FAQ

F-Secure Internet Security 2013

Contents ....

Before installation

How can I check which version of the Windows operating system I have?

You can check the operating system version in Windows system properties.

To check your system properties in Microsoft Windows:

1. Click **Start**.
2. Click **Control Panel**.
3. Do one of the following:
    - In Windows 7:
        1. Select **System and Security**.
        2. Click **System**.
    - In Windows Vista:
        1. Select the **System and Maintenance** category.
           Note: This step may not be necessary in all computers.
        2. Click **System**. The System Properties window opens.
    - In Windows XP:
        1. Select the **Performance and Maintenance** category.
           Note: This step may not be necessary in all computers.
        2. Double-click **System**. The System Properties window opens.
           Note: To find out whether your computer is running a 32-bit or a 64-bit version of Windows XP, click here.

You can view the properties of your computer, such as operating system version, processor information, and the amount of memory (RAM).

Determining whether your computer is running a 32-bit or a 64-bit version of Windows XP

There are several ways to determine whether your computer is running a 32-bit or a 64-bit version of Windows XP.

1. If you have a Windows keyboard, press the **Windows** key + **Pause/Break** to display the System Properties dialog box. If the system information mentions nothing about a 32-bit or a 64-bit version, the system is running a 32-bit version of Windows XP.
2. Open My Computer to check system properties:
    a. Click **Start**.
    b. Right-click **My Computer** and select **Properties**. The **System Properties** window opens.
    c. On the **General** tab, check the first line under **Computer**:
        - In 64-bit versions of XP, **Itanium** or **Itanium 2** is shown.
        - In 32-bit XP, some other value is shown.

3. Open the Winmsd.exe tool to check the system type or processor:
    a. Select **Start > Run**.
    b. Type winmsd.exe in the **Open** field, and click **OK**.
    c. Do either of the following:
        ▪ Locate **System Type** in the right pane under **Item**. Check the value:
            ▪ In 64-bit XP, the value is Itanium-based system.
            ▪ In 32-bit XP, the value is X86-based PC.
        ▪ Locate **Processor** in the right pane under **Item**. Check the value:
            ▪ In 64-bit XP, the value starts with ia64.
            ▪ In 32-bit XP, the value starts with x86.
4. Use the Diagnostic Utility tool to check the version:
    a. Select **Start > Run**.
    b. Type dxdiag in the **Open** field, and click **OK**.
    Note: If a Windows dialog box is shown, asking you to verify your drivers, you can safely click **No** and continue. The DirectX Diagnostic Tool dialog box opens. Allow the program to finish loading.
    c. Locate **Operating System** in System Information: In 64-bit XP, the value is, for example, Microsoft Windows XP 64-bit Edition.
    d. Locate **Processor** in System Information: In 64-bit XP, the value is either **Itanium** or **Itanium2**.

How can I check if my computer meets the system requirements for the product?

Your computer must meet the requirements listed below.

Supported operating systems:

- Windows 8 (32-bit and 64-bit): all editions.
- Windows 7 (32-bit and 64-bit): all editions.
- Windows Vista (32-bit and 64-bit): all editions, Service Pack 2 or later.
- Windows XP (32-bit): Home, Professional, Service Pack 3 or later.

Recommended requirements for Microsoft Windows 8, 7 and Vista:

- Processor: Intel Pentium 4 2 GHz or higher.
- Memory: 1 GB or more.
- Disk space: 800 MB of free hard disk space (500 MB for Anti-Virus only).
- Display: 16-bit or more (65000 colors).
- Internet connection: an Internet connection is required to validate your subscription and receive updates.

Recommended requirements for Microsoft Windows XP:

- Processor: Intel Pentium III 1GHz or higher.
- Memory: 512 MB or more.
- Operating system: Microsoft Windows XP, Service Pack 3.
- Disk space: 800 MB of free hard disk space (500 MB for Anti-Virus only).
- Display: 16-bit or more (65000 colors).
- Internet connection: an Internet connection is required to validate your subscription and receive updates.

Supported web browsers:

- Internet Explorer 7 & 8 (Windows XP) and Internet Explorer 8 & 9 (Windows Vista & Windows 7, 32-bit and 64-bit), Internet Explorer 10 (Windows 8, 32-bit and 64-bit)
- Mozilla Firefox, two latest major versions
- Google Chrome, two latest major versions

How do I remove conflicting security products manually?

We recommend that you have just one good security product on your computer. The security product needs to open files to scan them. If another security product is trying to open the same files at the same time, it has to wait for the files to become free. This often causes problems. For example, programs may not start correctly or the whole system may crash.

The security product detects and removes security and firewall products of **the largest security software vendors** automatically during installation. However, it is possible that for some reason the removal fails. In this case, you need to remove any other security or firewall product manually. You can do this also before starting the installation.

Removing security products manually

If you know the name of the security product, you can try and uninstall it in the following way:

1. Click **Start ‣ Control Panel**.
2. Double-click **Add or Remove Programs**.
3. If you can find the product in the list of currently installed programs, remove (uninstall) it.

If the product cannot be uninstalled, contact the vendor of the software for support and possibly ask for a removal tool.

Below you can find vendor-specific uninstallation instructions for some of the security products currently on the market:

- [Uninstall AVG 6](#)
- [Uninstall PC-cillin](#)

- [Uninstall Ad-Aware](#)
- [Uninstall McAfee](#)
- [Uninstall Norton](#)

To uninstall AVG 6:

1. Click **Start > Run**.
2. In the **Open** box, type 'C:\Program Files\Grisoft\AVG6\Setup.exe /uninstall' and click **OK**.
3. If you are asked whether you want to run the Virus Vault, click **No**.
4. If you are asked whether you wish to continue with the uninstallation, click **Yes**.
5. Select **Restart the Computer** and click **OK**.

To uninstall PC-cillin:

Uninstall a Trend Micro product by using the [Trend Micro Diagnostic Toolkit](#).

To uninstall Ad-Aware:

1. Click **My Computer**.
2. Go to C:\Program Files\Lavasoft\Ad-Aware.
3. Run the unregaaw.exe file.
4. Delete the entire Ad-Aware folder.
5. Remove the Lavasoft Ad-Aware link from your **Start** menu and the Ad-Aware icon(s) from your desktop (if present).
6. Go to C:\Documents and Settings\[User Name]\Application Data\Lavasoft\
7. Delete the entire Lavasoft folder.
8. Empty the Recycle Bin.
9. Restart your computer.

To uninstall McAfee:

Uninstall a McAfee consumer product by using the McAfee Consumer Products Removal Tool (MCPR.exe). Search for the tool in the Internet by using keywords "McAfee Consumer Products Removal tool (MCPR.exe)".

To uninstall Norton:

Uninstall a Norton security product by using [Nortol Removal Tool](#).

More information

If, however, your computer does still not start correctly after installing the F-Secure product, do the following:

1. Start your computer in safe mode. For instructions, see article 2110 – Computer stops working after installation.
2. Remove the F-Secure product.
3. Restart your computer.
4. Create an FSDiag file. For instructions, see Creating an FSDiag file.
5. Send the FSDiag file to F-Secure support by submitting a support request.

Installation

Why is F-Secure using a network installer for downloading and installing the product?

F-Secure uses the small network installer for the following reasons:

- Thanks to the small size of the network installer, the initial download is quicker than ever. The network installer takes over the downloading of additional components, thus making the installation also more reliable.
- The installation of the products is now also faster because only the required product components will be downloaded and installed.
- The latest version is always installed. This means that the user doesn't need to upgrade the product after installation.

How do I install the product?

Before you can start installing the security product, you need:

- the product CD **or** a downloaded version of the product (http://www.f-secure.com/en/web/home_global/support/installers)
- a valid subscription key for the product
- to be connected to the Internet.

If more than one person uses the computer and you have created user accounts for everyone, you have to log on as a user with administrator rights before starting the installation.

Note: The product cannot be installed on a computer that uses other antivirus or firewall products.

The product detects and removes security and firewall software of the largest security software vendors automatically during installation. However, it is possible that for some reason the removal fails. In this case, you need to remove any other security or firewall software manually. For more information, see article 6752 - Removing other vendors' security software.

Installing the security product

To install the product:

1. Do one of the following:
    a. If you purchased the product online, you have received an e-mail message which contains the download link and your unique subscription key for the product. Once you have downloaded the installation package, double-click the installer (.exe) file to start the installation.
    b. If you want to install the product from CD, the installation should start automatically once you insert the CD. If it doesn't start, browse to the root folder of the CD and double-click the autorun.exe or installer (.exe) file to start the installation. Your unique subscription key can be found inside the product box.

    The Welcome to My F-Secure setup window is displayed:
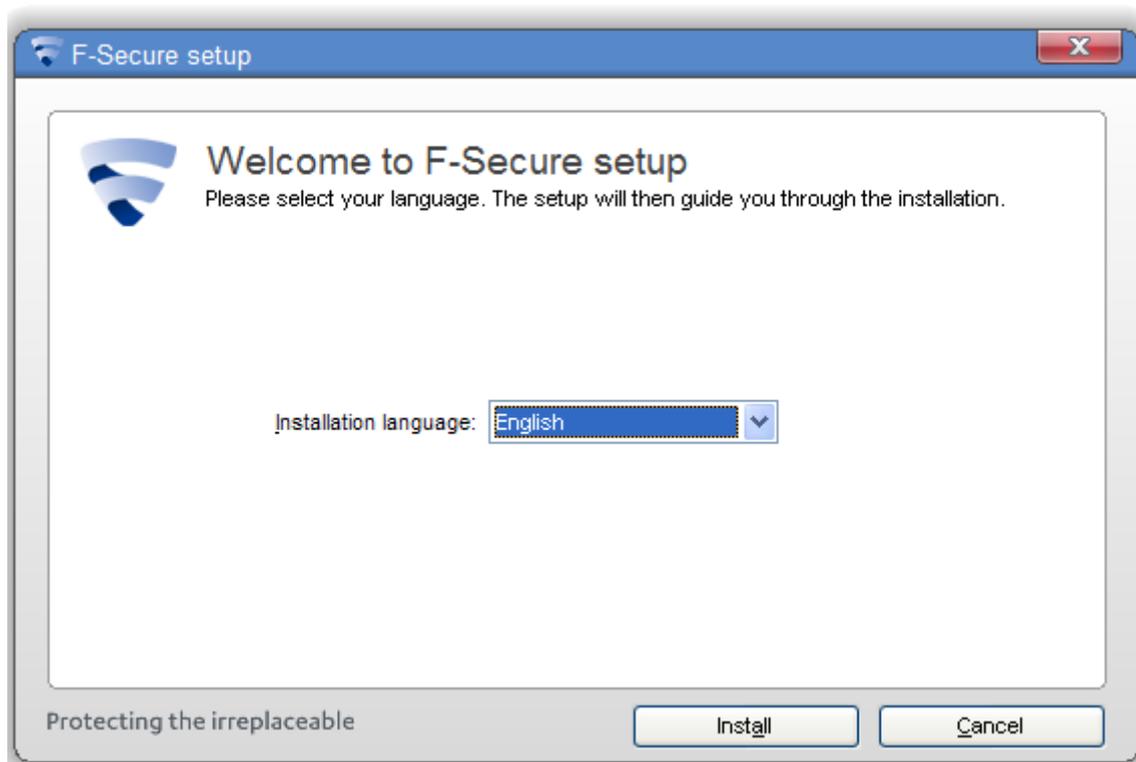
2. Select your language and click Install. The License terms window is displayed:
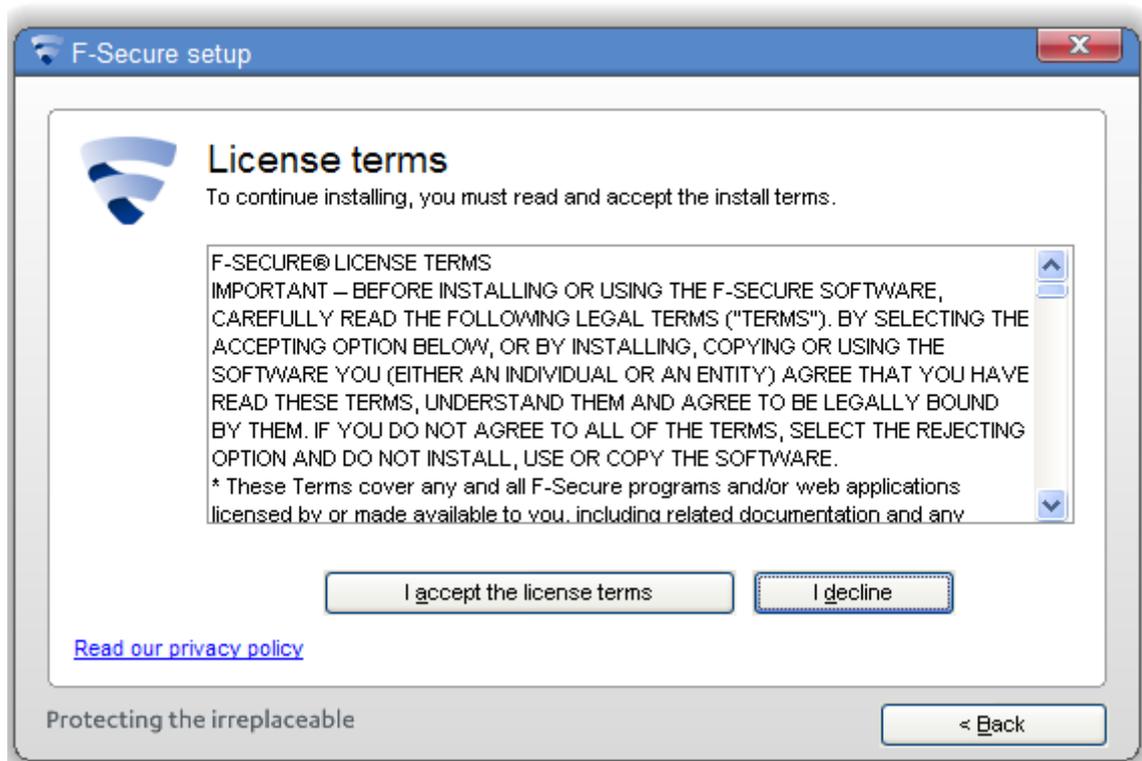
3. Read the license terms. If you accept them, click the **I accept the license terms** button.
4. Once you have accepted the license terms, the downloading of files starts. This phase may take a few minutes. Once the downloading of files is completed, the Automatic installation window is displayed:
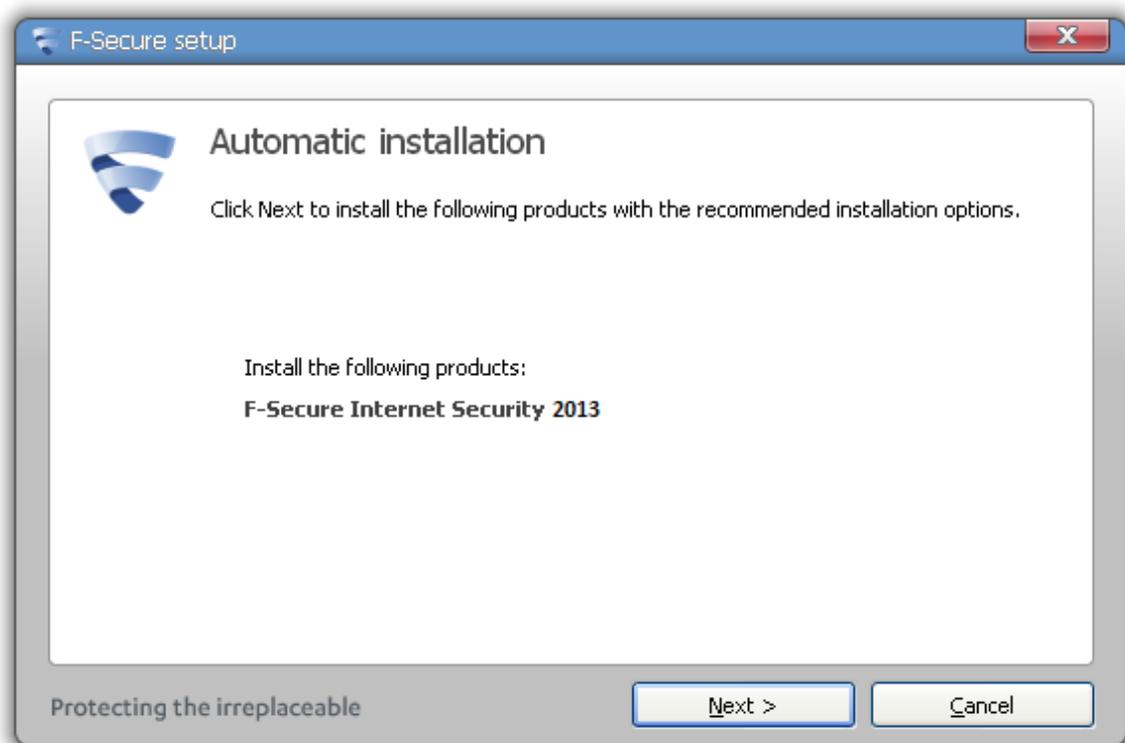
5. Click **Next** to continue the installation. The Real-time Protection Network window is displayed:

6. If you want to contribute anonymized data for analysis to improve the product's detection rate, click **Next**. If you decide not to do so, clear the selection before clicking **Next**. The installation continues with the removal of conflicting software, installing of computer security and online safety.

Installation of the product is now completed.

Note: If your computer is running on Windows XP, you need to restart it to complete the installation.

To open the product user interface, click the F-Secure icon in the lower-right corner of your screen. The launch pad is displayed:

The launch pad contains all your applications. To open any of the applications available, click the application icon on the launch pad. You can also change common settings and manage your subscriptions through the launch pad; just right-click the right-most icon on the launch pad and select the desired option from the pop-up menu.

How do I uninstall the product?

To uninstall F-Secure Internet Security or F-Secure Anti-Virus 2013, 2012, 2011 or 2010 from Windows XP:

1. Click **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Scroll down to your F-Secure product and click **Change/Remove**.
4. When asked, restart your computer.

To uninstall F-Secure Internet Security or F-Secure Anti-Virus 2013, 2012, 2011 or 2010 from Windows Vista:

1. Click **Start > Control Panel**.
2. Click **Uninstall a program**.
3. Scroll down to your F-Secure product and click **Uninstall/Change**.
4. When asked, restart your computer.

To uninstall F-Secure Internet Security or F-Secure Anti-Virus 2013, 2012, 2011 or 2010, from Windows 7:

1. Click **Start > Control Panel**.
2. Double-click **Programs and Features**.
3. Scroll down to your F-Secure product and click **Uninstall/Change**.
4. When asked, restart your computer.

Subscription and registration

Can I install the product on top of a trial version?

When you are using a trial version of the product, you can easily upgrade to a full commercial version.

Note: If you have not yet purchased a full product version from a reseller, you can buy it online at http://www.f-secure.com//en/web/home_global/protection/. Follow the instructions on the page.

When you have the new subscription key for the product, you need to activate it.

Activate the new subscription in the following way:

1. On the launch pad, right-click the right-most icon. A pop-up menu appears.
2. Select **View my subscriptions**. The My subscriptions window is displayed.
3. Click the **Activate subscription** link to display the Activate subscription dialog.
4. Enter your new subscription key and click **OK**.

After you have entered the new subscription key, the new subscription validity date is shown on the Subscription status page.

How do I change my F-Secure Anti-Virus installation to F-Secure Internet Security?

If you have F-Secure Anti-Virus installed on your computer and would like to upgrade the product to F-Secure Internet Security, [purchase](#) first the latest version of F-Secure Internet Security and then install the new product on top of F-Secure Anti-Virus.

During the installation when you are asked for the subscription key, enter the new F-Secure Internet Security subscription key.

Where can I find the product subscription key?

Web store

If you have bought the product in a web store, the subscription key is included in the confirmation e-mail that you received after the purchase.

Retail store

If you have bought the product CD in a retail store, the subscription key is on the front cover of the Quick installation guide.

Using - Changing settings

What has happened to the firewall?

The product's firewall functionality has been redesigned. The new firewall design makes the use of the product easier than ever.

Now the product uses operating system's own Windows Firewall for basic firewall functionality, such as inbound network traffic filtering, location-specific settings and HomeGroup support. On top of this basic protection by Windows Firewall, the product has been complemented with the following security mechanisms to improve the firewall functionality:

- Blocking download of exploits and other harmful files. Each downloaded file is scanned and all harmful files are blocked automatically.
- Preventing suspicious applications from accessing the Internet. If the safety of an application cannot be verified, DeepGuard starts to monitor its behavior. Based on the behavior analysis, DeepGuard will either allow or deny the network access or it asks the user whether to permit the access or not.
- Browser manipulation detection. DeepGuard detects if malware is trying to manipulate user's browser and prevents the attempt.

How do I allow an application to access my computer through the firewall?

When the firewall is turned on, it restricts access to and from your computer. Some applications may require that you allow them through the firewall to work properly. The product uses Windows Firewall to protect your computer.

To change Windows Firewall settings:

1. Open Computer Security.
2. On the main page of Computer Security, click **Settings**.
    Note: You need administrative rights to change the settings.
3. Select **Computer Security > Firewall**.
4. Click **Change Windows Firewall settings**.
    Note: You need administrative rights to edit the settings.

For more information on Windows Firewall, refer to Microsoft Windows documentation.

How can I allow an application that DeepGuard has blocked?

Sometimes DeepGuard may block a safe application from running, even if you want to use the application and know it to be safe. This happens because the application tries to make system changes that might be potentially harmful. You may also have unintentionally blocked the application when a DeepGuard pop-up has been shown.

To allow the application that DeepGuard has blocked:

1. Open Computer Security.
2. On the main page of Computer Security, click **Tools**.
3. Click **Applications**. The Monitored applications list is shown.
4. Find the application that you want to allow.
    Note: You can click column headings to sort the list. For example, click the Permission column to sort the list into groups of allowed and denied programs.
5. Select **Allow** in the Permission column.
6. Click **Close**.

DeepGuard allows the application to make system changes again.

How do I exclude a file or folder from scanning?

Sometimes you may want to exclude a file or folder from the scan. Excluded items are not scanned unless you remove them from the excluded items list.

Note: Exclusion lists are separate for real-time and manual scanning. For example, if you exclude a file from the real-time scan, it is scanned during the manual scan unless you exclude it from the manual scan as well.

To exclude a file or folder from scanning:

1. Open Computer Security.
2. On the main page of Computer Security, click **Settings**.
3. Do one of the following:
    - Select **Computer Security** > **Virus and spyware scanning**.
    - Select **Other settings** > **Manual scanning**.
4. Click the **Exclude files from the scan** link. The Exclude from scanning dialog is displayed.
5. Depending on what you want to exclude from scanning, do one of the following:

    - To exclude a file, drive, or folder:

        1. Select the **Objects** tab
        2. Select the **Exclude objects (files, folders...)** check box.
        3. Click **Add**.
        4. Select the file, drive, or folder that you want to exclude from virus scanning.
           Note: Some drives may be removable drives, such as CD, DVD or network drives. Network drives and empty removable drives cannot be excluded.
        5. Click **OK** to close the Exclude from scanning dialog.

    - To exclude a specific file type:
        1. Select the **File Types** tab.
        2. Select the **Exclude files with these extensions** check box.
        3. Type the file extension, which identifies the type of files you want to exclude, in the field next to the **Add** button.
        4. Click **Add**.
        5. Repeat the steps 3 and 4 for any other extension you want to exclude from scanning.
        6. Click **OK** to close the Exclude from scanning dialog.

Note: Some files cannot be excluded and will always be scanned, such as executable files.

How can I exclude an application from scanning?

You cannot exclude applications directly. New applications appear on the exclusion list only if you have excluded them during scanning.

If the scanning detects an application that behaves like spyware or riskware but you know it to be safe, you can exclude it from scanning so that the product does not warn you about it anymore. However, if an application behaves like a virus or other malicious software, it cannot be excluded.

You can view the applications that you have excluded from scanning, and remove them from the excluded items list if you want to scan them in the future. To view the applications that are excluded from scanning:

1. Open Computer Security.
2. On the main page of Computer Security, click **Settings**.
3. Do one of the following:
   - Select **Computer Security** > **Virus and spyware scanning**.
   - Select **Other settings** > **Manual scanning**.
4. Click the **Exclude files from the scan** link. The Exclude from scanning dialog is displayed.
5. On the **Applications** tab, you can see the applications that you have excluded from scanning.

How can I allow all network traffic temporarily?

By turning off the firewall, you allow all network traffic.

Warning: We recommend that you keep the firewall turned on always. If you turn off the firewall, you computer is vulnerable to network attacks. If an application stops working because it cannot connect to the Internet, change the firewall settings instead of turning the firewall off.

To turn the firewall on or off:

1. Open Computer Security.
2. On the main page of Computer Security, click **Status**.
3. Click **Change settings on this page**.
   Note: You need administrative rights to turn off security features.
4. Click the corresponding slider to turn the firewall on or off.

How can I prevent applications from downloading harmful files?

You can prevent applications on your computer from downloading harmful files from the Internet.

Some web sites contain exploits and other harmful files that may harm your computer. With advanced network protection, you can prevent any application from downloading harmful files before they reach your computer.

To block any application from downloading harmful files:

1. Open Computer Security.
2. On the main page of Computer Security, click **Settings**.
   Note: You need administrative rights to change the settings.
3. Select **Computer Security > Firewall**.
4. Select **Do not allow applications to download harmful files**.
   Note: This setting is effective even if you turn off the firewall.

I don't want to see the safety ratings for web sites anymore. How can I turn them off?

You can turn off the safety ratings in your browser in two ways.

1. Open the launch pad and click **Online Safety**.
2. Click **Users** and select the user whose Online Safety features you want to edit.
3. Click the Browsing protection **Settings** link. The Browsing protection settings window is displayed.
4. Clear the check boxes under **Show ratings** and click **OK**.

Using - Scanning

How can I clean Recycle Bin from malware?

The F-Secure product may detect infected files inside the Recycle Bin folders. These folders are used to store files that the user has deleted. You can usually find the folders here:

- C:\RECYCLED
- C:\RECYCLER
- C:\$RECYCLE.BIN\

To remove the infected files inside these folders, you need to empty Recycle Bin.

To empty Recycle Bin, do as follows:

1. Double-click the Recycle Bin icon on your desktop.
2. From the **File** menu, select **Empty Recycle Bin**.
3. Click **OK**.

All files inside the Recycle Bin folders on all drives are removed. Note that because these files are meant to be deleted, no real data is lost in the operation.

The second full scan of the computer was quite fast. Did the product really scan my whole computer?

A full computer scan scans all hard drives for malware, such as spyware, viruses and rootkits. The second full computer scan will be significantly faster because only the files that have changed will be scanned. This also accounts for differences in the number of files scanned between scans.

If an archive has not changed between scans, then it will not be touched in the second scan. If the archive contains 100 files, then the number of scanned files will be 101 higher in the initial scan. A second manual scan will typically take a matter of minutes.

Other files which are skipped include digitally-signed files from trusted vendors where the signature is intact. Examples of such files are Windows system files, Adobe's Acrobat Reader or Microsoft Excel. F-Secure's own files are also not checked if they have not changed; they were created by the software itself and therefore there is no point in scanning them.

It should also be noted that scheduled scans may find more viruses than a manual scan. The reason for this is that scheduled scans run as an administrative user, which may mean access to additional files.

Should I manually scan my hard disks daily?

Normally, it is not necessary to scan your hard disks manually. Virus and spyware scanning includes real-time scanning, which means that your computer is scanned for viruses in real time. If you want, you can scan manually for viruses by using scheduled scanning.

Note: Scanning for malware is an intensive process. It requires the full power of your computer and takes some time to complete. For this reason, you might want to set the program to scan your computer when you are not using it.

Setting up a scheduled scan

You can set the program to scan your computer at regular times, for example, weekly, daily, or monthly. To start a scheduled scan:

1. Open Computer Security.
2. On the main page of Computer Security, click **Settings**.
3. Select **Other settings > Scheduled scanning**.
4. Select **Turn on scheduled scanning**.
5. Select which days you would like to scan for viruses and spyware regularly:

Option	Description
Daily	To scan every day.
Weekly	To scan on selected days during the week. Select from the list to the right on which days to scan.

Monthly	To scan on up to three days a month. To select which days: 1. Select one of the **Day** options. 2. Select the day of the month from the list next to the selected day. 3. Repeat if you want to scan on another day.

6. Select when you want to start the scan on the selected days:

Option	Description
Start time	The time when the scan will start. Select a time when you expect not to use the computer.
After computer is not used for	Select a period of idle time after which the scanning starts if the computer is not used.

7. Click **OK**.

How can I clean an infected System Volume Information folder or a System Restore folder?

If a virus infects your computer, it is possible that the virus is backed up in the System Restore folder. System Restore is a feature of the Windows operating systems.

To clean the System Restore folder, you need to first turn it off, and then scan and clean the folder. By turning off System Restore, you lose your last system restore point. Unfortunately, there is no other way to remove infections from System Restore. If you want to continue using the System Restore feature, it is important to turn it on after removing the infected files.

To turn off System Restore in **Windows 7**:

1. Close all open programs.
2. Right-click **Computer** , and select **Properties**. The View basic information about your computer dialog box opens.
3. Click **System protection**. The System Properties dialog box opens.
4. Click the **System protection** tab.
5. Click **Configure**.
6. Select **Turn off System protection**.

7. Click **Apply**.
8. When the system asks if you want to turn off system protection, click **Yes**.
9. Click **OK**.
10. Scan all hard drives and all files for viruses with your F-Secure security product.

Once you have scanned and cleaned the files, turn on System Restore in Windows 7 as follows:

1. Right-click **Computer** , and select **Properties**. The View basic information about your computer dialog box opens.
2. Click **System protection**.
3. Click the **System protection** tab.
4. Click **Configure**.
5. Select **Restore system settings and previous versions of files**.
6. Click **Apply**.
7. Click **OK**.

To turn off System Restore in **Windows XP**:

1. Close all open programs.
2. Right-click **My Computer** , and select **Properties**. The System Properties dialog box opens.
3. Click the **System Restore** tab.
4. Select the **Turn off System Restore on all drives** check box.
5. Click **Apply**.
6. When the system asks if you want to turn off System Restore, click **Yes**.
7. Click **OK**.
8. Scan all hard drives and all files for viruses with your F-Secure security product.

Once you have scanned and cleaned the files, turn on System Restore in Windows XP as follows:

1. Right-click **My Computer** , and select **Properties**. The System Properties dialog box opens.
2. Click the **System Restore** tab.
3. Clear the **Turn off System Restore on all drives** check box.
4. Click **Apply** , and then click **OK**.

To turn off System Restore in **Windows Vista**:

1. Close all open programs.
2. Click **Start**.
3. Select **All Programs > Maintenance**.
4. Select **Maintenance > Backup and Restore Center**.
5. Click **Create a restore point or change settings**. If asked, click **Continue**.
6. Under Available disks, clear the check boxes for all drives.
7. Click **Apply**.
8. When the system asks if you want to turn off System Restore, click **Turn System Restore Off**.

9. Click **OK**.
10. Restart your computer.
11. Scan all hard drives and all files for viruses with your F-Secure security product.

Once you have scanned and cleaned the files, turn on System Restore in Vista as follows:

1. Close all open programs.
2. Click **Start**.
3. Select **All Programs › Maintenance**.
4. Select **Maintenance › Backup and Restore Center**.
5. Click **Create a restore point or change settings**. If asked, click **Continue**.
6. Under Available Disks, select all drives.
7. Click **Apply**.
8. When the system asks if you want to turn on System Restore, click **Turn System Restore On**.
9. Click **OK**.

How can I submit samples to F-Secure?

With [Sample Analysis System (SAS)](#) , you can send us anything suspicious that you encounter when online. We will immediately analyze your submission and update the databases accordingly if necessary.

Note: Samples can be submitted anonymously without an account. Signup for an account only if you want to:

- Get feedback on samples
- Submit large batches of samples
- Submit URLs

Tasks related to sample submission

The following collection of articles will help you in completing tasks that are necessary when sending samples to us:

- [Creating a ZIP archive and password-protecting it](#)
- [Saving a scanning report to a file](#)
- [Saving a spam, ham or phishing message to a file](#)
- [Making sure that your security software has the latest updates](#)

Updates

The product shows that the virus definitions are out of date. What can I do?

Updates are considered old after seven days. You should always try to keep your virus definition database up-to-date as viruses can change very quickly, and F-Secure may release several updates per day.

If this is the first time the computer has been turned on in the last seven days, for example after a holiday, the entire update package will be automatically downloaded and installed within 30 minutes.

If the F-Secure product still indicates that the virus definitions are out of date, try the following:

1. Open the F-Secure launch pad, right-click the F-Secure icon and select **Check for updates**.
2. Open the F-Secure launch pad, right-click the F-Secure icon and select **View my subscriptions**. In the My subscriptions window, you can check the status of your subscription.
3. Check that the Windows date and time are correct because incorrect settings can cause the product to report that your virus definitions are out of date even though this is not the case. You can see the date and time in the Windows system tray. You can change the clock settings in the Date and Time Properties. To open the properties, double-click the clock.
4. Download and run fsaua-reset.exe. When the command window opens, press Y. The program will close by itself.
5. Download and run fsdbupdate9.exe which contains a new copy of the virus definitions.

If the above actions do not help, we recommend that you first uninstall the product and then reinstall it.

How do I know that I have the latest updates?

Automatic updates are turned on as soon as you install the F-Secure software. Whenever your computer is connected to the Internet, the F-Secure product checks for the newest updates automatically and downloads them once every two hours.

The entire update package is quite large, and the download time depends on the speed of your Internet connection. If your computer has not been turned on in the last seven days, the entire update package will be downloaded and installed, and this takes longer than the normal daily updates.

Note: To make the download as fast as possible, we recommend that you connect your computer to the Internet at least once a week if possible.
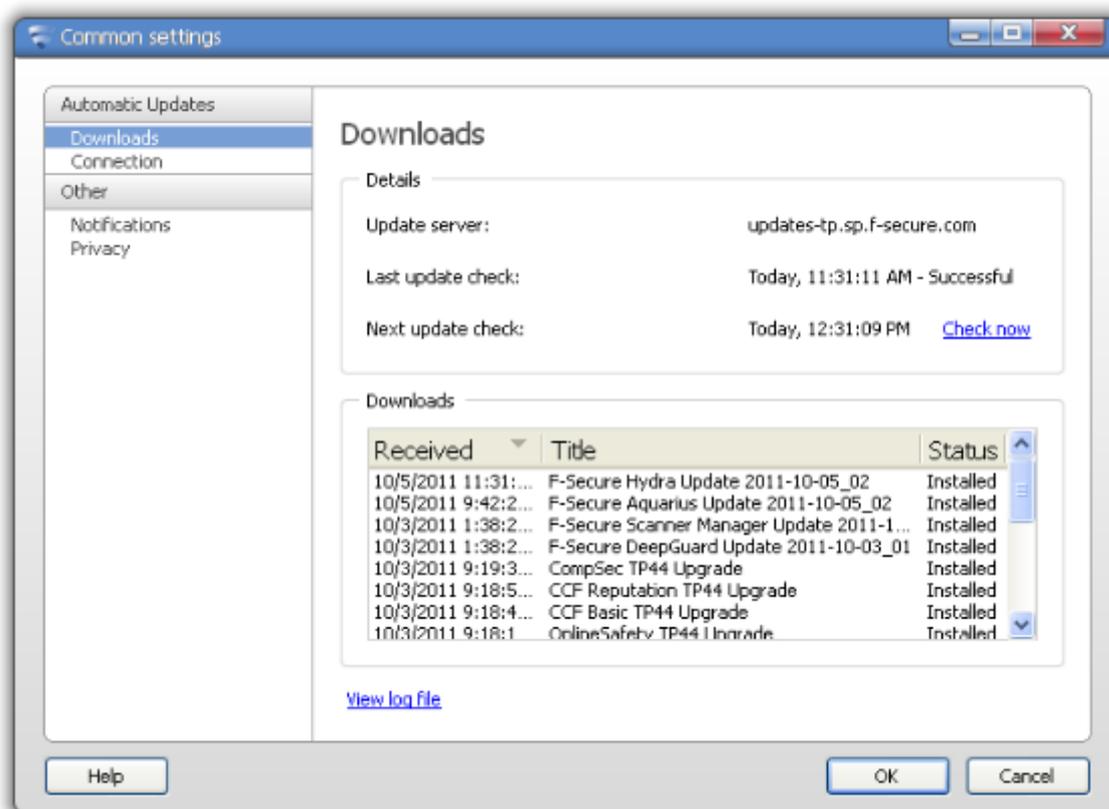
Checking for the latest updates

To check for the latest database updates:

1. On the launch pad, click **Computer Security**.
2. On the main page of Computer Security, click **Settings**.
3. Select **Other settings > Database versions** to view the Database versions page.

The date and version of the database update package with the highest version number is displayed on the page. Note that the update package with the highest version number is not necessarily the latest update that has been downloaded.

If you want to see the latest updates installed for each of the scanning engines available in the product, do the following:

1. On the launch pad, right-click the right-most icon. A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Automatic updates > Downloads**:

On the Downloads table, you can check the corresponding engine name and the version of its latest update.

Note: If you are using a modem, or have an ISDN connection to the Internet, the connection must be active to check for updates.

Checking for updates manually

The product receives the latest updates automatically as soon as you are connected to the Internet. However, if you want to be sure and check that you have the latest updates:

1. On the launch pad, right-click the right-most icon. A pop-up menu appears.
2. Select **Check for updates**. The Checking for updates window is displayed.

The product checks for new updates and installs them immediately.

How can I check that my computer is protected and that automatic updates are working?

The Status page shows you a quick overview of all installed product features and their current status.

To open the Status page, click **Status** on the main page of Computer Security.

The icons show you the status of the program and its security features:

Status icon	Status name	Description
✅	OK	Your computer is protected. The feature is turned on, and working properly.
ℹ️	Information	The product informs you about a special status of a feature. This icon is shown, for example, when a feature is being updated.
⚠️	Warning	Your computer is not fully protected. For example, the product has not received updates is a long time, or the status of a feature requires attention.
❌	Error	Your computer is not protected. For example, your subscription has expired, a critical feature is turned off.

⊗	Off	A non-critical feature is turned off.

More information

What is the launch pad?

Once you have downloaded the F-Secure network installer (F-SecureNetworkInstaller.exe) and installed the product, the launch pad is displayed at the bottom of your screen:

If it is not visible on the screen, you can open it from the F-Secure icon on your desktop. This is where you can access all your F-Secure applications and manage your subscriptions.

The launch pad's common settings are settings that apply to all of the programs installed on the launch pad. Instead of changing the settings separately in each program, you can simply edit the common settings, which are then used by all of the installed programs.

You can use the launch pad to change the following common settings:

- **Downloads** - where you can view information about what updates have been downloaded and manually check if new updates are available.
- **Connection** settings - where you can change how your computer connects to the Internet.
- **Notifications** - where you can view past notifications and set what kind of notifications you want to see.
- **Privacy** settings - where you can select whether or not your computer is allowed to connect to the Real-time Protection Network.

Note: For security reasons, some of the settings can be changed only by a user with administrative access rights.

You can also manage your subscriptions for installed programs through the launch pad:

1. On the launch pad, right-click the right-most icon. A pop-up menu appears.
2. Select **View my subscriptions**. The My subscriptions window opens.
3. Do one of the following:

   - Select **Subscription status** to view information about your subscriptions for installed programs.
   - Select **Installation status** to see what programs are available to be installed.

For more information about F-Secure launch pad:

1. On the launch pad, right-click the right-most icon. A pop-up menu appears.
2. Select **Help**.

What is Online Safety?

Online Safety helps you and your family to browse the web safely. In addition to protecting you against malicious software and web sites, you can also restrict the type of content that can be viewed by your children. You can also control when and for how long someone is allowed to browse the Internet.

The product uses Windows user accounts to control the settings for each member of your family. Only someone with administrative access rights is allowed to change the product settings for the various Windows user accounts.

We recommend that you set up a separate Windows user account for each family member. For example, parents can have administrative access rights, and children can have normal access rights for their Windows user accounts.

For more information about how to use Online Safety:

1. On the F-Secure launch pad, right-click the Online Safety icon. A pop-up menu appears.
2. Select **Help**.

What is Computer Security?

Computer Security protects your computer against all kinds of malicious attacks. It keeps viruses, worms, and spyware away from your computer. It blocks spam and phishing e-mails.

The firewall stops unwanted visitors getting into your computer via the Internet and protects you from hackers.

If you are using Microsoft Windows 7, the product also makes sure that you will not receive surprising bills when you are using mobile broadband.

Note: For security reasons, some of the settings can be changed only by a user with administrative access rights.

For more information about how to use Computer Security:

1. On the F-Secure launch pad, right-click the Computer Security icon. A pop-up menu appears.
2. Select **Help**.