

Kerio Control

Administrator's Guide

Kerio Technologies

Contents

Installing Kerio Control	12
Product editions	12
Installing Software Appliance edition	12
Installing VMware Virtual Appliance	13
Installing virtual appliance for Hyper-V	13
Installing virtual appliance for Parallels	14
Setting Up Kerio Control Box	15
Kerio Control Box models	15
Connecting Kerio Control box to the network	15
Initial setup	16
Configuring the Activation Wizard	17
Configuring the Activation Wizard	17
Select a language	17
Connect to the Internet	17
Set the time zone, date and time	17
Activate Kerio Control	17
Register offline	18
Help us make Kerio Control even better	19
Set the password for the administrator user account	19
Configuration Assistant	20
Configuration Assistant overview	20
Configure Internet connection and the local network	21
Single Internet Link	21
Two Internet links with load balancing	22
Two Internet links with failover	23
General notes	24
Define traffic policy	24
Export your configuration	25
Import configuration	25
Install license / Register product with a purchased license number / Register trial version / Update registration info	25
Licenses and registrations	26
Deciding on a number of users (licenses)	26
Licenses, optional components and Software Maintenance	26
Registering Kerio Control in the administration interface	26

Registering the trial version	27
Registering full version	27
Registering Kerio Control via WWW	29
Importing license key	29
Connecting to Kerio Control	30
Web interfaces overview	30
Web interface and certificate settings information	30
User authentication at the web interface	32
Configuring network interfaces	33
Interfaces overview	33
Configuring interfaces	33
Moving an interface to another group	33
Configuring Internet connectivity	33
Adding new interfaces	34
Configuring PPPoE mode in the Internet interface	34
Configuring PPPoE tunnel	35
Configuring PPTP tunnel	35
VPN tunnel	36
Configuring Ethernet ports	36
Box Edition	36
Appliance Editions	37
Configuring VLANs	38
VLAN support in Kerio Control	38
Creating VLAN interfaces	38
Removing VLAN interfaces	38
Configuring Kerio VPN server	40
VPN overview	40
Configuring Kerio VPN Server	40
Configuring routing	40
Configuring Kerio VPN clients	41
Configuring Kerio VPN tunnel	42
Kerio VPN overview	42
Prerequisites	42
Configuring Kerio VPN tunnel	42
Configuring routing	43
Example of Kerio VPN configuration: company with a filial office	44
Overview	44

Example of Kerio VPN configuration: company with two filial offices	50
Overview	50
Configuring IPsec VPN	60
IPsec overview	60
Configuring IPsec VPN server with a preshared key	60
Configuring IPsec server with a SSL certificate	62
Configuring clients with a preshared key	63
Supported mobile devices	63
Configuring IPsec VPN tunnel	64
IPsec overview	64
Configuring IPsec VPN tunnel with a preshared key authentication	64
Configuring IPsec VPN tunnel with a SSL certificate authentication	64
Support for IPv6 protocol	66
Support for IPv6 protocol	66
Filtering IPv6 overview	66
IPv6 router advertisement	67
Configuring traffic rules	68
How traffic rules work	68
Configuring traffic rules	68
Example 1: Port mapping	69
Other examples	70
User accounts and groups in traffic rules	70
Demilitarized zone (DMZ)	72
Policy routing	72
Configuring IP address translation	73
IP address translation (NAT) overview	73
Configuring IP address translation	73
A default NAT rule description	75
Configuring traffic rules — multihoming	77
Multihoming overview	77
Configuring traffic rules — limiting Internet access	79
Limiting Internet Access	79
Configuring traffic rules — exclusions	81
Configuring exclusions	81

Configuring Demilitarized Zone (DMZ)	82
Demilitarized Zone (DMZ)	82
Configuring DMZ	82
Configuring policy routing	84
Policy routing overview	84
Configuring a preferred link for email traffic	84
Configuring an optimization of network traffic load balancing	86
Configuring intrusion prevention system	87
Intrusion prevention system overview	87
Configuring intrusion prevention	87
Configuring ignored intrusions	88
Configuring protocol-specific intrusions	88
IP blacklists overview	89
Automatic updates	89
Filtering MAC addresses	90
Filtering MAC addresses overview	90
Configuring the filter	90
Configuring Universal Plug-and-Play (UPnP)	91
Universal Plug-and-Play (UPnP) overview	91
Configuring the UPnP support	91
Configuring bandwidth management	93
Bandwidth management overview	93
How bandwidth management works	93
Internet Links Speed	93
Configuring bandwidth management	93
Configuring HTTP policy	96
HTTP policy overview	96
Conditions for HTTP filtering	96
Adding HTTP rules	97
Applying rules also for local servers	99
URL Groups	99
Defining a new URL group	100
Configuring HTTP cache	101
HTTP cache overview	101
Configuring a HTTP cache	101
Configuring TTL	101
Configuring cache size	102
Cache status and administration	102

Proxy server	103
Proxy Server overview	103
Filtering web content by word occurrence	106
Kerio Control word filter overview	106
Adding a new forbidden word	106
Defining a URL rule filtering by word occurrence	107
Using Kerio Control Web Filter	108
Kerio Control Web Filter overview	108
Enabling Kerio Control Web Filter	108
Testing URLs	109
Creating a URL whitelist	109
Using Web Filter in URL rules	109
Antivirus protection	111
Antivirus overview	111
Conditions and limitations of antivirus scan	111
Antivirus scan setup	112
HTTP and FTP scanning	114
Email scanning	117
Using DHCP module	120
Why to use DHCP server in Kerio Control	120
Automatic configuration of IP scopes	120
Manual definition of Scopes and Reservations	121
Defining individual scopes	122
Leases and Reservations	123
Reserving an IP address	123
Using the DNS module	124
DNS forwarding service in Kerio Control	124
Configuring simple DNS forwarding	124
Hosts table	125
Configuring custom DNS Forwarding	126
Defining a rule	126
Clearing the cache	128
Configuring a routing table	129
Routing table overview	129
Statistics and reports	132
Statistics and reports overview	132
Monitoring and storage of statistic data	132
Settings for statistics, reports and quota	134

Logging on the web interface and viewing of statistics	136
Administrative settings	139
System Configuration (editions Appliance and Box)	139
Update Checking	139
Configuring the SMTP server	141
SMTP Server Configuration	141
P2P Eliminator	143
P2P Eliminator overview	143
P2P Eliminator Configuration	143
Parameters for detection of P2P networks	144
Dynamic DNS for public IP address of the firewall	146
Dynamic DNS for public IP address of the firewall	146
Creating user accounts	148
User accounts overview	148
Adding new accounts	148
Adding local accounts	148
Adding accounts from a directory service	149
Using templates	149
Configuring accounts	149
Configuring user quota	149
Automatic login on static IP addresses	150
Deleting user accounts	151
Disabling users temporarily	151
Deleting users permanently	151
Troubleshooting	152
Setting access rights in Kerio Control	153
Setting access rights	153
What levels of access rights are available	153
Connecting Kerio Control to directory service	155
Which directory services are supported	155
What is the connection used for	155
Microsoft Active Directory	155
Conditions for mapping from Active Directory domains	155
Connecting to Microsoft Active Directory	156
Connecting to Apple Open Directory	156
Connecting to other domains	157
Configuring encrypted connection (LDAPS)	157
Collision of directory service with the local database and conversion of accounts	158

User authentication	159
User authentication overview	159
Firewall User Authentication	159
Creating user groups in Kerio Control	162
User groups overview	162
Creating user groups	162
Creating local groups	162
Configuring SSL certificates in Kerio Control	163
SSL certificates overview	163
Creating a new Local Authority	163
Creating a certificate signed by Local Authority	164
Creating a certificate signed by a Certification Authority	164
Configuring IP address groups	165
Using IP address groups	165
Configuring IP address group	165
Creating time ranges in Kerio Control	166
Time ranges overview	166
Defining time ranges	166
Using services	168
Services	168
Using services	168
Protocol inspectors	169
Disabling a protocol inspector	169
Using Status - Active Hosts	171
Status - Active Hosts overview	171
Using Status - Active Connections	177
Status - Active Connections overview	177
Using Status - VPN Clients	180
Status - VPN Clients overview	180
Using Status - Alert Messages	181
Status - Alert Messages overview	181
Using Status - Statistics	185
Status - Statistics overview	185
Volume of transferred data and quota usage	185
Traffic Charts	187
Using Status - System Health	190

Status - System Health overview	190
Using logs	191
Logs overview	191
Logs Context Menu	191
Logs Settings	193
Alert Log	195
Config Log	195
Connection Log	197
Debug Log	198
Dial Log	199
Error Log	201
Filter Log	203
Http log	205
Security Log	207
Warning Log	210
Web Log	211
Generating a Software Appliance installation USB flash disk	213
Generating a Software Appliance installation USB flash disk	213
Linux	213
Mac OS X	213
Automatic user authentication using NTLM	215
Automatic user authentication using NTLM overview	215
General conditions	215
Configuring Kerio Control	215
Web browsers	216
NTLM authentication process	217
FTP over Kerio Control proxy server	218
FTP over proxy server overview	218
Configuration files	221
Configuration files overview	221
Configuring backup and transfer	223
Backup and transfer	223
Tips for tablets	224
Tips	224

Legal Notices	225
Trademarks and registered trademarks	225
Used open source software	225

Installing Kerio Control

Product editions

Software Appliance

[Kerio Control Software Appliance](#) is a package of Kerio Control and a special Linux-based operating system. Install the appliance on a PC without an operating system.

Virtual Appliance

Kerio Control Virtual Appliance is the software appliance edition pre-installed on a virtual host for the particular hypervisor. Virtual appliances for [VMware](#), [Hyper-V](#) and [Parallels](#) are available.

Kerio Control Box

Kerio Control Box is a hardware device with Kerio Control Software Appliance pre-installed. Two models are available. For more details, refer to the [Setting up Kerio Control Box](#) article.

Installing Software Appliance edition

Install this edition on a PC without operating system.



Any existing OS and files on the target hard disk will be erased!

For hardware requirements, read [Technical Specifications](#).

1. Download the ISO image from the [Download page](#).
2. Select one of these actions:
 - Burn the ISO image on a CD/DVD
 - Use the ISO image to create a bootable USB flash disk
3. Boot from the appropriate drive. The installation runs automatically.
4. Follow the instructions on the computer's console to perform the basic configuration.
5. To perform the initial setup, open the following address in your web browser:
`https://kerio_control_ip_address:4081/admin`
6. Follow the Activation Wizard.

After finishing the wizard, Kerio Control displays the login page.

Installing VMware Virtual Appliance

For hardware requirements and supported VMware products, read [Technical Specifications](#).

For **VMware Server, Workstation, Player and Fusion**:

1. Download the zipped VMX package from the [Download page](#) and unpack.
2. Open the .vmx file in your VMware hypervisor.

For **VMware ESX and ESXi**:

1. Copy the .ovf file location from the [Download page](#).
2. Paste the OVF file location into the import dialog in your VMware hypervisor.



After the import, it is recommended to check the shutdown and restart actions settings for the imported virtual machine. To avoid loss of data in the virtual appliance, use "soft power operations" (**Shutdown Guest** and **Restart Guest**).

Complete the installation:

1. Follow the instructions on the virtual appliance console to perform the basic configuration.
2. To perform the initial setup, open the following address in your web browser:
`https://kerio_control_ip_address:4081/admin`
3. Follow the Activation Wizard.

After finishing the wizard, Kerio Control displays the login page.

Installing virtual appliance for Hyper-V

For hardware requirements and supported Hyper-V hypervisors, read [Technical Specifications](#).

Kerio Control Virtual Appliance for Hyper-V is distributed as a virtual hard disk.

1. Download the Hyper-V package from the [Download page](#).



After importing the appliance into Hyper-V, the location cannot be changed.

Installing Kerio Control

2. Go to the Server Manager control panel to add the Hyper-V role (**Roles → Add Roles**).
3. Go to the Hyper-V Manager control panel and select the local Hyper-V server.
4. Run the new virtual machine wizard (**New → Virtual machine**).
5. As the virtual machine location, select the directory with the unpacked virtual harddisk. Assign RAM and virtual network adapters (read [Technical Specifications](#)).
6. Select **Use existing virtual harddisk**. Browse for the virtual harddisk unpacked from the distribution package.
7. After finishing the wizard, connect to the virtual appliance and start it.
8. Follow the instructions on the virtual appliance console to perform the basic configuration.
9. To perform the initial setup, open the following address in your web browser:
`https://kerio_control_ip_address:4081/admin`
10. Follow the Activation Wizard.

After finishing the wizard, Kerio Control displays the login page.

Installing virtual appliance for Parallels

For hardware requirements and supported Parallels hypervisors, read [Technical Specifications](#).

1. Download the zipped Parallels package from the [Download page](#) and unpack.
2. Open the virtual appliance in Parallels and start it.
3. Follow the instructions on the virtual appliance console to perform the basic configuration.
4. To perform the initial setup, open the following address in your web browser:
`https://kerio_control_ip_address:4081/admin`
5. Follow the Activation Wizard.

After finishing the wizard, Kerio Control displays the login page.

Setting Up Kerio Control Box

Kerio Control Box models

Kerio Control Box is a hardware appliance with an optimized operating system and Kerio Control pre-installed.

There are two Kerio Control Box models available:

1000 Series

A small desktop appliance featuring four Gigabit Ethernet ports.

3000 Series

A 1U rack-mount appliance featuring eight Gigabit Ethernet ports.

Connecting Kerio Control box to the network

For the initial setup, please connect Kerio Control Box according to the following schemes.

Kerio Control Box 1000 Series

Connect Ethernet port number 1 to the Internet (e.g. DSL or Cable modem) using an Ethernet cable.

Connect Ethernet port number 4 to the computer which will be used to configure the appliance.

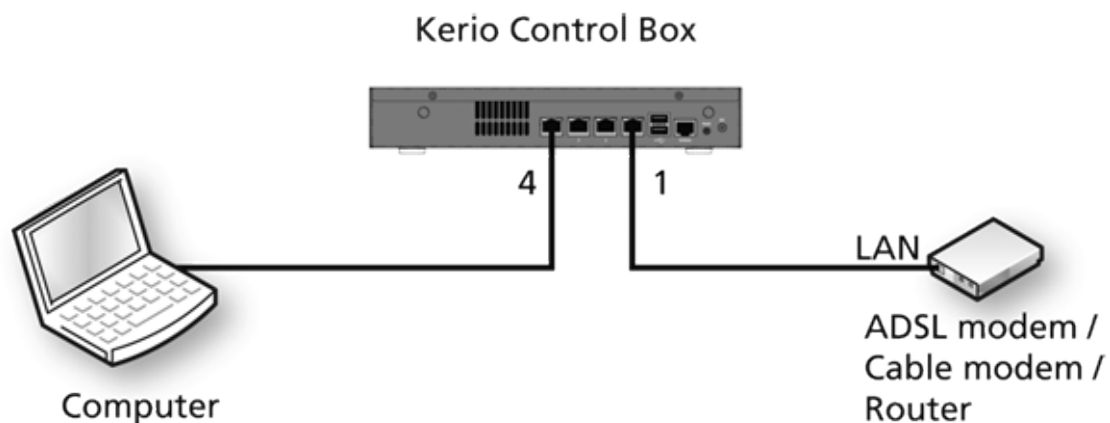


Figure 1 Kerio Control Box 1000 Series connection

Setting Up Kerio Control Box

Kerio Control Box 3000 Series

Connect Ethernet port number 1 to the Internet (e.g. DSL or Cable modem) using an Ethernet cable.

Connect Ethernet port number 8 to the computer which will be used to configure the appliance.

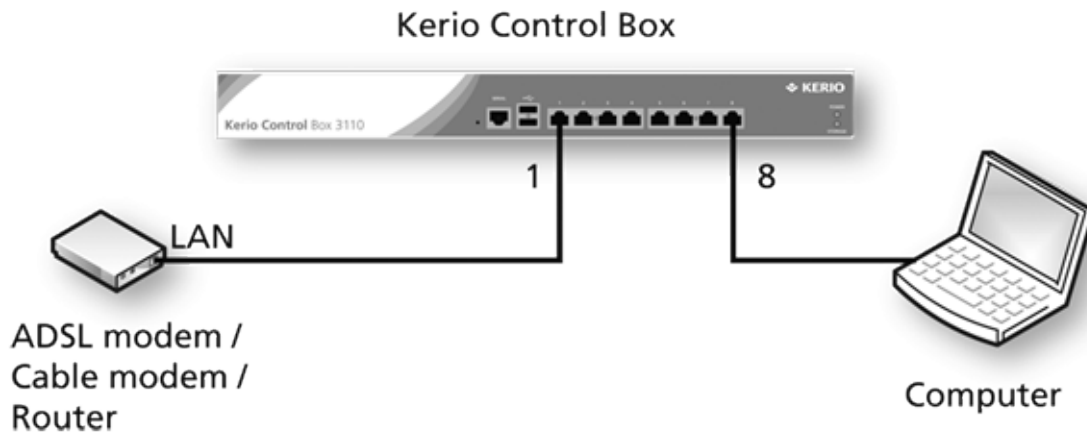


Figure 2 Kerio Control Box 1000 Series connection

Initial setup

Take the following steps to make Kerio Control Box running:

1. Make sure that the automatic TCP/IP configuration (using DHCP) is set on the appropriate network interface on your computer.
2. Turn on the appliance and make sure the power is on.
3. Make sure that your computer got the IP address of 10.10.10.11.
4. Open the web interface by entering the following address into your browser:
`https://10.10.10.1:4081/admin`
5. Ignore SSL certificate warnings and proceed to the configuration wizard.
6. Follow the instructions provided by the wizard until the login screen appears.
7. Login to continue with the appliance configuration.

Configuring the Activation Wizard

Configuring the Activation Wizard

The first logon to the administration interface after the installation automatically runs the product activation wizard:

Select a language

This language will be used by the activation wizard and it will also be set as a default language after the first logon to the administration interface. Once logged in, the language settings can be changed as needed.

Connect to the Internet



This step appears only if Kerio Control is not able to connect to the Internet.

Select an interface connected to the Internet. Configure the connection method (DHCP, static configuration or PPPoE) and specify the required parameters. This procedure can be reused until the Internet connection starts working.

It is also possible to select **offline registration** and [register Kerio Control later](#).

Set the time zone, date and time

Kerio Control requires correct configuration of the date, time and time zone.

Select your time zone and verify (and change, if necessary) date and time settings.

It is recommended to enable synchronization of time against a time server. NTP servers of *Kerio Technologies* are used for this purpose.

Activate Kerio Control

This step allows:

- registering a license number of the purchased product
- the 30-day trial version
- put the license.key file into Kerio Control
- to skip the registration and [register Kerio Control later](#)

Registration of a purchased license

For registration, you need your license number for the purchased product.

Configuring the Activation Wizard

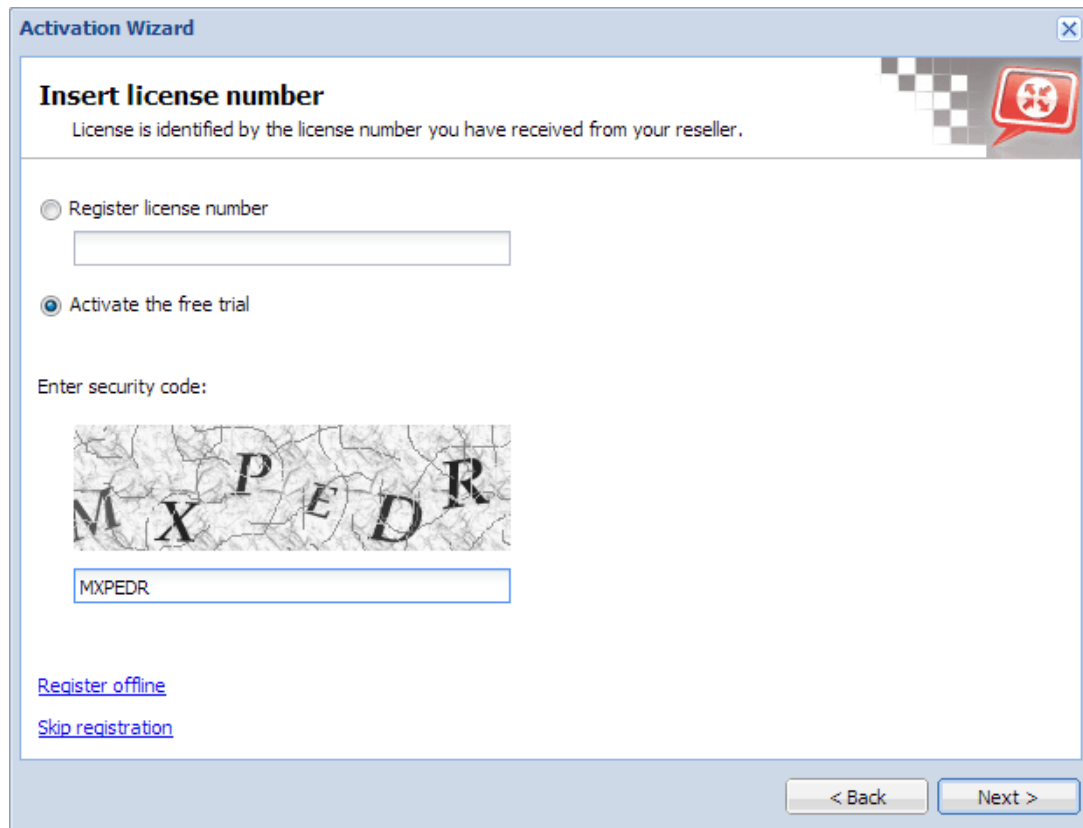


Figure 1 Activation Wizard — Insert license number

1. Select **Register license number**.
2. Insert the license number and enter the security code displayed in the picture.
3. On the next page, edit your registration details.

Upon a successful registration, the product will be activated with a valid license.

Registration of the trial version

Registration of the trial version allows testing of features unavailable in the unregistered trial version (the *Kerio Control Web Filter* module, updates of the integrated antivirus engine and the intrusion prevention system). The registration provides you with free technical support for the entire trial period.

1. Select **Activate the free trial**.
2. Enter the security code displayed in the picture.
3. On the next page, edit your registration details.



Registration of the trial version does not prolong the trial period.

Register offline

If you have a file with the license key (usually `license.key`), you can use link **Register offline** (see screenshot [1](#)).



You can have this file saved from your previous installation of Kerio Control.

If you do not have the license key file (or you changed operating systems), [register Kerio Control via WWW](#).

Help us make Kerio Control even better

Information on the product usage helps us develop Kerio Control as close to your needs as possible. By sending your usage statistics, you participate in the product improvement.

Statistics do not include any confidential data (passwords, email addresses, etc.) and their submission can be disabled any time under **Advanced Options** → **Updates**.

Set the password for the administrator user account

Enter the admin password — i.e. the password of the main administrator of the firewall. Username **Admin** with this password is then used for:

- Access to the remote administration of the firewall via the web administration interface
- Logon to the firewall's console.



Remember this password or save it in a secured location and keep it from anyone else!

After finishing the wizard, login page appears. Use the admin credentials for login and configure your Kerio Control.

Configuration Assistant

Configuration Assistant overview

The configuration assistant is used for an easy instant basic configuration of Kerio Control. By default, it is opened automatically upon logon to the administration interface. If this feature is disabled, you can start the wizard by clicking on **Configuration Assistant** on **Dashboard**.

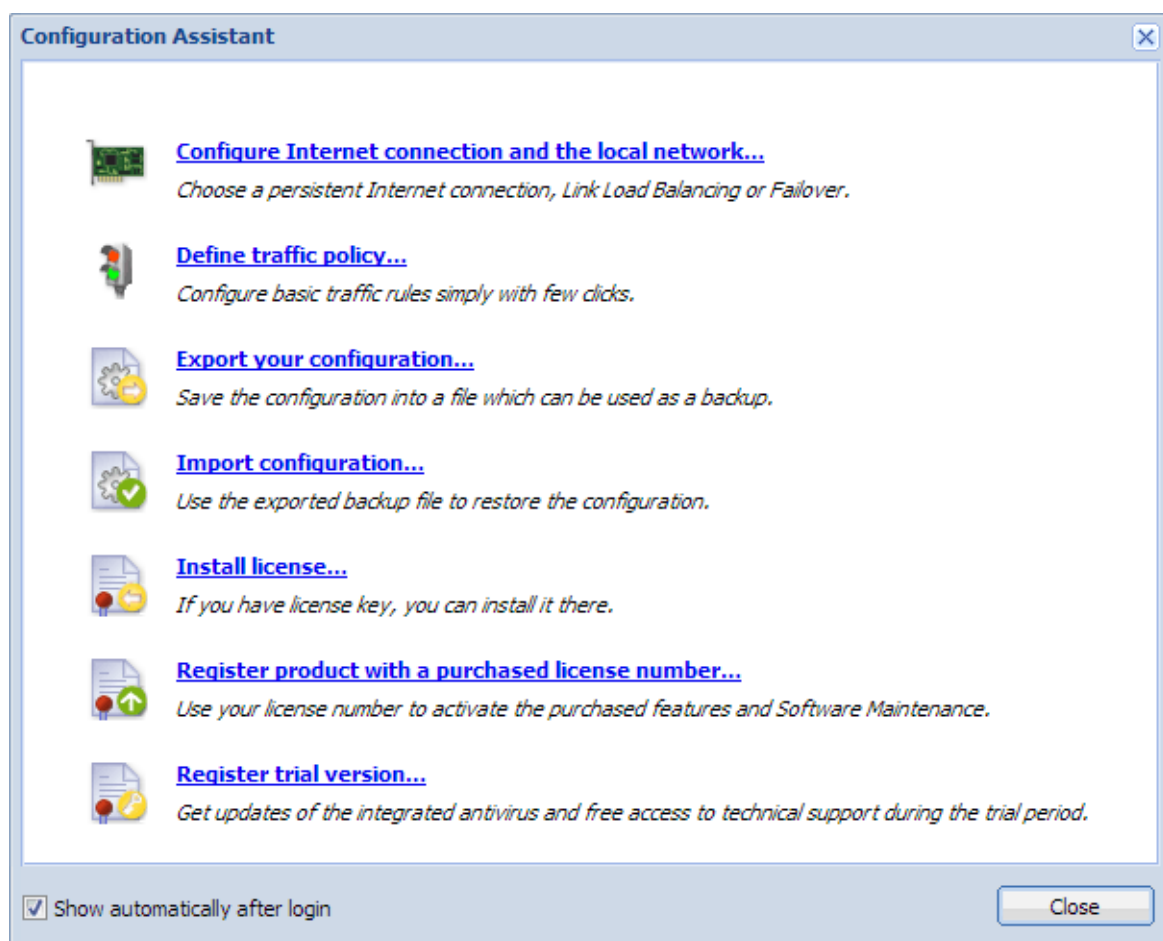


Figure 1 Configuration Assistant



It is not necessary to use the configuration assistant or its individual features. Experienced administrators can configure Kerio Control without these tools.

The configuration assistant allows the following settings:

Configure Internet connection and the local network

Once these parameters are configured, the Internet connection (IPv4) and access from local devices behind the firewall should work. The wizard automatically configures the DHCP server and the DNS forwarder modules.

Select your connectivity mode:

Single Internet Link

1. On the first page of the wizard, select **A Single Internet Link**.
2. Click **Next**.
3. Select a network interface (Internet link).
4. Select mode:
 - **Automatic** — the interface where Kerio Control detected the default gateway is used. Therefore, in most cases the appropriate adapter is already set within this step.
 - **Manual** — you can change configuration of the default gateway, DNS servers, IP address and subnet mask.



If the more IP addresses are set for the interface, the primary IP address will be displayed.

- **PPPoE** — enter the username and password from your Internet provider.
5. Click **Next**.
 6. Select interface connected to the local network.

If multiple interfaces are connected to the local network, select the interface you are currently using for connection to the Kerio Control administration.
 7. Click **Next**.
 8. Verify your configuration and click **Finish**.

You can check the result in section **Interfaces**. The **Internet Interfaces** group includes only the Internet interface selected in the second page of the wizard. The LAN adapter selected on the third page of the wizard is included in the group **Trusted/Local Interfaces**.

Other interfaces are added to the group **Other Interfaces**. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule).

Two Internet links with load balancing

If at least two Internet links are available, Kerio Control can divide traffic between both of them:

1. On the first page of the wizard, select **Two Internet links with load balancing**.
2. Click **Next**.
3. Select two interfaces to be used as Internet links with traffic load balance.

For each link it is necessary to specify link weight, i.e. its relative throughput. The weight of individual links indicates how Internet traffic is distributed among the links (it should correspond with their speed ratio).

Example

You have two Internet links with connection speed 4 Mbit/s and 8 Mbit/s. You set weight 4 for the first link and weight 8 for the other one. The total Internet connection load will therefore be divided in the proportion 1:2.

4. Select mode:
 - **Automatic** — the interface where Kerio Control detected the default gateway is used. Therefore, in most cases the appropriate adapter is already set within this step.
 - **Manual** — you can change configuration of the default gateway, DNS servers, IP address and subnet mask.



If the more IP addresses are set for the interface, the primary IP address will be displayed.

- **PPPoE** — enter the username and password from your Internet provider.
5. Click **Next**.
 6. Select the interface connected to the local network.

If multiple interfaces are connected to the local network, select the interface you are currently using for connection to the Kerio Control administration.
 7. Click **Next**.
 8. Verify your configuration and click **Finish**.


You can check the result in section **Interfaces**. The **Internet Interfaces** group includes the Internet links selected in the third page of the wizard.

Only the LAN adapter selected on the third page of the wizard is included in the group **Trusted/Local Interfaces**.

Other interfaces are added to the group **Other Interfaces**. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule).

Two Internet links with failover

Kerio Control allows guarantee Internet connection by an alternative (back-up) connection. This connection back-up is launched automatically whenever failure of the primary connection is detected. When Kerio Control finds out that the primary connection is recovered again, the secondary connection is disabled and the primary one is re-established automatically.

1. On the first page of the wizard, select **Two Internet links with failover**.
 2. Click **Next**.
 3. Select a network interface to be used for the primary connection and for the secondary connection.
 4. Select mode:
 - **Automatic** — the interface where Kerio Control detected the default gateway is used. Therefore, in most cases the appropriate adapter is already set within this step.
 - **Manual** — you can change configuration of the default gateway, DNS servers, IP address and subnet mask.
-  If the more IP addresses are set for the interface, the primary IP address will be displayed.
- **PPPoE** — enter the username and password from your Internet provider.

5. Click **Next**.
6. Select the interface connected to the local network. If multiple interfaces are connected to the local network, select the interface you are currently using for connection to the Kerio Control administration.
7. Click **Next**.
8. Verify your configuration and click **Finish**.

You can check the result in section **Interfaces**.

Only the LAN adapter selected on the third page of the wizard is included in the group **Trusted/Local Interfaces**.

Configuration Assistant

Other interfaces are considered as not used and added to the group *Other Interfaces*. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule).



When using failover, only two Internet Connections may be applied, one for the primary, and the other as a failover.

General notes

- A default gateway must not be set on any of the local interfaces.
- If the interface configuration does not correspond with the real network configuration, edit it (e.g. if the firewall uses multiple interfaces for the local network, move corresponding interfaces to the group **Trusted/Local Interfaces**).

Define traffic policy

The network rules wizard demands only the data that is essential for creating a basic set of traffic rules:

1. In the **Configuration Assistant** dialog, click **Define traffic policy**.
2. Enable the **Kerio Control Administration** and **VPN services**, if you want to establish VPN connections, or to remotely administer Kerio Control.
3. Click **Next**.
4. Select Kerio Control services to be available from the Internet:
 - **VPN Services** — connection to the [Kerio VPN server](#) or [IPsec VPN server](#). Enable these services if you want to create VPN tunnels and/or connect remotely to the local network by using [Kerio VPN Client](#) or IPsec VPN clients.
 - **Kerio Control Administration** — enables remote administration of Kerio Control. This option allows HTTPS traffic on port 4081 (port of the administration interface cannot be changed).
5. Click **Next**.
6. Make any other services on the firewall or servers in the local network available from the Internet (mapping).
7. Click **Add**.

In the Inbound policy dialog, you can configure the following parameters:

- **Service** — services can be chosen either from the list of defined services or it is possible to define another service by its protocol and port number.
- **Runs on** — firewall or IP address of the local server on which the service is running.

8. Save the settings in the **Inbound Policy** dialog.

9. Click **Finish**.

Export your configuration

Configuration is exported to a **.tgz** package (the tar archive compressed by gzip) which includes all the key Kerio Control configuration files. Optionally, it is possible to include SSL certificates in the package.



Exported configuration does not include Kerio Control license key.

Import configuration

To import configuration, simply browse for or enter the path to the corresponding file which includes the exported configuration (with the **.tgz** extension).

If network interfaces have been changed since the export took place (e.g. in case of exchange of a defective network adapter) or if the configuration is imported from another computer, Kerio Control will attempt to pair the imported network interfaces with the real interfaces on the machine. This pairing can be customized — you can match each network interface from the imported configuration with one interface of the firewall or leave it unpaired.

If network interfaces cannot be simply paired, it is desirable to check and possibly edit interface group settings and/or traffic rules after completion of the configuration import.

Install license / Register product with a purchased license number / Register trial version / Update registration info

See article [Licenses and registrations in Kerio Control](#).

Licenses and registrations

Deciding on a number of users (licenses)

Kerio Control is licensed as a server with the Admin account and 5 user accounts in the basic license. Users can be added in packages of five users.

User is defined as a person who is permitted to connect to Kerio Control. Each user can connect from up to five different devices represented by IP addresses, including VPN clients.

If any user tries to connect from more than five devices at a time, another user license is used for this purpose.

Current license usage is displayed in the administration interface on **Dashboard**.



Kerio Control does not limit number of defined user accounts. However, if the maximal number of currently authenticated users is reached, no other user can connect.

Licenses, optional components and Software Maintenance

Kerio Control has the following optional components:

- Sophos antivirus
- Kerio Control Web Filter module for web pages rating

These components are licensed individually.

Software Maintenance

Software Maintenance is a right to update the software. If Software Maintenance expires, it is still possible to keep using the existing version of the product, but it is no longer possible to update for versions released after the expiration date. Updates will be available again upon purchasing of Software Maintenance for a new period.

Registering Kerio Control in the administration interface

If you skip the registration in the [Activation Wizard](#), you can register the product from **Dashboard** in the administration interface (displayed after each login).

When installed, the product can be registered as trial or as a full version.

Registering the trial version

The trial version is intended to allow the customer to become familiar with the product's features and configuration. Once you register the trial version, you will be provided free Kerio Technologies technical support during the entire trial period (up to 30 days).


License 	
License Number	Unregistered trial version. Register...
Licensed users	Unlimited
Product expiration	2013-02-02
Software Maintenance expiration	Unlicensed
Active users / devices	0 / 0
Antivirus	Licensed
Kerio Control Web Filter	Unlicensed

Figure 1 Product Registration

The trial version can be registered by clicking on **Register** on the product's main page (see figure 1). In the dialog box just opened, set the following parameters:

1. enter security code (CAPTCHA) from the image.



The code is not case-sensitive.

2. enter information about your company and agree with the privacy policy terms.
3. choose how many computers you have in your company and how you learned of Kerio Control.

Now, a special identification code called Trial ID gets generated. This ID is later required for contacting technical support. After successful registration, Trial ID can be found in the license information in the administration interface.

Registering full version

If your trial version is registered, the license file will be automatically imported to your product within 24 hours from your purchase. The Trial ID you entered in your product upon registration will be activated as a standard license number.

If you haven't registered your trial version:

1. Open the administration interface.
2. Click **Configuration Assistant** on **Dashboard**.

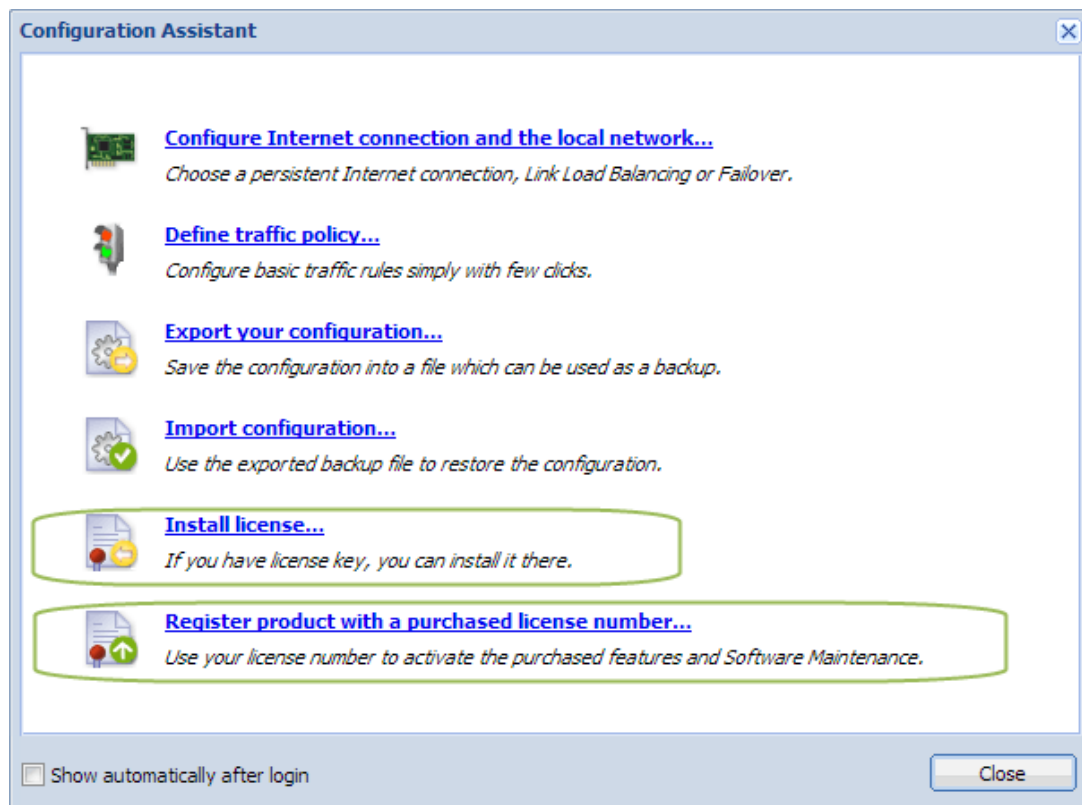


Figure 2 Configuration Assistant

3. Click **Register product with a purchased license number**.
4. In the first step of the registration, enter the license number and enter security code (CAPTCHA) from the image.



The code is not case-sensitive.

Click **Next** to make Kerio Control establish a connection to the registration server and check validity of the number entered. If the number is invalid, the registration cannot be completed.

5. Type the registration information about the company the product is registered to.
6. Kerio Control connects to the registration server, checks whether the data inserted is correct and downloads automatically the license file (digital certificate).
7. Click **Finish** to close the wizard.

Registering Kerio Control via WWW

If you purchased a license and your Kerio Control cannot access the Internet, follow these steps to register the product:

1. Go to <https://secure.kerio.com/reg/>
2. Register using your purchased license number.
3. By registering, you will download a license key (the `licence.key` file including the corresponding certificate) which must be [imported to Kerio Control](#).

Importing license key

1. Prepare the file with license.
2. Open the administration interface.
3. Click **Configuration Assistant** on **Dashboard** (see screenshot [2](#)).
4. Click **Install license**.

On Dashboard in the **License** section you can check that the license was installed successfully.

Connecting to Kerio Control

Web interfaces overview

Kerio Control includes a special web server which provides an interface where statistics can be viewed, as well as for firewall administration via web browser (the *Kerio Control Administration* interface) and for setting of some user account parameters. Access to the web interface is secured by SSL so that the network communication cannot be tapped and fragile data such as user password and other cannot be misused.

Use the following URL (server refers to the name or IP of the *Kerio Control* host, 4081 represents a web interface port) to open the firewall's web interface.

`https://server:4081/`

It is also possible to use the unsecured version of the administration web interface on port 4080:

`http://server:4080/`

By default, the unsecured web interface is available only on the firewall's local loopback address (localhost, typically 127.0.0.1). Connections to port 4080 from outside computers will be redirected to the secured web interface automatically (`https://server:4081/`). This behavior can be changed under **Configuration** → **Advanced options**, on the **Web Interface** tab.

Web interface ports cannot be changed.

This chapter addresses the web interface configuration in the *Kerio Control's* administration program. The web user interface is described thoroughly in the *Kerio Control — User's Guide*.

Web interface and certificate settings information

To configure *Kerio Control* web interface, go to the **Web Interface** folder in **Configuration** → **Advanced Options**.

In the upper section you can find links to unsecured versions of the firewall's web interface and the administration interface (*Kerio Control Administration*). Lower you can get information about the SSL certificate used for the secured version of the web interface and an option to change the certificate if desirable.

By disabling option *Force SSL secured connection* it is possible to allow access to the unsecured web interface (including the administration interface) from any computer. However, for security reasons, it is recommended to keep this option enabled and always use the secure web interface.

SSL Certificate for the Web Interface

The principle of an encrypted *Kerio Control* web interface is based on the fact that all communication between the client and server is encrypted to protect it from wiretapping and misuse of the transmitted data. The SSL protocol uses an asymmetric encryption first to facilitate exchange of the symmetric encryption key which will be later used to encrypt the transmitted data.

The asymmetric cipher uses two keys: a public one for encrypting and a private one for decrypting. As their names suggest, the public (encrypting) key is available to anyone wishing to establish a connection with the server, whereas the private (decrypting) key is available only to the server and must remain secret. The client, however, also needs to be able to identify the server (to find out if it is truly the server and not an impostor). That is what a certificate is for. A certificate contains a public server key, the name of the server, validity period and other data. To ensure the authenticity of the certificate it must be certified and signed by a third party, the certification authority.

Communication between the client and server then follows this scheme: The client generates a symmetric encryption key for and encrypts it with the public server key (obtained from the server certificate). The server decrypts it with its private key (kept solely by the server). Thus the symmetric key is known only to the server and client. This key is then used for encryption and decipher any other traffic.

Generate or Import Certificate

During *Kerio Control* installation, a testing certificate for the SSL-secured Web interface is created automatically (it is stored in the `sslcert` subdirectory under the *Kerio Control's* installation directory, in the `server.crt` file; the private key for the certificate is saved as `server.key`). The certificate created is unique. However, it is issued against a non-existing server name and it is not issued by a trustworthy certificate authority. This certificate is intended to ensure functionality of the secured Web interface (usually for testing purposes) until a new certificate is created or a certificate issued by a public certificate authority is imported.

Click on the **Change SSL certificate** (in the dialog for advanced settings for the Web interface) to view the dialog with the current server certificate. By selecting the **Field** (certificate entry) option you can view information either about the certificate issuer or about the subject represented by your server.

You can obtain your own certificate, which verifies your server's identity, by two means.

You can create your own self-signed certificate. Click **Generate Certificate** in the dialog where current server status is displayed. Insert required data about the server and your company into the dialog entries. Only entries marked with an asterisk (*) are required.

Click on the **OK** button to view the **Server SSL certificate** dialog. The certificate will be started automatically (you will not need to restart your operating system). When created, the certificate is saved as `server.crt` and the corresponding private key as `server.key`.

Connecting to Kerio Control

A new (*self-signed*) certificate is unique. It is created by your company, addressed to your company and based on the name of your server. Unlike the testing version of the certificate, this certificate ensures your clients security, as it is unique and the identity of your server is guaranteed by it. Clients will be warned only about the fact that the certificate was not issued by a trustworthy certification authority. However, they can install the certificate in the browser without worrying since they are aware of who and why created the certificate. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

Another option is to purchase a full certificate from a public certification authority (e.g. *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode*, etc.).

To import a certificate, open the certificate file (*.crt) and the file including the corresponding private key (*.key). These files are stored in `sslcert` under the *Kerio Control's* installation directory.

The process of certification is quite complex and requires a certain expertise. For detailed instructions contact Kerio technical support.

User authentication at the web interface

User authentication is required for access to the *Kerio Control's* web interface. Any user with their own account in *Kerio Control* can authenticate to the web interface. Depending on the statistics settings, either user's statistics are opened or a page with status information and personal preferences is displayed upon login.

If more than one domain are used, the following rules apply to the user name:

- *Local user account* — the name must be specified without the domain (e.g. `admin`),
- *Primary domain* — missing domain is acceptable in the name specification (e.g. `jsmith`), but it is also possible to include the domain (e.g. `jsmith@company.com`),
- *Other domains* — the name specified must include the domain (e.g. `drdolittle@usoffice.company.com`).

If none or just one domain is mapped, all users can authenticate by their usernames without the domain specified.



Authentication at the web interface is a basic user authentication method at the firewall.

Configuring network interfaces

Interfaces overview

Kerio Control represents a gateway between two or more networks (typically between the local network and the Internet) and controls traffic passing through network adapters which are connected to these networks.

In Kerio Control, you can define the following groups of interfaces:

- **Internet Interfaces** — interfaces which can be used for Internet connection,
- **Trusted / Local Interfaces** — interfaces connected to local private networks protected by the firewall,
- **VPN interfaces** — virtual network interfaces (Kerio VPN, IPsec VPN),
- **Other interfaces** — interfaces which do not belong to any of the groups listed above (i.e. dial-like links).

Configuring interfaces

A configuration wizard is available for the setup of basic interface parameters:

1. In the administration interface, go to **Interfaces**.
2. Click **More Actions** → **Configure in Wizard**.
3. Read article [Configuration Assistant](#).

During the initial firewall configuration by the wizard, interfaces will be arranged into groups automatically. [This classification can be changed later](#).

Moving an interface to another group

To move an interface to another group, drag it by mouse to the desired destination group, or select the group in the properties of the particular interface — see below.

Configuring Internet connectivity

For networks using IPv4, it is possible to use one or more Internet connections.

1. In the administration interface, go to **Interfaces**.
2. Select one of the following options:

Configuring network interfaces

- **A Single Internet Link** — the most common connection of local networks to the Internet. In this case, only one Internet connection is available and it is used persistently. It is also possible to use dial-like links which can be connected persistently — typically PPPoE connections.



Only a single link connection is for IPv6.

- **Multiple Internet Links - Failover** — if the primary link fails, Kerio Control switches to the secondary link automatically. When the connection on the primary link is recovered, Kerio Control automatically switches back to it.
- **Multiple Internet Links - Load Balancing** — Kerio Control can use multiple links concurrently and spread data transferred between the LAN and the Internet among these links. In standard conditions and settings, this also works as connection failover — if any of the links fails, transferred data are spread among the other links.

3. Click **Apply**.

Adding new interfaces

You can add an interface for a new type of tunnel:

- PPTP — use when your DSL provider requires this type of protocol.
- PPPoE — use when your DSL provider requires this type of protocol.
- VPN

Configuring PPPoE mode in the Internet interface

Configuring PPPoE mode in the Internet interface is recommended if you use a single Internet link. The advantage is using only one interface.

You need the following information from your provider:

- username
- password

1. In the administration interface, go to **Interfaces**.
2. Double-click on the Internet interface.
3. Select PPPoE mode.

4. In the **PPPoE Interface Properties** dialog, type a new interface name.
5. Type the username and password.
6. Save the settings.

Configuring PPPoE tunnel

If this connection is used as a single Internet link, it is recommended to define [PPPoE connection in the Ethernet interface](#).

If you need to create another interface to the Internet, use these instructions:

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **PPPoE**.
3. In the **PPPoE Interface Properties** dialog, type a new interface name.
4. The **Interface Group** leave as it is.
You can change it later.
5. On tab **Dialing Settings**, select the interface.



If you set the interface to **Any**, Kerio Control will automatically select the appropriate interface which will be used for connection.

6. Type the username and password from your provider.
7. Set time intervals in which the connection should be established persistently and when it should be disconnected.

Out of these intervals, the link will demand manual dialing. The link can be hung up automatically after defined period of idleness.

Configuring PPTP tunnel

You need the following information from your provider:

- PPTP server hostname
- username and password for PPTP server access

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **PPTP**.

Configuring network interfaces

3. In the **PPTP Interface Properties** dialog, type a new interface name.
4. The **Interface Group** leave as it is.
You can change it later.
5. On tab **Dialing Settings**, type the PPTP server hostname, username and password.
6. Set time intervals in which the connection should be established persistently and when it should be disconnected.
Out of these intervals, the link will demand manual dialing. The link can be hung up automatically after defined period of idleness.
7. Save the settings.

VPN tunnel

Read more in special articles [Configuring Kerio VPN tunnel](#) and [Configuring IPsec VPN tunnel](#).

Configuring Ethernet ports

Box Edition

Kerio Control Box contains Gigabit Ethernet ports. Individual ports can be set as:

- Standalone interface
- Switch for LAN
- Not assigned — the port will be inactive.

It is also possible to use a virtual network (VLAN).

1. In the administration interface, go to **Interfaces**.
2. Click **Manage Ports**.
3. In the **Manage Ports** dialog, double-click **Port Name**.
4. In the **Configure Port** dialog, you can set a port as:
 - **Standalone interface** — the port will be used as a standalone Ethernet interface.
 - **Switch for LAN** — port will be a part of the switch which, in Kerio Control, behaves as one Ethernet interface.
 - **Not assigned** — the port will be inactive. This can be used for example for temporary disconnection of the computer of a network segment connected to the port.

5. **Speed and duplex** leave as it is.
6. On Ethernet interfaces, you can [create one or more tagged virtual networks \(VLAN\)](#).
7. Save the settings.

Appliance Editions

Appliance editions can set speed and duplex mode for Ethernet interfaces and create virtual networks (VLAN) on these interfaces:

1. In the administration interface, go to **Interfaces**.
2. Click **Manage Ports**.
3. In the **Manage Ports** dialog, double-click **Port Name**.
4. Set **Speed and duplex**.

In most cases, interconnected devices agree on speed and communication mode automatically.

5. On Ethernet interfaces, you can [create one or more tagged virtual networks \(VLAN\)](#).
6. Save the settings.

Physical interfaces (ports) cannot be added to the LAN switch. This functionality is available only in the box edition.

Configuring VLANs

VLAN support in Kerio Control

VLANs (Virtual LANs) are virtual networks created on a single physical Ethernet interface (trunk interface).

Kerio Control supports 802.1Q VLANs. You can create up to 4094 VLANs on each Ethernet interface.

Each VLAN works as a standalone interface. The physical Ethernet interface works the standard way (as an untagged VLAN).

Creating VLAN interfaces

To define new VLANs:

1. Go to section **Configuration** → **Interfaces**.
2. Double-click the Ethernet interface.
3. Open the **VLAN** tab.
4. Click **Add or Remove VLANs...**
5. Check **Create VLAN subinterfaces**.
6. Enter VLAN IDs separated by semicolons. VLAN ID is a number between 1 and 4094.
Kerio Control creates a new network interface for each VLAN. The new interfaces are added in the **Other Interfaces** group.
7. You can move VLANs to other interface groups.
8. Double-click a VLAN interface to [set the IPv4 and/or IPv6 parameters](#).

Now you can use the VLAN interface in traffic rules.

Removing VLAN interfaces

To remove a VLAN, remove the VLAN ID from the trunk interface:

1. Go to section **Configuration** → **Interfaces** section.
2. Double-click the Ethernet interface.

3. Open the **VLAN** tab.
4. Click **Add or Remove VLANs...**
5. Delete the VLAN ID from the list.

To remove all VLANs, uncheck the **Create VLAN subinterfaces** option.

The VLAN interface is removed from the **Interfaces** section and from all traffic rules.

Configuring Kerio VPN server

VPN overview

Kerio Control supports VPN (Virtual Private Network). Kerio Control includes a proprietary implementation of VPN, called Kerio VPN. Kerio VPN can be used for:

- Kerio VPN server for connecting clients (desktops, notebooks, mobile devices etc...)
- [Kerio VPN tunnel](#) for connecting LANs

This article describes using Kerio VPN server.

Configuring Kerio VPN Server

Firstly you must enable communication through VPN in **Traffic Rules**. Then:

1. In the administration interface, go to **Interfaces**.
2. Double-click on **VPN Server**.
3. In the **VPN Server Properties** dialog, check **Enable Kerio VPN Server**.
4. On tab **Kerio VPN**, select [a valid certificate](#).
5. The port 4090 (both TCP and UDP protocols are used) is set as default.



Do not switch to another port without a proper reason.

If it is not possible to run the VPN server at the specified port (the port is used by another service), the error will be reported in the **Error** log.

6. To specify a VPN route manually, read section [Configuring routing](#).
7. Save the settings.

Configuring routing

By default, routes to all local subnets at the VPN server's side are defined. Other networks to which a VPN route will be set for the client can be specified:

1. In the administration interface, go to **Interfaces**.
2. Double-click the **VPN Server**.

3. On tab **Kerio VPN**, click **Custom Routes**.
4. Click **Add**.
5. In the **Add Route** dialog, define a network, mask and description.
In case of any collisions, custom routes are used instead.
6. Save the settings.

TIP

Use the 255.255.255.255 network mask to define a route to a certain host. This can be helpful for example when a route to a host in the demilitarized zone at the VPN server's side is being added.

Configuring Kerio VPN clients

The following conditions must be met to enable connection of remote clients to local networks:

- [Kerio VPN Client must be installed at remote clients](#).
- In the **Users and Groups** → **Users** section, check a right **Users can connect using VPN** for your users.
- Connection to the VPN server from the Internet as well as communication between VPN clients must be allowed by traffic rules.

There is a default traffic policy rule which should be enabled. Otherwise there is a ddefined service for Kerio VPN (TCP/UDP 4090) in case you do not have this rule.

Hint:

VPN clients correctly connected to the firewall can be overviewed in the administration interface, section **Status** → **VPN clients**.

Configuring Kerio VPN tunnel

Kerio VPN overview

Kerio Control supports VPN (Virtual Private Network). Kerio Control includes a proprietary implementation of VPN, called Kerio VPN. Kerio VPN can be used for:

- Kerio VPN tunnel for connecting LANs
- [Kerio VPN server](#) for connecting clients (desktops, notebooks, mobile devices etc...)

This article describes using Kerio VPN tunnel.

Prerequisites

- Enable VPN tunnel in **Traffic Rules**
- Set the DNS settings for using the DNS names in the remote network

DNS must be set properly at both endpoints. One method is to add DNS records of the hosts (to the hosts file) at each endpoint. If the DNS module in Kerio Control is used as the DNS server at both ends of the tunnel, DNS queries can be forwarded to hostnames in the corresponding domain of the DNS module at the other end of the tunnel. DNS domain (or subdomain) must be used at both sides of the tunnel.

Configuring Kerio VPN tunnel

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **VPN Tunnel**.
3. Type a name of the new tunnel.

Each VPN tunnel must have a unique name. This name will be used in the table of interfaces, in traffic rules and interface statistics.

4. Set the tunnel as: active (and type the hostname of the remote endpoint) or passive.
 - active — type the remote VPN server. If the remote VPN server does not use the port 4090, a corresponding port number must be specified (e.g. `server.company.com:4100`).
 - passive — the passive mode is only useful when the local end of the tunnel has a fixed IP address and when it is allowed to accept incoming connections.

5. Select **Type**: Kerio VPN.
6. On tab **Authentication**, specify the fingerprint for the remote VPN server certificate and vice versa — specify the fingerprint of the local server in the configuration at the remote server.



If the local endpoint is in the active mode, the certificate of the remote endpoint and its fingerprint can be downloaded by clicking **Detect remote certificate**.

7. Save the settings.

Configuring routing

By default, routes to all local subnets at the VPN server's side are defined. Other networks to which a VPN route will be set for the client can be specified:

1. In the administration interface, go to **Interfaces**.
2. Double-click the VPN tunnel.
3. On tab **Routing** check **Use custom routes**.

In this case is also enabled **Use routes provided automatically by the remote endpoint**. In case of any collisions, custom routes are used instead. This option easily solves the problem where a remote endpoint provides one or more invalid route(s).

4. Click **Add**.
5. In the **Add Route** dialog, define a network, mask and description.
6. Save the settings.

Example of Kerio VPN configuration: company with a filial office

Overview

This article provides an exemplary description on how to create an encrypted tunnel connecting two private networks using the Kerio VPN.

This example can be customized. The method described can be used in cases where no redundant routes arise by creating VPN tunnels (i.e. multiple routes between individual private networks).

Specification

Supposing a company has its headquarters in New York and a branch office in London. We intend to interconnect local networks of the headquarters by a VPN tunnel using the Kerio VPN. VPN clients will be allowed to connect to the headquarters network.

The server (default gateway) of the headquarters uses the public IP address 85.17.210.230 (DNS name is `newyork.company.com`), the server of the branch office uses adynamic IP address assigned by DHCP.

The local network of the headquarters consists of two subnets, LAN 1 and LAN 2. The headquarters uses the `company.com` DNS domain.

The network of the branch office consists of one subnet only (LAN). The branch office `filial.company.com`.

Figure [1](#) provides a scheme of the entire system, including IP addresses and the VPN tunnels that will be built.

Suppose that both networks are already deployed and set according to the figure and that the Internet connection is available.

Traffic between the network of the headquarters, the network of the branch office and VPN clients will be restricted according to the following rules:

1. VPN clients can connect to the LAN 1 and to the network of the branch office.
2. Connection to VPN clients is disabled for all networks.
3. Only the LAN 1 network is available from the branch office. In addition to this, only the WWW, FTP and Microsoft SQL services are available.

4. No restrictions are applied for connections from the headquarters to the branch office network.
5. LAN 2 is not available to the branch office network nor to VPN clients.

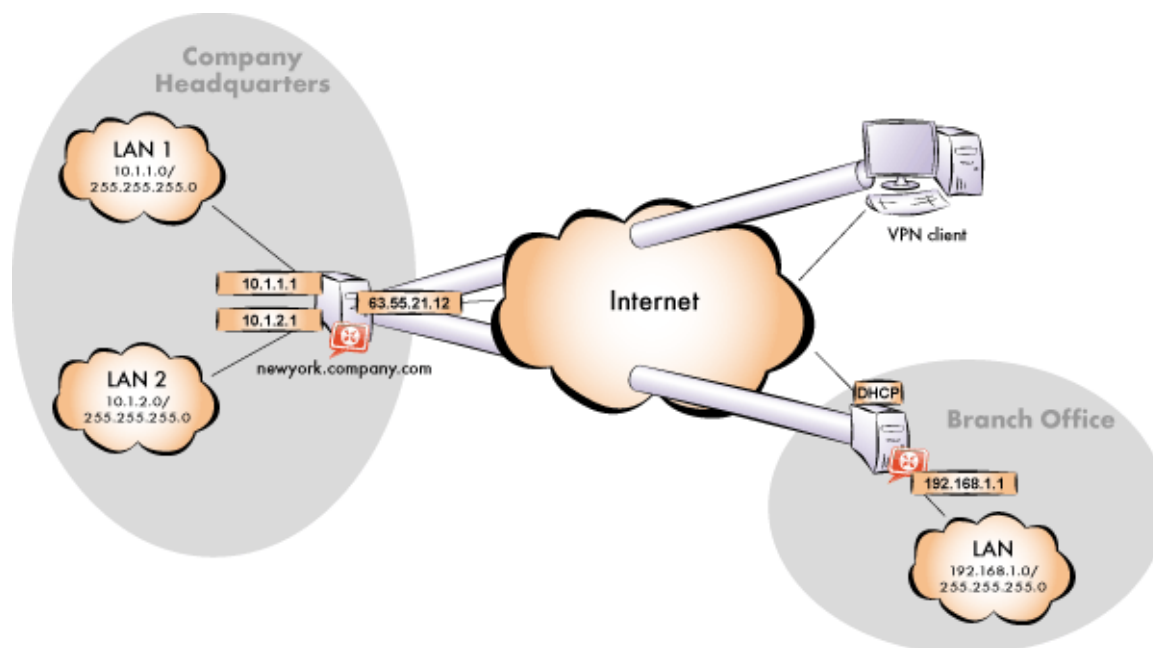


Figure 1 Example — interconnection of the headquarter and a filial office by VPN tunnel (connection of VPN clients is possible)

Common method

The following actions must be taken in both local networks (i.e. in the main office and the filial):

1. Kerio Control must be installed on the default gateway of the network.
For every installation of Kerio Control, a stand-alone license for the corresponding number of users is required!
2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the Kerio Control host's IP address as the default gateway and as the primary DNS server.
3. In configuration of the DNS module set DNS forwarding rules for the domain in the remote network. This enables to access hosts in the remote network by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hosts table (if they use IP addresses) or enable cooperation of the DNS

Example of Kerio VPN configuration: company with a filial office

module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts).

4. In the **Interfaces** section, allow the VPN server.
5. Check whether the automatically selected VPN subnet does not collide with any local subnet either in the headquarters or in the filial and select another free subnet if necessary.
6. Define the VPN tunnel to the remote network. The passive endpoint of the tunnel must be created at a server with fixed public IP address (i.e. at the headquarter's server). Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the **Error** log, check fingerprints of the certificates and also availability of the remote server.

7. In traffic rules, allow traffic between the local network, remote network and VPN clients and set desirable access restrictions. In this network configuration, all desirable restrictions can be set at the headquarter's server. Therefore, only traffic between the local network and the VPN tunnel will be enabled at the filial's server.
8. Test reachability of remote hosts from each local network. To perform the test, use the `ping` and `tracert` (`tracert`) system commands. Test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (**Unknown host**) when a corresponding DNS name is tested, then check configuration of the DNS.

The following sections provide detailed description of the Kerio VPN configuration both for the headquarter and the filial offices.

Headquarters configuration

1. On the default gateway of the headquarters (referred as "server" in further text) install Kerio Control.
2. Perform basic configuration of Kerio Control by using the connectivity wizard and the traffic policy wizard.

In the traffic policy wizard, allow access to the Kerio VPN server service. This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Kerio VPN Server	Any	Firewall	Kerio	Allow
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	Allow

Figure 2 Headquarter — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

- In the Kerio Control's DNS module configuration, enable DNS forwarder (forwarding of DNS requests to other servers).
- Enable the **Use custom forwarding** option and define rules for names in the `filial.company.com` domain. Specify the server for DNS forwarding by the IP address of the internal interface of the Kerio Control host (i.e. interface connected to the local network at the other end of the tunnel).

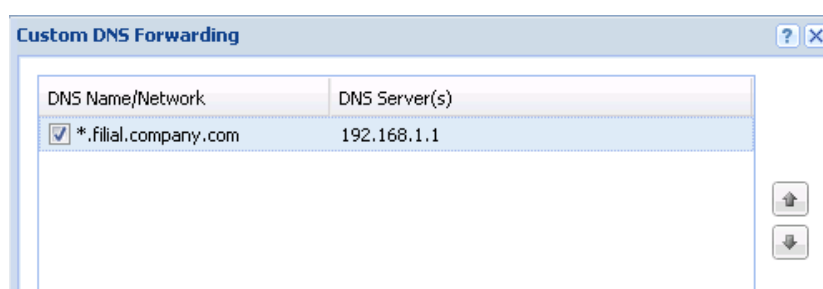


Figure 3 Headquarter — DNS forwarding settings

- No DNS server will be set on interfaces of the Kerio Control host connected to the local networks LAN 1 and LAN 2.
- On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (10.1.1.1 or 10.1.2.1). Hosts in the local network can be configured automatically by DHCP protocol.



For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hosts table (if they use IP addresses) or enable cooperation of the DNS module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts).

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

Example of Kerio VPN configuration: company with a filial office



The **VPN network** and **Mask** entries now include an automatically selected free subnet.

5. Create a passive end of the VPN tunnel (the server of the branch office uses a dynamic IP address). Specify the remote endpoint's fingerprint by the fingerprint of the certificate of the branch office VPN server.

VPN Tunnel Properties

General

Name: Tunnel to branch office

☒ Enable this tunnel

☐ Active - it connects to the remote endpoint

Remote endpoint hostname or IP address:

☐ Passive - it only accepts incoming connections

Type: IPsec Kerio VPN

Authentication Routing

Local endpoint's SSL certificate fingerprint: 74:07:9b:6e:cb:1e:ad:94:a5:2e:7b:99:2b:fa:9f:86

Remote endpoint's SSL certificate fingerprint: e1:8f:89:7c:e1:8f:89:7c:e1:8f:89:7c:e1:8f:89:1f

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Detect remote certificate...

OK Cancel

Figure 4 Headquarter — definition of VPN tunnel for a filial office

6. Customize traffic rules according to the restriction requirements.
 - In the **Local Traffic** rule, remove all items except those belonging to the local network of the company headquarters, i.e. except the firewall and the group of interfaces **Trusted/ Local interfaces**.
 - Define (add) the **VPN clients** rule which will allow VPN clients to connect to *LAN 1* and to the network of the branch office (via the VPN tunnel).
 - Create the **Branch office** rule which will allow connections to services in *LAN 1*.
 - Add the **Company headquarters** rule allowing connections from the local network to the branch office network.



















Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Kerio VPN Server	Any	 Firewall	 Kerio VPN	 Allow
<input checked="" type="checkbox"/> Local traffic	 Firewall  Trusted/Local interfaces	 Firewall  Trusted/Local interfaces	Any	 Allow
<input checked="" type="checkbox"/> VPN Clients	 VPN clients	 LAN 1  Tunnel to branch office	Any	 Allow
<input checked="" type="checkbox"/> Branch office	 Tunnel to branch office	 LAN 1	Any	 Allow
<input checked="" type="checkbox"/> Company headquarters	 Trusted/Local interfaces	 Tunnel to branch office	Any	 Allow

Figure 5 Headquarter — final traffic rules

Rules defined this way meet all the restriction requirements. Traffic which will not match any of these rules will be blocked by the default rule.

VPN test

Configuration of the VPN tunnel has been completed by now. At this point, it is recommended to test availability of the remote hosts from each end of the tunnel (from both local networks). For example, the `ping` or/and `tracert` (`tracert`) operating system commands can be used for this testing. It is recommended to test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (**Unknown host**) when a corresponding DNS name is tested, then check configuration of the DNS.

Example of Kerio VPN configuration: company with two filial offices

Overview

This article provides a complex VPN scenario where redundant routes arise between interconnected private networks (i.e. multiple routes exist between two networks that can be used for transfer of packets).

The only difference of Kerio VPN configuration between this type and VPN with no redundant routes is setting of routing between endpoints of individual tunnels. In such a case, it is necessary to set routing between individual endpoints of VPN tunnels by hand. Automatic route exchange is inconvenient since Kerio VPN uses no routing protocol and the route exchange is based on comparison of routing tables at individual endpoints of the VPN tunnel.

For better reference, the configuration is here described by an example of a company with a headquarters and two filial offices with their local private network interconnected by VPN tunnels.

Specification

The network follows the pattern shown in figure [1](#).

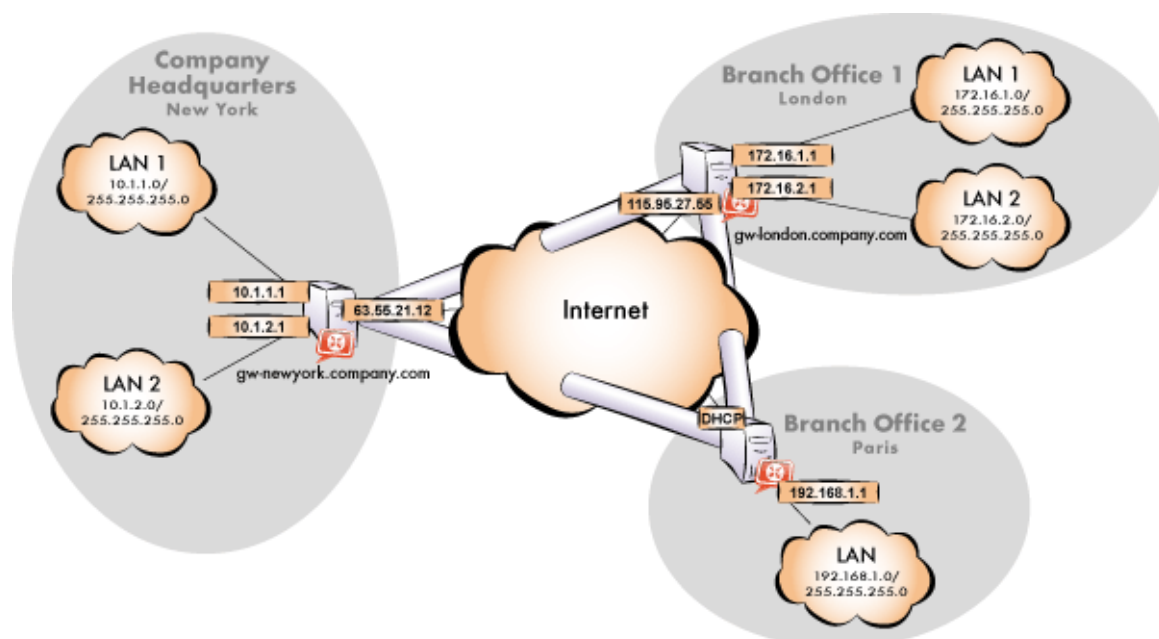


Figure 1 Example of a VPN configuration — a company with two filials

The server (default gateway) uses the fixed IP address 85.17.210.230 (DNS name is gw-newyork.company.com). The server of one filial uses the IP address 195.39.22.12 (DNS name gw-london.company.com), the other filial's server uses a dynamic IP address assigned by the ISP.

The headquarters uses the DNS domain company.com, filials use subdomains santaclara.company.com and newyork.company.com.

Common method

The following actions must be taken in all local networks:

1. Kerio Control must be installed on the default gateway of the network.



For every installation of Kerio Control, a stand-alone license for the corresponding number of users is required.

2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the Kerio Control host's IP address as the default gateway and as the primary DNS server.
3. In configuration of the DNS module, set DNS forwarding rules for domains of the other filials. This enables to access hosts in the remote networks by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

For proper functionality of the DNS, at least one DNS server must be specified to which DNS queries for other domains (typically the DNS server of the ISP).



The DNS database must include records of hosts in the corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hosts table (if they use IP addresses) and/or enable cooperation of the DNS module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts).

4. In the **Interfaces** section, allow the VPN server.

Check whether the automatically selected VPN subnet does not collide with any local subnet in any filial and select another free subnet if necessary.

Reserve three free subnets in advance that can later be assigned to individual VPN servers.

5. Define the VPN tunnel to one of the remote networks. The passive endpoint of the tunnel must be created at a server with fixed public IP address. Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

Example of Kerio VPN configuration: company with two filial offices

Set routing (define custom routes) for the tunnel. Select the **Use custom routes only** option and specify all subnets of the remote network in the custom routes list.

If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the **Error** log, check fingerprints of the certificates and also availability of the remote server.

6. Follow the same method to define a tunnel and set routing to the other remote network.
7. Allow traffic between the local and the remote networks. To allow any traffic, just add the created VPN tunnels to the **Source** and **Destination** items in the **Local traffic** rule.
8. Test reachability of remote hosts in both remote networks. To perform the test, use the **ping** and **tracert** (**tracert**) system commands. Test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (**Unknown host**) when a corresponding DNS name is tested, then check configuration of the DNS.

The following sections provide detailed description of the Kerio VPN configuration both for the headquarter and the filial offices.

Headquarters configuration

1. Kerio Control must be installed on the default gateway of the headquarter's network.
2. In Kerio Control set basic traffic rules by using the connectivity wizard and the traffic policy wizard.

In the traffic policy wizard, allow access to the Kerio VPN server service.

This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Kerio VPN Server	Any	Firewall	Kerio	Allow
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	Allow

Figure 2 Headquarter — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

- In the Kerio Control's DNS module configuration, enable DNS forwarder (forwarding of DNS requests to other servers).
- Enable the **Use custom forwarding** option and define rules for names in the `filial1.company.com` and `filial2.company.com` domains. To specify the forwarding DNS server, always use the IP address of the Kerio Control host's inbound interface connected to the local network at the remote side of the tunnel.

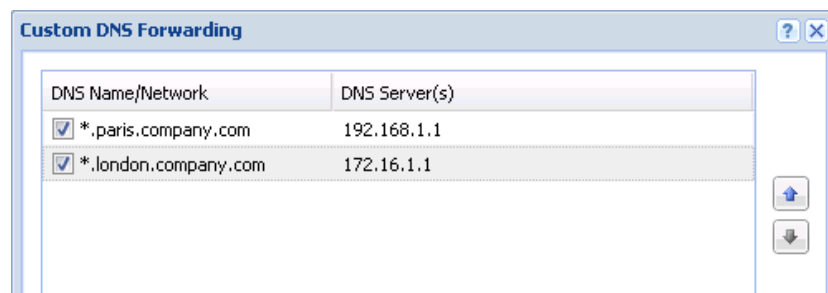


Figure 3 Headquarter — DNS forwarding settings

- No DNS server will be set on interfaces of the Kerio Control host connected to the local networks *LAN 1* and *LAN 2*.
 - On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (10.1.1.1 or 10.1.2.1). Hosts in the local network can be configured automatically by DHCP protocol.
4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).



The **VPN network** and **Mask** entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

5. Create a passive endpoint of the VPN tunnel connected to the London filial. Use the fingerprint of the VPN server of the London filial office as a specification of the fingerprint of the remote SSL certificate.

Example of Kerio VPN configuration: company with two filial offices

On the **Advanced** tab, select the **Use custom routes only** option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *London* filial).

The screenshot shows the 'Routing' tab in the Kerio VPN configuration. The 'Use custom routes' checkbox is checked. Below it is a table with the following data:

Network	Mask	Description
172.16.1.0	255.255.255.0	London - LAN1
172.16.2.0	255.255.255.0	London - LAN 2

Figure 4 The headquarters — routing configuration for the tunnel connected to the London filial



In case that the VPN configuration described here is applied (see figure 1), it is unrecommended to use automatically provided routes! In case of an automatic exchange of routes, the routing within the VPN is not be ideal (for example, any traffic between the headquarters and the Paris filial office is routed via the London filial whereas the tunnel between the headquarters and the Paris office stays waste).

6. Use the same method to create a passive endpoint for the tunnel connected to the *Paris* filial.

On the **Advanced** tab, select the **Use custom routes only** option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *Paris* filial).

The screenshot shows the 'Routing' tab in the Kerio VPN configuration. The 'Use custom routes' checkbox is checked. Below it is a table with the following data:

Network	Mask	Description
192.168.1.0	255.255.255.0	Paris - LAN

Figure 5 The headquarters — routing configuration for the tunnel connected to the Paris filial

Configuration of the London filial

1. Kerio Control must be installed on the default gateway of the filial's network.
2. In Kerio Control set basic traffic rules by using the connectivity wizard and the traffic policy wizard.

In the traffic policy wizard, allow access to the Kerio VPN server service.

This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Kerio VPN Server	Any	Firewall	Kerio	Allow
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	Allow

Figure 6 The London filial office — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

- In the *Kerio Control's* DNS module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).
- Enable the **Use custom forwarding** option and define rules for names in the *company.com* and *filial2.company.com* domains. To specify the forwarding DNS server, always use the IP address of the Kerio Control host's inbound interface connected to the local network at the remote side of the tunnel.

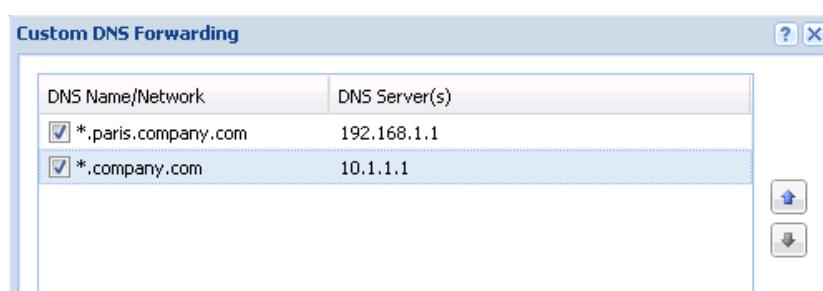


Figure 7 The London filial office — DNS forwarding settings

- No DNS server will be set on interfaces of the Kerio Control host connected to the local networks *LAN 1* and *LAN 2*.
 - On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (172.16.1.1 or 172.16.2.1). Hosts in the local network can be configured automatically by DHCP protocol.
4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).



The **VPN network** and **Mask** entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

Example of Kerio VPN configuration: company with two filial offices

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (newyork.company.com). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

VPN Tunnel Properties

General

Name:

☒ Enable this tunnel

☒ Active - it connects to the remote endpoint ⓘ

Remote endpoint hostname or IP address:

☐ Passive - it only accepts incoming connections ⓘ

Type:

Authentication **Routing**

Local endpoint's SSL certificate fingerprint:

Remote endpoint's SSL certificate fingerprint:

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 8 The London filial office — definition of VPN tunnel for the headquarters

On the **Advanced** tab, select the **Use custom routes only** option and set routes to London's local networks.

Authentication **Routing**

☐ Use routes provided automatically by the remote endpoint

☒ Use custom routes:

<input checked="" type="checkbox"/> Network ▲	Mask	Description
<input checked="" type="checkbox"/> 10.1.1.0	255.255.255.0	Company headquarters - LAN1
<input checked="" type="checkbox"/> 192.168.2.0	255.255.255.0	Company headquarters - LAN2

Figure 9 The London filial — routing configuration for the tunnel connected to the headquarters

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the **Connected** status will be reported in the **Adapter info** column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server in our example, the following command can be used at the London branch office server:

```
ping gw-newyork.company.com
```


6. Create a passive endpoint of the VPN tunnel connected to the Paris filial. Use the fingerprint of the VPN server of the Paris filial office as a specification of the fingerprint of the remote SSL certificate.

On the **Advanced** tab, select the **Use custom routes only** option and set routes to Paris' local networks.

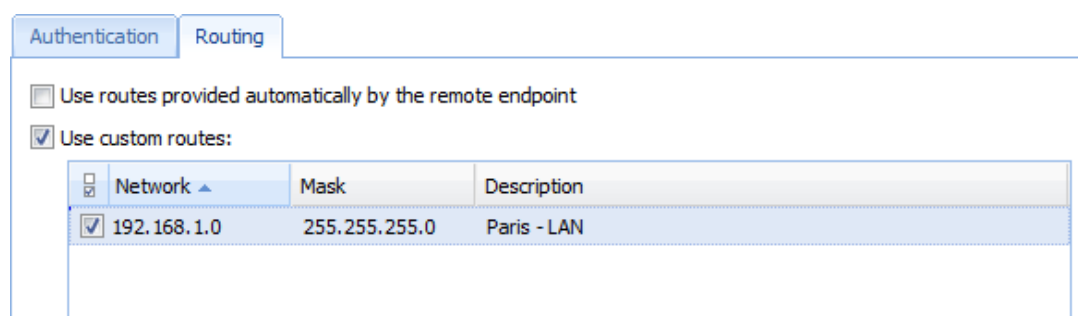


Figure 10 The London filial — routing configuration for the tunnel connected to the Paris branch office

Configuration of the Paris filial

1. Kerio Control must be installed on the default gateway of the filial's network.
2. In Kerio Control set basic traffic rules by using the connectivity wizard and the traffic policy wizard.

In this case there is no reason to enable the Kerio VPN server service (the server uses dynamic public IP address).

3. Customize DNS configuration as follows:
 - In the Kerio Control's DNS module configuration, enable DNS forwarder (forwarding of DNS requests to other servers).
 - Enable the **Use custom forwarding** option and define rules for names in the `company.com` and `filial1.company.com` domains. Specify the server for DNS forwarding by the IP address of the internal interface of the Kerio Control host (i.e. interface connected to the local network at the other end of the tunnel).

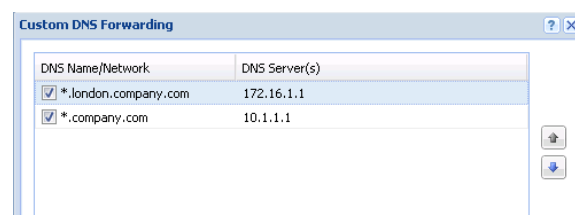


Figure 11 The Paris filial office
— DNS forwarding settings

Example of Kerio VPN configuration: company with two filial offices

- No DNS server will be set on the interface of the Kerio Control host connected to the local network.
 - Set the IP address 192.168.1.1 as a primary DNS server also for the other hosts.
4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).



The **VPN network** and **Mask** entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (newyork.company.com). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

On the **Advanced** tab, select the **Use custom routes only** option and set routes to London's local networks.

Network	Mask	Description
10.1.1.0	255.255.255.0	Company headquarters - LAN1
192.168.2.0	255.255.255.0	Company headquarters - LAN2

Figure 12 The Paris filial — routing configuration for the tunnel connected to the headquarters

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the **Connected** status will be reported in the **Adapter info** column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server in our example, the following command can be used at the Paris branch office server:

```
ping gw-newyork.company.com
```

6. Create an active endpoint of the tunnel connected to London (server gw-london.company.com). Use the fingerprint of the VPN server of the London filial office as a specification of the fingerprint of the remote SSL certificate.

On the **Advanced** tab, select the **Use custom routes only** option and set routes to London's local networks.

Authentication Routing

☐ Use routes provided automatically by the remote endpoint

☒ Use custom routes:

<input type="checkbox"/> Network ▲	Mask	Description
<input checked="" type="checkbox"/> 172.16.1.0	255.255.255.0	London - LAN1
<input checked="" type="checkbox"/> 172.16.2.0	255.255.255.0	London - LAN2

Figure 13 The Paris filial — routing configuration for the tunnel connected to the London branch office

Like in the previous step, check whether the tunnel has been established successfully, and check reachability of remote private networks (i.e. of local networks in the London filial).

7. The **All VPN Clients** group from the **Local Traffic** rule (no VPN clients will connect to this branch office network).

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Kerio VPN Server	Any	Firewall	Kerio	Allow
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local interfaces All VPN tunnels	Firewall Trusted/Local interfaces All VPN tunnels	Any	Allow

Figure 14 The Paris filial office — final traffic rules

VPN test

The VPN configuration has been completed by now. At this point, it is recommended to test reachability of the remote hosts in the other remote networks (at remote endpoints of individual tunnels).

For example, the ping or/and tracert (traceroute) operating system commands can be used for this testing.

Configuring IPsec VPN

IPsec overview

Kerio Control supports IPsec. IPsec (IP security) is a security extension for Internet Protocol (read more in [Wikipedia](#)).

Kerio Control uses IPsec for VPN implementation. IPsec can be used for:

- IPsec VPN server for connecting clients (desktops, notebooks, mobile devices etc...)
- [IPsec VPN tunnel](#) for connecting LANs

This article describes using IPsec VPN server and configuring clients.

For securing the communication you can use:

- a preshared key (PSK, shared secret)
- a SSL certificate
- both methods in Kerio Control (client application must use only one method).

Each user must provide their credentials for authentication.

Configuring IPsec VPN server with a preshared key

The preshared key is a shared password for all users using an IPsec VPN.

1. In the administration interface, go to **Interfaces**.
2. Double-click on **VPN Server**.
3. In the **VPN Server Properties** dialog (see screenshot [1](#)), check **Enable IPsec VPN Server**.

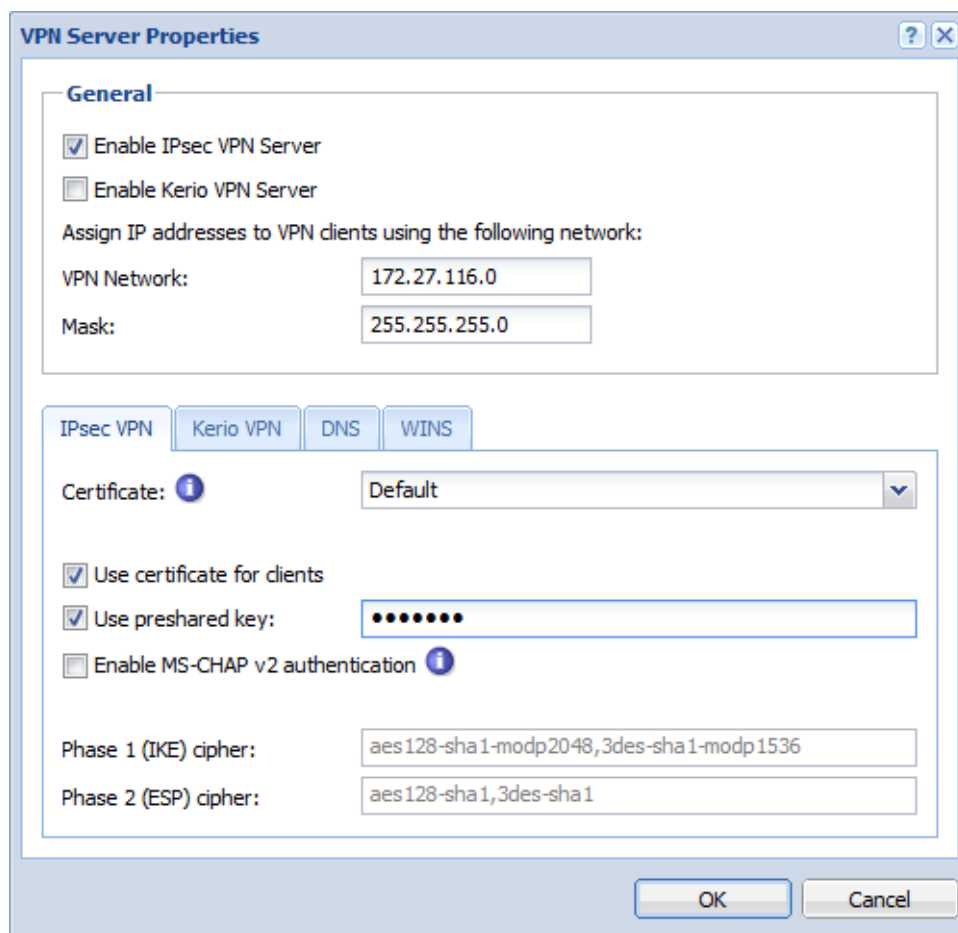


Figure 1 VPN Server Properties



Kerio Control is able to provide the Kerio VPN server and IPsec VPN server simultaneously.

4. On tab **IPsec VPN**, select a [valid SSL certificate](#) in the **Certificate** pop-up list.
5. Check **Use preshared key** and type the key.
6. Check **Enable MS-CHAP v2 authentication**, if the users' passwords are stored in a format which supports MS-CHAP v2.

User passwords are stored in a format supports MS-CHAP v2, if they are:

- mapped from Microsoft Active Directory
- local, but authenticate in Microsoft Active Directory
- local + **Store password in MS-CHAP v2 compatible format** is checked in the user dialog (see screenshot [2](#))

Configuring IPsec VPN

7. Save the settings.

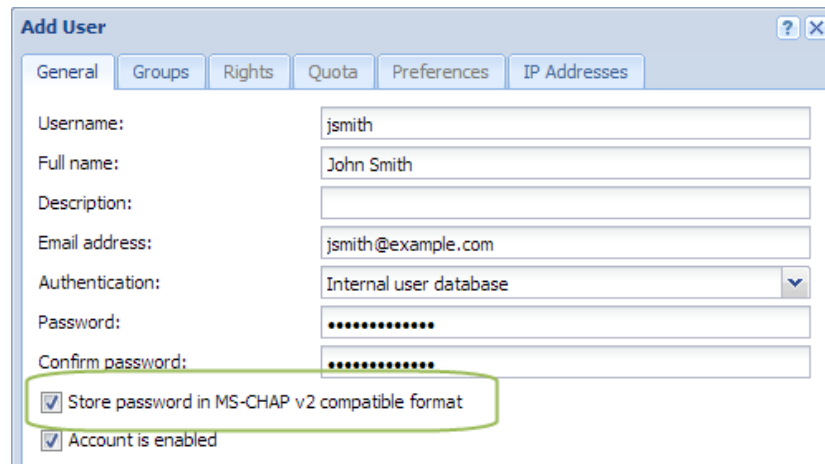


Figure 2 Add/Edit user dialog in section Users

Configuring IPsec server with a SSL certificate

1. In the administration interface, go to **Interfaces**.
2. Double-click on **VPN Server**.
3. In the **VPN Server Properties** dialog, check **Enable IPsec VPN Server**.
4. On tab **IPsec VPN**, select a **valid SSL certificate** in the **Certificate** pop-up list.
5. On tab **IPsec VPN**, check **Use certificate for clients**.
6. Check **Enable MS-CHAP v2 authentication**, if the users' passwords are stored in a format which supports MS-CHAP v2.

Users passwords are stored in a format supports MS-CHAP v2, if they are:

- mapped from Microsoft Active Directory
- local, but authenticate in Microsoft Active Directory
- local + **Store password in MS-CHAP v2 compatible format** is checked in the user dialog (see screenshot [2](#))

7. Save the settings.

Configuring clients with a preshared key

Tell your users what to prepare for the configuration of their clients:

- VPN type: L2TP IPsec PSK
- Kerio Control hostname or IP address
- preshared key (PSK, shared secret)
- username and password for access to firewall

Supported mobile devices

Many mobile devices support IPsec VPN and may work with Kerio Control. However, Kerio Control officially supports the following list:

- Android 4 and higher
- iOS 6 and higher

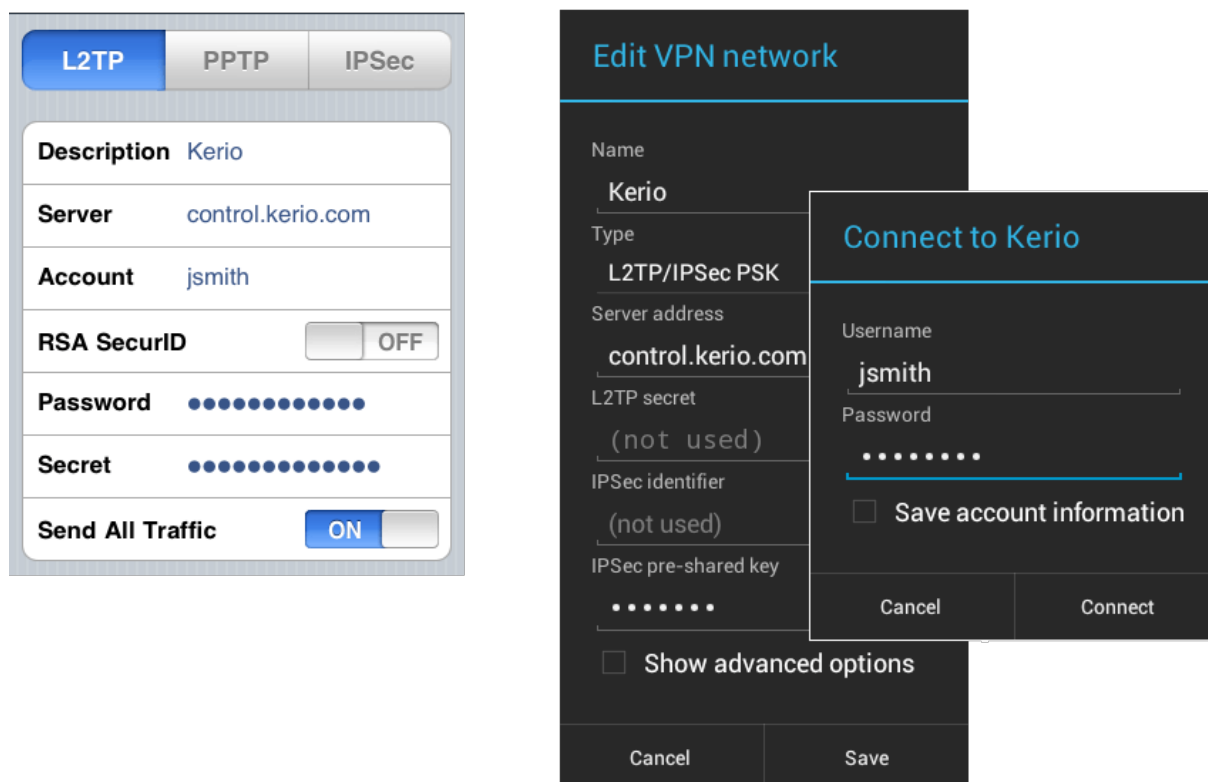


Figure 3 Examples of Apple iPhone and Android settings

Configuring IPsec VPN tunnel

IPsec overview

Kerio Control supports IPsec. IPsec (IP security) is a security extension for Internet Protocol (read more in [Wikipedia](#)).

Kerio Control uses IPsec for VPN implementation. IPsec can be used for:

- [IPsec VPN server](#) for connecting clients (desktops, notebooks, mobile devices etc...)
- IPsec VPN tunnel for connecting LANs

This article describes using IPsec VPN tunnel.

Configuring IPsec VPN tunnel with a preshared key authentication

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **VPN Tunnel**.
3. Type a name of the new tunnel.
4. Set the tunnel as active (and type the hostname of the remote endpoint) or passive.
5. Select **Type**: IPsec.
6. Select **Preshared key** and type the key.
7. Save the settings.

Configuring IPsec VPN tunnel with a SSL certificate authentication

You have two choices:

- [The SSL certificate of the remote endpoint is imported in the Kerio Control \(Definitions → SSL Certificates\)](#).
- The authority that signed the remote certificate is imported in the Kerio Control (**Definitions** → **SSL Certificates**). You also need to know the Local ID (Distinguish name) of the remote certificate.

If the SSL certificate/Authority is imported, follow these instructions:

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **VPN Tunnel**.
3. Type a name of the new tunnel.
4. Set the tunnel as active (and type the hostname of the remote endpoint) or passive.
5. Select **Type**: IPsec.
6. If the SSL certificate is imported: Select the remote certificate
If only the authority is imported: copy the value of the **Local ID** field from the remote certificate (Distinguish name) to the **Remote ID** field.
7. Save the settings.

Support for IPv6 protocol

Support for IPv6 protocol

- Configuring IPv6 parameters on network interfaces,
- Routing between individual interfaces,
- Stateless address autoconfiguration of hosts and devices in the LAN (SLAAC),
- Basic firewall without configuration options (blocking traffic directed from the Internet to the local network),
- Bandwidth management (without the option to define custom rules and bandwidth reservation),
- Overview of active connections,
- Volumes of data transferred on individual network interfaces,
- Monitoring IP traffic in the Debug log.

Kerio Control can therefore be used as an IPv6 router and allows access from hosts in the local network to the Internet via IPv6.

Filtering IPv6 overview

Kerio Control supports blocking of traffic by IPv6. In newer operating systems, this protocol is enabled by default and the computer has an automatically generated IPv6 address. This can cause a security hazard.

For security reasons, any tunneled IPv6 traffic is disabled by default.

Kerio Control allows the following settings:

1. In the administration interface, go to **Security Settings** → **IPv6**.
2. Check **Block tunelled IPv6**.

To ease the transition to IPv6. Some protocol can encapsulate IPv6 packets into IPv4 and thus communicate via network without IPv6 support.

3. In the **Definitions** → **IP Address Groups**, add a new group of allowed hosts.

4. Go back to **Security Settings** → **IPv6**.
5. Check **Except for the following IPv4 hosts** and select the IP address group.

IPv6 router advertisement

IPv6 router advertisement is used for automatic stateless configuration of IPv6 devices in the LAN (SLAAC). Add a record for every network in which Kerio Control is supposed to advertise as a default router.

1. In the administration interface, go to **IPv6 Router Advertisements**
2. Click **Add**.
3. Select an interface connected to the network where the router should advertise.
4. Double-click **Prefix** and type the IPv6 prefix (subnet address).
It has form of an IPv6 address and has to fit the set prefix length, i.e. all bits higher than the prefix length must be null.
5. Double-click **Prefix length** and type number of bits of IPv6 address which are considered as a prefix (subnet address).

Configuring traffic rules

How traffic rules work

The traffic policy consists of rules ordered by their priority. When the rules are evaluated they are processed from the top downwards and the first matched rule is applied. The order of the rules can be changed with the two arrow buttons on the right side of the window, or by dragging the rules within the list.

An implicit rule denying all traffic is shown at the end of the list. This rule cannot be removed. If there is no rule to allow particular network traffic, then the implicit rule will discard the packet.



Traffic rules only work for IPv4. By default, IPv6 traffic initiated from the LAN is allowed while traffic initiated from the Internet and directed to the LAN is denied (default firewall).



To control user connections to WWW or FTP servers and filter contents, use the special tools available in Kerio Control for these purposes rather than traffic rules.

Configuring traffic rules

If you do not have any traffic rules created in Kerio Control, use [configuration wizard](#) (go to **Traffic Rules** and click **More Actions** → **Configure in Wizard**).

Then create your own rules:

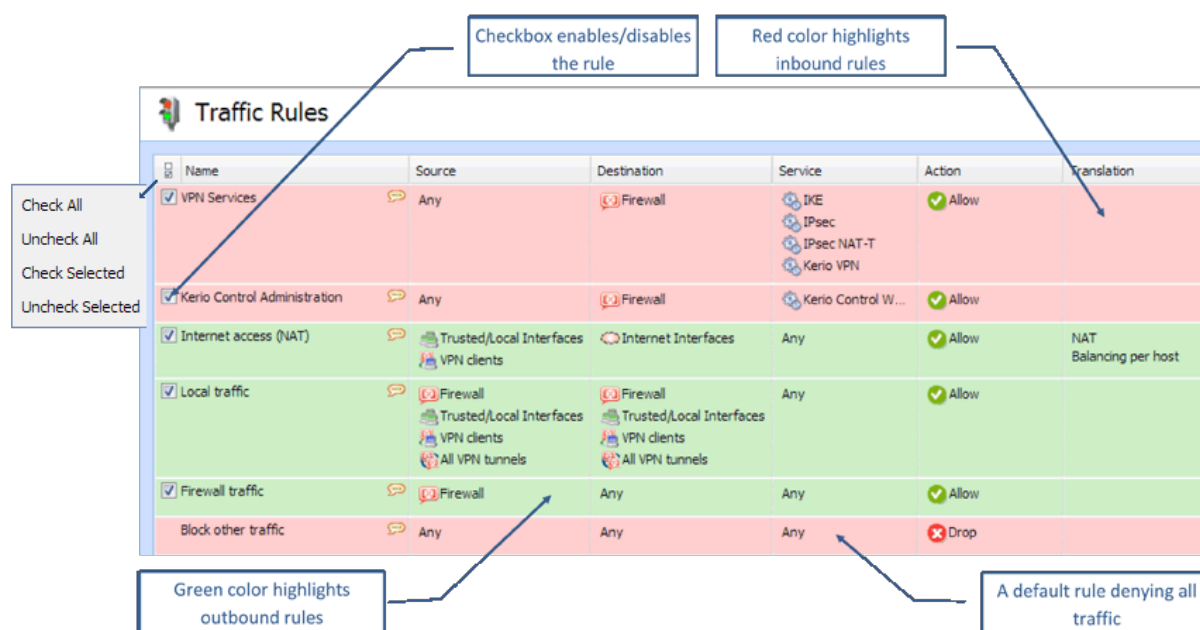


Figure 1 Basic traffic rules configured by Wizard

Example 1: Port mapping

We need to enable the SMTP service for Kerio Connect placed in your local network protected by Kerio Control.

1. In the administration interface, go to **Traffic Rules**.
2. Click **Add**.
3. Type a name of the rule — SMTP for Kerio Connect.
4. In column **Source** leave **Any**.

Mapped services can be accessed by clients both from the Internet and from the local network. For this reason, it is possible to keep the **Any** value in the **Source** entry.

5. Double-click **Destination** and select **Firewall**.

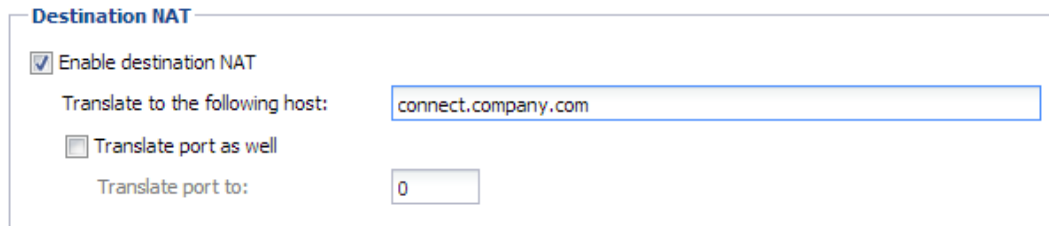
SMTP service will be available at all addresses of the interface connected to the Internet.

6. Double-click **Service** and select **SMTP**.
7. Double-click **Action** and select **Allow**.
8. Double-click **Translation**.

9. In the **Traffic Rule - Translation** dialog, check **Enable destination NAT** and type the hostname or IP address of the SMTP server placed in your local network (e.g. Kerio Connect).

Configuring traffic rules

10. Move the rule to the top of the table of traffic rules.



The image shows a configuration window titled "Destination NAT". It contains the following elements:

- A checked checkbox labeled "Enable destination NAT".
- A text field labeled "Translate to the following host:" containing the value "connect.company.com".
- An unchecked checkbox labeled "Translate port as well".
- A text field labeled "Translate port to:" containing the value "0".

Figure 2 Enabling destination NAT

Other examples

- [Network address translation](#)
- [Multihoming](#)
- [Limiting Internet Access](#)
- [Exclusions](#)

User accounts and groups in traffic rules

In traffic rules, source/destination can be specified also by user accounts or/and user groups. In the traffic policy, each user account represents the IP address of the host from which a user is connected. This means that the rule is applied to users authenticated at the firewall only (when the user logs out, the rule is not effective any longer):

Step 1: Enabling certain users to access the Internet

Assuming that this problem applies to a private local network and Internet connection is performed through NAT. Then specify these users in the **Source** item in the NAT rule.






Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	 jsmith  lcarr  mwayne	 Internet interfaces	Any	 Allow	NAT Balancing per host

Figure 3 This traffic rule allows only selected users to connect to the Internet

Such a rule enables the specified users to connect to the Internet (if authenticated). However, these users must open the Kerio Control interface's login page manually and authenticate.



With the rule defined, all methods of automatic authentication will be ineffective (i.e. redirecting to the login page, NTLM authentication as well as automatic authentication from defined hosts). Automatic authentication (redirection to the login page) is performed at the very moment of establishing connection to the Internet. However, this NAT rule blocks any connection unless the user is authenticated.

Step 2: Enabling automatic authentication


The automatic user authentication issue can be solved as follows:

- Add a rule allowing an unlimited access to the HTTP service before the NAT rule.

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> WWW without authentication	Trusted/Local interfaces	Internet interfaces	HTTP	<input checked="" type="checkbox"/> Allow	NAT Balancing per host
<input checked="" type="checkbox"/> Internet access (NAT)	jsmith lcarr mwayne	Internet interfaces	Any	<input checked="" type="checkbox"/> Allow	NAT Balancing per host

Figure 4 These traffic rules enable automatic redirection to the login page

- In URL rules, allow specific users to access any web site and deny any access to other users.

 HTTP Policy

URL Rules			
Name	Action	URL	Users
<input checked="" type="checkbox"/> Allow access to selected users	<input checked="" type="checkbox"/> Allow		jsmith lcarr mwayne
<input checked="" type="checkbox"/> Deny access to all other users	<input checked="" type="checkbox"/> Deny		

Figure 5 These URL rules enable specified users to access any Web site

User not authenticated yet who attempts to open a Web site will be automatically redirected to the authentication page (or authenticated by NTLM, or logged in from the corresponding host). After a successful authentication, users specified in the NAT rule (see figure 4) will be allowed to access also other Internet services. Users not specified in the rules will be disallowed to access any web site or/and other Internet services.

Configuring traffic rules



In this example, it is assumed that client hosts use the Kerio Control DNS Forwarder or local DNS server (traffic must be allowed for the DNS server). If client stations used a DNS server in the Internet, it would be necessary to include the DNS service in the rule which allows unlimited Internet access.

Demilitarized zone (DMZ)

This topic is covered in a special article: [Configuring demilitarized zone \(DMZ\)](#).

Policy routing

This topic is covered in a special article: [Configuring policy routing](#).

Configuring IP address translation

IP address translation (NAT) overview

[Network Address Translation](#) (NAT) is a term used for the exchange of a private IP address in a packet going out from the local network to the Internet with the IP address of the Internet interface of the Kerio Control host. This technology is used to connect local private networks to the Internet by a single public IP address.

Configuring IP address translation

1. In the administration interface, go to **Traffic Rules**.
IP address translation must be configured for the particular rules.
2. Double-click **Translation** in the selected rule.
3. In the **Traffic Rule - Translation** dialog, you can configure the following:

Source IP address translation (NAT — Internet connection sharing)

Source address translation is used in traffic rules applied to traffic from the local private network to the Internet. In other rules (traffic between the local network and the firewall, between the firewall and the Internet, etc.), NAT is unnecessary.

For source address translation, check **Enable source NAT** and select:

Default setting (recommended)

By default, in packets sent from the LAN to the Internet the source IP address will be replaced by IP address of the Internet interface of the firewall through which the packet is sent. This IP address translation method is useful in the [general rule](#) for access from the LAN to the Internet, because it works correctly in any Internet connection configuration and for any status of individual links.

For a single leased link, or connection failover, the following options have no effect on Kerio Control's functionality. If Kerio Control works in the mode of network traffic load balancing, you can select:

- **Perform load balancing per host** — traffic from the specific host in the LAN will be routed via the same Internet link.
This method is set as default, because it guarantees the same behavior as in case of clients connected directly to the Internet. However, load balancing dividing the traffic among individual links may be not optimal in this case.
- **Perform load balancing per connection** — the Internet link will be selected for each connection established from the LAN to the Internet to spread the load optimally.

Configuring IP address translation

This method guarantees the most efficient use of the Internet connection's capacity. However, it might also introduce problems and collisions with certain services. The problem is that individual connections are established from various IP addresses (depending on the firewall's interface from which the packet is sent) which may be considered as an attack at the destination server.

Hint

For maximal efficiency of the connection's capacity, go to the [Configuring policy routing](#) article.

Use specific outgoing interface

Packets will be sent to the Internet via this specific link. This allows definition of rules for forwarding specific traffic through a selected Interface — so called [policy routing](#).

If the selected Internet link fails, Internet will be unavailable for all services, clients, etc. specified by this rule. To prevent from such situations, check **Allow using of a different interface if this one becomes unavailable**.

Use specific IP address

An IP address for NAT will be used as the source IP address for all packets sent from the LAN to the Internet.

- It is necessary to use an IP address of one of the firewall's Internet interfaces.
- Definition of a specific IP Address cannot be used in combination with network load balancing or connection failover.

Full cone NAT

The typical behavior of NAT allows returning traffic only from a specific IP Address. The behavior can be adjusted to allow returning traffic from any IP Address. This is called full cone NAT.

If this option is off, Kerio Control performs so called port restricted cone NAT. In outgoing packets transferred from the local network to the Internet, Kerio Control replaces the source IP address of the interface with the public address of the firewall (see above). If possible, the original source port is kept; otherwise, another free source port is assigned. For returning traffic, the firewall allows only packets arriving from the same IP address and port to which the outgoing packet was sent. This translation method guarantees high security — the firewall will not let in any packet which is not a response to the sent request.

However, many applications (especially applications working with multimedia, Voice over IP technologies, etc.) use another traffic method where other clients can (with direct connection established) connect to a port opened by an outgoing packet. Therefore, Kerio Control supports also the full cone NAT mode where the described restrictions are not applied for incoming packets. The port then lets in incoming packets with any source IP address and port. This translation method may be necessary to enable full functionality of certain applications.



Full cone NAT may introduce certain security threats — the port opened by the outgoing connection can be accessed without any restrictions being applied. For this reason, it is recommended to enable full cone NAT only for a specific service (i.e. to create a special rule for this purpose).

Destination NAT (port mapping):

Destination address translation (also called port mapping) is used to allow access to services hosted in private local networks behind the firewall.

For port mapping:

1. Check **Enable destination NAT**.
2. In field **Translate to the following host**, type a host address or DNS name.
IP address that will substitute the packet's destination address. This address also represents the address/name of the host on which the service is actually running.
3. If you want to change a port, check **Translate port as well** and type the port of a service.
During the process of IP translation you can also substitute the port of the appropriate service. This means that the service can run at a port that is different from the port where it is available from the Internet.



This option cannot be used if multiple services or ports are defined in the **Service** entry within the appropriate traffic rule.

For examples of traffic rules for port mapping and their settings, refer to article [Configuring traffic rules](#).

A default NAT rule description




Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	 Trusted/Local interfaces	 Internet interfaces	Any	 Allow	NAT Balancing per host

Figure 1 A typical traffic rule for NAT (Internet connection sharing)

Configuring IP address translation

Source

Group **Trusted/Local Interfaces** (from the **Interfaces** section). This group includes all segments of the LAN connected directly to the firewall. If access to the Internet from some segments is supposed to be blocked, the most suitable group to file the interface into is **Other interfaces**.



If the local network consists of cascaded segments (i.e. it includes other routers), it is not necessary to customize the rule in accordance with this fact — it is just necessary to set routing correctly.

Destination

The *Internet Interfaces* group. With this group, the rule is usable for any type of Internet connection.

Service

This entry can be used to define global limitations for Internet access. If particular services are defined for NAT, only these services will be used for the NAT and other Internet services will not be available from the local network.

Actions

The **Action** must be set to **Allow**.

Translation

In the **Source NAT** section select the **Default settings** option (the primary IP address of the outgoing interface will be used for NAT). The default option will ensure that the correct IP address and Interface are used for the intended destination.



Destination NAT should not be configured for outgoing rules, except under very unique circumstances.

Placing the rule

The rule for destination address translation must be preceded by all rules which deny access to the Internet from the local network.

Such a rule allows access to the Internet from any host in the local network, not from the firewall itself (i.e. from the Kerio Control host).

Traffic between the firewall and the Internet is enabled by a special rule by default. Since the Kerio Control host can access the Internet directly, it is not necessary to use NAT.

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any	Any	Allow	

Figure 2 Rule for traffic between the firewall and hosts in the Internet

Configuring traffic rules — multihoming

Multihoming overview

Multihoming is a term used for situations when one network interface connected to the Internet uses multiple public IP addresses. Typically, multiple services are available through individual IP addresses (this implies that the services are mutually independent).

A web server web1 with IP address 192.168.1.100 and a web server web2 with IP address 192.168.1.200 are running in the local network.

The interface connected to the Internet uses public IP addresses 195.39.55.12 and 195.39.55.13:

- web1 to be available from the Internet at the IP address 195.39.55.12
- web2 to be available from the Internet at the IP address 195.39.55.13

The two following traffic rules must be defined in Kerio Control to enable this configuration:







Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Web1 server mapping	Any	 195.39.55.12	 HTTP	 Allow	MAP 192.168.1.100
<input checked="" type="checkbox"/> Web2 server mapping	Any	 195.39.55.13	 HTTP	 Allow	MAP 192.168.1.200

Figure 1 Multihoming — web servers mapping

1. In the administration interface, go to **Traffic Rules**.
2. Click **Add**.
3. Type a name of the rule — Web1 server mapping.
4. In column **Source** leave **Any**.
5. Double-click **Destination** and select **Host**.

The IP address of the interface connected to the Internet must be added (our example: 195.39.55.12).

6. Double-click **Service** and select **HTTP**.
7. Double-click **Action** and select **Allow**.

8. Double-click **Translation**.

Go to the **Destination NAT** section, select the **Translate to the following host** option and specify IP address of a corresponding Web server (web1).

9. Repeat steps 1 — 8 for Web2 server.

Configuring traffic rules — limiting Internet access

Limiting Internet Access

Access to Internet services from the local network can be limited in several ways. In the following examples, the limitation rules use IP translation (see [Configuring IP address translation](#) article).

Other methods of Internet access limitations can be found in the [Configuring traffic rules - exclusions](#) article.



Rules mentioned in these examples can be also used if Kerio Control is intended as a neutral router (no address translation) — in the **Translation** entry there will be no translations defined.

1. Allow access to selected services only. In the translation rule in the **Service** entry, specify only those services that are intended to be allowed.

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	DNS FTP FTPS HTTP HTTPS SSH	Allow	NAT Balancing per host

Figure 1 Internet connection sharing — only selected services are available

2. Limitations sorted by IP addresses. Access to particular services (or access to any Internet service) will be allowed only from selected hosts. In the **Source** entry define the group of IP addresses from which the Internet will be available. This group must be formerly defined in **Definitions** → **IP Address Groups**.

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	Internet access	Internet interfaces	Any	Allow	NAT Balancing per host

Figure 2 Only selected IP address group(s) is/are allowed to connect to the Internet



This type of rule should be used only for the hosts with static IP addresses.

3. Limitations sorted by users. Firewall monitors if the connection is from an authenticated host. In accordance with this fact, the traffic is permitted or denied.




Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	 Internet access	 Internet interfaces	Any	 Allow	NAT Balancing per host

Figure 3 Only selected user group(s) is/are allowed to connect to the Internet

Alternatively you can define the rule to allow only authenticated users to access specific services. Any user that has a user account in Kerio Control will be allowed to access the Internet after authenticating to the firewall. Firewall administrators can easily monitor which services and which pages are opened by each user.




Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	 Authenticated users	 Internet interfaces	Any	 Allow	NAT Balancing per host

Figure 4 Only authenticated users are allowed to connect to the Internet



Usage of user accounts and groups in traffic policy follows [specific rules](#).

Configuring traffic rules — exclusions

Configuring exclusions

You may need to allow access to the Internet only for a certain user/address group, whereas all other users should not be allowed to access this service.

This will be better understood through the following example (how to allow a user group to use SSH for access to servers in the Internet). Use the following rule to meet these requirements:

The rule will allow selected users (or a group of users/IP addresses, etc.) to access SSH servers in the Internet. The default rule (Block other traffic) blocks the other users and communication.







<input checked="" type="checkbox"/> Allow SSH to a group	 SSH allowed	 Internet Interfaces	 SSH	 Allow	NAT Balancing per host
Block other traffic	 Any	Any	Any	 Drop	

Figure 1 Exception — SSH is available only for selected user group(s)

Configuring Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ)

Demilitarized zone (DMZ) is a special segment of the local network reserved for servers accessible from the Internet. It is not allowed to access the local network from this segment — if a server in the DMZ is attacked, it is impossible for the attacker to reach other servers and computers located in the local network.

Configuring DMZ

As an example we will suppose rules for a web server located in the DMZ. The demilitarized zone is connected to the DMZ interface included in group **Other Interfaces**. The DMZ uses subnet 192.168.2.x, the web server's IP address is 192.168.2.2.

Now you will add the following rules:

- Make the web server accessible from the Internet — mapping HTTP service on the server in the DMZ,
- Allow access from the DMZ to the Internet via NAT (IP address translation) — necessary for correct functionality of the mapped service,
- Allow access from the LAN to the DMZ — this makes the web server accessible to local users,
- Disable access from the DMZ to the LAN — protection against network intrusions from the DMZ. This is globally solved by a default rule blocking any other traffic (here we have added the blocking rule for better understanding).














Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Web server in DMZ	 Internet interfaces	 Firewall	 HTTP	 Allow	MAP 192.168.2.2
<input checked="" type="checkbox"/> Allow Internet access from DMZ	 DMZ	 Internet interfaces	Any	 Allow	NAT Balancing per host
<input checked="" type="checkbox"/> Allow access from LAN to DMZ	 Trusted/Local interfaces	 DMZ	Any	 Allow	
<input checked="" type="checkbox"/> Deny access from DMZ to LAN	 DMZ	 Trusted/Local interfaces	Any	 Deny	

Figure 1 Traffic rules for the DMZ

Hint

To make multiple servers accessible in the DMZ, it is possible to use multiple public IP addresses on the firewall's Internet interface — so called [multihoming](#).

Configuring policy routing

Policy routing overview

If the LAN is connected to the Internet by [multiple links with load balancing](#), it may be necessary to force certain types of traffic out a particular Interface. For example, sending VoIP traffic out a different Interface than your web browsing or streaming media. This approach is called policy routing.

In Kerio Control, policy routing can be defined by conditions in traffic rules for Internet access with IP address translation (NAT).



Policy routing traffic rules are of higher priority than routes defined in the routing table.

Configuring a preferred link for email traffic

The firewall is connected to the Internet by two links with load balancing with speed values of 4 Mbit/s and 8 Mbit/s. One of the links is connected to the provider where the mailserver is also hosted. Therefore, all email traffic (SMTP, IMAP and POP3) is routed through this link.

Define traffic rules:

- The first rule defines that NAT is applied to email services and the Internet 4 Mbit interface is used.
- The other rule is a general NAT rule with automatic interface selection.

<input checked="" type="checkbox"/> NAT - preferred link for email	Trusted/Local Interfaces	Internet Interfaces	IMAP IMAPS POP3 POP3S SMTP SMTPS	Allow	NAT (Internet 4 Mbit)
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces VPN clients	Internet Interfaces	Any	Allow	NAT Balancing per host

Figure 1 Policy routing — a preferred link for email traffic

Setting of NAT in the rule for email services is shown in figure 2. Allow use of a back-up link in case the preferred link fails. Otherwise, email services will be unavailable when the connection fails.

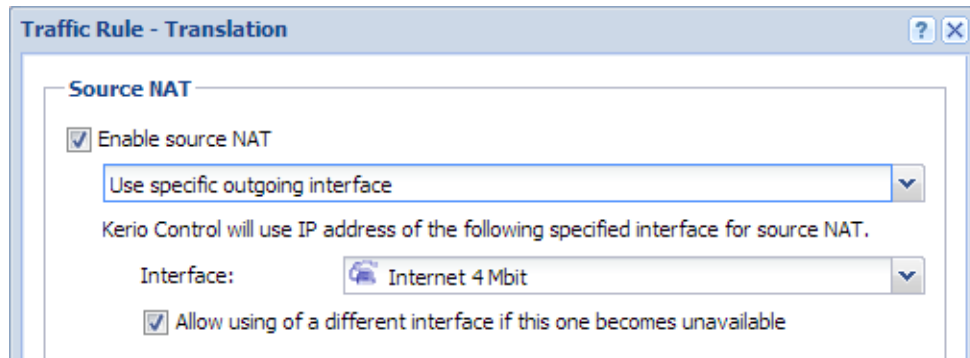


Figure 2 Policy routing — setting NAT for a preferred link



In the second rule, automatic interface selection is used. This means that the Internet 4 Mbit link is also used for network traffic load balancing. Email traffic is certainly still respected and has higher priority on the link preferred by the first rule. This means that total load will be efficiently balanced between both links all the time.

If you need to reserve a link only for a specific traffic type (i.e. route other traffic through other links), go to **Interfaces** and [uncheck the Use for Link Load Balancing option](#). In this case the link will not be used for automatic load balancing. Only traffic specified in corresponding traffic rules will be routed through it.

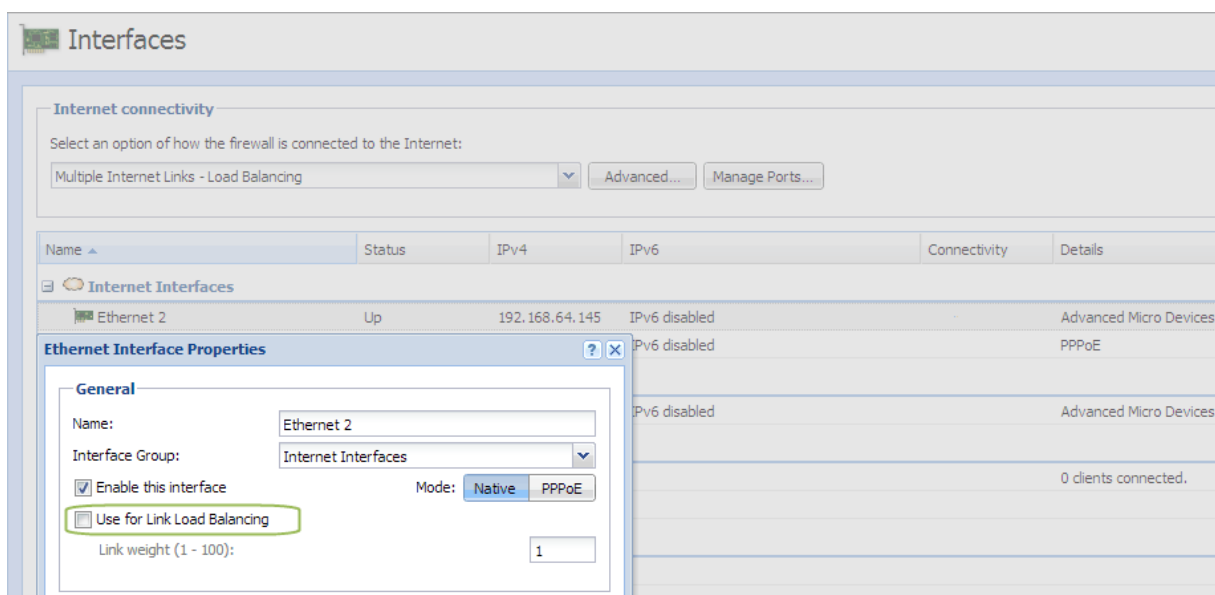


Figure 3 Interfaces — Uncheck the Use for Link Load Balancing option

Configuring an optimization of network traffic load balancing

Kerio Control provides two options of network traffic load balancing:

- per host (clients)
- per connection

The best solution (more efficient use of individual links) proves to be the option of load balancing per connection. However, this mode may encounter problems with access to services where multiple connections get established at one moment (web pages and other web related services). The server can consider source addresses in individual connections as connection recovery after failure or as an attack attempt.

This problem can be bridged over by policy routing. In case of problematic services (e.g. HTTP and HTTPS) the load will be balanced per host, i.e. all connections from one client will be routed through a particular Internet link so that their IP address will be identical (a single IP address will be used). To any other services, load balancing per connection will be applied — thus maximally efficient use of the capacity of available links will be reached.

Meeting of the requirements will be guaranteed by using two NAT traffic rules:

- In the first rule, specify corresponding services and set the **per host** NAT mode.
- In the second rule, which will be applied for any other services, set the **per connection** NAT mode.









Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> NAT - balancing per host	 Trusted/Local interfaces	 Internet interfaces	 HTTP  HTTPS	 Allow	NAT Balancing per host
<input checked="" type="checkbox"/> NAT - balancing per connections	 Trusted/Local interfaces	 Internet interfaces	Any	 Allow	NAT Balancing per connection

Figure 4 Policy routing — load balancing optimization

Configuring intrusion prevention system

Intrusion prevention system overview

Kerio Control integrates [Snort](#), an intrusion detection and prevention system (IDS/IPS) protecting the firewall and the local network from known network intrusions.

A network intrusion is network traffic that impacts the functionality or security of the victim-host. A typical attribute of intrusions is their apparent legitimacy and it is difficult to uncover such traffic and filter it simply by traffic rules. Let us use Denial of Service intrusion as an example — too many connections are established on a port to use up the system resources of the server application so that no other users can connect. However, the firewall considers this act only as access to an allowed port.



- The intrusion prevention system works on all network interfaces included in the **Internet Interfaces** group. It detects and blocks network intrusions coming from the Internet, not from hosts in local networks or VPN clients.
- [Use of NAT is required](#).
- Intrusion detection is performed before [traffic rules](#).

Configuring intrusion prevention

1. In the administration interface, go to **Intrusion Prevention**.
2. Check **Enable Intrusion Prevention**.
3. Leave Severity levels in the default mode.

Kerio Control distinguishes three levels of intrusion severity:

- **High severity** — activity where the probability that it is a malicious intrusion attempt is very high (e.g. Trojan horse network activity).
 - **Medium severity** — activities considered as suspicious (e.g. traffic by a non-standard protocol on the standard port of another protocol).
 - **Low severity** — network activities which do not indicate immediate security threat (e.g. port scanning).
4. Test the intrusion prevention system by clicking the link **On the Kerio website, you can test these settings**.

Configuring intrusion prevention system

Upon startup of the test, three fake harmless intrusions of high, middle, and low severity will be sent to the IP address of your firewall.

The Security log will report when the firewall identified and possibly blocked an intrusion.

Configuring ignored intrusions

In some cases, legitimate traffic may be detected as an intrusion. If this happens, it is helpful to define an exception for the intrusion:

1. In the administration interface, go to the **Security** log.
2. Locate the log event indicating the filtered traffic.
For example: "IPS: Alert, severity: Medium, Rule ID: 1:2009700 ET VOIP Multiple Unauthorized SIP Responses"
3. Copy the rule ID number.
4. In the administration interface, go to **Intrusion Prevention**.
5. Click **Advanced**.
6. In the **Advanced Intrusion Prevention Settings** dialog, click **Add**.
7. Paste the rule ID number and a description.

The legitimate traffic will be allowed now.

Configuring protocol-specific intrusions

Some intrusions may target security weaknesses in specific application protocols. Therefore, some security rules are focused on special protocols on standard and frequently used ports.

If an application is available from the Internet that uses any of the listed protocols on a non-standard port (e.g. HTTP on port 10000), it can be helpful to add this port in list of ports on which protocol-specific intrusions will be detected:

1. In the administration interface, go to **Intrusion Prevention**.
2. Click **Advanced**.
3. In the **Advanced Intrusion Prevention Settings** dialog, find the desired service (HTTP in our example).
4. Double-click the selected row and type the port (10000 in our example).
5. Save the settings.

The service running on the non-standard port will be protected by the protocol-specific intrusions.

IP blacklists overview

Kerio Control is able to log and block traffic from IP addresses of known intruders (so called blacklists). Such method of detection and blocking of intruders is much faster and also less demanding than detection of individual intrusion types. However, there are also disadvantages. Blacklists cannot include IP addresses of all possible intruders. Blacklist also may include IP addresses of legitimate clients or servers. Therefore, you can set the same actions for blacklists as for detected intrusions.

Automatic updates

For correct functionality of the intrusion detection system, it is necessary to update databases of known intrusions and intruder IP addresses regularly.

Under normal circumstances there is no reason to disable automatic updates — non-updated databases decrease the effectiveness of the intrusion prevention system.



Automatic updates are incremental. If you need to force a full update, click **Shift + Update now**.



For database updates, a valid Kerio Control license or a registered trial version is required.

Filtering MAC addresses

Filtering MAC addresses overview

Kerio Control allows filtering by hardware addresses (MAC addresses). Filtering by MAC addresses ensures that specific devices can be allowed or denied, regardless of their IP Address.



The MAC address filter is processed independently of [traffic rules](#).

Configuring the filter

1. In the administration interface, go to **Security Settings**.
2. On tab **MAC filter**, check the network interface for where the MAC filter will be applied (usually LAN).
3. Select the right mode:
 - **Prevent listed computers from accessing the network** — the filter will block only MAC addresses included on the list.
This mode can be used to block known MAC addresses, but will not filter traffic of new, unknown devices.
 - **Permit only listed computers to access the network** — the filter allows only MAC addresses included on the list, any other address will be blocked.
4. Add MAC addresses to the list.
MAC addresses can be separated by:
 - colons (e.g.: a0:de:bf:33:ce:12)
 - dashes (e.g.: a0-de-bf-33-ce-12)
 - without separators (a0debf33ce12)
5. Double check that listed addresses are correct.
6. Check **Enable MAC filter**.
7. Click **Apply**.

Your filter is fully configured and active.

Configuring Universal Plug-and-Play (UPnP)

Universal Plug-and-Play (UPnP) overview

Kerio Control supports UPnP protocol (*Universal Plug-and-Play*). This protocol enables client applications (i.e. *Microsoft MSN Messenger*) to detect the firewall and make a request for mapping of appropriate ports from the Internet for the particular host in the local network. Such mapping is always temporary — it is either applied until ports are released by the application (using UPnP messages) or until expiration of the certain timeout.

The required port must not collide with any existing mapped port or any traffic rule allowing access to the firewall from the Internet. Otherwise, the UPnP port mapping request will be denied.

Configuring the UPnP support

UPnP can be enabled under **Security Settings**, the **Miscellaneous** tab.

Enable UPnP

This option enables UPnP.

Log packets

If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the **Filter** log.

Log connections

If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the **Connection** log.



1. Apart from the fact that UPnP is a useful feature, it may also endanger network security, especially in case of networks with many users where the firewall could be controlled by too many users. The firewall administrator should consider carefully whether to prefer security or functionality of applications that require UPnP.

Using traffic policy you can limit usage of UPnP and enable it to certain IP addresses or certain users only.

Example:

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Allow UPnP for selected hosts	UPnP clients	Firewall	UPnP	Allow	NAT Balancing per host
<input checked="" type="checkbox"/> Deny UPnP	Any	Firewall	UPnP	Deny	

Figure 1 Traffic rules allowing UPnP for specific hosts

The first rule allows UPnP only from **UPnP Clients** IP group. The second rule denies UPnP from other hosts (IP addresses).

Configuring bandwidth management

Bandwidth management overview

Kerio Control includes bandwidth management, which regulates network traffic to ensure reliability of essential services, and to avoid congestion.

How bandwidth management works

The bandwidth management feature provides two basic functions:

- **Limiting bandwidth for data transfers** — this approach is designed to reduce congestion caused by non-essential traffic (e.g. large data transfers, video streaming, etc.).
- **Reserving bandwidth for specific services** — it is possible to reserve bandwidth for services crucial for the company's basic operations (email, IP telephony, etc.). This bandwidth will be always available, regardless of the current traffic load on the link.

Internet Links Speed

For correct management of the bandwidth, it is necessary to assign a link speed to each Internet interface.

In order for the bandwidth management to be most effective, it is suggested to use a conservative link speed estimation which is approximately 80% of the actual speed.

Example: For ASDL line with declared 8192/512 Kbit/s, set download speed to 6250 Kbit/s and upload speed to 400 Kbit/s.

Configuring bandwidth management

For example we want to restrict user John Smith — his limit will be set to 50% of the link for download in all interfaces in his working hours:

1. In the administration interface, go to **Bandwidth Management and QoS**.
2. For creating a new rule, click **Add**.
3. Type a name of the rule (John Smith).
4. Double-click **Traffic**.

Configuring bandwidth management

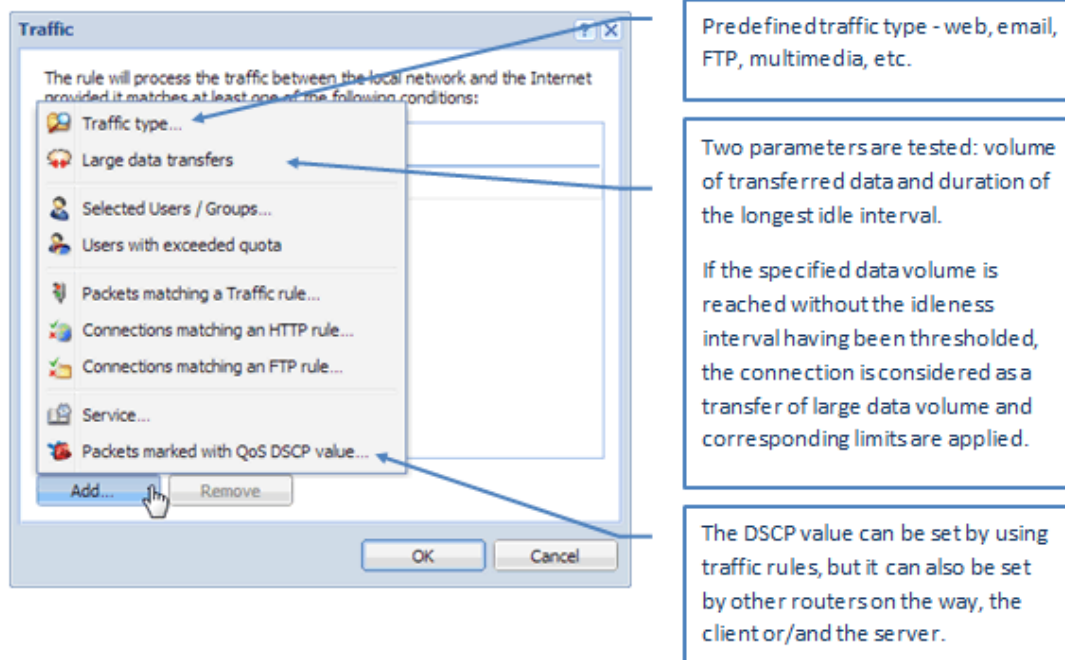


Figure 1 The Traffic dialog

5. In the **Traffic** dialog, click **Add** and choose **Selected Users / Groups**.
6. Double-click **Download**, check **Do not exceed** and set the limit (see screenshot 2).

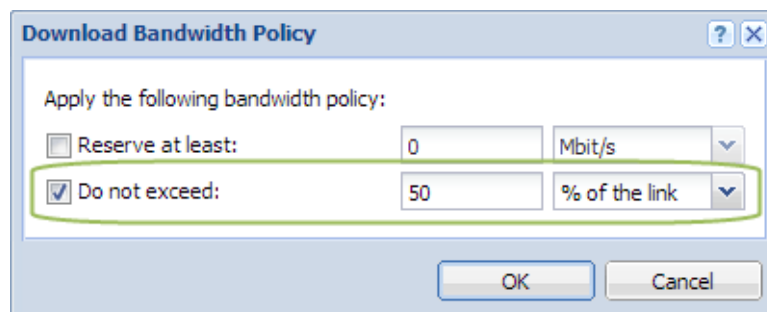


Figure 2 The Download Bandwidth Policy dialog

7. **Upload** leave as it is (No limit).
8. **Interface** leave as it is (All)
9. Double-click **Valid Time** and select a time range.
You can create a new time range in **Definitions** → **Time Ranges**.
10. Check **Chart**.
Timeline for traffic matching the rule can be viewed under **Status** → **Traffic Charts** (up to 24 hours back). The chart shows how much the particular traffic loads the link and helps you optimize bandwidth management rules. Local traffic is not accounted.
11. Click **Apply** for saving the new rule.



Rules arrangement is important. Rules are processed from the top.

Bandwidth Management and QoS Admin ▼

The Bandwidth Management allows you to fine-tune your Internet bandwidth utilization. You can reserve as well as limit bandwidth for selected traffic.

Bandwidth Management rules

<input type="checkbox"/>	Name	Traffic	Download	Upload	Interface	Valid Time	<input type="checkbox"/>	Chart
<input checked="" type="checkbox"/>	SIP VoIP	SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	VPN	VPN Services	Reserve: 32 KB/s	Reserve: 32 KB/s	Ethernet 2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Remote Access	Remote Access	Reserve: 20% of the link	Reserve: 20% of the link	Ethernet 2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	John Smith	jsmith	Limit: 50% of the link	No limit	All	Working hours	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Other traffic	Any	No limit	No limit	All			

Figure 3 Bandwidth Management and QoS

Configuring HTTP policy

HTTP policy overview

Kerio Control provides a wide range of filters for HTTP protocol. You can block access to undesirable web sites, block certain types of files and limit viruses, worms and Trojan horses with this tool.

Here are the main purposes of HTTP content filtering:

- access limitations according to URL (substrings contained in URL addresses)
- blocking of certain HTML items (i.e. scripts, ActiveX objects, etc.)
- filtering based on classification by the [Kerio Control Web Filter](#) module (worldwide website classification database)
- limitations based on occurrence of denied words (strings)
- antivirus control of downloaded objects

Conditions for HTTP filtering

For HTTP content filtering, the following conditions must be met:

1. Traffic must be controlled by an appropriate protocol inspector.
An appropriate protocol inspector is activated automatically unless its use is denied by traffic rules.
2. Kerio Control performs URL based filtering for encrypted traffic (HTTPS protocol). Note that HTTPS filtering of URLs is limited only to the domain name. The resource identifier part of the request (e.g. /path/index) is not considered as part of the condition of a rule.
3. HTTP/HTTPS rules are applied also when the Kerio Control's proxy server is used.
4. If the proxy server is used, it is also possible to filter HTTPS servers. However, it is not possible to filter individual objects at these servers.

Adding HTTP rules

1. In the administration interface, go to **HTTP Policy**.
2. On tab **URL Rules**, click **Add**.
3. Type a name of the new rule.
4. Double-click **Action** and select:
 - **Allow** — traffic allowed, user does not even notice anything happening.
In the **Properties**, you can add additional actions (see screenshot [1](#)).
 - **Deny** — user will be redirected to the firewall page with information that access is denied.
In the **Properties**, you can add information about forbidden pages and you can check **Users can unlock this rule**. All unlocked pages are logged in the Security log.
 - **Drop** — access is denied and the user will see the page as unavailable.
 - **Redirect** — user will be automatically redirected to the specified URL (see screenshot [1](#)).
5. Double-click **URL** and set:
 - **Site** — any URL starting with the specified string. It is possible to use wildcards * (asterisk) and ? (question mark).
Example: Blocking rule for *.kerio.com blocks access to http://www.kerio.com/, http://mail.kerio.com/ and http://kerio.com/, yet not to http://www.mykerio.com/ or http://mykerio.com/.
 - **URL from the group** — you can select from existing groups or you can go to Definitions → URL Groups and add a new one (see section [??](#)).
 - **URL rated by Kerio Control Web Filter rating system** — all pages sorted in the selected categories by the Kerio Control Web Filter module.
 - **Any URL where server is specified by an IP address** — this can be used only for unsecured traffic (HTTP).
 - **Also apply to secured connections (HTTPS)** — Kerio Control will apply the domain part of the defined URL to this rule for secure websites.

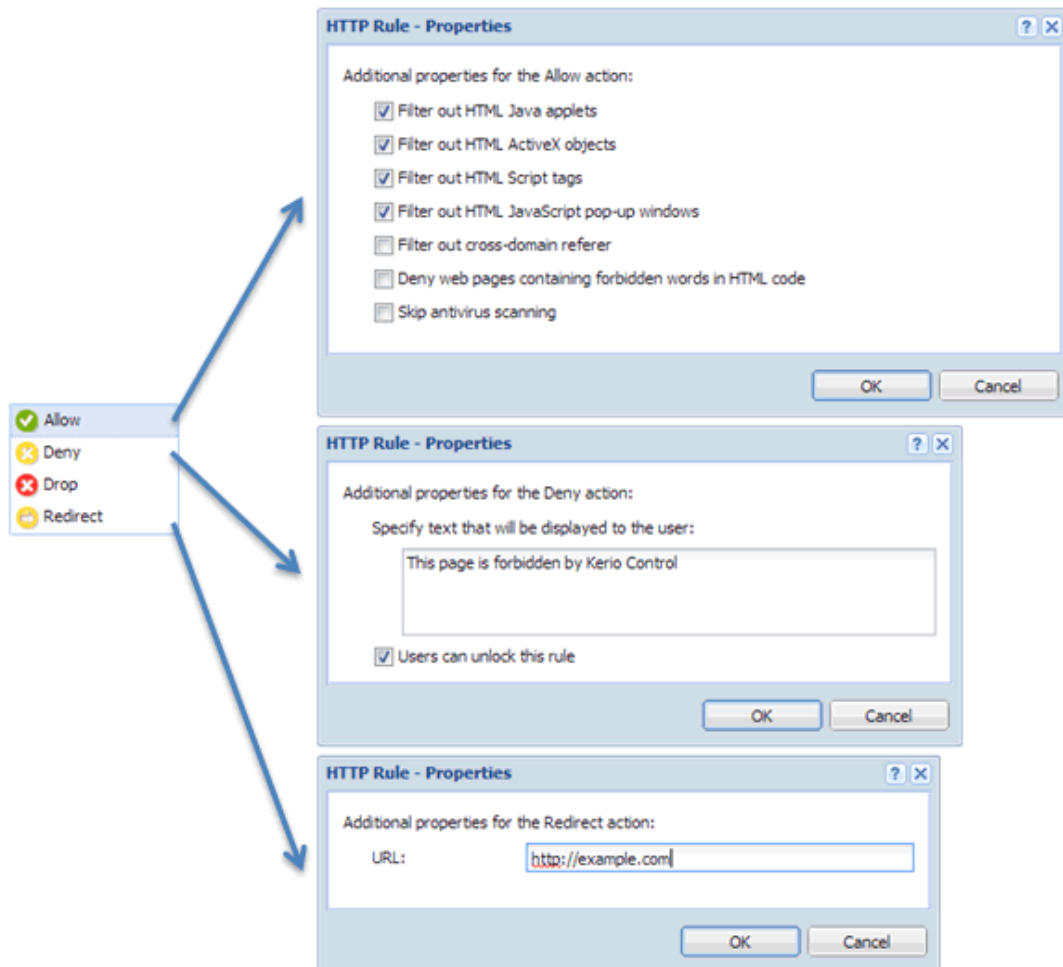


Figure 1 Action / Properties



For technical reasons, it is not possible to apply HTTPS blocking to clients using Internet Explorer on Windows XP.

6. Double-click **Users** and decide to whom the rule will apply.
7. Double-click **MIME Type** and select one option.
MIME type of downloaded files. It is possible to use wildcard * (asterisk) for any MIME type.
8. Double-click **Source** and select an IP address group.
You can create a new IP address group in **Definitions** → **IP address Groups**.
9. Double-click **Valid Time** and select a time range.
You can create a new time range in **Definitions** → **Time Ranges**.

10. Check **Log**.

Logging of all HTTP queries matching this rule in the **Filter** log.

11. Click **Apply**.

Rules are tested from the top of the list downwards. If a requested URL passes through all rules without any match, access to the site is allowed.



URLs which do not match with any URL rule are available for any authenticated user (any traffic permitted by default). To reverse this policy, a rule denying access to any URL must be placed at the end of the rule list.

Applying rules also for local servers

HTTP rules can be applied to local WWW servers which are available from the Internet:

1. In the administration interface, go to **HTTP Policy**.
2. Check **Apply filtering rules also for local servers** placed at the bottom of the page.
3. Click **Apply**.

URL Groups

URL Groups enable the administrator to define HTTP rules. For example, to disable access to a group of web pages, you can define a URL group and assign permissions to the URL group, rather than defining permissions to each individual URL rule. A URL group rule is processed faster than a greater number of separate rules for individual URLs.

The default Kerio Control installation already includes predefined URL groups:

- **Ads/Banners** — common URLs of pages that contain advertisements, banners, etc.
- **Search engines** — top Internet search engines.
- **Windows Updates** — URL of pages requested for automatic updates of Windows.



These URL groups are used in predefined URL rules.

Defining a new URL group

1. In the administration interface, go to **Definitions** → **URL Groups**
2. Click **Add**.
3. Type a name for the group.
4. In **Type**, select **URL**.

URL can be specified as follows:

- full address of a server, a document or a web page without protocol specification (http://),
- use substrings with the special * and ? characters. An asterisk stands for any number of characters, a question-mark represents one character.

Examples:

- `www.example.com/index.html` — a particular page
- `www.*` — all URL addresses starting with `www.`
- `*sex*` — all URL addresses containing the `sex` string
- `*sex??.cz*` — all URL addresses containing such strings as `sexxx.cz`, `sex99.cz`, etc.

5. Save the settings.

You can use the URL group in URL rules.

Configuring HTTP cache

HTTP cache overview

Using cache to access web pages that are opened repeatedly reduces Internet traffic. Downloaded files are saved to the hard drive of the *Kerio Control* host so that it is not necessary to download them from the web server again later.



HTTP cache is not available on Kerio Control Box.

The cache can be used either for direct access or for access via the proxy server. If you use direct access, the HTTP protocol inspector must be applied to the traffic. In the default configuration of Kerio Control, this condition is met for the HTTP protocol at the default port 80.

Configuring a HTTP cache

1. In the administration interface, go to **HTTP Policy** → **Cache**.
2. Check **Enable cache for direct access to web**.
3. If you are using proxy server, check **Enable cache on Kerio Control non-transparent proxy server**.
4. Click **Apply**.

Configuring TTL

TTL (Time To Live) means that you can configure a default time of how long the object is kept in the cache for.

1. On tab **Cache**, set HTTP protocol TTL (default value: 1 day).
This setting applies to all objects with no extra cache period is specified.
2. Click **URL Specific Settings** for objects on specific servers or pages.
3. In the **URL Specific Settings** dialog, click **Add**.
4. In the **Add URL** dialog, specify URL (or its part) of objects on which the rule will apply. The cache time is specified in hours. Value 0 means that the object will not be kept in the cache.

Configuring HTTP cache

Configuring cache size

Maximal cache size allowed is *2 GB (2047 MB)*. However tests in field prove that with size larger than *1 GB (1024 MB)*, the speed of object search and thus the efficiency of the cache decreases significantly. Therefore, it is not recommended to create cache larger than *1 GB*.

The cache is located in the `cache` subdirectory of the Kerio Control's head directory, i.e.:

`/opt/kerio/winroute/cache`

It is necessary that there is enough free space on the particular drive or to change cache size according to the free disk space. If the maximum cache size set is larger than the free space on the corresponding disk, the cache is not initialized and the following error is recorded in the **Error** log.



Clients can always require a check for updates from the web server (regardless of the cache settings). Use combination of the *Ctrl+F5* to do this using either the Internet Explorer or the Firefox/SeaMonkey browser. You can set browsers so that they will check for updates automatically whenever a certain page is opened (then you will only refresh the particular page).

Cache status and administration

Kerio Control allows monitoring of the HTTP cache usage as well as removal of its contents.

At the bottom of the **Cache** tab, basic status information is provided such as the current cache size occupied and efficiency of the cache. The efficiency status stands for number of objects kept in the cache in proportion to the total number of queries (since the startup of the Kerio Control Engine). The efficiency of the cache depends especially on user behavior and habits (if users visit certain web pages regularly, if any websites are accessed by multiple users, etc.) and, in a manner, it can be also affected by the configuration parameters described above. If the efficiency of the cache is permanently low (less than 5 percent), change the cache configuration.

The **Clear cache** button deletes all objects saved in cache.

Proxy server

Proxy Server overview

Even though the NAT technology used in Kerio Control enables direct access to the Internet from all local hosts, it contains a standard HTTP proxy server. Under certain conditions the direct access cannot be used or it is inconvenient . The following list describes the most common situations:

1. To connect from the Kerio Control host it is necessary to use the proxy server of your ISP.
Proxy server included in Kerio Control can forward all queries to so called *parent proxy server*).
2. Internet connection is performed via a dial-up and access to certain Web pages is blocked. If a direct connection is used, the line will be dialed before the HTTP query could be detected (line is dialed upon a DNS query or upon a client's request demanding connection to a Web server). If a user connects to a forbidden web page, Kerio Control dials the line and blocks access to the page — the line is dialed but the page is not opened.
Proxy server can receive and process clients' queries locally. The line will not be dialed if access to the requested page is forbidden.
3. Kerio Control is deployed within a network with many hosts where proxy server has been used. It would be too complex and time-consuming to re-configure all the hosts.
The Internet connection functionality is kept if proxy server is used — it is not necessary to edit configuration of individual hosts (or only some hosts should be re-configured).

The Kerio Control's proxy server can be used for HTTP, HTTPS and FTP protocols. Proxy server does not support the SOCKS protocol (a special protocol used for communication between the client and the proxy server).



For detailed information on using FTP on the Kerio Control's proxy server.

Proxy Server Configuration

To configure proxy server parameters open the **Proxy server** tab in **HTTP Policy**.

Enable non-transparent proxy server

This option enables the HTTP proxy server in Kerio Control on the port inserted in the **Port** entry (3128 port is set by the default).



If you use a port number that is already used by another service or application, Kerio Control will accept this port, however, the proxy server will not be able to run and the following report will be logged into the **Error** log:

failed to bind to port 3128: another application is using this port

If you are not sure that the port you intend to use is free, click on the **Apply** button and check the **Error** log (check whether the report has or has not been logged) immediately.

Enable tunneled connections to any TCP port

This security option enables to allow or block so called tunneling of other application protocols (than HTTP, HTTPS and FTP) via the proxy server (secured HTTPS connection). If this option is disabled, the proxy server allows to establish HTTPS connection only to the standard HTTPS port 443) — it is supposed that secured web pages are being opened. If the option is enabled, the proxy server can establish connection to any port. It can be a non-standard HTTPS port or tunneling of another application protocol.



This option does not affect the non-secured traffic performed by HTTP and/or FTP. In Kerio Control, HTTP traffic is controlled by a protocol inspectors which allows only valid HTTP and FTP queries.

Forward to parent proxy server

Tick this option for Kerio Control to forward all queries to the parent proxy server which will be specified by the following data:

- **Server** — DNS name or IP address of parent proxy server and the port on which the server is running (3128 port is used by the default).
- **Parent proxy server requires authentication** — enable this option if authentication by username and password is required by the parent proxy server. Specify the **Username** and **Password** login data.



The name and password for authentication to the parent proxy server is sent with each HTTP request. Only *Basic* authentication is supported.

The **Forward to parent proxy server** option specifies how Kerio Control will connect to the Internet (for update checks, downloads of *Sophos* updates and for connecting to the online Kerio Control Web Filter databases).

Set automatic proxy configuration script to...

If a proxy server is used, Web browsers on client hosts must be configured correctly. Most common web browsers (e.g. *Internet Explorer*, *Firefox/SeaMonkey*, *Google Chrome*, etc.) enable automatic configuration of corresponding parameters by using a script downloaded from a corresponding website specified by URL.

In the case of *Kerio Control*'s proxy server, the configuration script is saved at

`http://192.168.1.1:3128/pac/proxy.pac`

where 192.168.1.1 is the IP address of the Kerio Control host and number 3128 represents the port of the proxy server (see above).

The **Allow browsers to use configuration script automatically...** option adjusts the configuration script in accord with the current *Kerio Control* configuration and the settings of the local network:

- **Direct access** — no proxy server will be used by browsers
- **Kerio Control proxy server** — IP address of the Kerio Control host and the port on which the proxy server is running will be used by the browser (see above).



The configuration script requires that the proxy server is always available (even if the **Direct access** option is used).

Allow browsers to use configuration script automatically...

It is possible to let *Internet Explorer* be configured automatically by the DHCP server. To set this, enable the **Automatically detect settings** option.

Application of this function is conditioned by the running Kerio Control DHCP server. TCP/IP parameters at the host can be static — *Internet Explorer* sends a special DHCP query when started.

Hint

This method enables to configure all *Internet Explorer* browsers at all local hosts by a single click.

Filtering web content by word occurrence

Kerio Control word filter overview

Kerio Control filters web pages that include undesirable words.

Filtering mechanism: Denied words are matched with values, called weight (represented by a whole positive integer). Weights of these words contained in a required page are summed (weight of each word is counted only once regardless of how many times the word is included in the page). If the total weight exceeds the defined limit (so called threshold value), the page is blocked.



So called forbidden words are used to filter out web pages containing undesirable words. [URL rules](#) define how pages including forbidden content will be handled. Definition of forbidden words and threshold value is ineffective unless corresponding URL rules are set.

Adding a new forbidden word

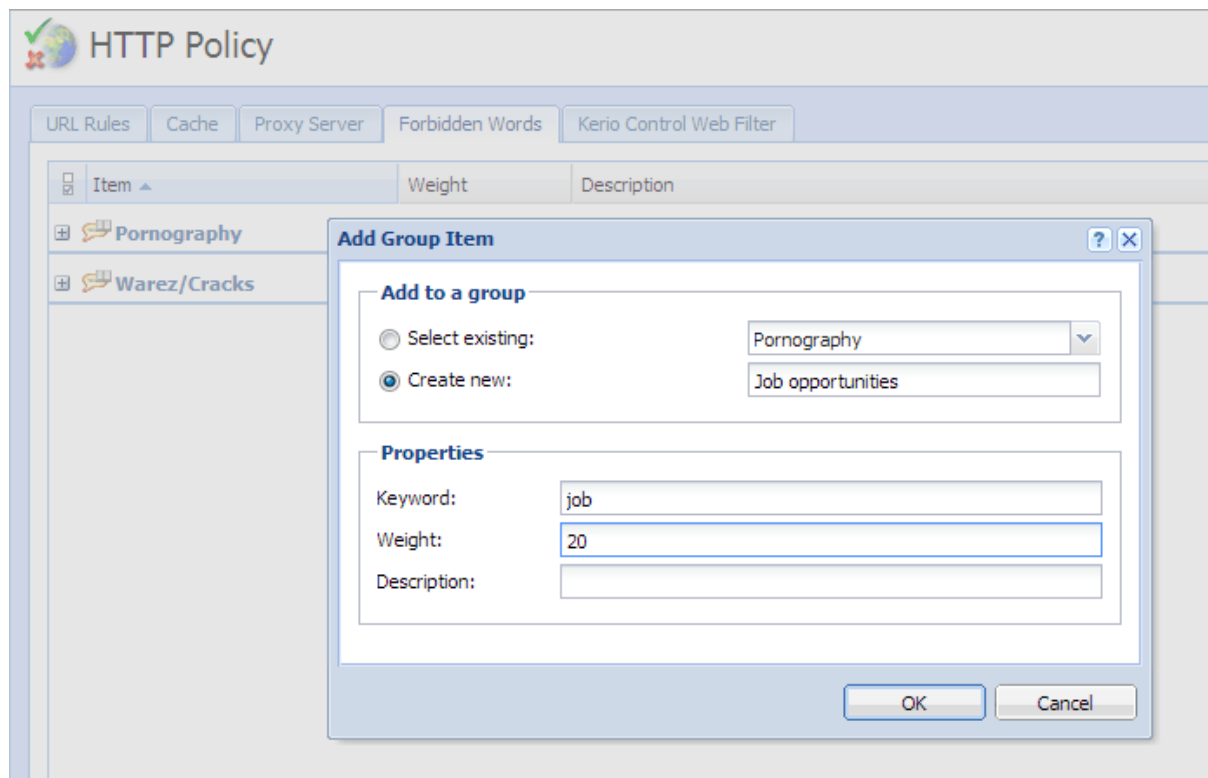


Figure 1 Adding forbidden words

1. In the administration interface, go to **HTTP Policy → Forbidden Words**.

2. Click **Add**.

3. You can select an existing group or create a new one (see screenshot [1](#)).

Words are sorted into groups. However, all groups have the same priority and all of them are always tested.

4. Type a keyword that is to be scanned for.

This word can be in any language and it should follow the exact form in which it is used on websites (including diacritics and other special symbols and characters). If the word has various forms (declension, conjugation, etc.), it is necessary to define separate words for each word in the group.

5. Type a weight.

The weight should respect frequency of the particular word (the more common word, the lower weight) so that legitimate webpages are not blocked.

6. Click **OK**.

Defining a URL rule filtering by word occurrence

The usage will be better understood through the following example that describes a rule denying all users to access pages if their weight was reached:

1. In the administration interface, go to **HTTP Policy → URL Rules**.

2. Click **Add**.

3. Type a name of the rule.

4. Double-click **Action** and select **Allow**.

5. Double-click **Properties** and select **Deny web pages containing forbidden words in HTML code**.

6. Double-click **URL** and type a site which will be filtered by forbidden words.

7. Double-click **Users** and select **any user + do not require authentication**.

8. Click **Apply**.

URL Rules are described in more details in a special article: [Configuring HTTP policy](#).

Using Kerio Control Web Filter

Kerio Control Web Filter overview

Kerio Control Web Filter rates web page content. For this purpose it uses a dynamic worldwide database which includes URLs and classification of web pages.

Whenever a user attempts to access a web page, Kerio Control sends a request on the page rating. According to the classification of the page the user will be either allowed or denied to access the page.



A special license is required with Kerio Control Web Filter. Unless Kerio Control includes this module, it behaves as a trial version only (this means that it is automatically disabled after 30 days from the Kerio Control installation and options in the Kerio Control Web Filter tab will not be available).

Enabling Kerio Control Web Filter

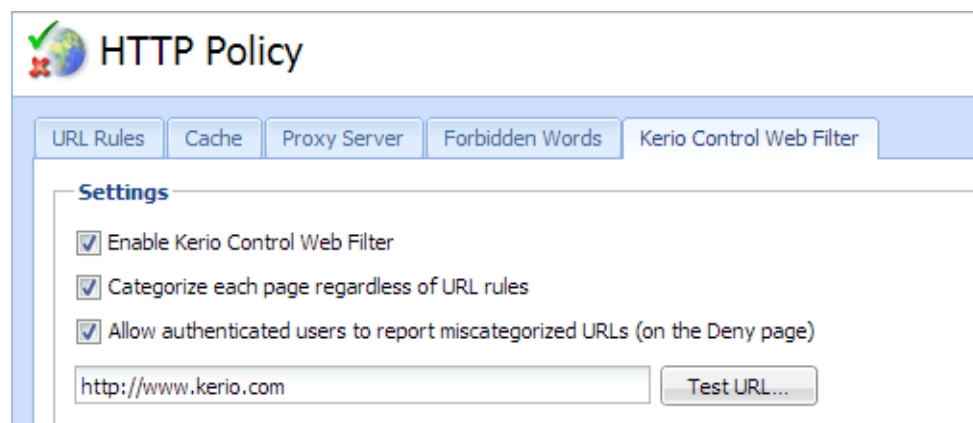


Figure 1 Kerio Control Web Filter

1. In the administration interface, go to **HTTP Policy**.
2. On tab **Kerio Control Web Filter**, check **Enable Kerio Control Web Filter**.
3. Check **Categorize each page regardless of URL rules**.

Categorization of all pages is necessary for statistics of the categories of visited web pages. If you do not intend to keep these statistics, disable this option (categorization of all web pages might be demanding and it might decrease Kerio Control performance).

4. Check **Allow authenticated users to report miscategorized URLs**

If the user believes that the page has been added to a wrong category (which makes Kerio Control block access to the page), they can suggest a change. The database administrator will then evaluate the suggestion within a few days. All suggestions are logged in the **Security** log.

5. Click **Apply**.

Testing URLs

In the administration interface, it is possible to test URL categorization. It is then possible to make recategorization suggestions on the result page, if desired.

1. In section **HTTP Policy**, go to **Kerio Control Web Filter**.
2. Type the URL to the blank field (see screenshot [1](#)) and click **Test URL**.
3. In the **URL Categorization** dialog, check if the category is correct.

Creating a URL whitelist

If Kerio Control Web Filter blocks correct URL, you can add it to the special list of enabled URLs:

1. In section **HTTP Policy**, go to **Kerio Control Web Filter**.
2. Click **Add**.
3. Type URL and description of the website. The following items can be specified:
 - server name (e.g. `www.kerio.com`). Server name represents any URL at a corresponding server,
 - address of a particular webpage (e.g. `www.kerio.com/index.html`),
 - URL using wildcard matching (e.g. `*.ker?o.*`). An asterisk stands for any number of characters (even zero), a `*.ker?o.*` question-mark represents just one symbol.
4. Save the settings.

Using Web Filter in URL rules

Whenever Kerio Control processes a URL rule that requires classification of pages, Kerio Control Web Filter is activated. The usage will be better understood through the following example that describes a rule denying all users to access pages containing job offers:

1. In the administration interface, go to **HTTP Policy**.
2. On tab **URL Rules**, enable the predefined rule **Deny sites rated in Kerio Control Web Filter Categories**.

Using Kerio Control Web Filter

3. Double-click the **URL** column and click **Select rating**.
4. Select the **Job Search** rating category.
5. Click **Apply**.



We recommend you to unlock rules that use the Kerio Control Web Filter rating system (the **Users can unlock this rule** option in the **Properties** column). This option will allow users to unlock pages blocked for incorrect classification. All unlock queries are logged into the **Filter** log.

URL Rules are described in more details in a special article: [Configuring HTTP policy](#).

Antivirus protection

Antivirus overview

Kerio Control provides antivirus check of objects (files) transmitted by HTTP, FTP, SMTP and POP3 protocols. In case of HTTP and FTP protocols, the firewall administrator can specify which types of objects will be scanned.

Kerio Control is distributed with the integrated Sophos antivirus. Use of the antivirus requires a special license.

Conditions and limitations of antivirus scan

Antivirus check of objects transferred by a particular protocol can be applied only to traffic where a corresponding protocol inspector which supports the antivirus is used. This implies that the antivirus check is limited by the following factors:

- Antivirus check cannot be used if the traffic is transferred by a secured channel (SSL/TLS). In such a case, it is not possible to decipher traffic and separate transferred objects.
- Within email antivirus scanning (SMTP and POP3 protocols), the firewall only removes infected attachments — it is not possible to drop entire email messages. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Check of outgoing traffic causes problems with temporarily undeliverable email.
- Object transferred by other than HTTP, FTP, SMTP and POP3 protocols cannot be checked by an antivirus.
- If a substandard port is used for the traffic, corresponding protocol inspector will not be applied automatically. In that case, simply define a traffic rule which will allow this traffic using a corresponding protocol inspector.

Example: You want to perform antivirus checks of the HTTP protocol at port 8080.

1. Define the *HTTP 8080* service (TCP protocol, port 8080).
2. Create a traffic rule which will allow this service applying a corresponding protocol inspector.

Antivirus protection

Name	Source	Destination	Service	Action	Inspector
<input checked="" type="checkbox"/> HTTP 8080 with inspection	Trusted/Local interfaces	Internet interfaces	HTTP 8080	Allow	HTTP

Figure 1 Traffic rule for HTTP protocol inspection at non-standard ports

Add the new rule before the rule allowing access to any service in the Internet (if such a rule exists). If the NAT (source address translation) technology is used for Internet connection, address translation must be set for this rule as well.



A corresponding protocol inspector can be also specified within the service definition, or both definition methods can be used. Both methods yield the same result, however, the corresponding traffic rule is more transparent when the protocol inspector is defined in it.

Antivirus scan setup

Parameters of the antivirus scan in Kerio Control can be set in **Antivirus**.

Integrated antivirus configuration

To enable the integrated *Sophos* antivirus, enable **Use the integrated Sophos antivirus engine** in the **Antivirus Engine** tab. This option is not available unless the license key for *Kerio Control* includes a license for the *Sophos* antivirus module or in trial versions. For detailed information about the licensing policy.

Use the **Integrated antivirus engine** section in the **Antivirus Engine** tab to set update parameters for *Sophos*.

Check for update every ... hours

Time interval of checks for new updates of the virus database and the antivirus engine (in hours).

If any new update is available, it will be downloaded automatically by Kerio Control.

If the update attempt fails (i.e. the server is not available), detailed information about the attempt will be logged into the **Error** log.

Each download (update) attempt sets the **Last update check performed** value to zero.



To make the antivirus control as mighty as possible, it is necessary that the antivirus module is always equipped by the most recent version of the virus database. Therefore, it is recommended to keep automatic updates running and not to set too long intervals between update checks (update checks should be performed at least twice a day).

Current virus database is

Information regarding the age of the current database.



If the value is too high, this may indicate that updates of the database have failed several times. In such cases, we recommend you to perform a manual update check by the **Update now** button and view the **Error** log.

Last update check performed

Time that has passed since the last update check.

Virus database version

Database version that is currently used.

Scanning engine version

Sophos scanning engine version used by *Kerio Control*.

Update

Use this button for immediate update of the virus database and of the scanning engine.

After you run the update check using the **Update now...** button, an informational window displaying the update check process will be opened. You can use the **OK** button to close it — it is not necessary to wait until the update is finished.

If updated successfully, the version number of the new virus database or/and the new antivirus version(s), as well as information regarding the age of the current virus database will be displayed. If the update check fails (i.e. the server is not available), an error will be reported and detailed information about the update attempt will be logged into the **Error** log.

Each download (update) attempt sets the **Last update check performed** value to zero.

Parameters for protocol and file scanning

Check items in the **Settings** section of the **Antivirus** tab to enable antivirus check for individual application protocols. By default, antivirus check is enabled for all supported modules.

In **Settings**, maximum size of files to be scanned for viruses at the firewall can be set. Scanning of large files are demanding for time, the processor and free disk space, which might affect the firewall's functionality dramatically. It might happen that the connection over which the file is transferred is interrupted when the time limit is exceeded.

The optimal value of the file size depends on particular conditions (the server's performance, load on the network, type of the data transmitted, etc.). *Caution! We strongly discourage administrators from changing the default value for file size limit. In any case, do not set the value to more than 4 MB.*

Parameters for HTTP and FTP scanning can be set in the **HTTP and FTP scanning**, while SMTP and POP3 scanning can be configured in the **Email scanning** tab.



1. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (from the local network to the Internet) might cause problems with temporarily undeliverable email — for example in cases where the destination SMTP server uses so called *greylisting*.

To perform smooth checks of outgoing traffic, define a corresponding traffic rule using the SMTP protocol inspector. Such rule may be useful for example if clients in the local network send their email via an SMTP server located in the Internet. Checking of outgoing SMTP traffic is not apt for local SMTP servers sending email to the Internet. An example of a traffic rule for checking of outgoing SMTP traffic is shown at figure 2.





Name	Source	Destination	Service	Action	Inspector	Translation
<input checked="" type="checkbox"/> Outgoing SMTP	 Trusted/Local interfaces	 Internet interfaces	 SMTP	 Allow	SMTP	NAT Balancing per host

Figure 2 An example of a traffic rule for outgoing SMTP traffic check

2. Non-standard extensions of the SMTP protocol can be used in case of communication of two *Microsoft Exchange* mailservers. Under certain conditions, email messages are transmitted in form of binary data. In such a case, Kerio Control cannot perform antivirus check of individual attachments.

In such cases, it is recommended to use an antivirus which supports *Microsoft Exchange* and not to perform antivirus check of SMTP traffic of a particular server in Kerio Control. To achieve this, disable antivirus check for SMTP protocol or define a corresponding traffic rule where no protocol inspector will be applied.

HTTP and FTP scanning

As for HTTP and FTP traffic, objects (files) of selected types are scanned.

The file just transmitted is saved in a temporary file on the local disk of the firewall. *Kerio Control* caches the last part of the transmitted file (segment of the data transferred) and performs an antivirus scan of the temporary file. If a virus is detected in the file, the last segment of the data is dropped. This means that the client receives an incomplete (damaged) file which cannot be executed so that the virus cannot be activated. If no virus is found, *Kerio Control* sends the client the rest of the file and the transmission is completed successfully.

Optionally, a warning message informing about a virus detected can be sent to the user who tried to download the file (see the **Notify user by email** option).



1. The purpose of the antivirus check is only to detect infected files, it is not possible to heal them!
2. If the antivirus check is disabled in HTTP and FTP filtering rules, objects and files matching corresponding rules are not checked.
3. Full functionality of HTTP scanning is not guaranteed if any non-standard extensions to web browsers (e.g. download managers, accelerators, etc.) are used!

To set parameters of HTTP and FTP antivirus check, open the **HTTP, FTP scanning** tab in **Configuration** → **Content Filtering** → **Antivirus**.

Use the **If avirus is found...** entry to specify actions to be taken whenever a virus is detected in a transmitted file:

- **Move the file to quarantine** — the file will be saved in a special directory on the firewall. *Kerio Control* administrators can later try to heal the file using an antivirus program and if the file is recovered successfully, the administrator can provide it to the user who attempted to download it.

The quarantine subdirectory under the *Kerio Control* installation directory is used for the quarantine:

```
/opt/kerio/winroute/quarantine
```

Infected files (files which are suspected of being infected) are saved into this directory with names which are generated automatically. Name of each file includes information about protocol, date, time and connection number used for the transmission.



When handling files in the quarantine directory, please consider carefully each action you take, otherwise a virus might be activated and the *Kerio Control* host could be attacked by the virus!

- **Alert the client** — *Kerio Control* alerts the user who attempted to download the file by an email message warning that a virus was detected and download was stopped for security reasons.

Kerio Control sends alert messages under the following circumstances: The user is authenticated and connected to the firewall, a valid email address is set in a corresponding user account and the SMTP server used for mail sending is configured correctly.



Regardless of the fact whether the *Alert the client* option is used, alerts can be sent to specified addresses (e.g. addresses of network administrators) whenever a virus is detected.

In the **If the transferred file cannot be scanned** section, actions to be taken when the antivirus check cannot be applied to a file (e.g. the file is compressed and password-protected, damaged, etc.):

- **Deny transmission of the file** — *Kerio Control* will consider these files as infected and deny their transmission.

Hint

It is recommended to combine this option with the **Move the file to quarantine** function — the firewall administrator can extract the file and perform manual antivirus check in response to user requests.

- **Allow the file to be transferred** — *Kerio Control* will treat compressed password-protected files and damaged files as trustful (not infected).

Generally, use of this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files and the antivirus is installed on the workstations.

HTTP and FTP scanning rules

These rules specify when antivirus check will be applied. By default (if no rule is defined), all objects transmitted by HTTP and FTP are scanned.

Kerio Control contains a set of predefined rules for HTTP and FTP scanning. By default, all executable files as well as all *Microsoft Office* files are scanned. The firewall administrator can change the default configuration.

Scanning rules are ordered in a list and processed from the top. Arrow buttons on the right can be used to change the order. When a rule which matches the object is found, the appropriate action is taken and rule processing is stopped.

New rules can be created in the dialog box which is opened after clicking the **Add** button.

Description

Comment on the rule (for use of the firewall administrator).

Condition

Condition of the rule:

- **HTTP/FTP filename**
 - this option filters out certain filenames (not entire URLs) transmitted by FTP or HTTP (e.g. *.exe, *.zip, etc.).

If only an asterisk is used for the specification, the rule will apply to any file transmitted by HTTP or FTP.

The other two conditions can be applied only to HTTP:

- **MIME type**
 - MIME types can be specified either by complete expressions (e.g. `image/jpeg`) or using a wildcard matching (e.g. `application/*`).
- **URL** — URL of the object (e.g. `www.kerio.com/img/logo.gif`), a string specified by a wildcard matching (e.g. `*.exe`) or a server name (e.g. `www.kerio.com`). Server names represent any URL at a corresponding server (`www.kerio.com/*`).

If a MIME type or a URL is specified only by an asterisk, the rule will apply to any HTTP object.

Actions

Settings in this section define whether or not the object will be scanned by the antivirus. If the **Do not scan** alternative is selected, antivirus control will not apply to transmission of this object.

The new rule will be added after the rule which had been selected before **Add** was clicked. You can use the arrow buttons on the right to move the rule within the list.

Checking the box next to the rule can be used to disable the rule. Rules can be disabled temporarily so that it is not necessary to remove rules and create identical ones later.

If the object does not match any rule, it will be scanned automatically. If only selected object types are to be scanned, a rule disabling scanning of any URL or MIME type must be added to the end of the list (the **Skip all other files** rule is predefined for this purpose).

Email scanning

SMTP and POP3 protocols scanning settings are defined through this tab. If scanning is enabled for at least one of these protocols, all attachments of transmitted messages are scanned.

Individual attachments of transmitted messages are saved in a temporary directory on the local disk. When downloaded completely, the files are scanned for viruses. If no virus is found, the attachment is added to the message again. If a virus is detected, the attachment is replaced by a notice informing about the virus found.



Warning messages can also be sent to specified email addresses (e.g. to network administrators) when a virus is detected.



1. Email antivirus control can only detect and block infected attachments. Attached files cannot be healed by this control!
2. Within antivirus scanning, it is possible to remove only infected attachments, entire email messages cannot be dropped. This is caused by the fact that the firewall cannot handle email messages like mailservers do. It only maintains network traffic coming through. In most cases, removal of an entire message would lead to a failure in communication with the server and the client might attempt to send/download the message once again. Thus, one infected message might block sending/reception of any other (legitimate) mail.
3. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (i.e. from the local network to the Internet) might cause problems with temporarily undeliverable email (for example in cases where the destination SMTP server uses so called *greylisting*).
To check also outgoing traffic (e.g. when local clients connect to an SMTP server without the local network), define a corresponding traffic rule using the SMTP protocol inspector.

Advanced parameters and actions that will be taken when a virus is detected can be set in the **Email scanning** tab.

In the **Specify an action which will be taken with attachments...** section, the following actions can be set for messages considered by the antivirus as infected:

- **Save message to quarantine** — untrustworthy messages will be moved to a special directory on the *Kerio Control* host. The *Kerio Control* administrator can try to heal infected files and later send them to their original addressees.

The quarantine subdirectory under the *Kerio Control* installation directory is used for the quarantine:

In other editions: `/opt/kerio/winroute/quarantine`

Messages carrying infected attached files (files which are suspected of being infected) are saved into this directory with names which are generated automatically. Each filename includes information about protocol, date, time and the connection number used for transmission of the message.

- **Prepend subject message with text** — use this option to specify a text to be attached before the subject of each email message where at least one infected attachment is found. This text informs the recipient of the message and it can be also used for automatic message filtering.



Regardless of what action is set to be taken, the attachment is always removed and a warning message is attached instead.

Use the **TLS connections** section to set firewall behavior for cases where both mail client and the server support TLS-secured SMTP or POP3 traffic.

In case that TLS protocol is used, unencrypted connection is established first. Then, client and server agree on switching to the secure mode (encrypted connection). If the client or the server does not support TLS, encrypted connection is not used and the traffic is performed in a non-secured way.

If the connection is encrypted, firewall cannot analyze it and perform antivirus check for transmitted messages. The firewall administrator can select one of the following alternatives:

- **Enable TLS.** This alternative is suitable for such cases where protection from wiretapping is prior to antivirus check of email.

Hint

In such cases, it is recommended to install an antivirus engine at individual hosts that would perform local antivirus check.

- **Disable TLS.** Secure mode will not be available. Clients will automatically assume that the server does not support TLS and messages will be transmitted through an unencrypted connection. Firewall will perform antivirus check for all transmitted mail.

The **If an attachment cannot be scanned** section defines actions to be taken if one or multiple files attached to a message cannot be scanned for any reason (e.g. password-protected archives, damaged files, etc.):

- **Reject the attachment** — *Kerio Control* reacts in the same way as when a virus was detected (including all the actions described above).
- **Allow delivery of the attachment** — *Kerio Control* behaves as if password-protected or damaged files were not infected.

Generally, this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files (typically password-protected archives) and the antivirus is installed on the workstations.

Using DHCP module

Why to use DHCP server in Kerio Control

Kerio Control includes a **DHCP** server. The DHCP server assigns clients IP addresses within a predefined scope for a certain period (lease time). If an IP address is to be kept, the client must request an extension on the period of time before the lease expires. If the client has not required an extension on the lease time, the IP address is considered free and can be assigned to another client. This is performed automatically and transparently.

So called reservations can be also defined on the DHCP server — certain clients will have their own IP addresses reserved. Addresses can be reserved for a hardware address (MAC) or a host name. These clients will have fixed IP address. These addresses are configured automatically.

Kerio Control also allows automatic configuration of the DHCP server. This option involves automatic creation and updates of IP address ranges and parameters in accordance with network interfaces included in group **Trusted/Local Interfaces**. This implies that the only thing to do is actually to run the DHCP server.

Automatic configuration of IP scopes

By default, the DHCP server works in the mode of automatic configuration of IP scopes. Kerio Control detects parameters of network interfaces included in group **Trusted/Local Interfaces** and uses them to generate and update IP scopes for the corresponding subnets. Whenever an interface is changed, the DHCP server's configuration will be updated automatically.

1. In the administration interface, go to **DHCP Server**.
2. Select option **Enable DHCP server**.
3. Click **Apply**.

For each interface's subnet, a scope of the following parameters will be created:

- *Range* — by IP address of the interface and the corresponding subnet mask.
The range should cover the particular subnet with free resources for assigned static addresses (e.g. for mask 255.255.255.0, the range from x.x.x.11 to x.x.x.254 will be created). If an interface's address is covered by a range, then an exception is automatically defined for it.
- *Subnet mask* — according to the particular interface.
- *Default gateway* — IP address of the particular interface.
- *DNS server* — IP address of the particular interface.

Manual definition of Scopes and Reservations

If you do not want to use the automatic configuration of IP ranges, you can switch to the manual mode. However, bear in mind that changes of interfaces in group **Trusted/Local Interfaces** (e.g. adding of a new interface, change of IP address, etc.) require manual update of address scopes defined in the DHCP server.

Only one scope can be defined for each IP subnet.



In the administration interface, it is also possible to use a scope template where parameters are already predefined in accordance with the particular firewall's interface. For details, see above, section *Automatic configuration of IP scopes*.

1. In the administration interface, go to **DHCP Server**.
2. Click on the **Click to configure scopes manually** link and confirm the change.
3. Click **Add → Manual**.



You can use **Add → Use Interface Template**, where parameters are already predefined in accordance with the particular firewall's interface.

4. In the **Add Scope** dialog, type a name of the new scope.
5. Define the first and the last address of the scope.



If possible, define the scope larger than it would be defined for the real number of users within the subnet.

6. Type a mask of the appropriate subnet.
7. In table **DHCP Options**, click **Add**.
8. Select option **003: Default Gateway** and type an IP address. Save it.
9. Select option **006: DNS server** and type an IP address where Kerio Control is running.

You can type any DNS server (or more DNS servers separated with semicolons). However, it is recommended to use the Kerio Control host's IP address as the primary DNS server (i.e. at the top). The DNS module can cooperate with DHCP server so that it will always use correct IP addresses to response to requests on local host names.



DHCP protocol enables adding several optional parameters, such as:

- **015: Domain name** — local Internet domain (not to be used for specification of Windows NT domain name).
- **066: TFTP server name** — name or IP address of a TFTP server. TFTP protocol is used by [Kerio Operator](#) to autoconfigure telephones.

10. Save the DHCP parameter.
11. [To create more individual scopes, click Exclusions.](#)
12. Save the settings.
13. If you need other scopes, repeat this procedure from step 3.
14. Select option **Enable DHCP server**.

Defining individual scopes

Kerio Control enables the administrator to define only one scope in within each subnet. To create more individual scopes, follow these instructions:

- create address scope covering all desired scopes [manually](#)
- define so called exclusions that will not be assigned:
 1. In the **Add Scope** dialog, click **Exclusions**.
 2. In the **Exclusions**, click **Add**.
 3. Add **From** and **To** IP addresses.

Example

In 192.168.1.0 subnet you intend to create two scopes: from 192.168.1.10 to 192.168.1.49 and from 192.168.1.61 to 192.168.1.100. Addresses from 192.168.1.50 to 192.168.1.60 will be left free and can be used for other purposes.

Create the scope from 192.168.1.10 to 192.168.1.100 and click on the **Exclusions** button to define the scope from 192.168.1.50 to 192.168.1.60. These addresses will not be assigned by the DHCP server.

Leases and Reservations

IP scopes can be viewed in the **Leases and reservations** table.

Using the **Remove** button you can release the selected IP address and/or cancel IP address reservation on the spot. *DHCPRELEASE* control message will be sent to the corresponding client.

Reserving an IP address

DHCP server enables you to book an IP address for any host or MAC address. Reservations can be set in both scope configuration modes, manual and automatic. The act of adding a reservation in the automatic mode does not switch to manual mode.

Any IP address included in a defined subnet can be reserved. This address can but does not have to belong to the scope of addresses dynamically leased, and it can also belong to any scope used for exceptions.

Adding reservations

1. In the administration interface, go to **DHCP Server**.
2. In the **Leases and reservations** table, click **Add** → **Add Reservation**.
3. Type a name of the reservation.
4. Select MAC address or hostname for device identification and type the identification.
5. Type a reserved IP address.
6. Click **OK**.

If you want to check your settings, icons marked with R represent reserved addresses.

Reserving leases

1. In the administration interface, go to **DHCP Server**.
2. In the **Leases and reservations** table and click (highlight) the desired device with leased address.
3. Click **Add** → **Reserve lease**.
4. In the dialog, click **OK**.

If you want to check your settings, in the **Status** column appears **Reserved**, **Leased**.

Using the DNS module

DNS forwarding service in Kerio Control

In Kerio Control, the DNS forwarding service can be used to enable easier configuration for DNS hosts within local networks or to speed up responses to repeated DNS queries. To use the DNS forwarding service, clients must be directed to the IP address of Kerio Control. This is defined in the DHCP server configuration.



In case of Active Directory or Open Directory environments, Kerio Control will forward DNS queries to the internal Domain Name Server if Kerio Control is configured to authenticate users in the domain. For details refer to [Connecting Kerio Control to directory service](#)



The DNS forwarding service only works for IPv4. IPv6 is not supported.

Configuring simple DNS forwarding

1. In the administration interface, go to **DNS**.
2. Check that **Enable the DNS forwarding service** is enabled.
If the DNS forwarding service is disabled, the DNS module is used only as a Kerio Control's DNS resolver.
3. Check that **Enable DNS cache for faster responses to repeat queries** is enabled.
Responses to repeated queries will be much faster (the same query sent by various clients is also considered as a repeated query).
4. Before forwarding a DNS query, Kerio Control can perform a local DNS lookup in a hosts table, or from hostnames found in the DHCP lease table:
 - If you use the DHCP server in Kerio Control, select **DHCP lease table**
 - If you do not use the DHCP server in Kerio Control, select **Hosts table** and fill the table with IP addresses and DNS hostnames.

5. In the **When resolving name from the hosts table or lease table combine it with DNS domain below** entry, specify name of your local DNS domain.
6. Click **Apply**.

Example

The local domain's name is example.com. The host called jsmith is configured so as to obtain an IP address from the DHCP server. After the operating system is started the host sends to the DHCP server a query with the information about its name (jsmith). The DHCP server assigns the host IP address 192.168.1.56. The DHCP server then keeps the information that the IP address is assigned to the jsmith host.

Another host that wants to start communication with the host will send a query on the jsmith.example.com name. If the local domain name would not have been known by the DNS module, the forwarder would pass the query to another DNS server as it would not recognize that it is a local host. However, as DNS forwarder knows the local domain name, the example.com name will be separated and the jsmith host with the appropriate IP address will be easily looked up in the DHCP table.

Hosts table

Hosts table includes a list of IP addresses and corresponding DNS hostnames. Kerio Control uses this table to detect the IP address of hostname-specified local hosts, for example, if you have a local server which should be accessed using an internal, local IP address.

DNS names can be specified without a domain, if the local domain is specified in the **When resolving name from the hosts table or lease table combine it with DNS domain below** entry.

Each IP address can have multiple DNS names assigned. This can be defined in the following ways:

- To write all information in a single record and separate individual names with semicolons. Example:

```
192.168.1.10 server;mail
```

The main advantage of this method is space-saving. First name written is always considered as primary (so called canonical name) and the other names are used as its aliases.

- Create an individual record for each name. Example:

```
192.168.1.10 server
```

```
192.168.1.10 mail
```

In case of this method, the primary name can be set as needed. To move records, use arrow buttons on the right side of the window. The name written as first at the IP address will be used as primary.

Each DNS name can have multiple IP addresses assigned (e.g. a computer with multiple network adapters). In that case, a record must be added to the table for each IP address, while DNS name will be identical in all these records.

Configuring custom DNS Forwarding

The DNS module allows forwarding of DNS requests to DNS servers. This feature can be helpful when we intend to use a local DNS server for the local domain (the other DNS queries will be forwarded to the Internet directly — this will speed up the response). DNS forwarder's settings also play a role in the configuration of private networks where it is necessary to provide correct forwarding of requests for names in domains of remote subnets.

Request forwarding is defined by rules for DNS names or subnets. Rules are ordered in a list which is processed from the top. If a DNS name or a subnet in a request matches a rule, the request is forwarded to the corresponding DNS server. Queries which do not match any rule are forwarded to the default DNS servers (see above).



If the [simple DNS resolution](#) is enabled, the forwarding rules are applied only if the DNS module is not able to respond by using the information in the hosts table and/or by the DHCP lease table.

Defining a rule

For custom DNS forwarding, follow these steps:

1. Configure [simple DNS resolution](#).
2. Select option **Enable custom DNS forwarding** to enable settings for forwarding certain DNS queries to other DNS servers and click **Edit**.
3. In the **Custom DNS Forwarding** dialog, click **Add**.

The rule can be defined for:

- DNS name queries requiring names of computers will be forwarded to this DNS server (A queries),
- a subnet queries requiring IP addresses of the particular domain will be forwarded to the DNS server (PTR queries).

Rules can be reordered by arrow buttons. This enables more complex combinations of rules — e.g. exceptions for certain workstations or subdomains. As the rule list is processed from the top downwards, rules should be ordered starting by the most specific one (e.g. name of a particular computer) and with the most general one at the bottom (e.g. the main domain of the company).

Similarly to this, rules for reversed DNS queries should be ordered by subnet mask length (e.g. with 255.255.255.0 at the top and 255.0.0.0 at the bottom). Rules for queries concerning names and reversed queries are independent from each other.

4. In the **Custom DNS Forwarding** dialog, you can create these types of rules:
 - **Match DNS query name** — it is necessary to specify a corresponding DNS name (name of a host in the domain).



In rules for DNS requests, it is necessary to enter an expression matching the full DNS name! If, for example, the `kerio.c*` expression is introduced, only names `kerio.cz`, `kerio.com` etc. would match the rule and host names included in these domains (such as `www.kerio.cz` and `secure.kerio.com`) would not!

- **Match IP address from reverse DNS query** alternative to specify rule for DNS queries on IP addresses in a particular subnet (i.e. `192.168.1.0/255.255.255.0`).
5. Use the **Forward the query** field to specify IP address(es) of one or more DNS server(s) to which queries will be forwarded.

If multiple DNS servers are specified, they are considered as primary, secondary, etc.

If the **Do not forward** option is checked, DNS queries will not be forwarded to any other DNS server — Kerio Control will search only in the hosts table or in the DHCP server table (see below). If requested name or IP address is not found, non-existence of the name/address is reported to the client.



Using the **Do not forward** option is meaningless for reverse DNS queries as the DNS module in Kerio Control cannot respond to them by itself.

6. Save the settings and create another rule if it is needed.

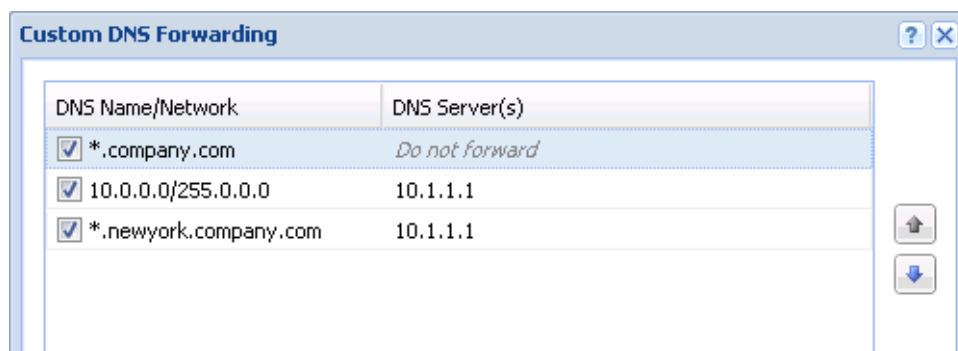


Figure 1 Custom DNS forwarding

Clearing the cache

Clear-out of all records from the DNS cache (regardless of their lifetime). This feature can be helpful e.g. for configuration changes, dial-up testing, error detection, etc.

Configuring a routing table

Routing table overview

The *Kerio Control Administration* interface allows to view and edit the IPv4 routing table. This can be useful especially to resolve routing problems remotely (it is not necessary to use applications for terminal access, remote desktop, etc.).

To view or modify the routing table go to **Configuration** → **Routing Table**. This section provides up-to-date version of the routing table of the operating system including so called *persistent routes* on Windows (routes added by the `route -p` command).



1. In the Internet connection failover mode, only the current default route is shown (depending on which Internet interface is currently active).
2. In case of multiple Internet links in the network load balancing mode, only a single default route will be displayed which is routed through the link with the highest proposed speed.
3. IPv6 is not supported.

Dynamic and static routes can be added and/or removed in section **Routing table**. Dynamic routes are valid only until the operating system is restarted or until removed by the `route` system command. Static routes are saved in *Kerio Control* and they are restored upon each restart of the operating system.

Route Types

The following route types are used in the *Kerio Control* routing table:

- *System routes* — routes downloaded from the operating system's routing table (including so called persistent routes). These routes cannot be edited some of them can be removed — see the **Removing routes from the Routing Table** section).
- *VPN routes* — routes to VPN clients and to networks at remote endpoints of VPN tunnels. These routes are created and removed dynamically upon connecting and disconnecting of VPN clients or upon creating and removing of VPN tunnels. VPN routes cannot be created, modified nor removed by hand.
- *Static routes* — manually defined routes managed by *Kerio Control* (see below). These routes can be added, modified and/or removed.

Configuring a routing table

The checking boxes can be used to disable routes temporarily.

Static routes

Kerio Control includes a special system for creation and management of static routes in the routing table. All static routes defined in *Kerio Control* are saved into the configuration file and upon each startup of the *Kerio Control Engine* they are added to the system routing table. In addition to this, these routes are monitored and managed all the time *Kerio Control* is running. This means that whenever any of these routes is removed by the `route` command, it is automatically added again.



1. The operating system's persistent routes are not used for implementation of static routes (for management of these routes, *Kerio Control* uses a proprietary method).
2. If a static connection uses a dial-up, any UDP or TCP packet with the *SYN* flag dials the line.

Definitions of Dynamic and Static Rules

Clicking on **Add** (or **Edit** if a particular route is selected) displays a dialog for route definition.

Network, Network Mask

IP address and mask of the destination network.

Interface

Selection of an interface through which the specific packet should be forwarded.

Gateway

IP address of the gateway (router) which can route to the destination network. The IP address of the gateway must be in the same IP subnet as the selected interface.

Metric

“Distance” of the destination network. The number stands for the number of routers that a packet must pass through to reach the destination network.

Metric is used to find the best route to the desired network. The lower the metric value, the “shorter” the route is.



Metric in the routing table may differ from the real network topology. It may be modified according to the priority of each line, etc.

Create a static route

Enable this option to make this route static which means that *Kerio Control* will refresh it automatically (see above). Add a brief **Description** providing various information (why the route was created, etc.) about the route can be attached.

If this option is not enabled, the route will be valid only until the operating system is restarted or until removed manually in the *Kerio Control Administration* interface or using the `route` command.

Removing routes from the Routing Table

Using the **Remove** button, records can be removed from the routing table. The following rules are used for route removal:

- Static routes in the **Static Routes** folder are managed by *Kerio Control*. Removal of any of the static routes would remove the route from the system routing table immediately and permanently (after clicking on the **Apply** button).
- Dynamic (system) route will be removed as well, regardless whether it was added in the *Kerio Control Administration* interface or by using the `route` command. However, it is not possible to remove any route to a network which is connected to an interface.
- Persistent route of the operating system will be removed from the routing table only after restart of the operating system. Upon reboot of the operating system, it will be restored automatically. There are many methods that can be used to create persistent routes (the methods vary according to operating system — in some systems, the `route -p` or the `route` command called from an execution script can be used, etc.). It is not possible to find out how a particular persistent route was created and how it might be removed for good.

Statistics and reports

Statistics and reports overview

Kerio Control provides detailed statistics on user activity, volume of transferred data, visited websites and web categories. This information may help figure out browsing activities and habits of individual users.

The statistics monitor the traffic between the local network and the Internet. Volumes of data transferred between local hosts and visited web pages located on local servers are not included in the statistics (also for technical reasons).

One of the benefits of statistics and reports is their high availability. User (usually a manager or team leader) can view the statistics in their web browser and/or set receiving of regularly sent email reports.

This chapter addresses setting of parameters in the Kerio Control administration. The web interface with statistics is described thoroughly in the *Kerio Control — User's Guide*.

Notes:

1. The firewall administrator should inform users that their browsing activities are monitored by the firewall.
2. Statistics and reports in Kerio Control should be used for reference only. It is highly unrecommended to use them for example to figure out exact numbers of Internet connection costs per user.

Monitoring and storage of statistic data

Diverse data is needed to be gathered for the statistics. This data is kept in so called primary database. Total period length for which Kerio Control keeps the statistics can be set in the **Accounting** section. By default, this time is set to *24 months* (i.e. 2 years).

For technical reasons, the Kerio Control Engine stores gathered statistic data in the cache and data is recorded in the database once per hour. The cache is represented by several files on the disk. This implies that any data is kept in the cache even if the Kerio Control Engine is stopped or another problem occurs (failure of power supply, etc.) though not having been stored in the database yet.

The statistics use data from the main database. This implies that current traffic of individual users is not included in the statistics immediately but when the started period expires and the data is written in the database.



Data in the database used for statistics cannot be removed manually (such action would be meaningless). In statistics, it is possible to switch into another view mode where data is related only to a period we need to be informed about. If you do not wish to keep older data, it is possible to change the statistics storage period (see above).

Requirements of the statistics

The following conditions must be met for correct function of all statistics:

- The firewall should always require user authentication. The statistics by individual users would not match the true state if unauthenticated users are allowed to access the Internet.
- For statistics on visited websites, it is necessary that a corresponding protocol inspector is applied to any HTTP traffic. This condition is met by default unless special traffic rules disabling the particular protocol inspector are applied.

As to secured traffic (HTTPS), it is not possible to view visited pages but only volume of transferred data.

If the *Kerio Control* proxy server is used, visited pages are monitored by the proxy server itself.

- For monitoring of web categories of visited websites, the *Kerio Control Web Filter* module must be enabled. In its configuration, the **Categorize each page regardless of HTTP rules** option should be enabled, otherwise web categories statistics would be unreliable.

Gathering of statistical information and mapped services

Connections from the Internet to mapped services on local hosts (or to services on the firewall available from the Internet) are also included in user statistics. If a user is connected to the firewall from the particular host, access to the mapped service is considered as an activity of this user. Otherwise, such connection is included in activity of unknown users (users who are not logged in).

The following example helps recognize importance of this feature. User *jsmith* is authenticated at the firewall and connected to it from a local workstation. The *RDP* service for this host is mapped on the firewall, allowing the user to work remotely on the workstation. If user *jsmith* connects from the Internet to the remote desktop on the workstation, this connection (and data transferred within the connection) will be correctly included in the user's statistics and quota.

The following example addresses case of a mapped web server accessible from the Internet. Any (anonymous) user in the Internet can connect to the server. However, web servers are

usually located on a special machine which is not used by any user. Therefore, all traffic of this server will be accounted for users who are “not logged in”.

However, if any user is connected to the firewall from the server, any traffic between clients in the Internet and the web server is accounted as an activity of this user. If this user also reaches their data volume quota, corresponding restrictions will be applied to this web server.

Settings for statistics, reports and quota

Under certain circumstances (too many connected users, great volume of transmitted data, low capacity of the *Kerio Control* host, etc.), viewing of statistics may slow the firewall and data transmission (Internet connection) down. Be aware of this fact while opening the statistics. Therefore, *Kerio Control* allows such configuration of statistics that is customized so that only useful data is gathered and useful statistics created. It is also possible to disable creation of statistics if desirable. This saves performance capacity and disk space on the firewall.

Statistics settings also affect monitoring of volume of transferred data against user quota.

Use the **Data Gathering** tab in **Configuration** → **Accounting** to set gathering of statistical data, accounting periods for quota and statistics and email reports sending parameters.

Enable/disable gathering of statistic data

The **Internet Usage statistics** option enables/disables all statistics (i.e. stops gathering of data for statistics).

The **Gather user's activity records** option enables monitoring and logging of browsing activity of individual users. If is not necessary to gather these statistics, it is recommended to disable this option (this reduces demands to the firewall and saves the server's disk space).

You can use the **Delete statistics older than...** parameter to specify a time period for which the data will be kept (i.e. the age of the oldest data that will be available). This option affects disk space needed for the statistics remarkably. To save disk space, it is therefore recommended to keep the statistics only for a necessary period.

Statistics and quota accounting periods

Accounting period is a time period within which information of transferred data volume and other information is gathered. Statistics enable generating of weekly and monthly overviews. In **Accounting Periods**, it is possible to define starting days for weekly and monthly periods (for example, in statistics, a month can start on day 15 of the civil month and end on day 14 of the following civil month).

The parameter of first day of monthly period also sets when the monthly transferred data counter of individual users will be set to zero.

Regular report

Kerio Control allows to send statistics by email.

Report sending is set in rules. Each rule defines one recipient of the report. Recipient can be either a Kerio Control user (with email address defined) or any email address. Optionally it is possible to send daily, weekly and monthly reports.

Kerio Control users will get their email reports in their preferred language, while reports in **Default language** will be delivered to external email addresses.

Note: For sending of email reports, it is necessary to set server for outgoing email messages correctly under **Configuration** → **Advanced Options** → **SMTP Server**.

Conditions for statistics

This feature helps avoid gathering of irrelevant information. Thus, statistics are kept transparent and gathering and storage of needless data is avoided.

Usage of individual exceptions:

- *Time Range*
Define a time period when information will be gathered and included in statistics and quota (e.g. only in working hours). Without this period, no traffic will be included in the statistics and in the quota neither.
- *Listening IP Addresses*
Define IP addresses of hosts which will be excluded from the statistics and to which quota will not be applied.
The selected group may include both local or Internet IP addresses. If any of these IP addresses belongs to the local network, bear in mind that no traffic of the host will be included in the statistics or the quota. In case of addresses of Internet servers, traffic of local users with the server will not be accounted in the statistics or any user quota.
- *Users and Groups*
Select users and/or user groups which will be excluded from the statistics and no quota will be applied to them. This setting has the highest priority and overrules any other quota settings in user or group preferences.
- *Web Pages*
Define a URL group. Connections to web sites with these URLs will not be accounted. Such exception can be used for example to exclude the own corporate web servers from the statistics (connection to corporate websites is usually considered a work-related activity) or to exclude ads connection to certain pages may download advertisements automatically, it is not the user's request. For this purpose, you can use the predefined URL group *Ads/banners*.
Wildcards can be used in URL groups items. This implies that it is possible to define exceptions for particular pages or for all pages on a particular server, all web servers in a domain, etc.
URL exceptions can be applied only to unsecured web pages (the *HTTP* protocol). Connections to secured pages (the *HTTPS* protocol) are encrypted and URL of such pages cannot be detected.



Unlike in case of exceptions described above, data transferred within connections to such web pages will be included in the quota.

Access to statistics

Settings for user access to Internet usage statistics and periodical email reporting according to set criteria.

Layout

Advanced options for the statistics and email reports formatting:

- Username format.
- Default language for email reports — for reports sent to external email addresses.

Access rights and email reports

Access to statistics and email reporting can be set by simple rules. There can be any number of rules added and their order is not important.

Rule definition.

- User — it is possible to select any number of users and/or groups from the Kerio Control internal database and/or mapped directory services.
Kerio Control users receive their reports at email addresses defined in their user account. They can also view online statistics in the Kerio Control web interface.
- Email address — an email address where email reports will be sent. Email address cannot be used to access online statistics. For sending reports to multiple addresses, define multiple separate rules.
- Data — statistics contained in reports and/or available online. It is possible to include statistics either for all users or just for selected users and groups (e.g. subordinates will not be allowed to access to statistics of their superiors).
- Regular reports — automatic sending of email reports according to conditions set (daily, weekly, monthly).

For email sending, the relay server must be set properly (**Configuration** → **Advanced Options** → **SMTP Server**).

You can click on **Send again** to resend latest email reports in case that they have not been sent or delivered for any reason.

User access

Bulk settings for all Kerio Control users:

- Permission to view their own statistics in the Kerio Control web interface,
- Automatically sent of email reports (daily, weekly, monthly).

Logging on the web interface and viewing of statistics

To view statistics, user must authenticate at the *Kerio Control's* web interface first. User (or the group the user belongs to) needs rights for statistics viewing. The web interface can be accessed by several methods, depending on whether connecting from the *Kerio Control* host (locally) or from another host (remotely).

Accessing the statistics from the Kerio Control host (Windows)

On the *Kerio Control* host, the web interface with statistics may be opened as follows:

- By using the **Internet Usage Statistics** link available in the *Kerio Control Engine Monitor* context menu (opened by the corresponding icon in the notification area).
- By using the **Internet Usage Statistics** link under **Start** → **Programs** → **Kerio** → **Kerio Control**.

Both links open the unsecured web interface directly on the local host (<http://localhost:4080/star>) using the default web browser.



Within local systems, secured traffic would be useless and the browser would bother user with needless alerts.

Remote access to the statistics

It is also possible to access the statistics remotely, i.e. from any host which is allowed to connect to the *Kerio Control* host and the web interface's ports, by using the following methods:

- If you are currently logged on to the *Kerio Control* administration, the **Internet Usage Statistics** link available in section **Status** → **Statistics** can be used. This link opens the secured web interface for statistics in the default web browser.



URL for this link consists of the name of the server and of the port of the secured web interface. This guarantees function of the link from the *Kerio Control* host and from the local network. To make **Internet Usage Statistics** link work also for remote administration over the Internet, name of the particular server must be defined in the public DNS (with the IP address of the particular firewall) and traffic rules must allow access to the port of the secured Web interface (4081 by default).

- At <https://server:4081/star> or <http://server:4080/star> This URL works for statistics only. If the user has not appropriate rights to view statistics, an error is reported.
- At <https://server:4081/> or <http://server:4080/>. This is the primary URL of the *Kerio Control's* web interface. If the user possesses appropriate rights for stats viewing, the welcome page providing overall or their own statistics (see below) is displayed. Otherwise, the *My Account* page is opened (this page is available to any user).



In case of access via the Internet (i.e. from a remote host) it is recommended to use only the secured version of the web interface. The other option would be too risky.

Updating statistics

First of all, the web interface is used for viewing statistics and creating reviews for certain periods. To Kerio Control, gathering and evaluation of information for statistics means processing of large data volumes. To reduce load on the firewall, data for statistics is updated approximately once in an hour. The top right corner of each web interface page displays information about when the last update of the data was performed.

For these reasons, the statistics are not useful for real-time monitoring of user activity. For these purposes, you can use the **Active Hosts** section in the administration interface.

Administrative settings

System Configuration (editions Appliance and Box)

In editions *Appliance* and *Box*, the *Kerio Control* administration console allows setting of a few basic parameters of the firewall's operating system. These settings are necessary for correct functionality of the firewall and they can be found in **Configuration / Advanced options**, on the **System Configuration** tab.

Date, time and time zone

Many *Kerio Control* features (user authentication, logs, statistics, etc.) require correct setting of date, time and time zone on the firewall.

Date and time can be set automatically but it is more useful to use an NTP server which provides information about the current time and allows automatic management of the firewall's system time. The time zone also includes information about daylight saving time settings.

Kerio Technologies offers the following free NTP servers for this purpose: 0.kerio.pool.ntp.org, 1.kerio.pool.ntp.org, 2.kerio.pool.ntp.org and 3.kerio.pool.ntp.org.

Update Checking

Kerio Control enables automatic check for new versions at the *Kerio Technologies* website. Update checker acts differently in dependence on the firewall's platform:

- in the *Windows* edition, only links to sources with more information and to installation package download are provided,
- in editions *Appliance* and *Box*, the firewall may download a new image of the drive and perform update of the entire appliance automatically.

may offer download and installation.

Open the **Update Checker** tab in the **Configuration → Advanced Options** section to view information on a new version and to set parameters for automatic checks for new versions.

Periodically check for new versions

Use this option to enable/disable automatic checks for new versions. Checks are performed:

- minutes after each startup of the *Kerio Control Engine*,
- and then every 24 hours.

Results of each attempted update check (successful or not) is logged into the **Debug** log.

Check also for beta versions

Enable this option if you want *Kerio Control* to perform also update checks for beta and *Release Candidate* versions of Kerio Control.

If you wish to participate in testing of *Kerio Control* beta versions, enable this option. In case that you use *Kerio Control* in operations in your company (i.e. at the Internet gateway of your company), we recommend you not to use this option (beta versions are not tested yet and they could endanger functionality of your networks, etc.).

Send anonymous statistics...

By sending anonymous statistics, you can help with Kerio Control development. The statistics do not contain any personal information such as email addresses, login names and/or passwords.

Download new versions automatically

This option is available only in editions *Appliance* and *Box*. If this option is enabled, once a new version of the product is detected, the corresponding update package is downloaded immediately and the firewall can be updated directly from the administration interface.

Last update check performed ... ago

Information on how much time ago the last update check was performed.

If the time is too long (several days) this may indicate that the automatic update checks fail for some reason (i.e. access to the update server is blocked by a traffic rule). In such cases we recommend you to perform a check by hand (by clicking on the **Check now** button), view results in the **Debug** log.

Check Now

Click on this button to check for updates immediately.

Any time a new version of the product is detected, then:

- In the *Windows* edition, a link is displayed referring to a page with detailed information and another one to the installation package download page.
- In editions *Appliance* and *Box*, a button for download of the update package is displayed (or for immediate start of the update in case that the automatic updates are enabled). Update of the firewall takes up to several minutes. Once it is finished, you will be informed that the firewall would be restarted. Upon the restart (in approximately 1 minute), the firewall will be fully available again.



Whenever a newer version is available, this information is displayed as a link in the welcome page of the administration window (an image providing information about the application and the license). Clicking on the link will take you to section **Configuration** → **Advanced Options**, the **Updates** tab.

Configuring the SMTP server

SMTP Server Configuration

Kerio Control provides a function which enables notification to users or/and administrators by email alerts. These alert messages can be sent upon various events, for example when a virus is detected, when a *Peer-to-Peer* network is detected, when an alert function is set for certain events or upon reception of an alert.

For this purpose, *Kerio Control* needs an SMTP Relay Server. This server is used for forwarding of infected messages to a specified address.



Kerio Control does not provide any built-in SMTP server.

To configure an SMTP server, go to the **SMTP server** tab in **Configuration** → **Advanced Options**.

Server

Name or IP address of the server.

Note: If available, we recommend you to use an SMTP server within the local network (messages sent by *Kerio Control* are often addressed to local users).

SMTP server requires authentication

Enable this option to require authentication through username and password at the specified SMTP server.

Specify sender email address in “From” header

In this option you can specify a sender's email address (i.e. the value for the From header) for email sent from *Kerio Control* (email reports or alerts sent to users). Preset From header does not apply to messages forwarded during antivirus check.

This item must be preset especially if the SMTP server strictly checks the header (messages without or with an invalid From header are considered as spams). The item can also be used for reference in recipient's mail client or for email classification. This is why it is always recommended to specify sender's email address in *Kerio Control*.

Test

Test of functionality of email sending via the specified SMTP server. *Kerio Control* sends a testing email message to the specified email address.



1. If SMTP is specified by a DNS name, it cannot be used until *Kerio Control* resolves a corresponding IP address (by a DNS query). The **IP address of specified SMTP server cannot be resolved** warning message is displayed in the **SMTP Relay** tab until the IP address is not found. If the warning is still displayed, this implies that an invalid (non-existent) DNS name is specified or the DNS server does not respond.
If the warning on the **SMTP server** tab is still displayed, it means that an invalid DNS name was specified or that an error occurred in the communication (DNS server is not responding). Therefore, we recommend you to specify SMTP server by an IP address if possible.
2. Communication with the SMTP server must not be blocked by any rule, otherwise an error is reported upon clicking the **Apply** button.

P2P Eliminator

P2P Eliminator overview

Peer-to-Peer (P2P) networks are worldwide distributed systems where each node can be used both as a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

In addition to illegal data distribution, utilization of P2P networks overload lines via which users are connected to the Internet. Such users may limit connections of other users in the same network and may increase costs for the line (for example when volume of transmitted data is limited for the line).

Kerio Control provides the P2P Eliminator module which detects connections to P2P networks and applies specific restrictions. Since there is a large variety of P2P networks and parameters at individual nodes (servers, number of connections, etc.) can be changed, it is hardly possible to detect all P2P connections.¹ However, using various methods (such as known ports, established connections, etc.), the P2P Eliminator is able to detect whether a user connects to one or multiple P2P networks.

The following restrictions can be applied to users of P2P networks (i.e. to hosts on which clients of such networks are run):

- *Block all traffic* — the host will not be allowed to access the Internet,
- *Allow only secure traffic* — only such traffic of the particular host is allowed that is for sure not using P2P networks (e.g. web, email, etc.).

P2P Eliminator Configuration

P2P networks are detected automatically (the P2P Eliminator module keeps running). To set the P2P Eliminator module's parameters, go to the **P2P Eliminator** tab in the **Advanced Options** section.

As implied by the previous description, it is not possible to block connections to particular P2P networks. P2P Eliminator allows to block all traffic (i.e. access to the Internet from the particular host) or to permit only such services where it is guaranteed that they do not use P2P networks. The settings will be applied to all clients of P2P networks detected by P2P Eliminator.

Check the **Inform user by email** option if you wish that users at whose hosts P2P networks are detected will be warned and informed about actions to be taken (blocking of all traffic /

¹ According to thorough tests, the detection is highly reliable (probability of failure is very low).

allowance of only certain services and length of the period for which restrictions will be applied). The email is sent only if a valid email address is specified in the particular user account. This option does not apply to unauthenticated users.

The **Traffic will be blocked for** value defines time when the restriction for the particular host will be applied. The P2P Eliminator module enables traffic for this user automatically when the specified time expires. The time of disconnection should be long enough to make the user consider consequences and to stop trying to connect to P2P networks.



1. If a user who is allowed to use P2P networks is connected to the firewall from a certain host, no P2P restrictions are applied to this host. Settings in the **P2P Eliminator** tab are always applied to unauthorized users.
2. Information about P2P detection and blocked traffic can be viewed in the **Status** → **Active Hosts** section.
3. If you wish to notify also another person when a P2P network is detected (e.g. the firewall administrator), define the alert on the **Alerts Settings** tab of the **Accounting** section.

Parameters for detection of P2P networks

Click **Advanced** to set parameters for P2P detection.

Ports of P2P networks

List of ports which are exclusively used by P2P networks. These ports are usually ports for control connections — ports (port ranges) for data sharing can be set by users themselves. Ports in the list can be defined by port numbers or by port ranges. Individual values are separated by commas while dash is used for definition of ranges.

Number of suspicious connections

Big volume of connections established from the client host is a typical feature of P2P networks (usually one connection for each file). The *Number of connections* value defines maximal number of client's network connections that must be reached to consider the traffic as suspicious.

The optimum value depends on circumstances (type of user's work, frequently used network applications, etc.) and it must be tested. If the value is too low, the system can be unreliable (users who do not use P2P networks might be suspected). If the value is too high, reliability of the detection is decreased (less P2P networks are detected).

Safe services

Certain legitimate services may also show characteristics of traffic in P2P networks (e.g. big number of concurrent connections). To ensure that traffic is not detected incorrectly and users of these services are not persecuted by mistake, it is possible to define list of so called secure services. These services will be excluded from detection of P2P traffic.

The **Define services...** button opens a dialog where services can be define that will not be treated as traffic in P2P network. All services defined in **Definitions** → **Services** are available.



Default values of parameters of P2P detection were set with respect to long-term testing. As already mentioned, it is not always possible to say that a particular user really uses P2P networks or not which results only in certain level of probability. Change of detection parameters may affect its results crucially. Therefore, it is recommended to change parameters of P2P networks detection only in legitimate cases (e.g. if a new port number is detected which is used only by a P2P network and by no legitimate application or if it is found that a legitimate service is repeatedly detected as a P2P network).

Dynamic DNS for public IP address of the firewall

Dynamic DNS for public IP address of the firewall

Kerio Control provides (among others) services for remote access from the Internet to the local network (VPN server). Also other services can be accessible from the Internet — e.g. the Kerio Control web interface, administration of Kerio Control or any other service (e.g. web server in local network). These services are available at the firewall's public IP address. If this IP address is static and there exists a corresponding DNS record for it, a corresponding name can be used for access to a given service (e.g. `server.company.com`). If there is no corresponding DNS record, it is necessary to remember the firewall's IP address and use it for access to all services. If the public IP address is dynamic (i.e. it changes), it is extremely difficult or even impossible to connect to these services from the Internet.

This problem is solved by Kerio Control's support for dynamic DNS. Dynamic DNS provides DNS record for a specific name of a server which will always keep the current IP address. This method thus allows making mapped services always available under the same server name, regardless of the fact if IP address changes and how often.

How cooperation with dynamic DNS works

Dynamic DNS (DDNS) is a service providing automatic update of IP address in DNS record for the particular host name. Typically, two versions of DDNS are available:

- free — user can choose from several second level domains (e.g. `no-ip.org`, `ddns.info`, etc.) and select a free host name for the domain (e.g. `company.ddns.info`).
- paid service — user registers their own domain (e.g. `company.com`) and the service provider then provides DNS server for this domain with the option of automatic update of records.

User of the service gets an account which is used for access authentication (this will guarantee that only authorized users can update DNS records). Update is performed via secured connection (typically HTTPS) to make sure that the traffic cannot be tapped. Dynamic DNS records can be updated either manually by the user or (mostly) by a specialized software — *Kerio Control* in this case.

If Kerio Control enables cooperation with dynamic DNS, a request for update of the IP address in dynamic DNS is sent upon any change of the Internet interface's IP address (including switching between primary and secondary Internet connection. This keeps DNS record for the particular IP address up-to-date and mapped services may be accessed by the corresponding host name.



1. Usage of DDNS follows conditions of the particular provider.
2. Dynamic DNS records use very short time-to-live (TTL) and, therefore, they are kept in cache of other DNS servers or forwarders for a very short time. Probability that the client receives DNS response with an invalid (old) IP address is, therefore, very low.
3. Some DDNS servers also allow concurrent update of more records. Wildcards are used for this purpose.

Example: In DDNS there exist two host names, both linked to the public IP address of the firewall: `fw.company.com` and `server.company.com`. If the IP address is changed, it is therefore possible to send a single request for update of DNS records with name `*.company.com`. This request starts update of DNS records of both names.

Kerio Control DDNS configuration

To set cooperation with the dynamic DNS server, go to the *Dynamic DNS* folder in **Advanced Options**.

As already mentioned, the first step is to make an account (i.e. required dynamic DNS record with appropriate access rights) at a DDNS provider. Kerio Control now supports these DDNS providers:

- *ChangeIP* (<http://www.changeip.com/>),
- *DynDNS* (<http://www.dyndns.org/>),
- *No-IP* (<http://www.no-ip.com/>).

On the Dynamic DNS tab, select a DDNS provider, enter DNS name for which dynamic record will be kept updated and set user name and password for access to updates of the dynamic record. If DDNS supports wildcards, they can be used in the host name.

Once this information is defined, it is recommended to test update of dynamic DNS record by clicking on **Update now**. This verifies that automatic update works well (the server is available, set data is correct, etc.) and also updates the corresponding DNS record (IP address of the firewall could have changed since the registration or the last manual update).

If an error occurs while attempting to update DNS record, an error is reported on the Dynamic DNS tab providing closer specification of the error (e.g. DDNS server is not available, user authentication failed, etc.). This report is also recorded in the **error** log.

Creating user accounts

User accounts overview

User accounts are used to:

- Authenticate users to their accounts
- Gather reporting data in Kerio Control Statistics
- Set access rights to Kerio Control administration
- Control user access to the Internet from local networks

Users are managed in the administration interface in section **Users**.

Adding new accounts

You can add either new local accounts or existing accounts from a directory service.

Adding local accounts

You need local accounts in the following cases:

- Microsoft Active Directory or Apple Open Directory is not used in your environment.
- You want to add a local administration account.

Administration accounts must be created locally. The advantage is that such users can authenticate locally even if the network communication fails.

Creating a local account:

1. In section **Users**, click **Add**.
2. On the **General** tab, fill in username and password.



Username are not case-sensitive and cannot include spaces, national and special characters.

Other items are optional.

3. Save the settings.



If you plan to create numerous local accounts with similar settings, [create a template](#).

Adding accounts from a directory service

Adding accounts from directory services is described in article [Connecting Kerio Control to directory service](#).

Using templates

If you plan to create numerous accounts with similar settings, create a template:

1. In section **Users**, click **Template**.
2. In the user template, specify all the settings which will be common for all users from this domain.
3. Save the settings.
4. Click **Add/Edit** a user.
5. In the **Add/Edit user** dialog, select **This user's configuration is defined by the domain template**.

Configuring accounts

You can:

- [add users to groups](#)
- [set transfer quotas for users](#)
- [configure access rights to the administration interface](#)
- filter web content per user
- [set automated login from a static IP address](#)

Configuring user quota

Kerio Control enables you to configure a limit for volume of data transferred by a user, as well as actions to be taken when the quota is exceeded.

Set the user quota in the following steps:

1. In the administration interface, go to **Users**.
2. Select a user (or a template) and click **Edit**.

Creating user accounts

3. Enable daily/weekly/monthly limit and set a quota.

Use the **Direction** combo box to select which transfer direction will be controlled (**download** — incoming data, **upload** — outgoing data, **all traffic** — both incoming and outgoing data).

4. Set actions which will be taken whenever a quota is exceeded:

- **Block any further traffic** — the user will be allowed to continue using the opened connections, however, they will not be allowed to establish new connections (i.e. to connect to another server, download a file through FTP, etc.)

If a quota is exceeded and the traffic is blocked, the restriction will be applied until the end of the quota period (day/week/month). To cancel these restrictions:

- disable temporarily the corresponding limit, raise its value or switch to the **Don't block further traffic** mode
- delete the data volume counter of the user in the **User Statistics** section.
- **Don't block further traffic** — Internet connection speed will be limited for the user. Traffic will not be blocked but the user will notice that the Internet connection is slower than usual.

5. Check **Notify user by email when quota is exceeded**.

Specify an email address in the **Edit User** dialog. Also set the SMTP relay in Kerio Control.



Kerio Control administrator can be notified when a user quota is almost exceeded. Set the alert parameters in **Configuration** → **Accounting** → **Alert Settings**.

Automatic login on static IP addresses

If a user works at a reserved workstation (i.e. this computer is not by any other user) with a fixed IP address (static or reserved at the DHCP server), the user can use automatic login from the IP address:

1. In the administration interface, go to **Users**.
2. Select a user and click **Edit**.
3. In the **Edit User** dialog, go to **IP Addresses** tab.
4. You have several choices:

- For one or several IP address: Check **Specific host IP addresses**.
- For more IP addresses: Go to **Definitions** → **IP Address Groups** and create a new group of IP addresses for automated login. Then return back to **IP Addresses** tab and check **IP address group**.
- If the user's host is at firewall (Kerio Control was installed on user's host), check **Firewall**.
- Save the settings.

Let users connect to the Internet from the host with the static IP address. If the settings are correct, users do not have to login to the firewall. They are logged automatically.

Deleting user accounts

User accounts can be suspended temporarily or deleted permanently.

You cannot disable/delete the following users:

- currently logged user
- automatically generated Admin user

Disabling users temporarily

When you disable user accounts temporarily, users cannot login to Kerio Control.

1. In the administration interface, go to **Users**.
2. Double-click the user and on tab **General** uncheck option **Account is enabled**.
3. Save the settings.

Deleting users permanently

1. In the administration interface, go to **Users**.
2. Select the user and click **Remove**.
3. Confirm.

Troubleshooting

Information about adding, removing or editing users can be found in the **Config log**.

Setting access rights in Kerio Control

Setting access rights

1. In the administration interface, go to **Users** or **Groups**.
2. Select a domain and double-click the user or group you wish to edit.
3. Go to tab **Rights** and select the desired level of access rights.
4. Confirm.

What levels of access rights are available

Users/groups can have assigned the following levels of access rights:

- no access to administration
- read only access to administration
- full access to administration

Additional rights:

User can override Web content rules

If you check this rule, users can see and edit **Web content scanning options** on the **Preferences** tab in the Kerio Control client interface.

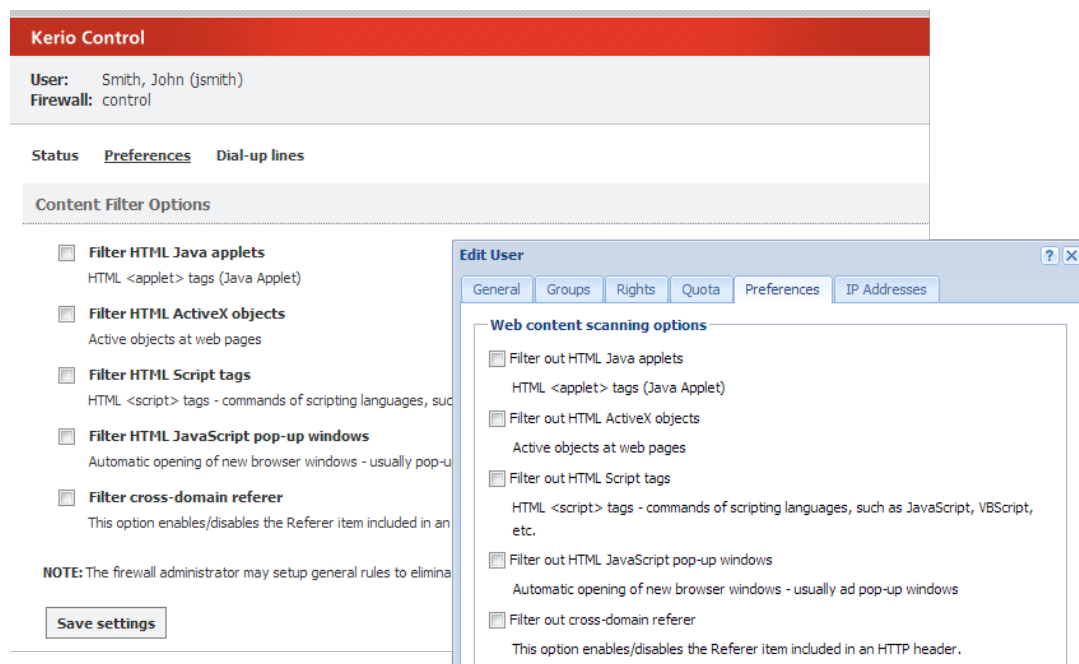


Figure 1 Content filter options in administration and user interface

Setting access rights in Kerio Control

User can unlock URL rules

The user with this right is allowed to bypass rules denying access to requested websites — at the page providing information about the denial, the **Unlock** button is displayed. The unlock feature must also be enabled in the corresponding URL rule.

User can control dial-up lines

If the Internet connection uses dial-up lines, users with this right will be allowed to dial and hang up these lines through the web interface.

User can connect using VPN

The user is allowed to connect through Kerio Control's VPN server or IPsec VPN server (using Kerio VPN Client or IPsec client).

Users are allowed to use P2P networks

Traffic of this user will not be blocked if P2P (Peer-to-Peer) networks are detected.

Connecting Kerio Control to directory service

Which directory services are supported

- Microsoft Active Directory
- Apple Open Directory

What is the connection used for

Easy account administration

Apart from the internal database of user accounts, Kerio Control can also import accounts and groups from an LDAP database. Using LDAP, user accounts can be managed from a single location. This reduces possible errors and simplifies the administration.

Online cooperation of Kerio Control and directory service

Additions, modifications or removals of user accounts/groups in the LDAP database are applied to Kerio Control immediately.

Using domain name and password for login

Users may use the same credentials for the domain login.



- Mapping is one-way only, data are synchronized from directory service to Kerio Control. Adding a new user in Kerio Control creates a local account.
- Use ASCII for usernames when creating user accounts in a directory service.
- If you disable users in Microsoft Active Directory, they are also disabled in Kerio Control.
- If you disable users in Apple Open Directory, they stay enabled in Kerio Control.

Microsoft Active Directory

Conditions for mapping from Active Directory domains

- Hosts in the local network (user workstations) should use the Kerio Control's DNS module as the primary DNS server, because it can process queries for Active Directory

Connecting Kerio Control to directory service

and forward them to the corresponding domain server. If another DNS server is used, user authentication in the Active Directory may not work correctly.

- The Kerio Control host must be a member of the mapped domain. Otherwise, authentication in the Active Directory may not work correctly.
- In case of mapping multiple domains, the Kerio Control host must be a member of one of the mapped domains (primary domain). The primary domain must trust all other domains mapped in Kerio Control.

Connecting to Microsoft Active Directory

1. In the administration interface, go to **Domains and User Login → Directory Services**.
2. You have to be a member of the Active Directory domain. If the firewall is not a member of the domain, click **Join Domain**.
3. In the **Join Domain** dialog, type the domain name and credentials with rights to join the computer to the Active Directory domain.

If you are successfully connected to the domain, you can see a green icon with the name of your domain on the **Directory Services** tab.

4. Check **Map user accounts and groups from a directory service** and select Microsoft Active Directory.
5. Type **Domain name**.
6. Type the username and password of a user with at least read rights for Microsoft Active Directory database. Username format is `user@domain`.
7. Click **Test Connection**.

In the **Users** section, you can select the new domain and display all users from the Active Directory domain.

Connecting to Apple Open Directory

1. In the administration interface, go to **Domains and User Login → Directory Services**.
2. Check **Map user accounts and groups from a directory service** and select Apple Open Directory.
3. Type the domain name.
4. Type the username and password of a user with at least read rights for Apple Open Directory database. Username format is `user@domain`.

5. In **Primary server/Secondary server**, type IP addresses or DNS names of the primary and secondary domain servers.

6. Click **Test Connection**.

In the **Users** section, you can select the new domain and display all users from the Open Directory domain.

Connecting to other domains

You are successfully connected to the primary domain.



Users of other domains must login with username including the domain (e.g. drdolittle@usoffice.company.com). User accounts with no domain specified (e.g. wsmith), will be searched in the primary domain or in the local database.

If you want to connect more domains:

1. In **Domains and User Login** → **Directory Services**, click **Advanced**.
2. In **Advanced Settings** dialog, go to **Additional Mapping**.
3. Click **Add**.
4. In the **Add New Domain** dialog, select Microsoft Active Directory or Apple Open Directory.
5. Type the domain name.
6. Type the username and password of a user with at least read rights for the database. Username format is user@domain.
7. In **Primary server/Secondary server**, type IP addresses or DNS names of the primary and secondary domain servers.
8. Click **Test Connection**.

In the **Users** section, you can select the new domain and display all users from the domain.

Configuring encrypted connection (LDAPS)

You can enable encrypted connection for the communication between Kerio Control and the directory service.



Encrypted connection must be supported by the directory service.

1. Go to **Domains and User Login** → **Directory Services**.
2. Click **Advanced**.
3. Check **Use encrypted connection**.

Collision of directory service with the local database and conversion of accounts

If a user with an identical name exists in both the domain and the local database, a collision occurs.

If a collision occurs, a warning is displayed at the bottom of the **Users** tab. Click the link in the warning to replace local accounts by corresponding directory service accounts.

The following operations will be performed automatically within each conversion:

- substitution of any appearance of the local account in the *Kerio Control* configuration (in traffic rules, URL rules, FTP rules, etc.) by a corresponding account from the directory service domain
- combination of local and domain account rights
- removal of the account from the local user database

Accounts not selected for the conversion are kept in the local database. Colliding accounts can be used — the accounts are considered as two independent accounts. However, directory service accounts must be always specified including the domain (even though it belongs to the primary domain); username without the domain specified represents an account from the local database. We recommend to remove all collisions by the conversion.

User authentication

User authentication overview

Kerio Control allows administrators to monitor connections (packet, connection, web pages or FTP objects and command filtering) related to each user. The username in each filtering rule represents the IP address of the host(s) from which the user is connected (i.e. all hosts the user is currently connected from). This implies that a user group represents all IP addresses its members are currently connected from.

In addition to authentication based access limitations, user login can be used to effectively monitor activities, using logs, and status and hosts and users. If there is no user connected from a certain host, only the IP address of the host will be displayed in the logs and statistics. In statistics, this host's traffic will be included in the group of *not logged in* users.

Firewall User Authentication

Any user with their own account in *Kerio Control* can authenticate at the firewall (regardless their access rights). Users can connect:

- Manually — in the browser, by opening the *Kerio Control* with the URL

`https://server:4081/` or `http://server:4080/`

It is also possible to authenticate for viewing of the web statistics at

`https://server:4081/star` or `http://server:4080/star`



Login to the *Administration* interface at `https://server:4081/admin` or `http://server:4080/admin` is not equal to user authentication at the firewall (i.e. the user does not get authenticated at the firewall by the login)!

- Automatically — IP addresses of hosts from which they will be authenticated automatically can be associated with individual users. This actually means that whenever traffic coming from the particular host is detected, *Kerio Control* assumes that it is currently used by the particular user, and the user is considered being authenticated from the IP address. However, users may authenticate from other hosts (using the methods described above).

IP addresses for automatic authentication can be set during definition of user account.

This authentication method is not recommended for cases where hosts are used by multiple users (user's identity might be misused easily).

- Redirection — when accessing any website (unless access to this page is explicitly allowed to unauthenticated users).

Login by re-direction is performed in the following way: user enters URL pages that he/she intends to open in the browser. *Kerio Control* detects whether the user has already authenticated. If not, *Kerio Control* will re-direct the user to the login page automatically. After a successful login, the user is automatically re-directed to the requested page or to the page including the information where the access was denied.

- Using NTLM — if *Internet Explorer* or *Firefox/SeaMonkey* is used and the user is authenticated in a *Windows NT* domain or *Active Directory*, the user can be authenticated automatically (the login page will not be displayed).

User authentication advanced options

Login/logout parameters can be set on the **Authentication Options** tab under **Users and Groups** → **Domains and User Login**.

Redirection to the authentication page

If the **Always require users to be authenticated when accessing web pages** option is enabled, user authentication will be required for access to any website (unless the user is already authenticated). The method of the authentication request depends on the method used by the particular browser to connect to the Internet:

- *Direct access* — the browser will be automatically redirected to the authentication page of the *Kerio Control*'s web interface and, if the authentication is successful, to the solicited web page.
- *Kerio Control proxy server* — the browser displays the authentication dialog and then, if the authentication is successful, it opens the solicited web page.

If the *Always require users to be authenticated when accessing web pages* option is disabled, user authentication will be required only for Web pages which are not available (are denied by URL rules) to unauthenticated users.



User authentication is used both for accessing a Web page (or/and other services) and for monitoring of activities of individual users (the Internet is not anonymous).

Force non-transparent proxy server authentication

Under usual circumstances, a user connected to the firewall from a particular computer is considered as authenticated by the IP address of the host until the moment when they log out manually or are logged out automatically for inactivity. However, if the client station allows multiple users connected to the computer at a moment (e.g. *Microsoft Terminal Services*, *Citrix Presentation Server* or *Fast user switching* on *Windows XP*, *Windows Server 2003*, *Windows Vista* and *Windows Server 2008*), the firewall requires authentication only from the user who starts to work on the host as the first. The other users will be authenticated as this user.

In case of *HTTP* and *HTTPS*, this technical obstruction can be passed by. In web browsers of all clients of the multi-user system, set connection to the Internet via the *Kerio Control's* proxy server, and enable the **Enable non-transparent proxy server** option in *Kerio Control*. The proxy server will require authentication for each new session of the particular browser.².

Forcing user authentication on the proxy server for initiation of each session may bother users working on “single-user” hosts. Therefore, it is desirable to force such authentication only for hosts used by multiple users. For this purpose, you can use the **Apply only for these IP addresses** option.

Automatic authentication (NTLM)

Browsers *Internet Explorer* and *Firefox/SeaMonkey* allow firewall authentication by NTLM. This means that the browser does not require username and password and simply uses the identity of the first user connected to *Windows*. However, the NTLM method is not available for other operating systems.

Automatically logout users when they are inactive

Timeout is a time interval (in minutes) of allowed user inactivity. When this period expires, the user is automatically logged out from the firewall. The default timeout value is 120 minutes (2 hours).

This situation often comes up when a user forgets to logout from the firewall. Therefore, it is not recommended to disable this option, otherwise login data of a user who forgot to logout might be misused by an unauthorized user.

² *Session* is every single period during which a browser is running. For example, in case of *Internet Explorer*, *Firefox* and *Google Chrome*, a session is terminated whenever all windows and tabs of the browser are closed, while in case of *SeaMonkey*, a session is not closed unless the *Quick Launch* program is stopped (an icon is displayed in the toolbar's notification area when the program is running).

Creating user groups in Kerio Control

User groups overview

User accounts can be sorted into groups. Creating user groups provides the following benefits:

- assigning access rights to groups of users
- using groups when defining access rules

Creating user groups

You can create either a local user group or [map existing groups from a directory service](#).

Creating local groups

Local groups are created and managed through the Kerio Control administration interface.

1. Go to the administration interface.
2. In section **Groups**, select **Local User Database**.
3. Click **Add**.
4. On the **General** tab, enter a group name.
5. On tab **Members** click **Add**.
6. Select users you wish to add to the group and confirm.



You can also go to **Users** and select a group in user's settings.

7. On tab **Rights**, you can configure access rights for this group. Read more in [Setting access rights in Kerio Control](#).
8. Save the settings.

Configuring SSL certificates in Kerio Control

SSL certificates overview

You need a [SSL](#) certificate to use encrypted communication (VPN, HTTPS etc.). SSL certificates are used to authenticate an identity on a server.

For generating SSL certificates, Kerio Control uses its own local authority. Kerio Control creates the first certificate during the installation. The server can use this certificate.

However, upon their first login, users will have to confirm they want to go to a page which is not trustworthy. To avoid this, you must generate a new certificate request in Kerio Control and send it to a certification authority for authentication.

Kerio Control supports certificates in the following format:

- Certificate (public key) — X.509 Base64 in text format (PEM). The file has suffix `.crt`.
- Private key — the file is in RSA format and it has suffix `.key` with 4KB max. Passphrase is supported.
- Certificate + private key in one file — format: PKCS#12. The file has suffix `.pfx` or `.p12`.

Creating a new Local Authority

Local authority is generated automatically during the installation. However, hostname and other data are incorrect. For this reason we recommend to generate a new certificate for the local authority.

To create and use a certificate for the local authority, follow these instructions:

1. Open **Definitions** → **SSL Certificates**.
2. Click **Add** → **New Certificate for Local Authority**.
3. In the **New Certificate for Local Authority** dialog box, type the Kerio Control hostname, official name of your company, city and country where your company resides and the period of validity.

The new Local Authority will be available and visible in **Definitions** → **SSL Certificates**, the old one will be:

- changed from Local Authority to Authority
- renamed to Obsolete Local Authority
- available as a trusted authority for IPsec

Creating a certificate signed by Local Authority

Create a new certificate if the old one is not valid anymore.

To create a certificate, follow these instructions:

1. Open section **Definitions** → **SSL Certificates**.
2. Click **Add** → **New Certificate**.
3. In the **New Certificate** dialog box, type the hostname of Kerio Control, the official name of your company, city and country where your company resides and the period of validity.
The **Hostname** entry is a required field.
4. Save the settings.

Now you can use this certificate. Using the certificate means that you have to select it in the specific settings (for example SSL certificate for VPN server you have to select in **Interfaces** → **VPN Server**).

Creating a certificate signed by a Certification Authority

To create and use a certificate signed by a trustworthy certification authority, follow these instructions:

1. Open **Definitions** → **SSL Certificates**.
2. Click **Add** → **New Certificate Request**.
3. In the **New Certificate Request** dialog box, type the hostname of Kerio Control, the official name of your company, city and country where your company resides and the period of validity.
The **Hostname** entry is a required field.
4. Select the certificate request and click **More Actions** → **Export**.
5. Save the certificate to your disk and email it to a certification organization.
For example, *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode* and so on.
6. Once you obtain your certificate signed by a certification authority, go to **Definitions** → **SSL Certificates**.
7. Select the original certificate request (the certificate request and the signed certificate must be matched)
8. Click **More Actions** → **Import**.

The certificate replaces the certificate request. You can use this certificate. Using the certificate means that you have to select it in the specific settings (for example SSL certificate for VPN server you have to select in **Interfaces** → **VPN Server**).

Configuring IP address groups

Using IP address groups

IP address groups help easily define who has access, for example, to traffic rules.

Configuring IP address group

1. In the administration interface, go to **Definitions** → **IP Address Groups**.
2. Click **Add** and enter a name for the group (or select an existing one).
3. Select the type and specify the address(es). The following types are available:
 - **Host**
 - **Network/Mask**
 - **Address Range**
An interval of IP addresses defined by starting and end IP address including the both limit values.
 - **IP address group**
Another group of IP addresses — groups can be cascaded.
 - **Firewall**
Firewall is a special group including all the firewall's IP addresses.
4. You can add a description for better reference.
5. Save the settings.

Creating time ranges in Kerio Control

Time ranges overview

Time ranges can be applied to various policies (e.g. Traffic or URL rules) to define intervals for when rules should be valid.

A time range may consist of multiple intervals with different settings.

Add Time Range

Add to a group

☐ Select existing: No groups available

☒ Create new: Working hours

Description

Weekday

Time settings

Type: Daily

From: 08:00

To: 17:59

Valid on: Weekdays

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Sun

Times set in the dialog correspond with server time zone.

OK Cancel

Figure 1 Time ranges

Defining time ranges

1. In the administration interface, go to **Definitions** → **Time Ranges**.
2. Click **Add**.
3. Enter a name for the group (or select an existing one).

4. You can add a description for the time interval.
5. Configure the **Time settings** — frequency, time interval and days if applicable.
6. Save the settings.

Using services

Services

Services are defined by a communication protocol and by a port number (e.g. the HTTP service uses the TCP protocol with the port number 80). You can also match so-called [protocol inspector](#) with certain service types.

Using services

Example: You want to perform [protocol inspection](#) of the HTTP protocol at port 8080:

1. In the administration interface, go to **Definitions** → **Services**.
Some standard services, such as HTTP, FTP, DNS etc., are already predefined.
2. Click **Add**.
3. In the **Add Service** dialog, type a name of a new service — TCP.
4. Type a description.
5. Select a TCP protocol.



The **other** option allows protocol specification by the number in the IP packet header. Any protocol carried in IP (e.g. GRE — protocol number is 47) can be defined this way.

6. Select the HTTP protocol inspector.



Each inspector should be used for the appropriate service only. Functionality of the service might be affected by using an inappropriate inspector.

7. Type 8080 to **Destination port**.

If the TCP or UDP communication protocol is used, the service is defined with its port number. In case of standard client-server types, a server is listening for connections on a particular port (the number relates to the service), whereas clients do not know their port in advance (ports are assigned to clients during connection attempts). This means that source ports are usually not specified, while destination ports are usually known in case of standard services.

Source and destination ports can be specified as:

- **Any** — all the ports available (1–65535)
- **Equal to** — a particular port (e.g. 80)
- **Greater than, Less than** — all ports with a number that is either greater or less than the number defined
- **Not equal to** — all ports that are not equal to the one defined
- **In range** — all ports that fit to the range defined (including the initial and the terminal ones)
- **List** — list of the ports divided by commas (e.g. 80, 8000, 8080)

8. Save the settings.

This ensures that the HTTP protocol inspector will be automatically applied to any TCP traffic at port 8080 and passing through Kerio Control.

Protocol inspectors

Kerio Control includes special subroutines that monitor all traffic using application protocols, such as HTTP, FTP or others. The modules can be used to modify (filter) the communication or adapt the firewall's behavior according to the protocol type. Benefits of protocol inspectors can be better understood through the two following examples:

HTTP protocol inspector monitors traffic between browsers and web servers. It can be used to block connections to particular pages or downloads of particular objects (i.e. images, pop-ups, etc.).

The protocol inspector is enabled if it is set in the service definition and if the corresponding traffic is allowed. Each protocol inspector applies to a specific protocol and service. By default, all available protocol inspectors are used in definitions of corresponding services (i.e. they will be applied to matching traffic automatically).

To apply a protocol inspector explicitly to other traffic, it is necessary to edit, or add a new service where this inspector will be used.



Protocol inspectors cannot be applied to secured traffic (SSL/TLS).

Disabling a protocol inspector

Under certain circumstances, appliance of a protocol inspector is not desirable. Therefore, it is possible to disable a corresponding inspector:

1. In the administration interface, go to **Definitions** → **Services**.
2. Select a service and double-click on it.
3. In the **Edit Service** dialog, select none in the **Protocol inspector** field.

Using services

4. Save the settings.

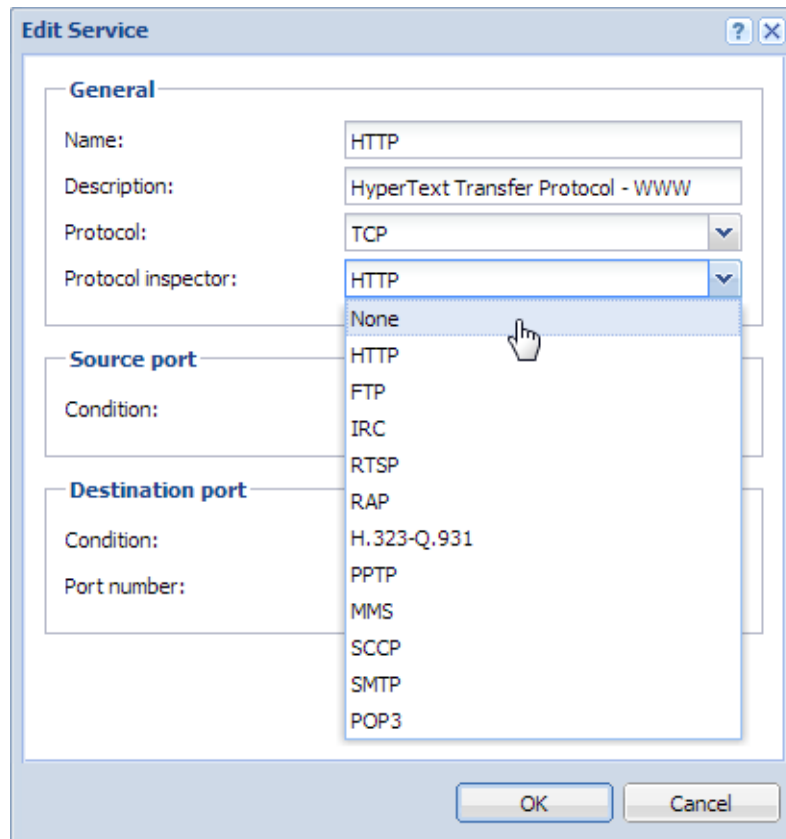


Figure 1 Disabling a protocol inspector

Using Status - Active Hosts

Status - Active Hosts overview

In **Status** → **Active Hosts**, the hosts within the local network or active users using *Kerio Control* for communication with the Internet will be displayed.

Look at the upper window to view information on individual hosts, connected users, data size/speed, etc.

The following information can be found in the **Active Hosts** window:

Hostname

DNS name of a host. In case that no corresponding DNS record is found, IP address is displayed instead.

User

Name of the user which is connected from a particular host. If no user is connected, the item is empty.

Currently Rx, Currently Tx

Monitors current traffic speed (kilobytes per second) in both directions (from and to the host — **Rx** values represent incoming data, **Tx** values represent outgoing data)

The following columns are hidden by default. To view these columns select the **Modify columns** option in the context menu (see below).

IP address

IP address of the host from which the user is connecting from (i.e. which communicates with the Internet via *Kerio Control*)

Login Time

Date and time of the recent user login to the firewall

Login Duration

Monitors length of the connection. This information is derived from the current time status and the time when the user logged on

Inactivity Time

Duration of the time with zero data traffic. You can set the firewall to logout users automatically after the inactivity exceeds allowed inactivity time.

Start Time

Date and time when the host was first acknowledged by *Kerio Control*. This information is kept in the operating system until the *Kerio Control Engine* disconnected.

Total received, Total transmitted

Total size of the data (in kilobytes) received and transmitted since the **Start time**

Connections

Total number of connections to and from the host. Details can be displayed in the context menu (see below)

Authentication method

Authentication method used for the recent user connection:

- **plaintext** — user is connected through an insecure login site **plaintext**
- **SSL** — user is connected through a login site protected by SSL security system **SSL**
- **proxy** — a *Kerio Control* proxy server is used for authentication and for connection to websites,
- **NTLM** — user was automatically authenticated in the NT domain by NTLM (works with *Internet Explorer* or *Firefox/SeaMonkey*),
- **VPN client** — user has connected to the local network using the *Kerio VPN Client*.



Connections are not displayed and the volume of transmitted data is not monitored for VPN clients.

Information displayed in the **Active Hosts** window can be refreshed by clicking on the **Refresh** button.

Use the **Show / Hide details** to open the bottom window providing detailed information on a user, host and open connections.

Active Hosts dialog options

Clicking the right mouse button in the **Active Hosts** window (or on the record selected) will display a context menu that provides the following options:

User Quota

Use this option to show quota of the particular user (the *Kerio Control Administration* interface switches to the **User Quota** tab in **Status** → **User Statistics** and selects the particular user automatically).

The **User quota** option is available in the context menu only for hosts from which a user is connected to the firewall.

Reload

This option refreshes information in the **Active Hosts** window immediately (this function is equal to the **Refresh** button displayed at the bottom of the window).

Automatic refresh

Settings for automatic refreshing of the information in the **Active Hosts** window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (**No refresh**).

Logout User

Immediate logout of a selected user.

Logout All Users

Immediate logout of all firewall users.

Manage Columns

By choosing this option you can select which columns will be displayed in the **Active Hosts** window.

Detailed information on a selected host and user

Detailed information on a selected host and connected user are provided in the bottom window of the **Active Hosts** section.

Open the **General** tab to view information on user's login, size/speed of transmitted data and information on activities of a particular user.

Login information

Information on logged-in users:

- **User** — name of a user, DNS name (if available) and IP address of the host from which the user is connected
- **Login time** — date and time when a user logged-in, authentication method that was used and inactivity time (idle).

If no user is connected from a particular host, detailed information on the host are provided instead of login information.

- **Host** — DNS name (if available) and IP address of the host
- **Idle time** — time for which no network activity performed by the host has been detected

Traffic information

Information on size of data received (**Download**) and sent (**Upload**) by the particular user (or host) and on current speed of traffic in both directions.

Overview of detected activities of the particular user (host) are given in the main section of this window:

Activity Time

Time (in minutes and seconds) when the activity was detected.

Activity Event

Type of detected activity (network communication). *Kerio Control* distinguishes between the following activities: *SMTP*, *POP3*, *WWW* (HTTP traffic), *FTP*, **Streams** (real-time transmission of audio and video streams) and *P2P* (use of Peer-to-Peer networks).



Kerio Control is not able to recognize which type of *P2P* network is used. According to results of certain testing it can only "guess" that it is possible that the client is connected to such network.

Activity Description

Detailed information on a particular activity:

- **WWW** — title of a Web page to which the user is connected (if no title is available, URL will be displayed instead). Page title is a hypertext link — click on this link to open a corresponding page in the browser which is set as default in the operating system.



For better transparency, only the first visited page of each web server to which the user connected is displayed.

- **SMTP, POP3** — DNS name or IP address of the server, size of downloaded/uploaded data.
- **FTP** — DNS name or IP address of the server, size of downloaded/saved data, information on currently downloaded/saved file (name of the file including the path, size of data downloaded/uploaded from/to this file).
- **Multimedia** (real time transmission of video and audio data) — DNS name or IP address of the server, type of used protocol (*MMS, RTSP, RealAudio*, etc.) and volume of downloaded data.
- **P2P** — information that the client is probably using Peer-To-Peer network.

Information about connections from/to the Internet

On the **Connections** tab, you can view detailed information about connections established from the selected host to the Internet and in the other direction (e.g. by mapped ports, *UPnP*, etc.). The list of connections provides an overview of services used by the selected user. Undesirable connections can be terminated immediately.

Information about connections:

Traffic Rule

Name of the *Kerio Control* traffic rule by which the connection was allowed.

Service

Name of the service. For non-standard services, port numbers and protocols are displayed.

Source, Destination

Source and destination IP address (or name of the host in case that the **Show DNS names** option is enabled —see below).

Bandwidth Management Rule

Bandwidth limiting or reservation rule applied to this connection (empty column means that no rule has been applied).

Load Balancing

If the firewall works in the load balancing mode, the interface over which the connection is directed is displayed here (for connections to/from the Internet).

Source port, Destination port

Source and destination port (only for TCP and UDP protocols).

Protocol

Protocol used for the transmission (TCP, UDP, etc.).

Timeout

Time left before the connection will be removed from the table of *Kerio Control* connections.

Each new packet within this connection sets timeout to the initial value. If no data is transmitted via a particular connection, *Kerio Control* removes the connection from the table upon the timeout expiration — the connection is closed and no other data can be transmitted through it.

Rx, Tx

Volume of incoming (**Rx**) and outgoing (**Tx**) data transmitted through a particular connection (in KB).

Information

Additional information (such as a method and URL in case of HTTP protocol).

Use the **Show DNS names** option to enable/disable showing of DNS names instead of IP addresses in the **Source** and **Destination** columns. If a DNS name for an IP address cannot be resolved, the IP address is displayed.

You can click on the **Colors** button to open a dialog where colors used in this table can be set.



1. Upon right-clicking on a connection, the context menu extended by the **Kill connection** option is displayed. This option can be used to kill the particular connection between the LAN and the Internet immediately.
2. The selected host's overview of connections lists only connections established from the particular host to the Internet and vice versa. Local connections established between the particular host and the firewall can be viewed only in **Status → Connections**. Connections between hosts within the LAN are not routed through *Kerio Control*, and therefore they cannot be viewed there.

Histogram

The **Histogram** tab provides information on data volume transferred from and to the selected host in a selected time period. The chart provides information on the load of this host's traffic on the Internet line through the day.

Using Status - Active Hosts

Select an item from the **Time interval** combo box to specify a time period which the chart will refer to (2 hours or 1 day). The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit *B/s*).

This chart includes volume of transferred data in the selected direction in certain time intervals (depending on the selected period). The green curve represents volume of incoming data (download) in a selected time period, while the area below the curve represents the total volume of data transferred in the period. The red curve and area provide the same information for outgoing data (upload). Below the chart, basic statistic information, such as volume of data currently transferred (in the last interval) and the average and maximum data volume per an interval, is provided.

Select an option for **Picture size** to set a fixed format of the chart or to make it fit the screen.

Using Status - Active Connections

Status - Active Connections overview

In **Status** → **Active Connections**, all the network connections which can be detected by *Kerio Control* include the following:

- client connections to the Internet through *Kerio Control*
- connections from the host on which *Kerio Control* is running
- connections from other hosts to services provided by the host with *Kerio Control*
- connections performed by clients within the Internet that are mapped to services running in LAN

Kerio Control administrators are allowed to close any of the active connections.



1. Connections among local clients will not be detected nor displayed by *Kerio Control*.
2. UDP protocol is also called connectionless protocol. This protocol does not perform any connection. The communication is performed through individual messages (so-called datagrams). Periodic data exchange is monitored in this case.

One connection is represented by each line of the **Connections** window. These are network connections, not user connections (each client program can occupy more than one connection at a given moment). Lines are highlighted: green color marks outgoing connections, while red color marks incoming connections.

The columns contain the following information:

Traffic Rule

Name of the *Kerio Control* traffic rule by which the connection was allowed.

Service

Name of transmitted service (if such service is defined in *Kerio Control*. If the service is not defined in *Kerio Control*, the corresponding port number and protocol will be displayed instead (e.g. **5004/UDP**).

Source, Destination

IP address of the source (the connection initiator) and of the destination.

Using Status - Active Connections

Bandwidth Management Rule

Bandwidth limiting or reservation rule applied to this connection (empty column means that no rule has been applied).

Load Balancing

If the firewall works in the load balancing mode, the interface over which the connection is directed is displayed here (for connections to/from the Internet).

Source port, Destination port

Ports used for the particular connection.

Protocol

Communication protocol (**TCP** or **UDP**)

Timeout

Time left until automatic disconnection. The countdown starts when data traffic stops. Each new data packet sets the counter to zero.

Age

Time for which the connection has been established.

Rx, Tx

Total size of data received (**Rx**) or transmitted (**Tx**) during the connection (in kilobytes). Received data means the data transferred from **Source** to **Destination**, transmitted data means the opposite.

Info

An informational text describing the connection (e.g. about the protocol inspector applied to the connection).

Type

Connection direction — either incoming or outgoing.

Information in **Connections** can be refreshed automatically within a user defined interval or the **Refresh** button can be used for manual refreshing.

Options of the Connections Dialog

The following options are available below the list of connections:

- **Hide local connections** — connections from or/and to the *Kerio Control* host will not be displayed in the **Connections** window.

This option only makes the list better-arranged (especially if we are curious only about connections between hosts in the local network and the Internet).

- **Show DNS names** — this option displays DNS names instead of IP addresses. If a DNS name is not resolved for a certain connection, the IP address will be displayed.

Right-click on the **Connections** window (on the connection selected) to view a context menu including the following options:

Kill Connection

Use this option to finish selected connection immediately (in case of UDP connections all following datagrams will be dropped).



This option is active only if the context menu has been called by right-clicking on a particular connection. If called up by right-clicking in the **Connections** window (with no connection selected), the option is inactive.

Reload

This option will refresh the information in the **Connections** window immediately. This function is equal to the function of the **Refresh** button at the bottom of the window.

Automatic refresh

Settings for automatic refreshing of the information in the **Connections** window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (**No refresh**).

Manage Columns

By choosing this option you can select which columns will be displayed in the **Connections** window.

Color settings

Clicking on the **Colors** button displays the color settings dialog to define colors for each connection:

For each item either a color or the **Default** option can be chosen. Default colors are set in the operating system (the common setting for default colors is black font and white background).

Text Color

- **Active connections** — connections with currently active data traffic
- **Inactive connections** — TCP connections which have been closed but 2 minutes after they were killed they are still kept active — to avoid repeated packet mishandling)

Background color

- **Local connections** — connections where an IP address of the host with *Kerio Control* is either source or destination
- **Inbound connections** — connections from the Internet to the local network (allowed by firewall)
- **Outbound connections** — connections from the local network to the Internet



Incoming and outgoing connections are distinguished by detection of direction of IP addresses — “out” (SNAT) or “in” (DNAT).

Using Status - VPN Clients

Status - VPN Clients overview

In **Status** → **VPN clients**, you can see an overview of VPN clients currently connected to the *Kerio Control*'s VPN server.

The information provided is as follows:

- Username used for authentication to the firewall. VPN traffic is reflected in statistics of this user.
- The operating system on which the user have the *Kerio VPN Client* installed.
- DNS name of the host which the user connects from. If *Kerio Control* cannot resolve the corresponding hostname from the DNS, its (public) IP address is displayed instead.
- IP address assigned to the client by the VPN server. This IP address “represents” the client in the local network.
- Session duration.
- *Kerio VPN Client* version, including build number.
- IP address — public IP address of the host which the client connects from (see the **Hostname** column above).
- Client status — *connecting*, *authenticating* (*Kerio Control* verifies username and password), *authenticated* (username and password correct, client configuration in progress), *connected* (the configuration has been completed, the client can now communicate with hosts within the local network).



Disconnected clients are removed from the list automatically.

Using Status - Alert Messages

Status - Alert Messages overview

Kerio Control enables automatic sending of messages informing the administrator about important events. This makes the firewall administration more comfortable, since it is not necessary to connect to the firewall too frequently to view all status information and logs (however, it is definitely worthy to do this occasionally).

Kerio Control generates alert messages upon detection of any specific event for which alerts are preset. All alert messages are recorded into the **Alert** log. The firewall administrator can specify which alerts will be sent to whom, as well as a format of the alerts. Sent alerts can be viewed in **Status → Alerts**.



SMTP relay must be set in *Kerio Control*, otherwise alerting will not work.

Alert Settings

Alerts settings can be configured in the **Alerts settings** tab under **Configuration → Accounting**.

This tab provides list of “rules” for alert sending. Use checking boxes to enable/disable individual rules.

Click on **Add**. Use the **Edit** button to (re)define an alert rule.

Alert

Type of the event upon which the alert will be sent:

- **Virus detected** — antivirus engine has detected a virus in a file transmitted by HTTP, FTP, SMTP or POP3.
- **Antivirus check failed** — for some reason, the antivirus engine failed to check the file (typical for password-protected or damaged files).
- **Host connection limit reached** — a host in the local network has reached the connection limit. This may indicate deployment of an undesirable network application (e.g. Trojan horse or a spyware) on a corresponding host.
- **Low free disk space warning** — this alert warns the administrator that the free space of the *Kerio Control* host is low (under 11 percent of the total disk capacity). *Kerio Control* needs enough disk space for saving of logs, statistics, configuration settings, temporary files (e.g. an installation archive of a new version or a file which is currently scanned by an antivirus engine) and other information. Whenever the *Kerio Control* administrator receives such alert message, adequate actions should be performed immediately.

- **New version available** — a new version of *Kerio Control* has been detected at the server of Kerio Technologies during an update check.
- **User transfer quota exceeded** — a user has reached daily, weekly or monthly user transfer quota and *Kerio Control* has responded by taking an appropriate action.
- **Connection failover event** — the Internet connection has failed and the system was switched to a secondary line, or vice versa (it was switched back to the primary line).
- **License expiration** — expiration date for the corresponding license or *Kerio Control* Software Maintenance or license of any module integrated in *Kerio Control* (such as *Kerio Control Web Filter*, the Sophos antivirus, etc.) is getting closer. The administrator should check the expiration dates and prolong a corresponding license or Software Maintenance.

Actions

Method of how the user will be informed:

- **Send email** — information will be sent by an email message,
- **Send SMS (shortened email)** — short text message will be sent to the user's cell phone.



SMS messages are also sent as email. User of the corresponding cell phone must use an appropriate email address (e.g. number@provider.com). Sending of SMS to telephone numbers (for example via GSM gateways connected to the *Kerio Control* host) is not supported.

To

Email address of the recipient or of his/her cell phone (related to the **Action** settings). Recipients can be selected from the list of users (email addresses) used for other alerts or new email addresses can be added by hand.

Valid at time interval

Select a time interval in which the alert will be sent. Click **Edit** to edit the interval or to create a new one.

Alert Templates

Formats of alert messages (email or/and SMS) are defined by templates. Individual formats can be viewed in the **Status** → **Alerts** section of the administration interface. Templates are predefined messages which include certain information (e.g. username, IP address, number of connections, virus information, etc.) defined through specific variables. *Kerio Control* substitutes variables by corresponding values automatically. The *Kerio Control* administrator can customize these templates.

Templates are stored in the `templates` subdirectory of the installation directory of *Kerio Control*:

- the `console` subdirectory — messages displayed in the left-positioned part of the section **Status** → **Alerts** (overview),
- the `console\details` subdirectory — messages displayed at the right part of the section **Status** → **Alerts** (details),
- the `email` subdirectory — messages sent by email (each template contains a message in the plain text and HTML formats),
- the `sms` subdirectory — SMS messages sent to a cell phone.

Each subdirectory includes a set of templates in all languages supported by *Kerio Control*. In the *Kerio Control Administration* interface, alerts are displayed in the currently set language. Email and SMS alerts sent are always in English.

Alerts overview in the administration interface

Section **Status** → **Alerts** displays all alerts sent to users since startup of *Kerio Control*. Alerts are displayed in the language of the *Administration Console*.



Email sending of individual alerts can be set under **Configuration** → **Accounting**, on the **Alerts** tab (see above).

On the left side of the **Alerts** section, all sent alerts (sorted by dates and times) are listed.

Each line provides information on one alert:

- **Date** — date and time of the event,
- **Alert** — event type.

Click an event to view detailed information on the item including a text description (defined by templates under `console\details` — see above) in the right-side section of the window.



Details can be optionally hidden or showed by clicking the **Hide/Show details** button (details are displayed by default).

Using Status - Alert Messages

Alert Log

The *Alert* log gathers records about all alerts generated by *Kerio Control* (no matter if they were or were not sent by email to user/administrator).

Using Status - Statistics

Status - Statistics overview

Statistical information about users (volume of transmitted data, used services, categorization of web pages) as well as of network interfaces of the *Kerio Control* host (volume of transmitted data, load on individual lines) can be viewed in *Kerio Control*.

In the *Kerio Control Administration* interface, it is possible to view basic quota information for individual users (volume of transferred data and quota usage information) and statistics of network interfaces (transferred data, traffic charts).

Detailed statistics of users, web pages and volume of transferred data are available in the firewall web user interface.

Volume of transferred data and quota usage

The **User Statistics** of the **Status** section provides detailed statistics on volume of data transmitted by individual users during various time periods (today, this week, this month and total).

The **Quota** column provides usage of transfer quota by a particular user in percents. Colors are used for better reference:

- green — 0%-74% of the quota is used
- yellow — 75%-99% of the quota is used
- red — 100% (limit reached)



1. User quota consists of three limits: daily, weekly and monthly. The **Quota** column provides the highest value of the three percentual values (if the daily usage is 50% of the daily quota, the weekly usage is 90% and the monthly usage is 70%, yellowed **90%** value is displayed in the **Quota** column).
2. Monthly quota is reset automatically at the beginning of an accounting period. This period may differ from a civil month.

The **all users** line provides total volume of data transmitted by all users in the table (even of the unrecognized ones). The **unrecognized users** item includes all users who are currently not authenticated at the firewall. These lines do not include quota usage information.



1. Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission is related to the user (the **IN** direction stands for data received by the user, while **OUT** represents data sent by the user).
2. Information of volume of data transferred by individual users is saved in the `stats.cfg` file in the *Kerio Control* directory. This implies that this data will be saved the next time the *Kerio Control Engine* will be started.

User Quota dialog options

Right-click on the table (or on an item of a selected user) to open the context menu with the following options:

Delete User Traffic Counters

Removal of the selected line with data referring to a particular user. This option is helpful for reference purposes only (e.g. to exclude blocked user accounts from the list, etc.). Removed accounts will be added to the overview automatically when data in the particular account is changed (e.g. when we unblocked an account and its user connects and starts to communicate again).



Be aware that using this option for the **all users** item resets counters of all users, including unrecognized ones!



Values of volumes of transferred data are also used to check user traffic quota. Reset of user statistics also unblocks traffic of the particular user in case that the traffic has been blocked for quota reasons.

View host...

This option is not available unless the selected user is connected to the firewall. The **View host** option switches to the **Status** → **Active Hosts** section of the host the particular user is connected from.

If the user is connected from multiple hosts, the **View host** option opens a submenu with a list of all hosts which the particular user is connected from.

Reload

This option will refresh the information on the **User Statistics** tab immediately. This function is equal to the function of the **Refresh** button at the bottom of the window.

Automatic refresh

Settings for automatic refreshing of the information on the **User Statistics** tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (**No refresh**).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table.

Traffic Charts

The **Interface statistics** tab in **Status** → **Statistics** provides detailed information on volume of data transmitted in both directions through individual interfaces of the firewall in selected time intervals (today, this week, this month, total).

Interfaces can be represented by network adapters, dial-ups or VPN tunnels. **VPN server** is a special interface — communication of all VPN clients is represented by this item in *Interface statistics*.

Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission is related to the interface (the **IN** direction stands for data received by the interface, while **OUT** represents data sent from the interface).

Example

The firewall connects to the Internet through the **Public** interface and the local network is connected to the **LAN** interface. A local user downloads 10 MB of data from the Internet. This data will be counted as follows:

- **IN** at the **Public** interface is counted as an **IN** item (data from the Internet was received through this interface),
- at the **LAN** interface as **OUT** (data was sent to the local network through this interface).



Interface statistics are saved into the `stats.cfg` configuration file in the *Kerio Control* installation directory. This implies that they are not reset when the *Kerio Control Engine* is closed.

Interface Statistics menu

A context menu providing the following options will be opened upon right-clicking anywhere in the table (or on a specific interface):

Reset Interface Statistics

This option resets statistics of the selected interface. It is available only if the mouse pointer is hovering an interface at the moment when the context menu is opened.

Reload

This option will refresh the information on the **Interface Statistics** tab immediately. This function is equal to the function of the **Refresh** button at the bottom of the window.

Automatic refresh

Settings for automatic refreshing of the information on the **Interface Statistics** tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (**No refresh**).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table.

Remove interface statistics

This option removes the selected interface from the statistics. Only inactive interfaces (i.e. disconnected network adapters, hung-up dial-ups, disconnected VPN tunnels or VPN servers which no client is currently connected to) can be removed. Whenever a removed interface is activated again (upon connection of the VPN tunnel, etc.), it is added to the statistics automatically.

Graphical view of interface load

The traffic processes for a selected interface (transfer speed in **B/s**) and a specific time period can be viewed in the chart provided in the bottom window of the **Interface statistics** tab. Use the **Show details** / **Hide details** button to show or hide this chart (the show mode is set by default).

The period (**2 hours** or **1 day**) can be selected in the **Time interval** box. The selected time range is always understood as the time until now ("last 2 hours", "last 24 hours").

The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit *B/s*).

The legend above the graph shows the sampling interval (i.e. the time for which a sum of connections or messages is counted and is displayed in the graph).

Example

Suppose the *1 day* interval is selected. Then, an impulse unit is represented by 5 minutes. This means that every 5 minutes an average traffic speed for the last 5 minutes is recorded in the chart.

Using Status - System Health

Status - System Health overview

The **System Health** section shows current usage of CPU, RAM and the disk space of the computer or device where *Kerio Control* is running.

Time Range

Selection of time period for which CPU load and RAM usage is displayed (2 hours or 1 day).

CPU

Timeline of the computer's (device's) CPU load. Short time peak load rates ("peaks" of the chart) are not unusual and can be caused for example by the network activity.

RAM

RAM usage timeline.

Storage Space

Currently used and free space on the disk space or a memory card.

Tasks

Restart of the system or shutdown of the device (available only in editions *Appliance* and *Box*).

Lack of system resources may seriously affect functionality of *Kerio Control*. If these resources are permanently overloaded, it is recommended to check other applications and services running on the system. In case of editions *Appliance* and *Box* it is recommended to restart *Kerio Control* and then check system resources usage once again.

If storage space is missing, it is possible to click on **Manage** and delete some files created by running *Kerio Control* (logs, statistics data, etc.) and set limits which prevent possible running out of storage space.

Storage space management

To get enough free space on the disk, you can use the following methods:

- Free disk space by deleting old or unnecessary files (logs, statistics, etc.),
- Set size limits for files created by *Kerio Control* appropriately.

The dialog shows only such components data of which occupy at least a certain amount of space (MB).

Using logs

Logs overview

Logs keep information records of selected events occurred in or detected by Kerio Control. Each log is displayed in a window in the **Logs** section.

Each event is represented by one record line. Each line starts with a time mark in brackets (date and time when the event took place, in seconds). This mark is followed by an information, depending on the log type. If the record includes a URL, it is displayed as a hypertext link. Follow the link to open the page in your default browser.

Optionally, records of each log may be recorded in files on the local disk³ and/or on the *Syslog* server.

Locally, the logs are saved in the files under the `logs` subdirectory where *Kerio Control* is installed. The file names have this pattern:

`log_name.log`

(e.g. `debug.log`). Each log includes an `.idx` file, i.e. an indexing file allowing faster access to the log when displayed in the *Kerio Control Administration* interface.

Individual logs can be rotated — after a certain time period or when a threshold of the file size is reached, log files are stored and new events are logged to a new (empty) file.

Kerio Control allows to save a selected log (or its part) in a file as plaintext or in HTML. The log saved can be analyzed by various tools, published on web servers, etc.

Logs Context Menu

When you right-click inside any log window, a context menu will be displayed where you can choose several functions or change the log's parameters (view, logged information).

Copy

This action makes a copy of the selected text from the log and keeps it in the clipboard. Text selection and copying through the context menu is supported only in *Internet Explorer* where it is necessary to allow access to the clipboard.

For this operation it is recommended to use shortcut `Ctrl+C` (or `Apple+C` on Mac). This method is compatible throughout operating systems.

³ The local disk is a drive of the host where *Kerio Control* is installed, not a disk of the host you perform the administration on!

Save Log

This option saves the log or selected text in a file as plaintext or in HTML.

Hint

This function provides more comfortable operations with log files than a direct access to log files on the disk of the computer where *Kerio Control* is installed. Logs can be saved even if *Kerio Control* is administered remotely.

The **Save log** option opens a dialog box where the following optional parameters can be set:

- **Target file** — name of the file where the log will be saved. By default, a name derived from the file name is set. The file extension is set automatically in accordance with the format selected.
- **Format** — logs can be saved as plaintext or in HTML. If the HTML format is used, colors will be saved for the lines background (see section *Highlighting*) and all URLs will be saved as hypertext links.
- **Source** — either the entire log or only a part of the text selected can be saved. Bear in mind that in case of remote administration, saving of an entire log may take some time.

Highlighting

Highlighting may be set for logs meeting certain criteria (for details, see below).

Log Settings

A dialog where log parameters such as log file name and path, rotation and *Syslog* parameters can be set.

Clear Log

Removes entire log. All information of will be removed from the log forever (not only the information saved in the selected window).



Removed logs cannot be refreshed anymore.



Only users with read and write rights are allowed to change log settings or remove logs.

Log highlighting

For better reference, it is possible to set highlighting for logs meeting certain criteria. Highlighting is defined by special rules shared by all logs. Seven colors are available (plus the background color of unhighlighted lines), however, number of rules is not limited.

Use the **Highlighting** option in the context pop-up menu of the corresponding log to set highlighting parameters.

Highlighting rules are ordered in a list. The list is processed from the top. The first rule meeting the criteria stops other processing and the found rule is highlighted by the particular color. Thanks to these features, it is possible to create even more complex combinations of rules, exceptions, etc. In addition to this, each rule can be “disabled” or “enabled” for as long as necessary.

Click on **Add**. Use the **Edit** button to (re)define a highlighting rule.

Each highlighting rule consists of a condition and a color which will be used to highlight lines meeting the condition. Condition can be specified by a substring (all lines containing the string will be highlighted) or by a so called regular expression (all lines containing one or multiple strings matching the regular expression will be highlighted).

The **Description** item is used for reference only. It is recommended to describe all created rules well (it is recommended to mention also the name of the log to which the rule applies).



Regular expression is such expression which allows special symbols for string definition. *Kerio Control* accepts all regular expressions in accordance with the POSIX standard.

For detailed instructions contact Kerio technical support. For detailed information, refer for example to

<http://www.gnu.org/software/grep/>

Logs Settings

In option **Log settings** in the log context menu, you can select options for saving the log and sending messages to the *Syslog* server. These parameters are saved separately for each log.

File Logging

Use the **File Logging** tab to define file name and rotation parameters.

Enable logging to file

This option enables/disables saving to a file. The file inherits the log’s name plus the .log extension. If log rotation is enabled, older logs are saved in files of the particular names including date and time of rotation.

All log files are stored in the **logs** subfolder of the *Kerio Control* head directory, i.e.:

- in *Windows* edition typically:
C:\Program Files\Kerio\WinRoute\Firewall\logs
- or run update of the product in editions *Appliance* and *Box* b going to
/opt/kerio/winroute/logs



If the log is not saved in a file on the disk, only records generated since the last login to *Kerio Control Engine* will be shown. After logout (or closing of the window with the administration interface), the records will be lost.

Rotate regularly

Set intervals in which the log will be rotated regularly. The file will be stored and a new log file will be started in selected intervals.

Weekly rotation takes effect on Sunday nights. Monthly rotation is performed at the end of the month (in the night when one month ends and another starts).

Rotate when file exceeds size

Set a maximal size for each file. Whenever the threshold is reached, the file will be rotated. Maximal size is specified in megabytes (MB).

Keep at most ... log file(s)

Maximal count of log files that will be stored. Whenever the threshold is reached, the oldest file will be deleted.



1. If both **Rotate regularly** and the **Rotate when file exceeds size** are enabled, the particular file will be rotated whenever one of these conditions is met.
2. Setting of statistics and quotas accounting period does not affect log rotation. Rotation follows the rules described above.

Syslog Logging

Tab **External log** allows sending of individual log records to the *Syslog* server. Simply enter the DNS name or the IP address of the *Syslog* server.

The *Syslog* server distinguishes logs by *Facility* and *Severity*. These values are fixed for each log (current values for individual logs can be found *External log*).

In *Kerio Control*, for all logs *Facility* is set to *16: Local use 0*. *Severity* values are provided in table [1](#).

Log	Severity
<i>Alert</i>	1: Alert
<i>Config</i>	6: Informational
<i>Connection</i>	6: Informational
<i>Debug</i>	7: Debug
<i>Dial</i>	5: Notice
<i>Error</i>	3: Error
<i>Filter</i>	6: Informational
<i>Http</i>	6: Informational
<i>Security</i>	5: Notice
<i>Sslvpn</i>	5: Notice
<i>Warning</i>	4: Warning
<i>Web</i>	6: Informational

Table 1 Severity of Kerio Control logs

Alert Log

The **Alert** log provides a complete history of alerts generated by *Kerio Control* (e.g. alerts upon virus detection, dialing and hanging-up, reached quotas, detection of P2P networks, etc.).

Each event in the **Alert** log includes a time stamp (date and time when the event was logged) and information about an alert type (in capitals). The other items depend on an alert type.

Hint

Email and SMS alerts can be set under **Accounting**. All sent alerts can be viewed in the **Status** → **Alert Messages** section.

Config Log

The **Config** log stores the complete history of communication between the administration interface and *Kerio Control Engine*. It is possible to determine what administration tasks were performed by a specific user.

The **Config** window contains three log types:

1. *Information about logging in to Kerio Control administration*

Example

```
[18/Apr/2011 10:25:02] winston - session opened  
for host 192.168.32.100  
[18/Apr/2011 10:32:56] winston - session closed  
for host 192.168.32.100
```

- [18/Apr/2011 10:25:02] — date and time when the record was written to the log
- winston — the name of the user logged in for *Kerio Control* administration
- session opened for host 192.168.32.100 — information about the beginning of the communication and the IP address of the computer from which the user connected
- session closed for host 192.168.32.100 information about the end of the communication with the particular computer (user logged out or the administration closed)

2. *Changes in the configuration database*

Changes performed in the administration interface. A simplified form of the SQL language is used when communicating with the database.

Example

```
[18/Apr/2011 10:27:46] winston - insert StaticRoutes  
set Enabled='1', Description='VPN',  
Net='192.168.76.0', Mask='255.255.255.0',  
Gateway='192.168.1.16', Interface='LAN', Metric='1'
```

- [18/Apr/2011 10:27:46] date and time when the record was written
- winston — the name of the user logged in for *Kerio Control* administration
- insert StaticRoutes ... — the particular command used to modify the *Kerio Control's* configuration database (in this case, a static route was added to the routing table)

3. *Other changes in configuration*

A typical example of this record type is the change of traffic rules. When the user hits **Apply in Configuration** → **Traffic Policy** → **Traffic Rules**, a complete list of current traffic rules is written to the **Config** log.

Example

```
[18/Apr/2011 12:06:03] Admin - New traffic policy set:
[18/Apr/2011 12:06:03] Admin - 1:  name=(ICMP traffic)
src=(any) dst=(any) service=("Ping")
snat=(any) dnat=(any) action=(Permit)
time_range=(always) inspector=(default)
```

- [18/Apr/2011 12:06:03] date and time of the change
- Admin — login name of the user who did the change
- 1: — traffic rule number (rules are numbered top to bottom according to their position in the table, the numbering starts from 1)
- name=(ICMP Traffic) ... — traffic rule definition (name, source, destination, service etc.)



The default rule is marked with `default` instead of the positional number.

Connection Log

The **Connection** log gathers information about traffic matching traffic rules with the **Log matching connections** enabled or meeting certain conditions (e.g. log of *UPnP* traffic). Information on all IPv6 connections is also logged.

How to read the Connection Log?

```
[18/Apr/2011 10:22:47] [ID] 613181 [Rule] NAT
[Service] HTTP [User] winston
[Connection] TCP 192.168.1.140:1193 -> hit.google.com:80
[Duration] 121 sec [Bytes] 1575/1290/2865 [Packets] 5/9/14
```

- [18/Apr/2011 10:22:47] — date and time when the event was logged (Note: Connection logs are saved immediately after disconnection)
- [ID] 613181 — *Kerio Control* connection identification number.
- [Rule] NAT — name of the traffic rule which has been used (a rule by which the traffic was allowed or denied).
- [Service] HTTP — name of a corresponding application layer service (recognized by destination port).

If the corresponding service is not defined in *Kerio Control*, the [Service] item is missing in the log.

Using logs

- [User] james name of the user connected to the firewall from a host which participates in the traffic.

If no user is currently connected from the corresponding host, the [User] item is missing in the log.

- [Connection] TCP 192.168.1.140:1193 - hit.top.com:80 — protocol, source IP address and port, destination IP address and port. If an appropriate log is found in the *DNS* module cache, the host's DNS name is displayed instead of its IP address. If the log is not found in the cache, the name is not detected (such DNS requests would slow *Kerio Control* down).
- [Duration] 121 sec — duration of the connection (in seconds)
- [Bytes] 1575/1290/2865 — number of bytes transferred during this connection (transmitted /accepted /total).
- [Packets] 5/9/14 — number of packets transferred through this connection (transmitted/accepted/total).

Debug Log

Debug (debug information) is a special log which can be used to monitor certain kinds of information, especially for problem-solving. Too much information could be confusing and impractical if displayed all at the same time. Usually, you only need to display information relating to a particular service or function. In addition, displaying too much information slows *Kerio Control's* performance. Therefore, it is strongly recommended to monitor an essential part of information and during the shortest possible period only.

Selection of information monitored by the Debug log

The window's context menu for the *Debug* log includes further options for advanced settings of the log and for an on-click one-time view of status information.

These options are available only to users with full administration rights for *Kerio Control*.

Format of Logged Packets

For logging network traffic a template is used which defines which information will be recorded and what format will be used for the log. This helps make the log more transparent and reduce demands on disk space.

Detailed help is available in the dialog for template definition.

IP Traffic

This function enables monitoring of IPv4 or IPv6 packets according to the user defined log expression.

The expression must be defined with special symbols. After clicking on the **Help** button, a brief description of possible conditions and examples of their use will be displayed.

Logging of IP traffic can be cancelled by leaving or setting the *Expression* entry blank.

Show Status

A single overview of status information regarding certain *Kerio Control* components. This information can be helpful especially when solving problems with *Kerio Technologies* technical support.

Messages

This feature allows advanced monitoring of functioning of individual *Kerio Control* modules. This information may be helpful when solving issues regarding *Kerio Control* components and/or certain network services.

- **WAN / Dial-up messages** — information about dialed lines (request dialing, auto disconnection down-counter),
- **Filtering** — logs providing information on filtering of traffic passing through *Kerio Control* (antivirus control, website classification, detection and elimination of P2P networks, intrusion detection and prevention, dropped packets, etc.),
- **Accounting** — user authentication and monitoring of their activities (protocol recognition, statistics and reporting, etc.),
- **Kerio Control services** — protocols processed by *Kerio Control* services (*DHCP server*, the *DNS* module, web interface, and *UPnP* support, IPv6 router advertisement),
- **Decoded protocols** — logs of specific protocols (*HTTP* and *DNS*),
- **Miscellaneous** — additional data (e.g. packet processing *Bandwidth Limiter*, switching between primary and secondary Internet connection, HTTP cache, license use, update checker, dynamic DNS, system configuration in editions *Appliance* and *Box*, etc.),
- **Protocol inspection** — reports from individual *Kerio Control's* protocol inspectors (sorted by protocol),
- **Kerio VPN** — detailed information on traffic within *Kerio VPN* VPN tunnels, VPN clients, encryptions, exchange of routing information, web server for *Clientless SSL-VPN*, etc.

Dial Log

Data about dialing and hanging up the dial-up lines, and about time spent on-line.

The following items (events) can be reported in the **Dial** log:

1. Manual connection (from the *Kerio Control Administration* interface or directly in the operating system)

[15/Mar/2011 15:09:27] Line "Connection" dialing,
console 127.0.0.1 - Admin

[15/Mar/2011 15:09:39] Line "Connection" successfully connected

Using logs

The first log item is reported upon initialization of dialing. The log always includes *Kerio Control* name of the dialed line. If the line is dialed from the administration interface, the log provides this additional information

- where the line was dialed from (console the administration interface, system — operating system),
- IP address of the client (i.e. the host from which administration is performed),
- login name of the user who sent the dial request.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

2. Line disconnection (manual or automatic, performed after a certain period of idleness)

[15/Mar/2011 15:29:18] Line "Connection" hang-up,
console 127.0.0.1 - Admin

[15/Mar/2011 15:29:20] Line "Connection" disconnected,
connection time 00:15:53, 1142391 bytes received,
250404 bytes transmitted

The first log item is recorded upon reception of a hang-up request. The log provides information about interface name, client type, IP address and username.

The second event is logged upon a successful hang-up. The log provides information about interface name, time of connection (connection time), volume of incoming and outgoing data in bytes (bytes received and bytes transmitted).

3. Disconnection caused by an error (connection is dropped)

[15/Mar/2011 15:42:51] Line "Connection" dropped,
connection time 00:17:07, 1519 bytes received,
2504 bytes transmitted

The items are the same as in the previous case (the second item — the disconnected report).

4. Requested dialing (as a response to a DNS query)

[15/Mar/2011 15:51:27] DNS query for "www.microcom.com"
(packet UDP 192.168.1.2:4567 -> 195.146.100.100:53)
initiated dialing of line "Connection"

[15/Mar/2011 15:51:38] Line "Connection" successfully connected

The first log item is recorded upon reception of a DNS request (the DNS module has not found requested DNS record in its cache). The log provides:

- DNS name from which IP address is being resolved,
- description of the packet with the corresponding DNS query (protocol, source IP address, source port, destination IP address, destination port),
- name of the line to be dialed.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

5. Dial of the link on demand (responding to a packet from the local network — only in *Windows* edition)

```
[15/Mar/2011 15:53:42] Packet
TCP 192.168.1.3:8580 -> 212.20.100.40:80
initiated dialing of line "Connection"
```

```
[15/Mar/2011 15:53:53] Line "Connection" successfully connected
```

The first record is logged when *Kerio Control* finds out that the route of the packet does not exist in the routing table. The log provides:

- description of the packet (protocol, source IP address, destination port, destination IP address, destination port),
- name of the line to be dialed.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

6. Connection error (e.g. error at the modem was detected, dial-up was disconnected, etc.)

```
[15/Mar/2011 15:59:08] DNS query for "www.microsoft.com"
(packet UDP 192.168.1.2:4579 -> 195.146.100.100:53)
initiated dialing of line "Connection"
```

```
[15/Mar/2011 15:59:12] Line "Connection" disconnected
```

The first record represents a DNS record sent from the local network, from that the line is to be dialed (see above).

The second log item (immediately after the first one) informs that the line has been hung-up. Unlike in case of a regular disconnection, time of connection and volume of transmitted data are not provided (because the line has not been connected).

Error Log

The *Error* log displays information about serious errors that affect the functionality of the entire firewall. The *Kerio Control* administrator should check this log regularly and try to eliminate problems found here. Otherwise, users might have problems with some services or/and serious security problems might arise.

Pattern of Error logs

[15/Apr/2011 15:00:51] (6) Automatic update error: Update failed.

- [15/Apr/2011 15:00:51] — timestamp (date and exact time when the error occurred),
- (6) — associated system error code (only for some errors),
- Automatic update error: Update failed. — error description (failure of the automatic update in this case).

Categories of logs recorded in the *Error* log:

- An issue associated with system resources (insufficient memory, memory allocation error, etc.),
- License issues (the license has expired, will expire soon, invalid license, etc.),
- Internal errors (unable to read routing table or interface IP addresses, etc.),
- License issues (the number of users would break license limit, unable to find license file, Software Maintenance expiration, etc.),
- Configuration errors (unable to read configuration file, detected a loop in the configuration of the *DNS* module or the *Proxy server*, etc.),
- Network (socket) errors,
- Errors while starting or stopping the *Kerio Control Engine* (problems with low-level driver, problems when initializing system libraries, services, configuration databases, etc.),
- File system errors (cannot open/save/delete file),
- SSL errors (problems with keys and certificates, etc.),
- *Kerio Control Web Filter* errors (failed to activate the license, etc.),
- *Kerio VPN* errors,
- HTTP cache errors (errors when reading/writing cache files, not enough space for cache, etc.),
- *Kerio Control Web Filter* errors,
- Checking subsystem errors,

- Antivirus module errors (antivirus test not successful, problems when storing temporary files, etc.),
- Dial-up errors (unable to read defined dial-up connections, line configuration error, etc.),
- LDAP errors (server not found, login failed, etc.),
- Errors in automatic update and product registration,
- Dynamic DNS errors (unable to connect to the server, failed to update the record, etc.),
- *Bandwidth Management* errors,
- Errors of the web interface,
- Crashdumps after failure of the application,
- NTP client errors (synchronization of time with the server),
- The *Kerio Control Administration* web interface errors,
- Intrusion prevention system errors.



If you are not able to correct an error (or figure out what it is caused by) which is repeatedly reported in the **Error** log, do not hesitate to contact our technical support.

Filter Log

This log gathers information on web pages and objects blocked/allowed by the HTTP and FTP filters and on packets matching traffic rules with the **Log matching packets** option enabled or meeting other conditions (e.g. logging of *UPnP* traffic).

Each log line includes the following information depending on the component which generated the log:

- When an HTTP or FTP rule is applied: rule name, user, IP address of the host which sent the request and object's URL.
- When a traffic rule is applied: detailed information about the packet that matches the rule (rule name, source and destination address, ports, size, etc.). Format of the logged packets is defined by template which can be edited through the **Filter** log context menu. Detailed help is available in the dialog for template definition.

Example of a URL rule log message

[18/Apr/2011 13:39:45] ALLOW URL 'Sophos update'

192.168.64.142 standa HTTP GET

http://update.kerio.com/antivirus/datfiles/4.x/dat-4258.zip

- [18/Apr/2011 13:39:45] date and time when the event was logged
- ALLOW — action that was executed (ALLOW = access allowed, DENY = access denied)
- URL — rule type (for URL or FTP)
- 'Sophos update' — rule name
- 192.168.64.142 — IP address of the client
- jsmith — name of the user authenticated on the firewall (no name is listed unless at least one user is logged in from the particular host)
- HTTP GET — HTTP method used in the request
- http:// ... — requested URL

Packet log example

```
[16/Apr/2011 10:51:00] PERMIT 'Local traffic' packet to LAN,
proto:TCP, len:47, ip/port:195.39.55.4:41272 -
192.168.1.11:3663, flags: ACK PSH, seq:1099972190
ack:3795090926, win:64036, tcplen:7
```

- [16/Apr/2011 10:51:00] — date and time when the event was logged
- PERMIT — action that was executed with the packet (PERMIT, DENY or DROP)
- Local traffic — the name of the traffic rule that was matched by the packet
- packet to — packet direction (either to or from a particular interface)
- LAN — name of the interface on which the traffic was detected
- proto: — transport protocol (TCP, UDP, etc.)
- len: — packet size in bytes (including the headers) in bytes
- ip/port: — source IP address, source port, destination IP address and destination port
- flags: — TCP flags
- seq: — sequence number of the packet (TCP only)
- ack: — acknowledgement sequence number (TCP only)
- win: — size of the receive window in bytes (it is used for data flow control TCP only)
- tcplen: — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

Http log

This log contains all HTTP requests that were processed by the HTTP inspection module or by the built-in proxy server.

Http log has the standard format of either the *Apache* WWW server (see <http://www.apache.org/>) or of the *Squid* proxy server (see <http://www.squid-cache.org/>). Format of the log can be set through the context menu. The change will take effect with the next new log record (it is not possible convert existing records).



1. Only accesses to allowed pages are recorded in the **HTTP** log. Request that were blocked by HTTP rules are logged to the **Filter** log, if the **Log** option is enabled in the particular rule.
2. The **Http** log is intended to be processed by external analytical tools. The **Web** log (see below) is better suited to be viewed by the *Kerio Control* administrator.

An example of an HTTP log record in the Apache format

192.168.64.64 - rgabriel

[18/Apr/2011:15:07:17 +0200]

"GET http://www.kerio.com/ HTTP/1.1" 304 0 +4

- 192.168.64.64 — IP address of the client host
- rgabriel — name of the user authenticated through the firewall (a dash is displayed if no user is authenticated through the client)
- [18/Apr/2011:15:07:17 +0200] — date and time of the HTTP request. The +0200 value represents time difference from the UTC standard (+2 hours are used in this example — CET).
- GET — used HTTP method
- http://www.kerio.com — requested URL
- HTTP/1.1 — version of the HTTP protocol
- 304 — return code of the HTTP protocol
- 0 — size of the transferred object (file) in bytes
- +4 — count of HTTP requests transferred through the connection

An example of Http log record in the Squid format

```
1058444114.733 0 192.168.64.64 TCP_MISS/304 0
GET http://www.squid-cache.org/ - DIRECT/206.168.0.9
```

- 1058444114.733 — timestamp (seconds and milliseconds since January 1st, 1970)
- 0 — download duration (not measured in *Kerio Control*, always set to zero)
- 192.168.64.64 — IP address of the client (i.e. of the host from which the client is connected to the website)
- TCP_MISS — the TCP protocol was used and the particular object was not found in the cache (“missed”). *Kerio Control* always uses this value for this field.
- 304 — return code of the HTTP protocol
- 0 — transferred data amount in bytes (HTTP object size)
- GET http://www.squid-cache.org/ — the HTTP request (HTTP method and URL of the object)
- DIRECT — the WWW server access method (*Kerio Control* always uses direct access)
- 206.168.0.9 — IP address of the WWW server

Security Log

A log for security-related messages. Records of the following types may appear in the log:

1. *Intrusion prevention system logs*

Records of detected intrusions or traffic from IP addresses included in web databases of known intruders (blacklists).

Example

[02/Mar/2011 08:54:38] IPS: Packet drop, severity: High,
Rule ID: 1:2010575 ET TROJAN ASProtect/ASPack Packed Binary
proto:TCP, ip/port:95.211.98.71:80(hosted-by.example.com)
-> 192.168.48.131:49960(wsmith-pc.company.com,user:wsmith)

- IPS: Packet drop — the particular intrusion had the action set for *Log and drop* (in case of the *Log* action, IPS: Alert)
- severity: High — severity level
- Rule ID: 1:2010575 — number identifier of the intrusion (this number can be used for definition of exceptions from the intrusion detection system, i.e. in the system's advanced settings)
- ET TROJAN ASProtect/ASPack... — intrusion name and description (only available for some intrusions)
- proto:TCP — traffic protocol used
- ip/port:95.211.98.71:80(hosted-by.example.com) — source IP address and port of the detected packet; the brackets provide information of the DNS name of the particular computer, in case that it is identifiable
- -> 192.168.48.131:49960(wsmith-pc.company.com,user:wsmith) — destination IP address and port in the detected packet; the brackets provide DNS name of the particular host (if identifiable) or name of the user connected to the firewall from the particular local host

2. *Anti-spoofing log records*

Messages about packets that were captured by the *Anti-spoofing* module (packets with invalid source IP address).

Example

[17/Jul/2011 11:46:38] Anti-Spoofing:

Packet from LAN, proto:TCP, len:48,

ip/port:61.173.81.166:1864 -> 195.39.55.10:445,

flags: SYN, seq:3819654104 ack:0, win:16384, tcplen:0

- packet from — packet direction (either from, i.e. sent via the interface, or to, i.e. received via the interface)
- LAN — name of the interface on which the traffic was detected
- proto: — transport protocol (TCP, UDP, etc.)
- len: — packet size in bytes (including the headers) in bytes
- ip/port: — source IP address, source port, destination IP address and destination port
- flags: — TCP flags
- seq: — sequence number of the packet (TCP only)
- ack: — acknowledgement sequence number (TCP only)
- win: — size of the receive window in bytes (it is used for data flow control TCP only)
- tcplen: — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

3. FTP protocol parser log records

Example 1

[17/Jul/2011 11:55:14] FTP: Bounce attack attempt:

client: 1.2.3.4, server: 5.6.7.8,

command: PORT 10,11,12,13,14,15

(attack attempt detected — a foreign IP address in the PORT command)

Example 2

[17/Jul/2011 11:56:27] FTP: Malicious server reply:

client: 1.2.3.4, server: 5.6.7.8,

response: 227 Entering Passive Mode (10,11,12,13,14,15)

(suspicious server reply with a foreign IP address)

Using logs

4. *Failed user authentication log records*

Message format:

Authentication: service: Client: IP adress: reason

- **service** — the *Kerio Control* service to which the client connects (**WebAdmin** = web administration interface, **WebAdmin SSL** = secured version of the web administration interface, **Proxy** = user authentication on the proxy server)
- **IP address** — IP address of the computer from which the user attempted to authenticate
- **reason** — reason of the authentication failure (nonexistent user/ wrong password)

5. *Information about the start and shutdown of the Kerio Control Engine*

a) *Start Engine:*

[17/Dec/2011 12:11:33] Engine: Startup.

b) *Engine shutdown:*

[17/Dec/2011 12:22:43] Engine: Shutdown.

Warning Log

The *Warning* log displays warning messages about errors of little significance. Warnings can display for example reports about invalid user login (invalid username or password), error in communication of the server and Web administration interface, etc.

Events causing display of warning messages in this log do not greatly affect *Kerio Control's* operation. They can, however, indicate certain (or possible) problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

Categories of warnings recorded in the *Warning* log:

- System warnings (e.g. an application found that is known as conflicting),
- *Kerio Control* configuration issues (invalid values retrieved from the configuration file),
- Warnings of *Kerio Control Engine* operations (e.g. DHCP, DNS, antivirus check, user authentication, etc.),
- License warnings (Software Maintenance expiration, forthcoming expiration of the *Kerio Control* license, *Kerio Control Web Filter* license, or the antivirus license),



License expiration (end of functionality of the product) is considered to be an error and it is logged into the **Error** log.

- *Bandwidth Management* warnings,
- *Kerio Control Web Filter* alerts,
- Crashdumps after failure of the application.

Examples of Warning logs

```
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Kerberos 5 auth: user james@company.com not authenticated
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Invalid password for user admin
[16/Apr/2011 10:53:20] Authentication subsystem warning:
User jsmith doesn't exist
```

- The first log informs that authentication of user jsmith by the *Kerberos* system in the company.com domain failed
- Log 2: The second log informs on a failed authentication attempt by user admin (invalid password)
- Log 3: The third log informs on an authentication attempt by auser which does not exist (johnblue)



With the above three examples, the relevant records will also appear in the **Security** log.

Web Log

This log contains all HTTP requests that were processed by the HTTP inspection module or by the built-in proxy server. Unlike in the **HTTP** log, the log displays only queries to text pages, not including objects within these pages. In addition to each URL, name of the page is provided for better reference.

For administrators, the **Web** log is easy to read and it provides the possibility to monitor which Websites were opened by each user.

Using logs

*How to read the **Web** Log?*

[24/Apr/2011 10:29:51] 192.168.44.128 james
"Kerio Technologies" http://www.kerio.com/

- [24/Apr/2011 10:29:51] — date and time when the event was logged
- 192.168.44.128 — IP address of the client host
- james — name of authenticated user (if no user is authenticated through the client host, the name is substituted by a dash)
- "Kerio Technologies" — page title
(content of the `title` HTML element)



If the page title cannot be identified (i.e. for its content is compressed), the "Encoded content" will be reported.

- http://www.kerio.com/ — URL pages

Generating a Software Appliance installation USB flash disk

Generating a Software Appliance installation USB flash disk

Kerio Control in the Software Appliance edition is distributed as an installation CD ISO image. The ISO image can be used also to generate a bootable USB flash disk.

Please follow the instructions according to your operating system:

Linux

1. Mount the USB flashdisk to your computer. If necessary, back up files saved on the disk. The flashdisk data will be rewritten completely!
2. Run the terminal (console) with superuser rights (e.g. by using commands `su` or `sudo -s` — according to your Linux distribution).
3. Use command `fdisk -l` to detect the USB flash disk name (e.g. `/dev/sdb`).
4. Save the drive image to the USB flash disk by using this command:

```
dd if=kerio-control-appliance.iso of=/dev/sdx bs=1M
```

replace `kerio-control-appliance.iso` by the real file name and `/dev/sdx` by the real appliance. It is necessary to enter the physical device (e.g. `/dev/sdx`), not only a partition (e.g. `/dev/sdx1`).
5. Use command `sync` to guarantee finishing all disk operations.
6. Unplug the USB disk from your computer.

Mac OS X

1. Mount the USB flashdisk to your computer. If necessary, back up files saved on the disk. The flashdisk data will be rewritten completely!
2. Run the terminal (**Applications** → **Utilities** → **Terminal**).
3. Use command `sudo diskutil list` to detect the USB flashdisk name (e.g. `/dev/diskX` or `/dev/DiskY` — mind the letter case).
4. Use command `sudo diskutil unmountDisk /dev/diskX` to unmount the disk.

Generating a Software Appliance installation USB flash disk

5. Save the drive image file to the USB flash disk by using this command:

```
sudo dd if=rescue.img of=/dev/disk1 bs=1m
```

replace `rescue.img` by the real file name and `/dev/diskX` by the real appliance.
6. Unplug the USB disk from your computer.

Automatic user authentication using NTLM

Automatic user authentication using NTLM overview

Kerio Control supports automatic user authentication by the NTLM method (authentication from web browsers). Users once authenticated for the domain are not asked for username and password.

This chapter provides detailed description on conditions and configuration settings for correct functioning of NTLM.

General conditions

The following conditions are applied to this authentication method:

1. The Kerio Control server must belong to the corresponding Windows NT (Windows NT Server) or Active Directory (Windows Server 2000/2003/2008) domain.
2. The NT domain or the Active Directory authentication method must be set for the corresponding user account under Kerio Control.
3. Client host belongs to the domain.
4. User at the client host is required to authenticate to the domain (i.e. local user accounts cannot be used for this purpose).

Configuring Kerio Control

NTLM authentication of users from web browsers must be enabled in **Domains and User Login** → **Authentication Options**. User authentication should be required when attempting to access web pages, otherwise enabling NTLM authentication is meaningless.

The configuration of the Kerio Control's web interface must include a valid DNS name of the Kerio Control server.

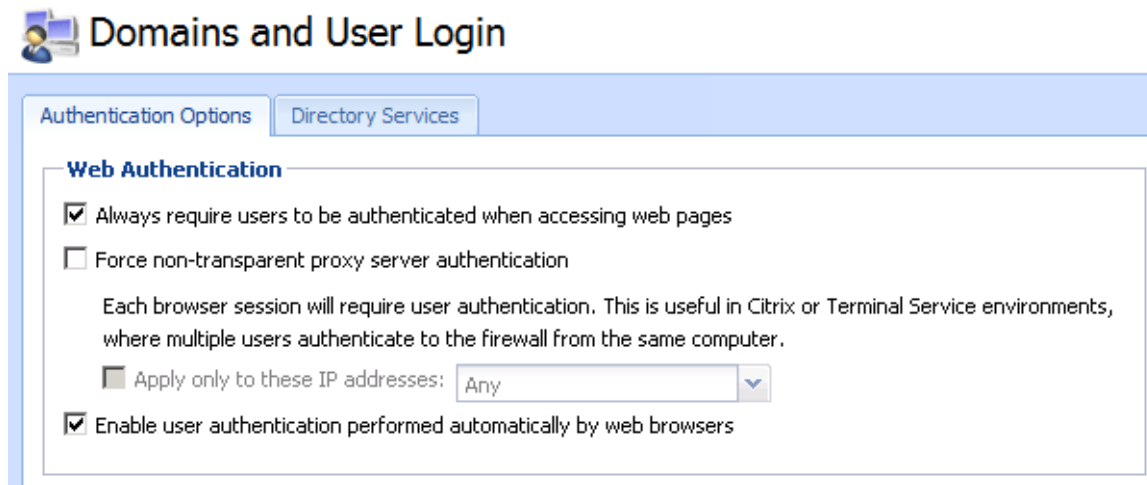


Figure 1 NTLM — user authentication options

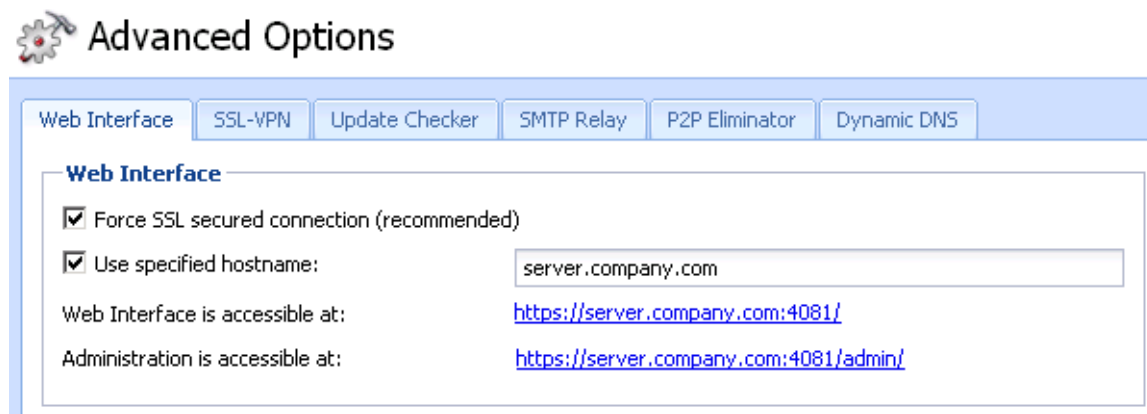


Figure 2 Kerio Control's Web interface configuration

Web browsers

For proper functioning of NTLM, a browser must be used that supports this method. By now, the following browsers are suitable:

- *Internet Explorer*
- *Firefox or SeaMonkey*

In both cases, it is necessary to set Kerio Control as a trusted server in your browser. Users cannot be authenticated on untrusted servers.

Internet Explorer settings

- In the main menu, select *Tools* → *Internet Options*.
- On the **Advanced** tab under *Security*, enable option **Enable integrated Windows authentication**. Computer reboot is required for changes to apply.

- On the **Security** tab, select *Local Intranet*, click on **Servers** and in the next dialog click on **Advanced**.
- Add *Kerio Control* as server name to the list of trusted servers — e.g. `gw.company.com`. For increased security, it is possible to allow only secure authentication — then enter server name following pattern `https://gw.company.com`. It is not possible to specify server by IP address!

Firefox/SeaMonkey configuration

- Insert `about:config` in the browser's address bar.
- Use the filter to search for `network.automatic-ntlm-auth.trusted-uris`.
- Enter *Kerio Control* as server name to the list of trusted servers — e.g. `gw.company.com`. For increased security, it is possible to allow only secure authentication — then enter server name following pattern `https://gw.company.com`. It is not possible to specify server by IP address!

NTLM authentication process

NTLM authentication runs in the background (users cannot see it).

The login dialog is displayed only if NTLM authentication fails (e.g. when user account for user authenticated at the client host does not exist in Kerio Control). In such case, information about failed authentication is recorded in the **error** log.



One of the reasons of NTLM authentication failure in Internet Explorer can be an invalid Kerio Control server authentication name/password saved in the Windows *Password Manager*. In such case, Internet Explorer sends saved login data instead of NTLM authentication of the user currently logged in.

Should any problems regarding NTLM authentication arise, it is recommended to remove all usernames/passwords for the server where Kerio Control is installed from the *Password Manager*.

FTP over Kerio Control proxy server

FTP over proxy server overview

The proxy server in Kerio Control supports FTP protocol. When using this method of accessing FTP servers, it is necessary to keep in mind specific issues regarding usage of the proxy technology and parameters of Kerio Control's proxy server.

1. It is necessary that the FTP client allows configuration of the proxy server. This condition is met for example by web browsers (Internet Explorer, Firefox/SeaMonkey, Google Chrome, etc.), Total Commander, CuteFTP, etc.

Terminal FTP clients (such as the `ftp` command in Windows or Linux) do not allow configuration of the proxy server. For this reason, they cannot be used for our purposes.

2. To connect to FTP servers, the proxy server uses the passive FTP mode. If FTP server is protected by a firewall which does not support FTP (this is not a problem of *Kerio Control*), it is not possible to use proxy to connect to the server.
3. Setting of FTP mode in the client does not affect functionality of the proxy server in any way. Only one network connection used by the FTP protocol is always established between a client and the proxy server.



It is recommended to use FTP over proxy server only in cases where it is not possible to connect directly to the Internet.

Client configuration example: Web interface

Web browsers allow to set the proxy server either globally or for individual protocols. In our example, configuration of *Internet Explorer* focused (configuration of any other browsers is very similar).

1. In the browser's main menu, select **Tools** → **Internet Options**, open the **Connections** tab and click on the **LAN Settings** option.
2. Enable the **Use a proxy server for your LAN** option and enter the IP address and port of the proxy server. IP address of the proxy server is the address of the *Kerio Control*'s host interface which is connected to the local network; the default port of the proxy server is 3128. It is also recommended to enable the **Bypass proxy server for local addresses** option — using proxy server for local addresses would slow down traffic and overburden Kerio Control.

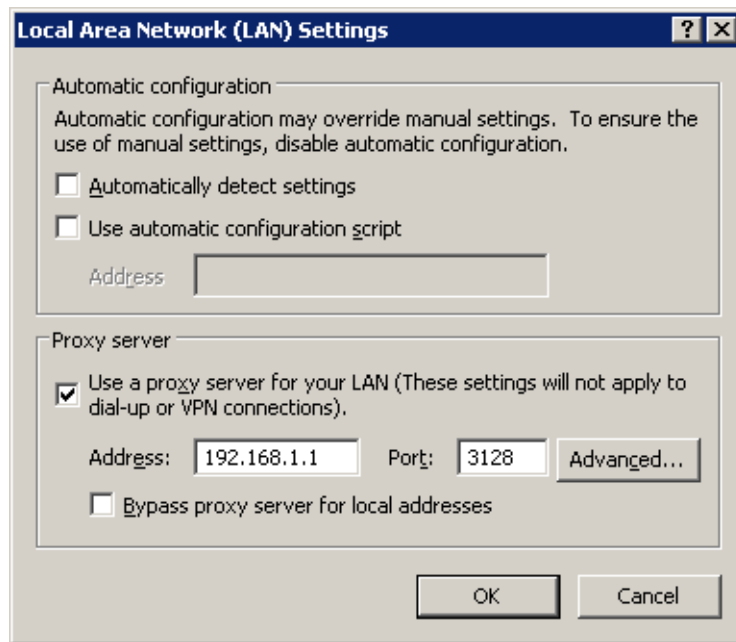


Figure 1 Configuring proxy server in Internet Explorer

Hint

To configure web browsers, you can use a configuration script or the automatic detection of configuration.



Web browsers used as FTP clients enable only to download files. Uploads to FTP server via web browsers are not supported.

Client configuration example: Total Commander

Total Commander allows either single connections to FTP server (by the **Net → FTP -New Connection** option available in the main menu) or creating a bookmark for repeated connections (**Net → FTP -Connect**). The proxy server must be configured individually for each FTP connection (or for each bookmark).

1. In the **FTP: connection details** dialog, enable the **Use firewall (proxy server)** option and click **Change**.
2. In the **Firewall settings** dialog box, select **HTTP Proxy with FTP support**. In the **Host name** textbox, enter the proxy server's IP address and port (separated by a colon, e.g. 192.168.1.1:3128). The **User name** and **Password** entries are optional (*Kerio Control* does not use this information).

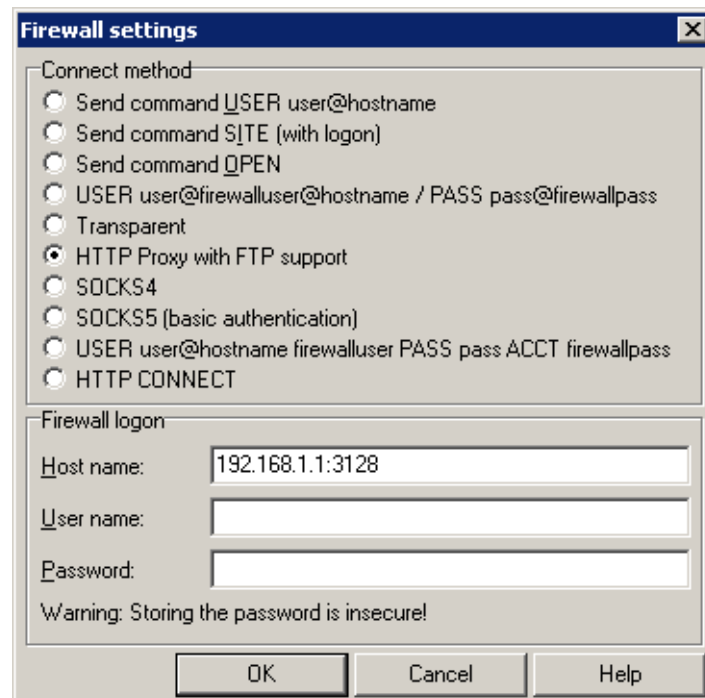


Figure 2 Setting proxy server for FTP in Total Commander

Hint

The defined proxy server is indexed and saved to the list of proxy servers automatically. Later, whenever you are creating other FTP connections, you can simply select a corresponding proxy server in the list.

Configuration files

Configuration files overview

This chapter provides clear descriptions of Kerio Control configuration and status files. This information can be helpful for example when troubleshooting specific issues in cooperation with the *Kerio Technologies* technical support department.

For backup and recovery of your firewall configuration, it is recommended to use configuration export and import tools.

Configuration files

All Kerio Control configuration data is stored in the following files under the same directory where Kerio Control is installed

(typically C:\Program Files\Kerio\WinRoute Firewall).

The following files are included:

winroute.cfg

Chief configuration file

UserDB.cfg

Information about groups and user accounts.

host.cfg

Preferences for backs-up of configuration, user accounts data, DHCP server database, etc.

logs.cfg

Log configurations



The data in these files are saved in XML format in UTF-8. Therefore the data can be easily modified by an advanced user or generated automatically using another application.

Files in the following directories are also considered as configuration data:

sslcert

SSL certificates for all components using SSL for traffic encryption (i.e. the web interface).

license

If Kerio Control has already been registered, the `license` folder includes a license key file (including registered trial versions). If Kerio Control has not been registered yet, the `license` folder is empty.

Configuration files

Status files

In addition, Kerio Control generates other files and directories where certain status information is saved:

Affected files:

dnscache.cfg

DNS files stored in the **DNS** module's cache.

leases.cfg

IP addresses assigned by the DHCP server.

This file keeps all information available on the **Leases** tab of the **DHCP server** section.

stats.cfg

Interface statistics and user statistics data.

vpnleases.cfg

IP addresses assigned to VPN clients.

Directories:

logs

The **logs** directory stores all Kerio Control logs.

star

The **star** directory includes a complete database for statistics of the Kerio Control web interface.

Handling configuration files

We recommend that Kerio Control Engine be stopped prior to any manipulation with the configuration files (backups, recoveries, etc.)! Information contained within these files is loaded and saved only upon starting or stopping the engine. All changes to the configuration performed while the Engine is running are only stored in memory. All modifications done during Engine performance will be overwritten by the configuration in the system memory when the Engine is stopped.

Configuring backup and transfer

Backup and transfer

If you need to reinstall the firewall's operating system (e.g. in case of new hardware installation), you can easily back up your Kerio Control configuration including local user accounts and possibly also SSL certificates. This backup can be later used for recovery of this configuration in your new installation of Kerio Control. This may save significant amount of your time as well as help you avoid solution of problems you have already figured out.

To export or import configuration, login to the administration interface, open the Configuration Assistant and click on the corresponding link.

Configuration export

Configuration is exported to a *tgz* package (the *tar* archive compressed by *gzip*) which includes all the key Kerio Control configuration files. Optionally, it is possible to include the web interface's VPN server's SSL certificates in the package. Exported configuration does not include Kerio Control license key.

Configuration import

To import configuration, simply browse for or enter the path to the corresponding file which includes the exported configuration (with the *.tgz* extension).

If network interfaces have been changed since the export took place (e.g. in case of exchange of a defective network adapter) or if the configuration is imported from another computer, Kerio Control will attempt to pair the imported network interfaces with the real interfaces on the machine. This pairing can be customized — you can match each network interface from the imported configuration with one interface of the firewall or leave it unpaired.

If network interfaces cannot be simply paired, it is desirable to check and possibly edit interface group settings and/or traffic rules after completion of the configuration import.

Tips for tablets


Tips

This article provides a few useful tips for a better administration user experience on tablet devices.

Screen orientation

It is recommended that the device is held in the landscape mode while working with the Kerio administration interface. For viewing longer dialog boxes, hold the device in the portrait mode.

Tree of sections

To get more space to view the section content, hide the tree of sections on the left with  .

Pop-up menu

To open context menu (e.g. in logs), tap the screen with two fingers at a time.

Sort by columns

Select the column and tap to set sorting or open a menu.

Editing table values

First, select a table row. To change the value, single-tap the particular spot.

Logs

- If you use search, you can go to the previous or next occurrence by using the arrow buttons.
- Log pages can be scrolled by dragging with fingers. The more fingers you use, the faster the page scrolls.

Note for iOS: If you have Multi-Touch allowed on iOS 5, you can use up to three fingers for log scrolling.

Legal Notices

Trademarks and registered trademarks

Microsoft®, *Windows®*, *Windows NT®*, *Windows Vista™*, *Internet Explorer®*, *ActiveX®*, and *Active Directory®* are registered trademarks or trademarks of *Microsoft Corporation*.

Mac OS®, *iPad®*, *Safari™* and *Multi-Touch™* are registered trademarks or trademarks of *Apple Inc.*

IOS® is registered trademark of Cisco Systems, Inc.

Linux® is registered trademark kept by Linus Torvalds.

VMware® is registered trademark of VMware, Inc.

Mozilla® and *Firefox®* are registered trademarks of *Mozilla Foundation*.

Chrome™ is trademark of *Google Inc.*

Kerberos™ is trademark of *Massachusetts Institute of Technology (MIT)*.

Snort® is registered trademark of *Sourcefire, Inc.*

Sophos® is registered trademark of Sophos Plc.

avast!® is registered trademark of AVAST Software.

ClamAV™ is trademark held by Tomasz Kojm.

ESET® and *NOD32®* are registered trademarks of ESET, LLC.

AVG® is registered trademark of AVG Technologies.

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

Used open source software

Kerio Control contains the following open-source software:

bindlib

Copyright © 1983, 1993 The Regents of the University of California. All rights reserved.
Portions Copyright © 1993 by Digital Equipment Corporation.

Firebird

This software embeds unmodified version of *Firebird* database engine distributed under terms of *IPL* and *IDPL* licenses.

All copyright retained by individual contributors — original code Copyright © 2000 *Inprise Corporation*.

Original source code can be downloaded from

<http://www.firebirdsql.org/>

h323plus

This product includes unmodified version of the *h323plus* library distributed under *Mozilla Public License (MPL)*.

Original source code can be downloaded from

<http://h323plus.org/>

KIPF — driver

Kerio IP filter driver for Linux (Kerio Control's network interface for Linux):

Copyright © Kerio Technologies s.r.o.

Homepage: <http://www.kerio.com/>

Kerio IP filter driver for Linux is distributed and licensed under *GNU General Public License* version 2.

Complete source code is available at

<http://download.kerio.com/archive/>

KIPF — API

Kerio IP filter driver for Linux API library (API library of the Kerio Control network driver for Linux)

Copyright © Kerio Technologies s.r.o.

Homepage: <http://www.kerio.com/>

Kerio IP filter driver for Linux API library is distributed and licensed under *GNU Lesser General Public License* version 2.

Complete source code is available at

<http://download.kerio.com/archive/>

KVNET — driver

Kerio Virtual Network Interface driver for Linux (driver for the *Kerio VPN* virtual network adapter)

Copyright © Kerio Technologies s.r.o.

Homepage: <http://www.kerio.com/>

Kerio Virtual Network Interface driver for Linux is distributed and licensed under *GNU General Public License* version 2.

Complete source code is available at

<http://download.kerio.com/archive/>

KVNET — API

Kerio Virtual Network Interface driver for Linux API library (API library for the driver of the *Kerio VPN* virtual network adapter)

Copyright © Kerio Technologies s.r.o.

Homepage: <http://www.kerio.com/>

Kerio Virtual Network Interface driver for Linux API library is distributed and licensed under *GNU Lesser General Public License* version 2.

Complete source code is available at

<http://download.kerio.com/archive/>

libcurl

Copyright © 1996-2008, Daniel Stenberg.

libiconv

libiconv converts from one character encoding to another through Unicode conversion. Kerio Control includes a modified version of this library distributed upon the *GNU Lesser General Public License* in version 3.

Copyright © 1999-2003 Free Software Foundation, Inc.

Author: Bruno Haible

Homepage: <http://www.gnu.org/software/libiconv/>

Complete source code of the customized version of *libiconv* library is available at:

<http://download.kerio.com/archive/>

libmbfl

Libmbfl is a multibyte character filtering and conversion library distributed upon the *GNU Lesser General Public License* in version 2.

Copyright © 1998-2002 HappySize, Inc. All rights reserved.

libxml2

Copyright © 1998-2003 Daniel Veillard. All Rights Reserved.

Copyright © 2000 Bjorn Reese and Daniel Veillard.

Copyright © 2000 Gary Pennington and Daniel Veillard

Copyright © 1998 Bjorn Reese and Daniel Stenberg.

Netfilter4Win

Netfilter4win is an implementation of the *libnetfilter_queue* interface for *Windows*. It is distributed under *GNU General Public License* version 2.

Copyright © Kerio Technologies s.r.o.

Copyright © 2005 Harald Welte

Distribution package of complete source codes is available at:

<http://download.kerio.com/archive/>

OpenSSL

This product contains software developed by *OpenSSL Project* designed for *OpenSSL Toolkit* (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young.

This product includes software written by Tim Hudson.

Legal Notices

Operating system

Kerio Control in editions *Appliance* and *Box* are based on various open source software. Please refer to

`/opt/kerio/winroute/doc/Acknowledgements`

files installed inside the appliance for exact licensing terms of each package the appliance is built from.

Distribution package of complete source codes is available at:

<http://download.kerio.com/archive/>

PHP

Copyright © 1999-2006 The PHP Group. All rights reserved.

This product includes *PHP* software, freely available from

<http://www.php.net/software/>

.

Prototype

Framework in JavaScript.

Copyright © Sam Stephenson.

The *Prototype* library is freely distributable under the terms of a *MIT* license.

For details, see the *Prototype* website: <http://www.prototypejs.org/>

ptlib

This product includes unmodified version of the *ptlib* library distributed under *Mozilla Public License (MPL)*.

Original source code can be downloaded from

<http://h323plus.org/>

ScoopyNG

The VMware detection tool.

This product includes software written by Tobias Klein.

Copyright © 2008, Tobias Klein. All Rights Reserved.

Snort

Snort is an open source network intrusion detection and prevention system (*IDS/IPS*). The distribution package includes the *Snort* system and the *pcre* and *pthread-win32* libraries. The package is distributed under the *GNU General Public License* version 2.

Copyright © Kerio Technologies s.r.o.

Copyright © 2001-2008 Sourcefire Inc.

Copyright © 1998-2001 Martin Roesch

Copyright © 1998 John E. Bossom

Copyright © 1999-2005 The *pthread-win32* library authors team

Copyright © 1997-2009 University of Cambridge

Copyright © 2007-2008 Google Inc.

Distribution package of complete source codes is available at:

<http://download.kerio.com/archive/>

strongSwan

strongSwan is an OpenSource IPsec implementation for the Linux operating system. It is based on the discontinued FreeS/WAN project and the X.509 patch which we developped over the last three years.

Except for code in the blowfish, des, md4 and md5 plugins the following terms apply:
For copyright information see the headers of individual source files.

zlib

Copyright © Jean-Loup Gailly and Mark Adler.