

Vodafone PC Protection Pro

IT admin guide

power to you



vodafone

Index

1.	Introduction	3
1.1	Welcome to PC Protection Pro	3
1.2	Features	3
2.	Getting started.....	5
2.1	Orientation of the management portal.....	5
2.2	Recovering your password	6
3.	Workstation security software installation	7
3.1	System requirements	7
3.2	Downloading the Workstation software.....	9
3.3	Uninstalling / removing previously installed antivirus programs.....	10
3.4	Workstation local installation	11
3.5	Workstation remote installation.....	12
4.	Server Protection software installation	13
4.1	System requirements	13
4.2	Server Protection installation	13
5.	Mail server Protection installation	15
5.1	System and installation requirements.....	15
5.2	Mail server Protection installation.....	16
6.	Virus and spyware protection.....	18
6.1	Quarantined objects	19
7.	Management portal system status	21
7.1	Is my network protected?	21
7.2	Checking the status of a group of computers.....	21
7.3	Checking the status of computers.....	22
7.4	Checking the status of a workstation.....	23
7.5	Keeping computers in the network safe	23
7.6	Managing the product settings locally	24
7.7	Assigning operations.....	25
7.8	Changing the portal language.....	25
8.	Frequently asked questions	26
8.1	Troubleshooting connection problems.....	28

1. Introduction

1.1 Welcome to PC Protection Pro

PC Protection Pro protects desktop PCs, laptops, and file servers as well as Microsoft Exchange servers. 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.

You can manage all security information with an easy-to-use, web-based management portal. It gives you an overview of the security status of your company network. You can also easily set and monitor the security settings of your company's desktop PCs, laptops and servers. The automated features make sure that your operations work 24/7 with minimum intervention and IT resource use.

1.2 Features

Two service components together offering a complete solution:

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

Management Portal

Using the online portal, you can manage your system's security settings, view the status and create reports anywhere, anytime. The PC Protection Management Portal is a web-based software provisioning and security management system for SMB's.

It allows continuous follow-up of the computer network security, and enables administrators to take required action to help SMB end users when security problems are detected. Through the portal, it is possible to monitor both the overall network security and the security status of individual PCs in the network.

- Online management – can be accessed anywhere, at any time
- At-a-glance security status check every time you log in the security portal
- Real-time visibility of the security of employees working at the office or remotely
- Easy-to-understand reports
- Intuitive built-in troubleshooting guide

The portal allows small business customer administrators to view trend reports on:

- The overall protection status on a given period
- The number of scanned and blocked viruses and potentially malicious network connections
- The status of updates

File server and e-mail server security

Antivirus (including automatic virus definition updates), antispymware, system control, malware detection, local setting of security features (if allowed in the portal).

Anti-Virus and Spam Control for Microsoft Exchange (including automatic updates). The Exchange components are managed with a local web-based management interface.

2. Getting started

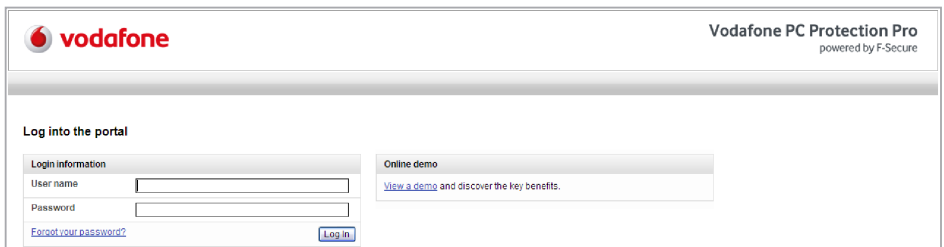
This chapter explains how to get started with PC Protection Pro from Vodafone. In this chapter, you find instructions how to download and install the PC Protection software.

2.1 Orientation of the management portal

During the activation of the PC Protection Pro service through one of the Vodafone channels, you are requested to indicate a valid e-mail address in order to send you a confirmation mail of purchase. In this mail you will find three elements that are needed to use the portal:

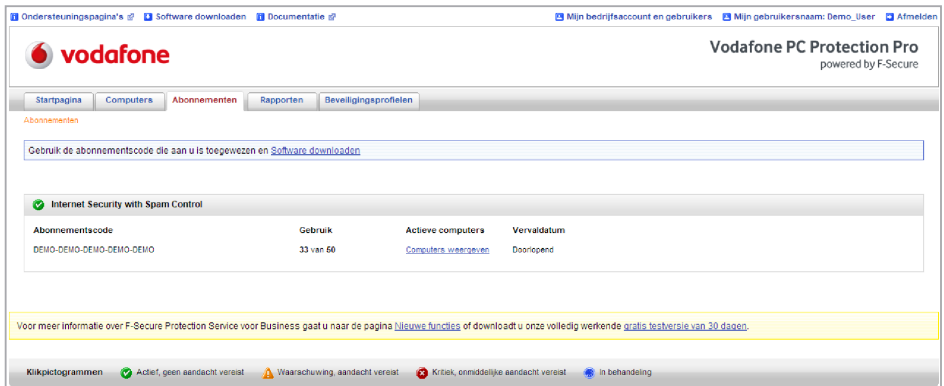
- Link to the PC Protection management portal

<https://vodafone-nl-portal.sp.f-secure.com/spe/session/login.action>



- Username for login. This username is identical to the e-mail address you provided for activating the PC Protection Service unto your account
- A password for login. For security reasons you are requested to change this password at first login. In case you loose or forget your password, use the guidelines in the next chapter to retrieve it by e-mail

When you are logged on with your personal access credentials, you will see a main task bar where you can review your subscriptions and manage your users. Click on 'Subscriptions' to see the bundle that is applicable to your account.



The size of the bundle is displayed under "Usage". More details about the status and management functions of the PC Protection portal are described under chapter 7.

2.2 Recovering your password

If you have forgotten your password, you can recover it through the 'Forgot your password' link.

To recover your password:

1. On the log-in page of the management portal, click 'Forgot your password?' link.
2. Enter your username, and click 'submit'.

The link to the management portal can be found via www.vodafone.nl/mccsupport and click on PC Protection Pro

3. 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.

3.1 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 |
| Processor: | Microsoft Windows 7 (32-bit and 64-bit). All editions
For Microsoft Windows XP and Windows 2000 (32-bit): <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

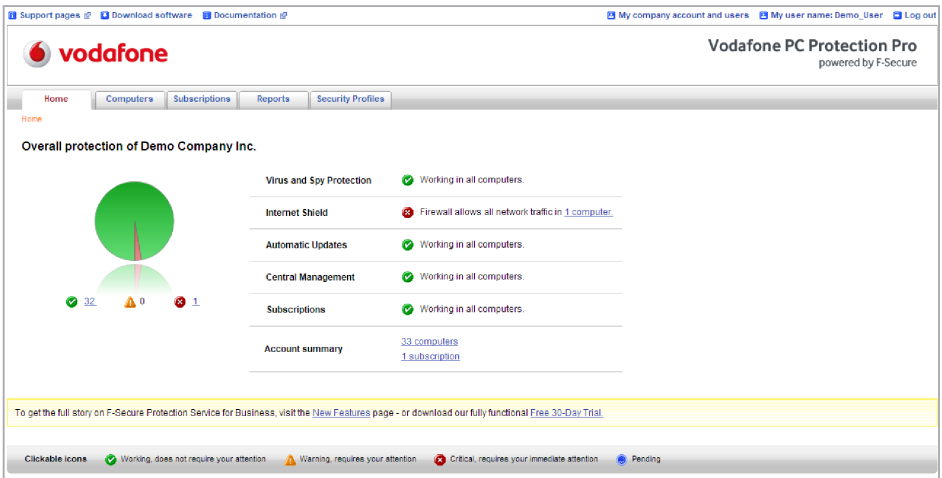
The following are the recommended requirements for installing and using the product:

- 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

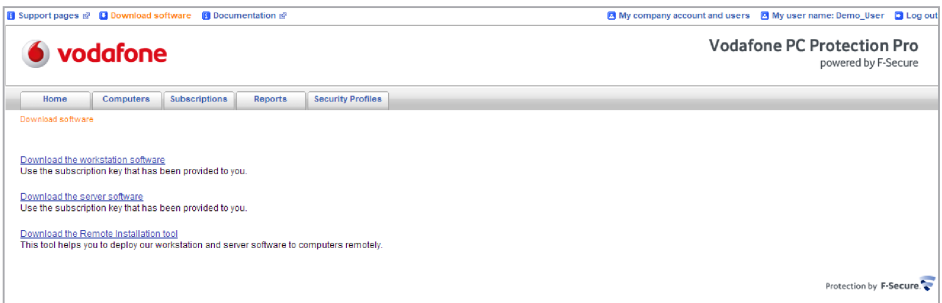
3.2 Downloading the Workstation software

You can download the PC Protection software through the management portal. To download the software:

1. Log in to the management portal
2. Enter the username and password, which you received upon the creation of your account with Vodafone. The protection status page opens.



3. Click the 'Download software' link at the top of the page. The Download software page opens.



4. In the Download software page, click the 'Download the workstation software' or the 'Download the server software' link.

3.3 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.

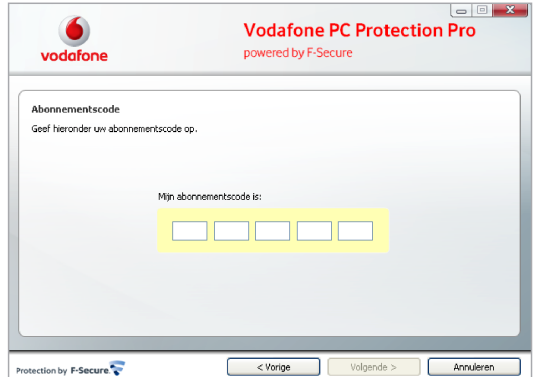
To uninstall other antivirus programs:

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.

3.4 Workstation local installation

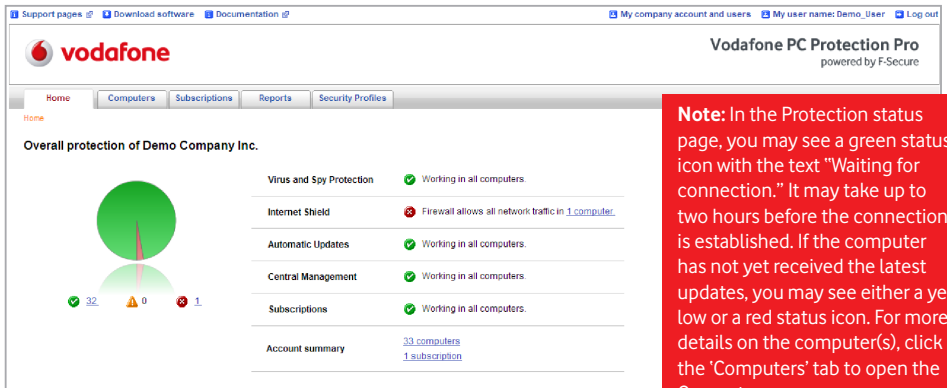
To install the program:

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'.

After the installation, log into the Portal to verify that the computer shows in the Portal.



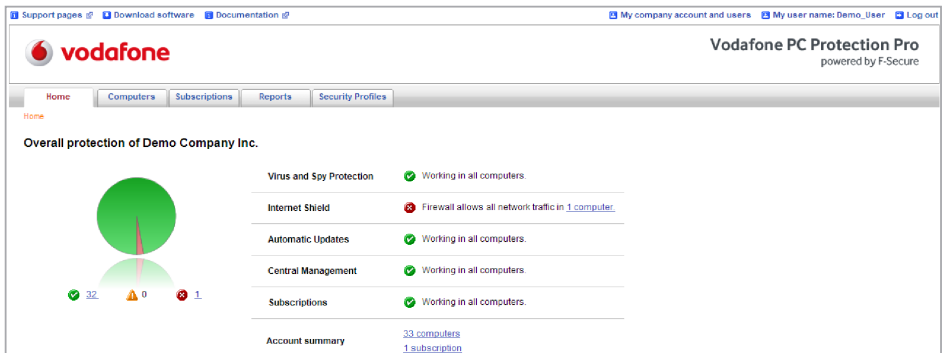
3.5 Workstation remote installation

Before you start the remote installation, make sure that the domain controller exists and that the computers on which you want to install the software belong to a domain. To be able to remotely install the software, you must have domain administrator rights.

To install the software:

1. Log in to the PC Protection Management Portal. Enter the user name and password, which you selected when you created your account. The Protection status page of the new account opens.
2. Click the 'Download software' link at the top of the page. The Download software page opens.
3. In the Download software page, click the 'Download the Remote Installation Tool' link. If you have not downloaded the workstation software yet, click also the 'Download the workstation software' link.
4. Extract the Remote Installation Tool zip file on a local drive.
5. Double-click the ritool.bat file. The Remote Installation Tool window opens.
6. In the Software to Install page, click **...**. The Software Installer Selection window opens.
7. Locate the downloaded workstation software file and click 'OK'.
8. Click 'Next'.
9. In the Target Computers page, do the following:
 - Under Domain Name, select the domain to which the computers belong.
 - Under Computer Name, select the computers on which you want to remote install the software.
10. Click 'Next'.
11. In the Account page, do the following:
 - a. Select 'Another account'.
 - b. Enter the domain administrator name and password.
 - c. Confirm the password.
12. Click 'Next'.
13. Click 'Install'. The workstation software is being installed on the selected computers.

In the PC Protection Management Portal, verify that the computer shows in the portal.



4. Server Protection software installation

This section describes the system requirements for installing and using the Server Protection product, and gives you step-by-step instructions on how to install the product.

4.1 System requirements

Read the following before starting to install and use the Server Protection software.

Your computer must meet the following requirements for installing and using the product:

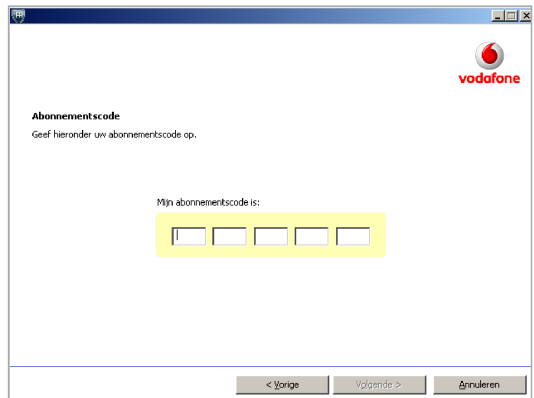
- Operating System:** Windows Server 2000 (32-bit), Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit).
- Processor:** Intel Pentium 4 2GHz or higher
- Memory:** 1 GB of RAM
- Disk space to install:** 260 MB free hard disk space
- Disk space for processing:** 10 GB or more free hard disk space
- Internet Connection:** An Internet connection is required to validate your subscription and receive updates.

4.2 Server Protection installation

Install the software on a computer and after the installation verify that the computer shows in the portal.

To install the software:

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, click 'Finish'.

5. Mail server Protection installation

This section describes the system requirements for installing and using the product, and gives you step-by-step instructions on how to install the product.

5.1 System and installation requirements

Read the following before installing Mail server Protection.

Your computer must meet the following requirements for installing and using the product:

Operating System:	Windows Small Business Server 2003 (32-bit)
Microsoft Exchange Server:	Microsoft Exchange Server 2003 with the latest service pack
Processor:	Intel Pentium 4 2GHz or higher
Memory:	1 GB of RAM
Disk space to install:	260 MB free hard disk space
Disk space for processing:	10 GB or more free hard disk space
	Note: The required disk space depends on the number of mailboxes, amount of data traffic, and the size of the Information Store.
SQL server (for quarantine database):	Microsoft SQL Server 2005 (Enterprise, Standard, Workgroup or Express edition) - recommended Microsoft SQL Server 2000 (Enterprise, Standard or Workgroup edition) with Service Pack 4 Microsoft SQL Server 2000 Desktop Engine (MSDE) with Service Pack 4
	Note: You must install a Microsoft SQL Server or Microsoft SQL Server Desktop Engine (MSDE) with Mixed Mode authentication before you install the Mail server Protection software. To install Microsoft SQL Server 2005, refer to http://www.microsoft.com/SqlServer/2005/en/us/default.aspx .
Internet Connection:	An Internet connection is required to validate your subscription and receive updates.

5.2 Mail server Protection installation

Before you install the Mail server Protection software, you must install Microsoft SQL Server.

Before installing the Mail server Protection software, make sure that you know the following:

- The password for the 'SA' account on the Microsoft SQL Server, and
- The correct instance name that will be used for the quarantine, if you have multiple instances of Microsoft SQL Server installed on the same server.

Install the software on a computer and after the installation verify that the databases have been updated.

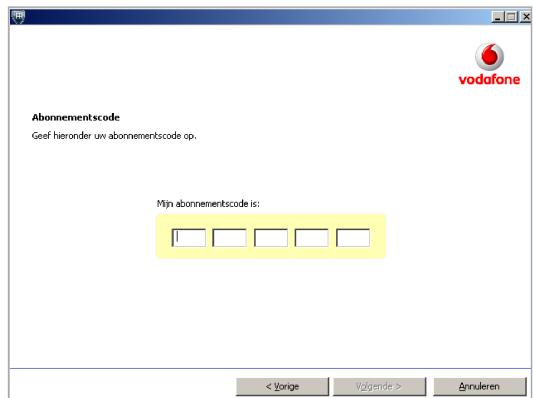
You must install a Microsoft SQL Server or Microsoft SQL Server Desktop Engine (MSDE) with Mixed Mode authentication before you install the Mail server Protection software.

To install Microsoft SQL Server 2005, refer to

<http://www.microsoft.com/Sqlserver/2005/en/us/default.aspx>

To install the software:

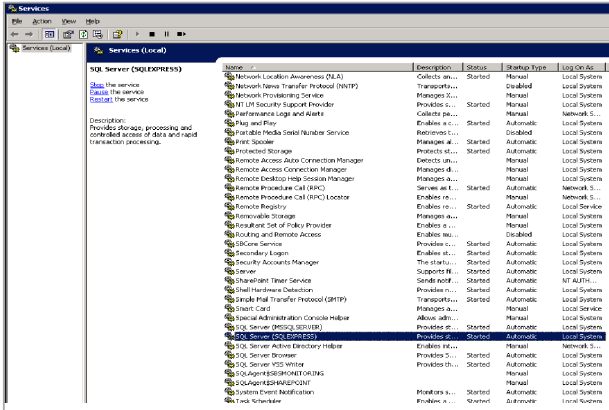
1. Locate the downloaded file and double-click the .exe file to start the installation.
2. Select the installation language, and click 'Next' to continue. If you are installing Mail server Protection, select English as the installation language.
3. Read the license agreement. To accept the agreement 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.

A screenshot of a web-based installation window. The window has a blue title bar and a white background. In the top right corner, there is a Vodafone logo. The main content area contains the text 'Abonnementcode' followed by 'Geef hieronder uw abonnementscode op.' Below this, there is a label 'Mijn abonnementscode is:' and a yellow rectangular input field containing five empty boxes for digits. At the bottom of the window, there are three buttons: '< Vorige', 'Volgende >', and 'Annuleren'.

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. In the SQL Server details page, enter the name of a local or remote SQL server instance.

Note: To find your HOSTNAME, type `ipconfig /all` at a command prompt. The server name is displayed in the command prompt window as "Host Name". You can also use an IP address or Fully Qualified Domain Name instead of hostname.

Note: To find your INSTANCE, click Start ► All Programs ► Administrative Tools ► Services. Then find the **SQL Server (INSTANCENAME)** service. The instance name is displayed in brackets. If you find multiple instance names, select the one that you want to use.



7. Enter your SA user password.

Note: If you are not sure that you remember your correct SA password, or if the installation fails because of an SQL server error, refer to the Troubleshooting section.

8. Click 'Next'.

9. When the installation is complete, click 'Finish'.

10. After the installation, open the PC Protection Management Portal and check that the databases have been updated:

- Select "Programs" ► "Vodafone Mail server Protection".
- In the "Automatic Update" Agent tab, in the Summary page, check that the last check result shows that there is nothing new available.
- Under "Summary", click 'Downloads' and check that the Available Packages list shows at least one update with a recent date on it.

11. In the Home tab, check that each component has a green status icon.

12. Next, configure Vodafone Mail server Protection.

Mail server Protection configuration

Please, refer to the [F-Secure Anti-Virus for Microsoft Exchange documentation](#) for detailed configuration descriptions.

6. 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.

6.1 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'.

7. Management portal system status

The portal shows you the security status of the computers in your network and points to any security problems that you should fix.

7.1 Is my network protected?

The Home page shows you the overall protection status of your network.

On the Home page, the pie chart shows the proportions of the network computers that are protected, or that have either minor or critical problems.

Note: The portal shows information only about the computers that are registered to the portal. If you have computers that are not registered to the portal, they may be a security risk.

The list on the right shows network information by each security component. If you only see green icons, all computers are protected. You can also see the overall number of the accounts and computers in your network.

The best way to monitor whether there are viruses on the network is to check the “Virus protection” section of the “Summary” tab. If it displays new infections, you can access more detailed information by clicking ‘View hosts’ infection status....’ It takes you to the “Status” tab and “Virus protection” page, where you can see details of each host’s infection status.

You can also check the “Alerts” and “Reports” tabs to see the scanning reports from different hosts.

7.2 Checking the status of a group of computers

You can check the status of computers that belong to the same group, that have the same subscription key or that share the same problem.

Viewing computers that have the same problem

You can view all the computers that have the same problem.

To view the computers:

1. On the “Home” tab, click one of the links that show the number of computers with a specific problem. For example, ‘virus definitions are very old in 3 computers’.
The Computers page opens.
2. You can view the computers that have the same problem.

Viewing computers that belong to the same group

You can view all the computers that belong to the same group.

To view the computers:

1. On the "Home" tab, click the 'Computers' tab. The Computers page opens.
2. Click the 'Central Management' tab.
3. In the "Central Management" view, do one of the following:
 - Click the 'Group' column title to sort the computers by their group name.
 - Enter the name of a group in the "Search" box at the top right corner of the computer list, and click 'Search'. The number of computers belonging to the group is shown. Click the link to view all the computers in the group.

View computers with the same subscription key

You can view all computers with the same subscription key.

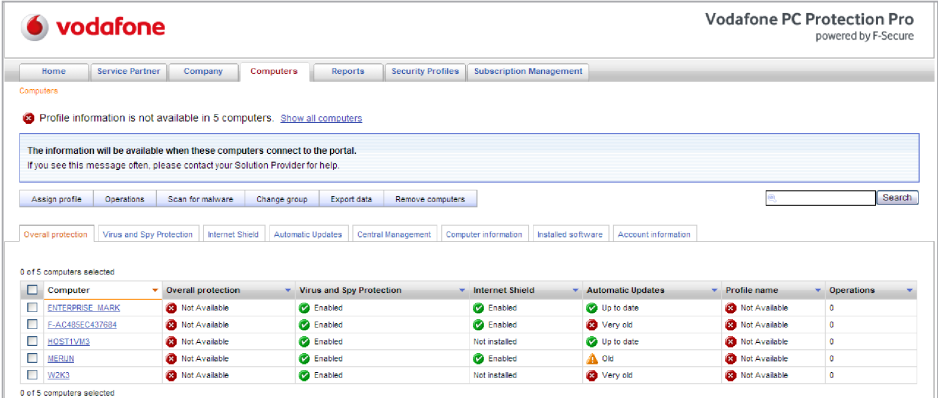
To view computers:

1. On the "Home" tab, click the 'Computers' tab. The Computers page opens.
2. Click the 'Installed software' tab.
3. In the "Installed software" view, click the 'Subscription' key column title to sort the computers by their subscription key. You can view the computers with the same subscription key also by first selecting the company the subscriptions of which you want to see. Then, click the 'View subscriptions for this account' link to see all the subscription keys of that company. On a Subscription key line, under "Active computers", click the 'Show computers' link to see all the computers with the same subscription key.

7.3 Checking the status of computers

On the Computers page, you can check the overall protection status of computers.

The Computers page shows you detailed information about the computers that are registered to the F-Secure PSB Portal.



The screenshot shows the Vodafone PC Protection Pro interface. At the top, there is a navigation bar with tabs: Home, Service Partner, Company, Computers (selected), Reports, Security Profiles, and Subscription Management. Below the navigation bar, there is a message: "Profile information is not available in 5 computers. [Show all computers](#)". A warning box states: "The information will be available when these computers connect to the portal. If you see this message often, please contact your Solution Provider for help." Below the warning box, there are buttons: Assign profile, Operations, Scan for malware, Change group, Export data, and Remove computers. A search box is also present. Below the buttons, there is a sub-navigation bar with tabs: Overall protection (selected), Virus and Spy Protection, Internet Shield, Automatic Updates, Central Management, Computer information, Installed software, and Account information. The main content area shows a table with 5 computers selected. The table has columns: Computer, Overall protection, Virus and Spy Protection, Internet Shield, Automatic Updates, Profile name, and Operations. The data rows are as follows:

Computer	Overall protection	Virus and Spy Protection	Internet Shield	Automatic Updates	Profile name	Operations
ENTERPRISE_MABK	Not Available	Enabled	Enabled	Up to date	Not Available	0
FAC483EC437834	Not Available	Enabled	Enabled	Very old	Not Available	0
HOST1V1Q3	Not Available	Enabled	Not installed	Up to date	Not Available	0
ME3UBJ	Not Available	Enabled	Enabled	Old	Not Available	0
W2K3	Not Available	Enabled	Not installed	Very old	Not Available	0

By clicking the different tabs, you can view the following:

- The protection status of computers by a security component;
- Computer information, such as DNS names and IP addresses;
- Information about software installed on the computers;
- And account information, including information about the company, Solution Provider and Service Partner associated with a computer.

The Computers page may show different computers depending on how you opened the page.

The Computers page may show:

- All the computers in the network that are registered to the portal;
- All the computers that have the same problem;
- All the computers that have the same subscription key.

Note: If there are more computers that can fit on one page, click 'Next' to see the rest of the computers.

7.4 Checking the status of a workstation

You can view detailed status information of a workstation on the Computers page.

The Computer page shows a list of all computers in your network. To view detailed information about a workstation, under Computers, click the name of the workstation. The information includes:

- Recently assigned operations
- Recent alerts
- Overall protection status of each security component
- Protection status of each feature in a security component
- Computer information, including the WINS- and DNS-name, IP address, and operating system
- Software installed on the workstation, including the product name, subscription key, version, and security components
- Account information, including information about the company, Service Partner, and Solution Provider associated with the account

7.5 Keeping computers in the network safe

You keep all the computers in the network safe.

To keep the computers in the network safe, do the following:

1. Make sure all your computers are registered to the portal.
2. Check whether any of the computers that are registered to the portal have security problems. Some of these problems you can fix directly from the portal; some of these problems you may have to fix locally.

7.6 Managing the product settings locally

This section explains how you can locally manage the product settings.

The “Home” tab shows you a quick overview of your security components and the status of the installed security components. The upper part of the “Home” tab shows the security status of your computer. For example, when the status is shown as Protected, your computer’s protection is up to date.

The security levels of the different security components, for example Normal or High, are shown next to the name of the component. The lower part of the “Home” tab shows the date and time of last update check.

By clicking the tabs on the left, you can see the details of all the security components (Virus&Spy Protection, Internet Shield, Spam Control, and Automatic Updates). The icons show you the status of the program and its security components. If you change program settings, also the icons change.

The icons and their meanings



A critical security component, for example Virus & Spy Protection, is working properly



One of the security components is not in use, but your computer is still protected.



A security component or one of its features is disabled, and your computer is not protected. The icon will change back to green when you enable the component again.



Your service subscription has expired.



An error state in the software.

7.7 Assigning operations

You can also assign operations to a remote computer from the portal, for example, enable the firewall or real-time virus scanning on a remote computer.

To assign an operation:

1. Select computers from the list by selecting the appropriate checkboxes.
2. Click 'Operations'. A list of operations appears.
3. Select one of the following operations from the list:

Select...	To...
Send full status update	force the remote computer to send a full report of it's status to the portal.
Enable Real-time Virus Scan	find and block viruses on the remote computer before they can cause harm.
Enable Real-time Spyware Scan	find and block spyware on the remote computer before they can cause harm.
Set the Virus and Spy Protection level to Normal	select the most commonly applicable level of protection from viruses and spyware for the remote computer.
Enable Application Control	let the user decide which applications are allowed to access the Internet on the remote computer.
Set the Internet Shield security level to Office	select the most commonly applicable level of protection from unsafe traffic on the remote computer.

4. Click 'Assign Operation' to assign the operation to the remote computer.

The operation is applied to the computer the next time the computers checks for updates with the portal.

7.8 Changing the portal language

The language of the management portal can be adjusted by modifying the user information. Click on "My user name: xxx" and select your preferred language. The portal will appear in the selected language once you submit the change.

8. Frequently asked questions

This chapter answers the most frequently asked questions.

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 through all other networks.

How can I change the language in the Vodafone PC Protection Management Portal?

To change the language, you will have to log in to the PC Protection Portal first. Then click your user name at the top right corner. In the "Edit" account page, from the Language drop-down list, select the language that you want, and click 'Submit'.

I installed the Server Protection Pro software on my computer, but I cannot see my computer in the Management PSB Portal. What should I do?

If you do not see your computer in the PC Protection Portal, click the 'Check now' button on your PC Protection client interface. If you still do not see your computer in the portal, check that the subscription key has been added to the portal.

I want to download the software for Mail server Protection, but I cannot find it in the Download software section in the PC Protection Portal?

You can download software for all server products from the "Download the server software" link.

Can I get reports out from the PC Protection Portal?

You can export information about your network computers on the "Export data" tab (under the "Computers" tab). On the "Reports" tab, you can only view information about your network computers, such as overall protection status and status by each security component.

During the installation of the PC Server Protection software, I am asked for information about SQL. Why?

You may have entered a wrong type of subscription key. For example, you are installing the Server Protection software and your subscription key is for the Mail server Protection software. You can check the type of your subscription key on the Subscriptions tab in the PC Protection Management Portal.

I need to find the Microsoft Exchange parameters in the PC Protection Portal. Where can I find them?

You cannot find them in the PC Protection Portal. You can find the Microsoft Exchange parameters through local web user interface.

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.

8.1 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.