

F-Secure PSB for Workstations



Getting Started	5
What Should I Do After Installation	5
How to Check That the Product is Working Properly	5
How to Open the Product	6
How Can I Make Sure That My Computer Is Protected.....	6
What Does the Status Tooltip Indicate	6
How to View the Overall Status of Your Protection	8
What is Security News	10
How to View Security News Details	10
What do Security News Details Indicate	10
What Are Flyers	11
How Can I Quickly Run the Most Common Tasks	11
How to Scan a File or Folder in Windows Explorer	11
How to Quickly Run Tasks from the Status Icon Shortcut Menu?	12
Use Server Queries to Improve Detection Accuracy.....	13
What Is Browsing Protection	14
Turn Browsing Protection On.....	14
What to Do If a Browsing Protection Dialog Box Appears.....	14
Cancelling a Scheduled Scan When You are Using Your Computer	15
Seeing the Results of a Scheduled Scan.....	15
Viewing Virus and Spyware History	15
Virus and Spyware History	16
Using the Internet Safely	17
What Are Security Levels	18
How are security levels related to firewall rules and services.....	18
Change the Security Level	19
What Is a Firewall	19
What to Do If an Internet Shield Alert Pop-Up Appears.....	19
Turn the Internet Shield Alert Pop-Ups On or Off.....	20
What Are Firewall Rules	21
When do you have to add a new firewall rule.....	21
What Are Firewall Services	22
Viewing Firewall Services.....	23

What Are Dynamic Firewall Rules.....	24
View Dynamic Firewall Rules.....	24
How Does the Priority Order of Firewall Rules Work	25
An example of how the priority order works	25
Create Firewall Services and Rules.....	25
Create a Firewall Service	26
Start Creating a Rule.....	28
Select the IP Addresses	28
How can you define an IP subnet	29
Select the Services and Direction	29
Select Alerting Options	30
Check and Accept the Rule.....	31
Define the Priority Order of Firewall Rules	31
Open a Port.....	32
Turn a Firewall Rule On or Off.....	32
View Firewall Rules	32
Firewall Rule Details.....	33
Change a Firewall Rule.....	34
Examples of Creating Firewall Rules.....	35
How to Create a Rule for A Network Game.....	35
How to Create a Rule for Sharing Files on a Home Network	36
Firewall Settings.....	38
Change the IPv6 Settings.....	38
What to Do if You Share an Internet Connection.....	39
What If You Use a Digital TV Card.....	40
Controlling Internet Connections for Applications.....	40
What Is the Difference Between the Firewall and Application Control	40
What to Do If an Application Control Pop-Up Appears	41
Safe and Unsafe Programs and Connection Attempts	42
Which programs and connection attempts you can consider safe.....	42
Which programs and connection attempts you cannot consider safe	43
Allow or Deny Connections for Programs	43
Turn Application Control Pop-Ups On or Off	44
What to Do If a Program Stops Working	44

Preventing Intruders from Accessing Your Computer.....	45
What Is the Difference Between the Firewall and Intrusion Prevention	45
Select How Intrusion Attempts Are Handled	46
Controlling Dial-Up Connections	46
What to Do If a Dial-Up Control Pop-Up Appears	47
Add, Edit or Remove Phone Numbers	48
View Programs that Are Allowed to Close Dial-Up Connections	49
View Dial-Up Connection Attempts.....	49
What to Do If You Cannot Access the Internet Through Your Modem	50
Viewing the Internet Shield Status, Alerts and Log Files.....	50
Check the Status of Internet Shield	51
Check the Current Internet Shield Settings	51
Check the Number of Recent Internet Shield Actions.....	51
Check Internet Shield Statistics.....	52
View Internet Shield Alerts	52
Internet Shield Alert Information.....	53
View Log Files	53
Action log	53
Packet log	54
View the Action Log.....	54
Action Log Examples.....	54
Opening a connection	55
Receiving a connection.....	55
Adding and removing a dynamic firewall rule.....	55
Use Packet Logging for Monitoring Network Traffic.....	56
Start Packet Logging.....	56
View the Packet Log.....	57
Automatic Updates	58
Checking the Update Status	58
Changing the Internet Connection Settings.....	59
Configuring the HTTP Proxy Manually	59
Add a Policy Manager Proxy Server.....	60
Central Management.....	60
About Central Management Policies	61

Manually Check for a Policy Update.....	61
Manually Import a Policy File.....	61
Open Windows Event Viewer.....	62
View the Central Management Log.....	62
Communication Settings.....	62

Getting Started

This section describes how to get started with using the product.

- [What Should I Do After Installation](#)
After you have installed the product, we recommend checking that the product is working properly.
- [How Can I Make Sure That My Computer Is Protected](#)
You can check the status icon on your system tray and the product status and subscription information on the Home tab to make sure that your computer is protected.
- [How Can I Quickly Run the Most Common Tasks](#)
You can scan a file or folder in Windows Explorer, or run various tasks from the status icon shortcut menu.

What Should I Do After Installation



After you have installed the product, we recommend checking that the product is working properly.

- [How to Check That the Product is Working Properly](#)
After you have finished the installation, check that the product status icon is shown on your Windows system tray at the bottom right corner of your screen.
- [How to Open the Product](#)
You can open the product by double-clicking the product status icon on your Windows system tray.

How to Check That the Product is Working Properly

After you have finished the installation, check that the product status icon is shown on your Windows system tray at the bottom right corner of your screen.

To view the icon:

1. If you are using Windows XP, click the  button to show the system tray icons.
2. Check that the  icon is shown on the system tray.



If the icon is shown, the product is working properly and your computer is protected.

[concept_1254230DC3F94D0BA2D69E75D0F9E591](#)

How to Open the Product

You can open the product by double-clicking the product status icon on your Windows system tray.

To open the product:

1. If you are using Windows XP, click the  button to show the system tray icons.
2. Double-click the  icon.

The **Home** tab of the product user interface shows you a summary of the protection status and the installed product components.

Tip: You can also open the product and help from Windows **Start** menu.

How Can I Make Sure That My Computer Is Protected

You can check the status icon on your system tray and the product status and subscription information on the *Home* tab to make sure that your computer is protected.










- [What Does the Status Tooltip Indicate](#)
When you place your mouse pointer over the product status icon on your Windows system tray, a tooltip that tells the product status appears.
- [How to View the Overall Status of Your Protection](#)
The Home tab shows you a quick overview of your security components and the status of the installed security components.


What Does the Status Tooltip Indicate

When you place your mouse pointer over the product status icon on your Windows system tray, a tooltip that tells the product status appears.

The icon may be different or may not appear at all depending on the product status.

Status icons and their meanings: Icon	Status	What to Do
	The product is working properly. Your computer is	You can use your computer

Status icons and their meanings: Icon	Status	What to Do
	protected.	normally.
	Download in progress. Your computer will be protected as soon as the download is complete.	This icon is shown, for example, when virus and spyware definitions or security levels are being downloaded. Wait until the download is complete.
	Error state. An error has occurred.	Place your mouse pointer over the  icon to see the reason for the error. If necessary, restart your computer.
	Warning. A protection feature, for example Real-time Scanning, is turned off or your virus and spyware definitions are out of date. Your computer is not fully protected.	Place your mouse pointer over the  icon to see the status tooltip. You may see this icon, for example, if you are defragmenting your hard drive, because some system functions cause all downloads to be suspended. Turn on the feature that is currently turned off, or check for updates.
	Critical warning state (flashing icon).	This icon is shown when the virus and spyware definitions have not been updated lately. Update the virus and spyware definitions immediately.
	Unloaded. The product is unloaded from the memory of your computer. Your computer is not protected.	Right-click the  icon and select Reload to activate the product.

Status icons and their meanings: Icon	Status	What to Do
	Indicates that the Parent profile is active.	You can access the Internet without limitations.
No icon	The product is not installed or there was an error that prevented starting the product.	Restart your computer. If the icon does not appear, re-install the product.

How to View the Overall Status of Your Protection

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 on the tabs on the left you can see the details of all the security components.

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.

- [What is Security News](#)
The Security News page shows a list of news items on recent virus outbreaks and other security news.
- [How to View Security News Details](#)
You can read a description of the security threat and access a web page with more information on the threat.
- [What do Security News Details Indicate](#)
In the Security News details dialog box you can read the news item and see whether your computer is protected against the threat yet.
- [What Are Flyers](#)
Flyers are small notifications that are shown at the bottom right-hand corner of your computer screen.
- [How to see what the product has done](#)

What is Security News

The *Security News* page shows a list of news items on recent virus outbreaks and other security news.

The list shows:

- the date and time of receiving each news item,
- the subject of the news item, and
- whether your computer is protected against the threat or not.

Also, a notification balloon appears on your system tray when you receive a new security news item.

How to View Security News Details

You can read a description of the security threat and access a web page with more information on the threat.

To view Security News details:

1. On the *Home* tab, click **Advanced**.
2. Select *General > Security News*.
3. Click **View News**.
4. Select a news item and click **Details**. This opens the *Security News* dialog box where you can read the news item. The dialog shows you whether your computer is protected against the threat.
5. To access the web for more information, click **More information (web)**.

What do Security News Details Indicate

In the *Security News* details dialog box you can read the news item and see whether your computer is protected against the threat yet.

The Security News Details window shows a short article on the news item that you selected. Above the article, you see whether your computer is protected against the threat:

Protection status and recommended action: Protection status	What to do
"This computer is not protected yet. The update will be available soon in definitions version yyyy-mm-dd_##."	There is no update available yet that could protect against this virus. A new update that protects against the virus will be available as soon as possible. Wait for the update to become available.

Protection status and recommended action: Protection status	What to do
"This computer is not protected against this virus. Update now..."	A new update is available but you do not have it yet. Click Update now to update the product.
"This computer is protected."	Your definition updates protect you against this threat. You can use your computer normally.
"This computer can be protected only with the Internet Shield. Read the description for more information how to protect your computer."	The malware reported in this news item uses network attacks to cause harm. To protect your computer against it, configure Internet Shield to block its access to your computer.

What Are Flyers

Flyers are small notifications that are shown at the bottom right-hand corner of your computer screen.

The flyers inform you about the actions that your security product has taken to protect your computer. They are shown, for example, if System Control has denied the use of a program. These flyers are informational, and do not require any action from you. You can view all the shown flyers in the flyer history.

How Can I Quickly Run the Most Common Tasks

You can scan a file or folder in Windows Explorer, or run various tasks from the status icon shortcut menu.

- [How to Scan a File or Folder in Windows Explorer](#)
You can scan disks, folders and files for viruses, spyware and riskware in Windows Explorer.
- [How to Quickly Run Tasks from the Status Icon Shortcut Menu?](#)
You can use the product status icon on Windows system tray to quickly run the most common tasks.

How to Scan a File or Folder in Windows Explorer

You can scan disks, folders and files for viruses, spyware and riskware in Windows Explorer.

To scan a disk, folder or file:

1. Place your mouse pointer on and right-click the disk, folder or file you want to scan.



- From the right-click menu, select **Scan Folders for Viruses and Spyware**. (The option name depends on whether you are scanning a disk, folder or file.) The *Scan Wizard* window opens and the scan starts.

If a virus or spyware is found, the *Scan Wizard* guides you through the cleaning stages.

How to Quickly Run Tasks from the Status Icon Shortcut Menu?

You can use the product status icon on Windows system tray to quickly run the most common tasks.

To run the tasks:

- If you are using Windows XP, click the  button to show the system tray icons.
- Right-click the  icon with your mouse. A menu with the most common tasks opens.
- Select the task you want to run from the menu.

General tasks: Option	What it does
Open [product name]	Opens the product user interface where you can see the status of all product components and access product settings to change your protection level.
Show Flyer History	Shows a list of informational messages displayed by the product. This list includes, for example: <ul style="list-style-type: none"> ○ System control events ○ Web Traffic Scanning events ○ Service news items ○ Scheduled scanning events
Suspend all downloads and updates	If you are using an Internet connection that you pay for by the amount data transferred, you can suspend all downloads and updates.
Tasks in Virus & Spy Protection submenu: Option	What it does
Scan target	Scans a specific file or folder for viruses, spyware and

General tasks: Option	What it does
	riskware. Select the target directory or file and click OK to start the scan.
Scan hard drives	Scans all files on your hard drives for viruses, spyware and riskware.
Quick malware scan	Scans the system for malware and riskware.
Quick rootkit scan	Scans the system for rootkits and other suspicious and hidden items.
Perform full computer check	Scans the computer for viruses, spyware and rootkits.
Tasks in Internet Shield submenu: Option	What it does
Block all network traffic	Blocks all network traffic. This option should be used only if you suspect that your computer is under a network attack.
Allow all network traffic	Lets all network traffic through. This option disables your firewall completely and renders computer vulnerable to all network attacks.
Show alert log	Opens the <i>Internet Shield Alerts</i> dialog.
About submenu: Option	What it does
About	Shows product information, for example, the version number.

[AutomaticallyCreatedBookmark14](#)

Use Server Queries to Improve Detection Accuracy

Using the server queries improves the detection rate of suspicious programs.

When you start a potentially suspicious program, System Control contacts the F-Secure server. If the server recognizes the program as suspicious, System Control blocks it. System Control does not contact the F-Secure server if you have specifically allowed the program to run.

To turn on server queries:

1. Click the *Virus & Spy Protection* tab.
2. Click **Configure** next to Real-time Scanning.
3. Click the *System Control* tab.
4. Under Settings, check **Use server queries to improve detection accuracy**.
5. Click **OK**.

If you are using a mobile connection, we recommend turning off the server queries option. Keeping on this option may increase the network traffic.

What Is Browsing Protection

Browsing Protection protects your web browser against hijack attempts.

When you are browsing the Internet, harmful trojans may try to hijack your web browser. The purpose of such an attempt may be to steal confidential information, such as your user name or password. Browsing Protection blocks all browser hijack attempts and notifies you of them.

Turn Browsing Protection On

Use Browsing Protection to protect your web browser against hijack attempts.

If a trojan tries to hijack your browser, the trojan is blocked and you are notified.

To turn Browsing Protection on:

1. Click the *Virus & Spy Protection* tab.
2. Click **Configure** next to Real-time Scanning.
3. Click the *System Control* page.
4. Make sure **Enable System Control** is selected. Browsing Protection works only when System Control is on.
5. Make sure **Enhanced Process Monitoring** is turned on. Browsing Protection works only when Enhanced Process Monitoring is on.
6. Select **Enable Browsing Protection**.
7. Click **OK**.

If your web browser seems to be working slowly, you may consider turning Browsing Protection off.

What to Do If a Browsing Protection Dialog Box Appears

If a trojan tries to hijack your web browser, the Browsing Protection dialog box appears.

This may happen when you open your web browser, or during web browsing. When the dialog box appears, you do not have to do anything. Browsing Protection has already blocked the trojan and you can safely use the Internet.

Cancelling a Scheduled Scan When You are Using Your Computer

If you want to continue to use your computer when a scheduled scan starts, you may want to cancel the scheduled scan.

Scheduled scanning may have a noticeable effect of your computers performance. To cancel the scheduled scan:

Note: In centrally managed mode you may not be able to cancel a scheduled scan.

1. Click **Scheduled scan has started** link on the *Virus & Spy Protection* flyer.
2. Click **Cancel** on the *Virus & Spy Protection* window.
3. Click **Close**.

The scheduled scan is canceled. The next scheduled scan will start as usual.

Related tasks

[Scan for Malware at Set Times](#)

Seeing the Results of a Scheduled Scan

When a scheduled scan finishes you can check if malware were found.

To check the results of a scheduled scan:

1. Click the **Scheduled scan has finished** on the *Virus & Spy Protection* flyer.
2. Click **Show Report** to see what happened during the scan.
Note: If you opened the dialog from the *Flyer History* dialog, the **Show report** button is disabled. You cannot see the results of previous scheduled scans.
3. Click **Close** to close the dialog.

Related tasks

[Scan for Malware at Set Times](#)

Viewing Virus and Spyware History

Virus and spyware history shows you what the program has done to found viruses and spyware.

To open the history:

1. Click the *Virus & Spy Protection* tab.
2. Click **Open virus and spyware history**.

- [Virus and Spyware History](#)
Virus and spyware history shows what the program has done to found viruses and spyware.

Virus and Spyware History

Virus and spyware history shows what the program has done to found viruses and spyware.

Under *Infections*, you can view a list of found infections. Below each infection, you can view all infected items separately. Infected items can be files, registry keys or processes. The *Action* column shows you what the program has done to the infections and infected items.


The performed action for an infection can be one of the following:

Action	Description
Removed	One or more infected items have been either deleted, disinfected, renamed, quarantined, restored or terminated.
Restart required	One or more infected items have required (or require) restarting the computer.
Blocked	One or more infected items have been blocked but not removed.
None	Nothing has been done to the infected items.
Failed	The program has failed to remove the virus or spyware from one or more infected items.

The performed action for an infected item (file, registry key or process) can be one of the following:

Action	Description
Disinfected	A virus or spyware has been removed from the infected item.
Deleted	An infected item has been deleted.
Blocked	Access to the infected item has been blocked.
Renamed	An infected item has been renamed. This happens if the virus or spyware cannot be removed from the infected item. The virus or spyware in the renamed item cannot harm your computer anymore.
Quarantined	The infected item was moved to the quarantine, from where the virus or spyware cannot harm your computer anymore.
Restored	A virus or spyware has modified a registry key, but the original registry key or file has been restored.
Terminated	An infected process has been terminated.
Restart required	An infected item has required (or requires) restarting your computer.
None	Nothing has been done to the infected item.

Action	Description
Failed	The program has failed to remove the virus or spyware from the infected item.

To view more information about the infection, click the  icon next to the infection. A web page opens. The page describes the virus or spyware, and the security risks it carries.

Using the Internet Safely

Internet Shield protects your computer against unsafe Internet traffic.

Internet Shield:

- Protects you against intruders who try to access your computer without your permission. They may, for example, try to steal your personal information, such as files, passwords or credit card numbers.
- Blocks malicious Internet traffic such as trojans. They may, for example, destroy files on your computer, crash your computer, or open ports for hackers to access your computer.
- Blocks harmful Internet traffic such as spyware. Spyware may, for example, gather information about your e-mail addresses, passwords and credit card numbers.
- Prevents malicious dialer programs from using your modem or ISDN connection to dial into expensive pay-per-minute phone numbers.

After you have installed the product, Internet Shield automatically keeps your computer protected.

- [What Are Security Levels](#)
Internet Shield security levels define the level of protection on your computer.
- [What Is a Firewall](#)
The firewall protects your computer by allowing safe Internet traffic and blocking unsafe traffic.
- [Controlling Internet Connections for Applications](#)
Application Control prevents harmful programs from connecting to the Internet.
- [Preventing Intruders from Accessing Your Computer](#)
Intrusion Prevention protects against network attacks aimed at open ports on your computer.
- [Controlling Dial-Up Connections](#)
Dial-up Control prevents malicious dialer programs from opening connections to expensive pay-per-minute phone numbers.
- [Viewing the Internet Shield Status, Alerts and Log Files](#)
By viewing the Internet Shield status, alerts and log files, you can find out how Internet Shield protects your computer.

What Are Security Levels

Internet Shield security levels define the level of protection on your computer.

Each security level has a predefined set of firewall rules, which define the type of traffic that is allowed to or denied from your computer. To some levels you can also add rules that you have created yourself.

Security levels also define

- if Internet connections are automatically allowed for all applications, or
- if you can separately allow or deny each new connection attempt in an Application Control pop-up.

There are several predefined security levels, which range from very strict to very loose:

- A very strict security level (**Block All**) usually blocks most of the network traffic. This may prevent you from using some of the programs on your computer.
- A medium level (**Normal**) usually allows all outbound Internet traffic from your computer. The medium level may deny some inbound services and generate alerts about them.
- A very loose level (**Allow all**) usually allows all network traffic, both inbound and outbound, and does not generate any alerts. Because this level leaves your computer unprotected, do not use it except for in special cases.

Note: Depending on the product you are using, the names of security levels can be different.

Your computer is safe with the predefined security level. You may need to change the level to a stricter one, for example, if you use your laptop outside your home and open the Internet using a WLAN connection.

You can define your own security level and add your own set of rules for it. However, we recommend that only experienced users define their own security levels.

How are security levels related to firewall rules and services

A security level consists of several firewall rules. A firewall rule consists of several firewall services. Services are defined by the protocols and ports they use.

For example, the *Normal* security level has a firewall rule called *Web browsing*. This rule allows you to browse the web. The rule includes the services that are needed for web browsing, such as the *HyperText Transfer Protocol (HTTP)* service. This service uses the TCP and port number 80.

- [Change the Security Level](#)
If you want to change the level of protection on your computer, change the security level.

Related concepts

[What Are Firewall Rules](#)

[What Are Firewall Services](#)

Change the Security Level

If you want to change the level of protection on your computer, change the security level.

To change the security level:

1. Click the *Internet Shield* tab.
2. Next to *Internet Shield* and the current security level, click **Change**.
3. Read the security level descriptions carefully.
4. Select the appropriate level from the list and click **OK**.

The *Internet Shield* page now shows the new security level. The firewall rules and Application Control settings change according to the selected security level.

Related tasks

[Create Firewall Services and Rules](#)

What Is a Firewall

The firewall protects your computer by allowing safe Internet traffic and blocking unsafe traffic.

Typically, the firewall allows all traffic from your computer to the Internet, but blocks all traffic from the Internet to your computer unless you specifically allow it. By blocking the inbound traffic, the firewall protects your computer against malicious software, such as worms, and prevents intruders from accessing your computer. Depending on your alerting settings, Internet Shield alert pop-ups may be shown about the actions of the firewall.

Your computer is protected with the predefined firewall settings. Usually, you do not have to change them. However, you may have to change the settings, if you use a very strict security level, or if you have added your own firewall rules or services.

CAUTION:

Do not turn the firewall off. If you do, your computer is vulnerable to all network attacks. If a program stops working because it cannot connect to the Internet, change the firewall rules or Application Control settings instead of turning the firewall off.

- [What to Do If an Internet Shield Alert Pop-Up Appears](#)
An Internet Shield alert pop-up appears on your computer screen when the firewall detects suspicious network traffic on your computer.
- [What Are Firewall Rules](#)
Firewall rules define what kind of Internet traffic is allowed or blocked.
- [Firewall Settings](#)
On the Settings tab, you can change the IPv6 settings and the alerting level, and allow all traffic between computers on a home network.

What to Do If an Internet Shield Alert Pop-Up Appears

An Internet Shield alert pop-up appears on your computer screen when the firewall detects suspicious network traffic on your computer.

A pop-up is shown when alert pop-ups have been turned on and either of the following happen:

- the traffic matches one of the current firewall rules, and alerting has been turned on for this rule, or
- there has been an intrusion attempt on your computer, and alerting has been turned on for Intrusion Prevention.

You do not necessarily have to do anything because the firewall blocks suspicious traffic automatically and prevents intrusion attempts (if **Block and log attempt** has been turned on in the Intrusion Prevention settings).

If an alert pop-up appears, do the following:

1. Read the alert information.
2. To view the alert details, click **Details >>**.
3. If you do not want Internet Shield alert pop-ups to be shown anymore, select the **Do not show alert dialog again** check box.
4. To get more information about the remote IP address, click **DNS name**. It shows the domain name of the IP address, for example, *www.example.com*. If the domain name cannot be resolved, the **DNS name** button becomes unavailable and no domain name is shown.
5. You can create a new firewall rule for the traffic that generated the alert. This rule can either allow or deny this kind of traffic in future. Click **Create Rule** and fill in the rule information.
6. To close the *Internet Shield alerts* dialog box, click **Close**.

Now you can continue using your computer normally.

- [Turn the Internet Shield Alert Pop-Ups On or Off](#)
You can select whether Internet Shield alert pop-ups are shown.

Turn the Internet Shield Alert Pop-Ups On or Off

You can select whether Internet Shield alert pop-ups are shown.

To turn the alert pop-ups on or off:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the **Settings** tab.
5. Click **Show Alert Log**.
6. To turn the pop-ups on, select the **Show alert pop-ups** checkbox. To turn the pop-ups off, clear the checkbox.

7. Click **Close**.

If you turned the pop-ups on, you see a pop-up the next time some traffic matches the current firewall rules. This applies only to rules which have the alert logging and pop-ups active. If you turned the pop-ups off, they do not appear anymore.

Related tasks

[Select Alerting Options](#)

What Are Firewall Rules

Firewall rules define what kind of Internet traffic is allowed or blocked.

Each security level has a predefined set of firewall rules, which you cannot change. You can only add new rules to some of the levels. For some levels you may not be able to add your own rules. There may also be a level that has no predefined rules and that allows you to freely add your own set of rules. The selected security level also affects the priority which your own rules receive in relation to the predefined rules.

A firewall rule can be applied to traffic from the Internet to your computer (inbound), or from your computer to the Internet (outbound). A rule can also be applied to both directions at the same time.

A firewall rule consists of firewall services, which specify the type of traffic and the ports that this type of traffic uses. For example, a rule called *Web browsing* has a service called *HTTP*, which uses the TCP and port number 80.

Firewall rules also define whether Internet Shield alert pop-ups are shown to you about the traffic that matches the firewall rules.

When do you have to add a new firewall rule

You may have to add a new firewall rule if you start using a new program or attach a new device to your computer, for example, a WLAN device or an IP camera.

By adding all the services that the program or device needs to the same rule, you can easily:

- turn the rule on or off later, or
- remove the rule if you uninstall the program or remove the device.

You also have to add a new rule if you have denied certain type of traffic but you want to allow it to certain IP addresses. In this case, you already have a general "deny" firewall rule. To allow the traffic to certain IP addresses, you have to create a more specific "allow" rule.

For example, if the general rule denies all outbound FTP traffic, you may still want to allow FTP traffic to your Internet Service Provider's site to be able to update your web pages. You can do this by adding a more specific rule that allows FTP traffic to the Internet Service Provider's IP address, and give the rule a higher priority than for the "deny" rule.

- [What Are Firewall Services](#)
Firewall services define the type of traffic to which a firewall rule applies.

- [What Are Dynamic Firewall Rules](#)
Dynamic firewall rules are created for connections from remote computers to server programs on your computer.
- [How Does the Priority Order of Firewall Rules Work](#)
Firewall rules have a priority order that determines the order in which the rules are applied to network traffic.
- [Create Firewall Services and Rules](#)
You can create your own firewall services and rules if you want to allow or deny some Internet traffic.
- [Open a Port](#)
You can open a port through the firewall if you want to allow some Internet traffic and you know the port number you want to open.
- [Turn a Firewall Rule On or Off](#)
You can turn a firewall rule off to temporarily allow some traffic that the rule denies.
- [View Firewall Rules](#)
You can view the currently active firewall rules to find out how the firewall allows or blocks traffic on your computer.
- [Change a Firewall Rule](#)
You can only change a firewall rule that you have created yourself.
- [Examples of Creating Firewall Rules](#)
You can create a new firewall rule if you want to play a new network game, or share files on your home network.

Related concepts

[What Are Security Levels](#)

Related tasks

[Create Firewall Services and Rules](#)

What Are Firewall Services

Firewall services define the type of traffic to which a firewall rule applies.

Network services, such as web browsing, file sharing or remote console access, are examples of these firewall services.

A service uses a certain protocol and port. For example, the HTTP service uses the TCP protocol and the port number 80.

A firewall service uses two kinds of ports:

- Initiator port: the port on the computer that starts the connection.

- Responder port: the port on the computer where the connection ends.

Whether the port on your own computer is an initiator port or responder port depends on the direction of the traffic:

- If the firewall service is for outbound traffic, the initiator port is the port on your own computer. The responder port is then the port on a remote computer.
- If the firewall service is for inbound traffic, the initiator port is the port on a remote computer. The responder port is then the port on your own computer.

The responder ports are typically mentioned in the software documentation. The initiator port can usually be any port higher than 1023. However, for some games you may also have to define specific initiator ports. In this case, they are also mentioned in the software documentation.

If you create a new firewall rule, you have several predefined services that you can add to the rule. You can also create and add your own services if the service that you need is not on the services list.

- [Viewing Firewall Services](#)
You can view the existing firewall services on the Services tab.

Related concepts

[What Are Security Levels](#)

Related tasks

[Create Firewall Services and Rules](#)

Viewing Firewall Services

You can view the existing firewall services on the *Services* tab.

To view the services:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Services* tab. You can view the following information:

Field	Description
Description	Description of the service.
In Use	Shows whether or not the service is used in any of the firewall rules.
Rule Name	If the service is used in firewall rules, shows the names of the rules.

5. To view details of a service, select the service on the list and click **Details**. The *Service Details* dialog box opens.

6. After viewing the service details, click **Close**.

Related tasks

[Create Firewall Services and Rules](#)

[Create a Firewall Service](#)

What Are Dynamic Firewall Rules

Dynamic firewall rules are created for connections from remote computers to server programs on your computer.

If an Application Control pop-up is shown, and you allow an inbound connection, for example, to a peer-to-peer server program on your computer, the firewall creates a temporary, dynamic firewall rule. This rule is added to the dynamic rules list on the *Activity* tab. The rule opens a port for this program and keeps it open as long as the program listens to the port for inbound connections.

When the program stops listening to the port, the rule closes the port and the dynamic rule is removed from the dynamic rules list. Depending on your Application Control settings, the Application Control pop-up may not be shown for all programs. If the pop-up is not shown, the dynamic firewall rule is automatically created for this program.

- [View Dynamic Firewall Rules](#)
The Activity tab shows the dynamic firewall rules which are currently active.

[concept_F980D184D74D4FF0A79562231548178C](#)

View Dynamic Firewall Rules

The *Activity* tab shows the dynamic firewall rules which are currently active.

Dynamic firewall rules are created for connections from remote computers to server programs on your computer.

To view the dynamic firewall rules:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Activity* tab. You can view the following information:
 - *Application*: The file name of the server program on your computer which currently listens to a port for inbound connections.
 - *Listening Port*: The port that the dynamic firewall rule has opened. The server program listens to this port for inbound connections.
 - *Remote Address*: The server program listens to the port for connections from the following IP addresses:
 - *0.0.0.0/0*: All IPv4 addresses.

- `::/0`: All IPv6 addresses.

How Does the Priority Order of Firewall Rules Work

Firewall rules have a priority order that determines the order in which the rules are applied to network traffic.

Firewall rules are shown as a list on the *Rules* tab. The rules are applied from top to bottom, and the first rule that matches the traffic overrides all the other rules below. The main principle is to allow only the needed traffic and block the rest. Therefore, the last rule of a security level is the *Deny rest* rule. It blocks all the traffic that the rules above it do not specifically allow.

Dynamic firewall rules are shown separately as a list on the *Activity* tab. The priority of the dynamic rules is lower than the priority of normal firewall rules. This means that if a firewall rule denies some traffic, the dynamic rule cannot allow it. However, the priority of the dynamic rules is higher than the priority of the predefined *Deny rest* rule.

An example of how the priority order works

- You have added a rule that denies all outbound FTP traffic. Above the rule in the rules list, you add another rule that allows an FTP connection to your Internet Service Provider's IP address. This rule allows you to create an FTP connection to that IP address.
- You have added a rule that allows you to create an FTP connection to your Internet Service Provider's IP address. Above the rule in the rules list, you add another rule that denies all FTP traffic. This rule prevents you from creating an FTP connection to your Internet Service Provider's IP address (or any other IP address).

Related tasks

[Define the Priority Order of Firewall Rules](#)

Create Firewall Services and Rules

You can create your own firewall services and rules if you want to allow or deny some Internet traffic.

Before starting to create a rule, select the security level to which you want to add this rule.

Note: You may not be able to add your own rules to all security levels.

1. [Create a Firewall Service](#)
You may need to create a new firewall service, for example, if you start using a new program which needs to connect to the Internet and which does not have a predefined service.
2. [Start Creating a Rule](#)
Enter a name for the rule and select whether the firewall rule denies or allows traffic.

3. [Select the IP Addresses](#)
Apply the rule to all network connections or specify the IP addresses and networks to which the new rule applies.
4. [Select the Services and Direction](#)
Select the services to which the firewall rule applies, and the direction of the traffic.
5. [Select Alerting Options](#)
Select how the product notifies you when the firewall rule denies or allows traffic.
6. [Check and Accept the Rule](#)
Check and accept the new rule.
7. [Define the Priority Order of Firewall Rules](#)
If you have created several new firewall rules, define their priority order.

Related concepts

[What Are Firewall Rules](#)

[What Are Firewall Services](#)

Related tasks

[Change the Security Level](#)

[How to Create a Rule for A Network Game](#)

[How to Create a Rule for Sharing Files on a Home Network](#)

[Viewing Firewall Services](#)

Create a Firewall Service

You may need to create a new firewall service, for example, if you start using a new program which needs to connect to the Internet and which does not have a predefined service.

The service defines the protocols and ports the program uses. To find out this information, consult the documentation of the program.

To create a firewall service:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the Services tab.
5. Click **Add**. The *Add New Service* dialog box opens.
6. In the **Name** field, enter a name for the service. Use a name that you can easily identify.
7. From the **Protocol** list, select the protocol for the service:
 - ICMP (1)
 - TCP (6)

- UDP (17)

If you want to use another IP protocol, enter the protocol number (0-255) in the field.

8. If the service uses the TCP or UDP protocol, define the initiator ports for the service. If the program documentation does not include the initiator ports, you can usually use any port number above 1023.
 - Next to the **Initiator ports** field, click **Edit**.
 - Add the ports:
 - To enter a single port, enter the port number in the **Single** field, for example, 1024.
 - To enter a port range, add the lowest and the highest port number of the range to the **Range** fields, for example, 1024-65535.
 - Click **Add To List**.
 - Repeat the steps a-c to add all necessary ports.
 - Click **OK**.
9. If the service uses the TCP or UDP protocol, define the responder ports for the service. The responder ports are usually mentioned in the program documentation.
 - Next to the **Responder ports** field, click **Edit**.
 - Add the ports:
 - To enter a single port, enter the port number in the **Single** field.
 - To enter a port range, add the lowest and the highest port of the range to the **Range** fields.
 - Click **Add To List**.
 - Repeat the steps a-c to add all necessary ports.
 - Click **OK**.
10. If the service uses the ICMP protocol, define the ICMP type and code for the service. Click **Edit** to enter the values in the *Type* and *Code* fields. The allowed values are 0-255.
11. If you will use this service for allowing inbound traffic, you can define whether you want to allow also broadcast and multicast traffic. This kind of traffic is created by streaming programs, such as web radio or television. To allow them, select the **Allow broadcasts** and **Allow multicasts** checkboxes. Usually, you can leave these checkboxes unselected.
12. In the *Add New Service* dialog box, click **OK**.

Your new service is now shown on the services list on the *Services* tab. To deny or allow the traffic that the service defines, you need to add the service to a firewall rule which allows outbound Internet connections.

Next topic: [Start Creating a Rule](#)

Related tasks

[Viewing Firewall Services](#)

[Select the Services and Direction](#)

Start Creating a Rule

Enter a name for the rule and select whether the firewall rule denies or allows traffic.

To start creating a rule:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Rules* tab.
5. Click **Add**. The *Add New Rule* dialog box opens.
6. In the **Name** field, enter a name for the rule. Use a name that you can easily identify.
7. To either deny or allow traffic, select either **Deny** or **Allow**.
8. To create a rule that is valid only when you have an active dial-up connection, select **Use this rule only with dial-up connection**. This option is relevant only if you use a modem or ISDN for your Internet connection. You may want to select this option, for example, if you use a laptop outside your home network and access the Internet through a modem or ISDN connection. Outside your home, your laptop is not protected by the router firewall, and you may want to create a stricter rule that denies all unnecessary inbound traffic and use this rule outside home. Usually, you do not have to create a rule, and the default security level protects your computer both inside and outside home.
9. Click **Next >**.

Previous topic: [Create a Firewall Service](#)

Next topic: [Select the IP Addresses](#)

Select the IP Addresses

Apply the rule to all network connections or specify the IP addresses and networks to which the new rule applies.

Note: The IPv6-related options are only available if your operating system is Microsoft Windows Vista.

To select the IP addresses:

1. Select one of the following options:
 - o To apply the rule to both IPv4 and IPv6 addresses, select **Any IP Address**.
 - o To apply the rule to all IPv4 addresses, select **Any IPv4 Address**.
 - o To apply the rule to all IPv6 addresses, select **Any IPv6 Address**.
 - o To apply the rule to specific IP addresses and networks, select **Custom** and click **Edit**. The *Addresses* dialog box opens.

- a. In the *Addresses* dialog box, select one of the following options on the *Type* list:

Type	Address Example
------	-----------------

Type	Address Example
IP address	192.168.5.16
DNS name	www.example.com
IP range	192.168.1.1-192.168.1.63
IP subnet	192.168.88.0/29
IPv6 address	2001:db8:85a3:8d3:1319:8a2e:370:733
IPv6 range	2001:db8:1234:: - 2001:db8:1234:FFFF:FFFF:FFFF:FFFF:FFFF
IPv6 subnet	2001:db8:1234::/48

- b. Enter the address in the **Address** field.
- c. To add the address to the addresses list, click **Add To List**.
- d. Repeat steps a-c to add all necessary addresses to the addresses list.
- e. Click **OK**.

2. Click **Next >**.

How can you define an IP subnet

If you want to define an IP subnet, use Classless Inter-Domain Routing (CIDR) notation. It is a standard notation that consists of a network address and subnet mask. For example:

Network Address	Subnet Mask	CIDR Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

Previous topic: [Start Creating a Rule](#)

Next topic: [Select the Services and Direction](#)




Select the Services and Direction




Select the services to which the firewall rule applies, and the direction of the traffic.

To select the services and direction:

1. Select the services to which you want to apply the rule:
 - If you want to apply the rule to all IP traffic, select **All IP traffic** on the list.
 - If the service you need is not on the list, you need to create it first.

The    icon appears in the *Direction* column for the services you selected.

2. For every service, select the direction of the traffic to which the rule applies. The direction is from your computer to the Internet or vice versa. To select the direction, click the    icon in the *Direction* column.

Direction	Explanation
	The service is allowed or denied in both directions.
	The service is allowed or denied if it is from the Internet to your own computer (inbound).
	The service is allowed or denied if it is from your own computer to the Internet (outbound).

3. Click **Next >**.

Previous topic: [Select the IP Addresses](#)

Next topic: [Select Alerting Options](#)

Related tasks

[Create a Firewall Service](#)

Select Alerting Options

Select how the product notifies you when the firewall rule denies or allows traffic.

To select the alerting option:

1. Select one of the following options:
 - If you do not want to be notified, select **No alert**. No alerts are generated to the alerts log, and no alert pop-ups are shown to you. We recommend that you select this option if you are creating a rule for allowing traffic.
 - If you want the product to generate alerts in the alerts log, select **Log**.
 - If you want the product to generate alerts in the alerts log and to show alert pop-ups to you, select **Log and pop-up**. Note that you have to turn on the alert pop-ups also in the *Internet Shield alerts* dialog box.
 - In the **Alert text** field, enter a description to be shown in the alerts log and pop-ups.
2. Click **Next >**.

Previous topic: [Select the Services and Direction](#)

Next topic: [Check and Accept the Rule](#)

Related tasks

[Turn the Internet Shield Alert Pop-Ups On or Off](#)

Check and Accept the Rule

Check and accept the new rule.

To do this:

1. Check the rule summary. If you need to edit the rule, click **< Previous**.
2. When you are satisfied with your new rule, click **Finish**.

Your new rule is now shown on the rules list on the *Rules* tab, and it is automatically turned on. If you have created several rules, you can now define their priority order.

Previous topic: [Select Alerting Options](#)

Next topic: [Define the Priority Order of Firewall Rules](#)

Define the Priority Order of Firewall Rules

If you have created several new firewall rules, define their priority order.

You may want to do this, for example, if a rule denies some traffic that you want to allow. In this case, you need to create a new "allow" rule and move this rule above the "deny" rule. In this way, the "allow" rule is first applied to traffic. You can only change the priority order of those rules that you have created yourself.

To define the priority order:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the **Rules** tab.
5. Click on the rule you want to move and with the mouse button pressed down, drag the rule to the new location in the table.

Rules are now applied to traffic according to the new priority order.

Previous topic: [Check and Accept the Rule](#)

Related concepts

[How Does the Priority Order of Firewall Rules Work](#)

Open a Port

You can open a port through the firewall if you want to allow some Internet traffic and you know the port number you want to open.

You may not be able to add your own rules to all security levels. Select the security level to which you want to add the new rule before you open the port.

When you open a port through the firewall, you create a new firewall rule and two new services.

1. Click the *Internet Shield* tab.
2. Click **Open a port**.
3. In the **Name** field, enter a name for the new firewall rule.
4. In the **Port number** field, define the responder port for the rule. The responder port is usually mentioned in the product documentation.
5. Click **OK**.

The new rule is added to the firewall rules list and two new services are created on the firewall services list for both the TCP and UDP protocols with the specified port number.

Turn a Firewall Rule On or Off

You can turn a firewall rule off to temporarily allow some traffic that the rule denies.

You can turn those rules on or off that you have created yourself.

To turn a rule on or off:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Rules* tab.
5. Do one of the following:
 - If you want to turn a rule off, clear the checkbox in the *Enabled* column.
 - If you want to turn the rule on, select the checkbox.

Depending on your selection, the firewall rule is now either on or off.

View Firewall Rules




You can view the currently active firewall rules to find out how the firewall allows or blocks traffic on your computer.

Each security level has its own set of active firewall rules. To view the rules:

1. Click the *Internet Shield* tab.

2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Rules* tab.

You can view a rules list, which contains the following information:

Field	Description
Enabled	If the checkbox is selected, the rule is currently on. If the checkbox is empty, the rule is currently off.
Name/Comment	Name of the rule. There are two types of rules: <ul style="list-style-type: none"> ○ Predefined rules: These rules are shown in gray. They have been predefined for the currently selected security level. ○ Your own rules: If you have added your own rules, they are shown in black above the <i>Your rules will be added here</i> row.
Type	Rule type: <ul style="list-style-type: none"> ○ : This rule allows network traffic. ○ : This rule denies network traffic. ○ : This rule generates alerts in the alert log and possibly shows an alert pop-up when the rule allows or denies network traffic.
Remote Host	IP addresses and networks to which the rule applies. If the rule applies to all IP addresses, this field shows one of the following values: <ul style="list-style-type: none"> ○ <i>0.0.0.0/0,::/0</i>: The rule applies to all IPv4 and IPv6 addresses. ○ <i>0.0.0.0/0</i>: The rule applies to all IPv4 addresses. ○ <i>::/0</i>: The rule applies to all IPv6 addresses.

5. To view the rule details, select a rule on the list and click **Details**.
 - If the rule has been predefined, the *Rule Details* dialog box opens and displays the predefined rule. After viewing the details, click **OK**.
 - If you have added the rule yourself, the *Rule Details* dialog box opens. Click **Next >** until you see a summary of the rule. After viewing the details, click **Cancel**.
- [Firewall Rule Details](#)
 Firewall rule details include the name and type of the rule, the IP addresses and services to which the rule applies, and alerting settings.

Firewall Rule Details

Firewall rule details include the name and type of the rule, the IP addresses and services to which the rule applies, and alerting settings.

You can view the following information in the *Rule Details* dialog box:

Field	Description
Rule name	Name of the rule.
Rule type	Type of the rule, which defines whether the rule allows or denies network traffic.
Remote address	IP addresses and networks to which the rule applies. If the rule applies to all IP addresses, the field shows one of the following values: <ul style="list-style-type: none">• <i>0.0.0.0/0,::/0</i>: The rule applies to all IPv4 and IPv6 addresses.• <i>0.0.0.0/0</i>: The rule applies to all IPv4 addresses.• <i>::/0</i>: The rule applies to all IPv6 addresses.
Services	The <i>Service</i> column shows the firewall services that the rule includes. The <i>Direction</i> column shows whether the rule applies to inbound services (<i>in</i>), outbound services (<i>out</i>) or <i>both</i> .
Alerting	Shows whether the rule generates alerts and shows alert pop-ups.
Alert text	If the rule generates alerts, shows the alert text that is shown in the alert log and pop-up.

Change a Firewall Rule

You can only change a firewall rule that you have created yourself.

To change a rule:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Rules* tab.
5. Select the rule and click **Details**. The *Rule Details* dialog box opens.
6. Make the necessary changes in each step and move to the next step by clicking **Next >**.
7. In the *Rule Details* dialog box, check the changes that you made.
8. If you are satisfied with the rule, click **Finish**.

The changes that you made are applied to the rule.

Examples of Creating Firewall Rules

You can create a new firewall rule if you want to play a new network game, or share files on your home network.

- [How to Create a Rule for A Network Game](#)
This is an example of how to create firewall services and a firewall rule for an imaginary network game called Game_1.
- [How to Create a Rule for Sharing Files on a Home Network](#)
This is an example of creating a new firewall rule for Windows file sharing to share files between computers on your home network.

How to Create a Rule for A Network Game

This is an example of how to create firewall services and a firewall rule for an imaginary network game called Game_1.

For creating the firewall services, you need to know the protocols that the game uses. You also need to know the ports that the game uses for inbound connections from the game server to your computer. In this case, they are the following:

Protocol	Port Type	Location	Ports
UDP	Initiator	Game server	1024
UDP	Responder	Own computer	8889, 9961
TCP	Initiator	Game server	1025
TCP	Responder	Own computer	17475, 9961

Note: You do not have to create firewall services or a firewall rule for outbound connections from your computer to the game server.



To create the services and a rule for the inbound connections:

1. Add the new services as follows:

Step	Example
Enter a name for the first service	Service_Game_1_UDP
Select the protocol	UDP
Enter the initiator port	1024

Step	Example
Enter the responder ports	8889, 9961
Enter a name for the second service	Service_Game_1_TCP
Select the second protocol	TCP
Enter the initiator port	1025
Enter the responder ports	17475, 9961

2. After you have added the services, they are shown on the services list.
3. Add a new firewall rule as follows:

Step	Example
Enter a name for the rule	Rule_Game_1
Select the rule type	Allow
Select the IP addresses	Any address
Select the services	Service_Game_1_UDP, Service_Game_1_TCP
Select the direction	 ←  (from the Internet to your computer)
Select the alert type	No alert

After you have added the rule, it becomes active and is shown on the rules list.

Related tasks

[Create Firewall Services and Rules](#)

How to Create a Rule for Sharing Files on a Home Network

This is an example of creating a new firewall rule for Windows file sharing to share files between computers on your home network.

If you use a router on your network, check the Dynamic Host Configuration Protocol (DHCP) settings of your router to find out the IP address range allocated to your home network. For more information, consult the router documentation.

The most usual IP address range for home networks is 192.168.1.1 - 192.168.1.254. If you want to share files between all your computers, you have to create the same rule on all of the computers.

To create the rule:



1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Rules* tab.
5. Click **Add**.
6. Enter a name and select the rule type:

Step	Example
Enter a name for the rule	FileSharing
Select the rule type	Allow

7. Select the IP addresses:

Step	Example
<ol style="list-style-type: none"> a. Click Custom. b. Click Edit. c. Select IP range and enter the addresses of your computers in the field. d. Click Add To List. 	192.168.1.1 - 192.168.1.254

8. Select the services and direction:

Step	Example
Select the services that Windows file sharing uses	<ol style="list-style-type: none"> a. SMB over TCP/IP (TCP) b. SMB over TCP/IP (UDP) c. Windows file sharing and network printers d. Windows network browsing e. ICMP / Internet Control Message Protocol
Select the direction for both services	 ←  (from the Internet to your computer)

- o Select the alerting type:

Step	Example
Select the alerting type	No alert

- Check the summary of the rule and click **Finish**. Your new rule is now shown on the rules list on the *Rules* tab, and it is automatically turned on.
- Test that the rule works. To do this, use Windows file sharing to share a folder or file and check whether you can access the folder or file from all of your computers.

Tip: If you want to share the printer on your home network, create a similar rule. In this case, you have to only create an inbound "allow" rule on the computer to which the printer is connected.

Related tasks

[Create Firewall Services and Rules](#)

Firewall Settings

On the *Settings* tab, you can change the IPv6 settings and the alerting level, and allow all traffic between computers on a home network.

The *Settings* tab also contains the **Block IP fragments shorter than** field. The firewall blocks IP packet fragments that are shorter than the recommended limit shown in this field. Short IP packet fragments may indicate a fragmentation attack, which may cause your computer to crash. We recommend that you do not change the limit in this field.

- [Change the IPv6 Settings](#)
On the Settings tab, you can define how the firewall handles IPv6 traffic.
- [What to Do if You Share an Internet Connection](#)
If you want to share an Internet connection on your computer with the rest of your home network, you need to allow all traffic through the firewall between these computers.

Change the IPv6 Settings

On the *Settings* tab, you can define how the firewall handles IPv6 traffic.

If your operating system is Microsoft Windows Vista, you can either block all IPv6 traffic or apply normal firewall rules to the traffic. If you use some other operating system, you can only block all or allow all IPv6 traffic.

To change the IPv6 settings:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the *Settings* tab.

5. To define how the firewall handles IPv6 traffic, select one of the following options on the *Select IPv6 traffic filtering options* list:
 - If you use Microsoft Windows Vista:
 - **Block:** Blocks all IPv6 traffic. We recommend that you keep this option selected.
 - **Normal:** Normal firewall rules define whether IPv6 traffic is allowed or blocked. You may want to select this option if you are using the IPv6 protocol on your computer.
 - If you use some other operating system:
 - **Block:** All IPv6 traffic is blocked. We recommend that you keep this option selected.
 - **Allow:** Allows all IPv6 traffic. You may want to select this option if you are using the IPv6 protocol on your computer.
Note: Allowing all IPv6 traffic is a security risk because no firewall rules are applied to the IPv6 traffic.

6. Click **OK**.

The changes that you made to the IPv6 settings are now active.

What to Do if You Share an Internet Connection

If you want to share an Internet connection on your computer with the rest of your home network, you need to allow all traffic through the firewall between these computers.

Note:

Allow all traffic through the firewall only if you use Windows Internet Connection Sharing. If you want to share other resources, such as drives, files or printers, we recommend that you create new firewall rules for this purpose.

You can allow all traffic through the firewall by defining the connection between the home network and the computer with the Internet connection as trusted. You can define a trusted network interface, if:

- You have a computer with an Internet connection.
- This computer has two network interface cards: One for the Internet connection, and one for the home network connection.
- You have activated Windows Internet Connection Sharing on the computer which has the Internet connection.
- You have installed our product with Internet Shield to all of your computers. This makes sure that it is safe to define a trusted interface between your computers.

To define the trusted network interface, you need to select the network interface card (adapter) which connects the computer to the home network.

To select the network interface card on the computer with the Internet connection:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Firewall*.
4. Click the **Settings** tab.
5. On the **Trusted network adapter** list, select the network interface card (adapter) which connects your computer to the home network. The IP address of the computer is shown in the **IP address** field.
Note: Because the firewall allows all traffic through the selected network interface, make sure that you do not select the Internet interface as trusted. If you do this, the firewall does not protect your computer anymore.
6. Click **OK**.

The firewall now allows all traffic between the computer with the Internet connection and your home network, and you can use the Internet from all your computers.

What If You Use a Digital TV Card

If you use a digital TV card, and the television picture freezes, you may also have to define the interface to the television as trusted.

Controlling Internet Connections for Applications

Application Control prevents harmful programs from connecting to the Internet.

Application Control protects you mainly against outbound threats that are caused by programs on your computer. Typically, when a program tries to connect to the Internet, Application Control shows a pop-up. In this pop-up you can allow or deny the connection:

- If you trust that the program is safe, you can allow the connection. For example, you can consider the program safe if you have just opened it yourself. When you allow the connection, the firewall opens a port for this program and allows the connection for as long as the program is open. When you close the program, the firewall closes the port.
- If you do not trust the program, you need to deny the connection. For example, a program can be unsafe if you do not recognize it or you have not installed it yourself.

Depending on your Application Control settings, Application Control pop-ups may not be shown for programs that System Control considers safe. These programs are allowed to connect to the Internet automatically.

Application Control also asks you whether you want to allow connections from the Internet to the programs on your computer. This happens, for example, if you are using Skype.

Note: If a program does not work on your computer, do not turn off Application Control. If you do, the level of protection reduces on your computer. Instead, change the Application Control settings or firewall rules.

What Is the Difference Between the Firewall and Application Control

A firewall provides you general protection on the network level, whereas Application Control allows you to control the use of specific programs. The firewall protects you against threats that are caused by connections from the Internet to your computer (inbound). The firewall allows or denies connections on the basis of the IP protocols and IP addresses that the connections use.

Application Control mainly protects you against threats that are caused by connections from your computer to the Internet (outbound). Application Control allows or denies connections on the basis of the programs that create the connections.

- [What to Do If an Application Control Pop-Up Appears](#)
If an Application Control pop-up appears, you need to decide whether you allow or deny a connection attempt for the program that is shown in the pop-up.
- [Allow or Deny Connections for Programs](#)
You can allow or deny Internet connections for programs on the Applications tab.
- [Turn Application Control Pop-Ups On or Off](#)
You can turn the Application Control pop-ups on or off.
- [What to Do If a Program Stops Working](#)
If you start using a new program, for example a network game, it may stop working if it cannot connect to the Internet.

What to Do If an Application Control Pop-Up Appears

If an Application Control pop-up appears, you need to decide whether you allow or deny a connection attempt for the program that is shown in the pop-up.

Application Control pop-ups may indicate malicious activity, such as trojans, worms or spyware. On the other hand, pop-ups are also shown when you use the programs on your computer normally.

To allow or deny a connection attempt:

1. Check the information about the connection attempt in the pop-up.
2. To view details of the connection attempt, such as the name of the program and IP address of the remote computer, click **Details >>**.
3. If you do not want pop-ups to be shown to you about this program anymore, select the **Do not show this dialog for this program again** checkbox.
4. Either allow or deny the connection:
 - Click **Allow** if you are sure that the connection attempt is safe. You can allow the connection in the following cases:

Pop-up Type	Description	Click Allow if
New connection attempt (outbound)	A client program on your computer is trying to connect to the Internet.	You have started this program yourself for the first time.
Changed application	A client program on your computer is trying to connect to the Internet but it	You have updated the program on your

Pop-up Type	Description	Click Allow if
(outbound)	has been changed since the previous connection.	computer since you last used it.
New server application (inbound)	A program on your computer is trying to act as a server and wants to start listening for inbound connections.	You have started the server program on your computer yourself.
Changed application (inbound)	A server program on your computer wants to start listening for inbound connections but it has changed since the previous connection attempt.	You have updated the server program on your computer since you last used it.

- Click **Deny** if you are not sure that the connection attempt is safe.

Depending on the selected action, the connection is either allowed or denied. If you selected the **Do not show this dialog for this program again** checkbox, the program is added to the list of allowed or denied programs on the *Applications* tab. No pop-ups are shown anymore about the connection attempts of this program.

Your network administrator may have denied the use of certain programs for security reasons. In this case, two kinds of pop-ups may be shown to you:

Pop-up Type	Description
Allowed application	You have started a program that your administrator does not recommend to be used. You can use the program only this one time. You need to update the program to the latest version, or use another program.
Denied application	You have started a program that your administrator has denied. You must use another program.

- [Safe and Unsafe Programs and Connection Attempts](#)
Before allowing a connection in an Application Control pop-up, consider whether the program is safe.

Safe and Unsafe Programs and Connection Attempts

Before allowing a connection in an Application Control pop-up, consider whether the program is safe.

Which programs and connection attempts you can consider safe

- A known program that you have started yourself.
- Microsoft Windows operating system, which connects to the Internet for update services.

Which programs and connection attempts you cannot consider safe

- Any program that you have received from an unknown source.
- Any program that you have not installed yourself, or you do not recognize.
- Any program, which you consider safe but which tries to connect to the Internet or act as a server without you starting it.

Allow or Deny Connections for Programs

You can allow or deny Internet connections for programs on the *Applications* tab.

You can, for example, allow a connection for a program that you have accidentally denied in an Application Control pop-up.

By default, the *Applications* tab shows the following programs:

- When the *Prompt for new applications* option is on: programs, which you have allowed or denied, and for which you have selected the **Do not show this dialog for this program again** option in an Application Control pop-up.
- When the *Allow and log new applications* option is on: allowed programs.
- The programs that you have manually added to the programs list on this tab.

This tab does not show automatically allowed operating system programs or programs that System Control considers safe.

To allow or deny the connection for a program:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Application Control*.
4. Click the *Applications* tab.
5. Select the program and click **Details**. The *Application Details* dialog box opens.
6. Under *Outbound (client) connection*, select the suitable option:
 - **Deny**: If you want to deny the program from connecting to the Internet the next time the program is started.
 - **Allow**: If you want to allow the program to connect to the Internet the next time the program is started.
 - **Prompt**: If you want that an Application Control pop-up is shown the next time the program tries to connect to the Internet. In this pop-up, you can either allow or deny the connection.
7. Under *Inbound (server) connection*, select the suitable option:
 - **Deny**: If you want to deny connections from the Internet to the program.
 - **Allow**: If you want to allow connections from the Internet to the program.

- **Prompt:** If you want that an Application Control pop-up is shown the next time there is a connection attempt from the Internet to this program. In this pop-up, you can either allow or deny the connection.

8. Click **OK**.

Tip: You can allow or deny Internet connections for a new program even before you have started to use it. You can do this by clicking the **Add** button and selecting the program file. After this, you can either allow or deny the inbound and outbound connections for this program.

Turn Application Control Pop-Ups On or Off

You can turn the Application Control pop-ups on or off.

If you turn Application Control pop-ups off, the product allows connections for all programs automatically.

To turn Application Control pop-ups on or off:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Application Control*.
4. Click the *Settings* tab.
5. Select one of the following options:
 - *Allow and log new applications:* Select this option if you want to turn Application Control pop-ups off. The product allows connections for all programs automatically.
 - *Prompt for new applications:* Select this option if you want to turn Application Control pop-ups on. A pop-up is shown to you the first time a new program tries to open a connection.
6. If you do not want Application Control pop-ups to be shown for programs that System Control considers safe, select **Do not prompt for applications that System Control has identified**. We recommend that you keep this checkbox selected.
7. Click **OK**.

Depending on your selection, the Application Control pop-ups are now either turned on or off.

What to Do If a Program Stops Working

If you start using a new program, for example a network game, it may stop working if it cannot connect to the Internet.

This can happen, for example, for the following reasons:

- Your current security level is very strict, and it denies Internet connections for most of the programs, including the network game you are using.
- You have missed an Application Control pop-up and the pop-up has remained active on the background.
- You have accidentally denied the connection in the pop-up.

To make sure that the program can connect to the Internet, do the following:

1. Click the *Internet Shield* tab.
2. Next to *Internet Shield*, check the current security level. If it is a very strict one, change it to a less strict:
 - a. Click **Change**.
 - b. Read the security level descriptions carefully.
 - c. Select a suitable security level and click **OK**.
3. Start the program and check whether it works now.
4. If the program does not work, turn Application Control pop-ups temporarily off to allow all connections for new programs.
 - a. To do this, next to *Application Control*, click **Change**. *Advanced Application Control* settings page opens.
 - b. Select **Allow and log new applications** and click **OK**.
5. Start the program and check whether it works now.
6. If the program works, turn Application Control pop-ups back on.
 - a. To do this, next to *Application Control*, click **Change**. *Advanced Application Control* settings page opens.
 - b. Select **Prompt for new applications** and click **OK**.

Preventing Intruders from Accessing Your Computer

Intrusion Prevention protects against network attacks aimed at open ports on your computer.

Intrusion Prevention uses predefined rules for recognizing network attacks. These rules contain information on known malicious traffic. When Intrusion Prevention recognizes traffic that matches a rule, it blocks the traffic (if the **Block and log** option is on) and generates an alert to the Internet Shield alerts log. Depending on your settings, an Internet Shield alert pop-up may also appear.

Intrusion Prevention recognizes and prevents malicious traffic caused by network worms such as the Sasser worm. The Sasser worm infects vulnerable systems by sending malicious traffic to the Microsoft network share service on TCP port 445. This service is used for sharing printers and files on a network. The worm opens a TCP connection to the port, and sends malicious traffic through the port. The traffic overflows the system, and may cause, for example, the whole system to crash.

Note: Do not turn Intrusion Prevention off. If you do, the level of protection on your computer reduces.

What Is the Difference Between the Firewall and Intrusion Prevention

The difference to the firewall is that Intrusion Prevention blocks only traffic that it considers malicious, and lets other traffic through a port. The firewall either allows or blocks all traffic that goes through the port.

- [Select How Intrusion Attempts Are Handled](#)
On the Intrusion Prevention tab, you can select how intrusion attempts are handled.

Select How Intrusion Attempts Are Handled

On the *Intrusion Prevention* tab, you can select how intrusion attempts are handled.

The intrusion attempts can be either automatically blocked and logged, or only logged.

To select how intrusion attempts are handled:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Intrusion Prevention*.
4. Select one of the following options:
 - **Block and log attempt:** Select this option if you want to both block and log the intrusion attempts. The attempts are blocked and information about the attempts is shown in the *Internet Shield alerts* dialog box.
 - **Log:** Select this option if you want to only log the intrusion attempts. Information about the attempts is shown in the *Internet Shield alerts* dialog box.
5. If you want that an *Internet Shield Alert* pop-up is shown if an intrusion attempt is suspected, select **Alert when intrusion attempt is suspected**.
6. Click **OK**.

The *Internet Shield* page now shows the changed intrusion prevention setting.

[concept_718B3C5B42754343848AB83CFF222B01](#)

Controlling Dial-Up Connections

Dial-up Control prevents malicious dialer programs from opening connections to expensive pay-per-minute phone numbers.

Malicious dialer programs may try to close your Internet connection and open a new dial-up connection to another number. The connection to this number may be very expensive and benefits the creator of this dialer program.

By using Dial-up Control, you can prevent these malicious dialer programs from closing and opening new connections. Dial-up Control also prevents you from dialing accidentally to wrong or expensive numbers. You can make sure that dial-up connections are safe by defining:

- the numbers to which programs can open a dial-up connection, and
- the programs that are allowed to close dial-up connections.

Note: Dial-Up Control is meant for users who use a modem or ISDN for their Internet connection.

Virus & Spy Protection recognizes the malicious dialer programs as spyware and can remove them from your computer. If a new malicious dialer program is not recognized, Dial-up Control prevents this dialer program from opening any dial-up connections.

If you suspect that you have an unrecognized dialer on your computer, you can send the dialer file as a sample to F-Secure. After that, F-Secure updates the virus and spyware definition databases and you can scan your computer again. The dialer is then recognized and can be removed from your computer.

- [What to Do If a Dial-Up Control Pop-Up Appears](#)
If a New Dial Attempt pop-up appears, you can either allow or deny the dial-up connection.
- [Add, Edit or Remove Phone Numbers](#)
You can add phone numbers to the numbers list on the Number list tab if you want to allow or deny dial-up connections to these numbers.
- [View Programs that Are Allowed to Close Dial-Up Connections](#)
You can view safe programs, which are allowed to close dial-up connections, on the Settings tab.
- [View Dial-Up Connection Attempts](#)
By activating the logging for Dial-up Control, you can view the dial-up connection attempts that the product has detected.
- [What to Do If You Cannot Access the Internet Through Your Modem](#)
If the dial-up connection to your Internet Service Provider (or to some other phone number) stops working, check that you have not accidentally denied connections to that number.

What to Do If a Dial-Up Control Pop-Up Appears

If a *New Dial Attempt* pop-up appears, you can either allow or deny the dial-up connection.

To allow or deny a dial-up connection:

1. Check the name of the program.
2. Check the phone number.
3. Either allow or deny the dial-up connection:
 - If the number is correct (given by your service provider) and the program is the one you have opened yourself:
 - a. Select **Remember this decision**.
 - b. Click **Allow**.
 - If the number is wrong, or the connection was opened automatically:
 - a. Select **Remember this decision**.
 - b. Click **Deny**.

The connection is allowed or denied based on the decision you made. The number and information about the program is added to the numbers list on the *Number list* tab. After this:

- If you have allowed the connection, no pop-up is shown if a program tries to open a dial-up connection to this number again.
- If you have denied the connection, and a program tries to open a dial-up connection to this number, a *Denied Dial Attempt* pop-up appears. Close the pop-up by clicking **Close**.



Note:

A *Close Connection* pop-up may appear if a program tries to close a dial-up connection. If the program is the one that you have closed yourself, you can allow the closing of the dial-up connection. You can do this by clicking **Allow**. If the program is not the one you have closed, you must deny the closing by clicking **Deny**. Denying the closing attempt makes sure that no malicious dialer programs can close your Internet connection and open a new connection to another number.

Add, Edit or Remove Phone Numbers

You can add phone numbers to the numbers list on the *Number list* tab if you want to allow or deny dial-up connections to these numbers.

To add a new number to the list:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Dial-up Control*.
4. Click the *Number list* tab.
5. Click **Add**. The *Add Number/Range* dialog box opens.
6. In the **Description** field, enter a description for the number.
7. In the **Number** field, enter the number:
 - You can use the following characters: #*1234567890.
 - You can use an area code and country code, for example, 040-1234567, 00 358 9 123 4567.
 - You can use other characters, such as a space or a hyphen, for grouping the numbers. However, note that Dial-up Control disregards other characters than the ones mentioned above. For example, it treats 09-1234567 as the same number as 091234567.
 - You can enter a number range by using the following wildcards:
 - "?" to replace any single number. For example, to deny the dial-up connection to certain service numbers, enter 0900?234567.
 - "X" or "x" to replace one or several numbers. You can use this wildcard, for example, if you want to deny dial-up connections to abroad. If you normally use "00" to dial abroad, enter "00x" to deny all dial-up connections abroad.
8. Select whether you want to deny or allow the dial-up connection attempts:
 - Select **Denied** to block all dial-up connection attempts to the number you entered.
 - Select **Allowed** to allow dial-up connections to the number you entered.
9. Click **OK**. The *Number list* tab now shows the phone number or number range, and the action you selected:
 - If you allowed the number, the  icon is shown in front of the number.
 - If you denied the number, the  icon is shown in front of the number.
10. If you need to change the priority order of numbers click on the number on the list you want to move and with the mouse button pressed down, drag the number to the new location in the table.

Note: The *Number list* tab may include some predefined numbers if your service provider has denied or allowed dial-up connections to certain numbers. You cannot change or remove these numbers.

View Programs that Are Allowed to Close Dial-Up Connections

You can view safe programs, which are allowed to close dial-up connections, on the *Settings* tab.

This tab shows the following programs:

- Safe programs that are always allowed to close dial-up connections, for example, the web browser that you are using.
- Programs for which you are asked whether you want to allow or deny the closing of the dial-up connection. The tab shows the programs that you have allowed to close dial-up connections.

This tab does not show the denied programs. If you have denied an application to close the dial-up connection in a pop-up, the application cannot close the connection until you restart the computer. If you allow an application to close the dial-up connection, the application can close it any time and you do not have to make the selection again.

To view the programs:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Dial-up Control*.
4. Click the *Settings* tab. This tab shows a list of programs that are allowed to close dial-up connections.

View Dial-Up Connection Attempts

By activating the logging for Dial-up Control, you can view the dial-up connection attempts that the product has detected.

By default, the Dial-up Control logging is off.

To turn the logging on:



1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Dial-up Control*.
4. Click the *Settings* tab.
5. To turn logging on, select **Enable Dial-up Control log**.
6. To view the log that has been created, click **Show Log**. You can view the following information:
 - Attempts to open or close dial-up connections.

- Whether the attempts were allowed or denied.
- Dialed phone numbers.

What to Do If You Cannot Access the Internet Through Your Modem

If the dial-up connection to your Internet Service Provider (or to some other phone number) stops working, check that you have not accidentally denied connections to that number.

To do this:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Dial-up Control*.
4. Click the *Number list* tab.
5. Check whether the number that you tried to dial to is on the list. If it is, and it is denied (the  icon is shown in front of it), do the following:
 - a. Select the number.
 - b. Click **Edit**.
 - c. Select **Allowed**.
 - d. Click **OK**. The icon in front of the number has changed to .

Test if the connection to the number works now.

Viewing the Internet Shield Status, Alerts and Log Files

By viewing the Internet Shield status, alerts and log files, you can find out how Internet Shield protects your computer.

- [Check the Status of Internet Shield](#)
You can check the status of Internet Shield components on the advanced Internet Shield page.
- [Check the Current Internet Shield Settings](#)
You can check the current Internet Shield settings on the Internet Shield page.
- [Check the Number of Recent Internet Shield Actions](#)
You can check the number of recent alerts and blocked programs on the Internet Shield page.
- [Check Internet Shield Statistics](#)
You can check how many Internet connections were allowed or denied and how many packets were sent through those connections.
- [View Internet Shield Alerts](#)
You can view a list of all generated Internet Shield alerts.
- [View Log Files](#)
Information about the Internet Shield actions and network traffic is gathered into log files.

Check the Status of Internet Shield

You can check the status of Internet Shield components on the advanced *Internet Shield* page.

To do this:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield* on the navigation pane on the left.
4. On this page, you can view whether the Internet Shield components, such as Application Control, are on or off.

Note: Do not turn off any of the components unless absolutely necessary.

Check the Current Internet Shield Settings

You can check the current Internet Shield settings on the *Internet Shield* page.

To do this:

1. Click the *Internet Shield* tab.
2. You can view the following settings:
 - Next to *Internet Shield*, you can view the current security level.
 - Next to the Internet Shield components, you can view their current settings. For example, the Application Control setting can be *Prompt* or *Allow and log*.

Check the Number of Recent Internet Shield Actions

You can check the number of recent alerts and blocked programs on the *Internet Shield* page.

To do this:

1. Click the *Internet Shield* tab.
2. You can view the following information:
 - *Applications allowed/denied*: Shows how many programs have been allowed or blocked to create connections.
 - *Recent alerts*: Shows how many Internet Shield alerts have been generated after you opened your computer. To view a list of alerts, click **View**.
 - *Latest alert*: Shows the time of the latest Internet Shield alert. To view details of the alert, click **Details**. You can view the following information:
 - Time of the latest alert, the IP address and service that generated the alert, and whether the traffic was inbound or outbound.
 - *Top 5 blocked addresses* shows the 5 IP addresses which have generated the most alerts within 24 hours. The firewall has blocked the traffic from your computer to these IP addresses, or from these IP addresses to your computer.

- *Top 5 blocked services* show the 5 services that have generated the most alerts within 24 hours. These services have generated traffic that the firewall has blocked.

After viewing the information, click **Close**.

Check Internet Shield Statistics

You can check how many Internet connections were allowed or denied and how many packets were sent through those connections.

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Statistics*.

You can see how many connections and packets were allowed and denied for both in-bound and out-bound connections.

View Internet Shield Alerts

You can view a list of all generated Internet Shield alerts.

The list contains alerts that the firewall and Intrusion Prevention have caused.

To view the list:

1. Click the *Internet Shield* tab.
2. Next to *Recent alerts*, click **View**. The *Internet Shield alerts* dialog box opens and shows the following information:

Field	Description
Time	Time of the alert.
Remote address	IP address of the computer from which you have received traffic, or sent traffic to.
Hits	Shows how many times a similar alert has been generated.
Description	An alert text that has been added for the firewall rule. If an intrusion attempt has caused the alert, the field shows information on the intrusion attempt pattern.

3. To view alert details, select the alert and click **Details**.
4. To move to the next or previous alert, click the **< Prev** or **Next >** button.
5. After viewing the details, click **Close** to close the *Internet Shield alerts* details dialog box.
6. Click **Close** to close the *Internet Shield alerts* list dialog box.

- [Internet Shield Alert Information](#)
An Internet Shield alert contains information on the traffic that caused the alert.

Internet Shield Alert Information

An Internet Shield alert contains information on the traffic that caused the alert.

An Internet Shield alert contains the following information:

Field	Description
Description	An alert text that has been added for the firewall rule. If the alert is caused by an intrusion attempt, the alert shows information on the intrusion attempt pattern.
Action	Shows what happened, for example that the firewall blocked or allowed the traffic.
Time	The date and time when the alert was generated.
Direction	Shows whether the traffic is inbound or outbound (from a remote computer to your own computer or vice versa).
Protocol	The used IP protocol.
Services	Shows the firewall services to which this traffic matched.
Remote address	The IP address of the remote computer.
Remote port	The port on the remote computer.
Local address	The IP address of your own computer.
Local port	The port on your own computer.

View Log Files

Information about the Internet Shield actions and network traffic is gathered into log files.

There are two log files, the action log and packet log, which you can open for viewing on the *Logging* page. On this page, you can also view the location of these files. Log files are mainly aimed at experienced users who are familiar with computer networks.

Action log

The action log is a text file (`action.log`) that automatically collects information about the Internet Shield actions. You may want to open the action log for viewing if a program cannot connect to the Internet, and you want to check if Application Control denies the connection. The maximum size of the file is 10 MB. After the file becomes full, the old log entries are deleted.

Packet log

The packet log collects information about the IP network traffic. By default, the packet logging is turned off. You can turn the packet logging on if you have created your own set of firewall rules, and want to check how they block traffic. You can also do this if you suspect malicious network activity.

Information is gathered into 10 files (`packetlog.0-packetlog.9`). Each time you turn on the logging, the packet log is collected into a new file. After the tenth file becomes full, the next log is collected again to the first file. In this way, you can view the previous logs while a new log is generated.

In addition to the IP traffic, the packet log also collects information about other types of network traffic, for example, about the protocols needed by your Local Area Network (LAN). This information includes, for example, routing information.

The packet log is in hexadecimal format and supports tcpdump format. This allows you to open the log files also in a packet logging program other than the default packet log viewer. You can also use a network protocol analyzer program to analyze the contents further.

- [View the Action Log](#)
If a program, such as a network game, does not work, you can check in the action log if Application Control has denied the program from connecting to the Internet.
- [Use Packet Logging for Monitoring Network Traffic](#)
You can start packet logging if you want to gather information about the IP network traffic.

View the Action Log

If a program, such as a network game, does not work, you can check in the action log if Application Control has denied the program from connecting to the Internet.

To view the action log:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Logging*.
4. Click **Show Action Log**.

The action log opens in a default text editor or viewer, for example, Notepad.

- [Action Log Examples](#)
The action log shows information about opened connections and firewall rule changes.

Action Log Examples

The action log shows information about opened connections and firewall rule changes.

Opening a connection

The following is an example of a log entry, which is created when you open your Internet Explorer and a connection is created to an HTTP server:

Date	Time	Type	Internal reason	Program	Control action	Network action	Protocol	Remote IP address	Remote port
2007-03-07	T13:07:15+02:00	info	appl control	C:\PROGRA~1\INTERN~1\iexplore.exe	allow	connect out	6	10.0.1.14	80

Receiving a connection

The following is an example of a log entry, which is created when a program on your computer is acting as a server for other computers. These other computers can connect to this server program through the port that Application Control has opened on your computer (dynamic firewall rule):

Date	Time	Type	Internal reason	Program	Control action	Network action	Protocol	Remote IP address	Local port
2007-03-04	T13:08:15+02:00	info	appl control	unknown	allow	receive	17	10.0.1.14	1386

Adding and removing a dynamic firewall rule

The following is an example of two firewall rule log entries:

- The first entry shows that Application Control has added a dynamic firewall rule. The rule allows a temporary inbound connection for a program.
- The second entry shows that Application Control has removed the dynamic firewall rule, and the connection has been closed.

Date	Time	Alert type	Rule type	Action	Remote IP address range minimum	Remote IP address range maximum	Remote port range from	Remote port range to	Local port range from	Local port range to	Rule action
2007-	T13:06:59+02:00	info	dynamic	added	0.0.0.0	255.255.255	0	65535	371	371	allow

Date	Time	Alert type	Rule type	Action	Remote IP address range minimum	Remote IP address range maximum	Remote port range from	Remote port range to	Local port range from	Local port range to	Rule action
03-05			rule			5.0					
2007-03-05	T13:07:23+02:00	info	dynamic rule	removed	0.0.0.0	255.255.255.0	0	65535	371	371	allow

Use Packet Logging for Monitoring Network Traffic

You can start packet logging if you want to gather information about the IP network traffic.

- [Start Packet Logging](#)
You can start packet logging if you suspect malicious network activity, or for example, a network game stops working.
- [View the Packet Log](#)
After you have generated a packet log, you can open it for viewing.

Start Packet Logging

You can start packet logging if you suspect malicious network activity, or for example, a network game stops working.

To start logging:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Logging*.
4. Use the recommended logging time and file size that are shown in the **Logging time** and **Max log file size** fields. You can also change them if you want to.
5. Click **Start Logging**. A new file is added to the log files list. The size of the file increases as information is gathered in the file. If the list already contains 10 log files, the next log is gathered into an existing file.
6. To stop the logging manually, click **Stop Logging**. The logging stops automatically after the defined logging time period has elapsed, or the defined maximum log file size has been reached.

A new log file is generated and added to the log files list.

Related tasks

[View the Packet Log](#)

View the Packet Log

After you have generated a packet log, you can open it for viewing.

To view the packet log:

1. Click the *Internet Shield* tab.
2. Click **Advanced**.
3. Select *Internet Shield > Logging*.
4. Select the packet log you want to view and click **Details**. The default packet log viewer opens. The upper pane of the window shows all the logged connections.

You can view the following information:

Field	Description
Time	Time in seconds from the moment when logging was started. If the defined logging time is 60 seconds, the starting time for the first packet is close to 0 seconds, and the starting time for the last packet is close to 60 seconds.
Drop (dir)	Shows whether the firewall let through or dropped the packet, and shows the direction of the packet: <ul style="list-style-type: none">• <i>No</i>: Allowed the packet.• <i>Yes</i>: Dropped the packet.• <i>In</i>: Inbound packet.• <i>Out</i>: Outbound packet. <p>This information is not available if you view the file in a packet logging program other than the default packet log viewer.</p>
Protocol	The used IP protocol.
Source	Source IP address of the packet.
Destination	Destination IP address of the packet.
ID	IP packet header information: Identifier of the packet.
TTL	IP packet header information: Time To Live value of the packet defines the number of network devices through which the packet can travel before it is discarded.
Len	IP packet header information: Total length of the packet.

Field	Description
Description	Description of the packet.

The pane on the right shows you the traffic types and their information.

The lower pane of the window shows the information in hexadecimal and ASCII format.

If you want to view all types of network traffic (and not only IP traffic), clear the **Filter non IP** checkbox.

Related tasks

[Start Packet Logging](#)

Automatic Updates

Automatic Update Agent keeps the protection on your computer updated.

The product retrieves the latest updates to your computer when you are connected to the Internet. It detects the network traffic and does not disturb other Internet use even with a slow network connection.

- [Checking the Update Status](#)
View the date and time of the latest update.
- [Changing the Internet Connection Settings](#)
You can configure how your computer is connected to the Internet so you can receive updates automatically.

Checking the Update Status

View the date and time of the latest update.

When automatic updates are turned on, Automatic Updates keep the product up-to-date any time you are connected to the Internet.

To make sure that you have the latest updates:

1. Click the *Automatic Updates* tab.
2. **Last update check** displays the time of the latest update.
3. Click **Check now**. Automatic Update Agent connects to the Internet and checks for the latest updates. If the protection is not up-to-date, it retrieves the latest updates.
Note: If you are using a modem, or have an ISDN connection to the Internet, the connection must be active to check for updates.

Changing the Internet Connection Settings

You can configure how your computer is connected to the Internet so you can receive updates automatically.

To change your Internet connection settings:

Note: Usually there is no need to change the default settings.

1. Click the *Automatic Updates* tab.
 2. Click **Advanced**.
 3. Click **Connection**.
 4. On the **Internet connection** list, select how your computer is connected to the Internet.
 - Select **Assume always connected** if you have a permanent network connection.
Note: If your computer does not actually have the permanent network connection and is set up for dial-on-demand, selecting **Assume always connected** can result in multiple dial-ups.
 - Select **Detect connection** to retrieve updates only when the product detects an active network connection.
 - Select **Detect traffic** to retrieve updates only when the product detects other network traffic.
Tip: If you have an uncommon hardware configuration that causes the **Detect connection** setting to detect an active network connection even when there is none, select **Detect traffic** instead.
 5. On the **HTTP Proxy** list, select whether or not your computer uses a proxy server to connect to the Internet.
 - Select **No HTTP Proxy** if your computer is connected to the Internet directly.
 - Select **Manually configure HTTP proxy** to configure the HTTP proxy settings.
 - Select **Use my browser's HTTP proxy** to use the same HTTP proxy settings that you have configured in your web browser.
- [Configuring the HTTP Proxy Manually](#)
You can configure the HTTP proxy that the product uses to connect to the Internet.
 - [Add a Policy Manager Proxy Server](#)
If you add a Policy Manager Proxy Server the product will download updates through this proxy: this can mean faster updates.

Configuring the HTTP Proxy Manually

You can configure the HTTP proxy that the product uses to connect to the Internet.

To configure the HTTP proxy:

1. Click the *Automatic Updates* tab. **Last update check** displays the time of the latest update.
2. Click **Advanced**.
3. Click **Connection**.

4. Select **Manually configure HTTP proxy**.
5. Click **Configure**.
6. Enter the address and the port number of the HTTP proxy.
7. Select **Allow proxy to cache updates** if you have multiple installations of the product in the same network and you want to share the updates.
8. If the proxy requires user authentication, select **Proxy requires user authentication** check box and enter the user name and password for the proxy.

Add a Policy Manager Proxy Server

If you add a Policy Manager Proxy Server the product will download updates through this proxy: this can mean faster updates.

1. Click the *Automatic Updates* tab.
2. Click **Advanced**.
3. Select *Automatic Updates > Policy Manager Proxy*.
4. Click **Add**.
5. Type the address of the Policy Manager Proxy.
6. Click **OK**.

The product will try to download updates through the Policy Manager Proxy.

Note: The product will attempt to download from the proxy at the top of the list first. If downloading from that proxy fails, it will try the next proxy in the list. You can change the order of the proxy servers by selecting a proxy from the list and clicking the arrows to the right of the list.

Central Management

This product can run in centrally managed mode: in this mode the product settings are controlled remotely by a trusted expert.

In centrally managed mode:

- some or all of the product settings may be set remotely.
- some of these settings may be locked, so that you cannot change them yourself.
- [About Central Management Policies](#)
A policy is a group of settings that control this product when it is in centrally managed mode.
- [Manually Check for a Policy Update](#)
You can manually check for a new policy from the central management server.
- [Manually Import a Policy File](#)
You may need to manually import a policy file in the rare case that this product cannot receive policy updates.

- [Open Windows Event Viewer](#)
If you suspect there was a problem with this product you can use the Windows event viewer to check if an error was recorded.
- [View the Central Management Log](#)
From the central management log file you can see detailed information about policy and other updates.
- [Communication Settings](#)
You may need to check the communication settings in the rare occurrence of communication problems between this product and the central management server.

About Central Management Policies

A policy is a group of settings that control this product when it is in centrally managed mode.

A policy is created and enforced in the following way:

1. Policies are defined centrally by a trusted expert.
2. Once defined, a policy is published. This new policy is now available for download.
3. This product checks periodically for new policies. If a new policy was published, the new policy is downloaded.
4. Once downloaded the policy is applied and the new settings take effect.

Manually Check for a Policy Update

You can manually check for a new policy from the central management server.

Note: This product will by default, automatically check for a new policy periodically. However, you can check manually.

1. Click the *Central Management* tab.
2. Click **Check now** next to Last connection.

If a new policy is available, the new policy is downloaded and applied.

Manually Import a Policy File

You may need to manually import a policy file in the rare case that this product cannot receive policy updates.

Note: Make sure that any policy file you import is from a trusted source. A policy file from a malicious source could leave your computer unprotected.

1. Click the *Central Management* tab.
2. Click **Import policy manually**.
3. Select the policy file from the file system and click **Open**.

The policy file is applied.

Open Windows Event Viewer

If you suspect there was a problem with this product you can use the Windows event viewer to check if an error was recorded.

The Windows event viewer stores details of important system events. This includes details of actions and errors of this product.

1. Click the *Central Management* tab.
2. Click **Advanced**.
3. Select *General > Central Management*.
4. Click **Open Event Viewer**. The Windows event viewer opens.
5. To find messages from this product, select either **Application** or **System**.

Note: You can click **Source** to order the messages by their source. This makes it easier to find messages from this product.

View the Central Management Log

From the central management log file you can see detailed information about policy and other updates.

For example, you can find any failed attempts to connect to a central management server. You can also find if and when the connection was restored.

1. Click the *Central Management* tab.
2. Click **Advanced**.
3. Select *General > Central Management*.
4. Click **Show Log File**.

The central management log opens in a default text editor or viewer, for example, Notepad.

Communication Settings

You may need to check the communication settings in the rare occurrence of communication problems between this product and the central management server.

The communication settings determine if this product is in stand-alone mode or which central computer manages it. In a centrally managed environment it is unlikely that you can change these settings. If you can change them we recommend that you do not. You can easily put the product in a state where it cannot receive new policies from the central management server.