How to set up popular firewalls to work with Web CEO

Contents

General instructions

For normal operation, Web CEO must be granted access to these ports and protocols:

20, 21 – FTP;
25 – SMTP;
80 – HTTP;
443 – HTTPS.

Grant access to HHTP 80 / HTTPS 443 ports and enable cookies for the following domains:
websiteceo.com
webceo.com

For detailed setting instructions concerning each firewall, find your firewall in the list below and follow the link.

Setting up Agnitum Outpost Firewall 2.5

At the first launch of Web CEO, while the software runs, Agnitum Outpost will ask for permission to allow "wsceokrnl.dll" and "webceo.exe" to access the Internet. This must be allowed by choosing "Allow all activities for this application" and pressing "OK".


In the process of download of Web CEO updates the program modules change, that's why the permission for the updated modules to access the Internet must be granted again.

In order to check current permissions for Web CEO program modules to access the Internet, open Outpost Firewall Pro and select "Application" in the Options dialog. The modules "wsceokrnl.dll" and "webceo.exe" must be in the "Trusted applications" section.
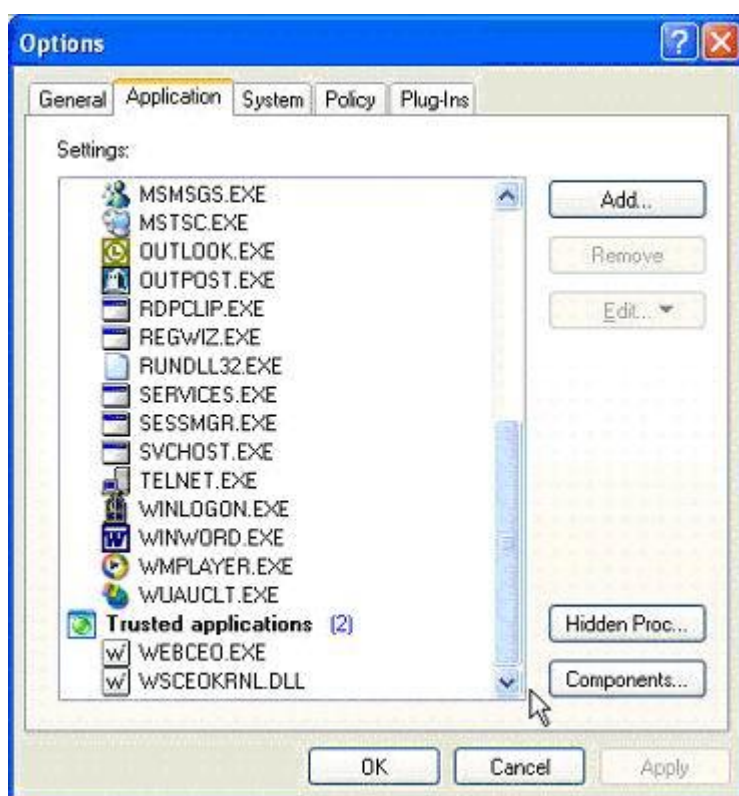

If these modules are not in the "Trusted applications" section, they must be granted full access. To do it, find these modules in the list or add them with the help of the "Add" button from the folder "C:\Program Files\Web CEO\BIN\". Then, right-click on the module and choose "Always Trust This App".
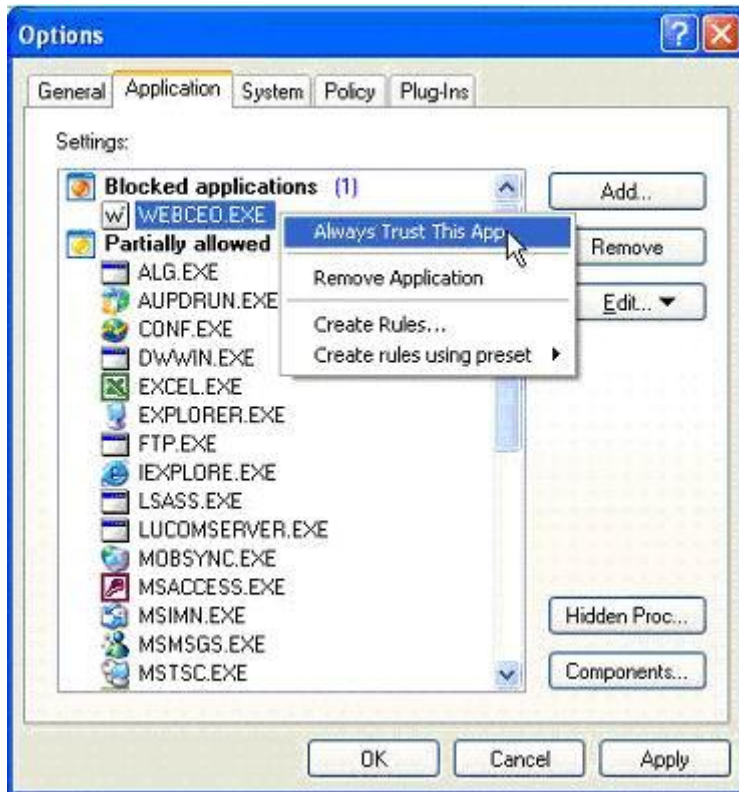
If cookies are disabled in your global settings, enable them for the sites "websiteceo.com" and "webceo.com".
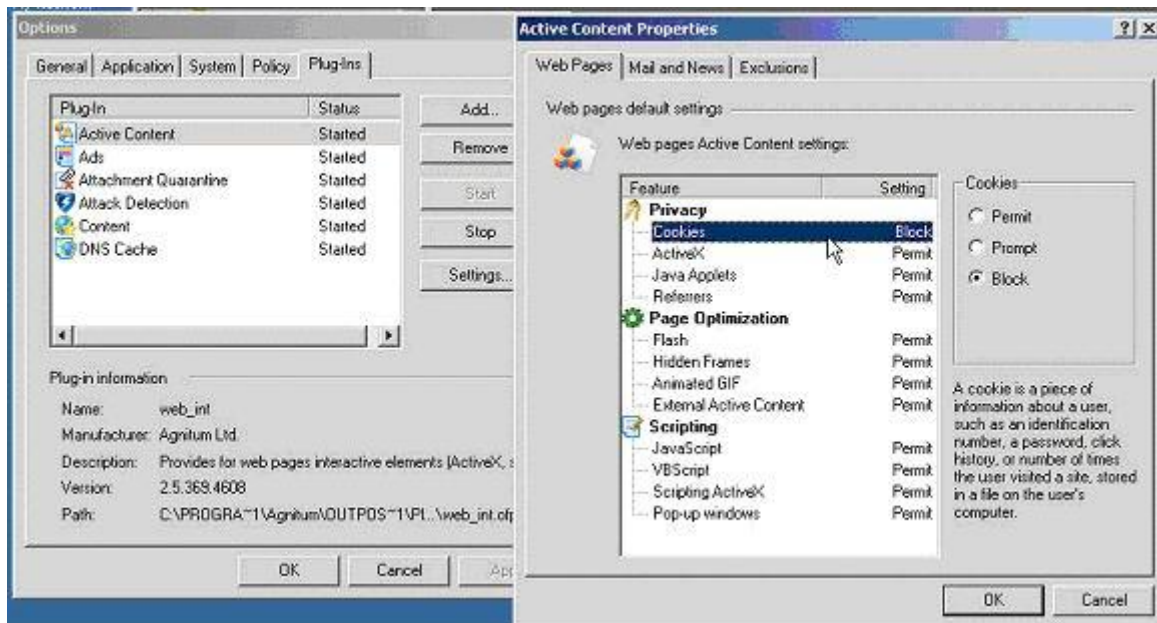
Go to the "Exclusions" tab in the window "Active content properties", press the "Add" button, enter
"websiteceo.com", and press "OK". In the "Edit properties for WEBSITECEO.COM" dialog window, click "Cookies", choose "Permit" and press "OK". Repeat this procedure for "WEBCEO.com".
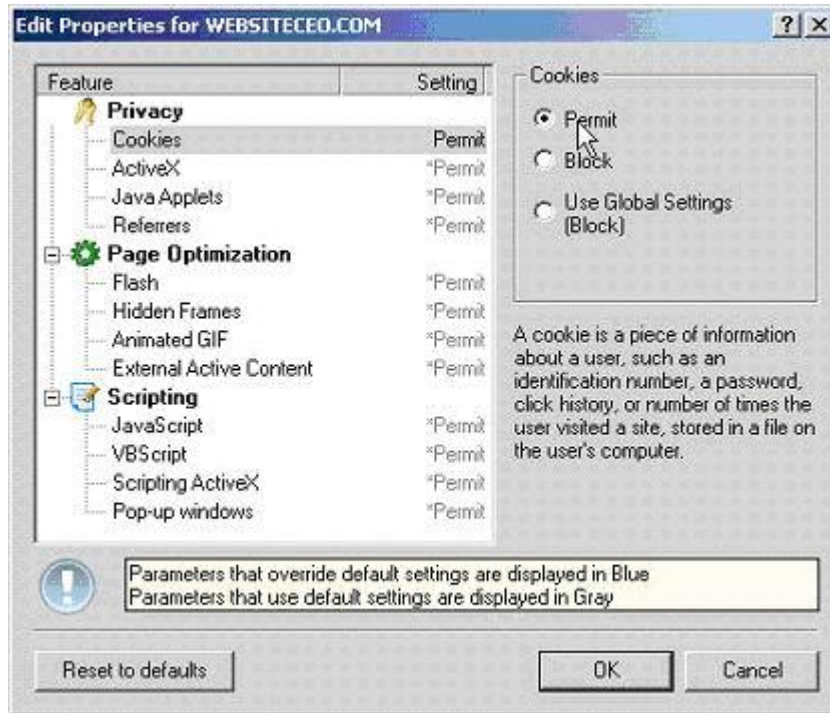
If the policy "Stop all mode" is active, Web CEO will be unable to work, while all remote connections will be blocked. If you choose the policy "Block most mode", Web CEO can work properly, provided the
above mentioned settings are done.

Setting up Black ICE 3

Installing Web CEO while the Application Protection is active.

Run the Web CEO installation. A window "Application Protection" will appear with a warning "unknown application detected" Web CEO500r--.exe. Press "Install Mode Options".

Below in the dialog window, press "Enable Install Mode". Continue with the Web CEO installation. Black ICE will add all installed files to the baseline list. On the installation completion, a window "Application Protection" will appear – press "Disable Install Mode". If the window "Application Protection" appears with the note "BlackICE will update baseline to include ....", press "Update". The installation process is completed.
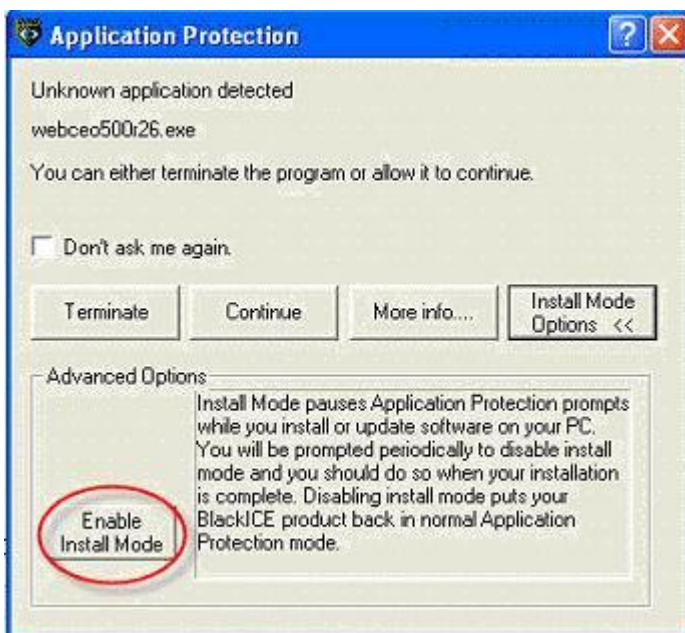
Web CEO update while the Application Protection is active.

After a Web CEO update is downloaded and its setup starts, a window with a warning will appear. Press "Continue".

After the Web CEO update is installed, you need to rescan the Web CEO folder and add the changed files to the baseline list. Go to Tools -> Advanced Applications Protection Setting, choose the "Baseline" tab, tick the folder where Web CEO is installed (usually C:\Program Files\Web CEO) and press "Run Baseline".

After the scanning process is complete, press "OK" and close the window "Advanced Applications Protection Setting". After this you can run Web CEO.

Web CEO uninstallation while the Application Protection is active.

During the uninstallation of Web CEO several new temporary files are created, which are not registered in the baseline list of the Application Protection, and blocked by Black ICE. As a result, the program uninstallation stops. Before you uninstall Web CEO, you should temporarily switch off the Application Protection. To do it, go to the "Tools" menu and choose "Stop BlackICE Application Protection".
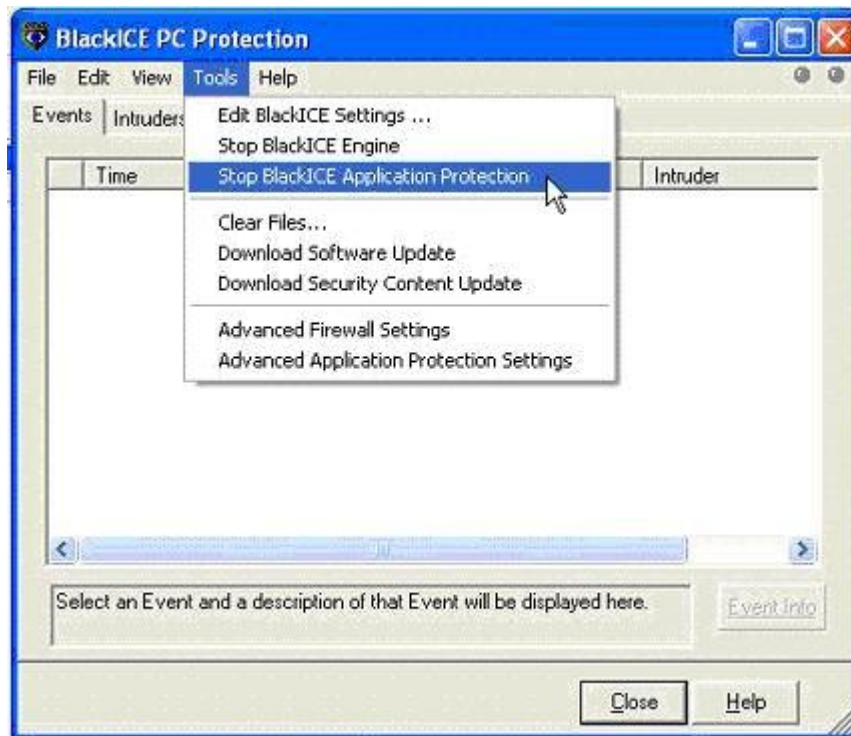
Then, uninstall Web CEO, switch the Application Protection again (the "Tools" menu – "Start BlackICE Application Protection").

Setting up the BlackICE firewall to work with Web CEO.

There are no special settings of the BlackICE firewall to work with Web CEO.
If you choose the "Paranoid" Protection Level, Web CEO will work properly.

Setting up ISA Firewall 2000

ISA Server works according to the principle: "What hasn't been explicitly allowed is by default disallowed", that's why, in order to let Web CEO work properly, you need to open in the ISA firewall the following ports: 20, 21 - FTP; 25 - SMTP; 80 - HTTP; 443 - HTTPS.

Open the "ISA server Access Policy" - > Protocol Rules.

Set up the access to the above mentioned fields. For example, 21 - FTP: Click "Create a Protocol Rule for Internet Access". In the dialog window that appears, enter the name of the new rule - "FTP Rule" and press "Next". In the next window in "Apply this Rule to:" choose "Selected protocols". In the "Protocols" list tick "FTP", then press "Next". In the net window in "Use this schedule" choose "Always" and press "Next". Then choose "Any request" and press "Next". In the dialog window that appears, press "Finish".

After that you need to set up the so-called "filters", which allow using various protocols and ports. The filters can be created in the "Access Policy " -> IP Packet Filters.
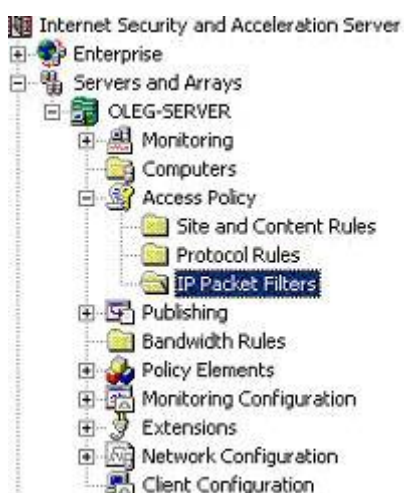
In the window "Configure Firewall Protection" choose "Create a packet filter", and enter the name of the FTP rule. In the next window it's better to choose "All ISA Server computer in the Array" by default. In the next window, choose to allow the programs working through this protocol. In the next window, "Filter Type", choose "Custom". Then, in the window "Filter Settings" fill in the protocol data:

IP protocol - TCP
Direction - Outbound
Local Port - Fixed Port
Local Port Number - 21
Remote Port - All Ports.

In the next window leave the default settings - "Default IP Addresses for each external ..." in the next window leave the default settings - "All Remote Computers".

For FTP, the 20th port might be required as well. Set it up in the way similar to the above described.

Also, to download the statistics, you will need to configure access through the HTTP protocol (port 80). Create the new rule. Enter the name for the HTTP rule. In the next window, choose "All ISA Server computer in the Array" by default. In the next window, choose to allow programs using this protocol. In the next window "Filter Type" choose "Custom". Then in the "Filter Settings" window fill in the protocol data:
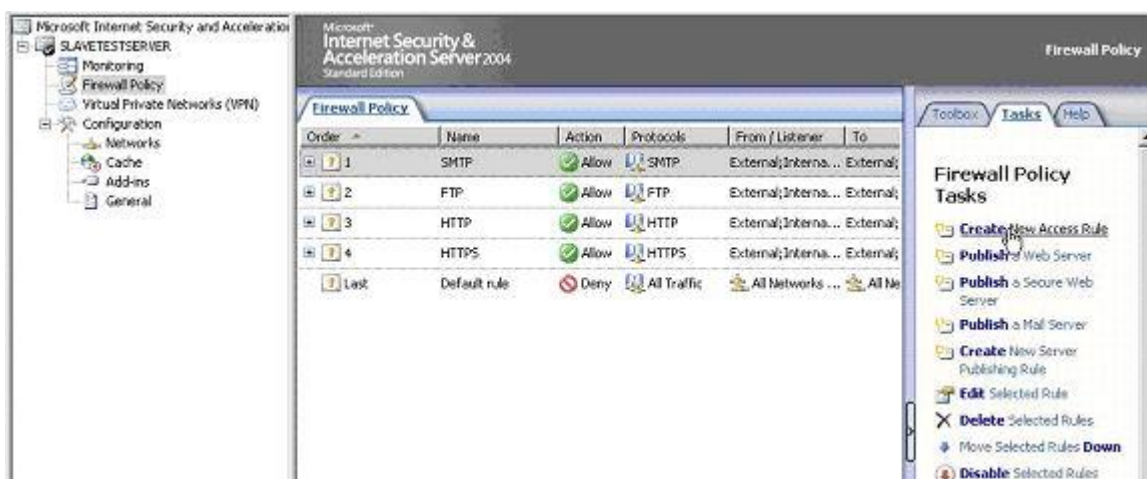
IP protocol - TCP
Direction - Both
Remote Port - Fixed Port (the number of port: 80).

In the next window, leave the default setting "Default IP Addresses for each external ..." In the next window leave the default setting "All Remote Computers".

All other protocols are configured the same way.

Setting up ISA Firewall 2004

Run the ISA Server Management. Click "Firewall Policy" – you will see the list of the rules. We need to open access through the following ports: 20, 21 – FTP; 25 – SMTP; 80 – HTTP; 443 – HTTPS.

For instance, here's how to allow access through the HTTP protocol. Open the "Tasks" tab and press "Create New Access Rule". In the window that appears, enter the "Access rule name" - "HTTP", press "Next". Choose to allow programs to work through this protocol and press "Next". In the window that appears, in the field "This rule applies to:" choose "Selected protocols". Press "Add", in the "Add protocols" window open the folder "Common Protocols", choose "HTTP" and press "Add", then "Close". Press "Next".
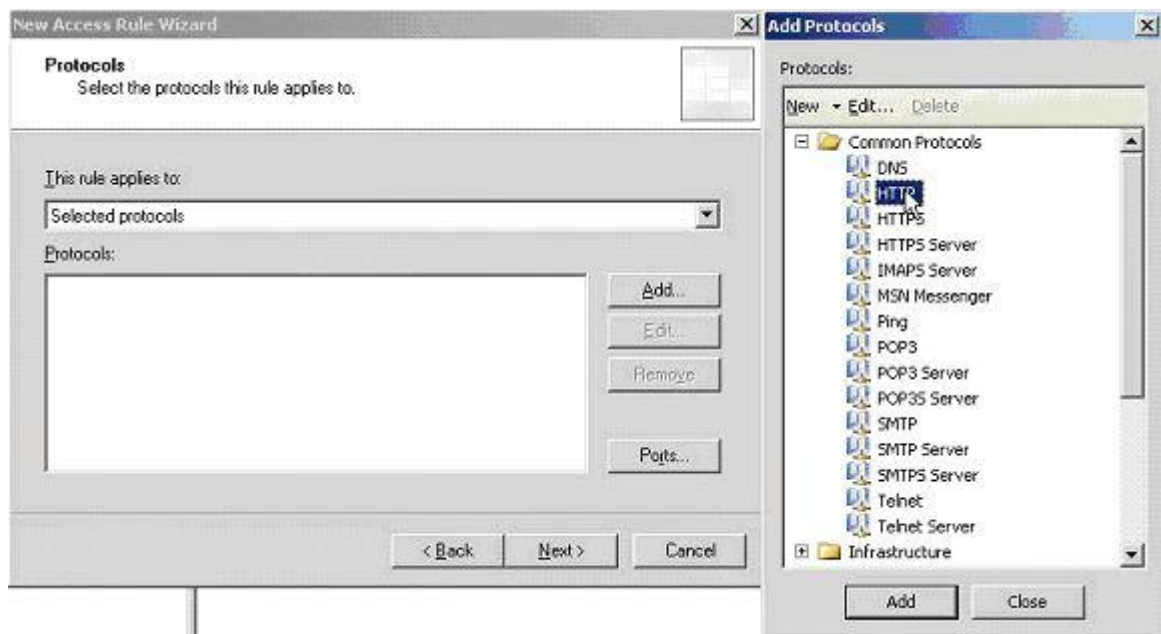
In the "Access Rule Sources" window press "Add" and in the window "Add Network Entities" choose the necessary network entities. Press "Add", then "Close". Press "Next". In the new window "Access Rule Destinations" choose and add the necessary network entities.
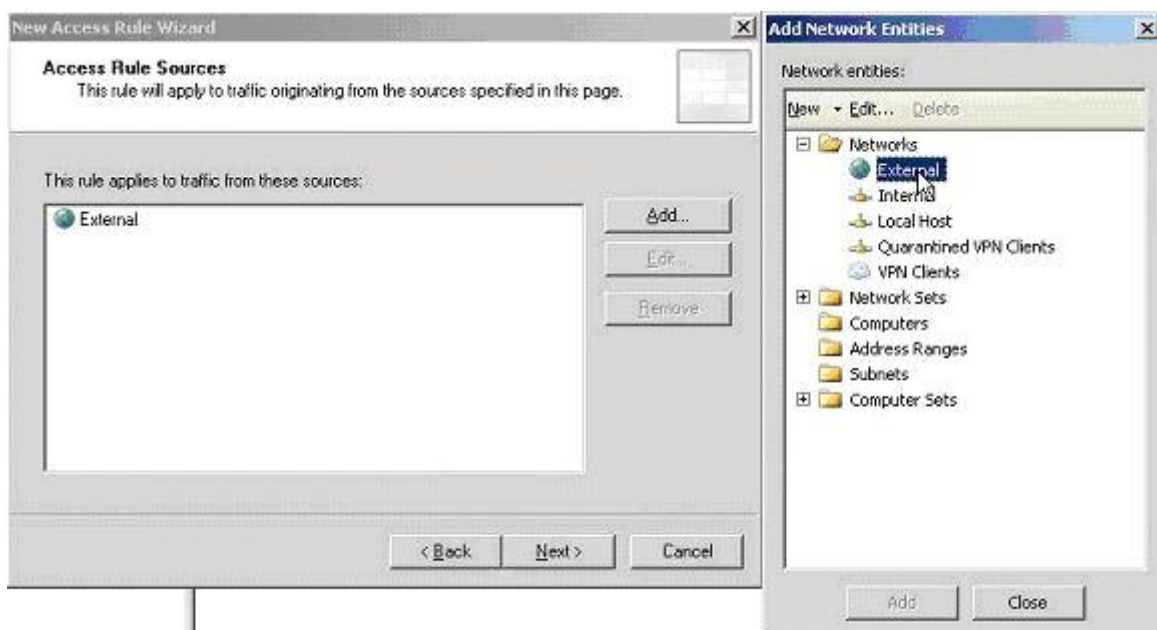
In the next window choose the users for this rule to apply to. Then, press "Finish". The rule is created. In order to save the changes and to update the configuration, press "Apply". In this way, create the rules for all other protocols.

Setting up McAfee Personal Firewall Plus 5.0.5

At the first launch of Web CEO you will see the window with the request to allow the module "wsceokrnl.dll" to access the Internet or block it. Choose "Grant Outbound Access". If the same window appears for "webceo.exe", also choose "Grant Outbound Access".

Attention! After the program updates the program files and their control sums can change, that's why you will probably have to confirm your permission to grant the Internet access for the modules "webceo.exe" or "wsceokrnl.dll". Depending on the warning, choose "Grant Outbound Access" or "Grant Server Access".

If you set the "Lockdown" Security Level, all incoming and outgoing packets will be blocked. If you set the

"Tight" Security Level, Web CEO will work properly, if Web CEO modules are granted the Internet access.

Setting up McAfee Security Center - McAfee Privacy Service 7.0

- McAfee Security Center includes the following products:
- Virus Scan – antivirus software;
- Personal Firewall – firewall. Can be set up in a way similar
- to McAfee Personal – firewall Plus (see above);
- Privacy Service – User privacy protection. The instructions to set up this package can be found below;
- Spam Killer – protection from spam.

In the "Privacy Service" user settings cookies must be obligatorily allowed for the sites "websiteceo.com" and "webceo.com". Open the "Privacy Service", click the "Users" tab, choose the user profile, under which you work with Web CEO, and press "Edit".

Go to the "Cookies" tab. For Web CEO to work properly, you need to select "Accept all cookies" or set up cookie blocking or permission for separate sites.

In order to do it, choose "Prompt user to accept cookies" and press "Edit". Choose "Web sites that can set cookies" and in the field "http://" enter "webceo.com" and press "Add", then enter "websiteceo.com" and press "Add". Press "Done", "Apply", "OK". The setup is complete.

Setting up Norton Internet Security 2004-2005

At the first launch of Web CEO the firewall will pop up with the message "wsceokrnl.dll is attempting to connect to DNS server". Choose "Always allow connections from this program on all ports". If the firewall asks "webceo.exe is attempting to connect to DNS server", choose "Always allow connections from this program on all ports".

To check up the permissions configuration for Web CEO to access the Internet, open "Norton Internet Security". On the left side, select "Status & Settings". In the middle, click "Personal Firewall". In the bottom right, "Configure". In the dialog window that appears, choose the "Programs" tab. Below in the list "Manual Program Control" in the "Programs" tab find "wsceokrnl.dll". In the "Internet Access" column, "Permit All" is required, in the "Category" column, "General". Then find "webceo.exe". In the "Internet Access" column, "Permit All" is required, in the "Category" column, "General".

In "High NIS Firewall" protection mode Web CEO will work properly, if the above described settings are completed.

To allow cookies, you need to set up a profile of the user who will work with Web CEO. To do it, open "Norton Internet Security", double-click "Privacy Control", press "Advanced", and in the dialog window that appears, click "User Settings". Click "Add Site" and enter "websiteceo.com". In the "Cookies" filed, "Permit" is required. The same way, "webceo.com" must be added.
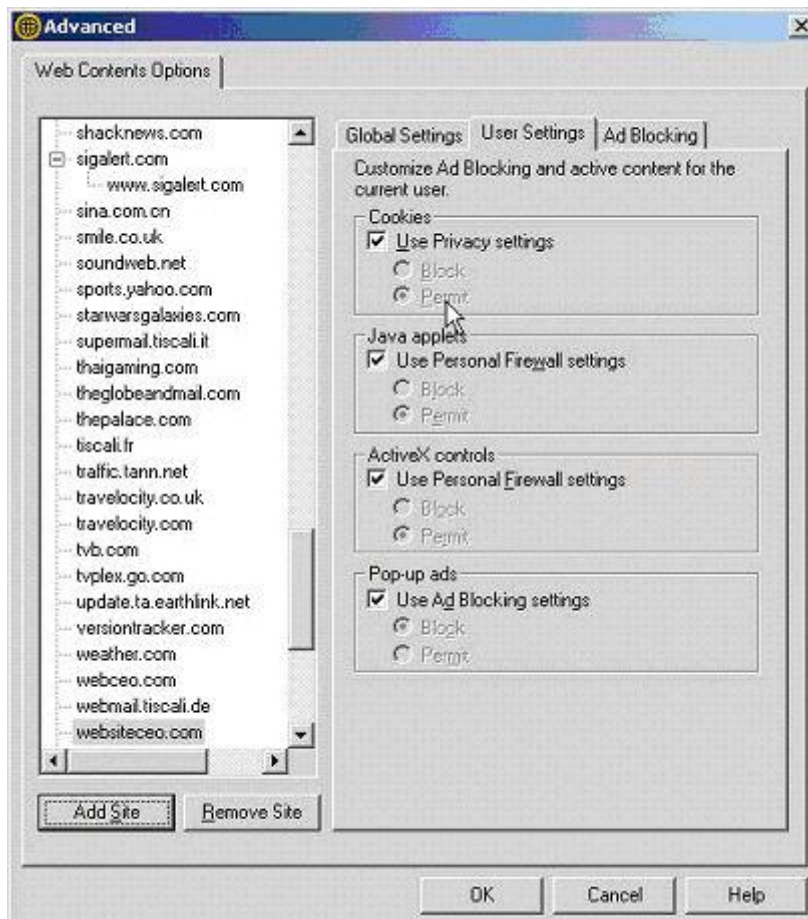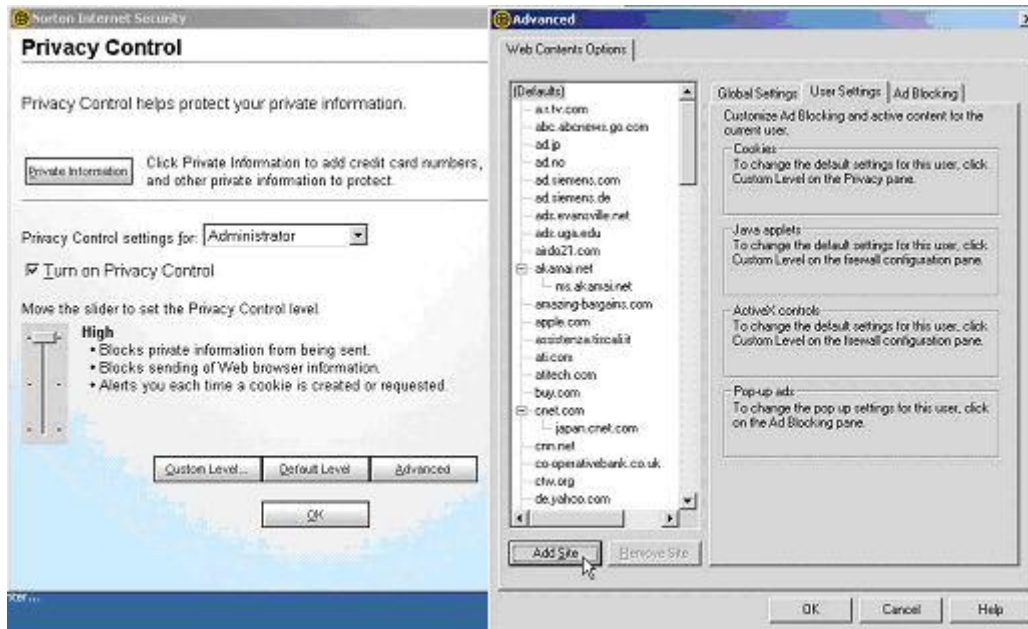
Setting Up Trend Micro PC-cillin Internet Security 2005

At the first launch of Web CEO the firewall will pop up with a dialog window. You need to allow the module "wsceokrnl.dll" the outgoing connection. Check the boxes "Do not warn me of future...", "Allow or deny connection on all ports", "Allow or deny connection on all IP addresses".
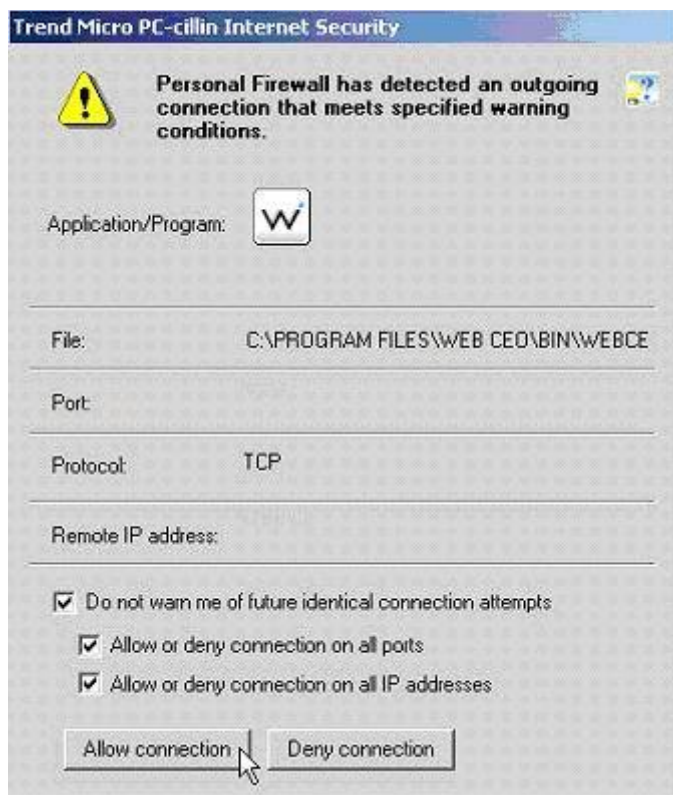

If during the Web CEO update download a dialog screen will pop up, allow the module "webceo.exe" the outgoing connection. Check the boxes "Do not warn me of future ...", "Allow or deny connection on all ports", "Allow or deny connection on all IP addresses".

To check the firewall settings for Web CEO, open PC-cillin Internet Security 2005, click the "Network Security" tab, and then click "Personal Firewall".
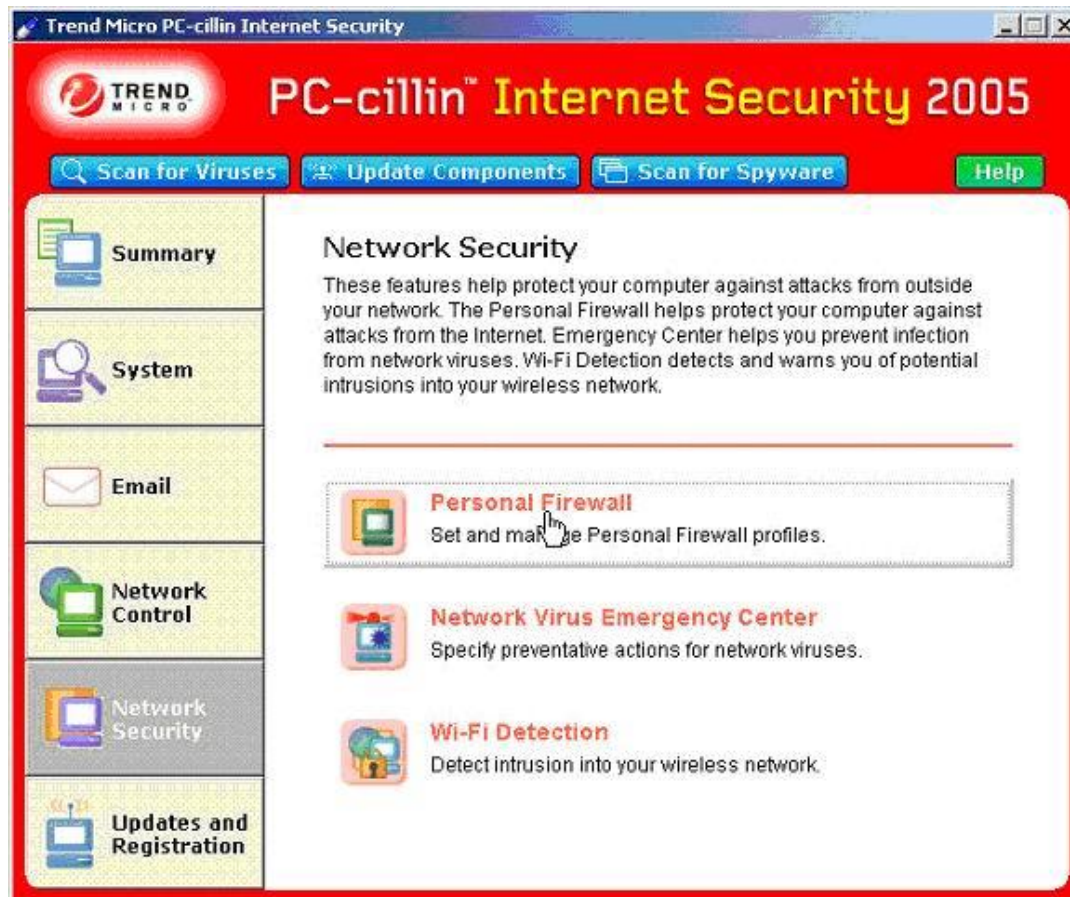
In the window that appears, first choose the profile, under which you work with the Internet, in the "Choose a profile" dropdown field, and click "Edit" for profile modification.
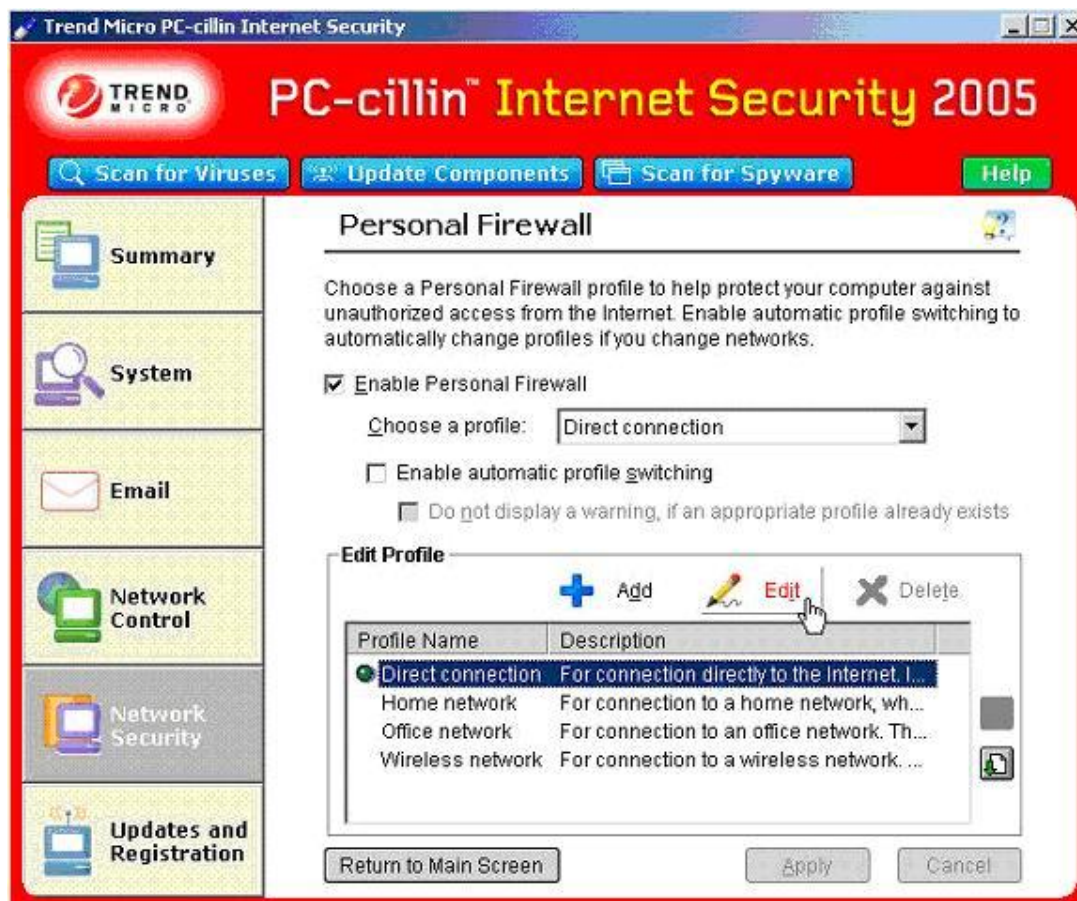
In the window that appears, go to the "Exception List" tab. For the modules "WSCEOKRNL.DLL" and "WEB CEO.EXE" in the "Access" field "Allow" is required, in the "Connection" field "Out" is needed.
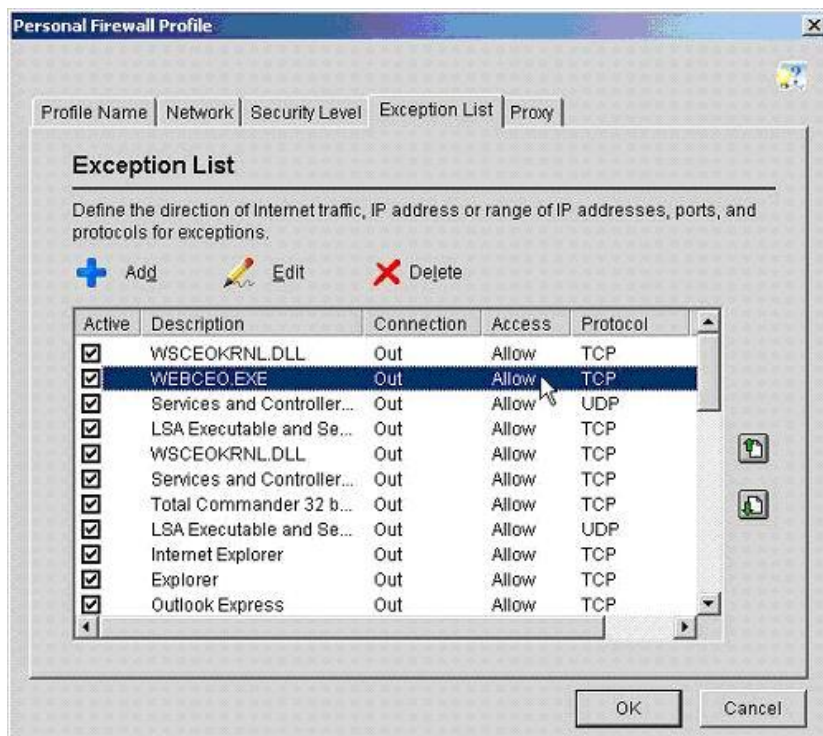
If it is not so, choose the appropriate module, press "Edit" and tick the radio buttons as shown below.
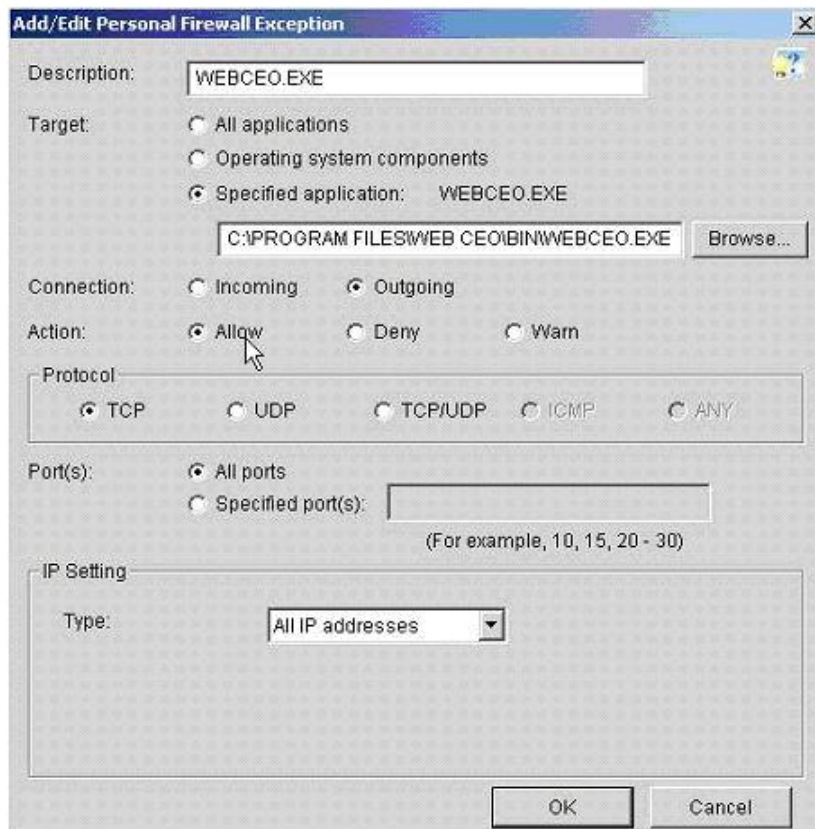
Under the "High" Security Level Web CEO works properly, provided the above mentioned settings are completed.

Setting up Windows SP2 Firewall

For Web CEO proper operation, no additional settings of the Windows Firewall are required.

Attention! Windows Firewall analyzes and can block the incoming traffic, but it does not deal with the outgoing one. By default, Windows Firewall blocks all incoming traffic, except the cases when data are sent in response to the preceding outgoing request.

Setting up Zone Alarm Internet Security Suite

When Web CEO tries to receive data from the Internet, the firewall will pop up with a "ZoneAlarm Pro Alert" and ask you to grant to the file "wsceokrnl.dll" the internet access or block it. Tick the "Remember this setting" checkbox and press the "Allow" button. If you do not choose to remember the setting, the firewall will ask you about this program each time it attempts to access the Internet.
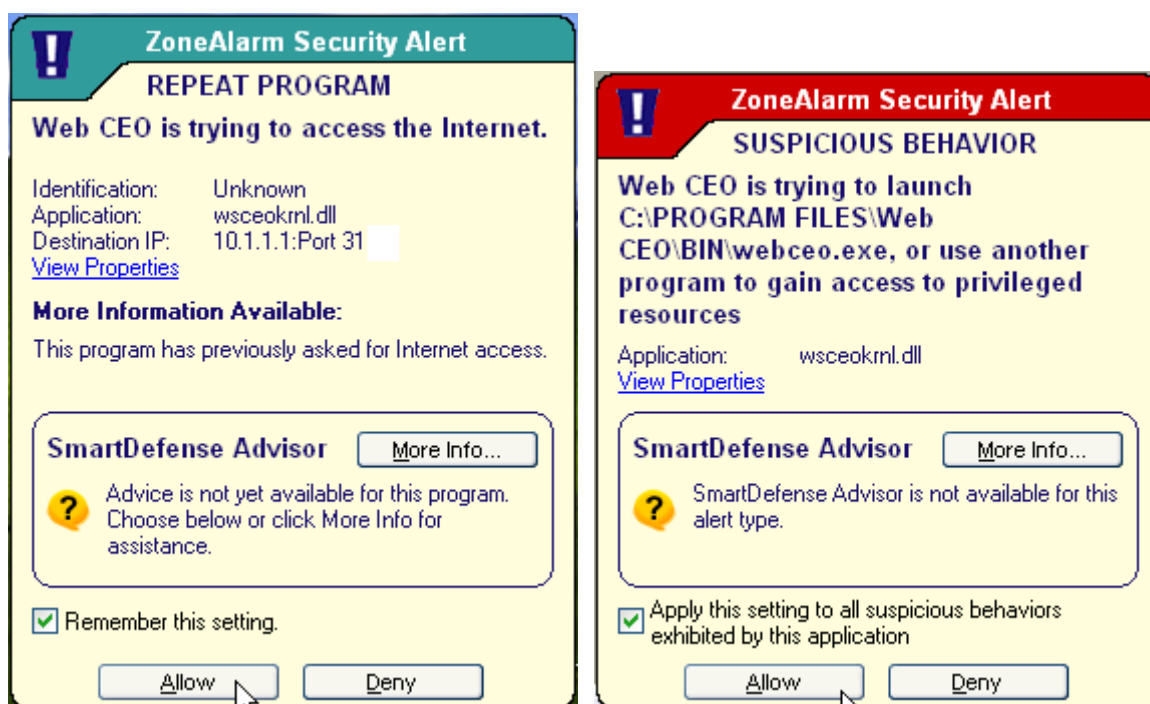
To check the firewall settings concerning Web CEO, open Zone Alarm and choose the "Programs" tab in the "Program Control". Next to Web CEO program module, "webceo.exe", in the "Access" section, there must be two ticks ("Allow") in the fields "Trusted" and "Internet". Complete the same settings for the second module, "wsceokrnl.dll".

ZoneAlarm Security Suite

ZONEALARM Internet Security Suite

- ☑ Overview
- ⬅ Firewall
- ➡ **Program Control**
    - Main
    - → Programs
    - Components
- ➕ Anti-virus/Anti-spyware
- ✉ E-mail Protection
- 🔒 Identity Protection
- 🚶 Parental Controls
- ▲ Alerts & Logs

Quick Tasks

Enter License Key
Scan Computer
Set Gaming Mode
Check for updates

❓ **Help**

| Active	Programs △	SmartDefense	Trust Level	Access Trusted	Access Internet	S Trusted
	TechSmith HTML He...	Auto ▾	▮▮▮	✗	✗	✗
	Userinit Logon Appli...	System ▾	▮▮▮	✓	✓	✓
	Verify Class ID	Auto ▾	▮▮▮	✓	✓	✓
	VMware Activation ...	Auto ▾	▮▮▮	✓	✓	✓
	VMware Tools Ser...	Auto ▾	▮▮▮	✓	✓	✓
	VMware Tools Ser...	Auto ▾	▮▮▮	✓	✓	✓
	VMware Tools tray ...	Auto ▾	▮▮▮	✓	✓	✓
●	Web CEO	Auto ▾	▮▮▮	✓	✓	?
●	Web CEO loader	Auto ▾	▮▮▮	✓	✓	✓
	Windows Explorer	System ▾	▮▮▮	✓	✓	✓
	Windows Logon UI	Auto ▾	▮▮▮	✓	✓	✓
	Windows NT Logon...	System ▾	▮▮▮	✓	✓	?
	Windows NT Sessi...	System ▾	▮▮▮	✗	✗	✗
	Windows TaskMan...	Auto ▾	▮▮▮	✓	✓	✗

Entry Detail

|	
Product name	Microsoft® Windows® Operating System
File name	C:\WINDOWS\system32\alg.exe
Last policy update	Not applicable
Version	5.1.2600.5512 (xpsp.080413-0852)
Last modified date	4/14/2008 15:00:00

Add

Options

Setting up COMODO Firewall Pro

At the first launch of Web CEO, while the software runs, COMODO Firewall Pro will ask for permission to allow "wsceokrnl.dll" to access the Internet. This must be allowed by choosing "Treat this application as" and selecting 'Trusted Application'. Click OK to confirm the selection.
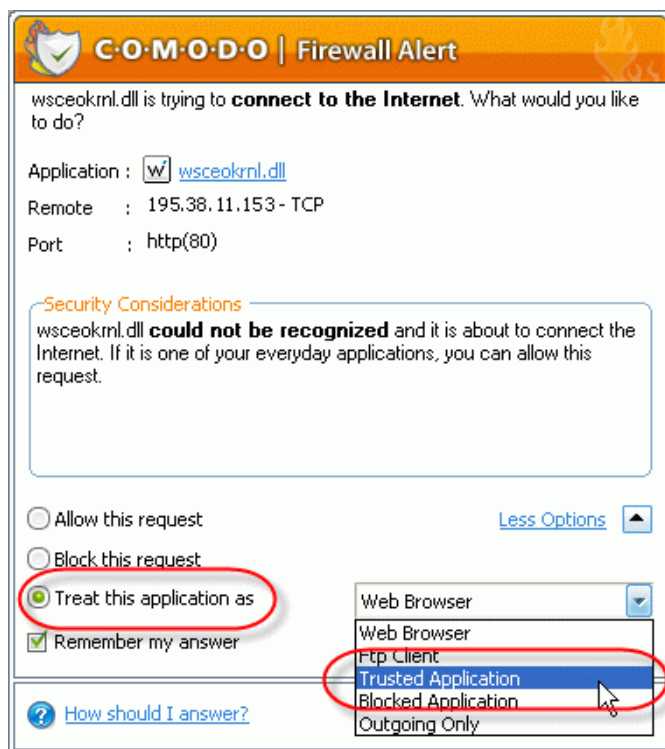
Please note that we release software bug fixes from time to time. These software updates are downloaded and installed by the webceo.exe application, that's why you'll be prompted to allow access to this module.
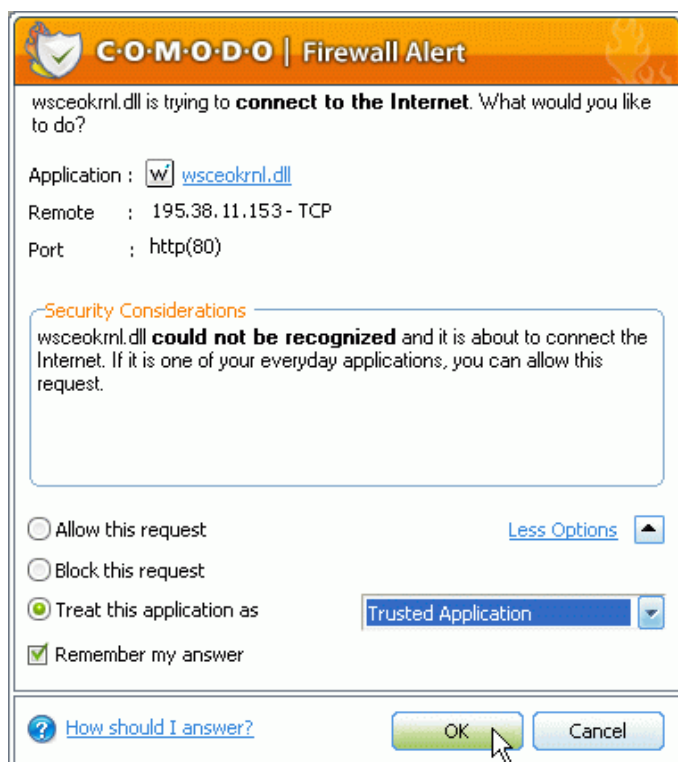
The firewall will ask you to allow the file "webceo.exe" access the Internet. This must be allowed by choosing "Treat this application as" and selecting 'Trusted Application'. Click OK to confirm the selection. Tick 'Remember my answer' in order not to be prompted in future.
After the software update installation, the files and their checksums can change, that's why you will most likely have to confirm your permission to grant the Internet access for the modules "wsceokrnl.dll" and "webceo.exe".

In order to check current permissions for Web CEO modules Internet access, open COMODO Firewall Pro and select "FIREWALL" in the main menu, then go to "Advanced' section on the left pane, and select 'Network security policy' menu item.

The modules "wsceokrnl.dll" and "webceo.exe" must be identified as 'Trusted Application'.
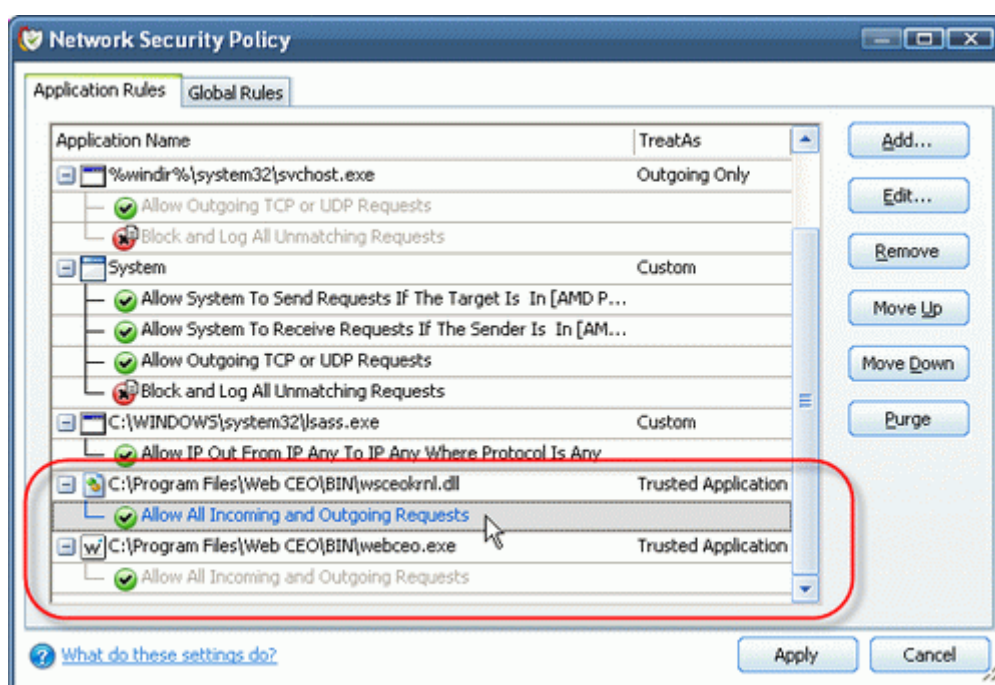
If these modules are identified as 'Blocked Application', click 'Edit' and change this to 'Trusted Application'.

In case there are no Web CEO modules in the list, they should be added: click the "Add" button and select the files from the folder "C:\Program Files\Web CEO\BIN\" or 'C:\Users\%username%\AppData\Local\Web CEO\BIN' if you run Windows Vista. Then, adjust the rules for both applications: check the 'Use a predefined policy' radio-button and choose the 'Trusted Application' option in the drop-down menu.
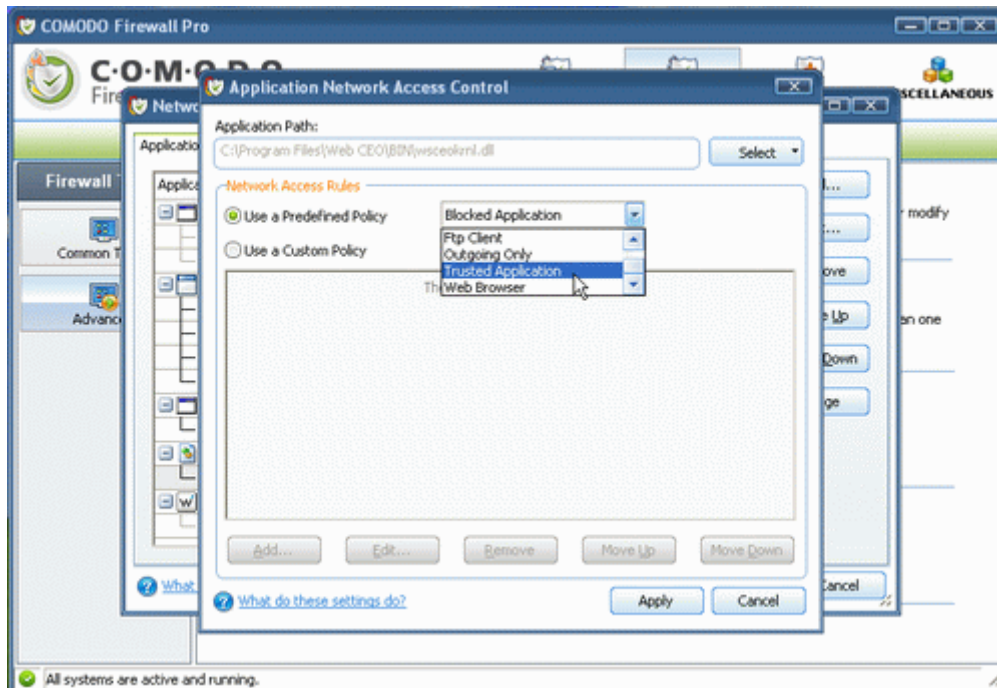
Setting up AVG Internet Security 2013

To allow Web CEO access the Internet, please follow these steps:

1. Open AVG Internet Security 2013 and click the "Firewall" button, then click "Settings".
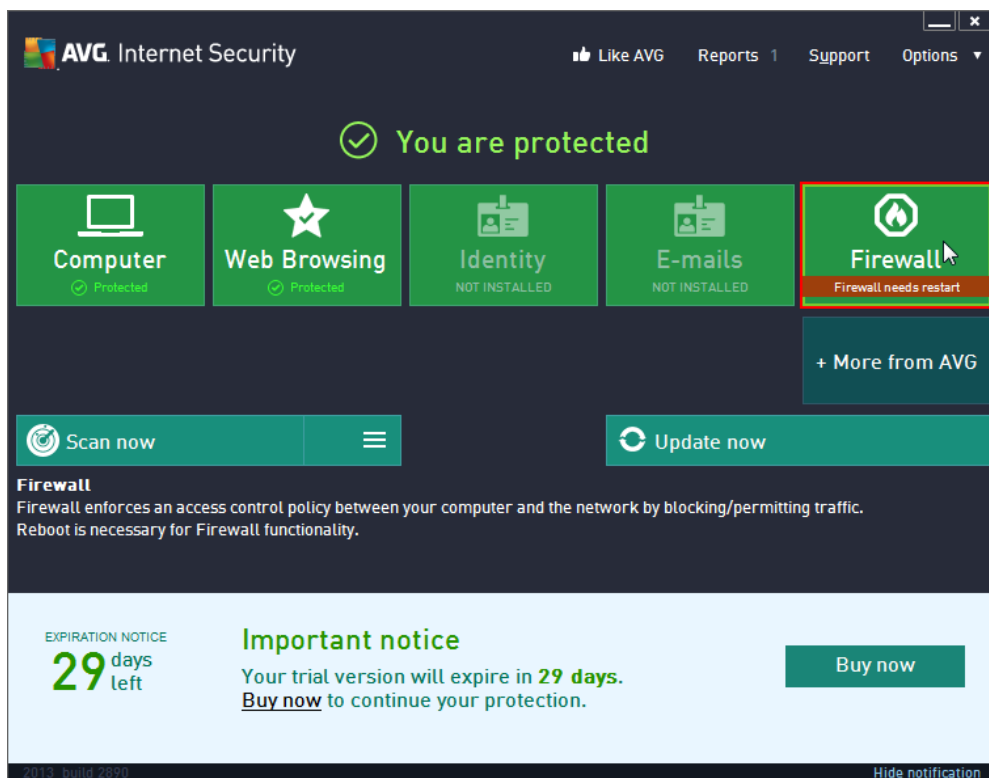
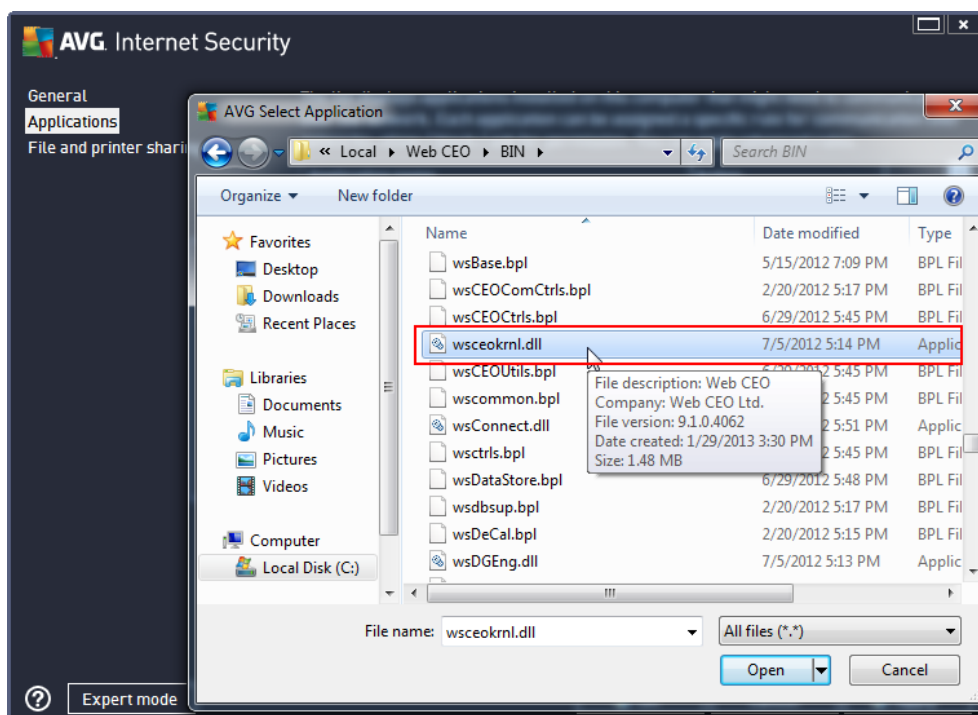2. Find the "Applications" menu, and then click "Add".

3. Browse for the BIN folder and find the **wsceokrnl.dll** application (the "All files" mode should be
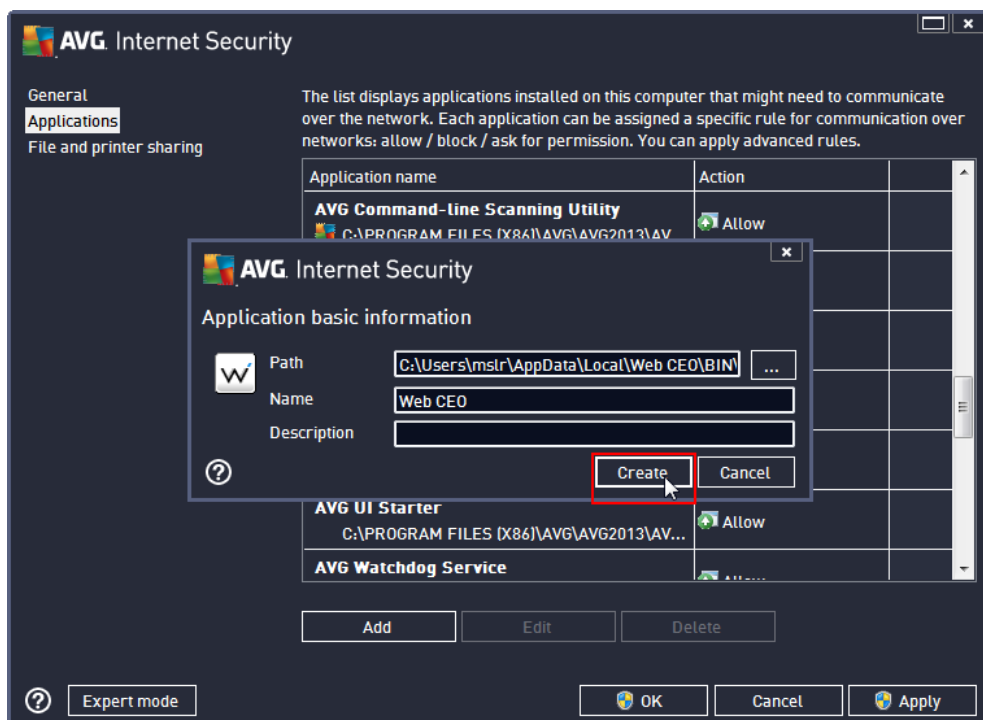
set) and click "Open".

The BIN folder can be found here:

C:\Program Files\Web CEO\Bin (Windows XP);

C:\Users\Username\AppData\Local\Web CEO\BIN\ (Windows Vista, Windows 7, Windows 8).

4. Click "Create" to create a rule and make sure that the "Application action" status is "Allow". Click OK to confirm the action.

5. Then, please follow the steps 2, 3, and 4 once again to add **webceo.exe**.

6. If done correctly, you will find **wsceokrnl.dll** and **webceo.exe** in the list of applications with the "Allow" status.

7. When done, click OK to close the Settings window.