

Vodafone PC Protection Pro

User guide

power to you



vodafone

Index

1.	Introduction	3
1.1	Welcome to PC Protection Pro	3
1.2	Workstation / client security	3
2.	Workstation security software installation	4
2.1	System requirements	4
2.2	Downloading the Workstation software	6
2.3	Uninstalling / removing previously installed antivirus programs	6
2.4	Workstation local installation	6
3.	Virus and spyware protection	7
3.1	Quarantined objects	8
4.	What to do in case of a virus outbreak?	10
4.1	Troubleshooting connection problems	11

1. Introduction

1.1 Welcome to PC Protection Pro

PC Protection Pro protects desktop PCs and laptops. It protects them against viruses, spyware and hidden malware. In addition, the solution contains a firewall, intrusion prevention and application control and automatic virus definition updates. Built-in spam control keeps your e-mail free from spam and other unwanted messages.

The automated features make sure that your operations work 24/7 with minimum intervention and IT resource use.

1.2 Workstation / client security

Comprehensive security for desktop and laptop computers: Antivirus, antispyware, intrusion prevention, application control, proactive protection (F-Secure DeepGuard™), hidden malware detection and spam filtering:

- Security software on computers
- Protects against threats such as viruses, hackers and hidden rootkits, with innovative award-winning solutions
- Blocks unauthorized access attempts and protects remote workers thanks to Internet Shield
- Blocks spam and phishing attempts thus freeing inboxes of junk mail and preventing financial losses to potential recipients of phishing e-mails
- Regular software updates. This ensures access to latest protection features and updates

2. Workstation security software installation

This section describes the system requirements for installing and using the Workstation (PC) product, and gives you instructions on how to install the product.

2.1 System requirements

Read the following before starting to install and use the PC Protection Workstation Security. Your computer must meet the following minimum requirements for installing and using the product:

- | | |
|----------------------------------|---|
| Operating system version: | Microsoft Windows 2000 SP4
Microsoft Windows XP (32-bit). All service packs: <ul style="list-style-type: none">- Home, Professional and Media Center editions Microsoft Windows Vista (32- and 64-bits). All service packs: <ul style="list-style-type: none">- Starter- Home Basic- Home Premium- Business- Ultimate- Enterprise Microsoft Windows 7 (32-bit and 64-bit). All editions |
| Processor: | Microsoft Windows 7 (32-bit and 64-bit). All editions: <ul style="list-style-type: none">- Intel Pentium III 600Mhz or higher For Microsoft Windows Vista (32- and 64-bits): <ul style="list-style-type: none">- Capable of running Microsoft Vista 32-bit |
| Memory: | For Microsoft Windows XP and Windows 2000 (32-bit): <ul style="list-style-type: none">- 256 MB For Microsoft Windows Vista (32- and 64-bits): <ul style="list-style-type: none">- 512MB |
| Display: | For Microsoft Windows XP and Windows 2000 (32-bit): <ul style="list-style-type: none">- 8-bit (256 colors) For Microsoft Windows Vista (32- and 64-bits): <ul style="list-style-type: none">- 16-bit or more (65000 colors) |
| Disk space: | For Microsoft Windows XP and Windows 2000 (32-bit): <ul style="list-style-type: none">- 600MB free HD space (300 MB for Anti-virus only) For Microsoft Windows Vista (32- and 64-bits): <ul style="list-style-type: none">- 600MB free HD space (300 MB for Anti-virus only) |

- Internet connection:** An Internet connection is required in order to validate your subscription and receive updates.
- Browser:** For Microsoft Windows XP and Windows 2000 (32-bit):
- Internet Explorer 5.0 or newer is required.
- For Microsoft Windows Vista (32- and 64-bits):
- Internet Explorer 7.0 or newer is required
- Supported browsers for using the PC Protection Management portal:
- Internet Explorer 6.x or newer is required. JavaScript and cookies must be enabled in the browser
 - Firefox 2.x or newer is required. JavaScript and cookies must be enabled in the browser

The following are the recommended requirements for installing and using the product:

- Processor:** For Microsoft Windows XP and Windows 2000 (32-bit):
- Intel Pentium III 1Gz or higher
- For Microsoft Windows Vista (32- and 64-bits):
- Intel Pentium 4 2GHz or higher
- Memory:** For Microsoft Windows XP and Windows 2000 (32-bit):
- 512 MB or more
- For Microsoft Windows Vista (32- and 64-bits):
- 1 GB or more
- Display:** For Microsoft Windows XP and Windows 2000 (32-bit):
- 16-bit or more (65000 colors)
- For Microsoft Windows Vista (32- and 64-bits):
- 16-bit or more (65000 colors)
- Disk space:** For Microsoft Windows XP and Windows 2000 (32-bit):
- 800MB free HD space (500 MB for Anti-virus only)
- For Microsoft Windows Vista (32- and 64-bits):
- 800MB free HD space (500 MB for Anti-virus only)
- Internet connection:** An Internet connection is required in order to validate your subscription and receive updates.
- Browser:** For Microsoft Windows XP and Windows 2000 (32-bit):
- Internet Explorer 6.0 or newer
- For Microsoft Windows Vista (32- and 64-bits):
- Internet Explorer 7.0 or newer

2.2 Downloading the Workstation software

You can download the PC Protection software on www.vodafone.nl/mccsupport onder 'Security ► PC Protection pro'.

2.3 Uninstalling / removing previously installed antivirus programs

The PC Protection installation does not necessarily remove all existing other antivirus programs currently in the market. It is therefore recommended that before you begin installing the PC Protection client, you should remove any other antivirus programs currently installed on the workstations.

To uninstall other antivirus programs:

1. Select the currently installed programs in the 'Start ► Settings ► Control Panel ► Add/Remove Programs' dialog.
2. Remove any related components.

Some programs may have several related components, which may need to be uninstalled separately. If you encounter problems, refer to the user documentation for the currently installed antivirus program.

3. Restart your computer.

2.4 Workstation local installation

To install the program:

1. Locate the downloaded file and double-click the .exe file to start the installation.
2. Select the installation language, and click 'Next' to continue.
3. Read the license agreement. To accept the agreement and to continue, click 'Accept'.
4. Enter your subscription key and click 'Next'.

You must enter the same subscription key that you used when you created the account.



5. Select the installation type, and click 'Next':

- Automatic installation: The product is installed automatically. Existing security products may be automatically replaced. The product is installed to the default directory.
- Step by step installation: During the installation, you can change the installation directory. However, we recommend using the default directory.

6. When the installation is complete, the computer restarts automatically after a while. To restart immediately, click 'Restart'.

3. Virus and spyware protection

Vodafone PC Protection keeps computers protected against file viruses, spyware, riskware, rootkits and viruses that are spread by e-mail attachments and in web traffic.

Automatic updates guarantee that virus and spyware protection is always up-to-date. Once you have set up Vodafone PC Protection you can be sure that your end-users are protected. You can also monitor the scanning results and other information the managed hosts send back to PC Protection Management Portal.

When a virus is found on a computer, one of the following actions will be taken:

- The infected file is disinfected,
- The infected file is renamed,
- The infected file is deleted,
- The infected file is quarantined,
- The user is prompted to decide what action to take with the infected file,
- The infected file or attachment (in e-mail scanning) is reported only
- The infected attachment (in e-mail scanning) is either disinfected, removed or blocked.

Real-time scanning

Real-time scanning keeps the computer protected all the time, as it is scanning files when they are accessed, opened or closed. It runs in the background, which means that once it has been set up, it is basically transparent to the user. Real-time scanning is enabled by default to the workstation and server software.

DeepGuard

DeepGuard is a host-based intrusion prevention system that analyzes the behavior of files and programs. DeepGuard is used to block intrusive ad pop-ups and to protect important system settings, as well as Internet Explorer settings against unwanted changes. If an application tries to perform a potentially dangerous action, it will be checked for trust. Safe applications are allowed to operate, while actions by unsafe applications are blocked.

DeepGuard asks users what to do only in those cases when DeepGuard does not trust an application. It is enabled by default and cannot be disabled.

3.1 Quarantined objects

Quarantine management gives you the possibility to process objects that have been quarantined on host machines in a centralized manner.

All infected files and spyware or riskware that have been quarantined on host machines are displayed on the “Settings” ► “Quarantine management” page. From there, you can either release the objects from quarantine, or delete them.

Note: Quarantine management should be used primarily for troubleshooting purposes. For example, if a business-critical application is considered riskware and it has not yet been included in the virus definition database, you can use quarantine management to allow it to be used. Such cases are relatively rare, and once new virus definition updates that treat the application as normal are available, the problem should be fixed automatically.

Deleting quarantined objects

Infected files, spyware or riskware that have been quarantined on hosts can be removed from quarantine, in which case they are deleted from the host machine.

1. Select the target domain.
2. Go to the “Settings” tab and select the “Quarantine management” page.
3. Select the quarantined object you want to delete on the “Quarantined objects” table, and click ‘Delete’. The object is moved to the “Actions to perform on quarantined objects” table, with “Delete” given as the “Action” for the object.
4. Click ‘Save’.

Releasing quarantined objects

Infected files, spyware or riskware that have been quarantined on hosts can also be released from quarantine, in which case they are allowed on the host machines and can be accessed and run normally.

1. Select the target domain.
2. Create an exclusion rule for the object.

Exclusion rules are required to make sure that the object will not be quarantined again in future. If the object is listed as a virus or infected file:

- Go to “Settings” ► “Quarantine management” page and copy the object’s file path.
- Go to “Settings” ► “Real-time scanning” page.
- Right-click ‘Enable excluded objects’ and select ‘Locate in advanced mode’ from the context menu. This will open the “Advanced mode” user interface.
- On the “Policy” tab, select ‘Excluded Objects’.
- Click ‘Add’ and enter the file path for the quarantined object.

- Select 'View' ► 'Anti-virus' mode from the menu to return to the "Anti-virus mode" user interface, and make sure that "Enable excluded objects" is selected on the "Settings" ► "Real-time scanning" page.

If the object is spyware or riskware:

- Go to "Settings" ► "Spyware control" page.
 - Select the object you want to allow on the Spyware and riskware reported by hosts table and click 'Exclude application'.
 - A dialog asking you to confirm the action opens, after which the selected application will be moved to the Applications excluded from spyware scanning table.
3. Go to the "Settings" tab and select the 'Quarantine management' page.
 4. Select the quarantined object you want to allow on the "Quarantined objects" table, and click 'Release'. The object is moved to the "Actions to perform on quarantined objects" table, with "Release" given as the "Action" for the object.
 5. Click 'Save'.

4. What to do in case of a virus outbreak?

You can use this checklist of what you should do and remember in case there is a virus outbreak in the company network.

1. Disconnect the infected computer from the network immediately. If the infection keeps spreading, the whole network should be taken down without delay. All outgoing traffic should be blocked. Employees must be instructed to report suspicious activities on their computers immediately.
2. Try to identify whether it is a real infection or a possible false alarm. Scan the computer with PC Protection and the latest virus definitions updates. If the infection is identified exactly, go to the next step. If the infection is identified as "possible new virus", "could be an image of a boot sector virus" and so on, send a sample together with the PC Protection client scan report through the Submit Malware Sample web tool at: <http://www.fsecure.com/samples>.
3. If it is a known infection, go to the F-Secure virus information pages and get a description of the malware. Download disinfection tools (if available) and print disinfection instructions. In case disinfection assistance is needed, contact Vodafone Support at 1200 through the Vodafone network or via +31(0) +31 654 500 100 through all other networks.
4. If it is a new virus, try to locate a sample and send it to F-Secure Security Labs through the sample submission webform at: <http://www.f-secure.com/samples>. Provide as much information about the problem as possible. It is important to know how many computers are affected with the virus.
5. If a computer is infected with malware that spreads in the local network, it is recommended to take down the network until all infected computers are disinfected. The network can be taken into use only after all computers are cleaned because a single infected machine can re-infect the whole network within minutes.
6. Wait for a report from the F-Secure Security Labs, and follow the provided disinfection instructions carefully. It is advised to backup any important data from the infected computer before disinfecting it. This backup should not be taken using the network; use external backup devices instead. Back up only data files, not executable files. If there is a need to restore the backup later, all restored files should be checked for infection.
7. When provided with a disinfection solution, test it on one computer first. If it works, it can be applied to all infected computers. Scan the cleaned computers with PC Protection and the latest virus definitions updates to ensure that no infected files are left.
8. Re-enable the network only after every single infected computer is cleaned. If the malware contained backdoors or data stealing capabilities, it is strongly recommended to change passwords and logins for all network resources.
9. Inform the employees about the outbreak and warn them against running unknown attachments and visiting suspicious Internet sites. Check the security settings of installed software

on workstations. Make sure that e-mail scanners and firewalls function correctly on servers. PC Protection should receive updates automatically, however it is recommended to periodically check that these automatic updates are working correctly.

10. Warn your partners about the outbreak and recommend them to scan their computers with PC Protection and the latest virus definitions updates to make sure that an infection did not leave your network.

If you do not find answers to your questions here, please contact the Vodafone support desk at 1200 through the Vodafone network or via +31(0) +31 654 500 100 (all other networks).

4.1 Troubleshooting connection problems

If there are connection problems, for example a host cannot access the Internet, and you suspect that the PC Protection client software might cause these problems, you can use the steps given here as a check list.

1. Check that the computer is properly connected.
2. Check that the problem is not in the network cable.
3. Check that ethernet is up and working properly.
4. Check that the DHCP address is valid.

You can do this by giving the command 'ipconfig' in the command prompt.

5. Next you should ping the default gateway.

If you do not know the address, you can find it out by issuing the command 'ipconfig -all' in the command prompt. Then ping the default gateway to see if it responds.

6. If normal Internet browsing does not work, you can try to ping a DNS server:

- Run 'nslookup' to make sure that the DNS service is running.
- You can also try to ping a known web address to make sure that the computer at the other end is not down.

If nothing else helps, it is likely that the problem is in routing or in some other component in the computer the user is trying to connect to.