

SOPHOS

Sophos Client Firewall version 1.5 user manual

For Windows

Document date: June 2007



Contents

- 1 Sophos Client Firewall.....4
- 2 How do I get started?.....5
- 3 How do I configure the firewall?.....15
- 4 How do I configure reporting and logging?.....31
- 5 How do I work in interactive mode?.....34
- 6 How do I use the log viewer?.....40
- 7 Glossary.....46
- 8 Technical support.....64
- Index65

1 Sophos Client Firewall



Welcome to **Sophos Client Firewall**, the latest in firewall technology.

Sophos Client Firewall offers extensive protection against unknown traffic. It has been designed to be suitable for both the experienced user and the beginner.

The advanced user can configure the firewall in great detail to suit their own needs.

For the beginner, we have made every effort to simplify the configuration procedure by supplying step-by-step help instructions and preset rules to get you started.

For instance, you can authorize the following common office functions at the click of a few buttons:

- Web browsing
- FTP downloads
- email
- file and printer sharing.

If you are using Sophos Client Firewall for the first time, see [Getting started](#) for further details.

2 How do I get started?

This section describes how to set up and modify key settings for the Sophos Client Firewall.

- Getting started
- The firewall interface
- The system tray icon
- Allow the use of a web browser
- Allow email
- Allow file and printer sharing
- Use the firewall interactively
- Turn the firewall on and off

2.1 Getting started

When the firewall is first installed, you may need to configure it to allow common applications network access. This depends on how the firewall has been installed. There are two types of installation:

- Installed and managed from the central management console
- Installed standalone.

You can find advice on getting started with each below.

Firewall installed and managed from a central management console

If the firewall is installed and managed from a central management console, it blocks or allows traffic according to rules set by the administrator.

Unless the administrator has put the firewall into Interactive mode, you should not be prompted with any messages.

Firewall installed standalone

If the firewall is not managed from the central console, it prompts you to allow or block traffic for which it does not have any rules. This is called "Interactive mode".

See [How do I work in interactive mode?](#) for details of how to deal with messages from the firewall.

You can also create rules at any time to allow common applications to:

- Allow the use of a web browser
- Allow email
- Allow file and printer sharing

When the firewall has been configured and recognizes the applications you use, we recommend that you put the firewall into Non-interactive mode. See [Select interactive or non-interactive working](#).

2.2 The firewall interface

The main areas of the firewall interface are the following:

- The **Sophos Client Firewall Configuration Editor**, see [How do I configure the firewall?](#) for further details.
- The **log viewer**, see [Introduction to the log viewer](#) for further details.
- [The system tray icon](#).

2.3 The system tray icon

What a user sees depends on which user group the System Administrator has placed them in.

- Members of **SophosAdministrator** and **SophosPowerUser** see the icon, all the menu options and all pages of the configuration editor.
- Members of **SophosUser** see the icon, all menu options and the four rule pages in the configuration editor (Global rules, Applications, Processes and Checksums).
- **Protected users** (members of no Sophos group) see the icon and three menu options (Help, About and Clear alerts) and have no access to the configuration editor.

When the firewall is disabled, the grey firewall icon is displayed in the system tray.



When the firewall is enabled, the blue firewall icon is displayed in the system tray.



When the firewall is enabled, and a new or modified application attempts to access the network, the red firewall icon is displayed in the system tray. When you have selected **Clear Alert** from the menu, the firewall icon turns blue.




If you right-click the firewall icon you can select the following:


- **View Log** to view the System log. See [Introduction to the log viewer](#) for further details.
- **Configure** to configure the Sophos Client Firewall Configuration Editor. See [How do I configure the firewall?](#) for further details.
- **Clear Alert** to clear an alert.
- **About** to view product information.
- **Help** to view the help file.

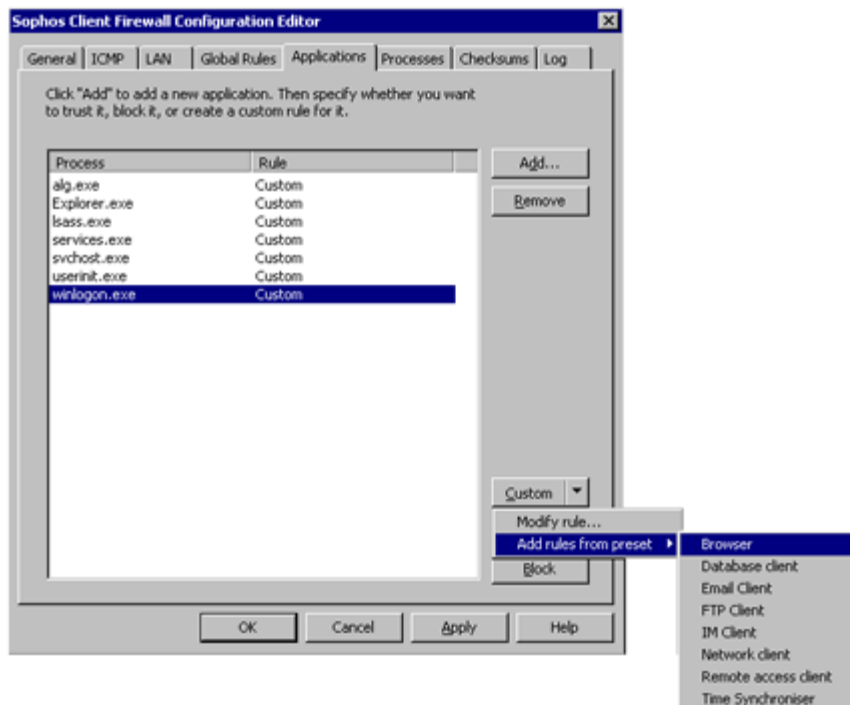
2.4 Allow the use of a web browser

To allow the use of a web browser:

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Applications** tab. Click **Add** and find the browser program, e.g. `iexplore.exe` for Internet Explorer, on the computer. The program is added to the list and is now "Trusted".
3. For greater security, you should apply a preset rule supplied by Sophos. Highlight the program, click the drop-down arrow on the **Custom** button, select **Add rules from preset** and then select **Browser**.
4. Click **OK**.

 If you want to set a custom rule for the browser program, consult the help page [Set rules for applications](#).

 When you allow the use of a web browser, you also allow FTP access.




2.5 Allow email

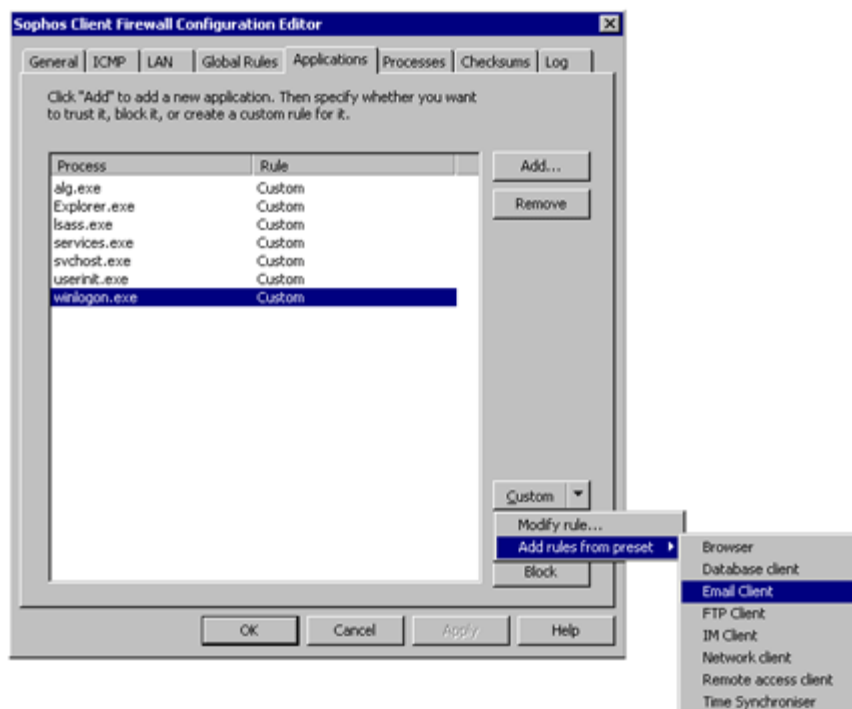
To allow email, do as follows.

1. Right-click the firewall icon in the system tray and select Configure.
2. In the Sophos Client Firewall Configuration Editor dialog box, click the Applications tab.
3. Click Add and find the email program the computers use. The program is added to the list and is now "Trusted".

For greater security, you should apply a preset rule supplied by Sophos. Highlight the program, click the drop-down arrow on the Custom button, select Add rules from preset and then select **Email Client**.

4. Click OK.

 If you want to set a custom rule for the email program, consult the help page [Set rules for applications](#).



2.6 Allow file and printer sharing

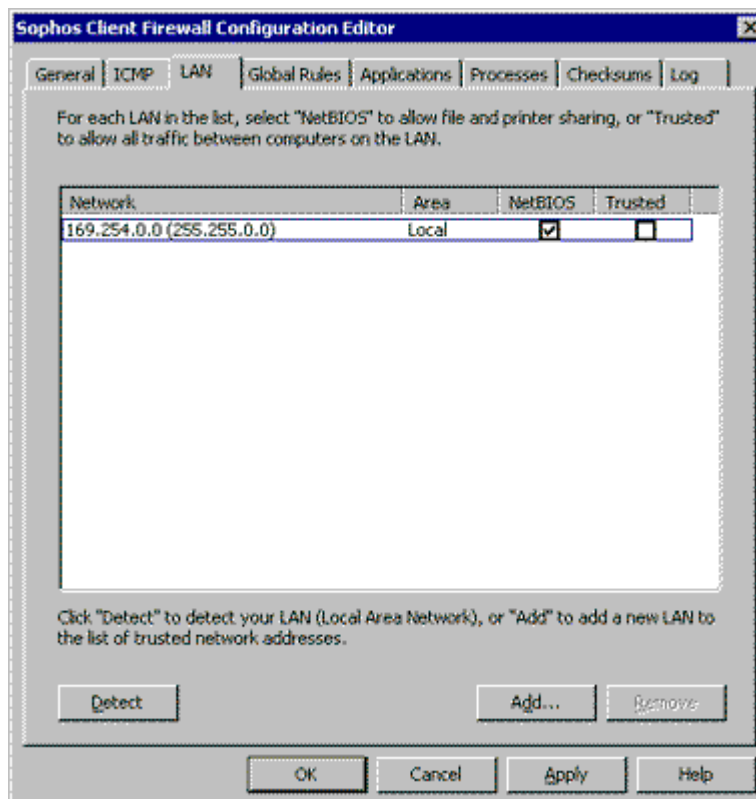
To allow file and printer sharing on a LAN (Local Area Network), do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the LAN tab.
3. Click **Detect** to detect the LAN(s) the computer is on and add them to the list automatically.

Alternatively, click **Add** to add a LAN to the list. The **Select address** dialog box appears. Use this dialog box to add domain names, IP numbers and IP addresses with subnet mask. The network address and subnet mask are displayed in the **Network** column and the type of network address is displayed in the **Area** column.

Click **NetBIOS** to allow file and print sharing.

4. Click **OK**.



2.7 Use the firewall interactively

You can set Sophos Client Firewall to work in two modes.

- **Interactive.** The firewall asks you how to deal with traffic.
- **Non-interactive.** The firewall deals with traffic automatically using your rules.

To change the working mode, do as follows:

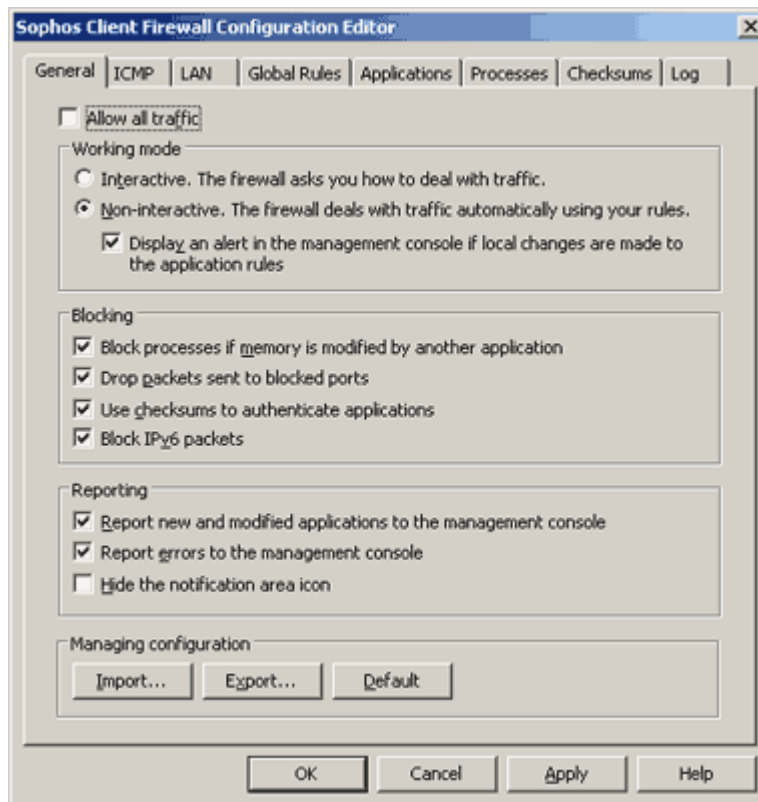
1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab.
3. Select **Interactive** or **Non-interactive**.
4. Click **OK**.



If you choose **Non-interactive**, you can also select the **Display an alert in the management console if local changes are made to the application rules** option. This displays an alert on the central management console (if one is being used) if changes are made to any rule (i.e. global or application rules, processes or checksums).



For further information, see [How do I work in interactive mode?](#)



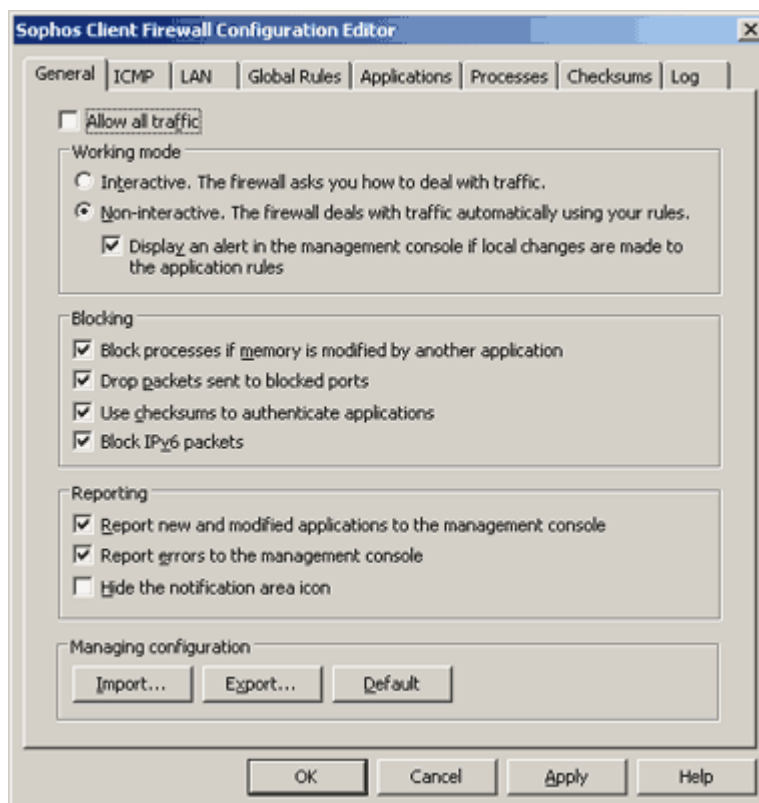
2.8 Turn the firewall on and off

By default the firewall is enabled, however, you can disable the firewall. To turn the firewall off, do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab.
3. Select **Allow all traffic**.
4. Click **OK**.



For day-to-day use, we recommend you keep your firewall enabled.



3 How do I configure the firewall?

You can configure the firewall and then enable it. You can configure it in many different ways using the **Sophos Client Firewall Configuration Editor**, however, a few common functions are listed below.

- Select interactive or non-interactive working
- Allow incoming and outgoing ICMP traffic
- Allow all traffic between computers on a LAN
- Allow FTP downloads
- Set global rules
- Set rules for applications
- Allow applications to launch hidden processes
- Allow applications to use rawsockets
- Use checksums to authenticate applications
- Importing and exporting existing configurations
- Which rule takes priority?


3.1 Select interactive or non-interactive working

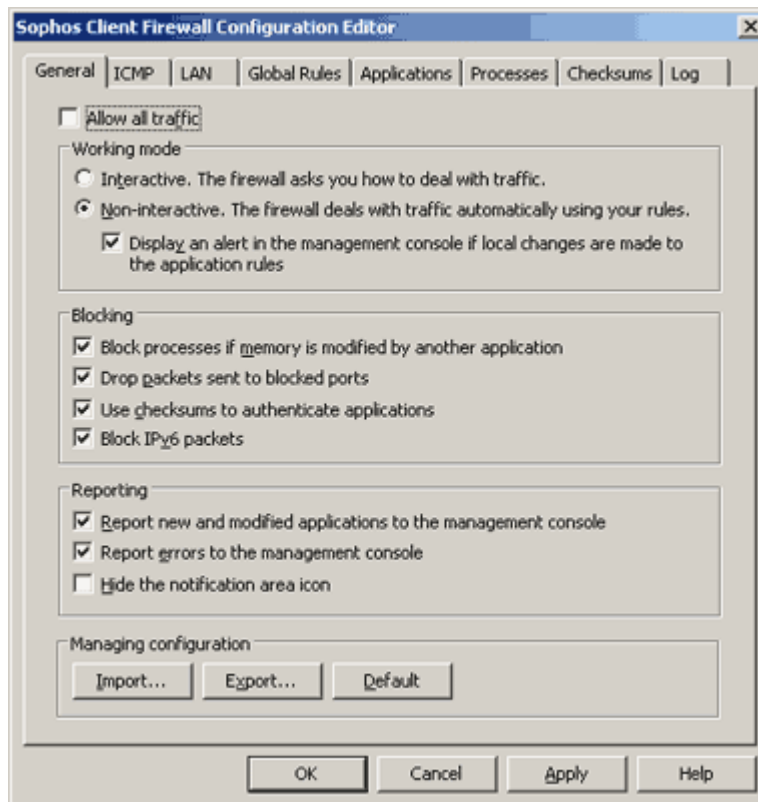
Sophos Client Firewall can work in two different modes:

- **Interactive.** The firewall asks the user how to deal with traffic.
- **Non-interactive.** The firewall deals with traffic automatically using your rules.


To change the working mode, do as follows:

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab.
3. Select **Non-interactive** or **Interactive**.
4. Click **OK**.

 If you select **Non-interactive**, you can also select the **Display an alert in the management console if local changes are made to the application rules** option. This displays an alert on the central management console (if one is being used) if changes are made to any rule (i.e. global or application rules, processes or checksums).



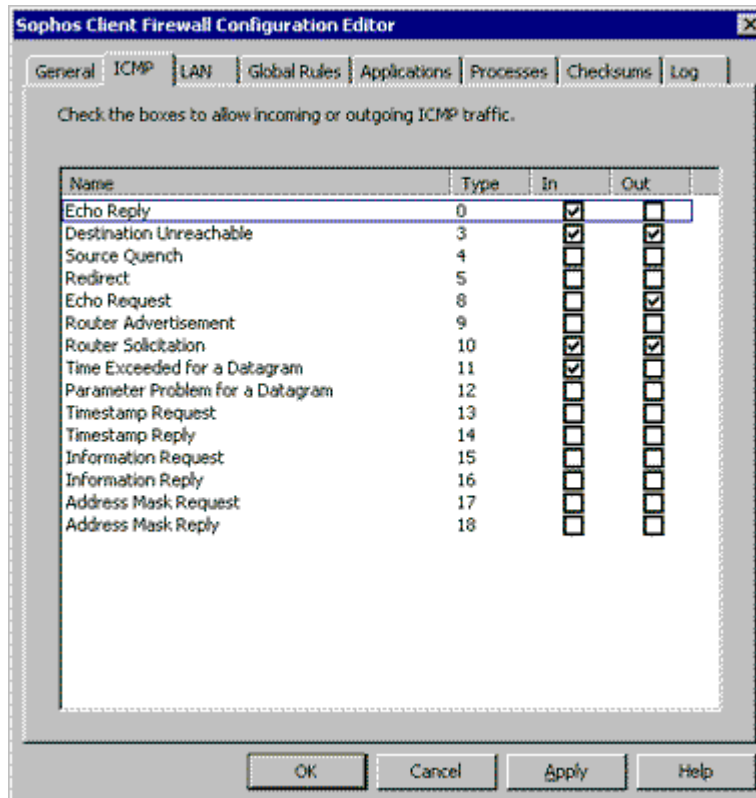
3.2 Allow incoming or outgoing ICMP traffic

 We recommend you specify types and directions of ICMP messages only if you know about networking protocols.

To specify the types and directions of ICMP messages, do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **ICMP** tab.
3. Click **In** to authorize incoming messages of the specified type.
Click **Out** to authorize outgoing messages of the specified type.
4. Click **OK**.

For [further information on ICMP traffic](#) click here. For a [definition of ICMP traffic](#) click here.



3.3 Allow all traffic between computers on a LAN

To allow all traffic between computers on a LAN (Local Area Network), do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **LAN** tab.
3. Click **Detect** to detect the LAN(s) the computer is on and add them to the list automatically.

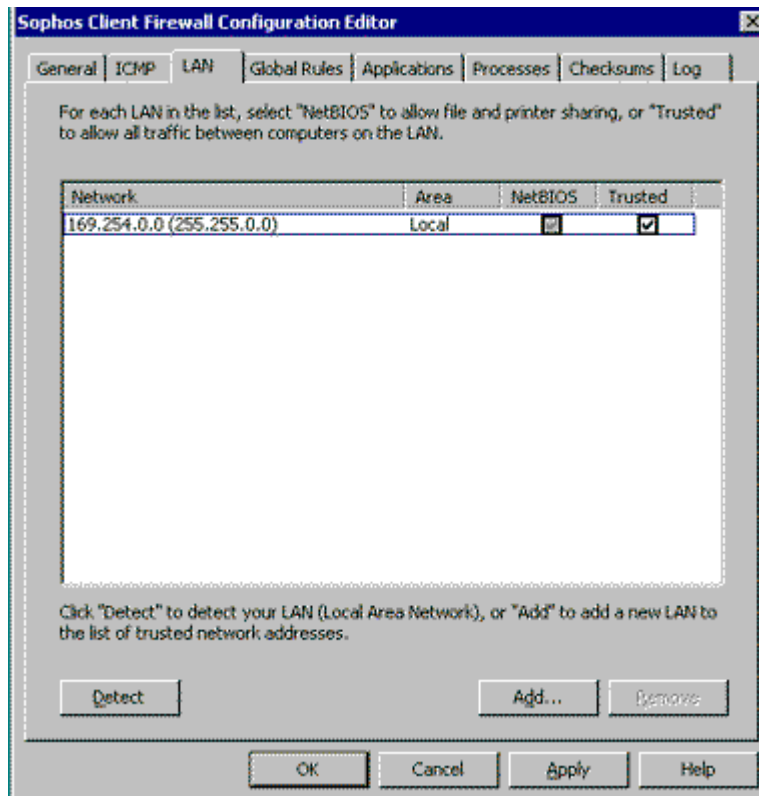
Alternatively, click **Add** to add a LAN to the list. The [Select address](#) dialog box is displayed. Use it to enter the LAN address.

Click **Trusted** to allow traffic between computers on a LAN.


4. Click **OK**.



If you click **Trusted** this also selects the NetBIOS option which enables file and printer sharing.



3.4 Allow FTP downloads


 If you have allowed the use of a web browser which can access FTP servers, you do not need to allow FTP downloads as well.

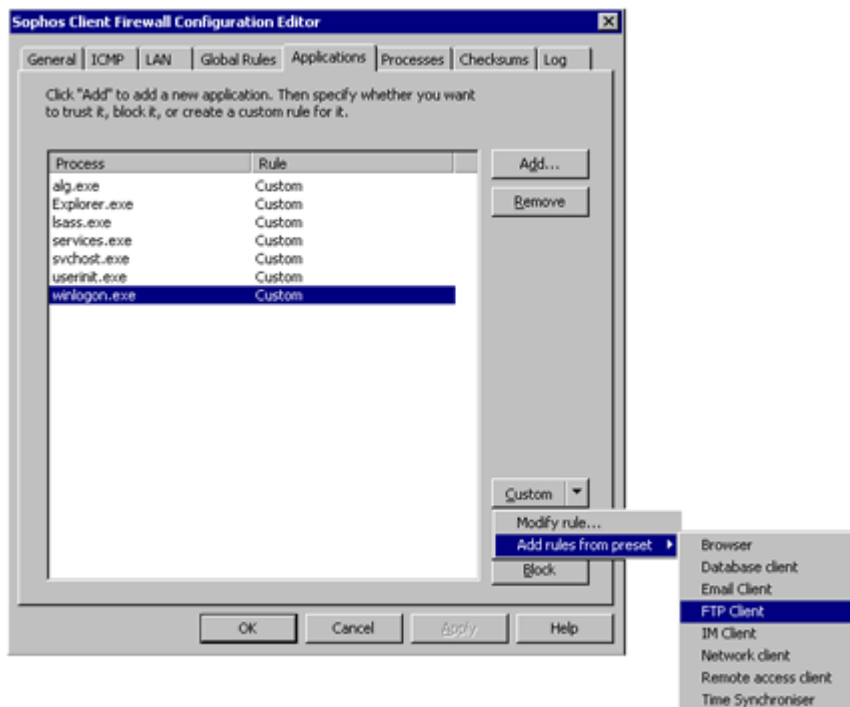
To allow FTP downloads, do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Applications** tab. Click **Add** and find the program used for FTP downloads. The program is added to the list and is now "Trusted".


For greater security, you should apply a preset rule supplied by Sophos. Highlight the program, click the drop-down arrow on the **Custom** button, select **Add rules from preset** and then select **FTP Client**.

4. Click **OK**.

 If you want to set a custom rule for the FTP program, consult the help page **Set rules for applications**.



3.5 Set global rules

 We recommend you set a rule only if you know about networking protocols.


You can specify **global rules** that apply to all network communications or applications which do not already have a rule.


To specify and prioritize global rules do as follows.

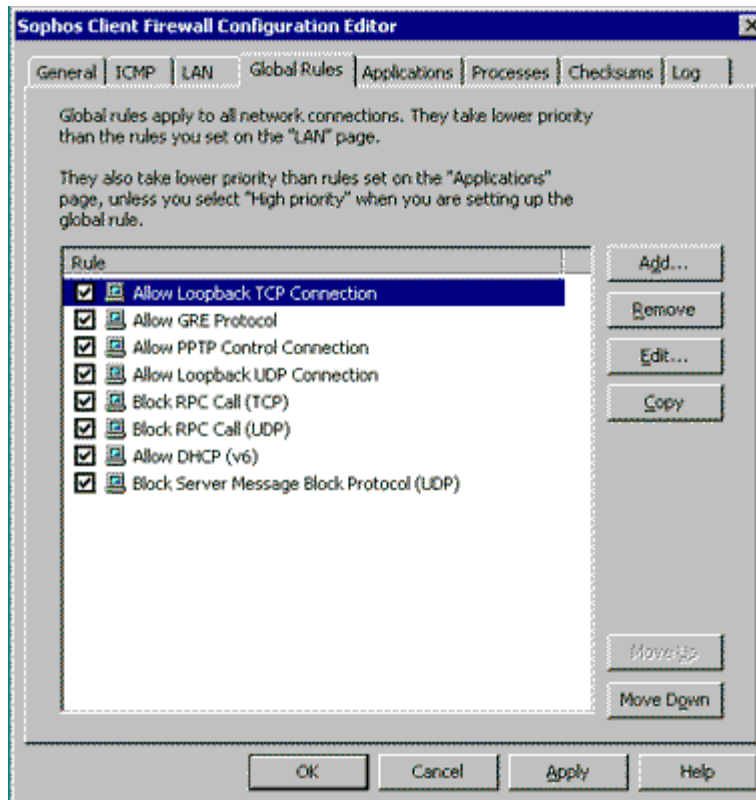
1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Global rules** tab.
3. Click **Add** to add a new rule to the list. See [Setting a rule](#) for further details.

Click **Move Up** or **Move Down** to prioritize the selected rule within the list.


4. Click **OK**.

 Global rules take lower priority than the rules you set on the LAN and Applications pages, unless you select High priority. High priority rules are applied before application rules.

 Default rules and custom rules are distinguished by having different icons. If you try and edit or delete a default rule, a warning appears.



3.6 Set rules for applications

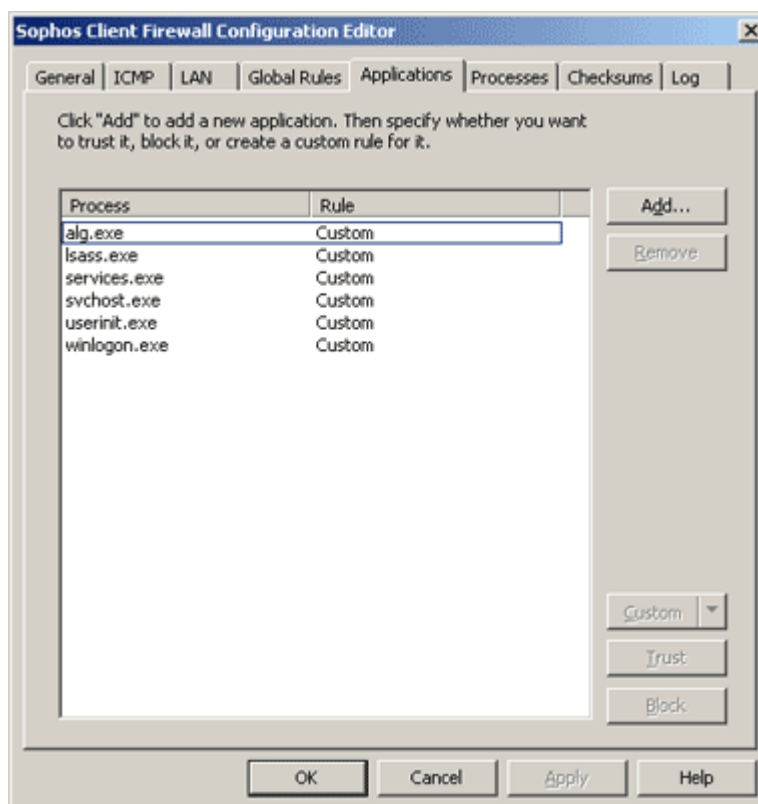
 We recommend you set a rule only if you know about networking protocols.

You can set rules for the way the firewall handles applications as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Applications** tab. Click **Add** to find an application and add it to the list. The application is now trusted, i.e. all network activity is allowed for this application.

Select the application and click **Block** if you want to block it or **Custom** if you want to create a rule that specifies when the application can run. If you click **Custom**, you can apply a preset rule created by Sophos, or use **Modify rules** to [create your own rule](#).

3. Click **OK**.



3.7 Allow applications to launch hidden processes

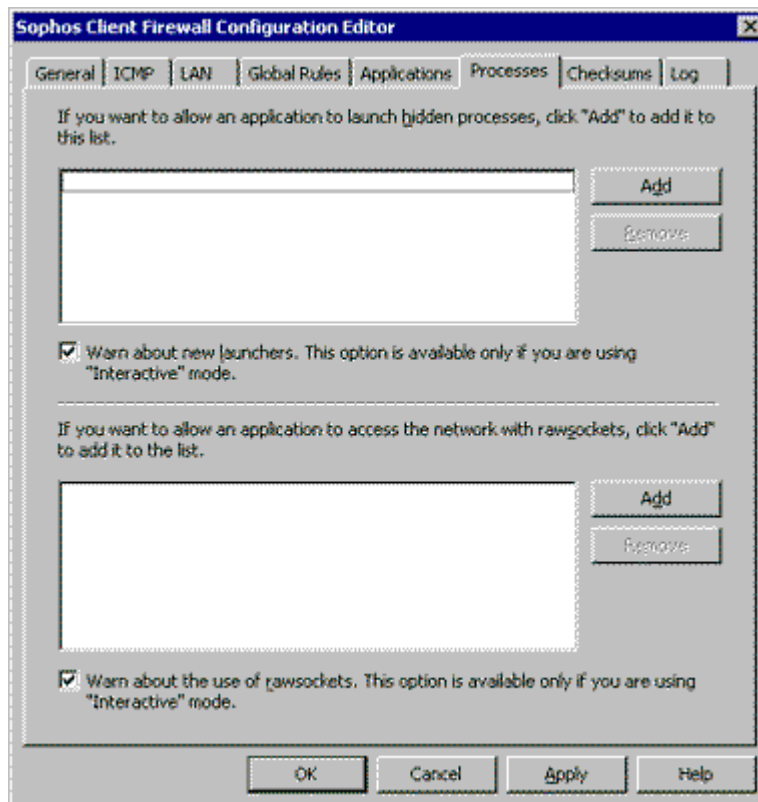
An application sometimes launches another hidden process to perform some network access for it. Malicious applications sometimes use this technique to evade firewalls; they launch a trusted application to access the network rather than doing so themselves.

To specify and manage applications that are allowed to launch hidden processes, do as follows.

1. Right-click the firewall in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Processes** tab.
3. Click the **Add** button next to the first, or upper box to find an application and add it to the list of applications that are allowed to launch hidden processes.

The firewall can inform you when a new launcher is detected. Select **Warn** about new launchers. This option is only available if you are using **Interactive** mode. If this is not selected, new launchers are blocked from launching hidden processes.

4. Click **OK**.



3.8 Allow applications to use rawsockets

Some applications can access a network through rawsockets, which gives them control over all aspects of the data they send over the network. Malicious applications can exploit rawsockets, for example to fake their IP address or send deliberately corrupt messages.

To specify and manage applications which use rawsockets do as follows.

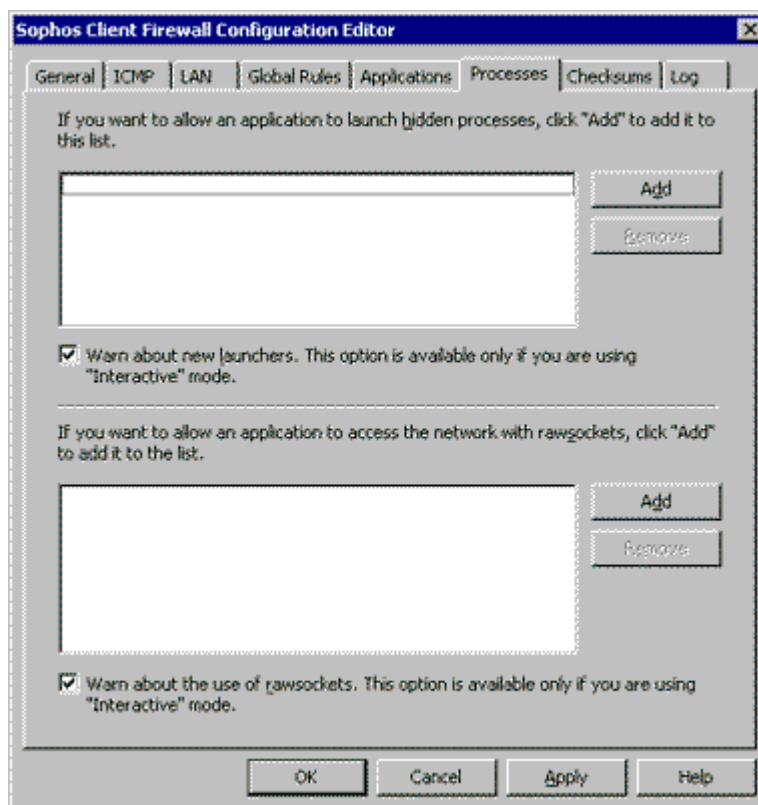
1. Right-click the firewall in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Processes** tab.
3. Click the **Add** button next to the lower list box to find an application and add it to the list of applications that are allowed to use rawsockets.

If you are using interactive mode, the firewall can inform you when a rawsocket is detected if you have selected **Warn about the use of rawsockets**. This option is only available if you are using "interactive" mode. If this is not selected, all rawsocket applications are blocked.

4. Click **OK**.



To receive these warnings, you must have selected Interactive mode on the General tabbed page.



3.9 Use checksums to authenticate applications

Each version of an application has a unique checksum. The firewall can use this checksum to decide whether an application is allowed or not.

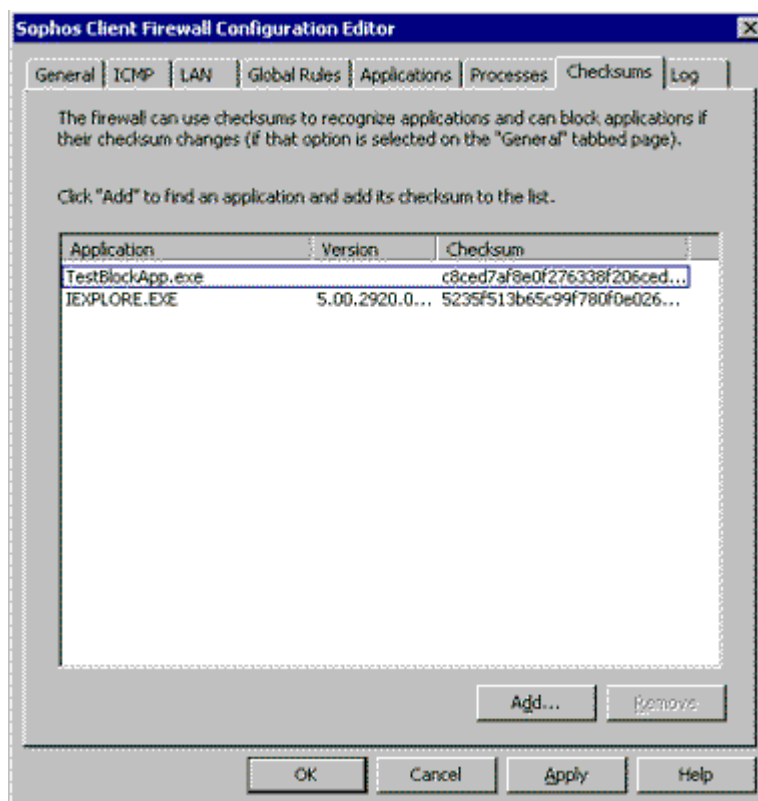
By default, the firewall checks the checksum of each application that runs. If the checksum is unknown or has changed, the firewall blocks it or (in interactive mode) asks the user what to do and changes the tray icon to red. The firewall also sends an alert to the management console, if one is being used, the first time a new or modified application is detected.

You can add checksums to the list of allowed checksums as follows:

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click **Checksums**.
3. To add a checksum click **Add** and select an application.
4. Click **OK**.



Ensure that the Use checksums to authenticate applications option is checked on the General tabbed page.



3.10 Importing and exporting existing configurations

You can import or export configurations that have already been created.

For example, you might want to make rules for the applications on one computer and then export that configuration so that it can be used on other computers running the same set of applications.

You can also take configurations created on several different computers and import them into your central administration console, merging them to create a policy that is valid for all computers on the network.

To manage your configuration files, do as follows.

1. Right-click the firewall icon in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab.
3. To import a policy click **Import**. From the **Import** configuration dialog box, select a configuration file and click **Open**. A pop-up appears.

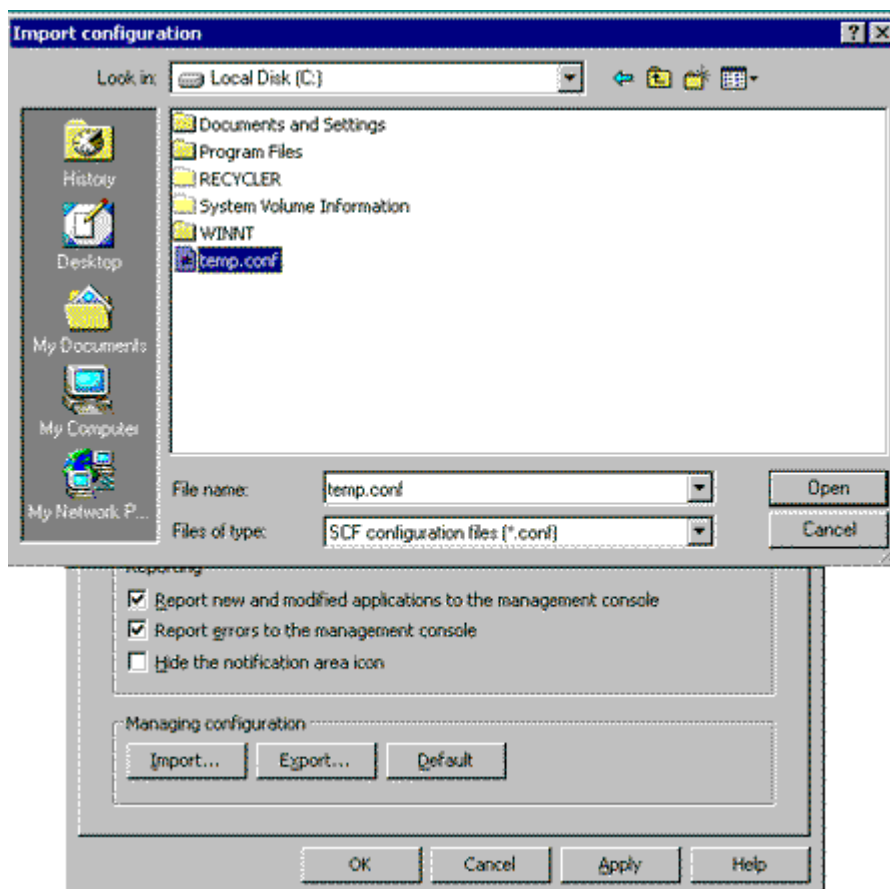
Select **Load the general configuration** checkbox and/or **Load the global and application rules**.

If you selected **Load the global and application rules** checkbox, then select either the **Merge** or the **Overwrite** radio button. Click **OK**.

To export a policy click **Export**. In the **Export** configuration dialog box, give your configuration a name and location and click **Save**.

To restore the default configuration click **Default**. A pop-up appears with the message **Do you really want to revert to the default settings**. Click **Yes** to complete the operation.

4. Click **OK**.



3.11 Which rules take priority?

For connections that do not use rawsockets (the majority), various rules are checked in the following order.

1. If the connection is to an address in one of the ranges specified on the LAN property page that has been marked as trusted the connection is allowed with no further checks.
2. If the network only allows NetBIOS any connection that meets the following criteria is allowed.
 - Any TCP connection where the remote port is in the range 137-139 or 445.
 - Any TCP connection where the local port is in the range 137-139 or 445.
 - Any UDP connection where the remote port is 137 or 138.
 - Any UDP connection where the local port is 137 or 138.
3. High priority global rules are checked in the order they are listed.
4. If the connection has not already been handled (had rules applied to it), the firewall checks the application rules.
5. If the connection has still not been handled, the firewall will apply the normal priority global rules.
6. If no rules have been found to handle the connection and the firewall is in Interactive mode, the user will be asked what to do.

4 How do I configure reporting and logging?

- Configure central reporting
- Configure logging


4.1 Configure central reporting

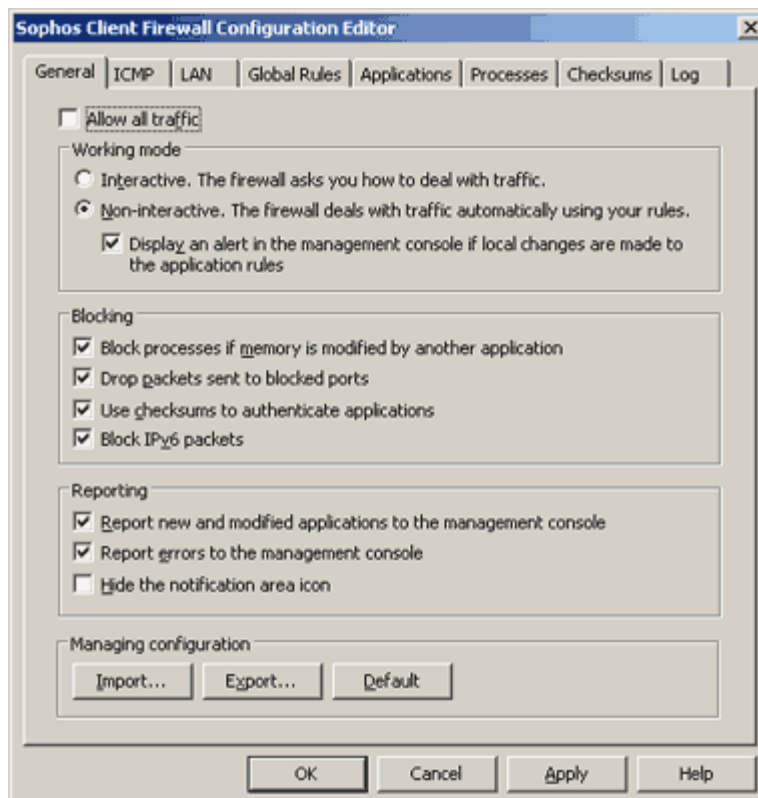
By default, the firewall reports the following to the central management console (if one is being used to manage the firewall):

- new and modified applications
- errors

To change the reporting settings, do as follows.

1. Right-click the firewall in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab. In the **Reporting** panel, enable or disable each type of reporting.
3. Click **OK**.

 Sophos Client Firewall can report new and modified applications only if **Use checksums to authenticate applications** is selected on this page.



4.2 Configure logging

To manage the size and contents of the event log database do as follows.

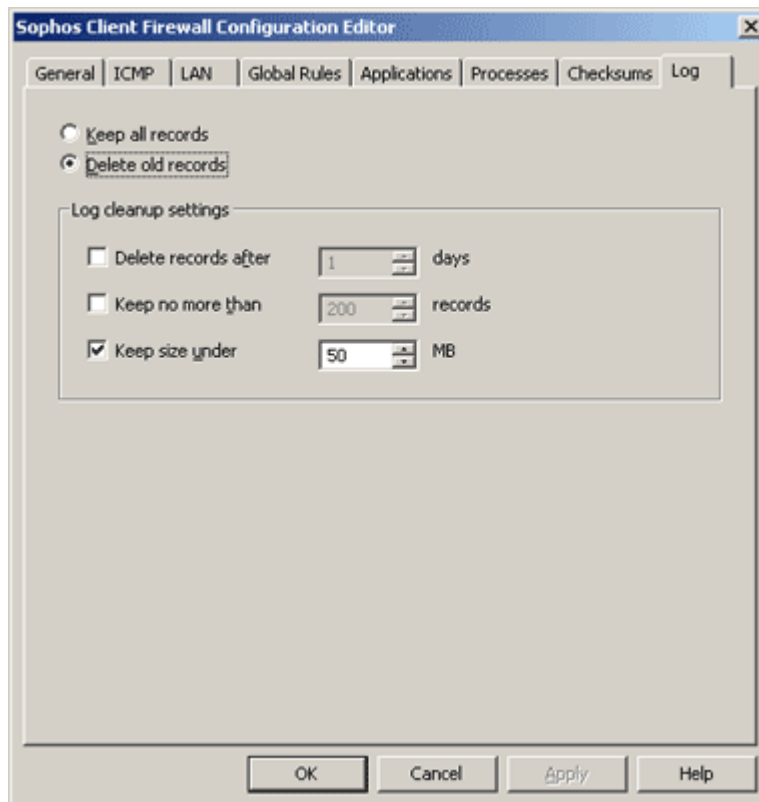
1. Right-click the firewall in the system tray and select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **Log** tab.
3. To allow the database to grow with out limit, click **Keep all records**.

To clear out old records when the size of the log reaches the limits specified in the **Log cleanup settings** control panel, click **Delete old records**. This is the default option.

To set **Log cleanup settings** select one or more of the following options:

- Click the **Delete records after** checkbox and enter or select a figure in the **Days** checkbox. This is unselected by default.
- Click the **Keep no more than** checkbox and enter or select a figure in the **Records** checkbox. This is unselected by default.
- Click the **Keep size under** checkbox and enter or select a figure in the **Mb** checkbox. This is selected by default and with the size set to 50Mb.

4. Click **OK**.



5 How do I work in interactive mode?

If you are in **Interactive** mode the firewall notifies you each time an unknown application requests network access. The firewall then asks you whether to allow the traffic once, block it once, or whether to make a rule for that type of traffic.

You will see the following message types.

- Hidden processes message
- Protocol message
- Application message
- Rawsocket message
- New or modified application message

5.1 Hidden process message

A hidden process is when one application launches another one to perform some network access for it. Malicious applications sometimes use this technique to evade firewalls; they launch a trusted application to access the network rather than doing it themselves.


The pop-up dialog box displays the hidden process and the application that launched it.

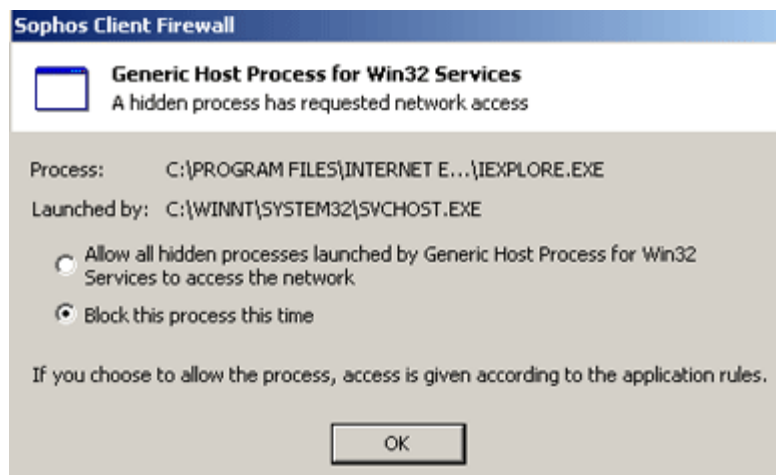
Select one of the following options:

Allow all hidden processes launched by ... to access the network adds a new rule and allows this application to launch hidden processes.

Block this process this time denies access for this particular process, at this point in time. This is the default option and will also be selected if you press the **Escape** key.

Click **OK**.

 This pop-up dialog box is only displayed if you have selected **Warn about new launchers**, on the Processes page.



5.2 Protocol message

Occasionally the firewall detects some network activity by the system that it cannot relate to a specific application. In this case it prompts for the creation of a protocol rule.

The pop-up dialog box displays the unrecognized network activity, i.e. the protocol and remote address.

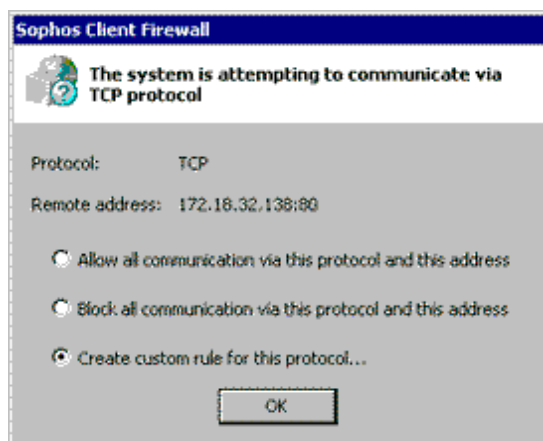
Select one of the following options:

Allow all communication via this protocol and this address adds a rule to allow communication with the specified address via the specified protocol.

Block all communication via this protocol and this address adds a rule to block communication with the specified address via the specified protocol. If you press **Escape**, you block communication via this protocol and this address on this occasion only.

Create custom rule for this protocol allows you to create a custom rule (which controls whether the communication is allowed or blocked). This is the default option. See [Setting a rule](#) for further details.

Click OK.



5.3 Application message

If the firewall detects an application attempting to access the network in a way that is not covered by any existing rule, it prompts for the creation of an application rule.

The pop-up dialog box displays the unrecognized network activity, i.e. the remote service and the remote address.

Select one of the following options:

Allow all activity for this application this time only allows this particular connection once. This does not create a rule, so the message will be displayed again next time the connection is attempted.

Allow all activity for this application creates a simple application rule allowing this application unrestricted network access.

Block all activity for this application this time only blocks this particular connection once. This does not create a rule, so the message will be displayed again next time the connection is attempted. This option will also be selected if you press the Escape key.

Block all activity for this application creates a simple application rule denying this application any network access.

Create a rule for this application using preset allows you to select a preset rule configured by Sophos. Alternatively, select **Custom...** to create your own rule. See [Setting a rule](#) for further details.

When you have finished click OK.



5.4 Rawsocket message

Rawsockets allow processes to control all aspects of the data they send over the network and can be used for malicious purposes. You can manage rawsockets by responding to a pop-up dialog box which the firewall displays when there is no rule to allow access for a particular rawsocket.

The pop-up dialog box displays details about the rawsocket.

Select one of the following options:

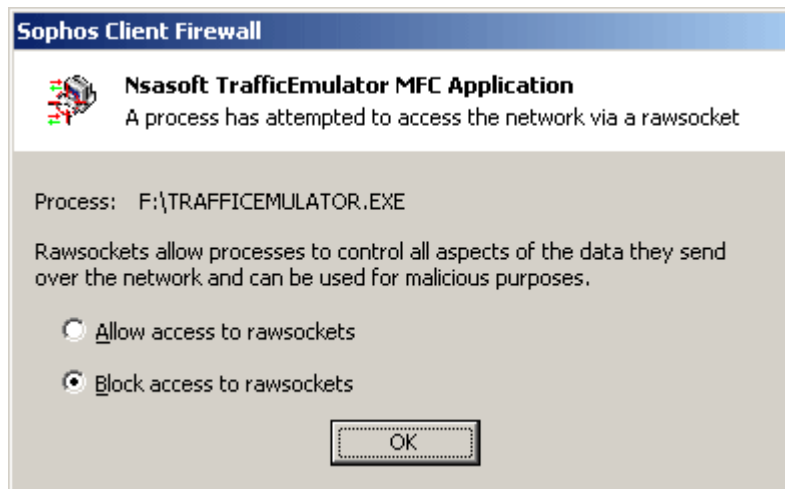
Allow access to rawsockets adds a rule to allow this application to use rawsockets (i.e. have unlimited network access).

Block access to rawsockets blocks this process instance from accessing the network. This does not add a rule, so next time the application runs you will see a prompt again. This is the default option and will also be selected if you press the **Escape** key.

Click **OK**.



This pop-up dialog box is only displayed if you have selected the Warn about the use of rawsockets. check box on the Processes page.



5.5 New or modified application message

If the firewall detects a new or modified application, it displays a message, (provided you have selected **Use checksums to authenticate applications** on the **General** configuration page).

If you want to allow the application to access the network, you must add its checksum (a unique identifier) to the list of recognized checksums.

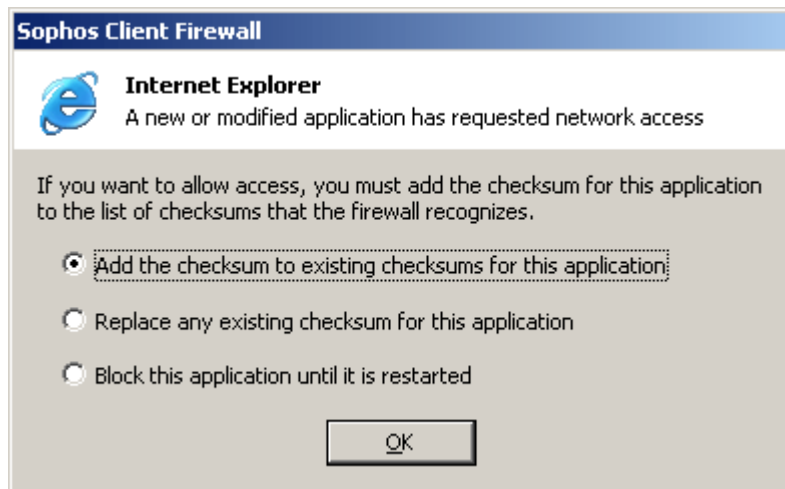
Select one of the following options:

Add the checksum to existing checksums for this application allows multiple versions of this application.

Replace any existing checksum for this application replaces all existing checksums for the application with the one requesting access, and thereby allows only the latest version of this application.

Block this application until it is restarted blocks the application on this occasion. This is the default option and will also be selected if you press the **Escape** key.

When you have finished, click **OK**.



6 How do I use the log viewer?

You can use the log viewer to see records of allowed and blocked traffic as well as a system log.

To access the system log, right-click the firewall icon in the system tray and select **View Log**:

This section describes the main settings for the log viewer.

- Introduction to the log viewer
- Blocked connections
- Allowed connections
- Processes
- System log

6.1 Introduction to the log viewer

The log viewer allows you to view details from the event database. This includes such things as the connections that have been allowed or blocked, the system log and any alerts that have been raised.

The log viewer is divided into two panes. The left-hand pane shows a menu tree where you can select different screens and the right hand pane lists relevant logged information for the particular screen. These include:

- Blocked connections
- Allowed connections
- Processes
- System log

You can also customize the screen layout, re-arrange the data display and export data to a file. Customization options include:

- Filter log entries
- Add/Remove columns
- Customize data format
- Customize screen layout

6.2 Blocked connections

The log viewer allows you to view details from the event database. This page deals with connections that have been blocked. The date and time of attempted connection is shown in the **Start Time** field. For today's blocked connections, only the time is displayed. The fields **Up Time**, **Data Rate**, **Sent**, and **Recv** display data once a connection is closed.

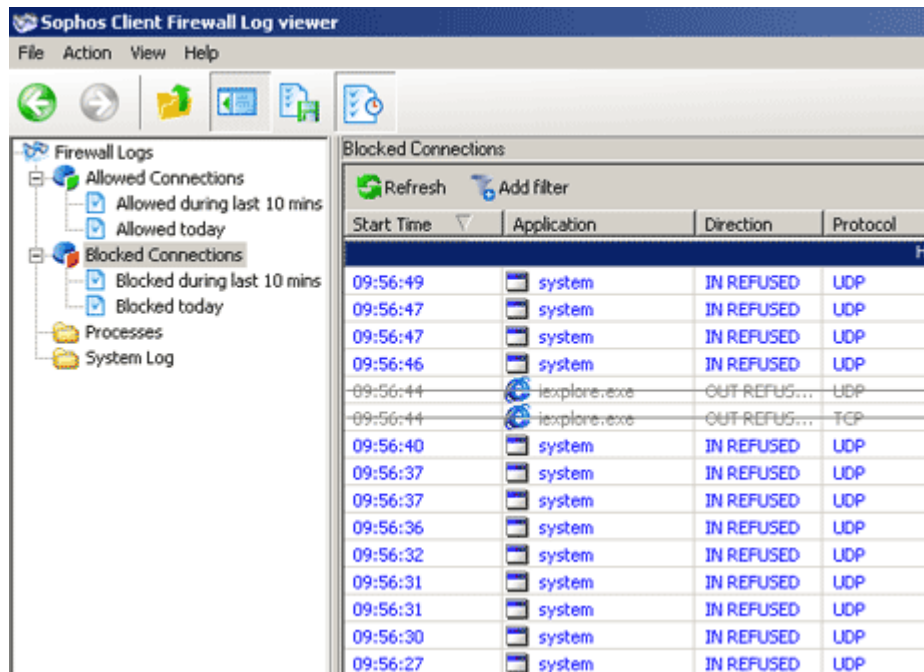
In some cases, the log may show a blocked connection which has a message such as 'Learning mode' in the **Reason** field. In this case, you are simultaneously being asked to respond to a corresponding learning dialog popup screen. The message will change to reflect your choices. If you allow the connection, the whole entry is moved to the [Allowed Connections](#) page and the entry is displayed in grey with a line through it.

By clicking on the relevant tree node, you can also see the following:

- Blocked during last 10 mins
- Blocked today

To manage the data further you can:

- Filter log entries
- Add/Remove columns
- Customize data format
- Customize screen layout



6.3 Allowed connections

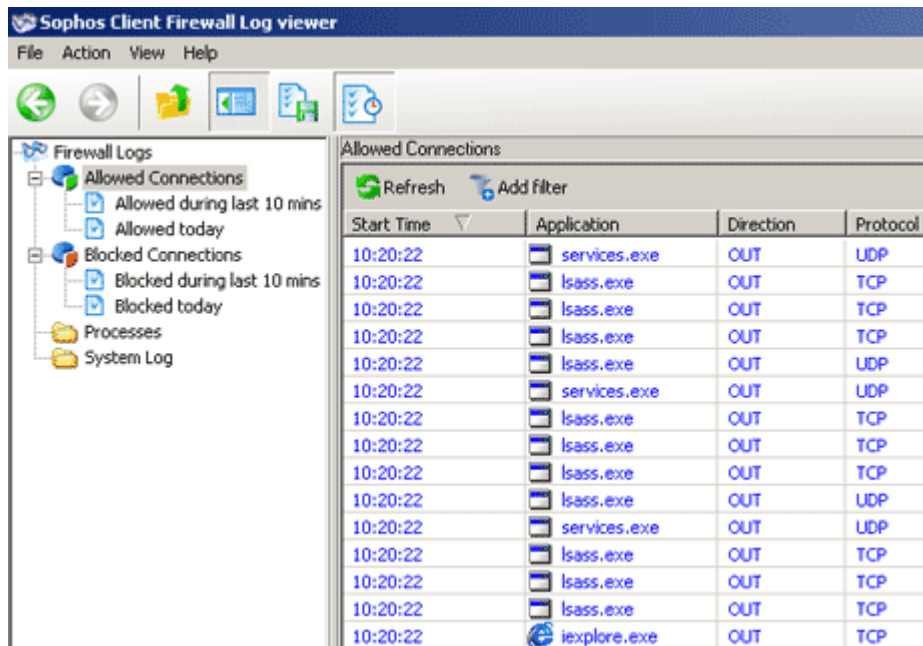
The log viewer allows you to view details from the event database. This page deals with connections that have been allowed. The date and time of connection is shown in the **Start Time** field. For today's connections, only the time is displayed. The fields **Up Time**, **Data Rate**, **Sent**, and **Recv** display data once a connection is closed.

By clicking on the relevant tree node, you can also see the following:

- Allowed during last 10 mins
- Allowed today

To manage the data further you can:

- Add/Remove columns
- Customize data format
- Customize screen layout

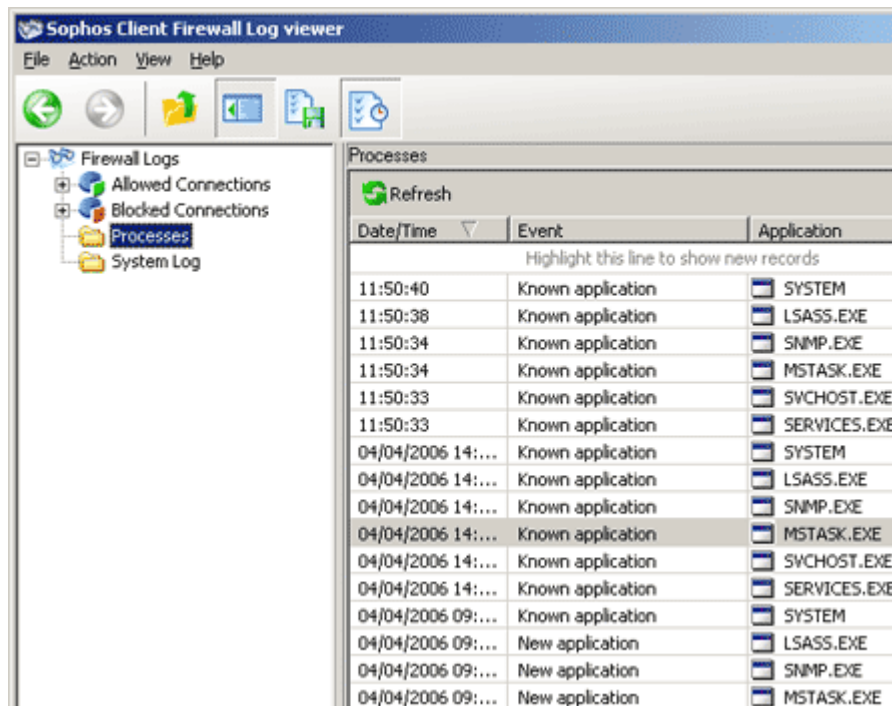


6.4 Processes

The log viewer allows you to view details from the event database. This page deals with processes and checksums. For today's events, only the time is shown in the **Date/Time** field.

To manage the data further you can:

- Add/Remove columns
- Customize data format
- Customize screen layout

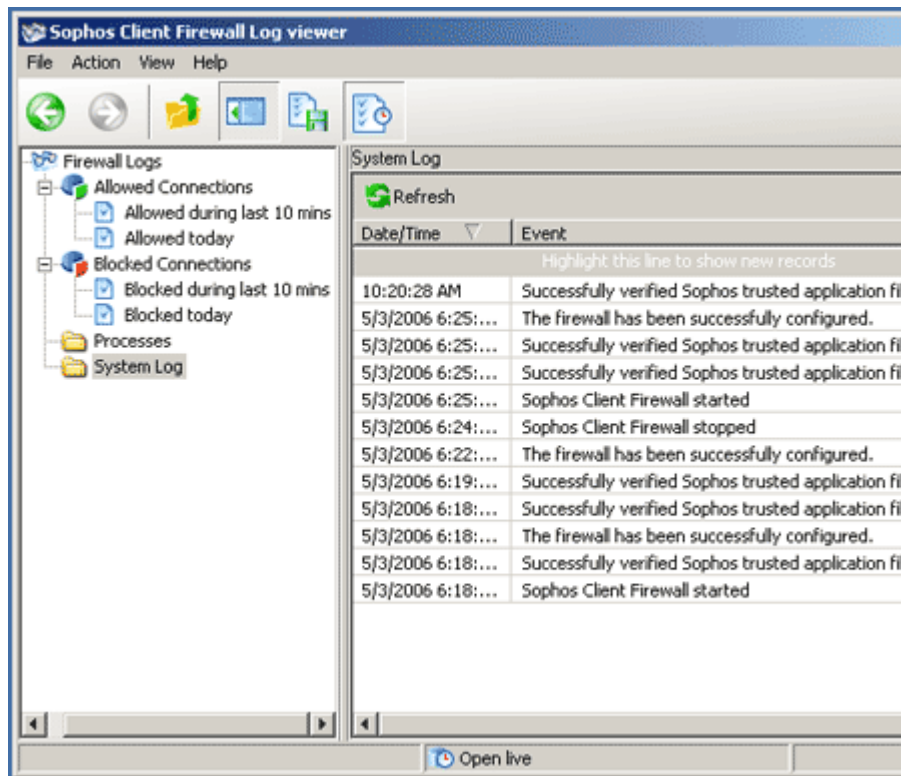


6.5 System log

The system log allows you to view network activity logged over a period of time. By default the screen displays the **Date/time** and the **Event** fields. For today's connections, only the time is displayed.

To manage the data further you can:

- Add/Remove columns
- Customize data format
- Customize screen layout



7 Glossary

The glossary provides definitions for terms used in this guide.

- What is an application rule?
- What is a global rule?
- What is a hidden process?
- What is a network protocol?
- What is a rawsocket?
- What is a checksum?
- What is ICMP traffic?
- What is NetBIOS?

7.1 What is an application rule?

An **application rule** is a rule that applies just to packets (data transferred over the network) to or from a particular application.

If you encounter a pop-up dialog box relating to application rules, see [Application message](#) for further information.

7.2 What is a global rule?

Global rules are rules applied to all network connections and applications which do not already have a rule. They take lower priority than the rules set on the LAN page. They also take lower priority than rules set on the **Applications** page, unless you specify otherwise.

If you encounter a pop-up dialog box relating to global rules, see [Protocol message](#) for further information.

7.3 What is a hidden process?

An application sometimes launches a **hidden process** to perform some network access for it. Malicious applications sometimes use this technique to evade firewalls; they launch a trusted application to access the network rather than doing so themselves.

If you encounter a pop-up dialog box relating to hidden processes, see [Hidden process message](#) for further information.

7.4 What is a network protocol?

A **network protocol** is a set of rules or standards designed to enable computers to connect with one another over a network and to exchange information with as little error as possible.

7.5 What is a rawsocket?

Rawsockets allow processes to control all aspects of the data they send over the network and can be used for malicious purposes.

If you encounter a pop-up dialog box relating to rawsockets, see [Rawsocket message](#) for further information.

7.6 What is a checksum?

Each version of an application has a unique **checksum**. The firewall can use this checksum to decide whether an application is allowed or not.

If you encounter a pop-up dialog box relating to an unknown checksum, see [New or modified application message](#) for further information.

7.7 What is ICMP traffic?

ICMP, or Internet Control Message Protocol is a network-layer Internet protocol that provides error correction and other information relevant to IP packet processing.

To manage ICMP traffic, see [Allow incoming or outgoing ICMP traffic](#) for further details.

7.8 What is NetBIOS?

NetBIOS, or Network Basic Input Output System is software developed by IBM that provides an interface between the PC operating system, the I/O bus and the network. Nearly all Windows-based LANs for PCs are based on NetBIOS.

7.9 Further information on ICMP traffic

Echo Request and **Echo Reply** ICMP messages are used to test destination accessibility and status. A host sends an **Echo Request** and listens for a corresponding **Echo Reply**. This is most commonly done using the ping command.

A **Destination Unreachable** is generated by a router when it cannot deliver an IP datagram. A datagram is the unit of data, or packet, transmitted in a TCP/IP network.

A **Source Quench** ICMP message is returned by a host or router if it is receiving data too quickly for it to handle. The message is a request that the source reduce its rate of datagram transmission.

A **Redirect** ICMP message is sent by a router if it receives a datagram that should have been sent to a different one. The message contains the address to which the source should direct future datagrams. This is used to optimize the routing of network traffic.

The **Router Advertisement** and **Router Solicitation** ICMP messages allow hosts to discover existence of routers. Routers periodically broadcast their IP addresses in a **Router Advertisement** message. Hosts may also request a router address by broadcasting a **Router Solicitation** message to which a router will reply with a **Router Advertisement**.

A **Time Exceeded for Datagram** ICMP message is sent by a router if the datagram has reached its maximum limit of routers through which it can travel.

A **Parameter Problem on Datagram** ICMP message is sent by a router if a problem occurs during the transmission of a datagram such that it cannot complete processing. One potential source of such a problem is invalid datagram header.

The **Timestamp Request** and **Timestamp Reply** ICMP messages are used to synchronize the clocks between hosts and to estimate transit time.

The **Information Request** and **Information Reply** ICMP messages are obsolete. They were used earlier by hosts to determine their inter-network addresses, but are now considered outdated and should not be used.

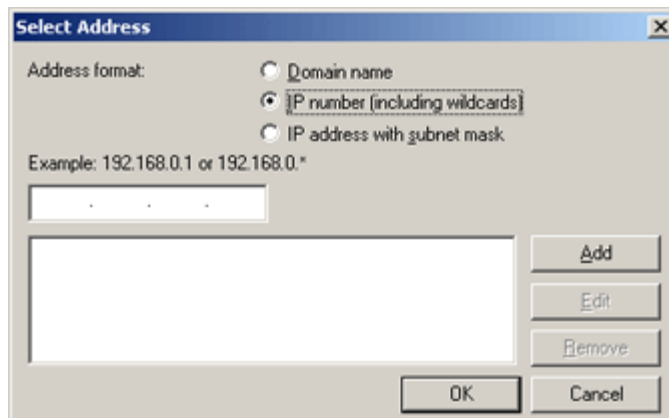
The **Address Mask Request** and **Address Mask Reply** ICMP messages are used to find the mask of the subnet (i.e. what address bits define the network). A host sends an **Address Mask Request** to a router and receives an **Address Mask Reply** in answer.

7.10 Select address

The Select Address pop-up is called from the LAN dialog box.

To specify one or more addresses for your LAN page do the following:

1. To add an address, click **Add**, and select an address format. There are three types of address:
 - Click **Domain name** to enter a domain name, e.g. www.sophos.com
 - Click **IP number (including wildcards)** to enter an IP number, e.g. 192.168.0.1 or use the wildcard * to replace any group of numbers, e.g. 192.168.0.*.
 - Click **IP address with subnet mask**, e.g. 192.168.0 (255.255.255.0)
2. To edit an address, highlight an address and click **Edit** and modify accordingly.
3. To remove an address, highlight an address and click **Remove**.
4. Click **OK**.



7.11 Further information on default global rules

This section describes the attributes and values of default global rules.

Allow DNS Resolving (TCP)

- **Protocol:** TCP
- **Direction:** Outbound
- **Remote port:** DOMAIN
- **Action:** Allow

Allow DNS Resolving (UDP)

- **Protocol:** UDP
- **Direction:** Outbound
- **Remote port:** DNS
- **Action:** Allow Stateful inspection

Allow Outgoing DHCP

- **Protocol:** UDP
- **Local port:** BOOTPS,BOOTPC,546,547
- **Action:** Allow

Allow Inbound Identification

- **Protocol:** TCP
- **Direction:** Inbound
- **Local port:** AUTH
- **Action:** Allow

Allow Loopback

- **Protocol:** TCP
- **Direction:** Inbound
- **Local port:** 127.0.0.0 (255.255.255.0)
- **Action:** Allow

Allow GRE Protocol

- **Protocol:** TCP
- **Protocol type:** Outbound
- **Action:** Allow

Allow PPTP Control Connection

- **Protocol:** TCP
- **Direction:** Outbound
- **Remote port:** PPTP
- **Local port:** 1024-65535
- **Action:** Allow

Block RPC Call (TCP)

- **Protocol:** TCP
- **Direction:** Inbound
- **Local port:** DCOM
- **Action:** Block

Block RPC Call (UDP)

- **Protocol:** UDP
- **Local port:** 135
- **Action:** Block

Block Server Message Block Protocol (TCP)

- **Protocol:** TCP
- **Direction:** Inbound
- **Local port:** MICROSOFT_DS
- **Action:** Block

Block Server Message Protocol (UDP)

- **Protocol:** TCP

- **Local port:** 445
- **Action:** Block

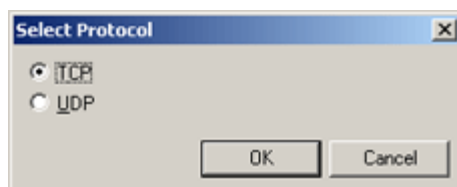
Allow Localhost UDP Connection

- **Protocol:** UDP
- **Remote host:** 255.255.255.255 (0.0.0.0)
- **Local host:** 255.255.255.255 (0.0.0.0)
- **Where the local port is equal to the remote port:** True
- **Action:** Allow

7.12 Selecting a protocol

The **Select protocol** pop-up is called from the **Edit Rules** dialog box. The pop-up differs according to whether you are setting a global or an application rule.

1. If you are setting a **global rule**, select one of the following:
 - **TCP** - Transmission control protocol
 - **UDP** - User Datagram Protocol
 - **IP** - Internet protocol
2. If you are setting an **application rule**, select one of the following:
 - **TCP** - Transmission control protocol
 - **UDP** - User Datagram Protocol



7.13 Selecting an address

The Select Address pop-up is called from the Rules Description box. This page allows you to specify one or more addresses to apply to your selected rule.

To specify one or more addresses do the following:

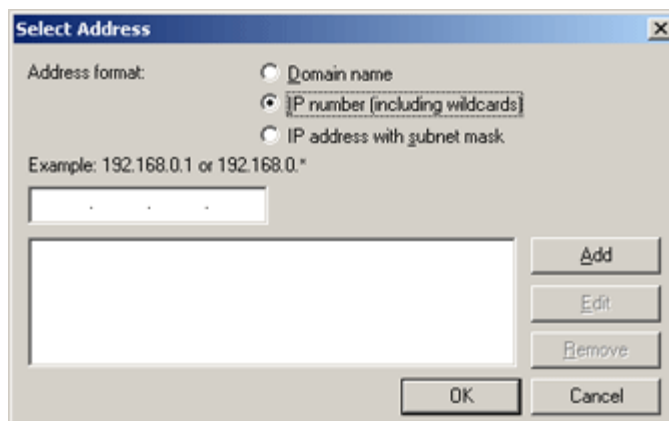
1. To add an address, select an address format and enter an address.

There are three types of address:

- Click **Domain name** to enter a domain name, e.g. www.sophos.com
- Click **IP number (including wildcards)** to enter an IP number, e.g. 192.168.0.1 or use the wildcard * to replace any group of numbers, e.g. 192.168.0.*.
- Click **IP address with subnet mask**, e.g. 192.168.0.1 (255.255.255.0)

Click **Add**.

2. To edit an address, highlight an address and click **Edit**, and modify accordingly.
3. To remove an address, highlight an address and click **Remove**.
4. To save click **OK**.



7.14 Selecting a direction

The **Direction** pop-up is called from the **Rules Description** dialog box. This page allows you to select one or more directions of communication relating to a specific rule. No option is selected by default.

1. Select one or both options:
 - Click **Inbound** (from the remote host to your computer)
 - Click **Outbound** (from your computer to the remote host)
2. Click **OK** to save.

7.15 Selecting a port

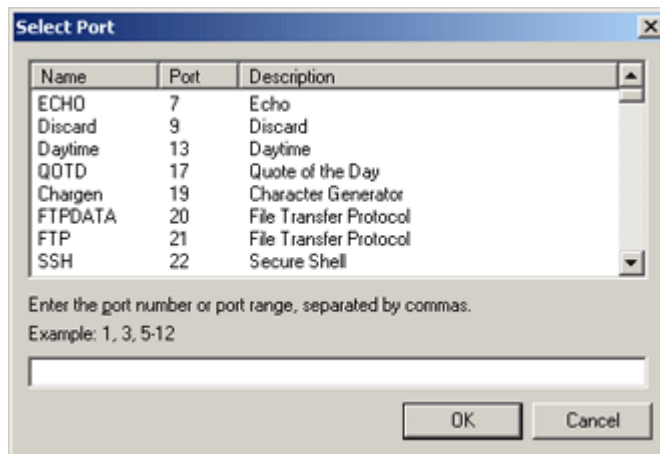
The **Select Port** popup is called from the **Rules Description** box. This page allows you to select a port relating to a specific rule. The list contains a list of common ports and what they are used for. The ports shown depend on the selected protocol.

To select one or more ports:

1. Double click or highlight a port and click **OK**.
Alternatively, enter the port name and number, e.g. "Chargen, 27, FTP-SSH".
2. To select more than one port, enter the port number or port range, separated by commas, e.g. 1.3, 5-15.
3. Click **OK** to save.



You can not specify the local or remote port, or that the local and remote port should be equal, if you have selected IP protocol.



7.16 Add/Remove columns


You can select and arrange the columns you view in the log.

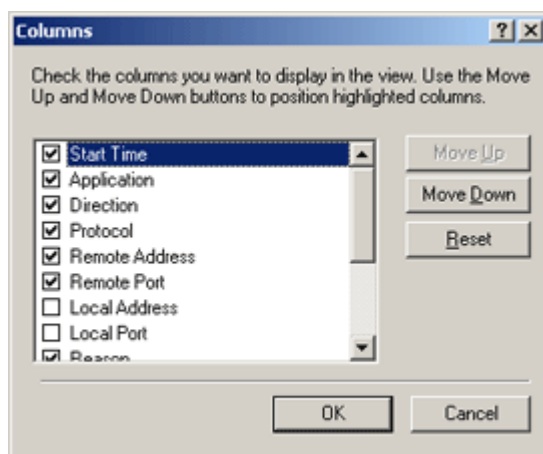
To specify the columns and their order do the following:

1. From the **View** menu, select **Add/Remove Columns**.
2. Click a checkbox to display the relevant field in the log.

Click **Move up** or **Move down** to position a highlighted field within the list. This determines the order of columns in the log.

3. Click **OK** to save.

 Click **Reset** to reset the column selection and order to the default setting,

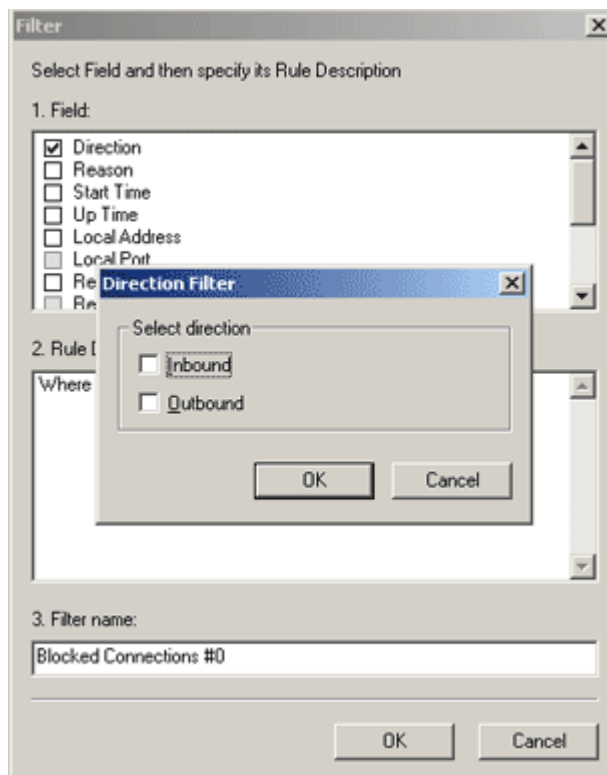


7.17 Filter log entries

You can sort the record set by creating a filter using one or more fields.

To create a filter:

1. Click the **Filter** icon, or from the **Action** menu, select **Filter**.
2. Click one or more checkboxes in the **Field** pane to sort by those fields (the contents of this list depend on the selected record set). The field appears in the **Rule description** box and is specified as **Undefined**.
3. Click the word **Undefined** in the **Rule description** pane and select a description from the relevant pop-up. For instance, in this example, click **Inbound** to create a filter of inbound traffic and click **OK**.
4. Enter the name of the filter in the **Filter name** box.
5. Click **OK** to save.



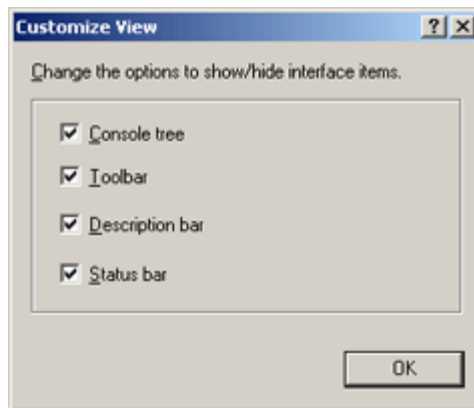
7.18 Customize screen layout

To specify which parts of the log viewer you want to display, do the following:

1. From the **View** menu, select **View Layout**.
2. In the **Customize View** dialog box, select the features you want to display.

The **Console** tree is the left-hand pane. The **Toolbar** is at the top of the viewer. The **Description** bar is above the data in the right-hand pane. The **Status** bar is at the bottom of the viewer.

3. Click **OK**.



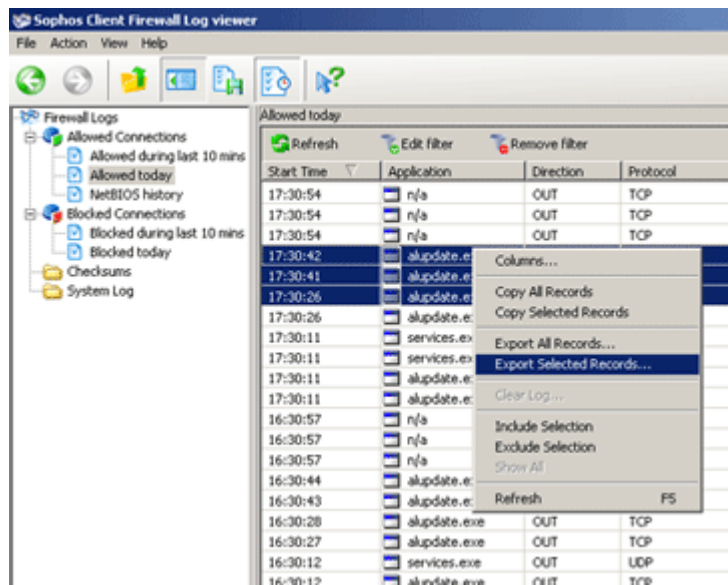
7.19 Exporting records from the Log viewer

To export records from the log viewer to a text file do the following:

1. Either highlight the records required and right-click and select **Export Selected Records** from the drop down menu.

Or right-click and select **Export all records**.

2. In the **Save As** dialog box, enter the name of the file and click **Save**.

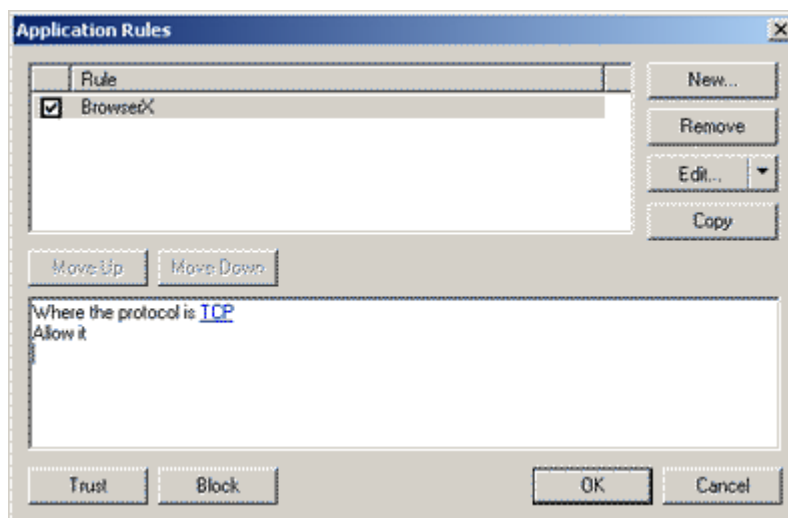


7.20 Application Rules dialog box

The Application Rules dialog box is available from the **Modify rules** option on the **Applications** page.

To specify an application rule, do the following:

1. To add an application rule click **New**. See [Setting a rule](#) for further details.
2. To remove a selected rule click **Remove**.
3. To customize a rule for a selected application, click **Edit**. You can either select a rule created for you by Sophos (a preset) to apply to your application or create your own rule.
 - Click **Add rules from preset** to append rules relating to that preset to the list of rules for the application. Presets include the following: FTP client, email client, browser, download manager, time synchronizer, telnet client, IRC client, ICQ client and allow ident.
 - Click **New rule...** to create custom rules which allow fine control over what access is allowed. See [Setting a rule](#) for further details.
4. To copy the selected rule and append it to the list of rules, click **Copy**.
5. To specify the selected application as **Trusted** click **Trust**.
To specify the selected application as **Blocked** click **Block**.
6. Click **OK** to save.

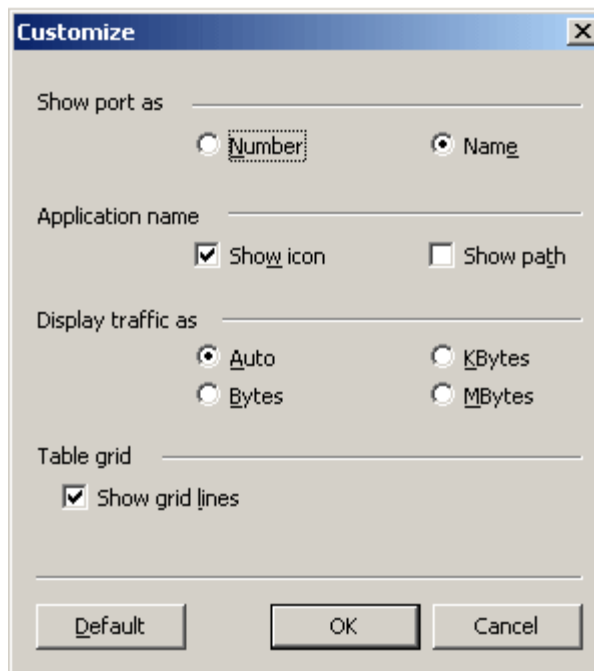


7.21 Customize data format

You can choose how to display the data in the log.

To customize the data format:

1. From the **View** menu, select **Customize**.
2. Specify how the port and application are shown in the log. You can also specify the units used to show traffic (if you select **Auto**, the firewall selects the most appropriate units automatically).
3. Click **OK** to save the new setting.



7.22 Setting a rule



We recommend you set a rule only if you know about networking protocols.

Rules check connections that do not use rawsockets. From this screen you can create global rules, if the screen was called from the global rules page, or application rules if the screen was called from the applications page.

To set a rule do the following:

1. Enter a rule name in the **Rule Name** box. The name must be unique within a group, e.g. two global rules cannot have the same name, nor can two rules for a particular application, but two applications can each have a rule with the same name.
2. Click the **High priority rule** checkbox if you want to set a global rule as high priority. High priority rules are applied before any other global or application rules. Next come application rules and finally normal priority global rules. This option is unselected by default.
3. In the **Select Event** the rule will handle box specify the events the connection must match for the rule to apply. All rules must specify the protocol. In addition they may include any of the following:
 - Where the direction is
 - Where the remote address is
 - Where the remote port is (only available if the protocol is not IP)
 - Where the local address is (not available for application rules)
 - Where the local port is (only available if the protocol is not IP)
 - Where the local port is equal to remote port (only available if the protocol is not IP)
4. In the **Select actions with which the rule will respond** box, select **Allow it** or **Block it** and optionally **Stateful inspection**. If you select Stateful inspection the rule will intelligently allow replies from the remote computer based on the initial connection.
 - Allow it
 - Block it

- Stateful inspection
5. The **Rule description** box displays a summary of your selected events and actions. Initially events are displayed with a default value which is linked to a popup. Click on a link to select a value relating to the event. Depending on the event you will see one of the following selection boxes
- Selecting a protocol
 - Selecting a direction
 - Selecting an address
 - Selecting a port

Add Rule

1. Rule name: High priority rule
block outward traffic where protocol is TCP

2. Select the events the rule will handle:

- Where the direction is
- Where the remote address is
- Where the local address is
- Where the remote port is
- Where the local port is
- Where the local port is equal to the remote port

3. Select the actions with which the rule will respond:

- Allow it
- Block it
- Stateful inspection

4. Rule description (click on a link to specify a value):
Where the protocol is [TCP](#)
and the direction is [Outbound](#)
Block it

OK Cancel

8 Technical support

For technical support, visit www.sophos.com/support.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

Index

A

address:select 54
application rule:definition 47
application rules:dialog box 60
application rules:set 22

C

checksum:definition 48
checksums:allow 27
configure:firewall 15

D

direction:select 55

E

email:allow 10

F

file and printer sharing:allow 11
FTP downloads:allow 19

G

getting started: what to do first 6
getting started:overview 5

global rule:definition 47
global rules:defaults 51
global rules:set 20
glossary:overview 46

H

hidden process:definition 47
hidden processes:allow 23

I

ICMP traffic 17
ICMP traffic:definition 48
ICMP traffic:descriptions of 49
importing configurations 29
interactive mode:application 37
interactive mode:checksum 39
interactive mode:global rule 36
interactive mode:hidden processes 35
interactive mode:overview 34
interactive mode:rawsocket 38
interactive mode:select 16
interactive mode:setting mode 12
interface:overview 7

L

LAN traffic:allow 18
log viewer:allowed connections 43
log viewer:blocked connections 42
log viewer:introduction 41
log viewer:overview 40
log viewer:processes 44

logging 31
logging:configure 33

N

NetBIOS:definition 48
non-interactive mode:select 16

O

off:turn firewall off 13
on:turn firewall on 13
overview:configure 15

P

port:select 55
protocol:definition 47
protocol:select 53

R

rawsocket:definition 47
rawsockets:allow 25
reporting 31
reporting:central 32
rule priority 31
rule:set 62

S

select address 50
setting a rule 62
system log:columns 56

system log:customize data 61
system log:customize screen 58
system log:export records 59
system log:filter 57
system log:overview 45
system tray icon 8

W

web browser:allow 9

Copyright © 2007 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.