SoftPerfect Bandwidth Manager

User Manual

www.softperfect.com

Contents

About

About Bandwidth Manager 3
Licence agreement 5
Purchase and contact 8

Reference

Getting started 9
Rules 12
Groups 19
Usage reports 21
Usage web-access 25
Live usage monitor 27
Notifications 28
Global settings 31
Internal bridging 37
Quotas 41
Quota boost 44
Scheduling 48
Event viewer 50
Usage examples 51
Port mapping 55

Troubleshooting

Known issues and FAQ 58

Integration with other products

Adding proxy server 60

Introduction

Are your Internet costs rocketing? Does inappropriate use of your network have an adverse effect on your business performance? Did the Internet access bandwidth become a major bottleneck in your network?

If your network has any of these problems, SoftPerfect Bandwidth Manager will provide a cost-effective solution. The software monitors your network traffic and limits bandwidth in whatever manner you specify. The result is an immediate increase in the efficiency of your network together with a reduction in your overall bandwidth requirements while allowing important Internet applications to run at full speed.

SoftPerfect Bandwidth Manager is a full-featured traffic management tool for Windows that offers cost-effective bandwidth control and quality of service based on built-in prioritised rules. These rules can specify a bandwidth limit for each Internet user. The software of this kind is otherwise known as bandwidth limiter or traffic shaper. With its help, you can apply speed-throttling rules to specified IP and MAC addresses, ports and even network interfaces with no changes to your existing network infrastructure. The rich feature set of SoftPerfect Bandwidth Manager software is easily managed via the intuitive Windows GUI.

SoftPerfect Bandwidth Manager's key features:

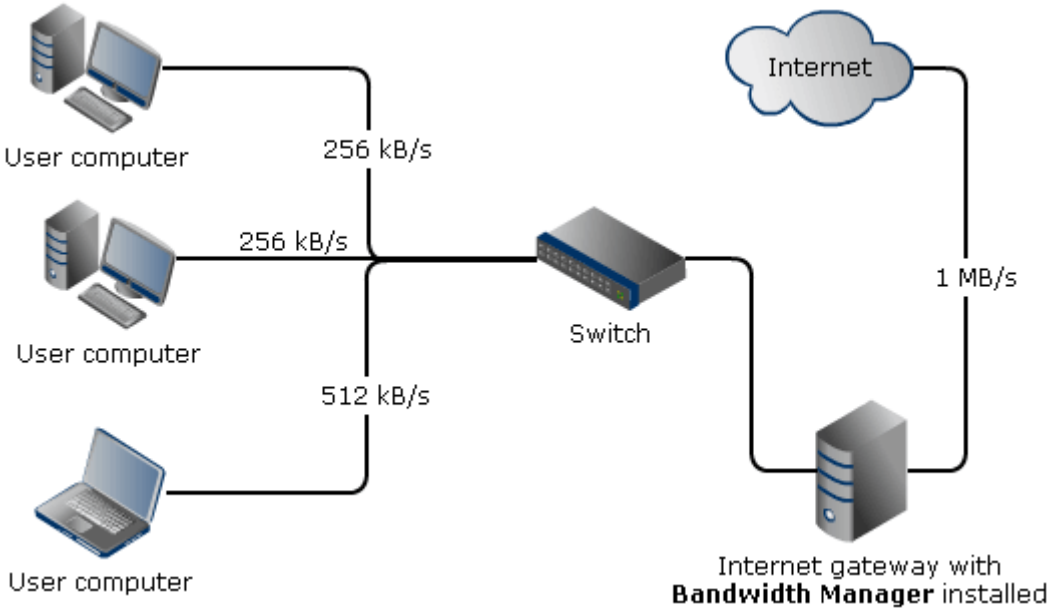
- Centralised configuration from a single network location.
- Flexible, prioritised, bidirectional rules to specify maximum data rates and usage allowances.
- Rules for IP and MAC addresses, protocols, ports (for TCP/IP) and network interfaces.
- Transparency for end users with no client software installation required in most cases.
- Quotas, scheduler, email notifications and comprehensive usage reports.

Software Installation

The software consists of two components: a Bandwidth Control Service and a Management Console.

The Management Console is usually installed on the system administrator PC. It is used to connect to the Bandwidth Control Service for monitoring and configuration.

The Bandwidth Control Service is essentially a filter that distributes bandwidth and enforces usage restrictions on the network connections that pass through. It should, ideally, be installed on the Internet gateway computer to manage user bandwidth usage as shown below:



This may not always be possible. For example, network users may access the Internet through a hardware router or a DSL modem. In this case, the software will be effective if it is installed on user computers. Please see the examples to learn more about the installation on specific network configurations.

End User Licence Agreement (EULA)

This software and the included documentation is copyright SoftPerfect Pty Ltd, Australia. All rights are reserved. The software may be used, installed or copied only in accordance with the terms of the licence described in the following paragraphs.

DISTRIBUTION TERMS

The evaluation version of the software may be freely distributed, provided that the original distribution package is not modified in any way.

EVALUATION VERSION

This is not free software. You are hereby licensed to use this software for evaluation purposes without charge. The evaluation version may be of a limited duration, or have some features limited or disabled. To use the software without these restrictions, you need to purchase a licence.

GRANT OF LICENCE

The software is licensed, not sold. Upon purchase of a licence, SoftPerfect grants you a non-exclusive, non-transferable right to use the software and all its features according to the terms of this EULA and the purchased licence type as described in the Licence Types section.

LICENCE TYPES

- **Single Device Licence** grants the purchaser, or agents of the purchaser, rights to install and use the software on **one** device only (e.g. computer, server, USB flash drive or virtual machine) at any given time. The licence can be reinstalled on the same device at any time, or deleted from one device and then moved to another. It can be used on any operating system compatible with the software. To install and use the software on more than one device simultaneously, you must purchase the corresponding number of single device licences or one of the special licences listed below.
- **Multiple Licence Pack** grants the purchaser, or agents of the purchaser, rights to simultaneously install and use the software on up to as many devices as is stipulated by the quantity in the pack. For example, the “Up to 10 Devices” pack allows installing and using the software on up to ten devices at the same time. Each device licence within the pack is identical to a single device licence. The licence pack can be used across multiple devices running different operating systems compatible with the software.
- **Site Licence** grants an organisation, or agents of an organisation, rights to install and use the software on an unlimited number of devices within one organisation site, including any cloud-based installation and use performed from that site. An

organisation site is defined as a location, or group of locations, used by the organisation that are all within 100 miles (160 kilometres) of each other.

- **Worldwide Licence** grants an organisation, or agents of an organisation, rights to install and use the software on an unlimited number of devices at an unlimited number of locations used by the organisation, including any cloud-based installations and use performed from those locations. If not listed, please contact us for the worldwide licence price.
- **OEM Licence** grants an organisation, or agents of an organisation, rights to use and distribute the software with their own hardware or software products. These products must provide substantial additional functionality to this software, and not include any potentially unwanted programs.

Where applicable, additional licence subtypes include:

- **Home Licence** grants a private individual rights to install and use the software at home, that is in a place of residence, for domestic purposes with no intention to generate income.
- **Business Licence** grants an organisation (a company, corporation, firm, enterprise or institution, or part thereof) or a person rights to install and use the software in a commercial and non-commercial environment for the purposes of or in connection with running a business, supplying products or services to other organisations or individuals, or generating income.

DISTRIBUTION OF LICENCE KEYS

Except for the specific purposes described in the Grant of Licence and the Licence Types sections, licence keys issued by SoftPerfect may not be distributed by any person, organisation or their agents without written permission from the copyright holder.

MODIFICATIONS

Unauthorised modification, decompilation or reverse engineering of the software or any subset of the software without written permission from the copyright holder is strictly prohibited.

USE

This software is distributed “as is”. No warranty of any kind is expressed or implied. You use it at your own risk. In no event shall SoftPerfect or its agents be liable for any loss or inaccuracy of data, loss or interruption of use, or cost of procuring substitute technology, goods or services, or any other loss or damages. If, despite the foregoing, SoftPerfect is found liable for any damages, its total cumulative liability shall not exceed the amount paid by you for the software licence.

You may not use this software in connection with any illegal, fraudulent, infringing, harmful or offensive activity.

TERMS OF ACCEPTANCE

Installation or use of this software signifies your acceptance of the terms and conditions of the licence. If you do not agree with them, you must stop using and remove the software from your devices. SoftPerfect reserves all rights not expressly granted here. SoftPerfect also reserves the right to terminate this licence immediately if you fail to comply with these terms. Upon termination, you must cease all use of the software and uninstall it from your devices.

GOVERNING LAW AND JURISDICTION

This EULA shall be governed by and construed in accordance with the laws of the State of Queensland, Australia, without regard to its conflict of law principles. The parties agree that the courts of Queensland, Australia, shall have the exclusive jurisdiction to resolve any dispute arising from or in connection with this EULA.

Purchase and Contact

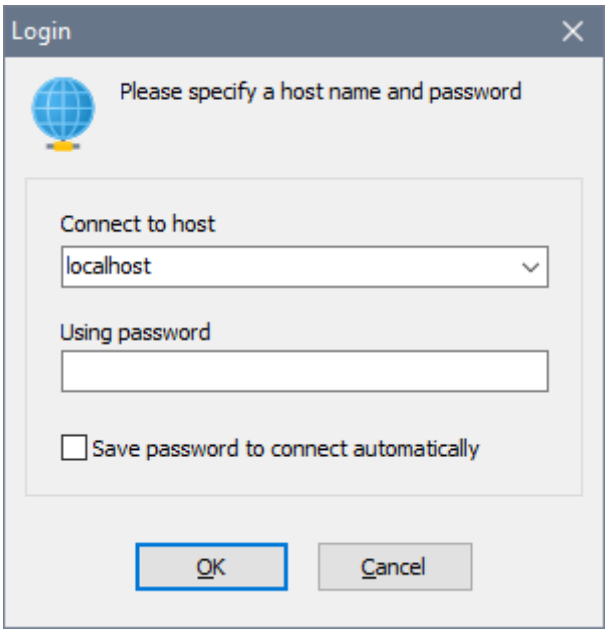
This software is provided as a free 30-day trial for evaluation purposes.

If you wish to continue using this software beyond the trial period, you will need to purchase a licence, which will entitle you to use Bandwidth Manager indefinitely. In addition, you will get a year of free updates.

Please visit www.softperfect.com website to find more information about licensing and pricing or to contact us.

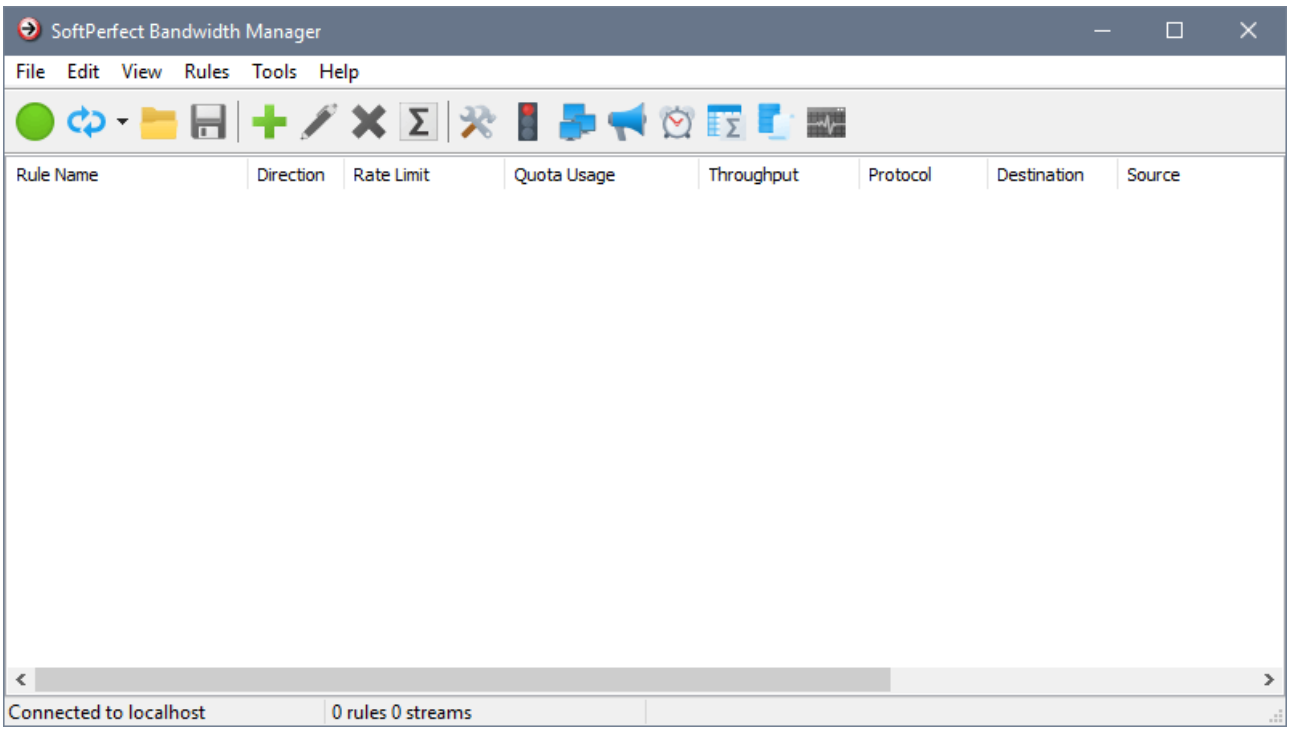
Getting Started

The SoftPerfect Bandwidth Manager software consists of two components: a Bandwidth Control Service that processes network traffic and enforces bandwidth restrictions, and a Management Console used for configuration and monitoring. When you launch the Management Console it asks you to enter the name of the host where the Bandwidth Control Service is running and a password. By default, the host name is localhost and the password is blank. If you have installed the service on another computer, enter its IP address or name to access it.



If you are getting the error messages like Connection Refused or Connection Timeout, it was most likely blocked by a firewall. In this case, you need to set it up to let the Bandwidth Manager connection through (TCP port 8701).

After a successful login, you will see the main window with a list of traffic filtering rules (initially blank):



The list of traffic filtering rules is initially empty

The toolbar buttons have the following functions:

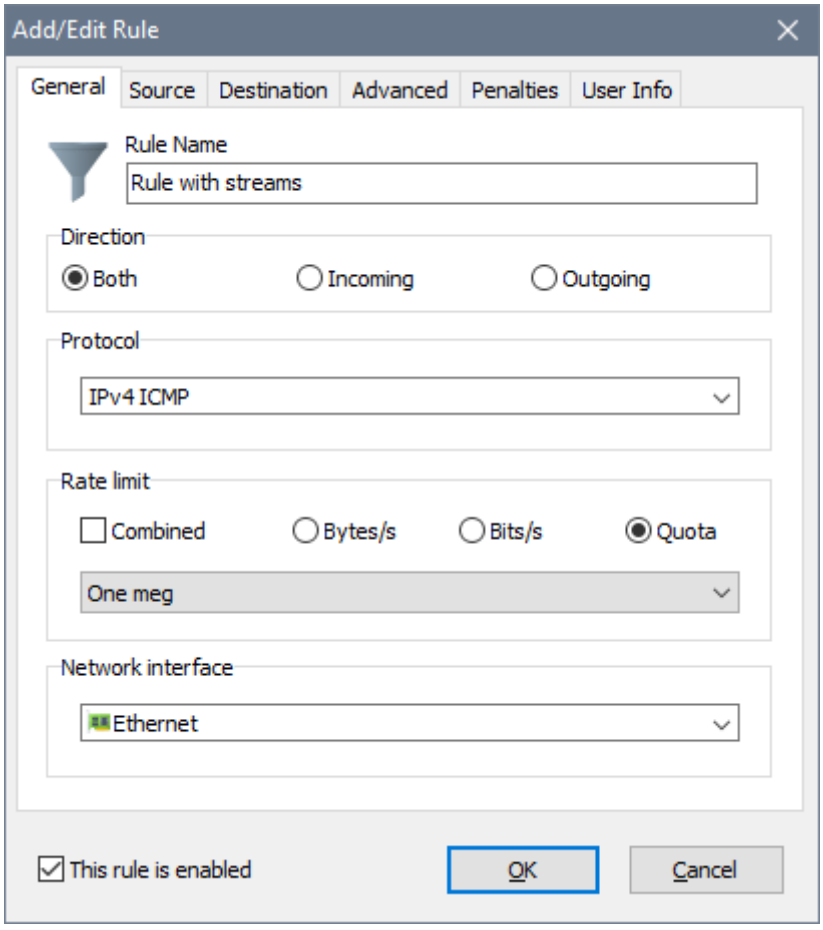
	Connects to a local or remote service
	Refreshes the list of rules
	Imports all rules from a file. Use this to restore previously created rules or to configure multiple instances
	Exports all rules to a file. Use this to backup the existing rules or to configure multiple instances
	Adds a new rule
	Edits an existing rule
	Deletes an existing rule
	Displays rule's usage information
	Opens the global settings
	Opens the group manager
	Opens the quota manager
	Opens the notification manager
	Opens the schedule manager

	Opens the usage reports
	Opens the event log
	Opens the live usage monitor

Rules

The software examines each data packet passing through the network. If the data packet matches a rule, then the specified speed limit is applied to that packet. The rules are matched in descending order of the rules list, with highest priority rules at the top. The first matching rule applies and no remaining rules are checked. The rules can be reordered if needed. If a network packet does not match any rule in the list, it is let through without limitations. See also the rule examples.

To add a new rule, or modify or delete an existing rule, select **Rules - Add New Rule/ Edit Rule/ Remove Rule** respectively from the main menu. To change the rule priority use **Rules - Move Up** or **Move Down** to move the rule within the list, or simply use drag & drop.



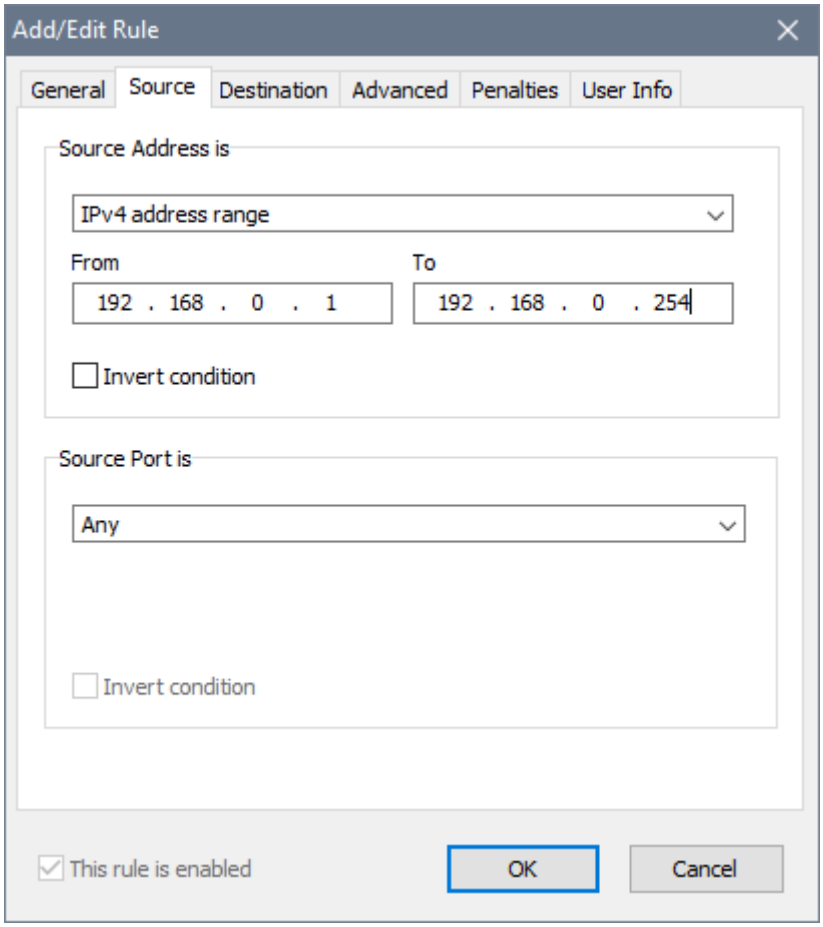
The input fields are as follows:

- **Rule Name**: a descriptive name for the rule.
- **Direction**: traffic direction on the network interface.
- **Protocol**: the network protocol this rule must match.
- **Rate limit**: a data transfer speed limit. You can specify this limit in bytes per second or bits per second, or use a quota for variable rates. In order to use different download/upload rates in a bidirectional rule, specify the rates separated by a colon.

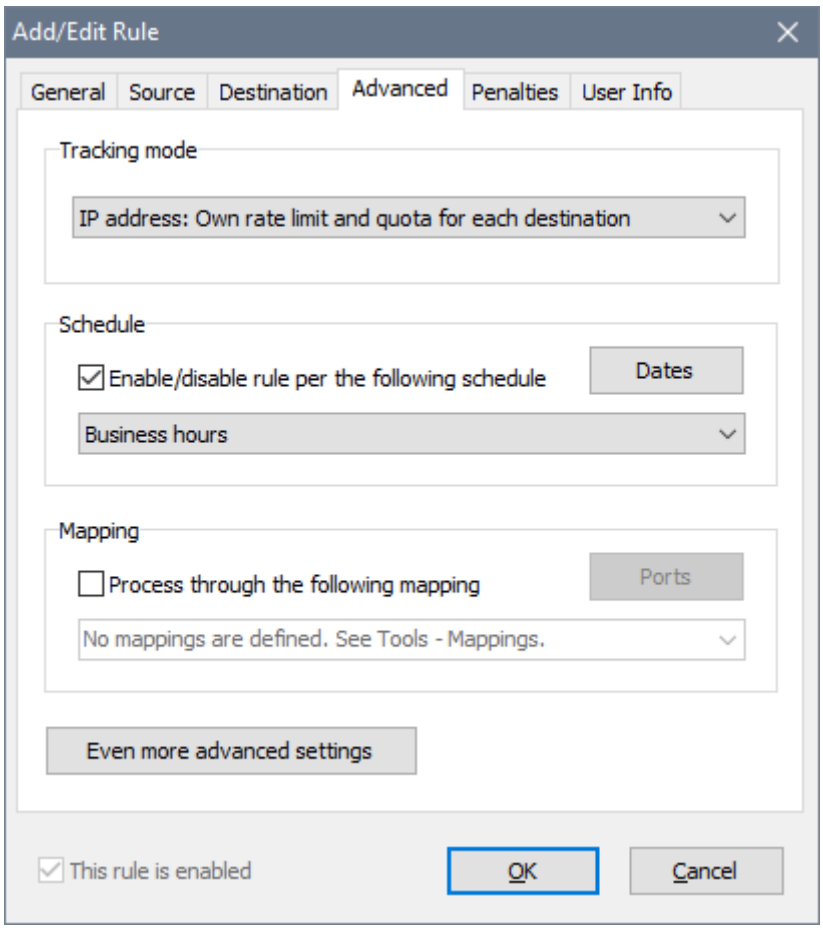
For example 100000:50000 would enforce a 100 kB/s limit on incoming traffic and a 50 kB/s limit on outgoing traffic.

- **Combined**: allows to share the transfer rate limit in a bidirectional rule. For example, if you set a 128 kB/s combined limit, the sum of upload and download rates will not exceed 128 kB/s.
- **Network interface**: the network interface type the rule applies to.

If you have specified an IP based protocol, you also need to specify **Source** and **Destination** parameters. These can be IP addresses, MAC addresses, address ranges or address groups. Other special parameters allowed are **Any** and **Local host**:



In order to specify the advanced rule properties, choose the **Advanced** tab:

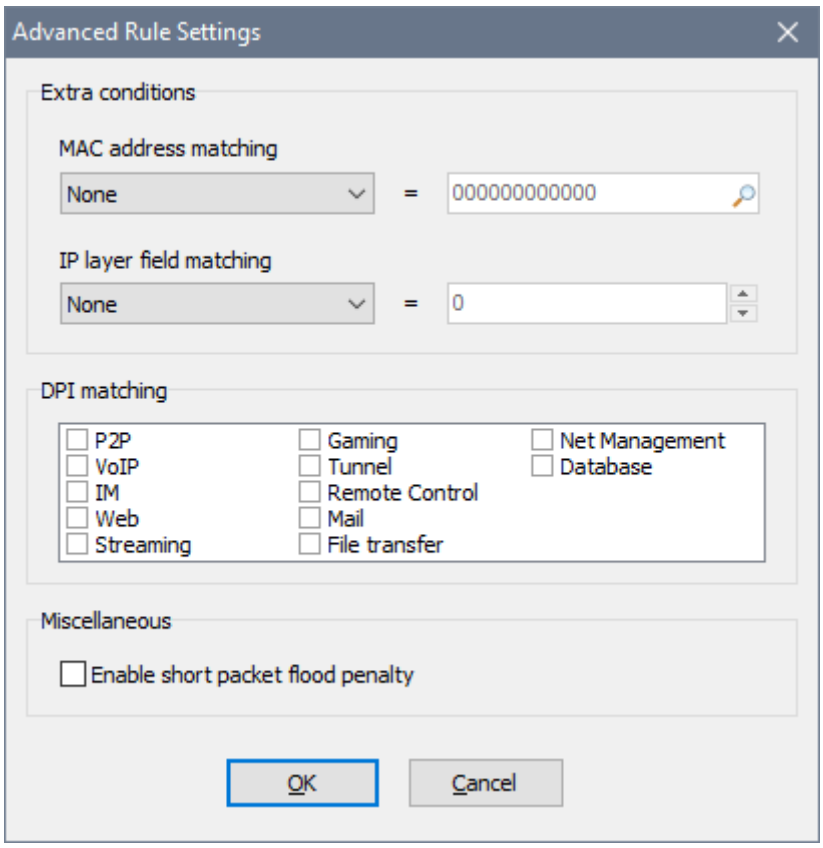


The **Tracking mode** option determines how the rule handles connections. When it is set to share the rate limit and quota, the rule does not identify individual connections. Whether there is one computer traffic flowing through the rule or multiple computers traffic, they have to compete for bandwidth and their individual usage is recorded as a whole. To limit individual connections, there are 4 options for setting the Tracking mode to do it: source IP address, source MAC address, destination IP address, destination MAC address. These individual connections are called **streams**, and you will see them dynamically emerging in the list of rules.

If you decide to use a **Schedule**, the rule will be either enabled or disabled according to the timetable you choose. For instance, you can configure your rules to allow high speed Internet access on working days and disable it at all on holidays. The **This rule is enabled** option becomes read-only and cannot be changed manually when the rule is linked to a schedule. See schedules for details.

The **Mapping** feature allows you to redirect incoming connections to a local port or a web-site. See mappings for details.

There are more features under **Even more advanced settings**:



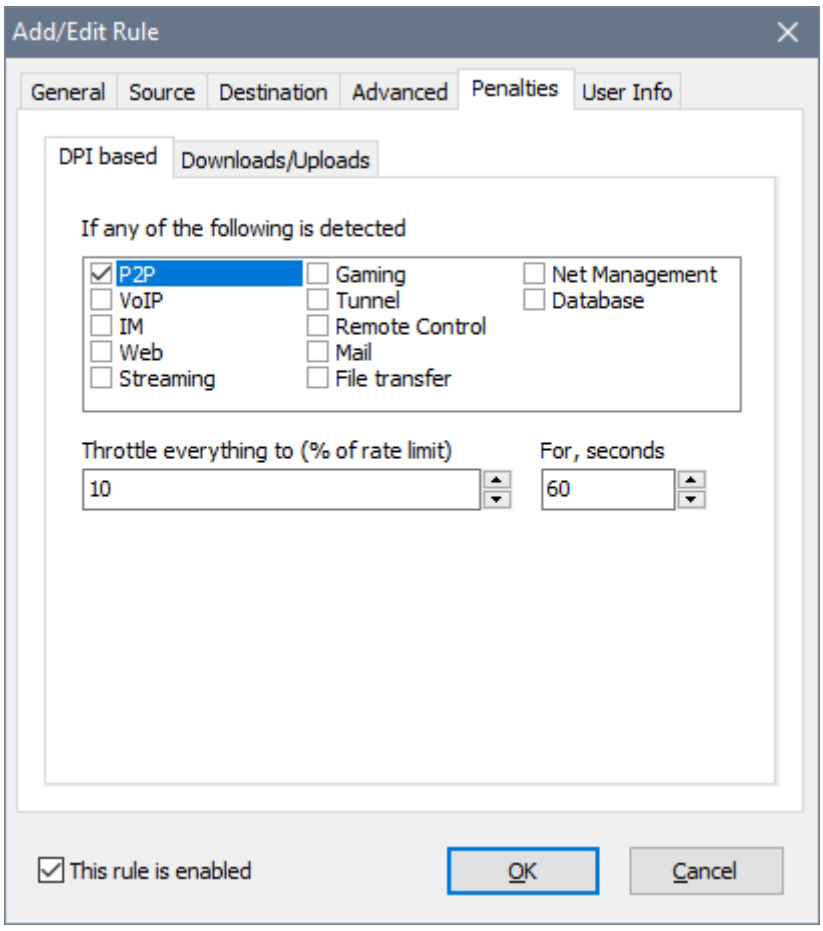
Here you can configure a couple of extra conditions. The **MAC address matching** requires the rule to match packets from/to the specified MAC address only. This could be useful if your network uses IP + MAC address authentication. **The IP layer field matching** requires the rule to match an IP header value in IPv4/IPv6 packets. If you need this, you probably know what you are doing.

The **DPI matching** group defines which type(s) of traffic this rule must match. This could be useful if, for example, you want to ban P2P applications and watching online videos.

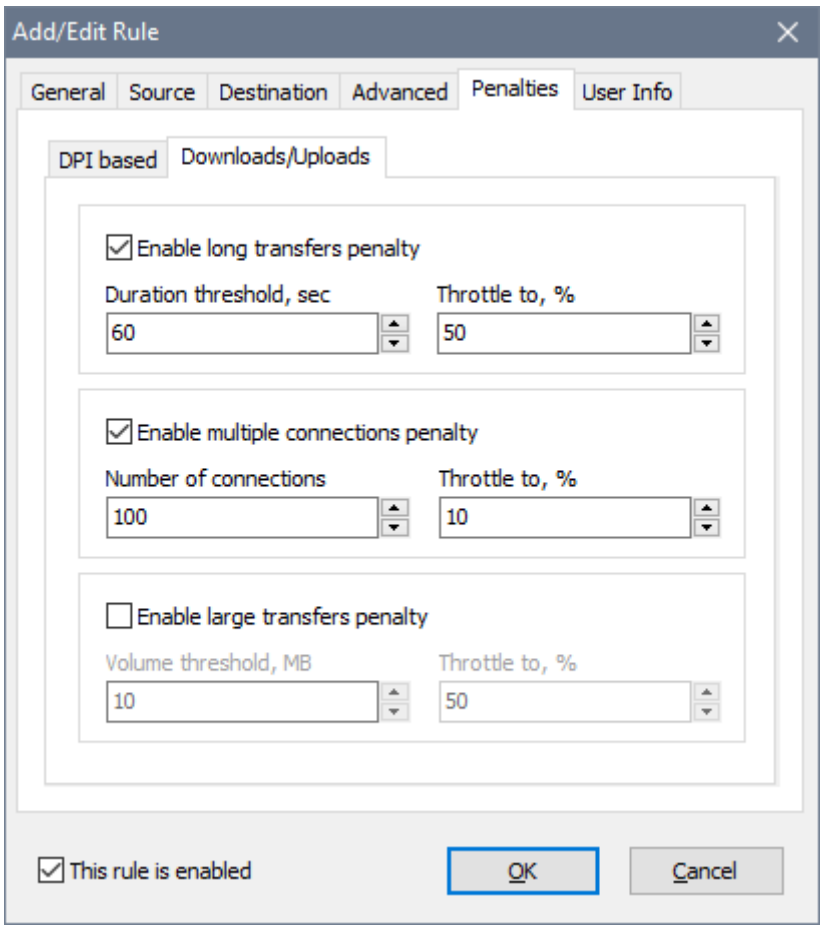
You can also **Enable short packet flood penalty** to penalise users that send a lot of small packets into the network; remember to adjust the global short packet flood penalty parameters if needed.

The **Penalties** tab can be used to discourage users from heavy downloads, watching online videos or using BitTorrent. Two types of penalties are available: DPI-based and Downloads/Uploads.

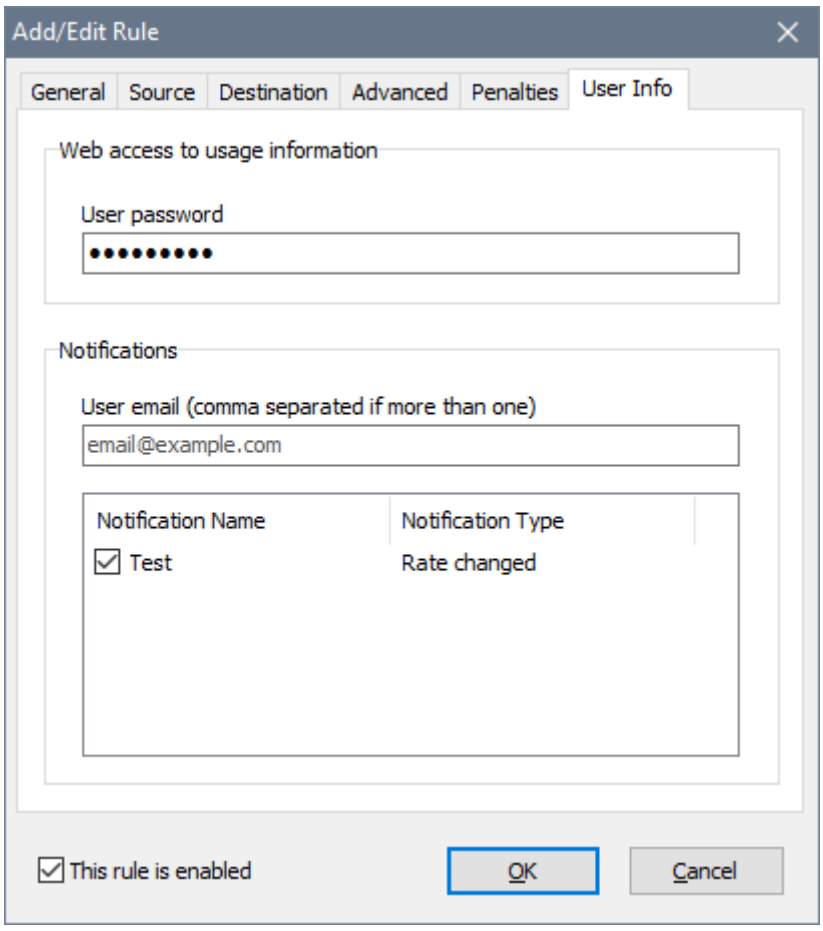
The **DPI-based** penalty allows you to throttle the entire rule's throughput upon detecting a prohibited activity. For example, with the P2P penalty switched on on and set to 60s, the user is penalised for 60s after a P2P packet was detected. If the user keeps running a torrent app, there normally is at least one P2P packet every 60s, so the user is penalised until the torrent app is closed. Once the torrent app is closed and consequently no P2P packets have been detected for 60s, the penalty is removed.



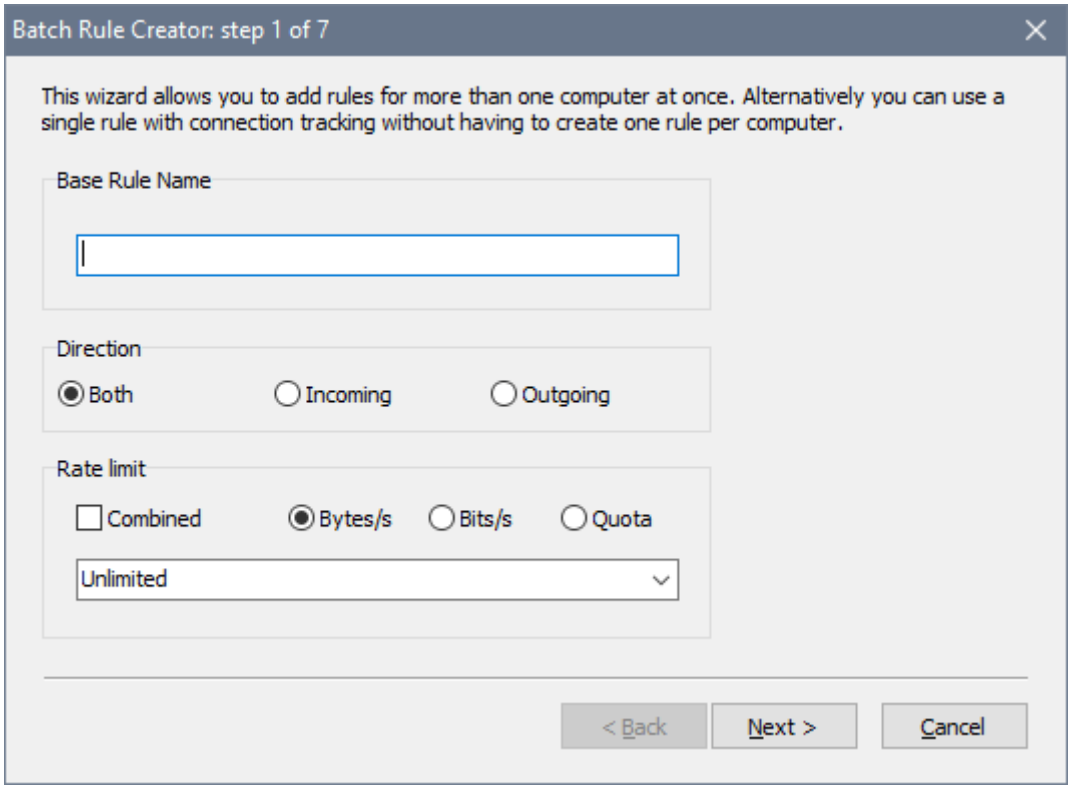
By using the **Downloads/Uploads** penalty, you can throttle long or large data transfers or the users who open too many connections. Unlike the DPI-based penalty, these apply to individual TCP/UDP connections and not the entire rule's throughput. For example, if the **Volume threshold** is set to 1 MB and **Allocate** is set to 50%, this means that if the user downloads or uploads anything larger than 1 MB, the user's connection speed will drop by 50% until the transfer ends. Once it ends, the normal transfer rate is restored in a few seconds. If multiple penalties are chosen and go off, the strictest one applies.



The **User Info** tab allows to set a password to access usage reports with a web-browser as well as to choose what notifications the user receives:



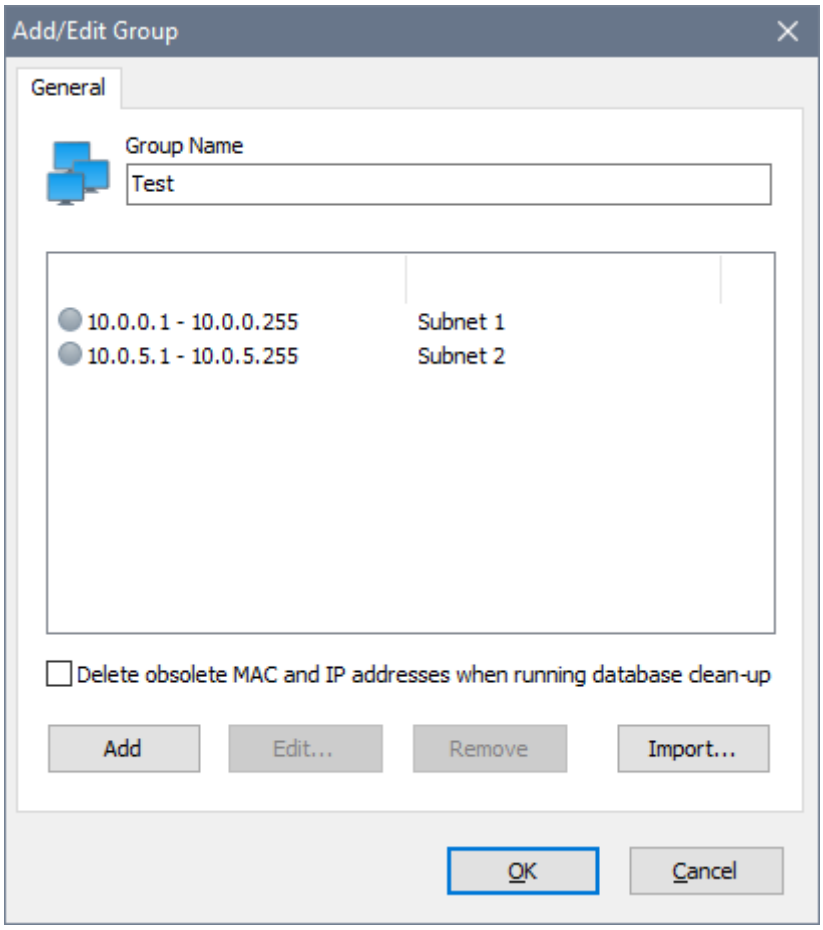
In order to facilitate multiple rule creation, the software has a batch wizard. If you would like to add a number of rules, for example to cover a LAN segment, use the **Rules - Add Batch** command. It helps you create many similar rules within a single action:



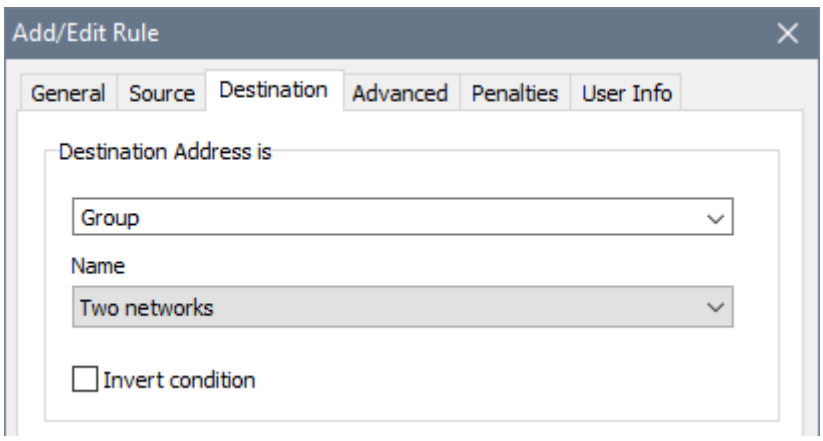
Groups

The software supports complex rules. A complex rule refers to multiple IP and MAC addresses, including non-contiguous IP ranges. To create a complex rule you need to define an address group first. To do so, choose **Tools - Groups** from the main menu.

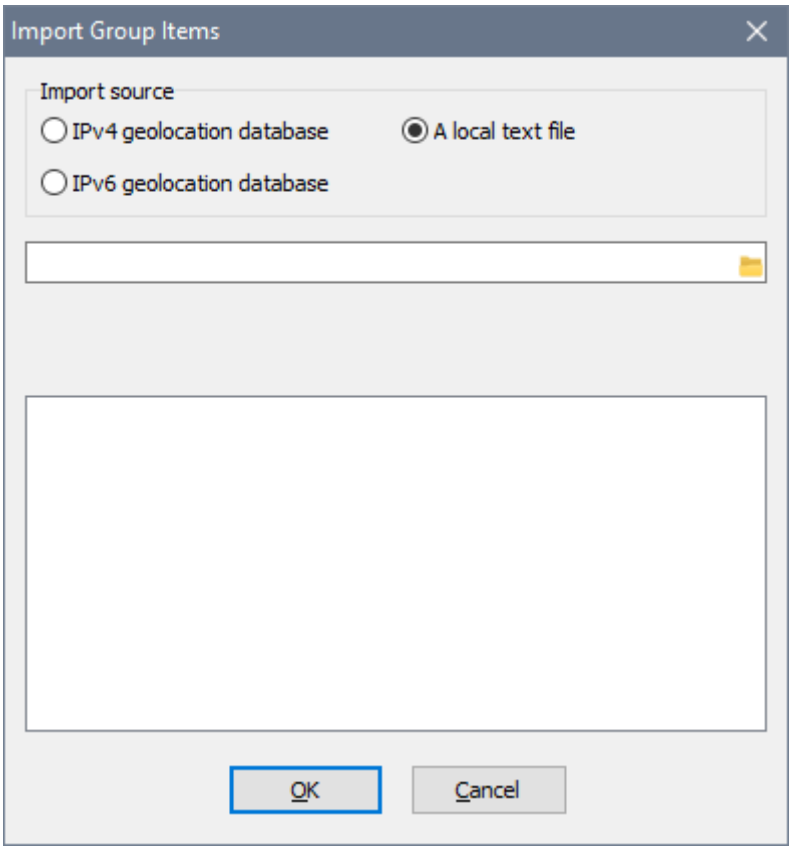
For instance, if you want to shape bandwidth from both networks 10.0.0.x and 10.0.5.x with a single rule, the group may look like this:



Once a group is defined, you can use it in a rule:



Group entries can be sourced from a text file that contains one MAC address, IP address or IP address range per line:

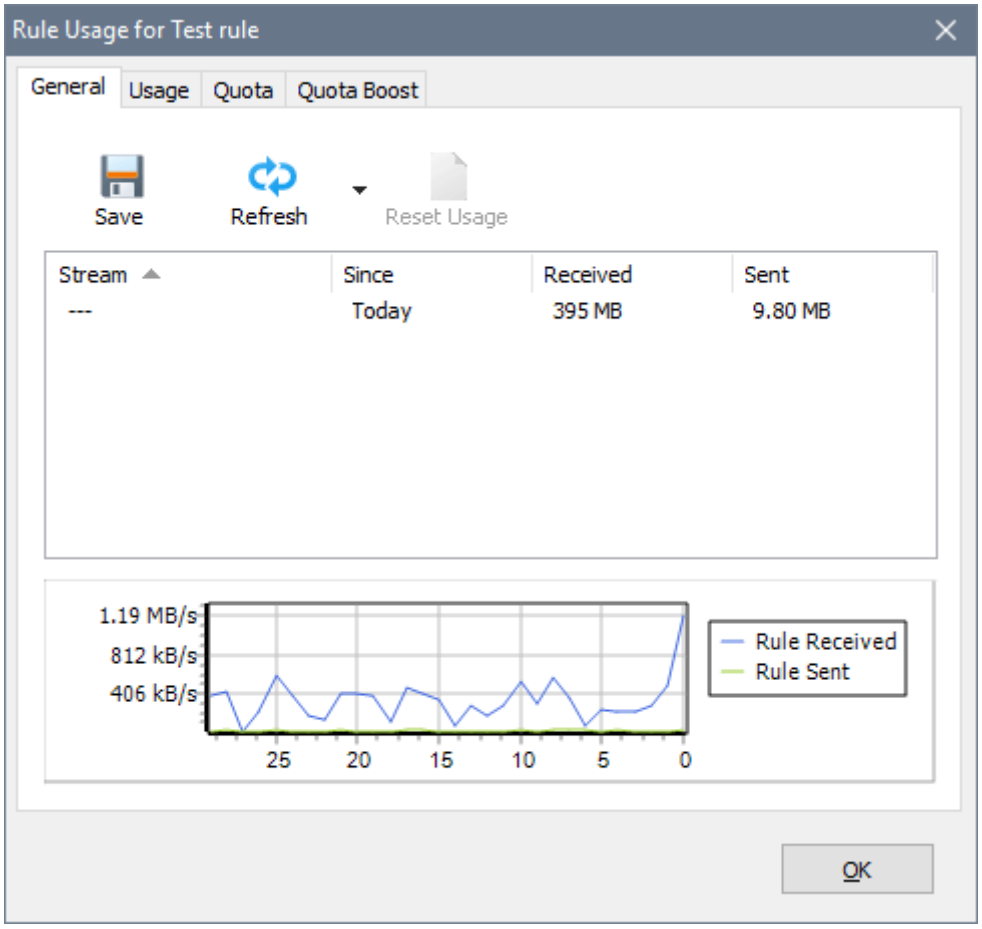


It is also possible to populate a group from the geolocation databases if you need to filter traffic by country.

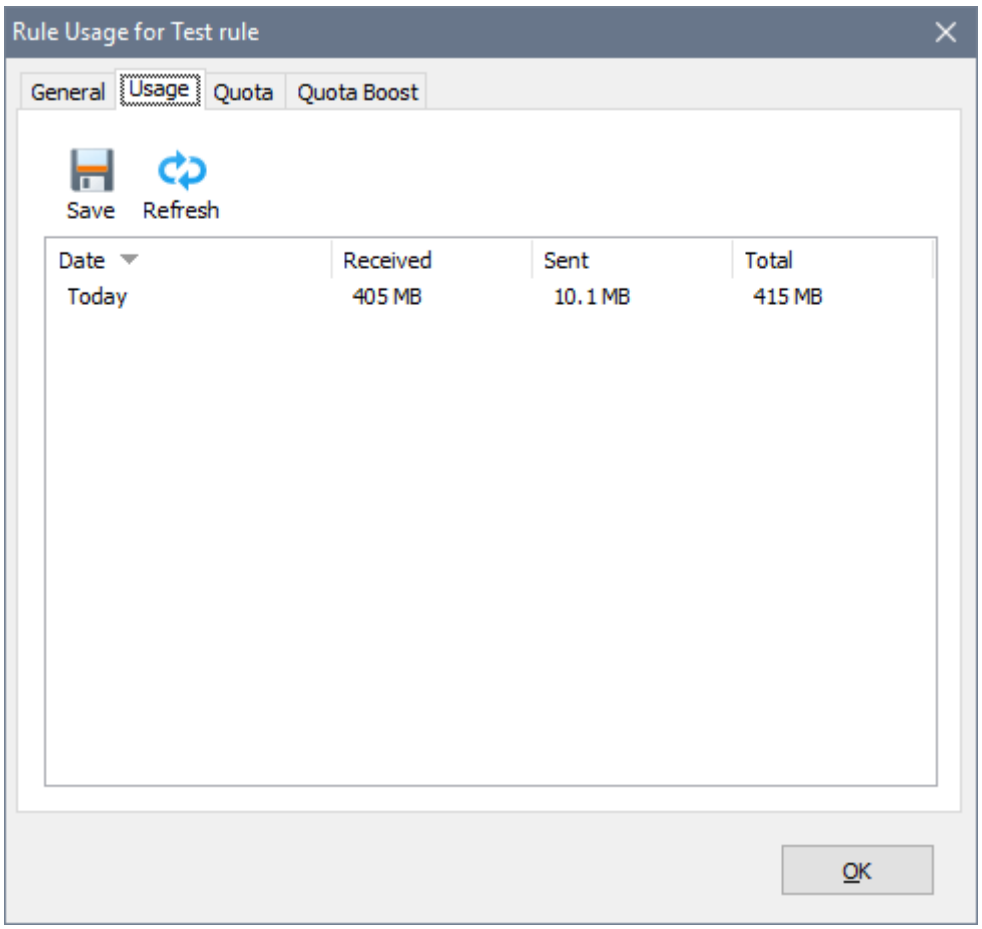
Usage Reports

To access usage information for any rule select **Rules - Rule Usage** from the main menu.

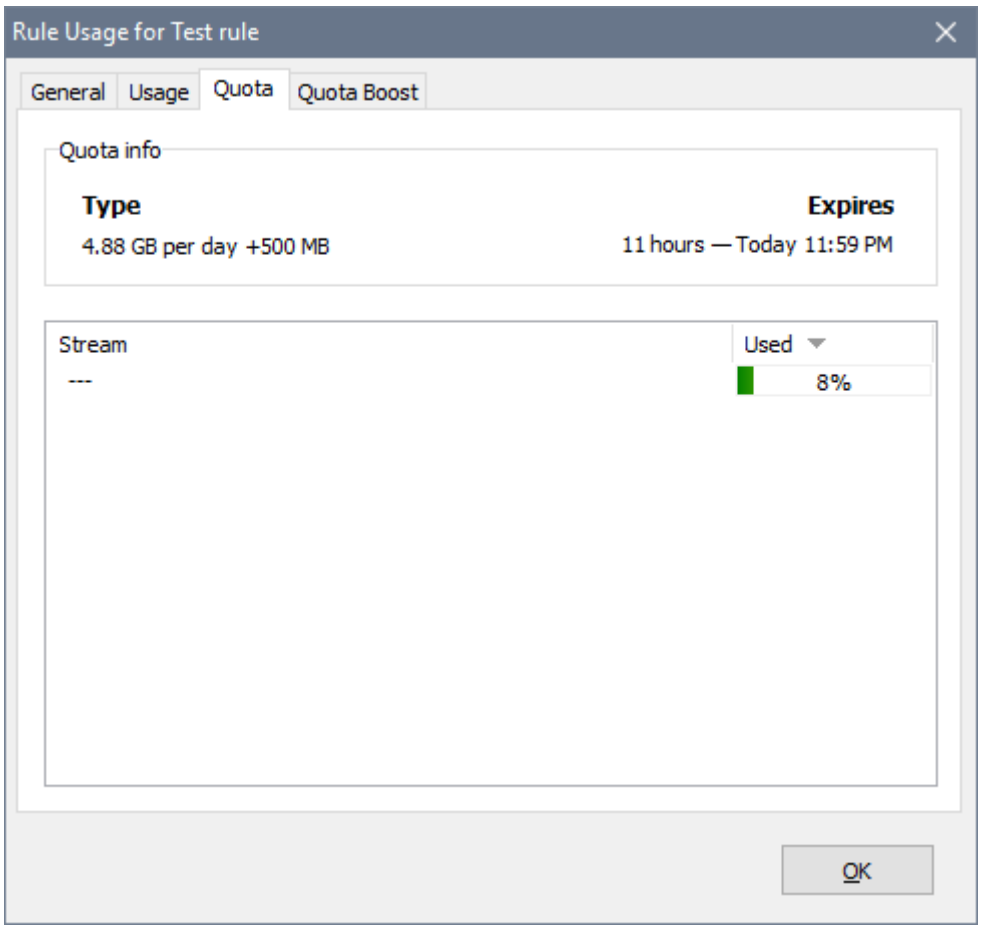
The **General** tab displays overall usage of the rule since it was created or last reset. If the rule has tracking turned on, there may be more than one stream displayed. The chart below represents activity through the rule within the last 30 seconds:



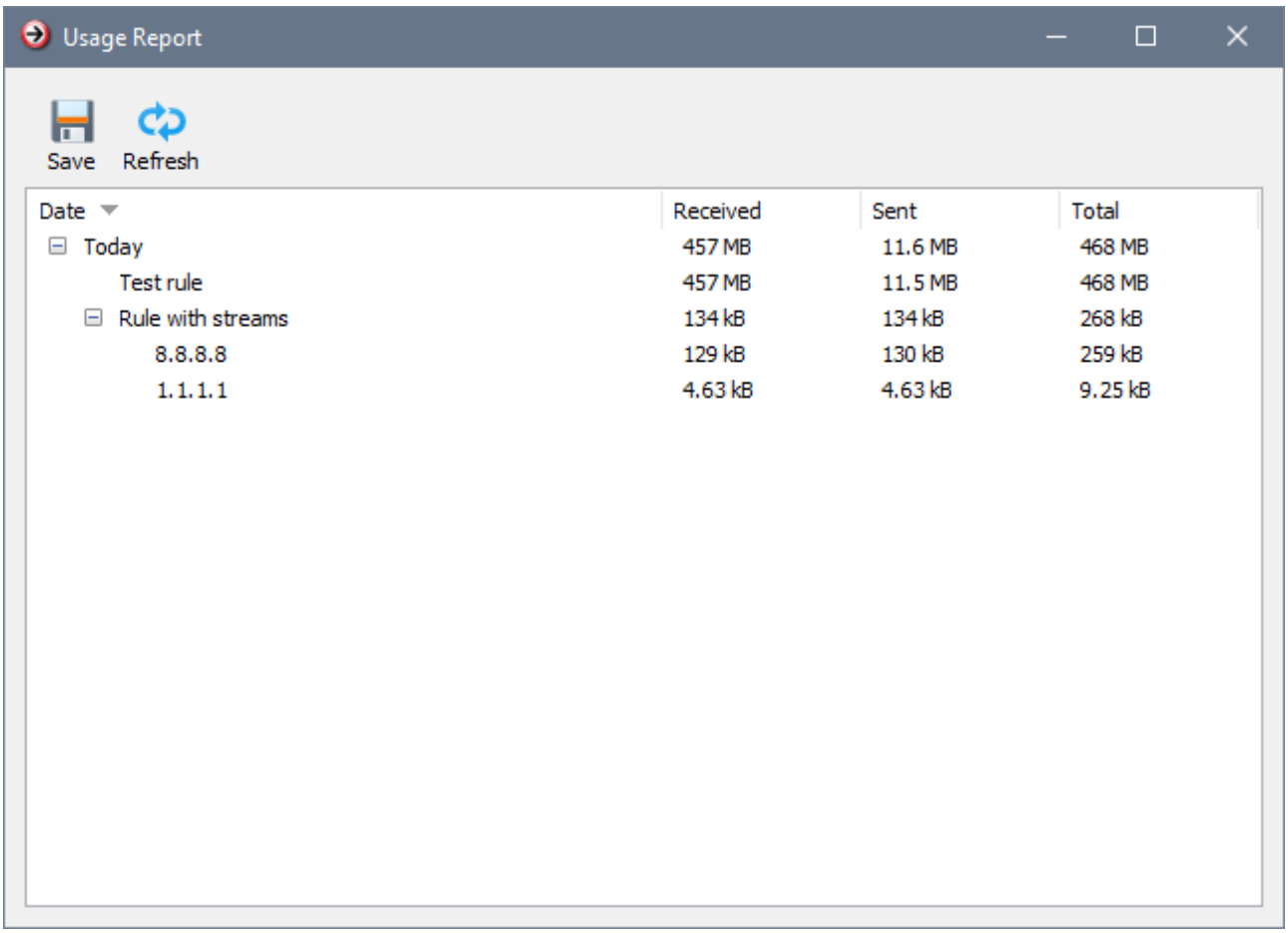
The **Usage** tab displays overall usage per day. Once again, if the rule has got tracking turned on, there may be sub-entries detailing per stream usage:



If a quota has been set for the rule, the **Quota** tab displays the usage of that quota:



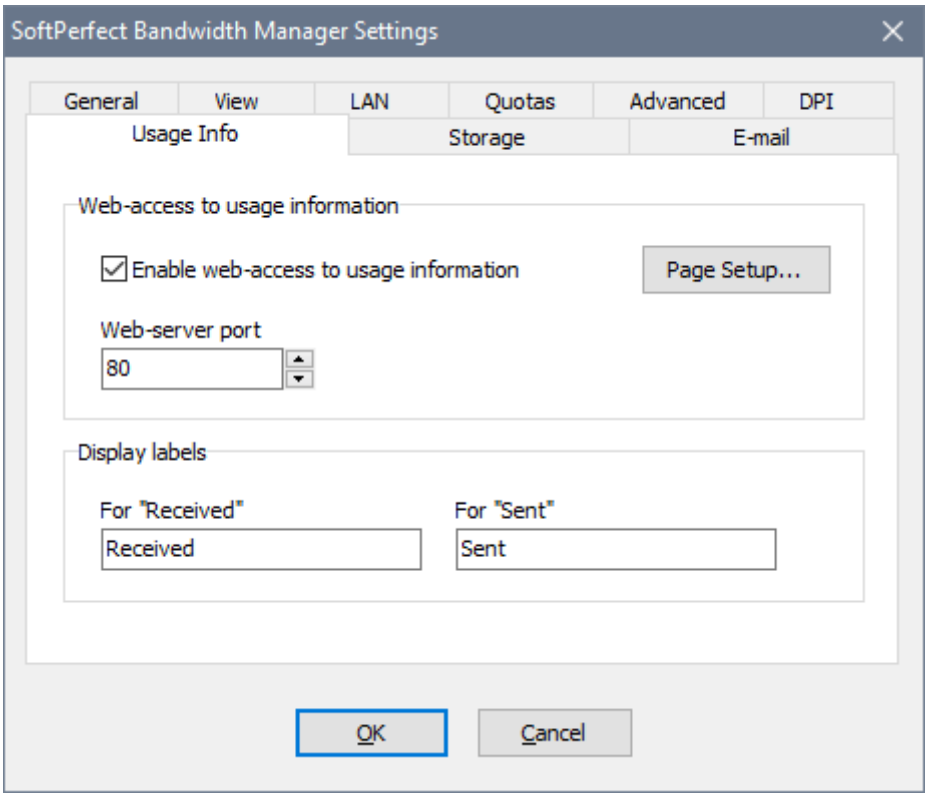
There is also a separate report accessible via **Tools - Usage Report** in the main menu. It contains usage information grouped by day, then by rule and finally by stream for rules with tracking turned on:


Usage Report
Save
Refresh
Date
Received
Sent
Total
Today
457 MB
11.6 MB
468 MB
Test rule
457 MB
11.5 MB
468 MB
Rule with streams
134 kB
134 kB
268 kB
8.8.8.8
129 kB
130 kB
259 kB
1.1.1.1
4.63 kB
4.63 kB
9.25 kB

Usage web-access

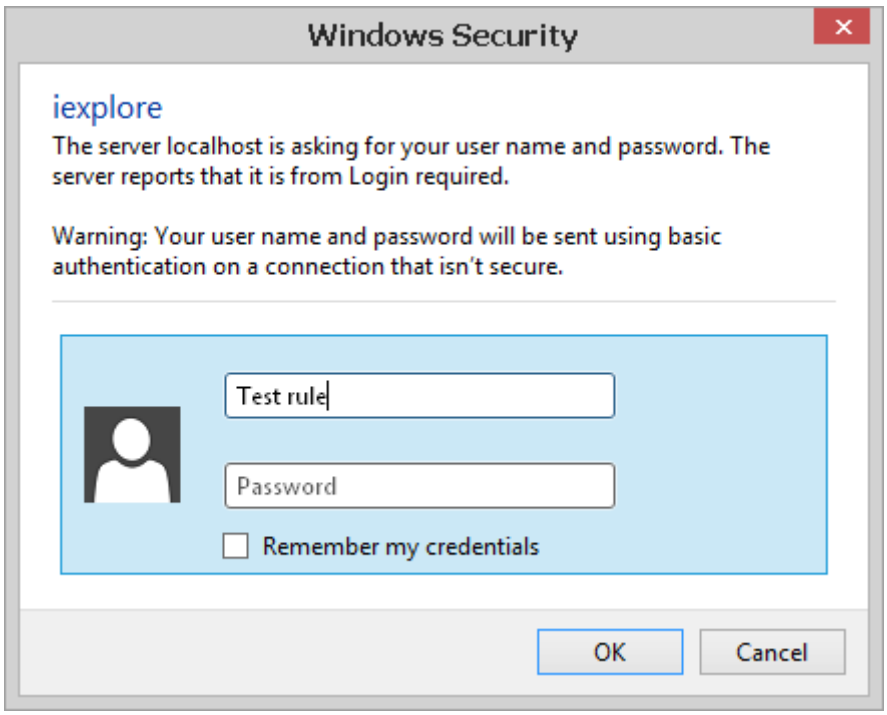
If you run a corporate or home network, you may want to let your users see their Internet usage. For this purpose, Bandwidth Manager contains a built-in web-server that enables users to access their usage reports remotely via their web-browsers. The following configuration steps need to be done to enable this feature.

1. Choose a port and activate the built-in web-server in the global settings:



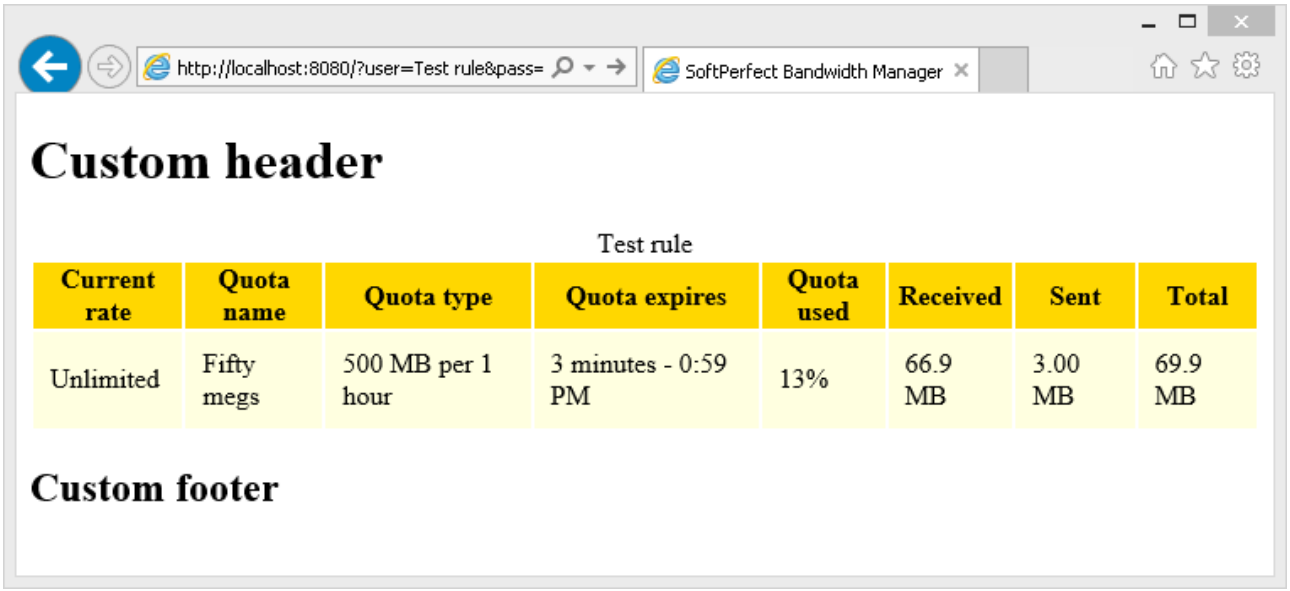
2. Make sure the web-server has started. If there is no error message in the event log, the web-server has started successfully.

3. Navigate your web-browser to the URL **http://localhost** if you have chosen port 80, or **http://localhost:port** otherwise. You will be asked for a user name and password. Enter the rule name (in place of the user name) and password (blank by default):



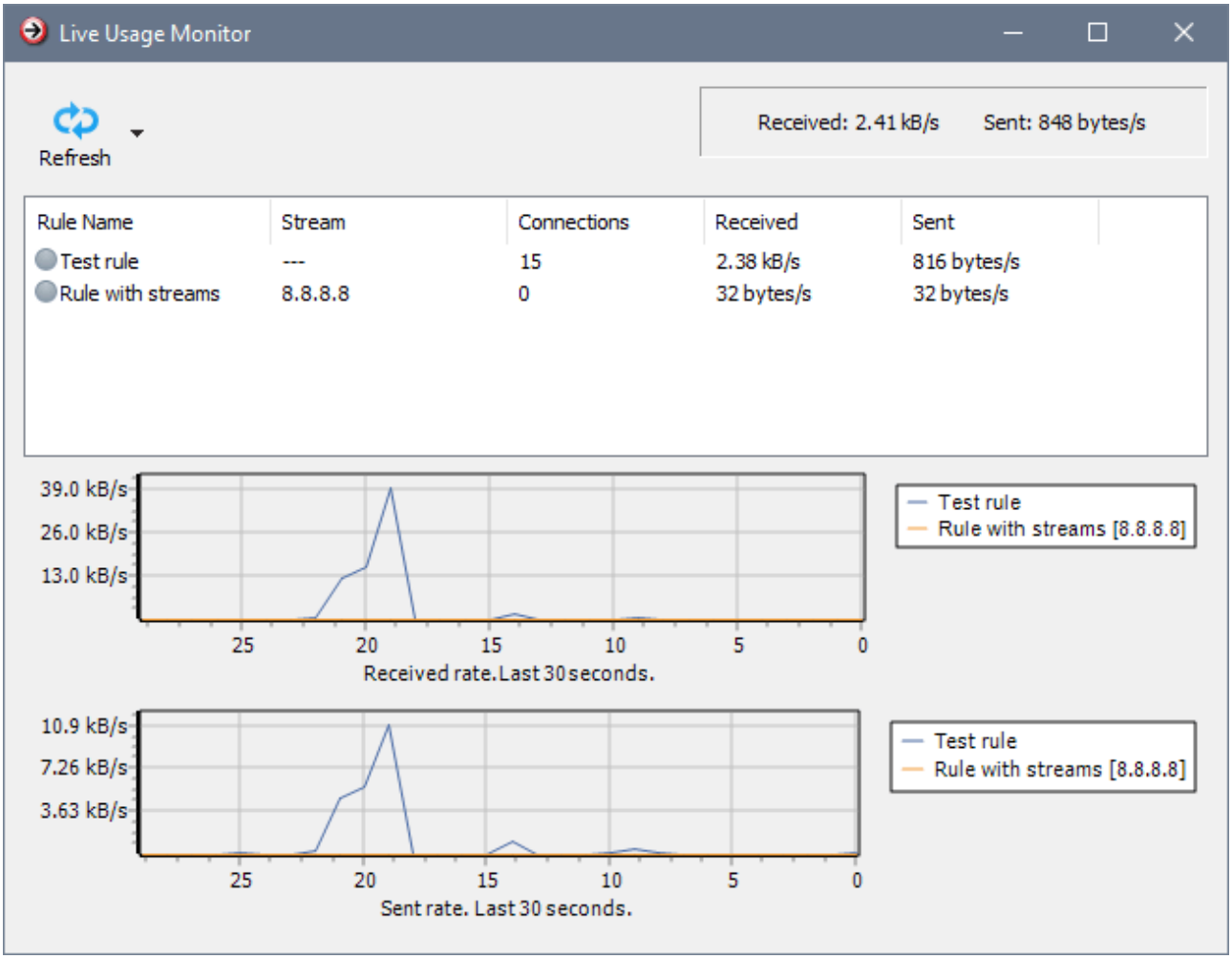
Note that both the rule name and password are case-sensitive. In this example the server name is **localhost** and we are accessing the rule named **Test rule**. Alternatively you can suppress the authentication window by passing the user name and password as CGI parameters: **http://localhost/?user=Test rule&pass=123**

4. After the successful authentication you will see the usage report:



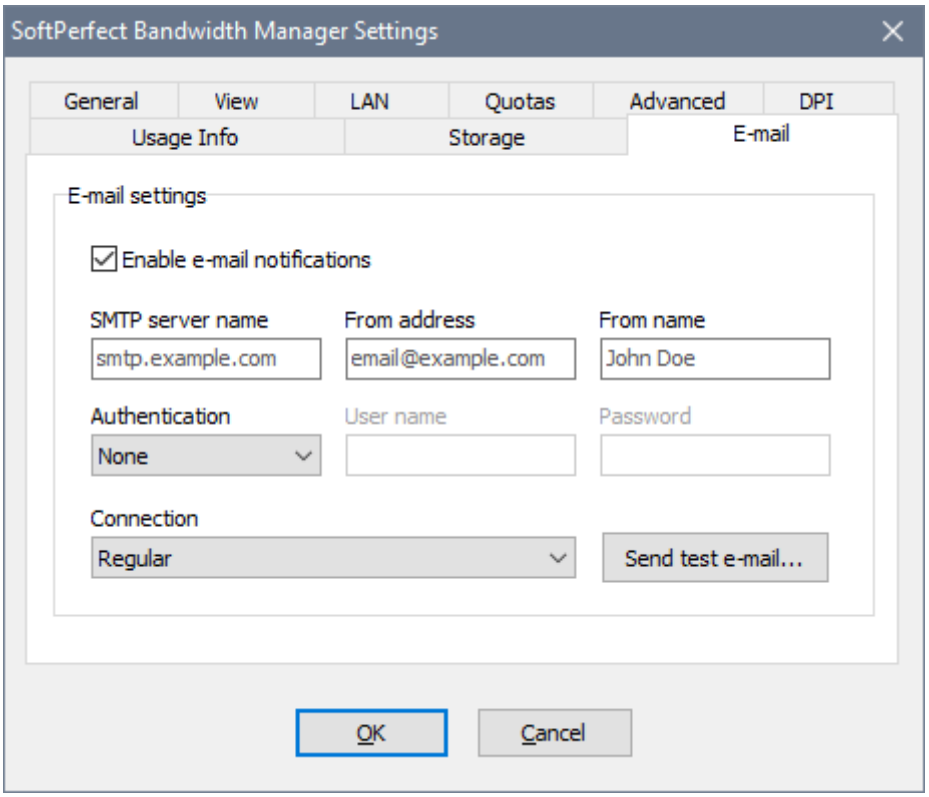
Live Usage Monitor

The live usage monitor can be accessed via **Tools - Live Usage Monitor** in the main menu. The In/Out panel in the top right corner displays the total used bandwidth through all the existing rules. The monitor allows to identify instantly which users (that is which rules and which streams) have been the most active in the last 30 seconds. It displays the top 10 active rules and streams in real time:



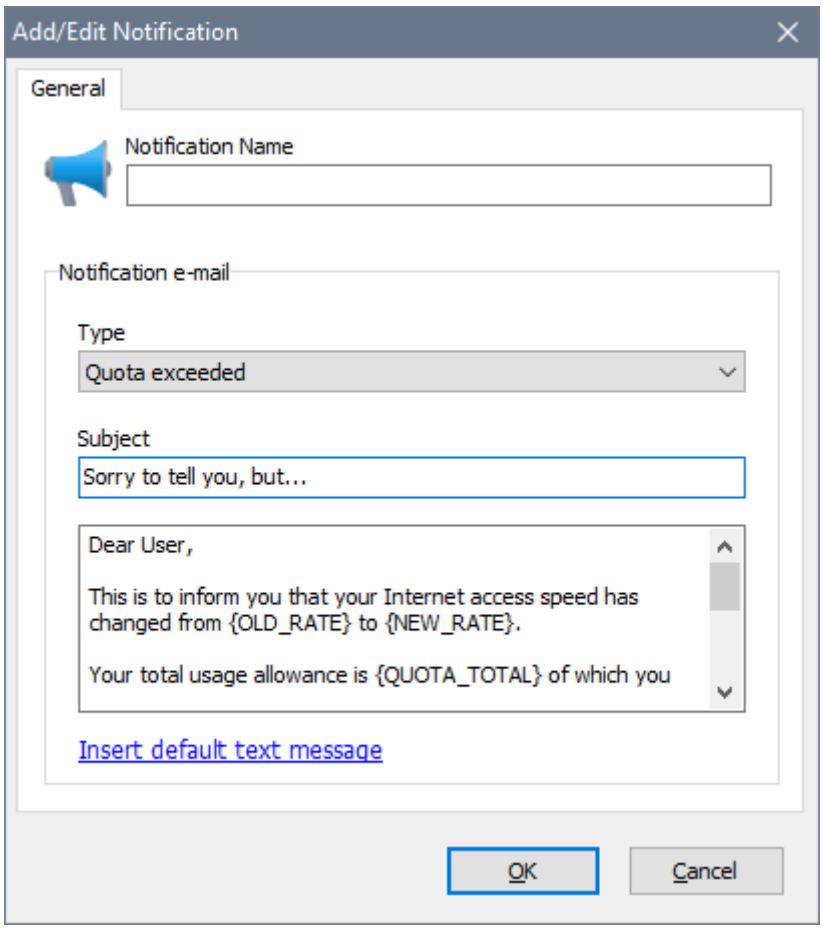
Notifications

Bandwidth Manager can send out e-mail notifications to users controlled by its quotas. The notifications are sent automatically when a specific event occurs, for example when a user has used up their quota. Before you setup notifications, you should enable this feature in the global settings and fill the appropriate parameters for sending mail:



Once the notifications have been enabled, you can proceed and define a new notification via **Tools - Notifications** in the main menu. There are the following types of notifications that can be configured:

- **Transfer rate limit changed** sends an e-mail whenever a transfer rate assigned to the rule changes as a result of gradual quota usage. This notification can be assigned to a rule linked with a smooth quota, i.e. a quota whose data transfer rate changes gradually as it is consumed. For example, if a user has a quota of 100 MB and the user's rule is assigned this notification, the user will be sent several e-mails as the quota is being consumed, an e-mail message for approximately every 10 MB consumed.
- **Quota exceeded** sends an e-mail when the rule has used up an assigned quota. This notification can be set for any rule with a quota.
- **Quota reset** sends an e-mail when a quota assigned to the rule has been reset. Likewise, this notification can be set for any rule with a quota.
- **Quota boost added** sends an e-mail when a quota boost is added. This notification can be set for any rule with a "boosted" quota.



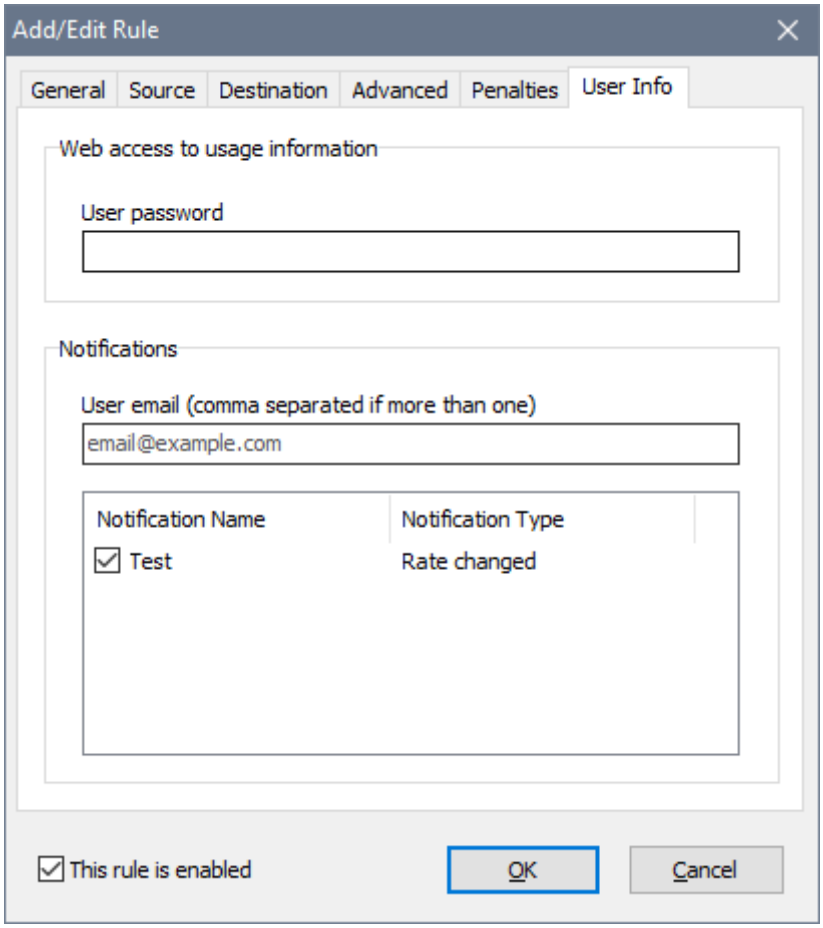
You can use the following tags in the e-mail templates:

Tag	Description
Tags that can be used with the **Transfer rate limit changed**, **Quota exceeded** and **Quota reset** notification types:	
{OLD_RATE}	Old transfer rate that was in effect before.
{NEW_RATE}	New transfer rate assigned to the rule.
{QUOTA_TOTAL}	Quota allowance.
{QUOTA_USED}	Used amount of the quota.
{QUOTA_LEFT}	Remaining amount of the quota.
{RULE_NAME}	The associated rule’s name.
{STREAM_ADDR}	User’s IP or MAC address when rule tracking is used.
{WEBINFO_HOST}	The name of the server the software is running on.
{WEBINFO_PATH}	Path to usage web-report. This makes a clickable URL in the e-mail which lets the users see their usage stats. This tag must follow the server name, e.g. http://{WEBINFO_HOST}/{WEBINFO_PATH} as in the provided default message.
Tag that can be used with the **Quota boost added** notification type:	

{QUOTA_BOOST}	The amount added to the quota in a quota boost.

Once a notification has been created, you need to add a quota.

Finally, you need to link a rule with both the quota and notification, and also specify the user's e-mail address that the notifications should be sent to. A rule can have multiple notifications assigned.



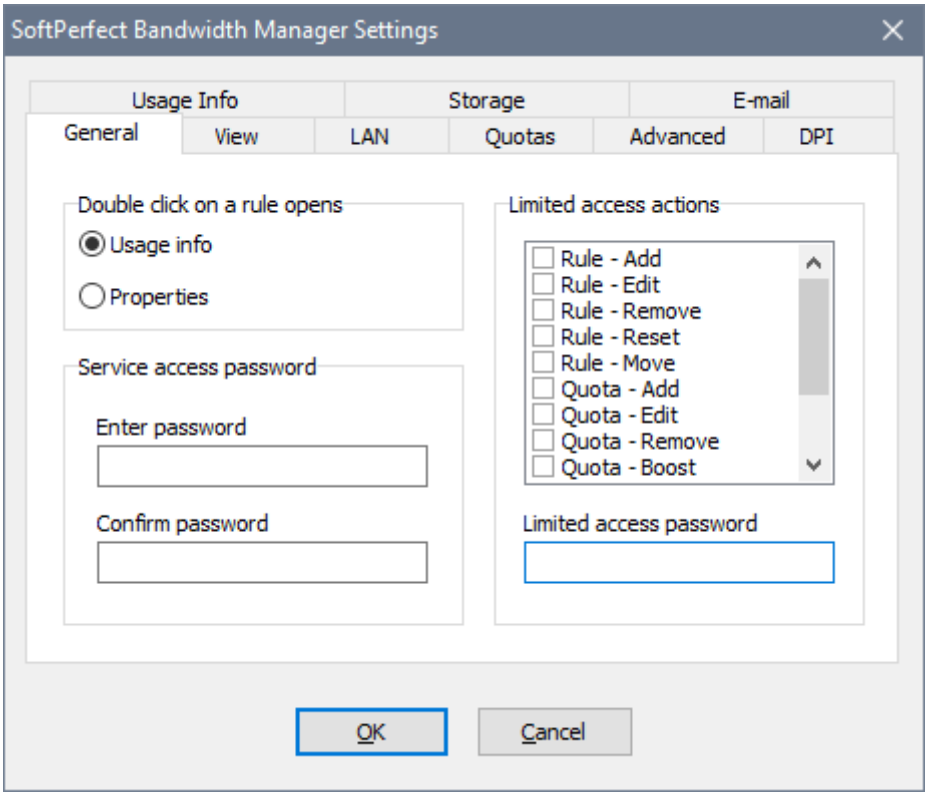
In this example, the user will be receiving an e-mail based on the template whenever their rule's rate changes.

Global Settings

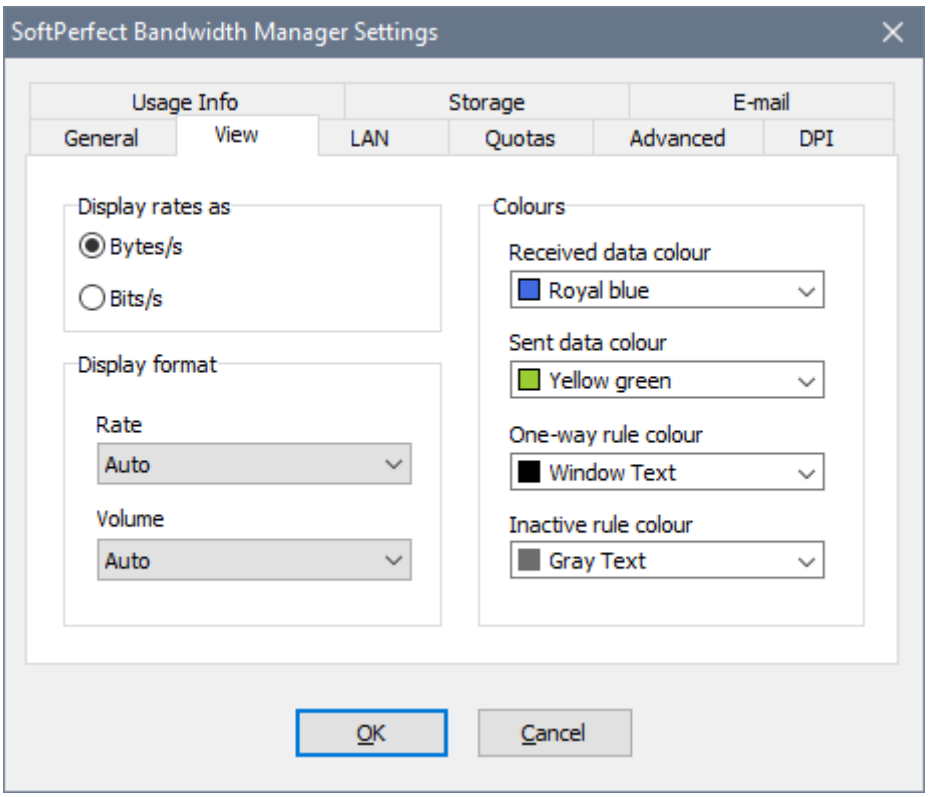
To access the software's global settings select **File - Settings** from the main menu.

At the **General** tab you can set a logon password that will protect the Bandwidth Control Service from unauthorised access. You can also set up a limited access password to allow access to certain actions only.

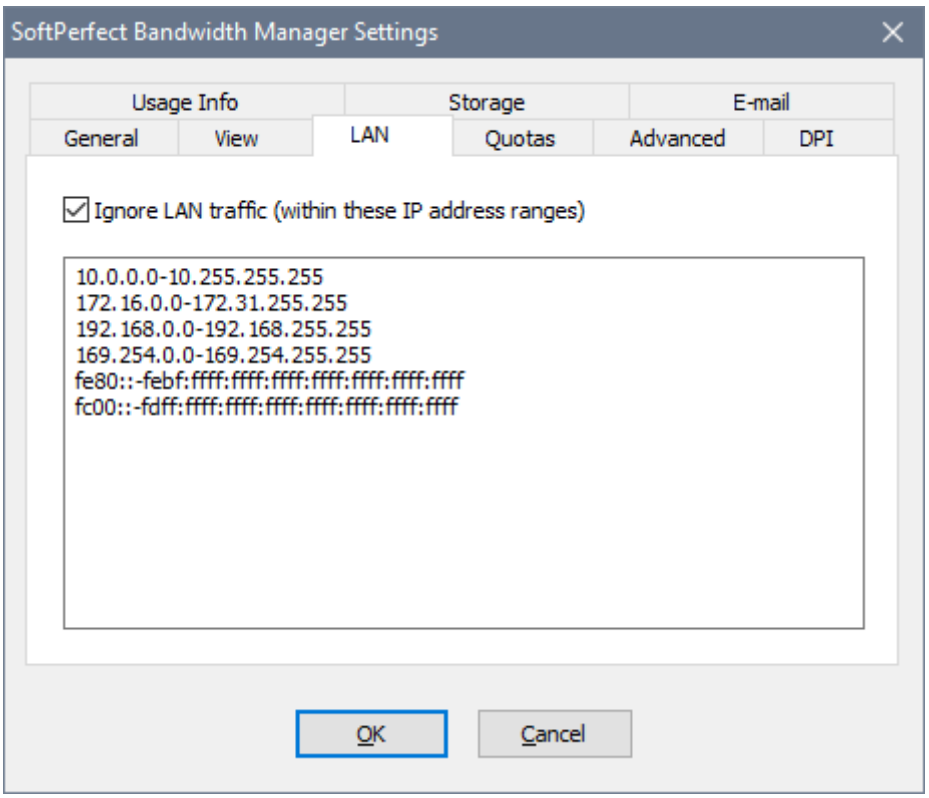
In addition, you can specify what you would like to see when you double click a rule:



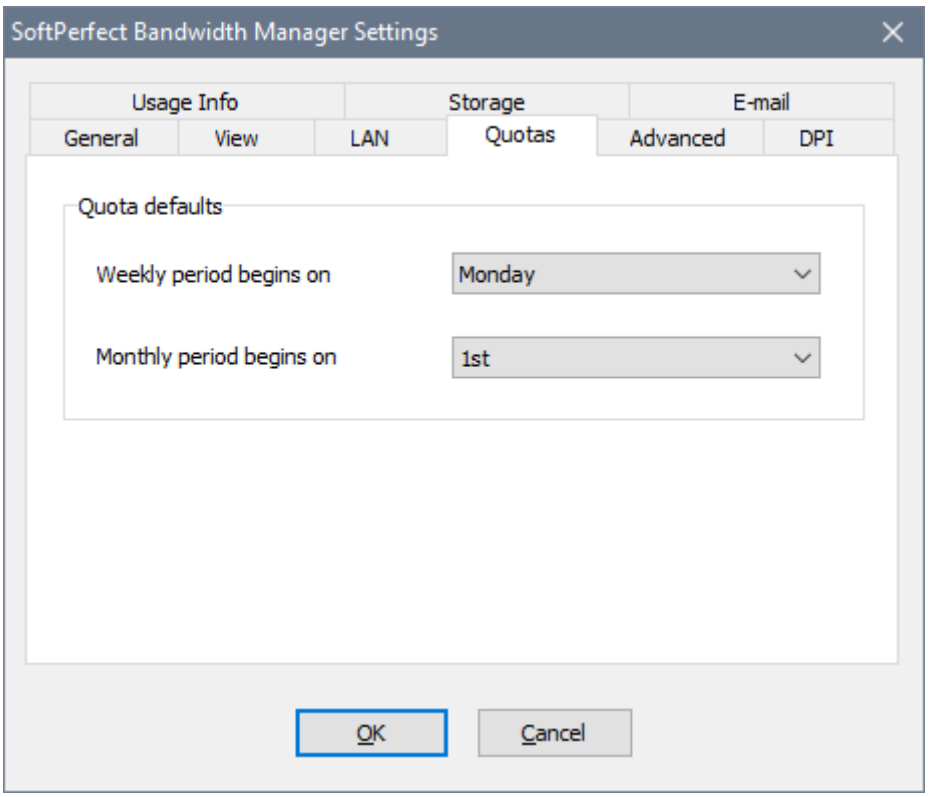
At the **View** tab you can choose your preferred display modes and chart colours:



The **LAN** tab lets you define a set of IP address ranges that should be ignored. This is useful if you require high performance and do not need to monitor or limit LAN traffic:

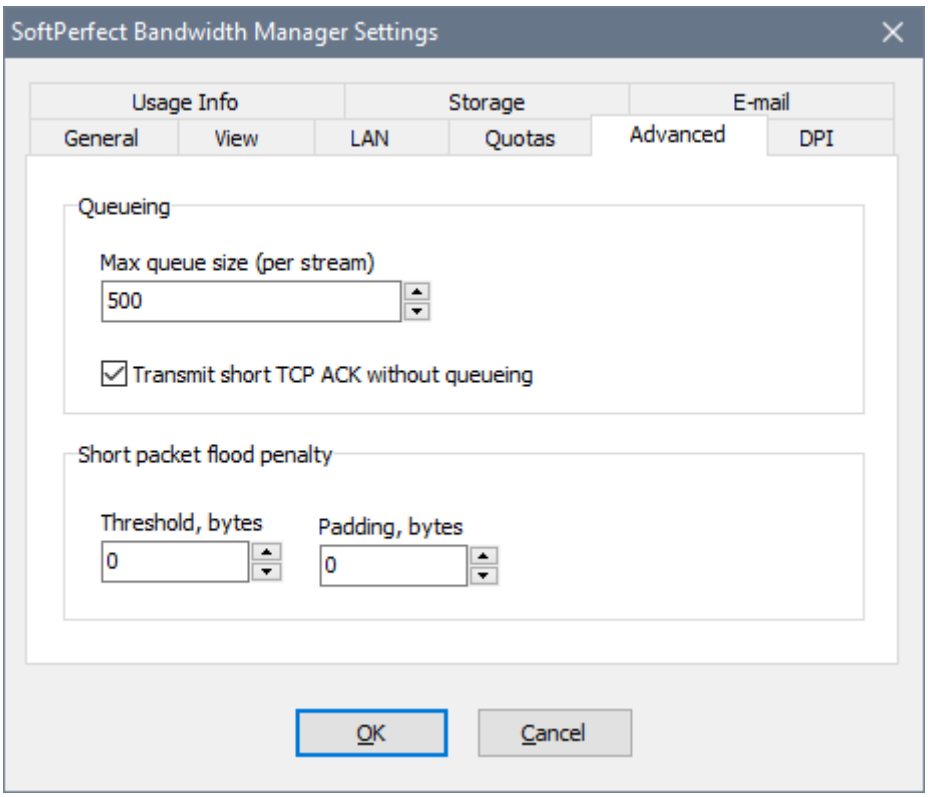


The **Quotas** tab determines when the weekly and monthly quotas are reset by default:



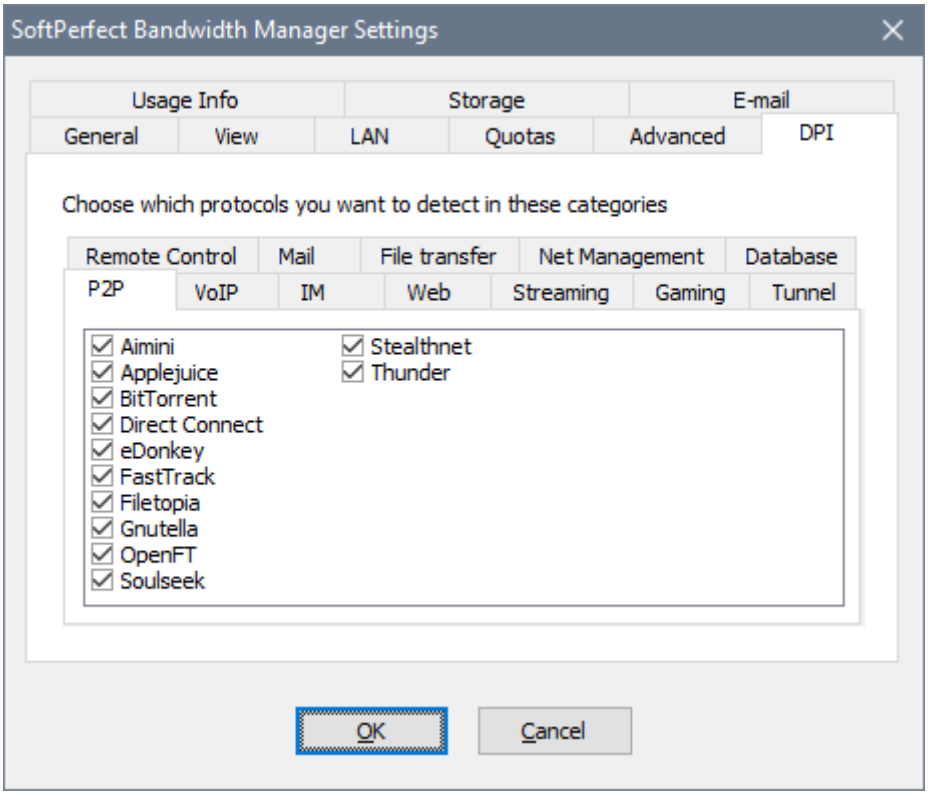
The **Advanced** tab represents the following internal processing options:

- **Max queue size** is the capacity of a rule's queue, which holds network packets when they exceed the bandwidth limit.
- **Transmit TCP ACK without queuing:** instructs the bandwidth manager to forward the TCP Acknowledge packets without any delay. This affects only the short TCPv4 packets sized 54 to 74 bytes and TCPv6 packets sized 74 to 94 bytes with the ACK flag set. This option can be useful for bidirectional rules to achieve simultaneous uploads and downloads close to the specified rate.
- **Short packet flood penalty** allows to pad too small network packets to prevent users who use software applications that send a lot of small packets from overfilling the network. This may be useful for wireless networks. There are two parameters, **Threshold** and **Padding**. Both must be in the range 1 to 1500. If either of them is zero, no user will be penalised. Otherwise, if the packet size is less than the threshold, it will be padded with the padding bytes and hence the user's bandwidth will decrease.

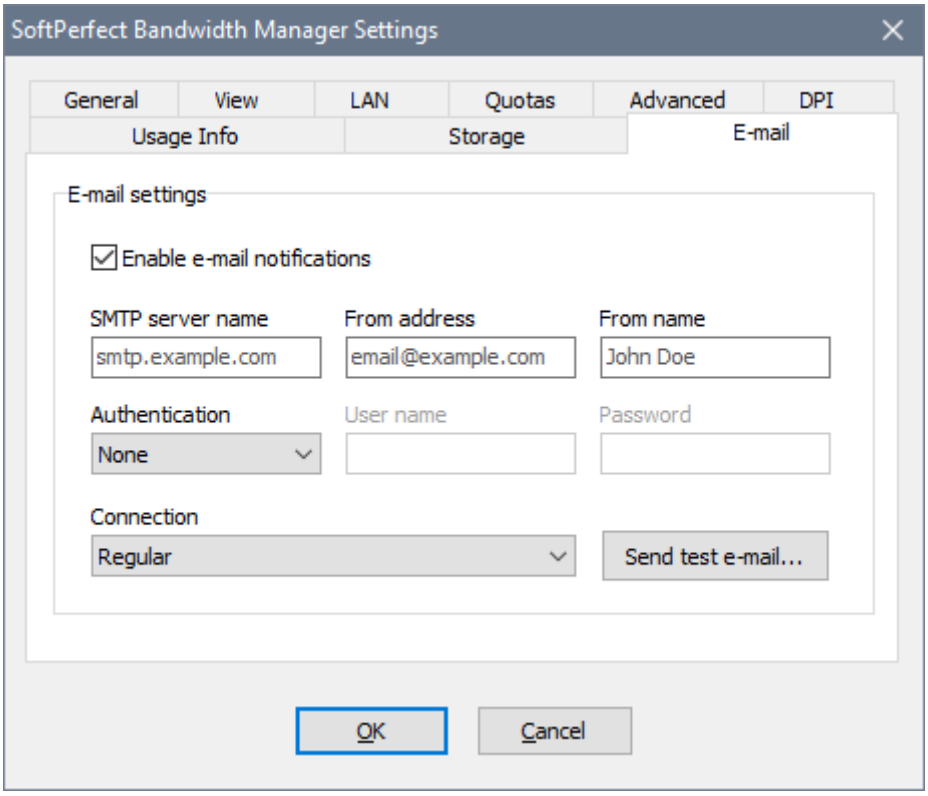


The **DPI** (Deep Packet Inspection) tab determines which protocols in these categories are detected. Generally there is no need to turn any of these off unless you are getting false detections.

In order to make a rule match one or more of these categories, open the rule properties and go to **Advanced - Even more advanced settings**.

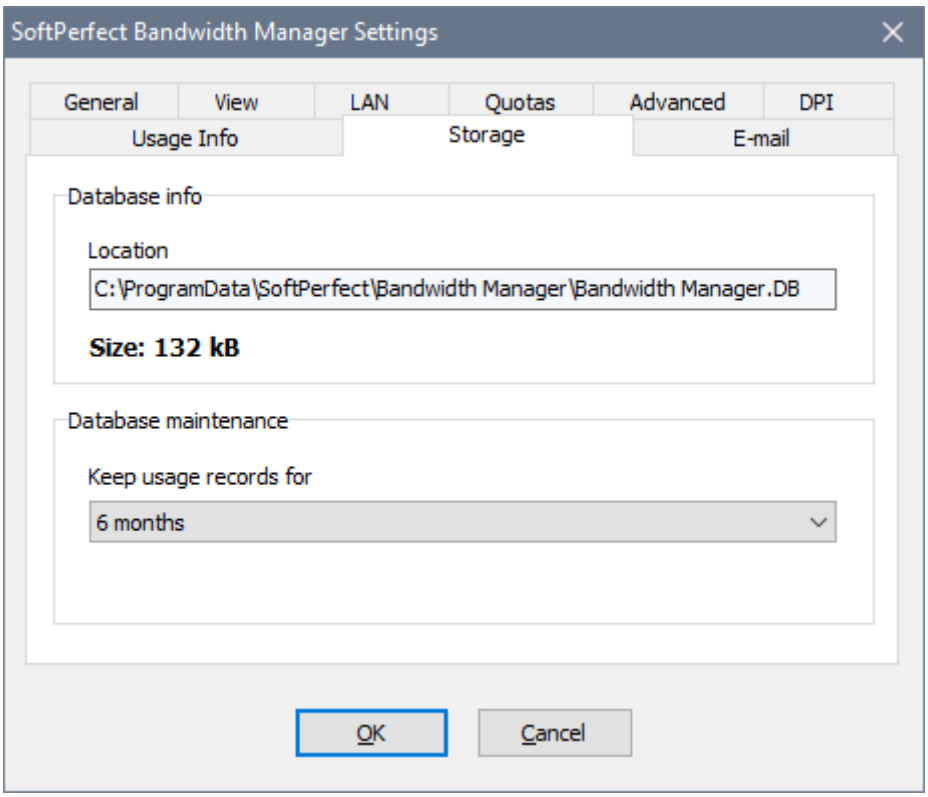


If you would like to use the E-mail notifications, open the **E-mail** tab, tick the corresponding option and specify your SMTP settings. The **SMTP server name**, **From address** and **From name** parameters are required. The **Authentication**, **User name** and **Password** parameters are optional:

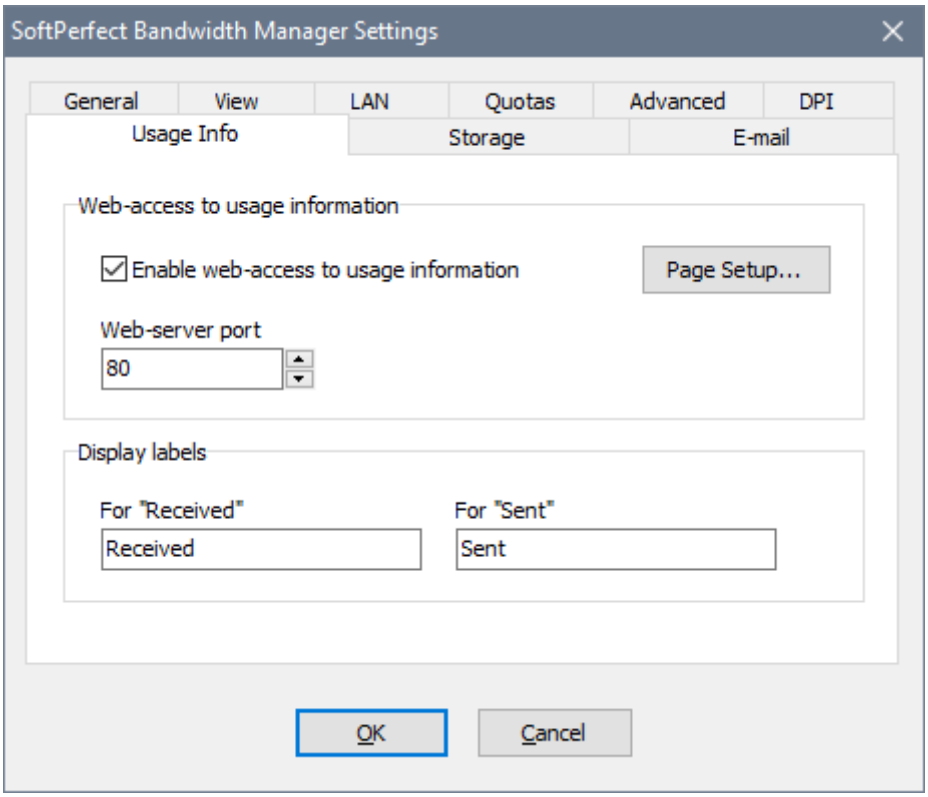


The **Storage** tab displays the bandwidth manager's database location and size. It also allows you to set for how long the usage records should be kept. You may want to reduce this period to optimise performance and have a smaller database.

The database is a standard SQLite 3 database and it can be opened in any SQLite management tool provided it is recent and supports SQLite databases created in the WAL mode.

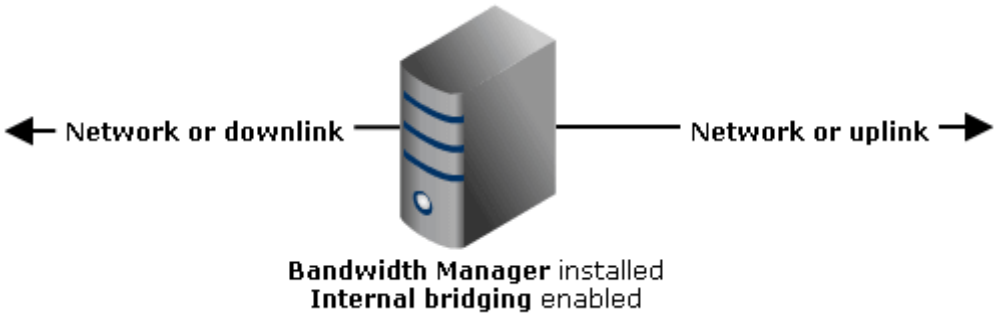


Using the **Usage Info** tab, you can provide users with web-access to their usage reports. In order to enable the built-in web-server, tick the corresponding option and make sure you have no other web-server software that may be using the chosen port:

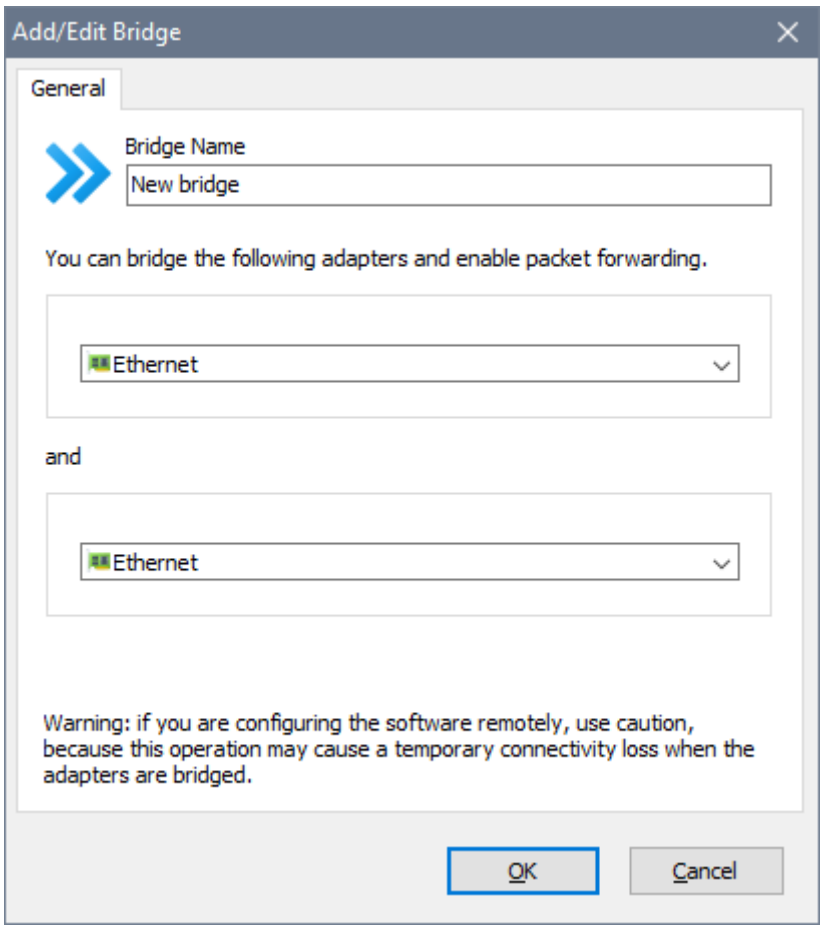


Adapter Bridging

Bandwidth Manager supports both the built-in Windows bridging feature and its own traffic forwarding implementation. This functionality is particularly useful when the PC running Bandwidth Manager acts as a bridge between two networks or between a network and an ISP connection. Additionally, a bridge can be seamlessly integrated into almost any network to manage and regulate traffic flow. In essence, it operates as a transparent bridge.



To enable bridging, you can use the recommended Windows adapter bridging feature: simply bridge two network adapters and apply traffic filtering to either one. Alternatively, open **Tools - Bridging** from the main menu and select the Ethernet adapters you wish to join:

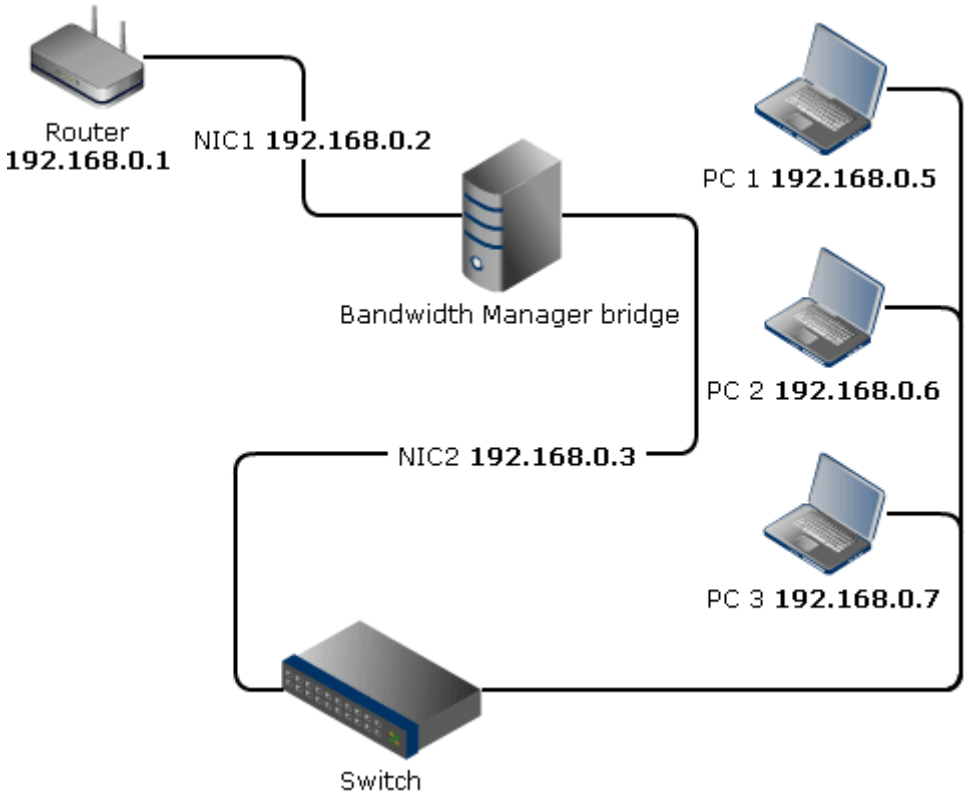


Once a bridge is defined, the software begins forwarding the traffic between the bridged adapters and you can proceed with rules. It is not recommended to configure rules with the **Any interface** scope as that might cause double packet processing and lower the performance.

Since the bridge is transparent, your network addressing scheme does not change. For example, you put the bridge between your network that uses 192.168.0.x addressing and a router that has address 192.168.0.1. Network cards merged into the bridge should be assigned any unused addresses in the 192.168.0.x range, so that the bridge itself will be able to communicate. The default gateway for network clients would still be 192.168.0.1 because requests from the clients would come through the bridge transparently to the router and back.

Potential connectivity issues

In some cases, after you have enabled bridging you can find that although the computers in the LAN can access the Internet normally, the bridge itself is unable to access the Internet or to connect to any computer in the LAN. This happens because of an incorrect IP configuration and routing of the bridge. In the following example we use a **192.168.0.x** network with a router assigned **192.168.0.1** to explain the problem and suggest a solution:



A common mistake is to specify the default gateway on both NICs in the bridge. The following configuration is **wrong** because both NIC1 and NIC2 are assigned the default gateway while the gateway is hooked up to NIC1.

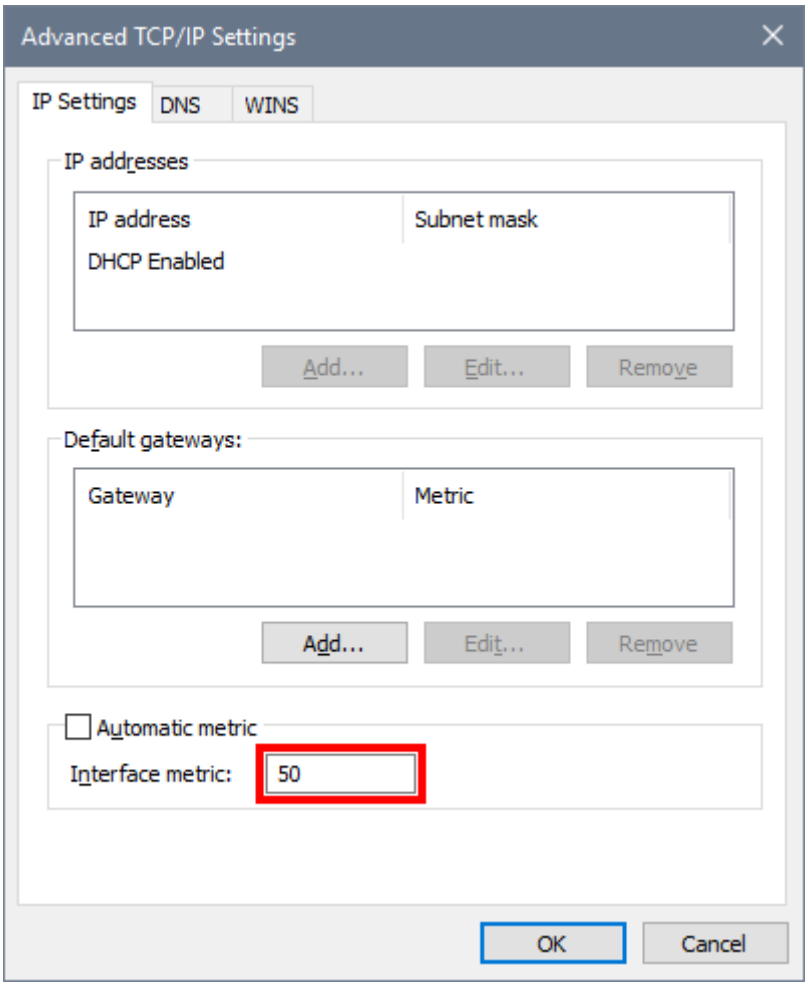
NIC1
IP address: 192.168.0.2
Mask: 255.255.255.0
Gateway: 192.168.0.1

NIC2
IP address: 192.168.0.3
Mask: 255.255.255.0
Gateway: 192.168.0.1

Essentially Windows does not know which NIC to use for Internet access, so it may be unable to establish the Internet connection. Simply remove the default gateway from all the NICs except the one connected to the router.

However, the bridge may still be unable to access the Internet and/or the LAN when both NICs are assigned IP addresses belonging to the same subnet. As the bridge has got two NICs assigned **192.168.0.2** and **192.168.0.3**, this is basically a routing issue. Suppose you want the bridge to connect to **192.168.0.7**. The question is which NIC should Windows choose to reach this address if it does not know which side it is hooked up to? Thereby we need to give Windows a hint using the route command and adjust the metrics.

Go to each NIC's **Advanced TCP/IP Settings** and assign a metric manually. The metric is merely a number representing the cost of a route. We need to assign a higher metric to NIC1. For example, you can assign 100 to NIC1 and 50 to NIC2:



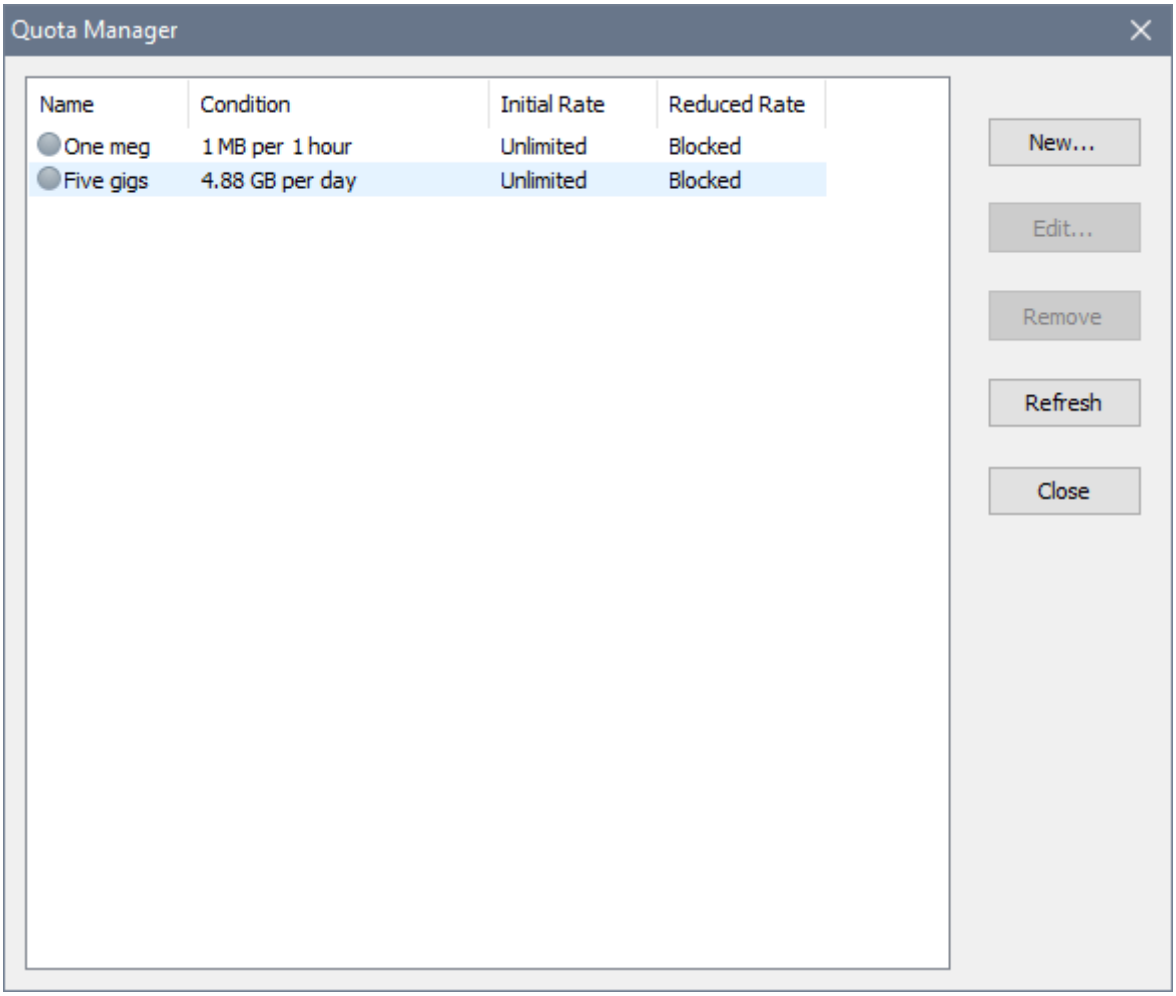
This will make Windows think the route through NIC2 is "cheaper" and it will route local traffic via this NIC properly. However, this will also break the Internet connection. In order to fix it, you need to execute the following command at a command prompt:

```
route -p add 192.168.0.1 mask 255.255.255.255 192.168.0.2
```

This tells Windows: access **192.168.0.1** via the NIC assigned **192.168.0.2**. So in this case Windows will access the Internet through gateway **192.168.0.1** via NIC1 due to this explicit routing record, and all remaining local addresses via NIC2.

Quotas

SoftPerfect Bandwidth Manager supports dynamic rule configuration based on quotas. When you create a rule, you can assign a previously defined quota instead of a fixed transfer rate. For example, you can permit users to upload or download a certain amount of data within a specified period at a certain speed, and decrease the speed if they exceeded the limit. The Bandwidth Control Service updates all rules according to the existing quotas once a minute.



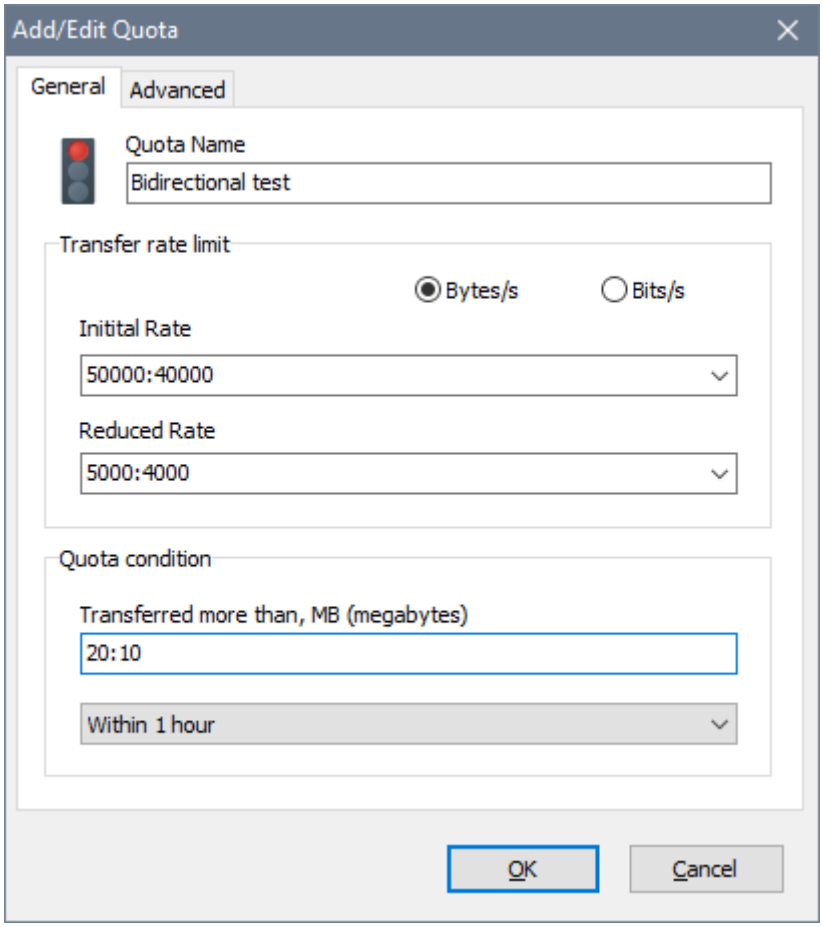
To define a quota, click the **New** button and in the new window specify the following:

- **Quota Name**: a descriptive name for the quota.
- **Initial Rate**: an initial transfer rate. This speed applies if a rule has not exceeded the limit.
- **Reduced Rate**: a reduced transfer rate. This speed applies if a rule has exceeded the limit. Choose **Block** if you would like to block the user completely, or choose **Suspend** to suspend the rule. A suspended rule is ignored and the user's traffic must be processed by one of the remaining rules in the ruleset, otherwise the user may gain unlimited access. Suspended rules allow to implement multilevel quotas or to show a custom message to the user. See the examples for details.

- **Transferred more than**: an amount of data in megabytes after which the transfer rate goes down.
- **Period**: a period the quota is for.

If you would like to use different download/upload rates and link this quota to a bidirectional rule, specify the rates separated by a colon. For example 100000:50000 would enforce a 100 kB/s limit on incoming traffic and a 50 kB/s limit on outgoing traffic. You can also specify a dual quota condition, for example 20:10 would give a user 20 MB of incoming data and 10 MB of outgoing data.

Note that for weekly quotas, a week by default means a period from Monday to Sunday. You can change this in the global settings.



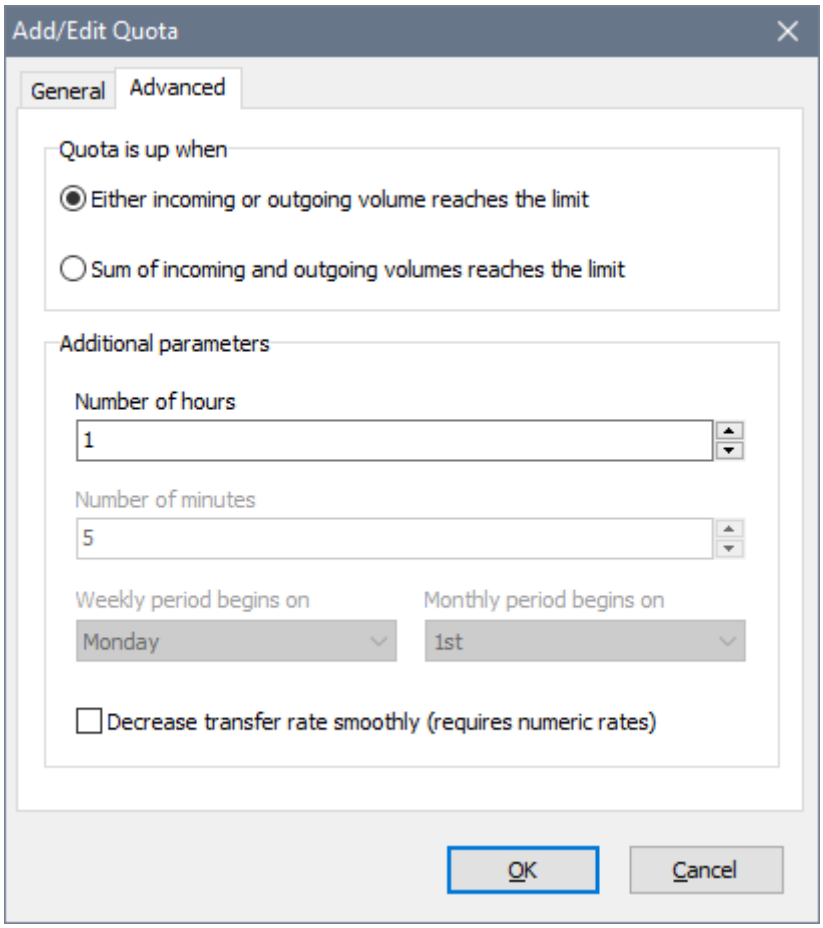
You may wish for the data transfer rate changes to take place gradually as the user quota is consumed. If the **Decrease transfer rate smoothly** option is enabled, the software will gradually decrease the transfer rate for all rules associated with the quota as it is used up.

Here is an example. The initial transfer rate is 100 kB/s, the reduced transfer rate is 10 kB/s and the quota limit is 100 MB. When the user consumes 10 MB of the quota, the transfer rate is decreased by 10% to 91 kB/s. When the user has consumed 20 MB, the transfer rate drops by another 10%, to 82 kB/s. This continues as the user quota is consumed, until the transfer rate reaches 10 KB/s.

On the **Advanced** tab you can specify how the quota limit is reached. This can be either:

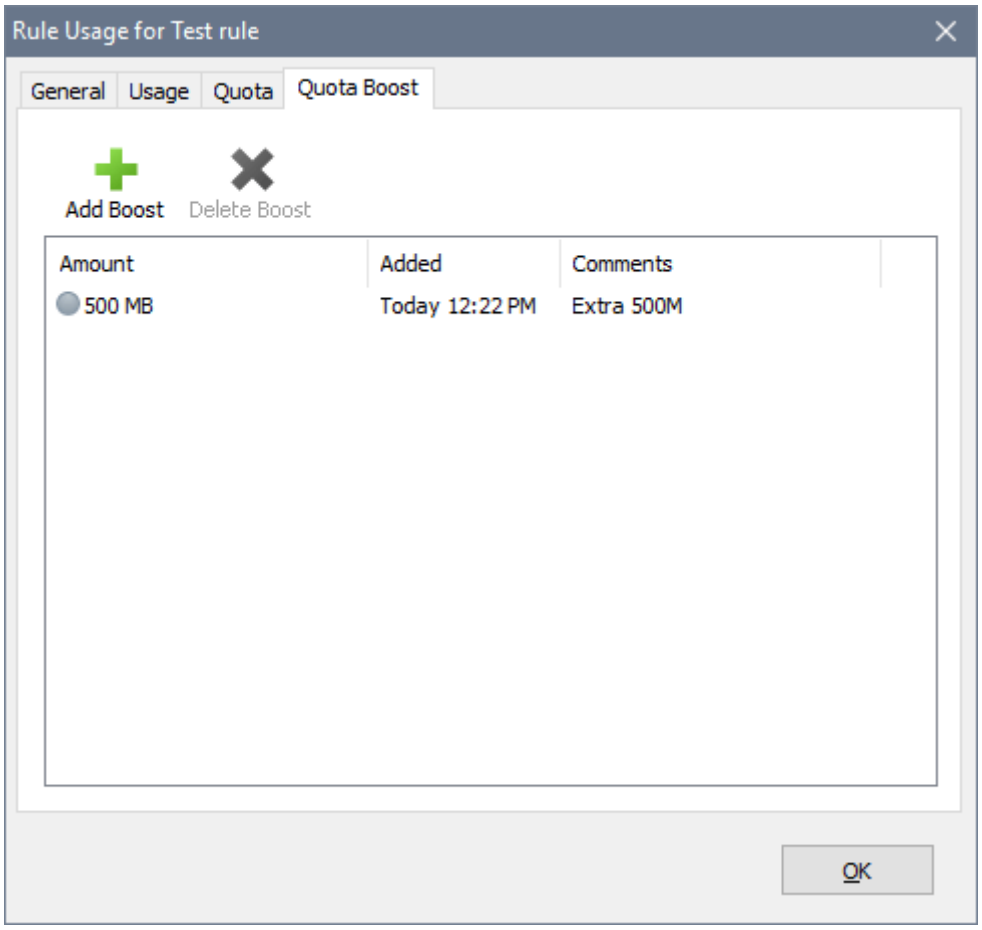
- When either incoming or outgoing traffic reaches the limit.
- When the sum of incoming and outgoing volumes reaches the limit.

You can also change the time span of minute and hour quotas, as well as specify when the billing period begins.



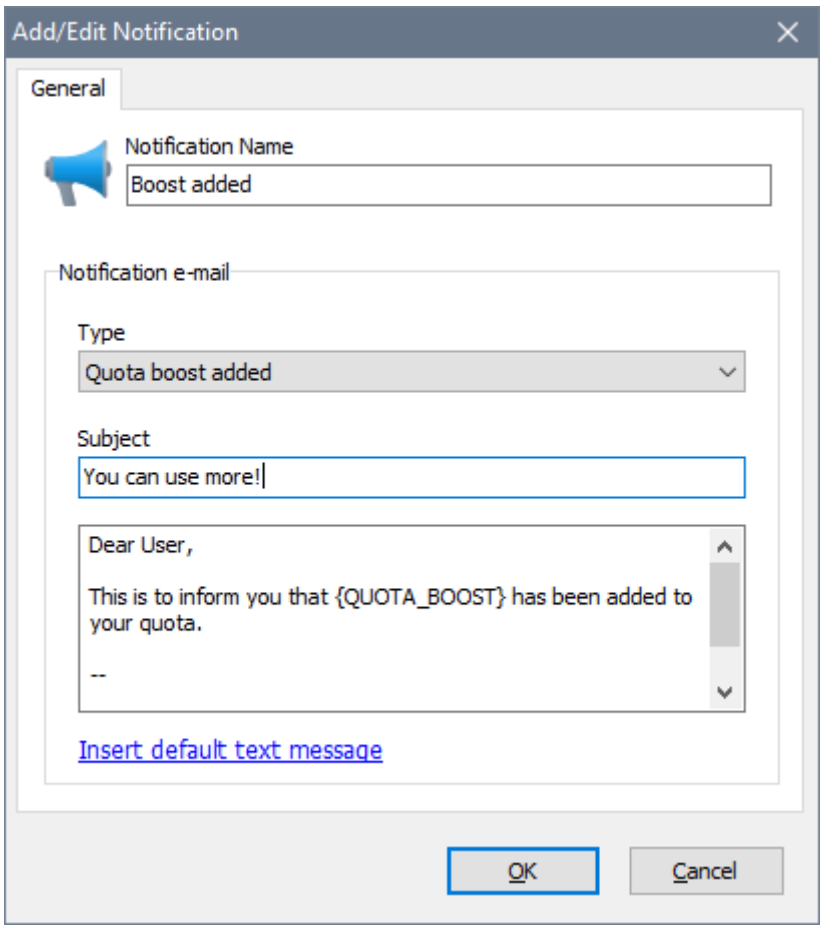
Quota Boost

The Quota Boost feature is useful when your users have an opportunity to get additional usage quota temporarily, for the current period. Once the period has lapsed, the quota automatically returns back to normal.

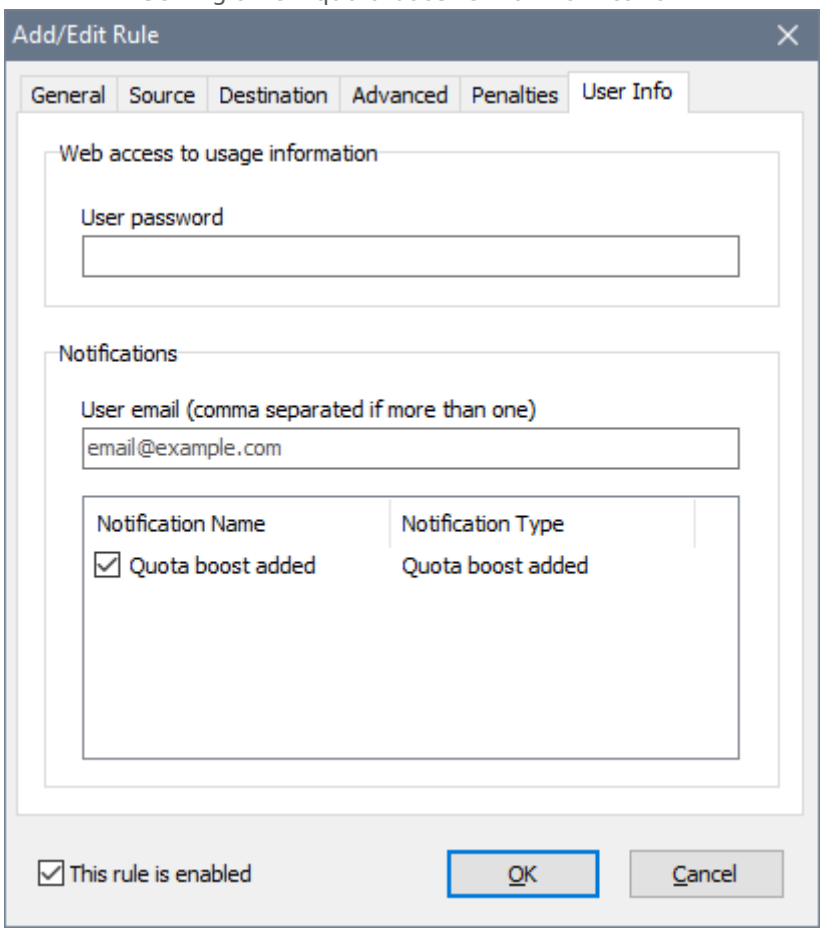


Adding a quota boost

Bandwidth Manager can also send an e-mail notification whenever a quota boost is added. Simply add a new notification of the **Quota boost added** type, and then activate it for the rule in the **User Info** tab:

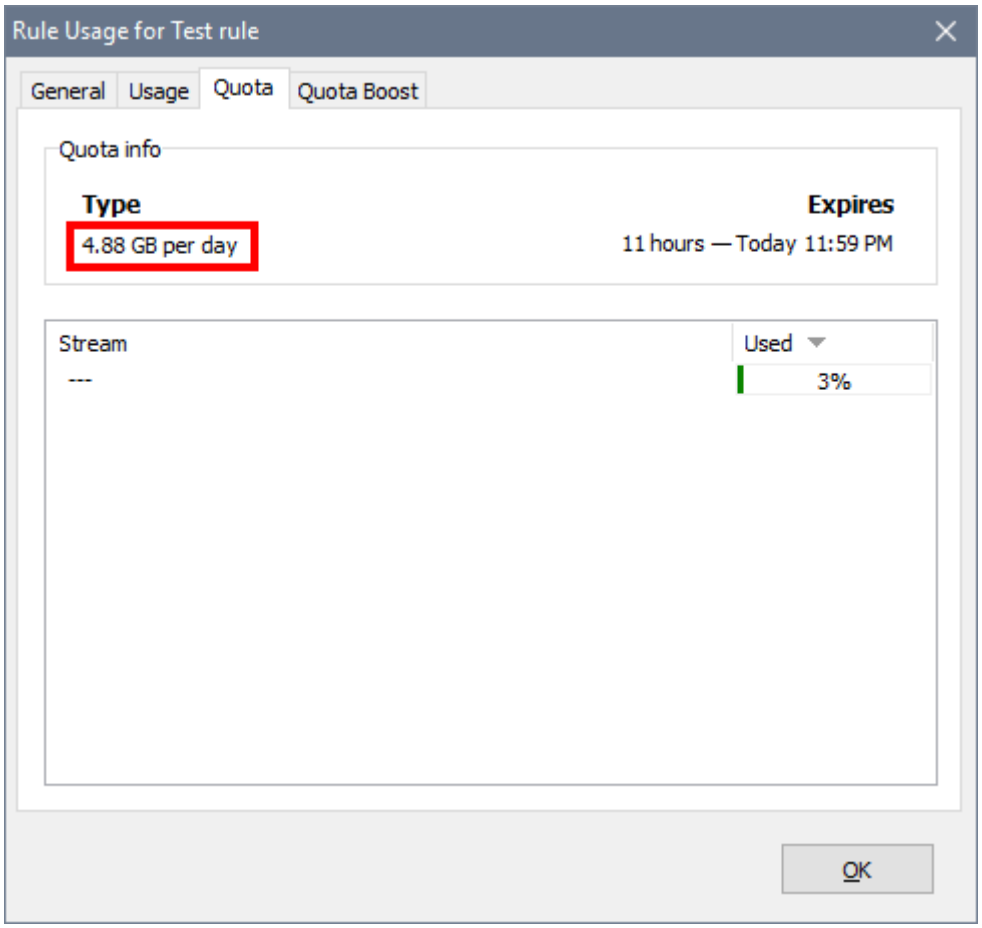


Setting a new quota boost e-mail notification

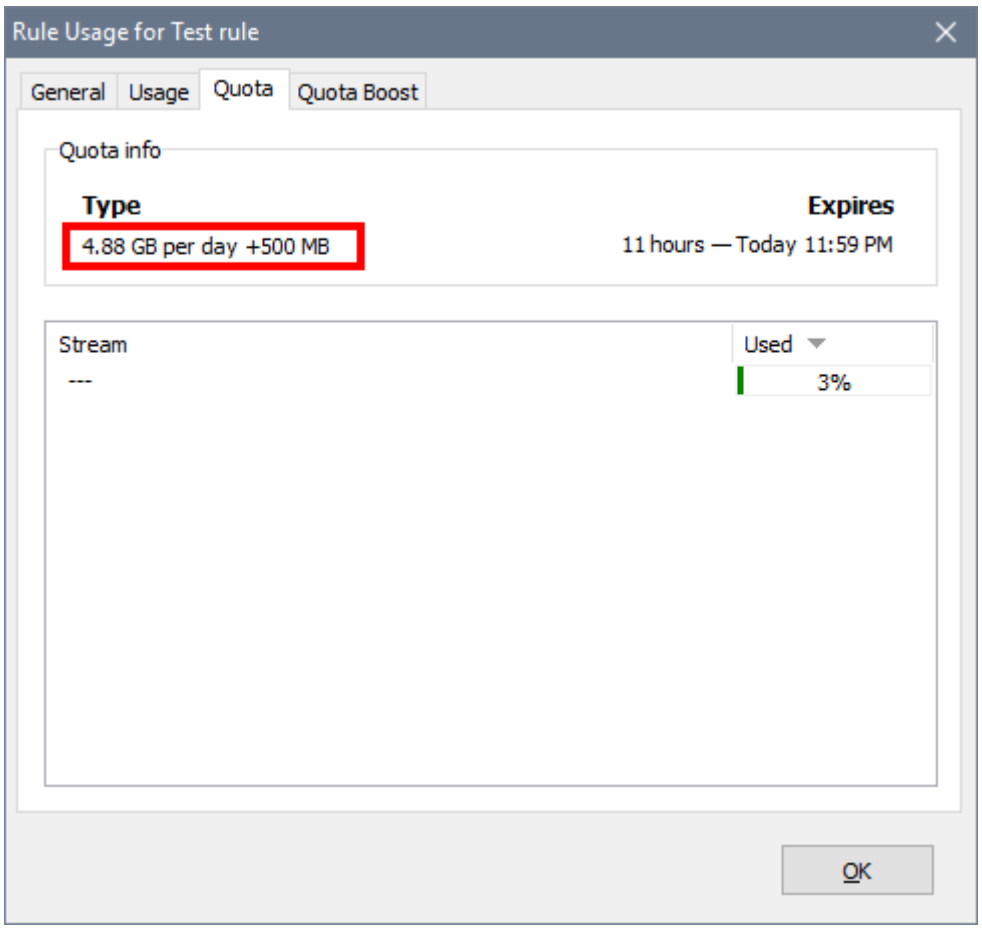


Activating the quota boost e-mail notification for the rule

The boosts are reflected both in the **Quota** tab of usage reports and in the web-reports.



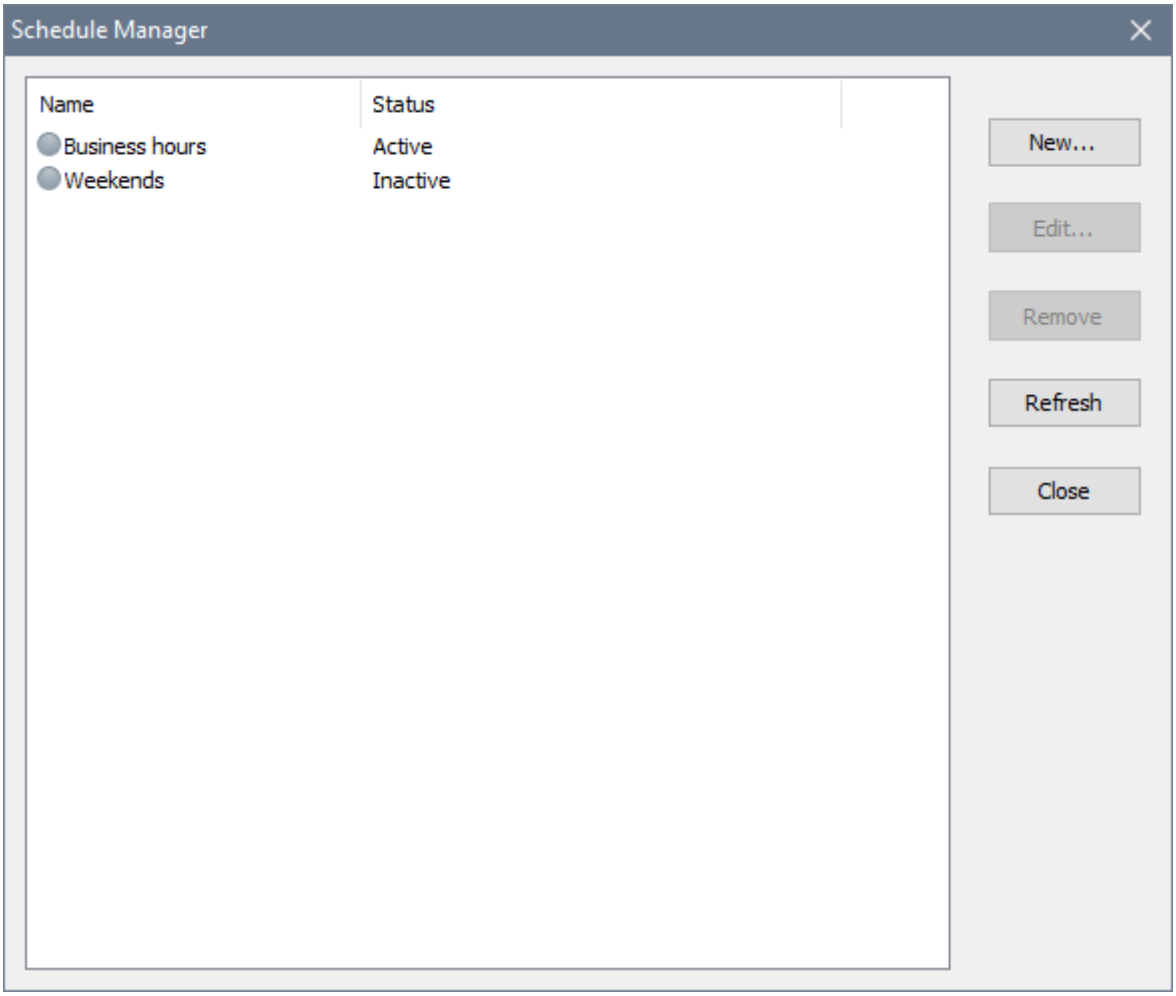
Quota before the boost



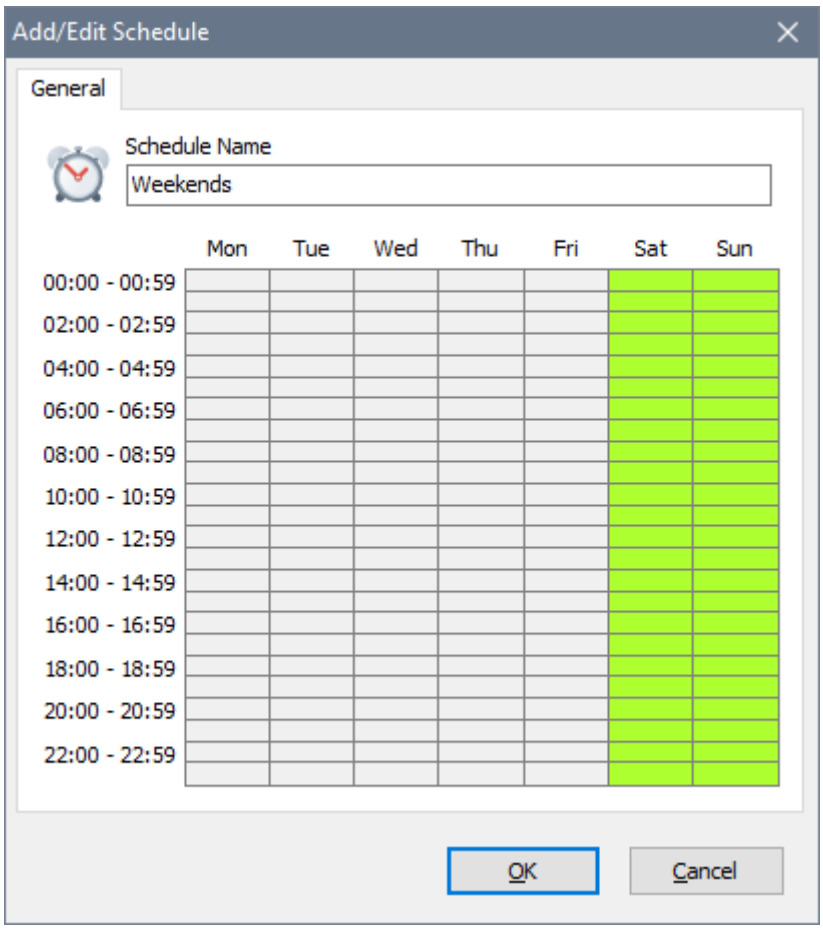
Quota after the boost, displaying normal + extra quota.

Scheduling

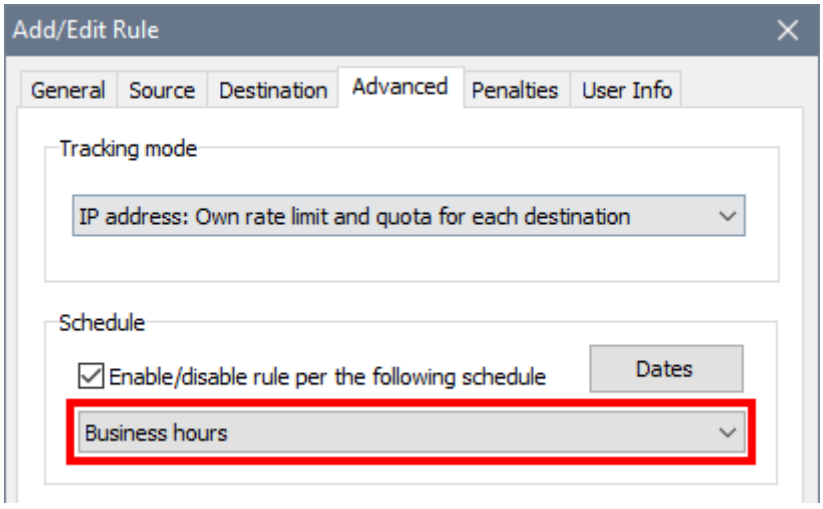
The software supports bandwidth management based on time of day and day of week. To access this feature, select **Tools - Schedules** from the main menu. Every schedule describes a weekly chart, when it is either active or inactive:



To define a schedule, click the **New** button. In the new window specify a schedule name and mark the hours when the schedule should be active. Green squares indicate active periods. In the example below, the entire weekend is made active:

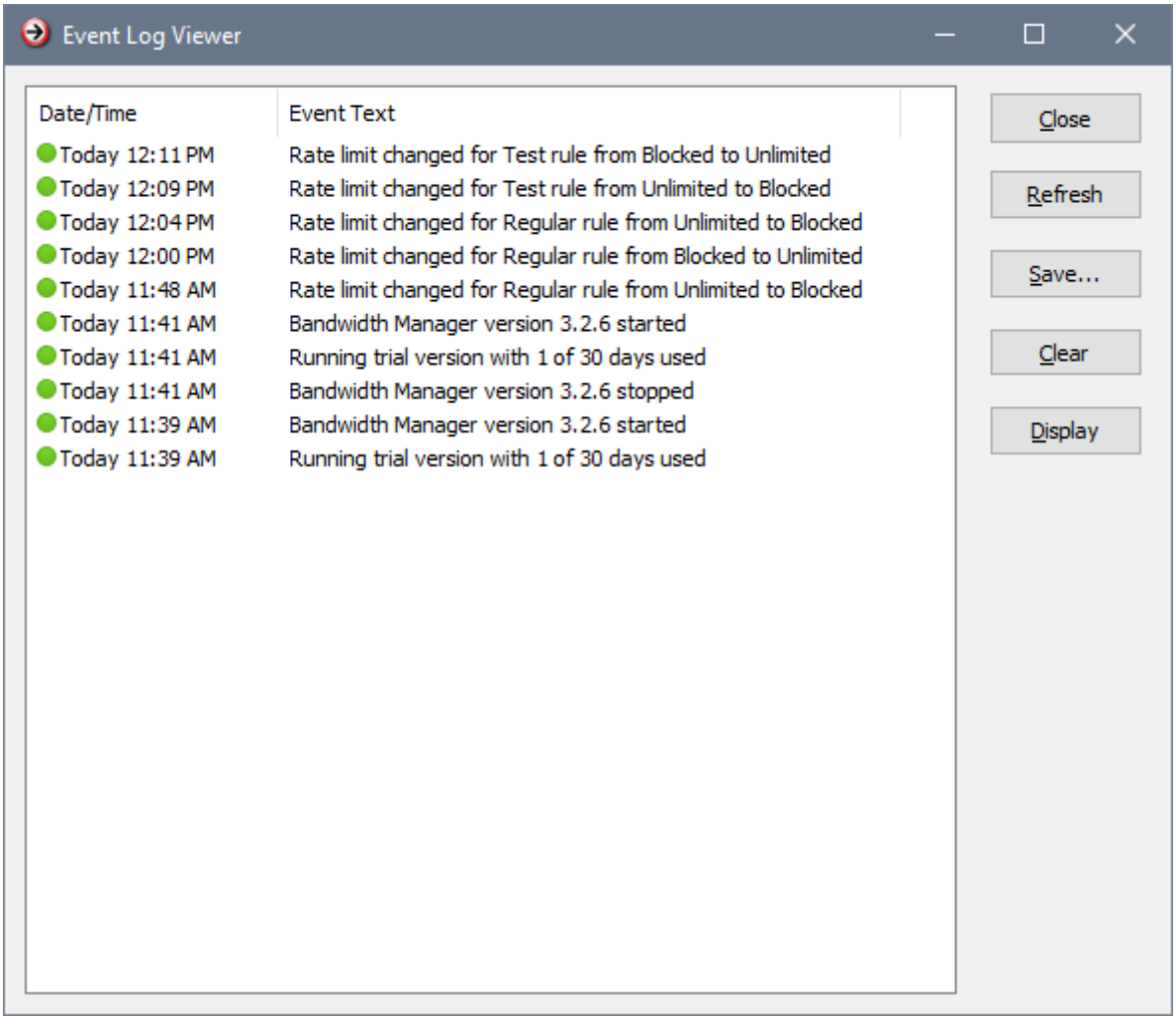


As soon as you create a schedule, you can link a rule with the newly created schedule in the **Advanced** tab in the rule properties. The software will enable and disable the rule in accordance with the schedule.



Event Viewer

The software keeps track of important events, problems and warnings and stores this information in a database. You can browse the events using the event viewer via **File - View Event Log** in the main menu:



Basic Usage Examples

Example 1: You have a network connected to the Internet through a Windows-based server. Users access the Internet through the server with ICS (Internet Connection Sharing) or NAT (Network Address Translation). You would like to limit Internet access speed for some or all users.

Install the Bandwidth Control Service on the Windows-based server and create rules with the Management Console. For example, if your network IP address range is 192.168.0.x and the server address is 192.168.0.1, your rules might look like this:

Rule #1:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.2
- Destination: Any IP Address
- Interface: LAN

Rule #2:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.3
- Destination: Any IP Address
- Interface: LAN

Rule #3:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.4
- Destination: Any IP Address
- Interface: LAN

In this case, a rule has been defined for three specific users and each rule would have an appropriate data rate limit. LAN is the network interface connected to the local network (not to the Internet). Any other network users not covered by the rules would have Internet access without restrictions. If you need to restrict Internet access speed for a larger number of users, it might be more convenient to use rules that apply to source address ranges or create a rule with tracking turned on.

This set of rules applies to any connection from selected network users to any IP address. If users access the Internet through a proxy server then example 2 applies.

Example 2: You have a network connected to the Internet through a Windows server. Users access the Internet through the proxy server. You would like to limit Internet access speed for some or all users.

Install the Bandwidth Control Service on the Windows server and create rules with the Management Console. If your network IP address range is 192.168.0.x, your rules might look like this:

Rule #1:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.2
- Destination: local host : proxy server port
- Interface: LAN

Rule #2:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.3
- Destination: local host : proxy server port
- Interface: LAN

Rule #3:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: 192.168.0.4
- Destination: local host : proxy server port
- Interface: LAN

This set of rules applies to any connection from selected network users to the proxy server port. LAN is the network interface connected to the local network (not to the Internet). For access to the Internet through the server with ICS (Internet Connection Sharing) or NAT (Network Address Translation) example 1 applies.

Example 3: You have a network connected to the Internet through a hardware router or a DSL modem. You would like to limit Internet access speed for some or all users but you do not need to limit traffic within your LAN.

In this case you need to install the software on each network computer on which you would like to set an Internet speed limit. Only the Bandwidth Control Service needs to be installed on each network computer. You will be able to configure the system services remotely with the Management Console installed on a single workstation. If your network IP address range is 192.168.0.x, your rules might be as follows:

Rule #1:

- Protocol: TCP/UDP
- Direction: Both
- Rate: Unlimited
- Source: Range 192.168.0.0 – 192.168.0.255
- Destination: Range 192.168.0.0 – 192.168.0.255

Rule #2:

- Protocol: TCP/UDP
- Direction: Both
- Rate: 10 KB/s
- Source: local host
- Destination: Any IP address

The first rule permits unlimited access to the LAN while the second sets an Internet access speed limit. Alternatively, instead of making the first rule, enable the **Ignore LAN traffic** option in the global settings. This will reduce the CPU's load and result in faster local file transfers.

If you do not want to install the software on each PC, there is another solution. In this case you may need to place an additional PC with Windows and two Ethernet cards between the local network and the uplink (modem, satellite, router). Then install the software on this PC and configure it to use the internal bridging or a third-party NAT solution. After that, create your rules as per example 1.

Advanced Usage Examples

The examples below involve quotas and suspended rules. When you define a quota, besides a flat transfer rate and "Blocked" options, you can also choose "Suspended". In this case, when the quota is used up, the rule will be suspended, which means it will be ignored until the quota is reset back. This feature has two useful applications as described below.

Multilevel quotas

For example, you could implement the following scenario: 80 MB download at full rate, then 10 MB at a reduced rate, after another 5 MB at even lower rate, and finally block the user completely. This can be done by defining three quotas and three rules as follows:

- Quota 1: Initial Rate: Unlimited, Reduced Rate: Suspended, Volume: 80 MB
- Quota 2: Initial Rate: 100 kB/s, Reduced Rate: Suspended; Volume: 10 MB
- Quota 3: Initial Rate: 10 kB/s, Reduced Rate: Blocked; Volume: 5 MB

- Rule 1: Source and Destination as needed, the rule is linked to Quota 1
- Rule 2: Source and Destination as needed, the rule is linked to Quota 2
- Rule 3: Source and Destination as needed, the rule is linked to Quota 3

In this case, provided that the rules are the same but linked with quotas 1, 2 and 3, these rules will come into effect sequentially. That is, Rule 1 will handle first 80 MB, Rule 2 will handle next 10 MB, and finally Rule 3 will let remaining 5 MB and then block the user.

“You have exceeded your quota” message

This might be useful for those who sell Internet access services to wired or wireless users and would like them to see a message (web-page) if they have used up their allocated quota. To do so, define a quota, for example:

Initial Rate: 100 kB/s, Reduced Rate: Suspended.

This will cause the software to skip the rule once the quota has been exceeded. Knowing this, you may define a ruleset as follows:

Rule 1. A regular rule linked with a quota to be consumed, which will later turn into the suspended state.

Rule 2. Redirect anyone to a web-page with a rule linked to a mapping.

Therefore, once the first rule is suspended, the second rule comes into play and the user will be redirected to a web-page of your choice. If the the quota is reset later, Rule 1 will come into effect again and the user can continue using the Internet.

Still not sure what to do? Please feel free to send us a message describing your network configuration and what you’d like to achieve. We will be glad to help.

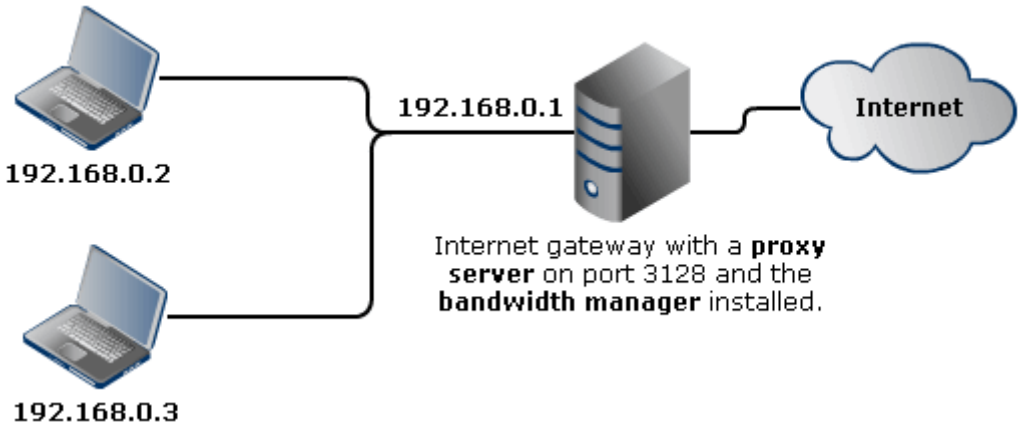
Port Mapping

This is an advanced topic. Port mapping allows any user requests sent to specific remote ports to be redirected to local ports instead. Choose **Tools - Mappings** from the main menu to access this feature. Port mapping can be used for transparent proxying, access control, etc. This feature can also redirect new network users, who are not currently configured in the bandwidth manager, to a “Welcome” web-page with your own content. This should be particularly useful for wireless ISPs.

While the port mapping feature has many useful applications, the current implementation has a limitation: it does not process outgoing traffic.

Here are further details on how transparent proxying and unknown user redirect are implemented using port mapping:

Transparent proxying is a complex technical task. You will need to have a thorough understanding of what you are doing, as well as a good understanding of the TCP layer, the HTTP protocol and what is happening in the connection. Basically, you will need a Windows-based computer to act as a gateway. The Bandwidth Manager and a proxy server should be installed on this computer as shown in the example below:



Here is a brief explanation for this example: You want the users with network addresses 192.168.0.2 and 192.168.0.3 to access the WWW through the proxy server. Currently, the users are able to access the WWW directly through the gateway. The proxy server runs on port 3128. First, you need to define a mapping which redirects data packets to local port 3128. Then set a rule for 192.168.0.2 and associate it with the mapping that was just defined. It looks like this:

- Source: 192.168.0.2
- Destination: Any address on port 80
- Protocol: TCP
- Interface: LAN

The rule for 192.168.0.3 will be similar. Now, if you have done everything correctly and the proxy server is properly configured, any HTTP request from 192.168.0.2 will be intercepted by the Bandwidth Manager and forwarded to the local proxy server through port 3128. The proxy server then analyses the request, downloads the requested information from the Internet, returns it to the Bandwidth Manager which, in turn, returns it to the user who initiated the request.

Note: configuring the proxy server is a separate task and is out of the scope of this document.

Unknown user redirect. This technique is very useful for wireless Internet service providers where new users can appear on the network at any time. You need a network configured like the one described above for transparent proxying. The workstations can be wired, wireless or a mixture.

Here is an example using the same network configuration as before. You want any new users who join your network to be redirected to a “Welcome” page where they can read how to pay for the Internet services you provide. You should run a local DHCP and web-server. Your current rule set should look like this:

Rule 1

- Source: 192.168.0.2
- Destination: Any IP address
- Protocol: TCP
- Interface: LAN

Rule 2

- Source: 192.168.0.3
- Destination: Any IP address
- Protocol: TCP
- Interface: LAN

Rule 3

- Rate: Unlimited
- Source: 192.168.0.0 – 192.168.0.255
- Destination: Any IP address on port 80
- Protocol: TCP
- Interface: LAN

Rule 4

- Rate: Blocked
- Source: 192.168.0.0 – 192.168.0.255
- Destination: Any IP address
- Protocol: TCP
- Interface: LAN

Rules 1 and 2 are associated with the existing workstations. Rule 3 must be associated with a port redirect to the specific local URL where your "Welcome" page is located. If, for example, the page is on host http://192.168.0.1/welcome.php, you need to define a mapping with this URL and associate it with the third rule. Any new user who is not listed in rules 1 and 2 will be allocated an address in the range 192.168.0.0 – 192.168.0.255 by the DHCP server. They will then be caught by the third rule and redirected to your "Welcome" web-page. Obviously this procedure works for HTTP requests only.

Known Issues and FAQ

Known Issues

Problem: SoftPerfect Bandwidth Manager does not support Windows bridged connections.

Solution: Use the Bandwidth Manager's internal bridging instead.

FAQ

Q: I am trying to connect to the Bandwidth Manager service, but getting a message like Connection Timeout or Connection Refused.

A: Try the following:

- Disable your firewall if it is installed. This includes the built-in Windows firewall.
- Make sure that you have installed the Bandwidth Control Service on this PC and it is running. It starts automatically on system boot. However, you can start it from the Administrative Tools – Services control panel applet.
- Look for any error messages in the Windows event log.

Q: Is your Bandwidth Manager compatible with the Microsoft ISA Server?

A: Yes, there are no known issues.

Q: Is your Bandwidth Manager compatible with the ICS (Internet Connection Sharing)?

A: Yes, it is fully compatible.

Q: How can I control the Bandwidth Manager remotely? Is there a web-based interface?

A: SoftPerfect Bandwidth Manager does not support a web-based interface, but it can be controlled remotely. It uses the standard TCP protocol, port 8701 to communicate between the Management Console and the Bandwidth Control Service. You can connect to the server with the Bandwidth Control Service through your LAN or the Internet using the GUI. Simply specify a host name or IP address of the machine with the running Bandwidth Manager service.

Q: Is there a way to control SoftPerfect Bandwidth Manager from our billing system? Is there any API?

A: There are two ways to access the Bandwidth Manager service:

- Direct reading of the database. The Bandwidth Manager uses a standard SQLite 3 database that can be read from many programming languages and environments.

The database can be found via the path shown under the Storage tab in the Bandwidth Manager's settings.
- There is an XML-based API, which however doesn't have an official documentation. To trace the exchange between the Bandwidth Manager console and the core, you need to use a protocol analyser. The protocol is quite self-explanatory.

Q: How do I configure SoftPerfect Bandwidth Manager to start automatically with Windows?

A: The Bandwidth Control Service actually starts automatically and runs as a service. This means it starts on every system boot before you log in, and it stops when the system shuts down. It controls bandwidth even when you do not have the Management Console running.

Adding proxy server: transparent proxying with Bandwidth Manager and Squid

Introduction

This article tells how to install and configure Squid and Softperfect Bandwidth Manager to enable transparent proxying in a Local Area Network (LAN). Transparent proxying lets you cut usage of your Internet connection and, as the name suggests, this process is invisible to the end users. In order to implement this, you need to have a running server with Windows XP or above, a latest copy of Softperfect Bandwidth Manager and a copy of Squid Cache. Since Squid is distributed in a form of source code, the next chapter will tell you where to get a ready-to-install Windows build and how to install it.

Getting and installing Squid

The latest stable version of Squid available at the time of publication was 2.7 stable 5. You can download it from the official Squid website. Once you have downloaded Squid, unpack the ZIP file to the **c:\squid** folder. You may want to choose a different folder for Squid, but bear in mind that this will require you to update paths throughout the Squid configuration file. The following instructions assume that you have unpacked Squid to **c:\squid**.

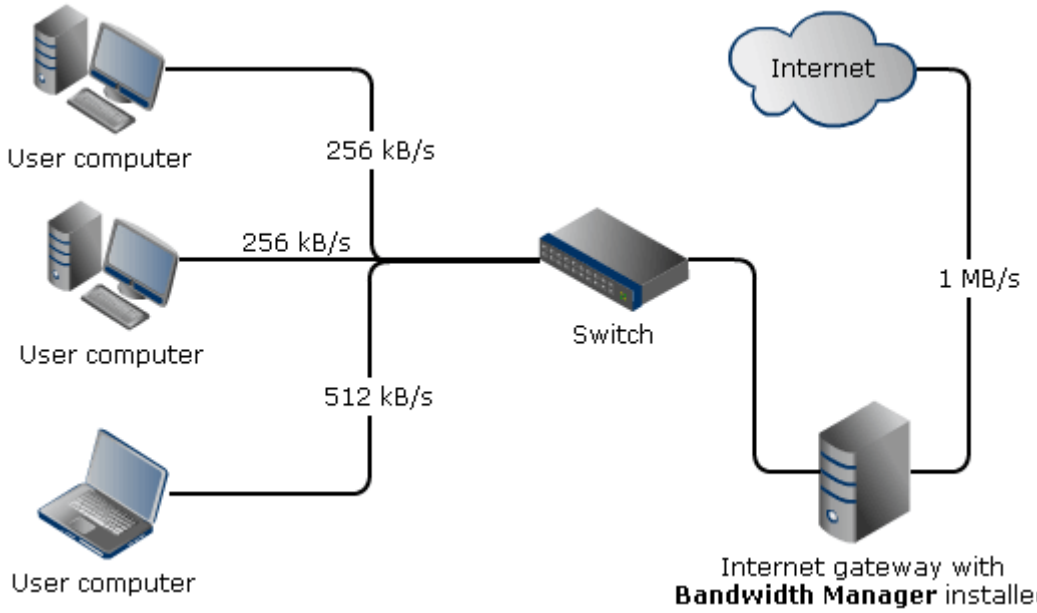
1. Go to **c:\squid\etc** and copy the Squid default configuration files as follows:

From	To
cachemgr.conf.default	cachemgr.conf
mime.conf.default	mime.conf
squid.conf.default	squid.conf

2. Open the newly copied **c:\squid\etc\squid.conf** in Notepad and locate the line **http_port 3128**. Add the keyword **transparent** to make Squid understand regular HTTP request, so the line is **http_port 3128 transparent**.
3. Before you start Squid for the first name, you must initialise its cache. Launch **c:\squid\sbin\squid.exe -z** to initialise the cache.
4. Install Squid as a Windows service. Launch **c:\squid\sbin\squid.exe -i** to install it as a service.
5. Attempt to start the service by typing **net start squid** at a command prompt. If it starts successfully, you have finished initial Squid configuration. If it does not and displays “The process terminated unexpectedly”, there is one more configuration parameter that you need to change. Open **c:\squid\etc\squid.conf** again and uncomment the **unlinkd_program** parameter. Then replace regular slashes with backslashes, i.e. change it from **c:/squid/libexec/unlinkd.exe** to **c:\squid\libexec\unlinkd.exe**. Now you should be able to start the Squid service cleanly.

Configuring Softperfect Bandwidth Manager

In order to setup transparent proxying, we will use the port mapping feature available in the Bandwidth Manager. This feature only works for incoming connections (i.e. requests made from client computers), so you will need to have the Bandwidth Manager installed on a server with two network cards and NAT or routing configured. In this article we assume that you have the Windows Internet Connection Sharing (ICS) enabled on this server and all the hardware is connected as shown below:



If your setup is similar to this, you can proceed with the Bandwidth Manager configuration. Choose **Tools - Port Mapping** from the main menu and define a mapping as shown below.

Example mapping:

```
Mapping name: Squid

Redirect to local port: 3128
```

Then define a bandwidth management rule. Set the source and destination according to your needs. In this example we redirect all HTTP traffic coming from client computers in the range 192.168.0.1 - 192.168.0.255. It is important to choose the correct network card to apply the rule on. In this example **Internal** refers to a network card facing the LAN clients.

Example rule:

```


General:

Rate limit: 100000
```

```
Protocol: TCP

Interface: Internal


Source:

Address range: 192.168.0.1 - 192.168.0.255

Port: Any


Destination:

Address: Any

Port: 80


Advanced:

Process through mapping: Squid
```

Now all users in the range 192.168.0.1 – 192.168.0.255 accessing web-resources via port 80 will have their requests processed by Squid. Check **c:\squid\var\logs\access.log** and **c:\squid\var\logs\cache.log** to make sure everything is working correctly. Whenever you design bandwidth management rules, bear in mind that it only makes sense to redirect HTTP requests to Squid. This is also the reason why we have set destination port to 80 to filter out all other types of traffic. Attempting to route DNS, SMTP, POP3 or any protocol other than HTTP via Squid will fail.

Further reading

- More information about Squid including FAQ and configuration guide is available at the official Squid website.
- Questions and comments are welcome at our online forum.