choose "Incoming IP rule" and confirm it with **OK**.

Avira Internet Security				
<i>©</i> avira	Avira Internet Security	Add new rule	ICMP protocol 1	
Expert mode Constraints of the second secon	Internet Protection > FireWall > Adap	Rule name: TCP Port Scan TCP Port Scan Allow Peer-To Block IP Block subnet Allow WMVAR Allow IP Allow WP con Allow VPN con Allow File and Incoming Rule Incoming Rule Incoming Scan Incoming Rule Incoming Rule	ICMP protocol 1 Peer network E connections Desktop connection nection Printer Sharing S ICMP rule IDP rule IDP rule IDP rule IDP rule IDP rule IDP rule IP Protocol rule	E
	Alows you to create a new rule. If you press this butto box you can select new rules.	Apply	K Cancel	

In your "Incoming rules" you can find the item "Incoming IP rule". Select this item. You can also rename it. Now you can enter the IP and its mask into the marked box below and enable or block it.

You can also decide if the package should be written into the log file or not.

### **Outgoing rules**

Outgoing rules help to control the outgoing data transfer by means of the Avira FireWall. You can define an outgoing rule for the following protocols:

- IP
- ICMP
- UDP
- TCP

In order to enter settings for the "Outgoing rules" you can proceed in the same way as for the settings of the "Incoming rules".

### Examples

• Peer to Peer

You can use these default templates if you use e.g. exchange systems, file systems or file sharing systems.

You can add the new rule via the following path:

# *AVIRA*

Internet protection > FireWall > Adapter rules > Local Area Connection 2 (Active)

Press the **Add rule** button and select in the next window "Allow Peer-To-Peer network". Click **OK** to confirm.

📿 Avira Internet Security	unity work	×
<b>RAVIRA</b>	Avira Internet Security	Add new rule
		Rule name: Allow Peer-To-Peer network
Expert mode	Internet Protection > FireWall > Ada	TCP Port Scan UDP Port Scan Allow Peer-To-Peer network
Internet Protection	Default     D	Block IP Block IP Block subnet
<ul> <li>FireWall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul>	Add rule Remove rule Rule up	Allow IP     Allow subnet     Allow VPs connections     Allow VPs connections     Allow VPs connection     Allow The and Printer Sharing
thild Protection	Adapter settings.	Incoming IP rule     Incoming ICMP rule     Incoming ICMP rule     Incoming ICMP rule     Incoming ICP rule     Incoming IP Protocol rule
	Allows you to create a new rule. If you press this but box you can select new rules.	

You only have to enable the needed TCP and UDP ports by clicking on the port address in case you need to change it.

Avira Internet Security	e cangalte le accars	×
<b>RAVIRA</b>	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Adapter rules	P Help
PC Protection	□	
<ul> <li>Internet Protection</li> <li>FireWall         <ul> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mal Protection</li> </ul> </li> <li>Child Protection</li> <li>Child Protection</li> <li>General</li> </ul>	Allow P2P program on TCP port 4662 and UDP on port 4672.	Rename rule
	Description       With a mouse click on the link a dialog box appears in which you can enter the permitted TCP p       Default values     QK       Qancel     Apply	ort.



#### • VMware

In case the Internet access should not be possible from your VMware, you have to enable it using the following template.



To change the settings of "Allow VMWARE connections", do the same as in the previous rule for the Peer-To-Peer network.

Avira Internet Security		
<b>RAVIRA</b>	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Adapter rules	? Help
PC Protection	Gradt     Gradt	^
<ul> <li>FireWall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul>	Local Area Connection 2 (ACIVE)     COMP protocol     TCP Port Scan     DDP Port Scan     Dup Port Scan     Dup Port Scan     Dup Connections     Incoming Rules     Outraine Dulae     Add rule     Remove rule     Rule yp     Rule down	E Re <u>n</u> ame rule
thild Protection	Allow VMware machine communication.	*
	Removes the selected rule.	
	Default values OK Cancel Apply	

# *<b>AVIRA*

# 3.2.2 Application rules

This list contains all users in the system. If you are logged on as administrator, you can choose a user and set a rule for him.

If you do not have administrative rights, the list only shows you the currently logged on users.

Avira Internet Security			_ <b>_</b> X	
<b>RAVIRA</b>	Avira Internet Security			
Expert mode	Internet Protection > FireWall > Applicati	ion rules	? Help	
PC Protection	Application rules for user:	/7U64EN\Administrator	•	
Internet Protection	Application	Active Connections	Action	
<ul> <li>FireWall Adapter rules Application rules Trusted vendors Settings Popup settings</li> <li>Web Protection</li> </ul>	<ul> <li>Firefox</li> <li>Windows Activation Client</li> <li>Windows Start-Up Application</li> <li>Windows Media Player Network Sharing Service Configur</li> </ul>	0 0 1 ration App 0	<u>Allow</u> <u>Allow</u> <u>Ask</u> <u>Deny</u>	
Mail Protection	Application details Name: Windows Activation Client Path: C:Windows\System32\sluie.exe	Application details Name: Windows Activation Client		
f General General	Add application Remove rule  Add application  This table shows the list of applications for which rules are de each application that was executed and had a rule saved sin	Show details	Reload the settings of	
	Default values OK Cancel	Apply		

### Example

This way an administrator can make sure that a web browser does not receive Internet access or that a chat program cannot be executed.

# Add application

If you click on the button "Add application", a new window opens with the programs that are already installed on your computer.

<ul> <li>Web Protection</li> <li>Mail Protection</li> </ul>	Application details	
the Child Protection	Name: Firefox Path: C:\Program Files (x86)\Mozilla F	Firefox\firefox.exe
i General	Add agplication Remove rule Description Allows you to create a new application rule. If you presselect the required application for creating a new rule.	Show details Reload
	Default values QK Gancel	Apply



By a simple click the application is marked and can be added to the list with the button "Add".



### **Application settings**

Here you can change the mode from "Filtered" to "Privileged". In the mode "Filtered" the adapter rules and the application rules are checked.

The application rules are checked only in the "Privileged" mode.

Furthermore, the action can be changed from "Allow" to "Deny" or "Ask". If you choose the action "Ask", you are always asked before executing a program if you really want to start the program. In case of the action "Deny", the program will be blocked by the Avira Firewall.

🐼 Avira Internet Security			
<b>RAVIRA</b>	Avira Internet Security		
Expert mode	Internet Protection > FireWall > Application ru	ıles	P Help
PC Protection	Application rules for user: RKW7U64E	N/Administrator	•
Internet Protection	Application	Active Connections	Action
<ul> <li>FireWall         <ul> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> </ul> </li> </ul>	<ul> <li>Firefox</li> <li>Windows Activation Client</li> <li>Windows Start-Up Application</li> <li>Windows Media Player Network Sharing Service Configuration A</li> </ul>	0 0 1 0	Allow Allow Ask Deny
Mail Protection     Child Protection	Application details           Name:         Firefox           Path:         C:\Program Files (x86)\Mozilla Firefox\firefox	(.exe	
E General	Add application         Remove rule           Description         This table shows the list of applications for which rules are defined.           This table shows the list of applications for which rules are defined.         each application that was executed and had a rule saved since the Appli	Show details	Reload the settings of
	Default values OK Cancel Ap	ply	



# 3.2.3 Trusted vendors

A list of reliable software manufacturers is shown in the menu "Trusted vendors". You can add or remove manufacturers on the list by using the option "Always trust this vendor" in the popup window of the network event.

You can allow the network access of applications that are signed by the listed vendors by default. Therefore you activate the option "Automatically allow applications created by trusted vendors".

Avira Internet Security		
«AVIRA	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Trusted ver	ndors 💽 Hel
PC Protection	Trusted vendors for user:	KW 7U64EN \Administrator 🔹
Internet Protection	Automatically allow applications created by trusted vendors	
<ul> <li>Fire/Wall         <ul> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul> </li> <li>Child Protection</li> <li>General</li> </ul>	Vendors Canon Inc. Canon Inc. CalingID Ltd. CalingID Ltd. CalingID Conc., CalingID Conc., Ltd. CalingID Conc., Ltd. CalingID Conc., Ltd. CalingID Conc., Ltd. CalingID Conc., CalingID Co	Rejoad
	Description The highlighted entry is removed from the list of trusted vendors provider from the list, click Apply or OK in the configuration windo Default values OK Cascal	:. To permanently remove the selected ow.

### Trusted vendors for user

This list contains all users in your system. If you are logged on as administrator, you can select a user and view as well as modify his list of trusted vendors.

#### Configuration

# *AVIRA*

If you are not a user with privileged rights, the list only shows you the logged-in user.

📿 Avira Internet Security			_ <b>D</b> X
<b>RAVIRA</b>	Avira Internet Security		
Expert mode	Internet Protection > FireWall	> Trusted vendors	P Help
PC Protection	Trusted vendors for user:	RKW7U64EN\Administrator	•
Internet Protection	Automatically allow applications created b	by trusted vendors	
<ul> <li>FireWall         <ul> <li>Adapter rules                  Application rules                 Trusted vendors                 Setings                 Popup settings</li>                 Web Protection</ul></li>                 Mail Protection                 full Protection                 General </ul>	Vendors  Canon Inc.  Canneverbe Limited  CalingID Ltd.  CalingID  CollingID SYSTEMS JAPAN Co.,Ltd.  Besore  Description  The highlighted entry is removed from the lisprovider from the list, click Apply or OK in the	t of trusted vendors. To permanently remove the e configuration window.	Rejoad
	Default values OK C	ancel <u>Apply</u>	

## Automatically allow applications created by trusted vendor

If this option is activated, applications with a signature of known and trusted vendors get automatically an access to the network. This option is activated by default.

Avira Internet Security		
<b>ØAVIRA</b>	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Trusted vendors	? Help
PC Protection	Trusted vendors for user: RKW 7U64EN (Administrator	•
Internet Protection	Automatically allow applications created by trusted vendors	
<ul> <li>FireWall         <ul> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul> </li> </ul>	Vendors  Contract Con	
the Child Protection	Image: Second	-
fill General	Remove Description The highlighted entry is removed from the list of trusted vendors. To permanently remove the provider from the list, click Apply or OK in the configuration window.	Reload
	Default values OK Cancel Apply	

We recommend that you keep this option activated since we have the contact data of those vendors. Therefore, the vendors are categorized as trusted vendors.

# *AVIRA*

### Vendors

The list shows all vendors that have been categorized as trustworthy.

Avira Internet Security		
<b>Ravira</b>	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Trusted vendors	? Help
PC Protection	Trusted vendors for user: RKW7U64EN\Administrator	-
Internet Protection	Automatically allow applications created by trusted vendors	
<ul> <li>FireWall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul>	Vendors  Vendors  Ctrix Online  Canon Inc.  Cannevrbe Limited  CalingID Ltd.  CalingID Ctd.  CollingID Ctd.  C	
Child Protection	Brother Industries, Ltd	-
fill General	Bemove           Description           The highlighted entry is removed from the list of trusted vendors. To permanently remove the provider from the list, click Apply or OK in the configuration window.	Reload e selected
	Default values OK Cancel Apply	

#### Remove

The marked entry is removed from the list of trusted vendors. To permanently remove the marked vendor from the list, click on **Apply** or **OK**.

MAVIKA	Avira Internet Security		
Expert mode	Internet Protection > FireW	/all > Trusted vendors	Pel
PC Protection	Trusted vendors for user:	RKW7U64EN\Administrato	r 🔻
Internet Protection	Automatically allow applications crea	ited by trusted vendors	
<ul> <li>⇒ FrevVall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> <li>Child Protection</li> </ul>	Vendors Vendor		
i General	Remove Description The highlighted entry is removed from t provider from the list, dick Apply or OK	he list of trusted vendors. To permanently remov in the configuration window.	Reload

# *AVIRA*

### Reload

With the "Reload" button all changes are cancelled. The last saved list will be loaded.

<b>RAVIRA</b>	Avira Internet Security		
1 Expert mode	Internet Protection > FireWa	ll › Trusted vendors	? Hel
PC Protection	Trusted vendors for user:	RKW7U64EN\Administrator	r 🔻
Internet Protection	Automatically allow applications created	d by trusted vendors	
<ul> <li>FireWall</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul>	Vendors Vendors Vullsoft Inc. VIDIA Corporation VIDIA Corporation Vol Data Corporation Vol Data Software Vorade America, Inc. Vorade Corporation		<u> </u>
the Child Protection	Pando Networks, Inc. Piriform Ltd		
E General	Remove Description The changes made are reversed. The last	list saved is loaded.	Reload

#### Note

If you remove a vendor from the list and click on **Apply** or **OK** the vendor will be removed for good. You can't reload it. But you have the possibility to add the vendor again to the list of trusted vendors using the option "Always trust this vendor" in the popup window of the network event.

The firewall prioritizes application rules: The application rule will be used if you create an application rule and the vendor of the application is part of the list of trusted vendors.

### 3.2.4 Settings

### Automatic rule timeout

Block forever

A rule that has been created for a portscan is automatically kept.

• Remove rule after n seconds

A rule that has been automatically created, e.g. for a portscan, is removed after the given time.



This option is activated by default.

Avira Internet Security	patter in accurs			
<i>©</i> AVIRA	Avira Internet Se	curity		
Expert mode	Internet Protectio	on > FireWall > Setti	ngs	P Help
PC Protection	Advanced options	l on startup		
<ul> <li>⇒ FreWal</li> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mal Protection</li> <li>Child Protection</li> <li>Meneral</li> </ul>	Automatic rule timeout Block forever Remove rule after Notifications Flooding Applications blocked IP blocked Description	1,200 📩 se	Application rules Advanced settings Basic settings	
	Default values	C <u>C</u> ancel	Apply	

### **Advanced options**

• Stop Windows Firewall on startup

This option deactivates the Windows Firewall on startup. This option is activated by default as the use of two firewalls at the same time might cause problems.

Two desktop firewalls interfere with each other.

Avira Internet Security	patter la ancara		
<i>©</i> AVIRA	Avira Internet Security		
Expert mode	Internet Protection > FireWall > Set	tings	? Help
PC Protection	Advanced options Stop Windows Firewall on startup		
<ul> <li>Internet Protection</li> <li>FireWall</li> </ul>	Automatic rule timeout	- I <sub>E</sub>	
Adapter rules Application rules Trusted vendors	Remove rule after	seconds	
Settings Popup settings	Port scan	Application rules Advanced settings	
Web Protection     Mail Protection	Flooding  Applications blocked	Basic settings	
Child Protection	IP blocked		
General	Description		
	Default values QK Cancel	Apply	



### Notifications

Here you can define the category of events that will send a notification from the FireWall.

Avira Internet Security	Avira Internet Security		
Expert mode	Internet Protection > FireWall	> Settings	Help
PC Protection	Advanced options Stop Windows Firewall on startup		
Internet Protection     FireWall     Adapter rules     Application rules     Trusted vendors     Settings     Popup settings     Web Protection     Mail Protection	Automatic rule timeout Block forever Remove rule after 1,20 Notifications Flooding Applications blocked	0 📩 seconds Application rules Advanced settings Basic settings	
General	Description		
	Default values OK O	ancel <u>A</u> pply	

• Portscan

If you activate this option you will receive a desktop notification in case a portscan has been detected by the FireWall.

Portscan are not always malicious, but can be a sign of a possible attack on your system.

• Flooding

You will receive a desktop notification in case a flooding attack has been detected by the FireWall, if you activate this option. Flooding attacks can overload your network with a high volume of data and paralyze your network.

• Applications blocked

In case an application should try to establish an external connection which you have not allowed in the FireWall or which is not privileged, the connection is blocked by the Avira FireWall and you receive a desktop notification.

This notification informs you about the application and why it has been blocked.



IP blocked

If this options is activated, you will receive a desktop notification in case the FireWall has rejected the data traffic from a certain IP address.

We recommend to deactivate this option since there are a lot of unwanted IP address requests in the Internet and as a result, you would receive lots of desktop notifications.

### **Application rules**

With these options you set the configurations for the application of the FireWall.

Avira Internet Security	patter is accars		
<b>RAVIRA</b>	Avira Internet Security		
Expert mode	Internet Protection > FireWa	all > Settings	P Help
PC Protection	Advanced options Stop Windows Firewall on startup		
Internet Protection	Automatic rule timeout		
<ul> <li>FireWall         <ul> <li>Adapter rules</li> <li>Application rules</li> <li>Trusted vendors</li> <li>Settings</li> <li>Popup settings</li> <li>Web Protection</li> <li>Mail Protection</li> </ul> </li> </ul>	Block forever     Block forever     Remove rule after     Notifications     Port scan     Flooding	,200 💼 seconds Application rules O Advanced settings O Basic settings	
the Child Protection	IP blocked		
fin General	Description		
	Default values OK	Cancel Apply	

• Advanced settings

If you activate this option, you have the possibility to manage different network accesses of an application individually. This means that you create a special application rule for an application. You can manage the traffic for an application individually or you only monitor the application.

Basic settings

If you activate this option, you can only set one action for different network accesses. Usually this is enough to allow or to block applications.



# 3.2.5 Pop-up settings

### Pop-up settings

• Inspect process launch stack

If this option is enabled, the process stack inspection will be more accurate. The FireWall assumes that each process in the stack being deemed as not trustworthy is the one whose child process enables the access to the network. Therefore, a popup-window is opened for each process in the stack that is deemed as untrustworthy.

These options are deactivated by default. We recommend you to keep the default settings as you would receive a flow of pop-ups otherwise.

• Allow multiple pop-ups per process

If this option is activated, a pop-up window is opened each time an application tries to build up a network connection. Alternatively, you are informed only on the first connection attempt.

This option is deactivated by default. We recommend you to keep the default settings. So you receive only one pop-up window per process.

Avira Internet Security	Avira Internet Security	
Expert mode	Internet Protection > FireWall > F	Popup settings
PC Protection  Internet Protection  FireWall	Popup settings Inspect process launch stack Allow multiple popups per process	Show details Show details on demand Always show details Remember last used state
Adapter rules Application rules Trusted vendors Settings Popup settings Web Protection & Mal Protection	Remember action for this application Always enabled Always disabled Enabled for signed applications Remember last used state	
Child Protection	Description	
	Default values OK Cance	



### Remember action for this application

• Always enabled

The option "Remember action for this application" of the dialog box "Network event" ist enabled as the default setting.

• Always disabled

The option "Remember action for this application" of the dialog box "Network event" ist disabled as the default setting.

• Enabled for signed applications

The option "Remember action for this application" of the dialogue box "Network event" is automatically activated for the network access by signed applications of certain vendors. These vendors are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

• Remember last used state

The option "Remember action for this application" in the dialog box "Network event" is enabled in the same way as for the last network event.

In case the option "Remember action for this application" has been activated for the last network event, the option will also be active for the following network event.

In case the option "Remember action for this application" has been deactivated for the last network event, the option won't be active for the following network event.

Avira Internet Security	The complex is second	
<i>©</i> AVIRA	Avira Internet Security	
Expert mode	Internet Protection > FireWall > Po	pup settings
PC Protection	Popup settings Inspect process launch stack	Show details Show details on demand
<ul> <li>Internet Protection</li> <li>FireWall</li> <li>Adapter rules</li> </ul>	Allow multiple popups per process	<ul> <li>Always show details</li> <li>Remember last used state</li> </ul>
Applications Application rules Trusted vendors Settings Popup settings Web Protection Mail Protection	Remember action for this application     Always enabled     Always disabled     Enabled for signed applications     Remember last used state	
Child Protection		
E General	Description If this option is enabled, the process stack inspecti that any of the untrustworthy processes in the sta its child process. Therefore a different popup wind process stack.	on allows a more accurate control. The FireWall will assume ck may actually be the one accessing the network through ow will be opened for each untrustworthy process in the
	Default values OK Cancel	



We recommend you to keep this option, so that all actions about the connections of the applications are saved automatically.

### Show details

Here you can configure which detailed information in the box network event is important to you.

• Show details on demand

The detailed information are only displayed on request in the "Network event". Details are shown only after a click on the button "Show details" in the "Network event" window.

• Always show details

The details are always shown in the "Network event" window.

• Remember last used state

The display of detailed information is managed in the same way as for the previous network event.

Avira Internet Security	The complex is access		X
«AVIRA	Avira Internet Security		
Expert mode	Internet Protection > FireWall > Po	pup settings	? Help
PC Protection	Popup settings	Show details Show details on demand	
Internet Protection FireWall	Allow multiple popups per process	<ul> <li>Always show details</li> <li>Remember last used state</li> </ul>	
Adapter rules Application rules Trusted vendors Settings Popup settings Web Protection Mail Protection	Remember action for this application Always enabled Always disabled Enabled for signed applications Remember last used state		
thild Protection			
🛗 General	Description If this option is enabled, the process stack inspectic that any of the untrustworthy processes in the star its child process. Therefore a different popup windo process stack.	on allows a more accurate control. The FireWall ck may actually be the one accessing the netw w will be opened for each untrustworthy proc	will assume ork through ess in the
	Default values OK Cancel	Apply	

# *CAVIRA*

# 4. General information about "Child Protection"

Avira Internet Security offers a "Child Protection" function to filter undesired or illegal Internet offers. You can assign different roles to different users. A user role is configurable and contains forbidden or allowed URLs (Internet addresses) and forbidden content categories.

Powerful URL filter lists are used to block Internet contents according to certain categories. In these URL filter lists URLs are categorized in content groups depending on the content of the websites.

The URL filter lists are updated, adjusted and extended every day. They support European languages (English, German, French, Italian, Russian ...). The roles child, young person, adult are preconfigured with the corresponding forbidden categories. In order to configure the parental control, you have to activate it first.

If this option is enabled, all the web pages requested by the user while navigating the Internet are scanned on the basis of the role assigned to the registered user in the parental control function. In case of a forbidden website the website is blocked and a note appears in the browser.

#### Example

If a blocked page is requested, the following browser window appears.





# 4.1 Enable "Safe Browsing" in "Child Protection"

In order to activate the "Child Protection", you need to open the configuration window by going to the Avira Control Center and selecting *Extras > Configuration*. Choose *Child Protection > Safe Browsing* on the left side panel and you should see the window shown below.

Activate "Enable Safe Browsing" on the right pane.

Avira Internet Security	M concertain	
100 AVIKA	Avira Internet Security	
Expert mode	Child Protection > Safe Browsing	? Help
PC Protection	Safe Browsing	
	Enable Safe Browsing	
Internet Protection	Administrator Vilser	Role
the Child Protection	Add >> (Default)	Child
Safe Browsing		
General		
	Change	Child
	(Maximum of 30 characters)	Young person
		Adult
	< Keiligve	
	Description	
	In this field you enter the name of the role that you want to	add to the user roles.
	Default values OK Cancel	Apply

# 4.2 User selection

Select a user and click on **Add**. The user appears on the right pane with the default setting "Child". You can change the role by a simple click.

Avira Internet Security	Avira Internet Security	
Expert mode	Child Protection > Safe Browsing	? Help
<ul> <li>Internet Protection</li> <li>Child Protection</li> <li>Safe Browsing</li> <li>General</li> </ul>	♥ Enable Safe Browsing       User selection       Support       Add ≥>       Add ≥       Add it       Add it         Koles       Change       (Maximum of 30 characters)       Ver         Change       Child       Young person       Adult	
	Description       The list shows all added roles. By double-clicking on a displayed role you can open the dialog for role.       Default values     QK       Qancel     Apply	defining the



# 4.3 Roles

You can add a new role or you can change the given roles.

In order to add new roles, enter the role name in the free box. Please note that the name should not exceed 30 characters.

### Example

The role "child under 16" should be added.

Click on **New**. The new role appears in the right box. In order to configure the role "Child under 16", choose the role and click on **Change**.

Avira Internet Security	Avira Internet Security		
Expert mode	Child Protection > Safe B	rowsing	? Help
PC Protection	Safe Browsing		
Child Protection Safe Browsing General	Support ▼ Add ≥> ≤< Delete	User (Default) Administrator	Role Child Adult
	Roles Child under 16 (Maximum of 30 characters)	Change Child New >> Adult	
	Description	ne role that you want to add to the user role	25.
	Default values OK	Cancel Apply	



## 4.3.1 Properties of the role

Here you can add URLs and block the access to URLs that belong to certain categories.

#### Example

www.google.com and URLs of the category Pornography, Erotica/Sex and Sects should be blocked.

Properties	×
Properties of the role Please select the required role properties 'Chil	ld under 16'.
Control access to the following URLs:	
URL	Rule
www.google.com	Block
Add URL: (Maximum of 512 characters)	A <u>d</u> d D <u>e</u> lete
V Pornography A VErotica / Sex Swimwear / Lingerie V Sects	lowed <u>u</u> sage duration
	ancel <u>H</u> elp

The categories are provided by a huge data base of the enterprise Cobion. Furthermore, the web filter has access to a data base of the consumer protection office Hamburg.

If you should find a website that belongs to one of those categories, you can categorize it via the Test-A-Site website and have it checked.

# *<b>AVIRA*

Additionally, it is possible to limit the time of the Internet usage by clicking the button *Allowed usage duration*.

Activate the category "Limit time of Internet use" and configure the desired maximum Internet surfing time for the current role.

Properties	×	Usage duration	×
Properties of the role Please select the required role properties 'Child und	er 16'.	Allowed usage duration Please specify the desired maximum surf time for the r 16'.	ole 'Child under
Control access to the following URLs:		Imit time of Internet use	
URL	Rule	Time limit per	
www.google.com	Block	Week:	03/00:00
		Month:	12/00:00 🚔
Add URL: (Maximum of 512 characters) Blocking access to URLs in the following categories:	Dglete	Time limit per day Mon-Fri:	hh:mm 01:00 🚔
Pornography     Frotica / Sex     Swimwear / Lingerie     Sects	usage duration	Exact usage period	
<u>Q</u> K <u>C</u> ancel			<u>H</u> elp

By clicking the button **Exact usage period** you will get the opportunity to configure the maximum online time at a specified time.

Enable "Only allow Internet use at the specified times" and then select the desired online times within the chart. The time frame for allowed online connection can be set varying from 30 minutes to 24 hours each day.

Allowed usage duration Please specify the desired maximum sur 16'.	f time for the role 'Child under	Usage perio	ł	Allow	ad u		tim													X
Limit time of Internet use		i		Please Select	spec the c	ify the	e des	es sired ling t	surf	time by h	es fo noldi	r the ng do	role ' wn ti	Child ne m	l und ouse	er 16 butt	5'. :on.			
Time limit per	Day/hh:mm	Only allo	v Inte	ernet us	e at	the sp 8	ecif	ied ti	imes 8 8	8	00:	8 9	8 8	8	8	88	8 8	8	88	88
Month:	12/00:00	Monday	8 5	1 1 1	3 4	05	8 3	2 8	38	9	=	1 1	3 4	15	16	71 č	ំ ដ	8	5 5	3 2
Time limit per day	hh:mm	Tuesday Wednesday																		
Mon-Fri:	01:00	Thursday																		
Sat-Sun:	02:00	Friday																		
Exact usage period		Sunday												[						
	Cancel Help	Legend		Inte Inte	rnet rnet	use al use bl	lowe ocke	ed ed				OK		זר	C	ancel			Hel	p

# *CAVIRA*

# 5. Changing the update intervals

The update of the virus definitions are predefined in the scheduler with an interval of two hours. You can change this setting in case a different time or a more frequent update should be necessary.

- Start the Avira Control Center
- Click on Extras > Configuration and enable the Expert mode

Follow the path *PC protection > Update* in the left menu item of the user interface. The scheduled time of the automatic update will be displayed in the main window.

Preconfigured is a frequent update every two hours with an additional activated job that starts an update every time a connection with the Internet has been established.

Avira Internet Security	WIRA Avra Internet Security	×
<b>RAVIRA</b>	Avira Internet Security	
Expert mode	PC Protection > Update	P Help
PC Protection Scan Scan Report Real-Time Protection Update Product update Restart settings Web server Backup	Automatic update All 00 Day(s) 02 Hour(s) 00 Minute(s) (min. 15 minutes) Also start job when Internet connection is established Repeat job if time has expired	
<ul> <li>Internet Protection</li> <li>Child Protection</li> <li>General</li> </ul>	Description           Description           Default values         QK         Cancel         Apply	

# *CAVIRA*

# 5.1 Changing an update job

In the Automatic update box you can specify the interval that defines when the updates should be performed.

To change the interval, highlight one of the time options in the box and change the input with the arrow keys on the right side.

Avira Internet Security	IFTER Avia Internet Security	
6 AVIRA	Avira Internet Security	
Expert mode	PC Protection > Update	P Help
PC Protection System Scanner Scan Report Real-Time Protection Update Product update Restart settings Web server Badup	Automatic update Al 00 Day(s) 02 Hour(s) 00 Minute(s) (min. 15 minutes) Also start job when Internet connection is established Repeat job if time has expired	
<ul> <li>Internet Protection</li> <li>Child Protection</li> <li>General</li> </ul>	Description	
	Default values QK Cancel Apply	

With the enabled option "Start job while connecting to the Internet (dial-up)" an update will be performed every time an Internet connection has been established in addition to the specified update interval.

The option "Repeat job if time has expired" gives the oportunity to perform past update jobs that could not be performed at the specified time.

# 5.2 Product update

Whithin the menu "Product update" you'll find four different configuration options to run an update.

• Download and install product updates automatically (recommended)

Updates will be downloaded and automatically installed as soon they become available.



 Download product updates. If a restart is necessary, install the update after the system restart, otherwise install it immediately

As soon as product updates are available, they will be downloaded and auto matically installed if no restart ist necessary. Otherwise, the product installation will be executed at the next user-controlled system reboot.

• Notify user when new product updates are available

This option sends a notification email when new updates become available.

Do not download product updates

No automatic update or notification of available product updates are performed.

#### Note

Updates to the virus definition file and search engine are performed independently of the settings within the option "Product updates".

Avira Internet Security	
RAVIRA	Avira Internet Security
Expert mode	PC Protection > Update > Product update
PC Protection System Scanner Scan Report Real-Time Protection Update Product update Restart settings Web server Backup	Product updates     Ownload and install product updates automatically (recommended)     Please note that a product update may require an automatic system restart     Download product updates. If a restart is necessary, install the update after the system restart, otherwise     install it immediately     Notify user when new product updates are available     Notify once again after     7
<ul> <li>Internet Protection</li> <li>Child Protection</li> <li>General</li> </ul>	Description
	Default values OK Cancel Apply

# *<b>AVIRA*

# 5.3 Restart settings

If you have selected automatic product updates under *Local protection > Update > Product update*, you can choose between the different restart notification and restart cancellation options.

• Restart the computer after n Seconds

The necessary restart after a product update is performed automatically at the specified interval. A countdown message appears with no option for canceling the computer restart.

• Periodic restart reminder

The restart which is necessary after a product update is not performed auto matically. At the specified interval, you will receive the restart notifications wit hout cancellation options. These notifications let you confirm the computer restart or select the "Remind me again" option.

• Query whether computer should be restarted

You will receive only one message that offers the option to perform a restart directly or cancel the restart routine.

• Restart computer without query

The restart which is necessary is performed automatically. You will not receive any notification.

Avira Internet Security	
<b>@avira</b>	Avira Internet Security
Expert mode	PC Protection > Update > Restart settings
PC Protection System Scanner Scan Report Real-Time Protection Update Product update Restart settings Web server Badup	Restart settings     Restart the computer after     300     Seconds (with countdown messages, cannot be canceled)     Periodic restart reminder     Query whether computer should be restarted     Restart computer without query
<ul> <li>Internet Protection</li> <li>Child Protection</li> </ul>	
General General	Description If this option is enabled, the restart which is necessary after a product update has been executed is performed automatically. You will not receive any notification.
	Default values QK Cancel Apply



You will find further information:

- In the online help of the program
- In the manual
- In our knowledge base

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

#### Issued Q3-2012

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.



# live *free*."

 $\ensuremath{\mathbb{C}}$  2012 Avira Operations GmbH & Co. KG. All rights reserved. Errors and technical modifications are subject to change.

Avira Operations GmbH & Co. KG Kaplaneiweg 1 88069 Tettnang Germany Telephone: +49 7542-500 0 Facsimile +49 7542-500 3000 www.avira.com