Avira Internet Security 2012

FireWall

HowTo

AVIRA

Table Of Contents

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 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

TCP
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.

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.

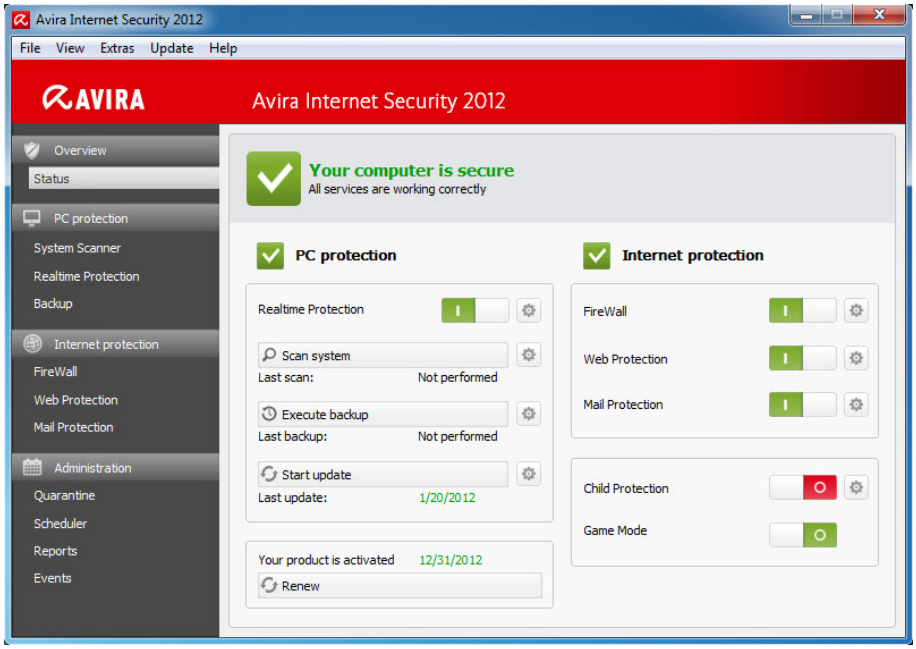
In general it can be said: If the PC is not connected with a local network and no network-compatible device (e.g. network printer) is located near the PC, the security level can be set to “High”. This means the computer is invisible in the network.

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.

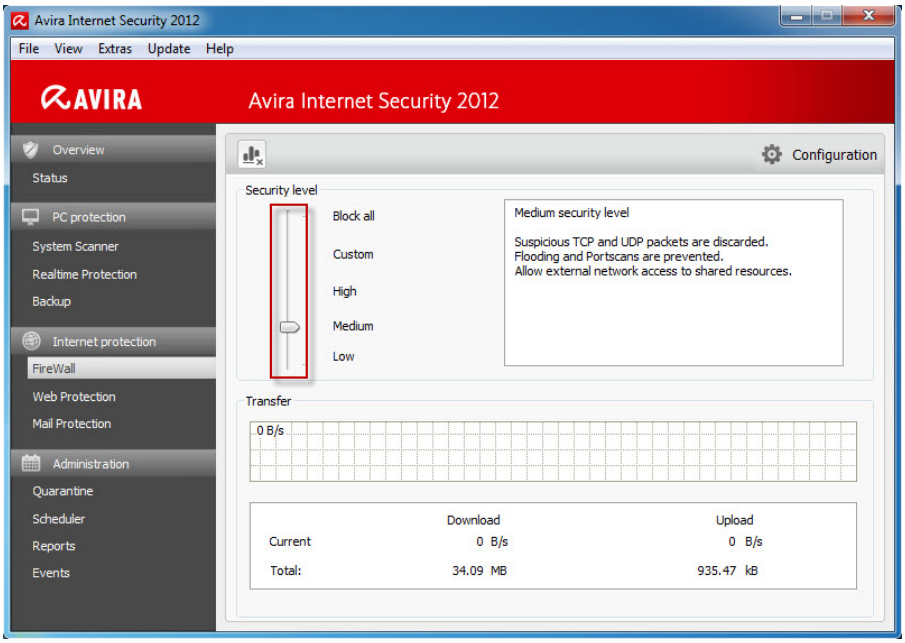
Please proceed as follows:

- Start the Avira Control Center



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“



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 „Internet 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.

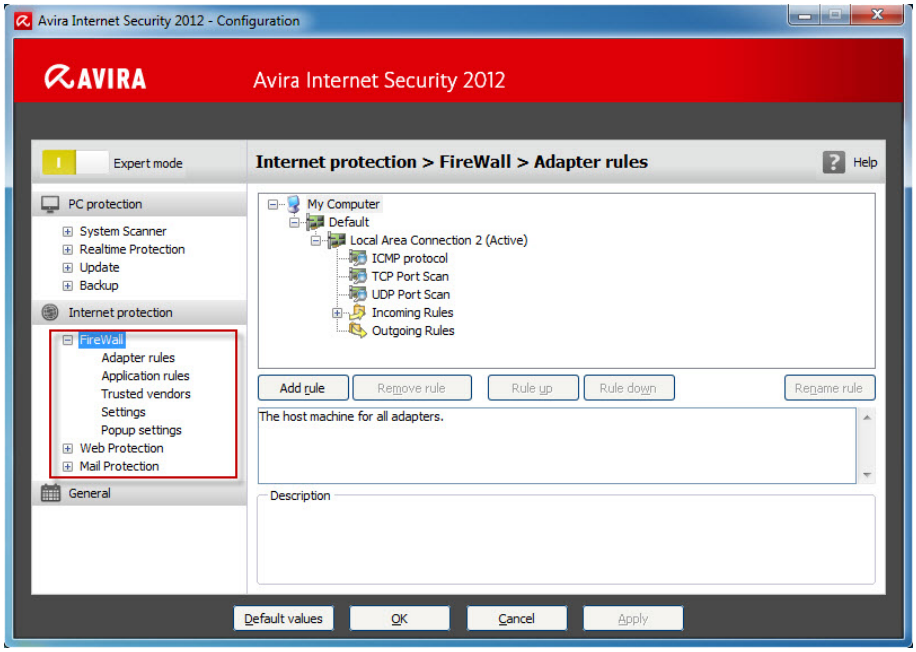
In case these settings are not enough for you or you have to activate different ports for an application, you can find more configurations in chapter 3.2 Configuration.

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 2012”. 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



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”.

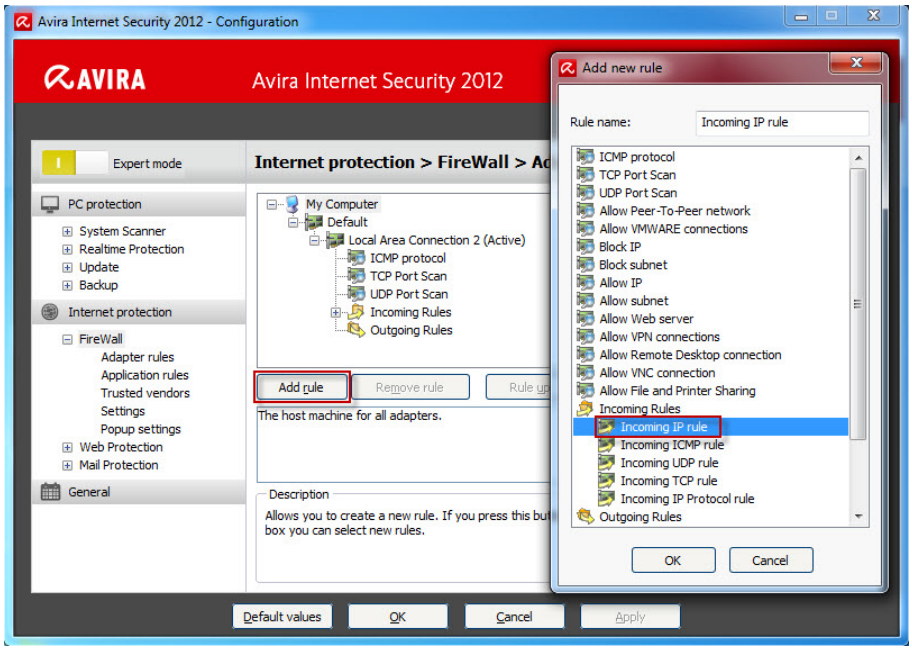
Incoming Rules

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.

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



In your “Incoming rules” you can find the item “Incoming IP rule”. Select this item. You can also rename it. You can now 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”.

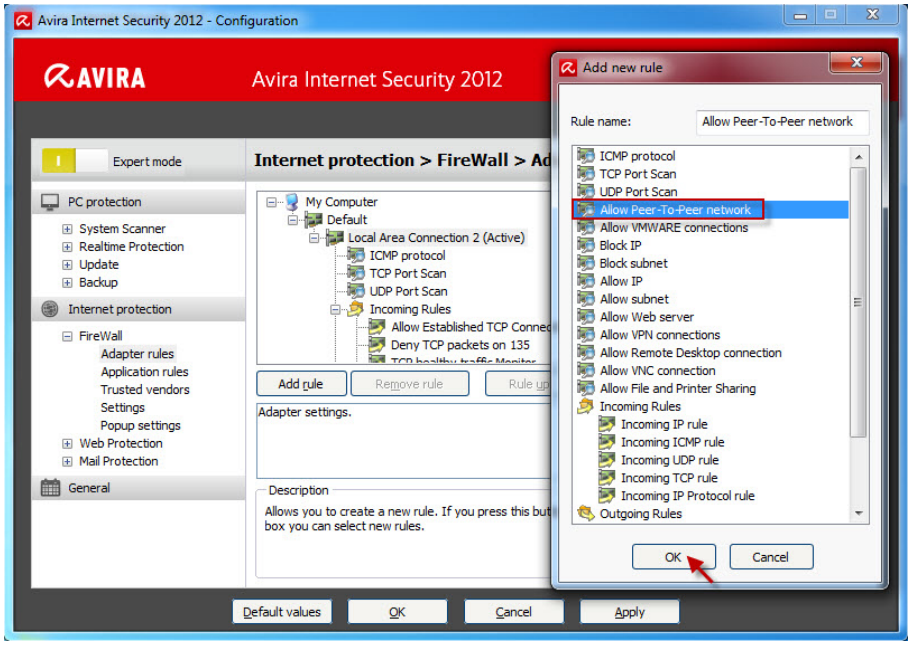
Examples

- Peer to Peer

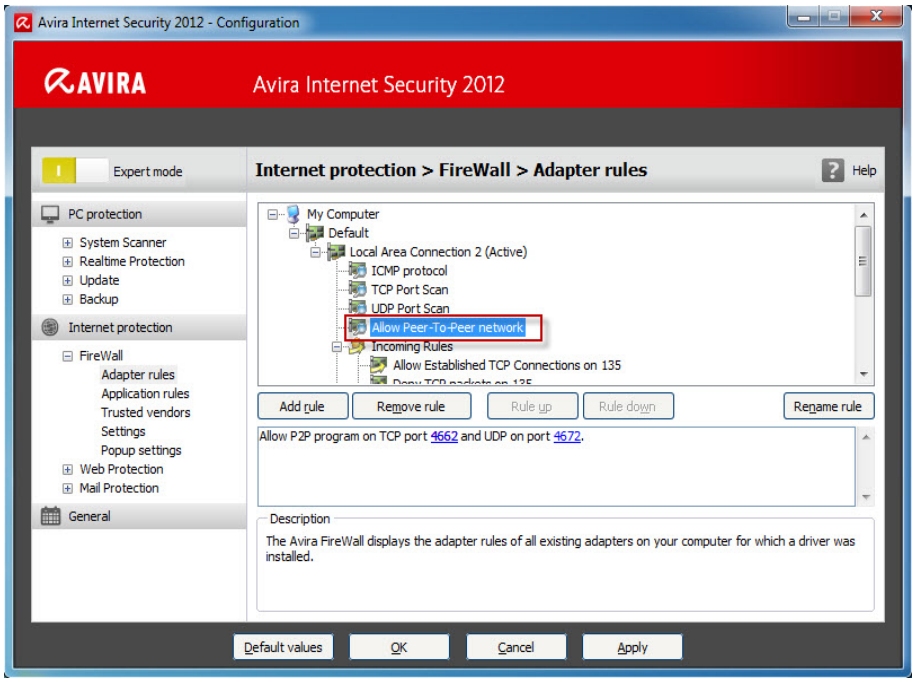
You can use these default templates if you use e.g. exchange systems, file systems or file sharing systems.

You can add the new rule via the following path:
Internet protection > FireWall > Adapter rules > Local Area Connection 2 (Active)

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

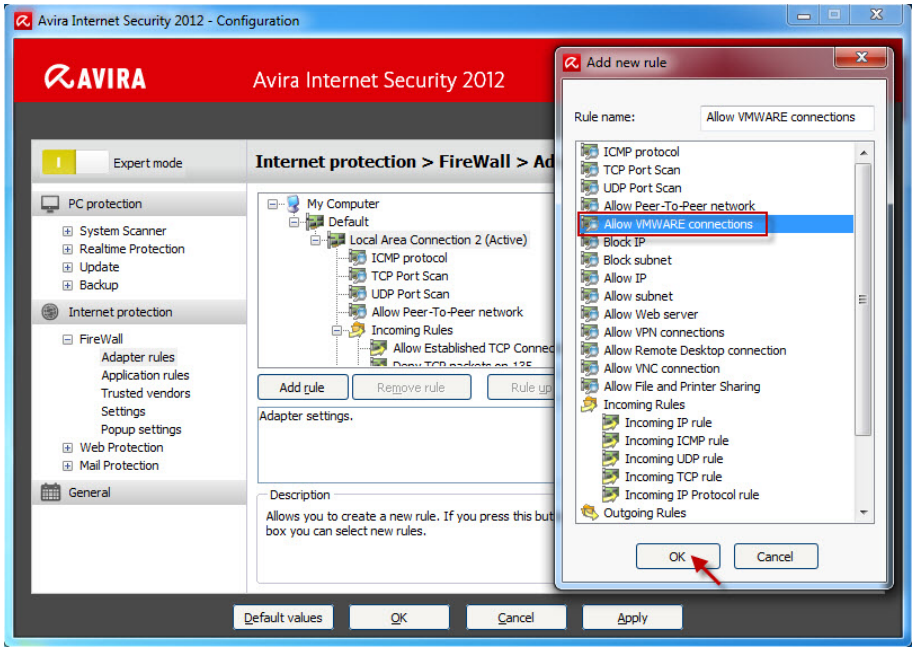


You only have to enable the needed TCP and UDP ports.

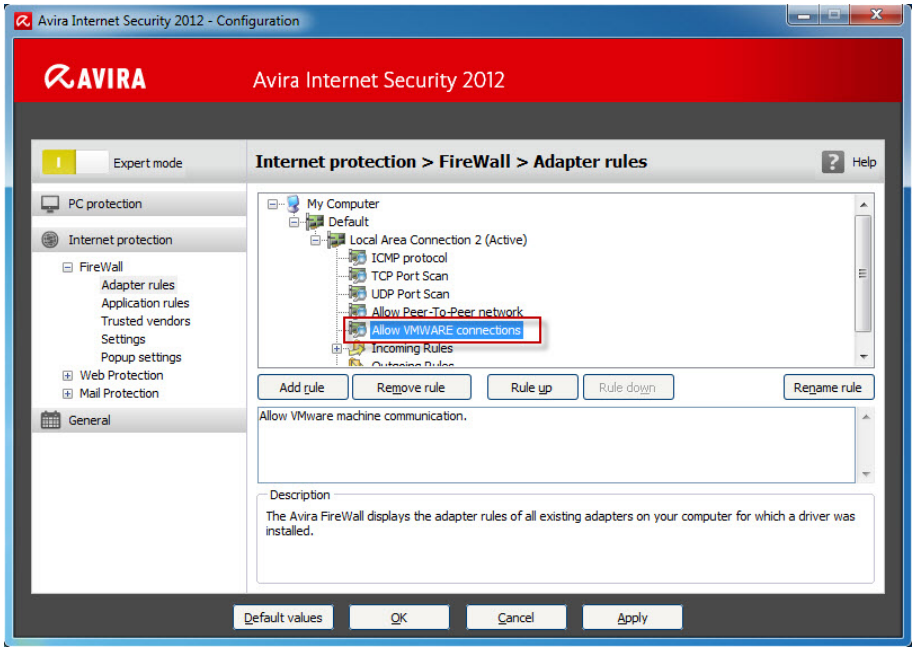


- VMware

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

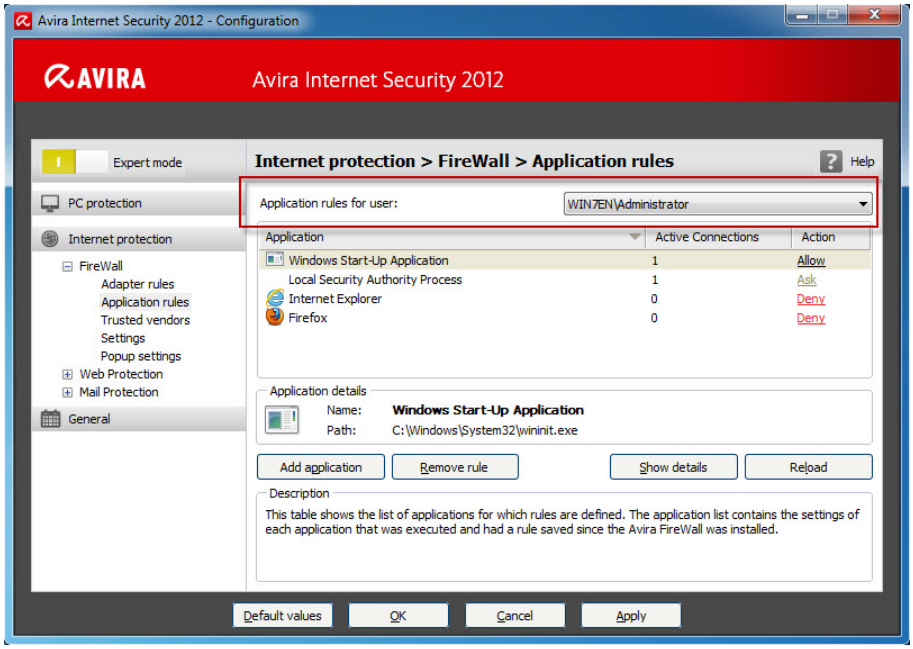


To change the settings of „Allow VMWARE connections“, do the same as in the previous rule for the Peer-To-Peer network.



3.2.2. Application rules

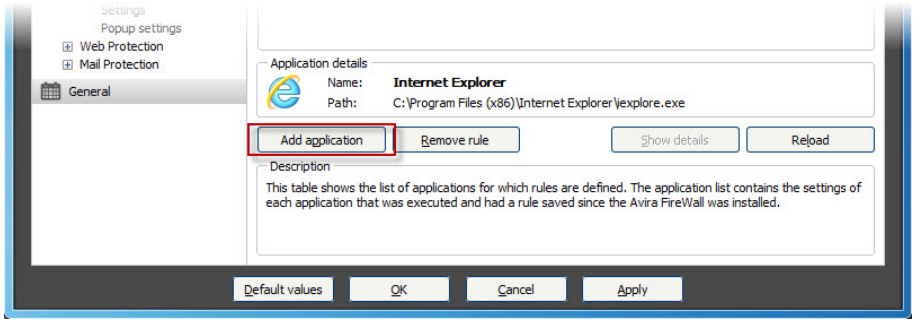
This list contains all users in the system. If you are logged on as administrator, you can choose a user and set a rule for him.
If you don't have administrative rights, the list only shows you the currently logged on users.



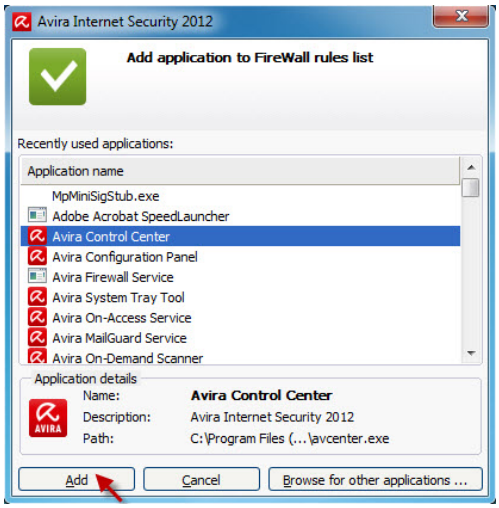
Example
This way an administrator can make sure that a web browser doesn't receive Internet access or that a chat program cannot be executed.

Add application

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



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

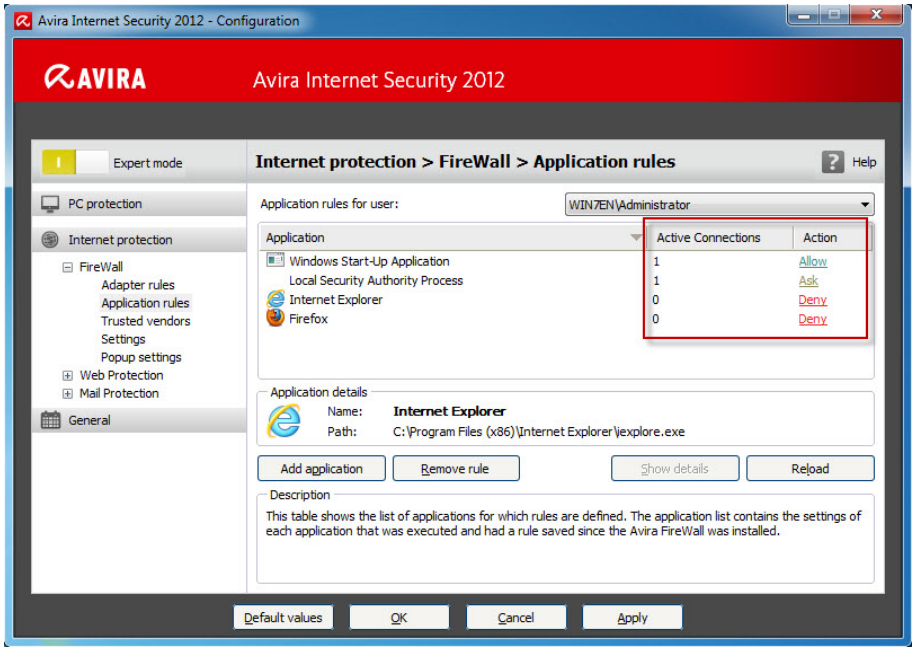


Application settings

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.

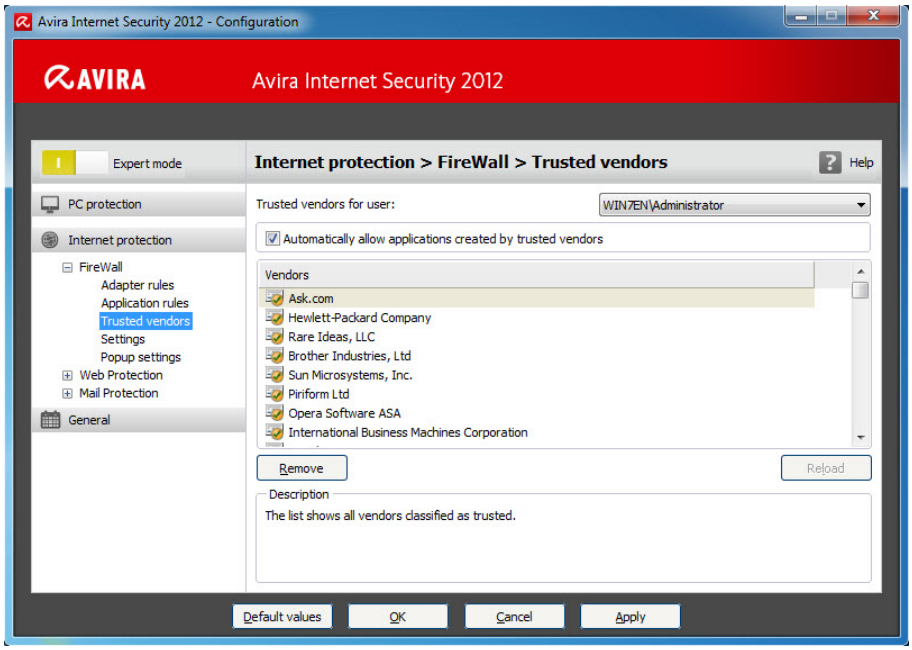
Furthermore, the action can be changed from “Allow” to “Deny” or “Ask”. If you choose the action “Ask”, you are always asked before executing a program if you really want to start the program. In case of the action “Deny”, the program will be blocked by the Avira Firewall.



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.

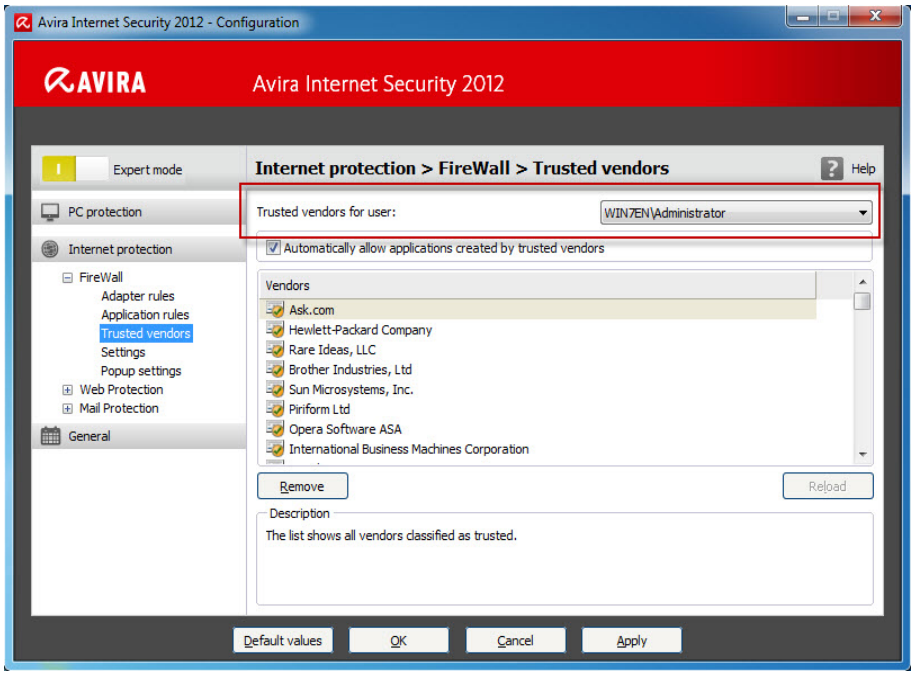
You can allow the network access of applications that are signed by the listed vendors by default. Therefore you activate the option “Automatically allow applications created by trusted vendors”.



Trusted vendors for user

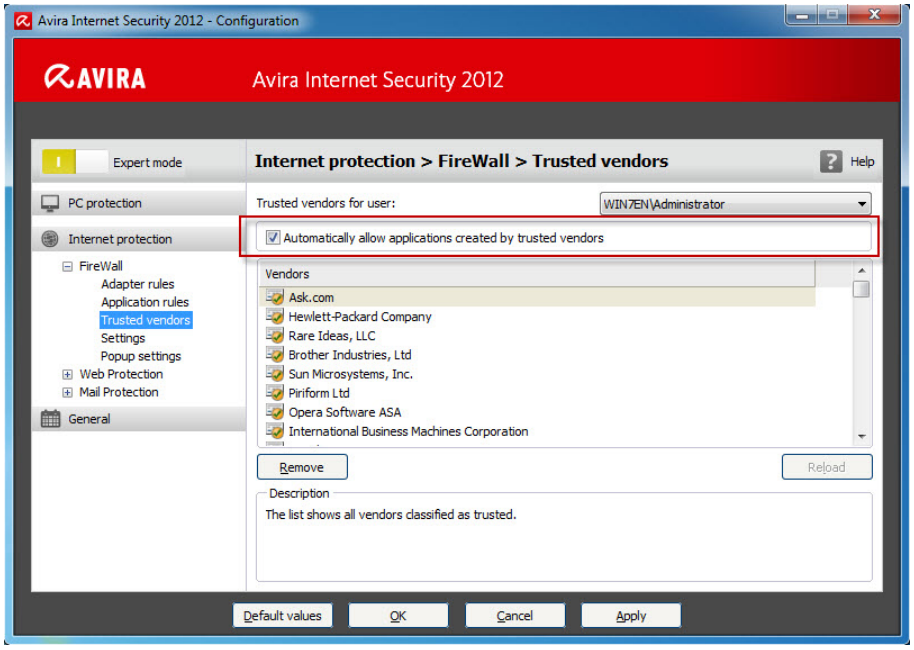
This list contains all users in your system. If you are logged on as administrator, you can select a user and view as well as modify his list of trusted vendors.

If you aren't a user with privileged rights, the list only shows you the logged in user.



Automatically allow applications created by trusted vendor

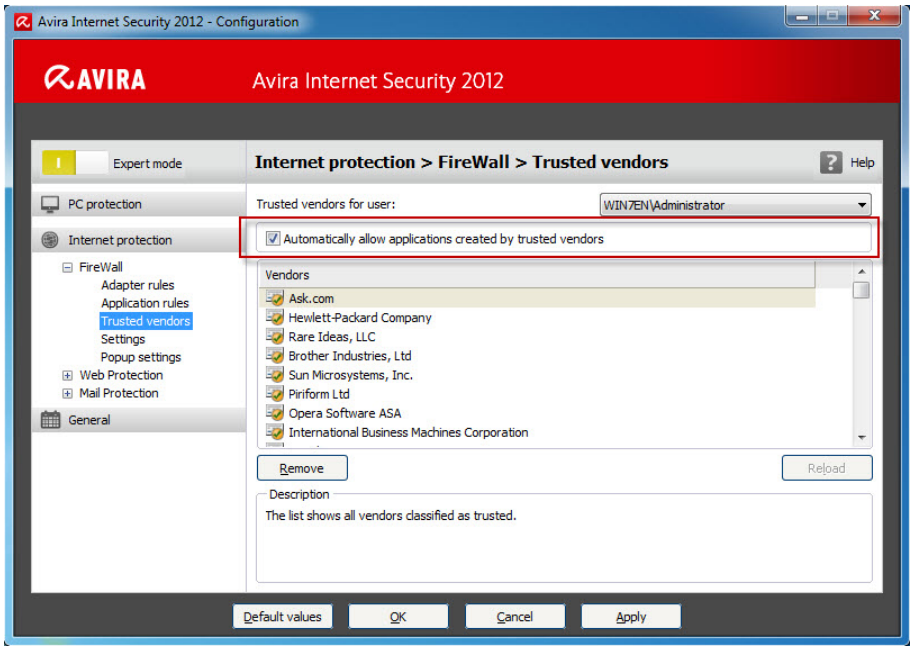
If this option is activated, applications with a signature of known and trusted vendors get automatically an access to the network. This option is activated by default.



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.

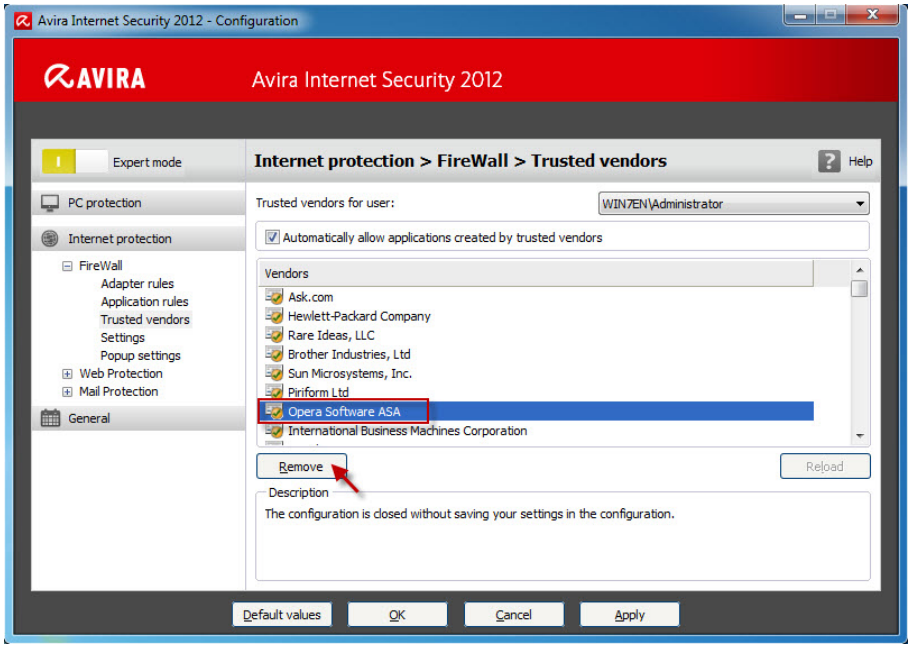
Vendors

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



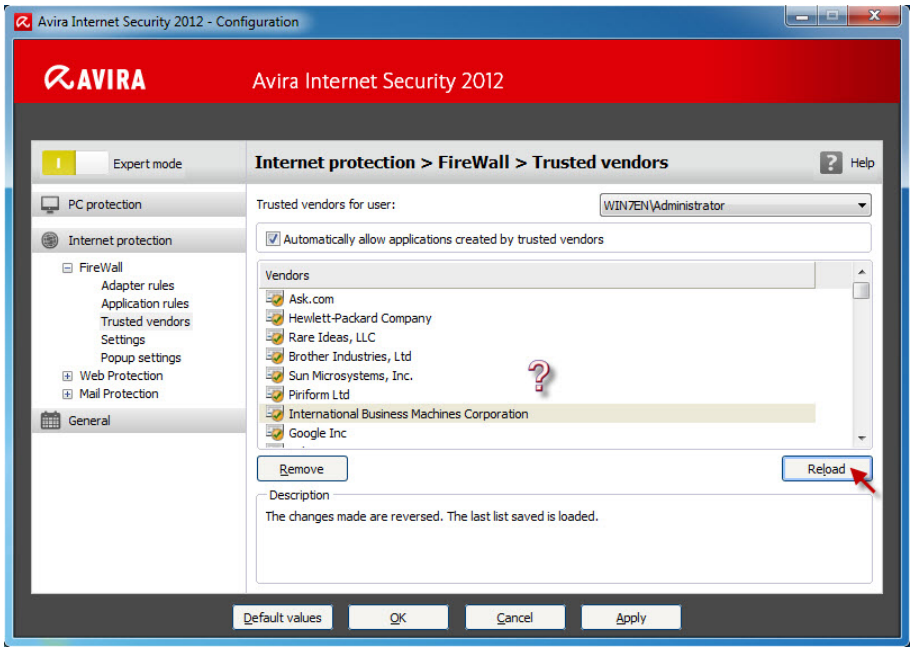
Remove

The marked entry is removed from the list of trusted vendors. In order to remove the marked vendor definitely from the list, press *OK*.



Reload

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



Note
If you remove a vendor from the list and click on “Apply” 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

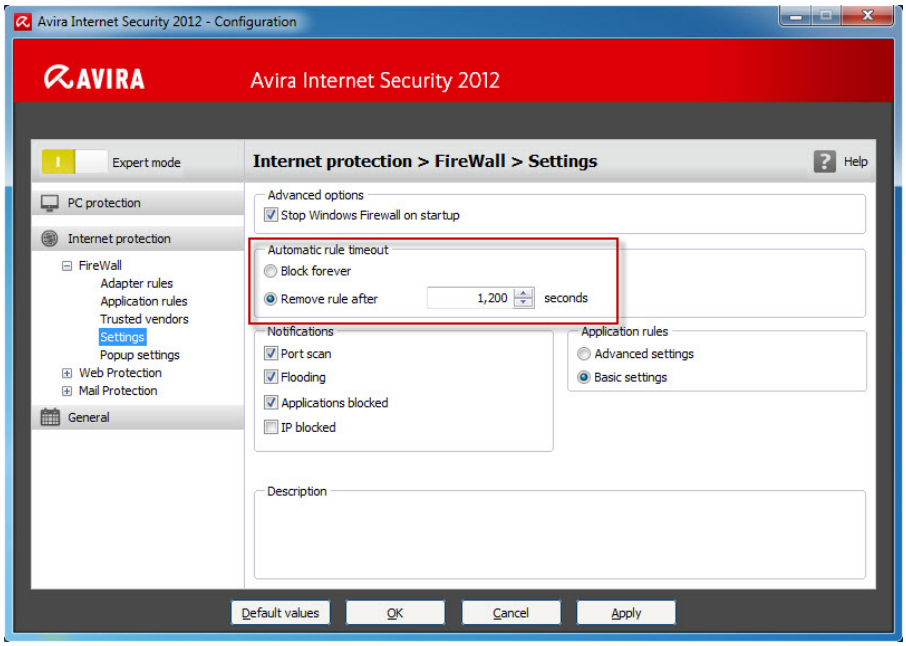
- Block forever

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.

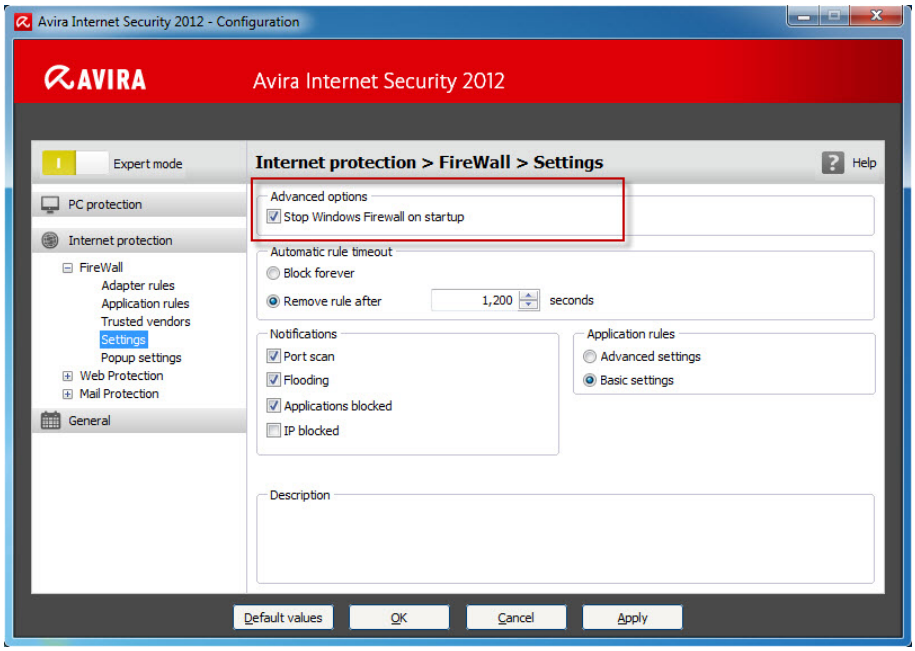


Advanced options

- Stop Windows Firewall on startup

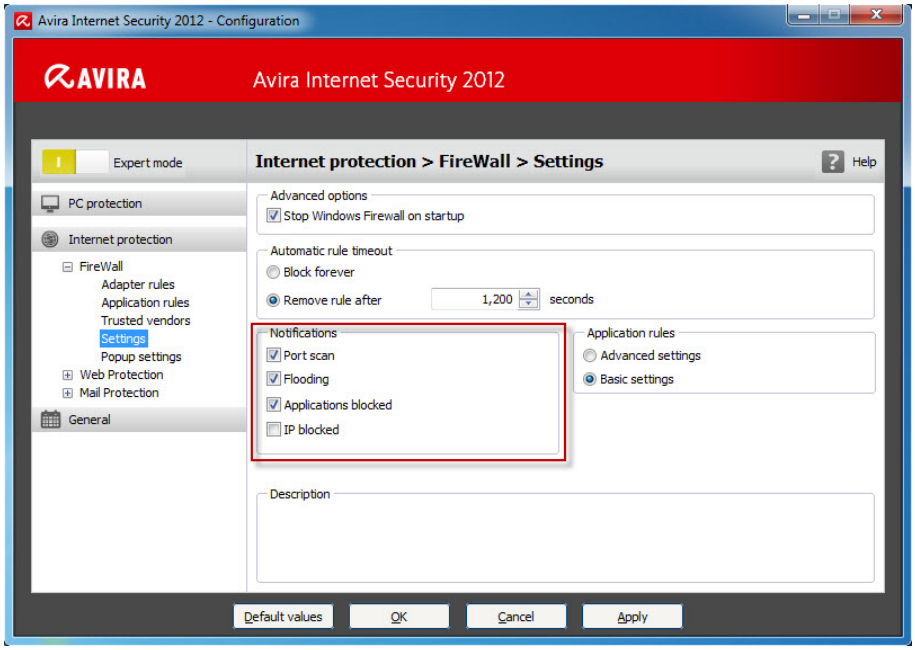
This option deactivates the Windows Firewall on startup. This option is activated by default as the use of two firewalls at the same time might cause problems.

Two desktop firewalls interfere with each other.



Notifications

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



- 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.

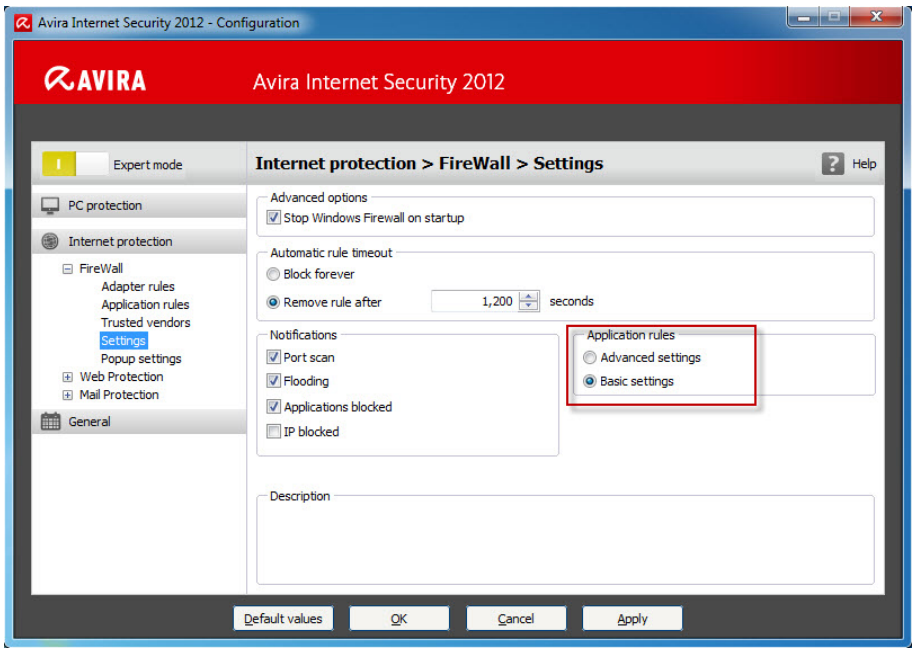
This notification informs you about the application and why it has been blocked.

- 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.



- 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

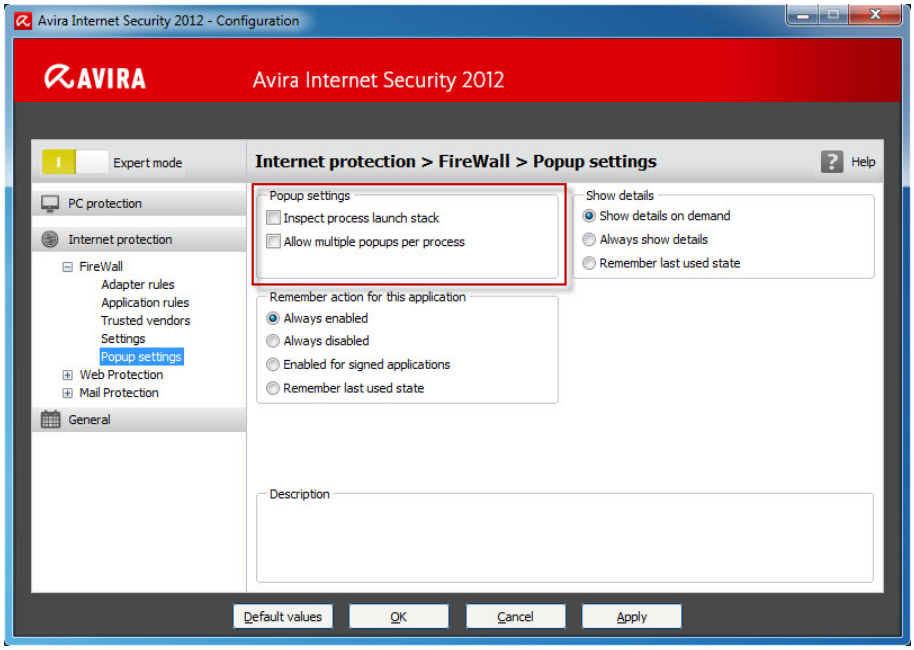
If this option is enabled, the process stack inspection will be more accurate.
The FireWall assumes that each process in the stack being deemed as not trustworthy is the one whose child process enables the access to the network. Therefore, a popup-window is opened for each process in the stack that is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



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

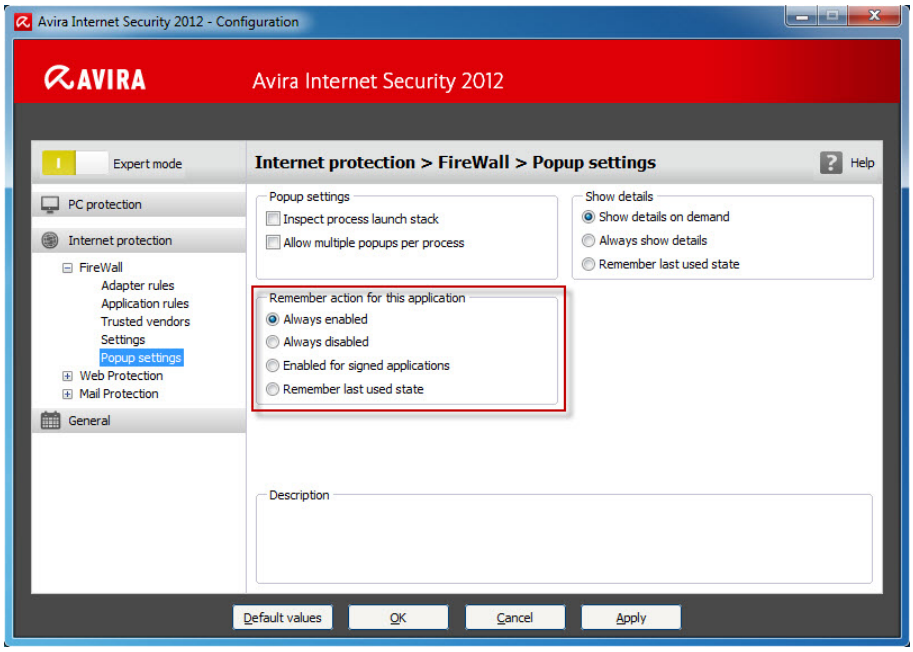
The option “Remember action for this application” of the dialogue box “Network event” is automatically activated for the network access by signed applications of certain vendors. These vendors are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI,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



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

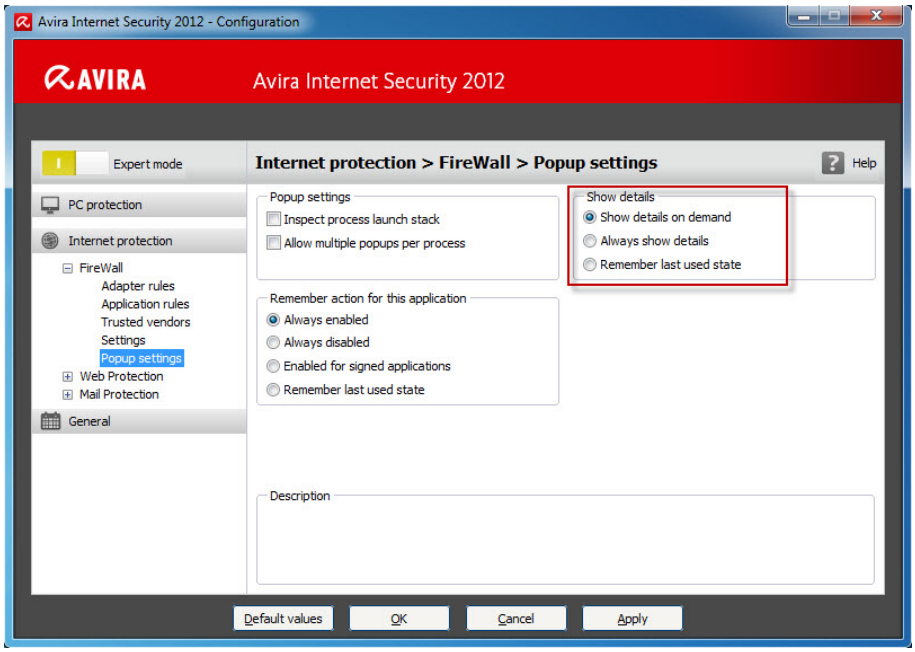
The detailed information are only displayed on request in the „Network event“. Details are shown only after a click on the button “Show details” in the „Network event“ window.

- 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.



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.

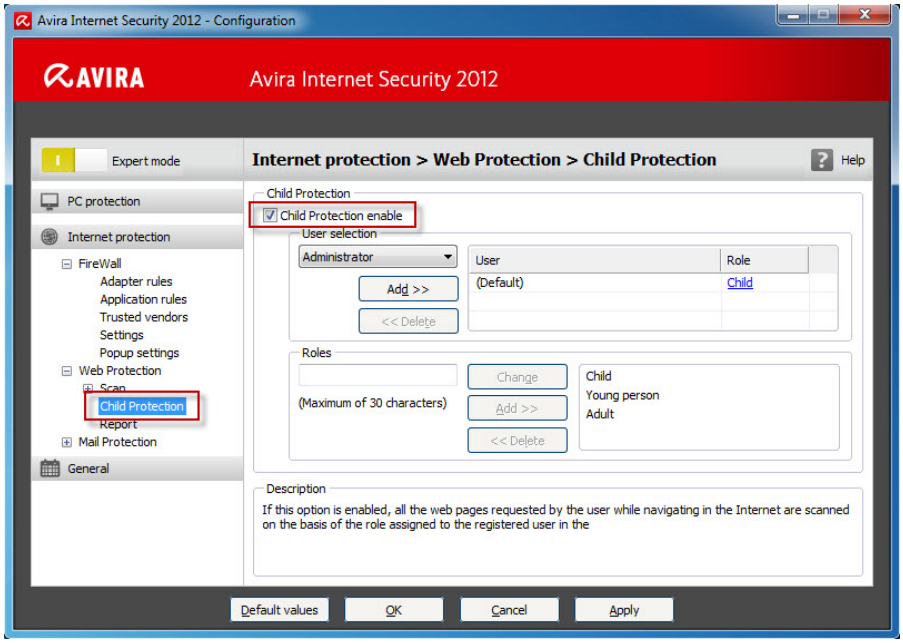
The URL filter lists are updated, adjusted and extended every day. They support European languages (English, German, French, Italian, Russian …). The roles child, young person, adult are preconfigured with the corresponding forbidden categories. In order to configure the parental control, you have to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

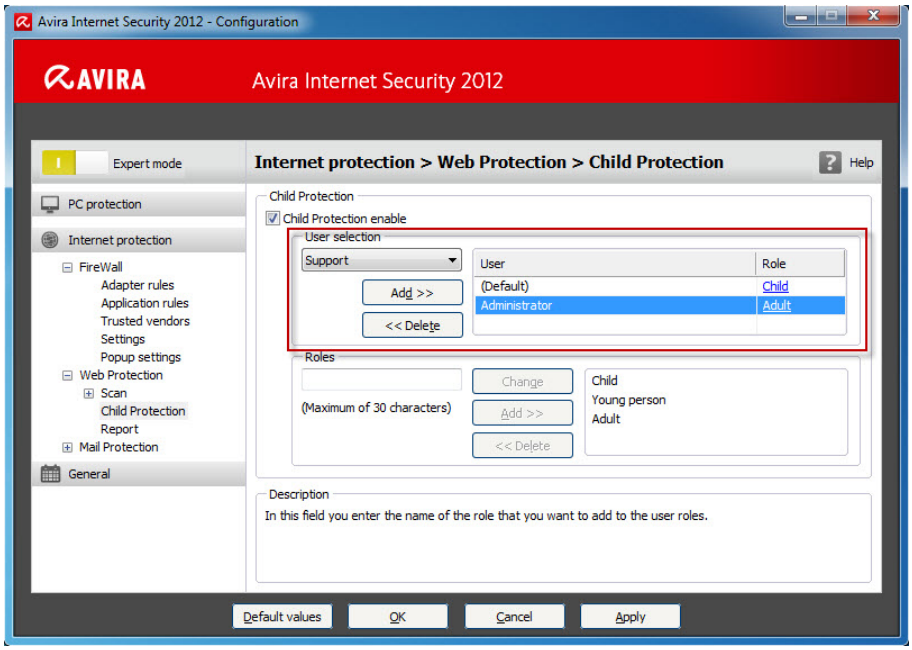
4.1. Enable „Child Protection“

In order to activate the „Child Protection“, go to the Avira Control Center and activate the *Expert mode* via *Extras* > *Configuration*. Choose *Internet Protection* > *Web Protection* on the left side panel.
You can open the windows by clicking on the plus in front of Web Protection. The „Child Protection“ is the third item. Select it and activate it on the right pane.



4.2. User selection

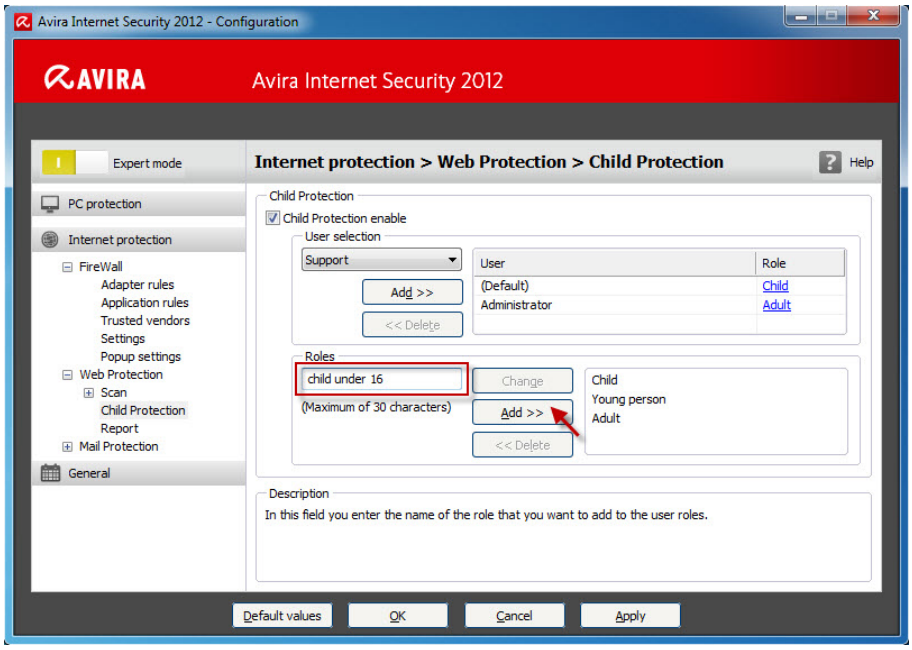
Select a user and click on “Add”. The user appears on the right pane with the default setting “Child”. You can change the role by a simple click.



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.

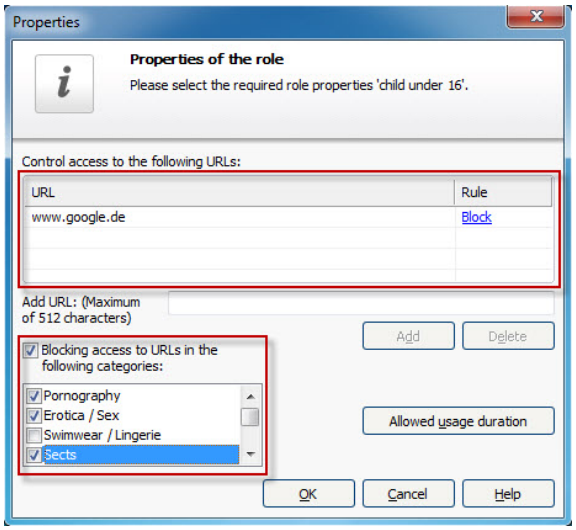


Click on *Add*. The new role appears in the right box. In order to configure the role “Child under 16”, choose the role and click on *Change*.

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.

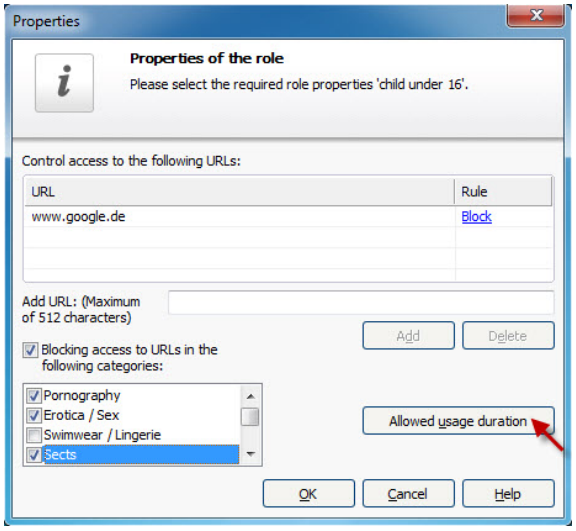


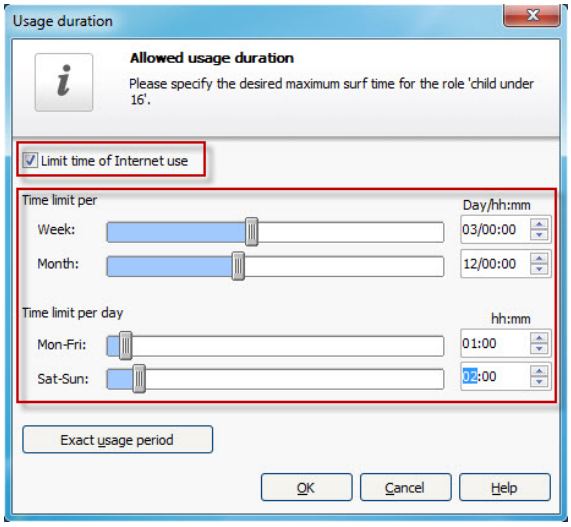
The categories are provided by a huge data base of the enterprise Cobion. Furthermore, the web filter has access to a data base of the consumer protection office Hamburg.

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.

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

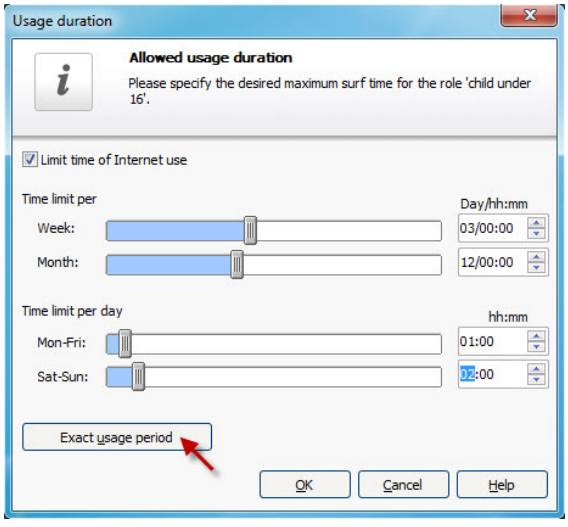
Activate the category „Limit time of Internet use“ and configure the desired maximum Internet surfing time for the current role.

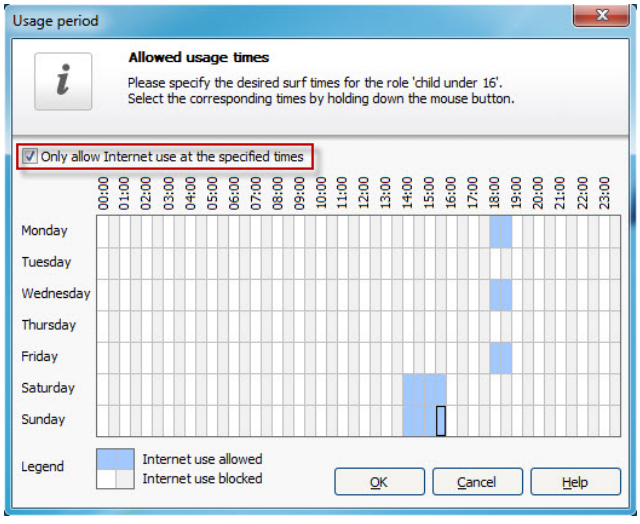




By clicking the button *Exact usage period* you'll get the opportunity to configure the maximum online time at a specified time.

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.





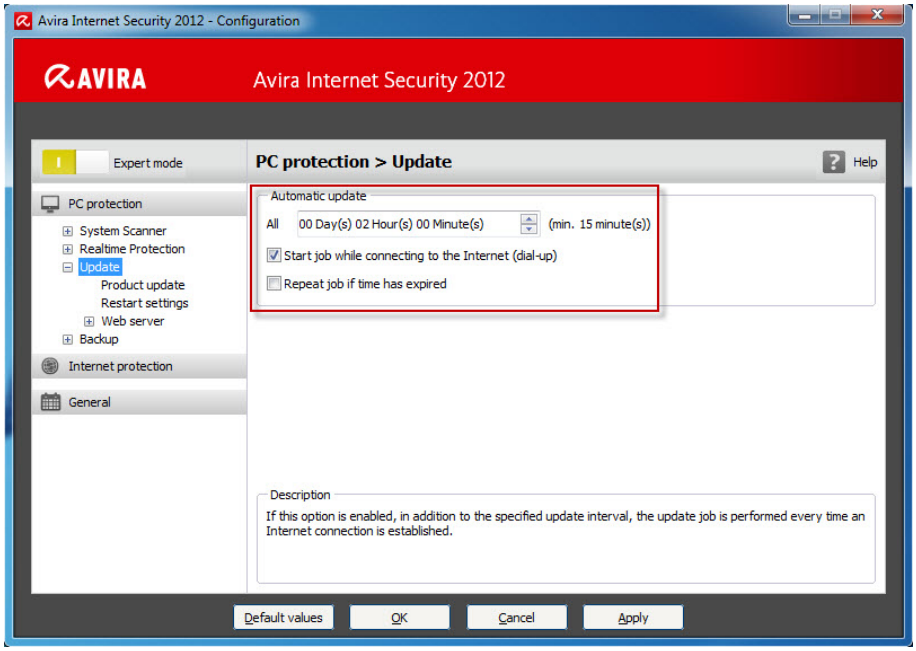
5. Changing the update intervals

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.

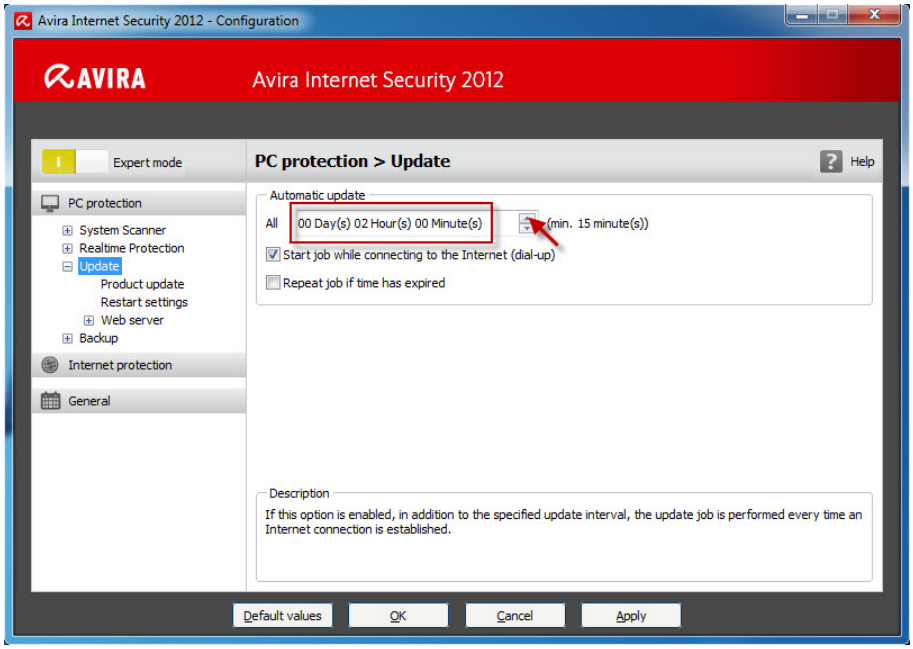
Preconfigured is a frequent update every two hours with an additional activated job that starts an update every time a connection with the Internet has been established.



5.1. Changing an update job

In the Automatic update box you can specifiy 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.



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.

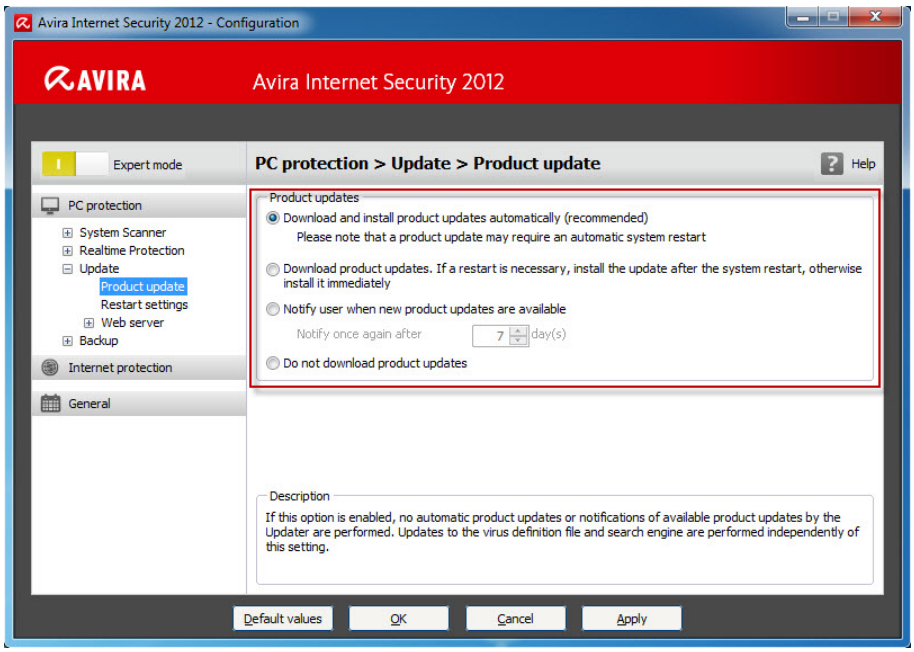
- Notify user when new product updates are available

  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 perfor - med.

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



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

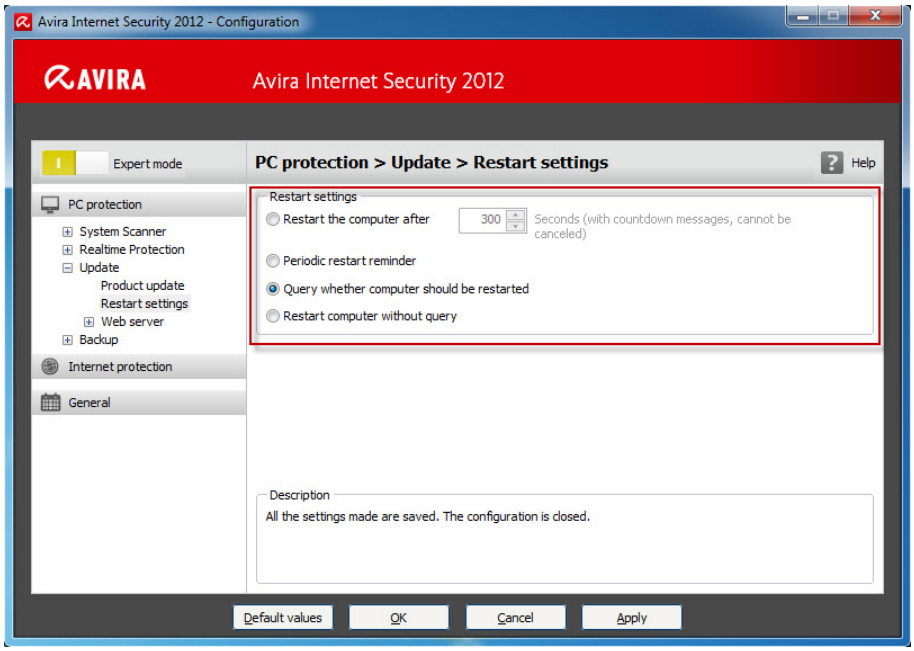
  The restart which is necessary after a product update is not performed auto matically. At the specified interval, you will receive the restart notifications wit hout cancellation options. These notifications let you confirm the computer restart or select the „Remind me again“ option.

- 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.



You find further information:

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

Issued Q4-2011

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