

Kerio Control

Administrator's Guide

Kerio Technologies

Contents

Installing Kerio Control	18
Product editions	18
Installing Software Appliance edition	18
Installing VMware Virtual Appliance	19
Installing virtual appliance for Hyper-V	20
Configuring the Activation Wizard	22
Configuring the Activation Wizard	22
Step 1: Select a language	22
Step 2: Setup connection	22
Step 3: Set the time zone, date and time	22
Step 4: Activate Kerio Control	22
Register Kerio Control trial version	23
Insert Kerio Control license number	24
Purchasing Kerio Control	26
Register offline with a licence key	26
Activate Kerio Control in unregistered mode	27
Step 5: Help us make Kerio Control even better	27
Step 6: Set the password for the administrator user account	
and sending alerts	27
Setting administrator password	27
Sending default alerts	28
Setting MyKerio cloud service	29
Configuration Assistant	30
Configuration Assistant overview	30
Configure Internet connection and the local network	31
Single Internet Link	31
Two Internet links with load balancing	32
Two Internet links with failover	33
General notes	34
Define traffic policy	34
Export your configuration	36
Import configuration	36
Register product	37

Licensing and registering Kerio Control	38
Deciding on the number of users (licenses)	38
Licenses, optional components, and Software Maintenance	38
Registering Kerio Control in the administration interface	38
Registering Kerio Control via the Internet	39
Importing the license key	40
Transferring the license	40
Using Dashboard in Kerio Control	41
Dashboard overview	41
Configuring the Kerio Control web interface	42
Using HTTP for access to web interface	42
Using a specified hostname	42
Changing a SSL certificate	43
Configuring network interfaces	44
Interfaces overview	44
Adding a new interface to the Interfaces section	44
Configuring interfaces	45
Moving an interface to another group	45
Configuring Internet connectivity	45
Adding tunnels	46
Configuring PPPoE mode in the Internet interface	46
Configuring PPPoE tunnel	46
Configuring PPTP tunnel	47
Configuring L2TP tunnel	47
VPN tunnel	48
Configuring Ethernet ports	48
Box Edition	48
Appliance Editions	48
Configuring L2TP tunnel	50
L2TP tunnel overview	50
Prerequisites	50
Configuring L2TP tunnel	50
Configuring L2TP tunnel with public IP address	51
Configuring the guest network	53
Guest network overview	53
Assigning guest interfaces	53
Setting DHCP scope	54
Customizing the welcome page	54
Creating HTML content in your Welcome page	55
Setting shared password for guest users	55

Traffic rules for the guest network	55
Configuring VLANs	57
VLAN support in Kerio Control	57
Creating VLAN interfaces	57
Removing VLAN interfaces	57
Changing MAC addresses of network interfaces	59
Overview	59
Changing MAC addresses	59
Configuring Kerio VPN Server	61
VPN overview	61
Configuring Kerio VPN Server	61
Configuring routing	62
Configuring DNS	63
Using the Kerio Control DNS server	63
Using external DNS servers	64
Configuring Kerio Control VPN Clients	64
Assigning static IP addresses for Kerio Control VPN Clients	65
Kerio Control VPN Client for administrators	66
Overview	66
System requirements	66
Licensing Policy	66
Connecting to Kerio VPN Server	66
Troubleshooting SSL certificates	67
Kerio Control VPN Client logs	67
Assigning static IP addresses for Kerio Control VPN Clients	69
Overview	69
Configuring Kerio VPN tunnel	71
Kerio VPN overview	71
Configuring the Kerio VPN tunnel	71
Configuring routing	72
Configuring VPN failover	72
Examples of Kerio VPN tunnel configuration	73
Example 1 - Company with one branch office	73
Example of Kerio VPN configuration: company with two filial offices	77
Overview	77

Configuring IPsec VPN	87
IPsec overview	87
Configuring IPsec VPN server with a preshared key	87
Configuring IPsec server with a SSL certificate	89
Configuring clients with a preshared key	89
Supported mobile devices	89
Configuring IPsec VPN tunnel	91
IPsec overview	91
Before you start	91
Configuring IPsec VPN tunnel with a preshared key authentication	91
Configuring IPsec VPN tunnel with a SSL certificate authentication	92
Configuring local networks	93
Configuring VPN failover	95
Configuring IPsec VPN tunnel (Kerio Control and another device)	96
IPsec tunnel overview	96
Default values in Kerio Control	96
Supported ciphers	97
Configuring traffic rules	99
How traffic rules work	99
Configuring traffic rules	99
Generic rule	100
Port mapping	102
Other examples	103
User accounts and groups in traffic rules	103
Demilitarized zone (DMZ)	105
Policy routing	105
Enabling protocol inspection on traffic rules	105
Configuring IP address translation	107
IP address translation (NAT) overview	107
Configuring IP address translation	107
A default NAT rule description	109
Configuring traffic rules - multihoming	111
Multihoming overview	111
Adding IP addresses to an interface	111
Configuring traffic rules for multihoming	112
Limiting Internet access with traffic rules	114
Limiting Internet Access	114

Troubleshooting traffic rules	116
Overview	116
Detecting IP addresses	116
Looking for dropped packets	117
Testing traffic rules	118
Configuring Demilitarized Zone (DMZ)	120
Demilitarized Zone (DMZ)	120
Configuring DMZ	120
Configuring policy routing	122
Policy routing overview	122
Configuring a preferred link for email traffic	122
Configuring an optimization of network traffic load balancing	124
Configuring intrusion prevention system	125
Intrusion prevention system overview	125
Configuring intrusion prevention	125
Configuring ignored intrusions	126
Configuring protocol-specific intrusions	126
IP blacklists	127
Automatic updates	127
Filtering MAC addresses	128
Filtering MAC addresses overview	128
Configuring the filter	128
Support for IPv6 protocol	130
Support for IPv6 protocol	130
IPv6 filtering	131
Allowing IPv6 for particular computers or prefixes	131
Blocking IPv6 tunneling	131
Configuring IPv6 networking in Kerio Control	133
Overview	133
Obtaining an IPv6 prefix from your ISP	133
Running IPv6 in the Kerio Control network	134
Enabling the IPv6 router advertisements	135
Manual configuration	135
Configuring Service Discovery forwarding in the Kerio Control network	136
Service Discovery forwarding overview	136
Configuring Service Discovery forwarding	136
Troubleshooting	137

Configuring Universal Plug-and-Play (UPnP)	139
Universal Plug-and-Play (UPnP) overview	139
Configuring the UPnP support	139
Configuring connection limits	141
Host connection limits in Kerio Control 9.0 and later	141
Overview	141
Changing default values	142
Disabling connection limits	142
Excluding an IP address group from all connection limits	143
Setting different limits for specific IP address groups	143
Host connection limits in Kerio Control 8.6.2 and earlier	144
Overview	144
Changing default values	144
Disabling connection limits	145
Excluding hosts from restrictions	145
Configuring bandwidth management	147
Overview	147
How bandwidth management works	147
Internet links speed	147
Configuring bandwidth management	147
Traffic types used in bandwidth management	149
Bandwidth management and VPN tunnels	149
Configuring the Content Filter	151
Content filter overview	151
Prerequisites	151
Configuring content rules	152
Duplicating content rules	153
Adding new rules	154
Detecting content	154
Setting actions	154
Allow	155
Deny	156
Drop	158
Unlocking rules	159
Examples	159
Adding new URLs for automatic updates	159
Blocking Facebook	159
Allowing all content from Samepage.io	161
Related articles	162

Eliminating Peer-to-Peer traffic	163
Peer-to-Peer (P2P) networks	163
Configuring/Adding the P2P traffic rule	163
Configuring parameters for detection of P2P networks	164
Application awareness in Kerio Control	166
Overview	166
Enabling application awareness	166
Setting content rules	167
Example: Social networks	167
Setting bandwidth rules	169
Example: Limiting music access	169
Application visibility in Active Connections	171
Debugging application awareness	172
Changes in licensing	173
Using Kerio Control Web Filter	174
Overview	174
Enabling Kerio Control Web Filter	174
Testing URLs	175
Creating a URL whitelist	175
Using Web Filter in URL rules	176
Configuring HTTP cache	177
HTTP cache overview	177
Configuring HTTP cache	177
Configuring TTL	177
Cache status and administration	178
Blocking inappropriate or explicit content in search results	179
Overview	179
How it works	179
Enabling SafeSearch	179
Excluding users from SafeSearch	180
Filtering web content by word occurrence	182
Overview	182
Adding a new forbidden word	182
Filtering HTTPS connections	184
Overview	184
Configuring HTTPS filtering	184
Setting HTTPS filtering exceptions	185
Excluding traffic to/from web applications	186
Excluding users from the HTTPS filtering	187

Importing a certificate for an untrusted web applications into Kerio Control	188
Installing certificates to Kerio Control	188
Configuring proxy server	190
Overview	190
Configuring the reverse proxy	194
Why use the reverse proxy server in Kerio Control	194
Configuring the reverse proxy	194
Adding new rules	195
Configuring a traffic rule	197
Creating SSL certificates with alternative DNS names	198
Configuring HTTP cache for the reverse proxy	200
Configuring antivirus protection	201
Antivirus protection overview	201
Conditions and limitations of antivirus scan	201
Configuring antivirus protection	201
Using DHCP module	203
DHCP server in Kerio Control	203
Automatic configuration of scopes	203
Manual definition of Scopes and Reservations	204
Defining individual scopes	205
Leases and Reservations	206
Reserving an IP address	206
Using the DNS module	208
DNS forwarding service in Kerio Control	208
Configuring simple DNS forwarding	208
Hosts table	209
Configuring custom DNS Forwarding	209
Defining a rule	210
Clearing the cache	212
Configuring a routing table in Kerio Control	213
Overview	213
Route types	214
Modifying static routes in the IPv4 routing table	214
Modifying routes in the IPv6 routing table	215

Using alert messages	217
Overview	217
Configuring alerts	217
System alerts	219
Sending log message alerts	221
Viewing alerts	221
Alert log	221
Sending log message alerts	222
Overview	222
Adding rules for log message alerts	223
Examples of log alerts	224
Configuring statistics and reports	226
Overview	226
Prerequisites	226
Settings for statistics, reports and quota	226
Using group statistics	228
Accounting exceptions	228
Setting access rights and email reports	229
Allowing users to see their own statistics	230
Allowing managers to see other users and group statistics	230
Configuring system settings date, time, time zone and server name	233
System Configuration overview	233
Configuring date and time	233
Configuring time zone	233
Configuring the server name	234
Upgrading Kerio Control	235
Using update checker	235
Checking new versions	235
Automatic upgrade of Kerio Control	235
Configuring email alerts	236
Manually uploading a binary image file	236
Upgrade with USB tools	237
Troubleshooting	237
Configuring the SMTP server	238
Configuring the SMTP Relay	238
Dynamic DNS for public IP address of the firewall	239
Overview	239
Configuring DDNS	239
Saving configuration to MyKerio	241

Overview	241
Saving configuration to MyKerio	241
Restoring configuration from a backup	242
Saving configuration to Samepage	243
Saving configuration to Samepage	243
Restoring configuration from backup	244
Saving configuration to FTP server	245
Configuring backup to an FTP server	245
Restoring configuration from backup	246
Composing FTP URLs	246
Example	247
Managing user accounts	248
User accounts overview	248
Adding new accounts	248
Adding local accounts	248
Adding accounts from a directory service	249
Using templates	249
Configuring accounts	249
Configuring user quota	249
Automatic login on static IP addresses	250
Deleting user accounts	251
Disabling users temporarily	251
Deleting users permanently	251
Setting access rights in Kerio Control	252
Setting access rights	252
What levels of access rights are available	252
Setting access rights to internet usage statistics and user's activity records	252
Configuring automatic user login	253
Automatic login overview	253
Configuring automatic login on MAC address	253
Configuring automatic login in the Active Hosts section	254
Configuring automatic login on static IP addresses	254
Why Kerio Control does not know the MAC address	254
Assigning static IP addresses for Kerio Control VPN Clients	255
Overview	255

Configuring 2-step verification	257
Overview	257
Configuring the 2-step verification in Kerio Control Administration	258
Disabling the 2-step verification for a particular user	259
Enabling the 2-step verification in Kerio Control Statistics	260
Connecting Kerio Control to directory service	261
Which directory services are supported	261
What is the connection used for	261
Microsoft Active Directory	261
Conditions for mapping from Active Directory domains	261
Connecting to Microsoft Active Directory	262
Connecting to Apple Open Directory	262
Connecting to other domains	263
Configuring encrypted connection (LDAPS)	263
Collision of directory service with the local database and conversion of accounts	264
Authenticating users to Kerio Control	265
Overview	265
Requiring user authentication when accessing web pages	265
Requiring user authentication when multiple users use one computer	266
User logout	267
Troubleshooting user authentication	267
Using RADIUS server in Kerio Control	268
RADIUS server overview	268
Configuring Kerio Control	268
Users authentication in Microsoft Active Directory	269
Configuring your Wi-Fi access point	269
Configuring Windows 7 clients	270
Protecting users against password guessing attacks	274
Protecting against password guessing attacks	274
Creating user groups in Kerio Control	275
User groups overview	275
Creating user groups	275
Creating local groups	275
Configuring SSL certificates in Kerio Control	276
SSL certificates overview	276
Creating a new Local Authority	276
Creating a certificate signed by Local Authority	277
Creating a certificate signed by a Certification Authority	277

Importing intermediate certificates	278
Configuring IP address groups	279
Using IP address groups	279
Adding a new IP address group	280
Adding item into existing address group	281
Moving items from one IP address group to another	281
Creating time ranges in Kerio Control	283
Overview	283
Defining time ranges	284
Configuring URL groups	285
Using URL groups	285
Defining a new URL group	286
Services in Kerio Control	288
Services	288
Using services	288
Creating service groups	289
Protocol inspection in Kerio Control	291
Overview	291
Applying protocol inspection to a non standard port	291
Disabling a protocol inspector	292
Disabling protocol inspectors in services	293
Disabling protocol inspectors in traffic rules	294
Monitoring active hosts	296
Overview	296
General	298
Activity	298
Connections	299
Histogram	299
Monitoring VPN clients	301
Overview	301
Disconnecting a VPN client	302
Monitoring alert messages	303
Overview	303
Configuring alerts	303
Alert log	303

Monitoring user statistics	304
Overview	304
Kerio Control Statistics	305
Monitoring System Health in Kerio Control	306
Overview	306
Using and configuring logs	307
Logs overview	307
Logs Context Menu	307
Log highlighting	308
Logs Settings	309
Detailed articles	311
Logging packets	312
Packet logging	312
Configuring packet logging	312
Logical Expression	312
Interpretation of logical expressions	312
Variables	313
Examples	314
Creating and downloading packet dumps	315
Log packet formatting	316
Log packet formatting	316
Creating expressions	316
Default template	316
Variables	316
Using the Config log	318
Config log overview	318
Reading the Config log	318
Using the Connection log	320
Connection log overview	320
Reading the Connection log	321
Using the Debug log	322
Debug log overview	322
Using the Debug log	322
Using the Dial log	324
Dial log overview	324
Reading the Dial log	324

Using the Error log	326
Error log overview	326
Reading the Error log	326
Using the Filter log	328
Filter log overview	328
Reading the Filter log	329
Example of a URL rule log message	329
Packet log example	329
Using the Host log	331
Host log overview	331
Reading the Host log	331
An example of user registration	331
An example of IP address leased from DHCP	332
An example of registering and removing an IPv6 address	332
Using the Http log	333
Http log overview	333
Reading the Http log	333
An example of an Http log record in the Apache format	333
An example of Http log record in the Squid format	334
Using the Security log	335
Security log overview	335
Reading the Security log	335
Intrusion prevention system logs	335
Anti-spoofing log records	336
FTP protocol parser log records	336
Failed user authentication log records	337
Information about the start and shutdown of the Kerio Control Engine and some Kerio Control components	337
Updating components	337
Using the Warning log	338
Warning log overview	338
Reading the Warning log	338
Using the Web log	340
Web log overview	340
Reading the Web Log	340

Using IP tools in Kerio Control	341
About IP tools	341
Ping	341
Traceroute	342
DNS Lookup	342
Whois	343
SNMP monitoring	344
Configuring Kerio Control	344
Cacti	344
Generating a bootable USB flash drive for Kerio Control software appliances	346
Overview	346
Windows	346
Linux	346
OS X	347
Automatic user authentication using NTLM	348
Automatic user authentication using NTLM overview	348
General conditions	348
Configuring Kerio Control	348
Web browsers	349
NTLM authentication process	350
FTP over Kerio Control proxy server	351
FTP over proxy server overview	351
Configuration files	354
Configuration files overview	354
Configuring backup and transfer	356
Backup and transfer	356
Tips for tablets	357
Tips	357
Legal Notices	358
Trademarks and registered trademarks	358
Used open source software	358

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](#) and [Hyper-V](#) 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.



Watch the [Installing the Software Appliance edition](#) video.



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.

Kerio Control checks all interfaces for a DHCP server in the network and the DHCP server provides a default route after the installation:

- Internet interfaces — All interfaces where Kerio Control detects the DHCP server and the default route in the network. If there is more than one Internet interface with a default route, Kerio Control arranges the Internet interfaces in the load balancing mode.
- LAN interfaces — All interfaces without any detected DHCP server. Kerio Control runs its own DHCP server through all LAN interfaces configured to **10.10.X.Y** where **X** is the index of the LAN interface (starting with 10). **Y** is 1 for the Control interface and 11-254 for DHCP assigned hosts.

To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**. For more information, read [Configuring network interfaces](#).

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`
 for example
`https://10.10.10.1:4081/admin`
 which is the IP address where Kerio Control is accessible from your LAN.

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**).

Installing Kerio Control

Complete the installation:

1. Kerio Control checks all interfaces for a DHCP server in the network and the DHCP server provides a default route after the installation:
 - Internet interfaces — All interfaces where Kerio Control detects the DHCP server and the default route in the network. If there is more than one Internet interface with a default route, Kerio Control arranges the Internet interfaces in the load balancing mode.
 - LAN interfaces — All interfaces without any detected DHCP server. Kerio Control runs its own DHCP server through all LAN interfaces configured to **10.10.X.Y** where X is the index of the LAN interface (starting with 10). Y is 1 for the Control interface and 11-254 for DHCP assigned hosts.

To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**. For more information, read [Configuring network interfaces](#).

2. To perform the initial setup, open the following address in your web browser:

`https://kerio_control_ip_address:4081/admin`

for example

`https://10.10.10.1:4081/admin`

which is the IP address where Kerio Control is accessible from your LAN.

3. Follow the Activation Wizard.

For more details, read the [Configuring the Activation Wizard](#) article.

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.

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**).

If your version of Windows offer you to create a type of machine, create a “Generation 1” machine. Kerio Control does not support “Generation 2”.

5. As the virtual machine location, select the directory with the unpacked virtual harddisk. Assign RAM and virtual network adapters (read [Technical Specifications](#)).

If you do not use the wizard or if you add the virtual hardware to existing machine, select **Network adapter**.

6. Select **Use existing virtual harddisk**. Browse for the virtual harddisk unpacked from the distribution package.

If you do not use the wizard or if you add hardware from an existing source, use IDE.

7. After finishing the wizard, connect to the virtual appliance and start it.

8. Kerio Control checks all interfaces for a DHCP server in the network and the DHCP server provides a default route after the installation:

- Internet interfaces — All interfaces where Kerio Control detects the DHCP server and the default route in the network. If there is more than one Internet interface with a default route, Kerio Control arranges the Internet interfaces in the load balancing mode.
- LAN interfaces — All interfaces without any detected DHCP server. Kerio Control runs its own DHCP server through all LAN interfaces configured to **10.10.X.Y** where X is the index of the LAN interface (starting with 10). Y is 1 for the Control interface and 11-254 for DHCP assigned hosts.

To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**. For more information, read [Configuring network interfaces](#).

9. To perform the initial setup, open the following address in your web browser:

`https://kerio_control_ip_address:4081/admin`

for example

`https://10.10.10.1:4081/admin`

which is the IP address where Kerio Control is accessible from your LAN.

10. [Follow the Activation Wizard](#).

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

Configuring the Activation Wizard

Configuring the Activation Wizard

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

Step 1: Select a language

This language is used by the activation wizard and it is also set as a default language after the first logon to the administration interface. You can change the language settings later.

Step 2: Setup connection



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.

If your internet connection is configured properly, click **Next**.

You can use other options:

It is also possible to select the **Activate in unregistered mode** link and [register Kerio Control later](#).

If you have a file with license, select the **Register offline by license file** link.

Step 3: Set the time zone, date and time

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

Select your time zone and verify the date and time settings.

We recommend to enable synchronization of time against a time server. Kerio Control uses the NTP servers of Kerio Technologies.

Step 4: Activate Kerio Control

This step allows you to:

- [register a license number of the purchased product](#)
- [purchase Kerio Control](#)

- use the 30-day trial version
- put the license.key file into Kerio Control
- skip the registration and register Kerio Control later

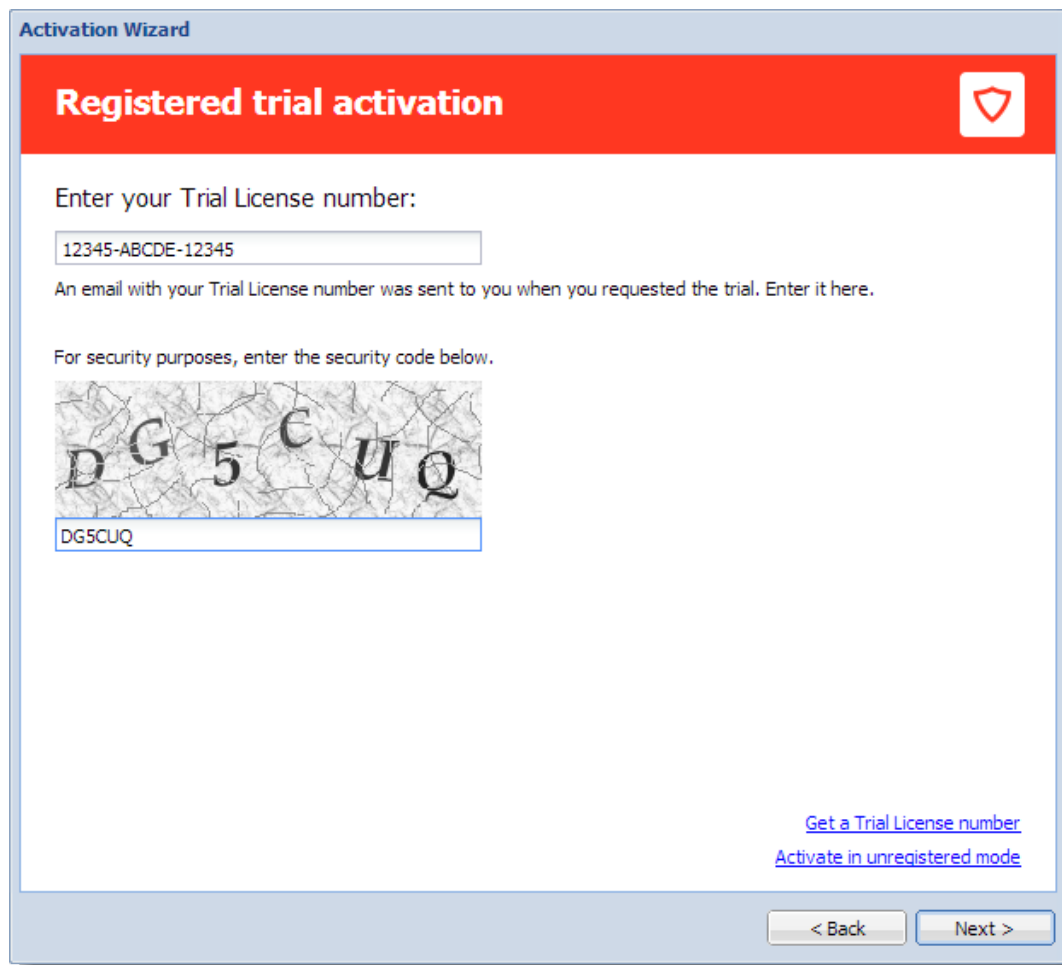


Figure 1 Licensing dialog

Register Kerio Control 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,
 - the intrusion prevention system,
 - free technical support for the entire trial period.
1. Click **Trial** in the [Licensing dialog](#).
 2. In the **Registered trial activation** dialog, type your trial license number (see [figure 2](#)). If you do not have a license number, click **Get a Trial License number** link.
 3. Enter the security code displayed in the picture and click **Next**.




The screenshot shows a window titled "Activation Wizard" with a red header bar containing the text "Registered trial activation" and a shield icon. The main content area has the following text and fields:

Enter your Trial License number:

An email with your Trial License number was sent to you when you requested the trial. Enter it here.

For security purposes, enter the security code below.



At the bottom right, there are two links: [Get a Trial License number](#) and [Activate in unregistered mode](#). At the very bottom, there are two buttons: "< Back" and "Next >".

Figure 2 Licensing dialog

4. Click the **Finish** button.



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

Insert Kerio Control license number

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

1. Click **License** in the [Licensing dialog](#).
2. [In the next step](#), click **Enter license**.
3. Insert the license number and enter the security code displayed in the picture (see [figure 4](#)).

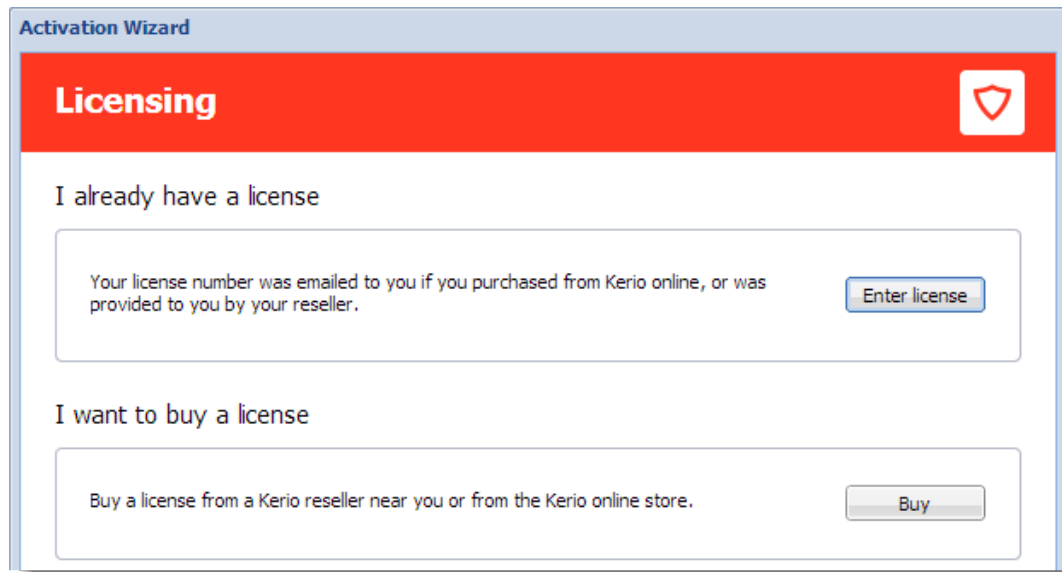


Figure 3 Licensing dialog

4. In the **License details** dialog, verify the license details.
If you want to add other license numbers, click **Register multiple license numbers**.
 5. In the **Contact details** dialog, type your contact information.
- Upon a successful registration, the product is activated with a valid license.

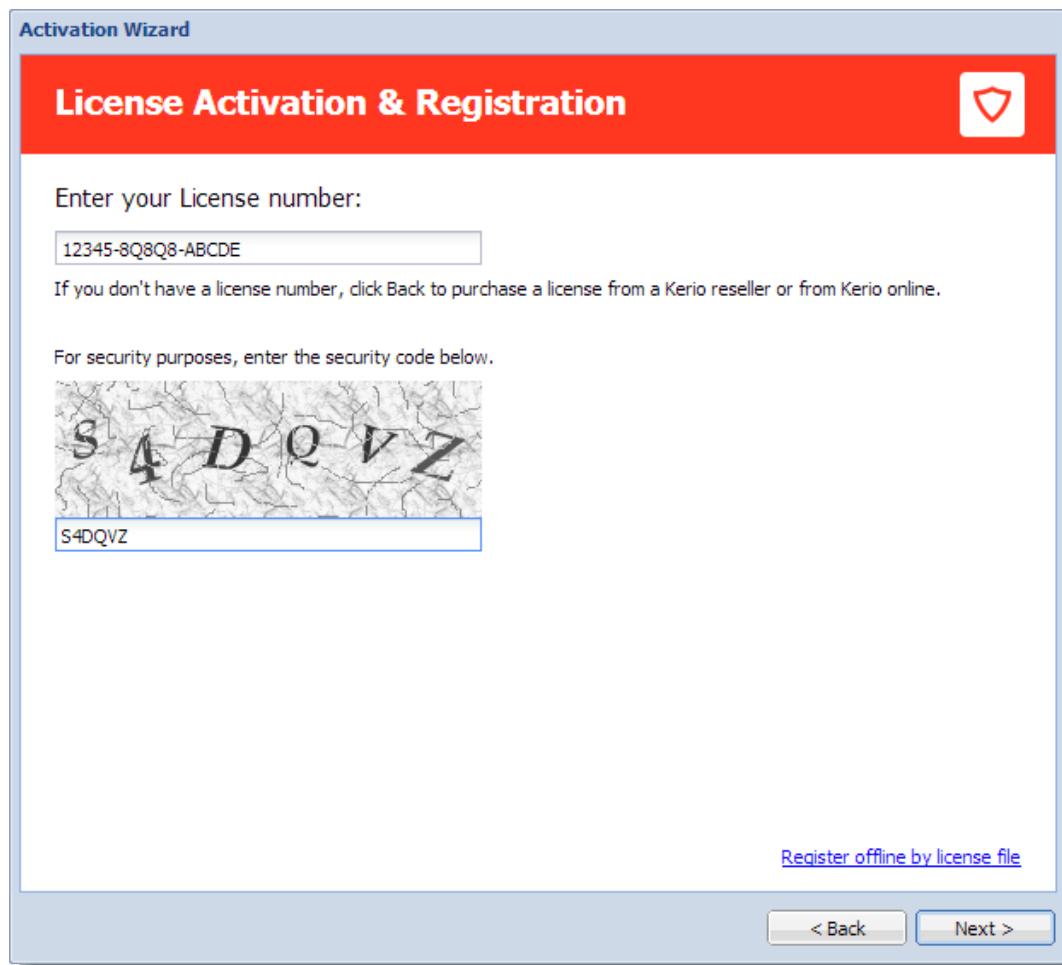


Figure 4 License Activation and Registration dialog

Purchasing Kerio Control

To purchase Kerio Control:

1. Click **License** in the [Licensing dialog](#).
2. In the next step, click **Buy**.
This opens www.kerio.com in your browser.
3. At www.kerio.com, purchase Kerio Control.

Register offline with a licence key

If you have a file with a license key from your previous installation of Kerio Control (usually `license.key`), you can use link **Register offline by license file** (see screenshot [4](#)).

Activate Kerio Control in unregistered mode

1. In the [Licensing dialog](#), click **Trial**.
2. In the **Registered trial activation** dialog, click **Activate in unregistered mode**.

Step 5: 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 you can disable it any time under **Advanced Options** → **Updates**.

Step 6: Set the password for the administrator user account and sending alerts

Setting administrator password

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

Activation Wizard

Administrator account

Please set a password for the administrator user account:

Username: Admin

Password:

Confirm password:

☒ Do you want to receive alerts?

Email address: asmith@company.com

☒ Allow remote administration from [MyKerio](#) cloud service

☒ Open MyKerio and join this appliance after you finish

You can change these settings later in Remote Services.

< Back Next >

Figure 5 Administrator account dialog

Sending default alerts

Kerio Control can send automatic email messages (alerts) about important events.

To enable sending alerts to defined email address:

1. Select **Do you want to receive default alerts?**
2. Type your email address to the **Email address** field.

Kerio Control associates this address with the default Kerio Control Admin account.

From now on, Kerio Control includes the predefined alerts group in the **Accounting and Monitoring** → **Alert Settings** (see screenshot below).

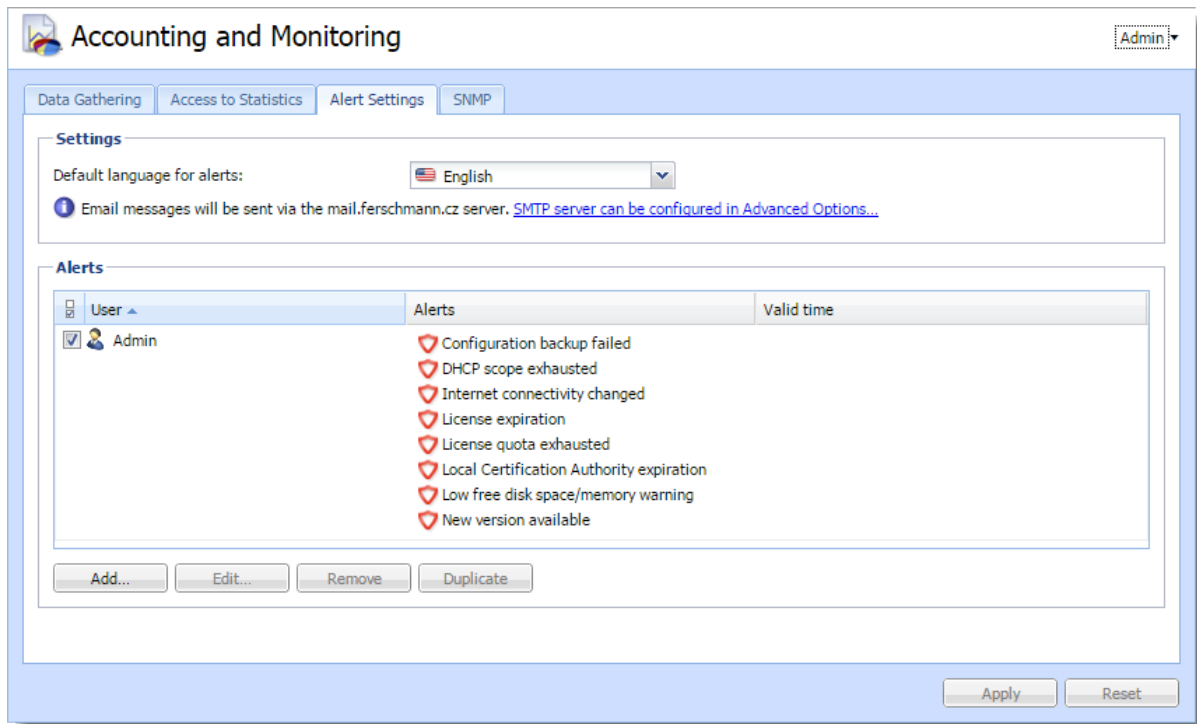


Figure 6 Alert Settings tab

For more information about particular alerts, refer to [Using Alert Messages](#).



Ensure your Kerio Control is connected to an SMTP server for sending alerts. Read more in the [Configuring the SMTP server](#) article.

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

Setting MyKerio cloud service

[MyKerio](#) is a cloud service which enables you to administer numerous Kerio Control appliances in a single dashboard.

To allow remote administration from MyKerio, select **Allow remote administration from MyKerio cloud service**.

To join this appliance of Kerio Control, select **Open MyKerio and join this appliance after you finish**.

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**.

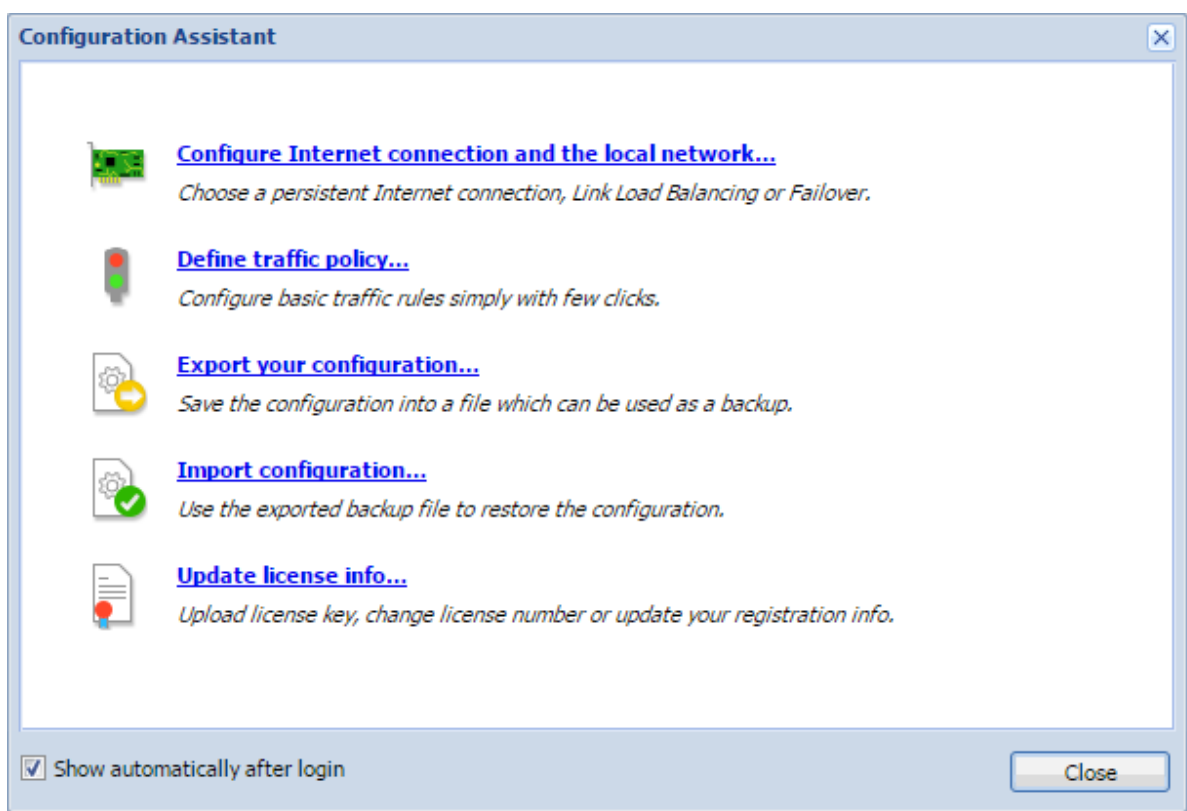


Figure 1 Configuration Assistant



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**.

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 enables you to configure only a basic set of traffic rules:

1. In the **Configuration Assistant** dialog, click **Define traffic policy**.
2. Enable any of the following options:
 - **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 (you cannot change the port of the administration interface).
 - **Web Services** — enables the HTTP/S communication on the 80/443 ports. Check this option, if you want to have your public web servers behind the firewall (mailserver, your company website, etc.).



Figure 2 Inbound policy

3. Click **Next**.
4. To make any other services on the firewall or servers in the local network available from the Internet (mapping), click **Add** (see screenshot 3).

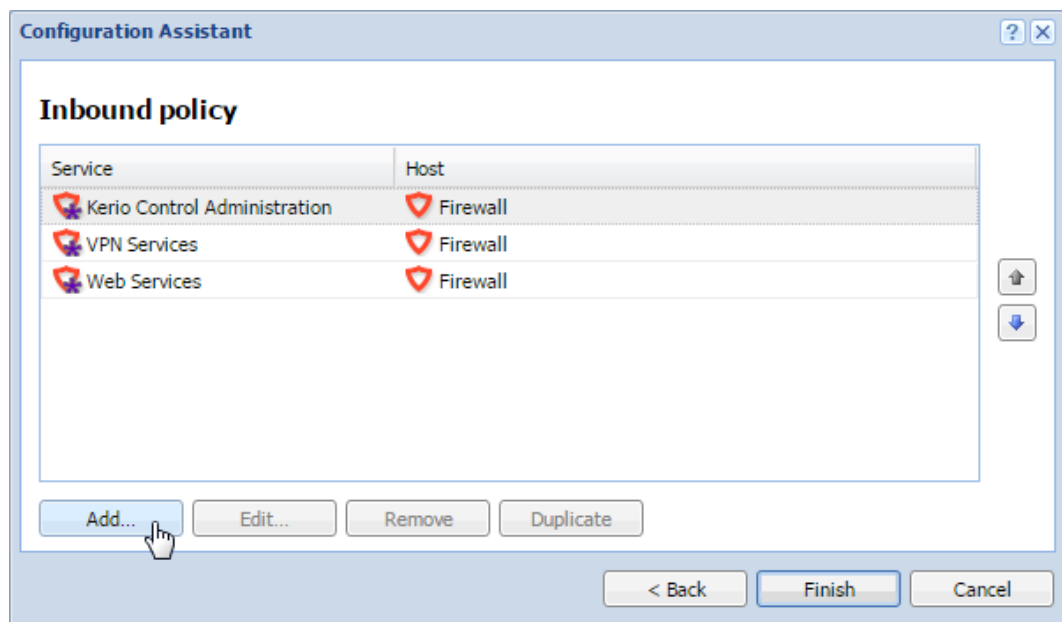


Figure 3 Inbound policy — create your own rules

5. In the **Inbound policy** section, you can configure the following parameters:

- **Service** (or a [group of services](#)) — select services from the list of defined services or define a protocol and a port number.
- **Runs on** — firewall or IP address of the local server on which the service is running.

6. Arrange the rules by order with arrows on the right side of the window.

The rules are processed from the top downwards and the first matched rule is applied.

7. Click **Finish**.

You can perform advanced configuration in the **Traffic Rules** section. Read more in the [Configuring traffic rules](#) article.

Export your configuration

Configuration is exported to a `.tgz` package which includes all the key Kerio Control configuration files. Optionally, it is possible to include SSL certificates and DHCP leases in the package.

Exported configuration does not include Kerio Control license key.



Kerio Control can automatically upload configuration files to Samepage.io or FTP (read articles [Saving configuration to Samepage](#) and [Saving configuration to FTP server](#) for more information).

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.

Register product

See article [Configuring the Activation Wizard](#).

Licensing and registering Kerio Control

Deciding on the number of users (licenses)

Kerio Control is licensed as a server. The admin account and five user accounts are included in the basic license. Additional users can be added in packages of five.

A 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. [Guests and their devices are exempted from the licensing system.](#)

If a user tries to connect from more than five devices at a time, this requires an additional user license.

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



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

Licenses, optional components, and Software Maintenance

Kerio Control has the following optional components:

- Sophos antivirus
- Kerio Control Web Filter module for web page ratings

These components are licensed individually.

Software Maintenance

The Software Maintenance agreement lets you update the software. If your Software Maintenance expires, you can continue using the existing version of the product, but you cannot install any updates released after the expiration date. Learn more at www.kerio.com.

Registering Kerio Control in the administration interface

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

Once it is installed, the product can be registered as a trial or full version.

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

If you have not registered your trial version:

1. Open the administration interface.
2. On the **Dashboard**, click **Configuration Assistant**.

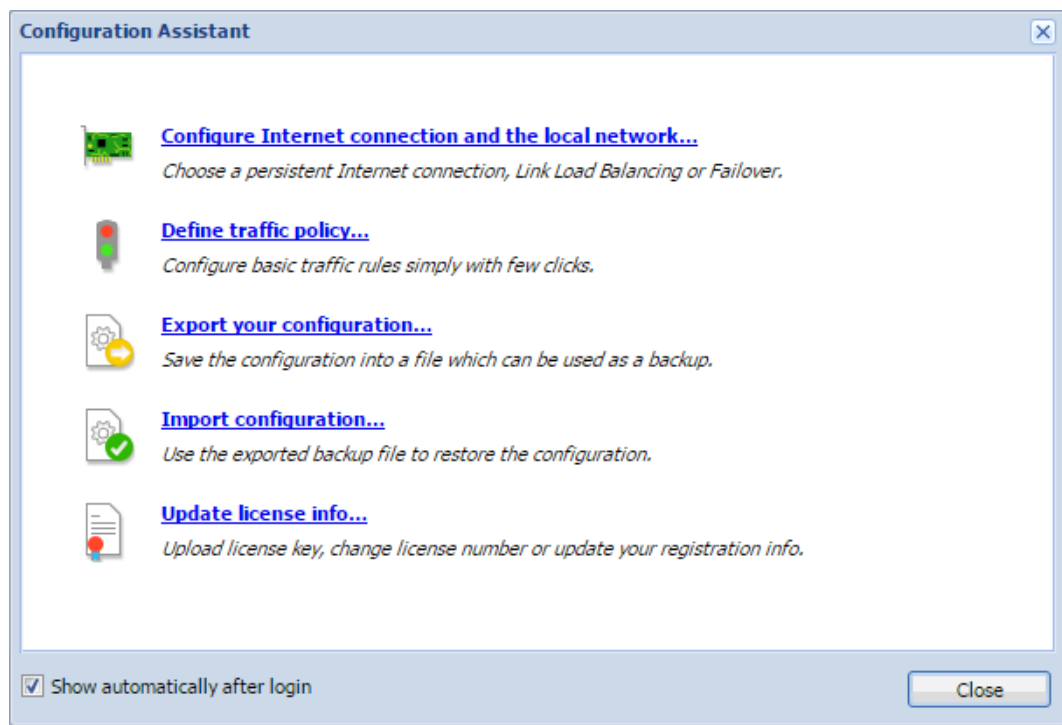


Figure 1 Configuration Assistant

3. In the **Configuration Assistant** dialog box, click **Register product**.
See the [Configuring the Activation Wizard](#) article for more information.

Registering Kerio Control via the Internet

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

1. In a browser, go to <https://secure.kerio.com/reg/>
2. Register using your purchased license number.
3. You can then download a license key (the `licence.key` file, including the corresponding certificate), which must be [imported to Kerio Control](#).

Importing the license key

1. Prepare the file with the license.
2. Open the administration interface.
3. On the **Dashboard**, click **Configuration Assistant**.
4. Click **Register product**.

See the [Configuring the Activation Wizard](#) article for more information.

You can check to be sure the license was installed successfully in the **License** section of the **Dashboard**.

Transferring the license

You can transfer the license between:

- Two virtual appliances
- Two software appliances
- A virtual appliance and a software appliance
- Two hardware appliances of the same type (if you are replacing equipment)



You cannot transfer the license between hardware appliances and software/virtual appliances or between two different types of hardware appliances.

For example: You can transfer a license from one Kerio Control NG100 to another Kerio Control NG100, but you cannot transfer a license from Kerio Control NG100 to Kerio Control NG500.

Transfer the configuration using the built-in export and import feature. Read more in the [Configuration Assistant](#) article.

During the installation, register the same license number using the [Activation Wizard](#). After registering the license on the appliance, uninstall the original Kerio Control.



Uninstall the old system. You cannot use the same license on multiple systems.

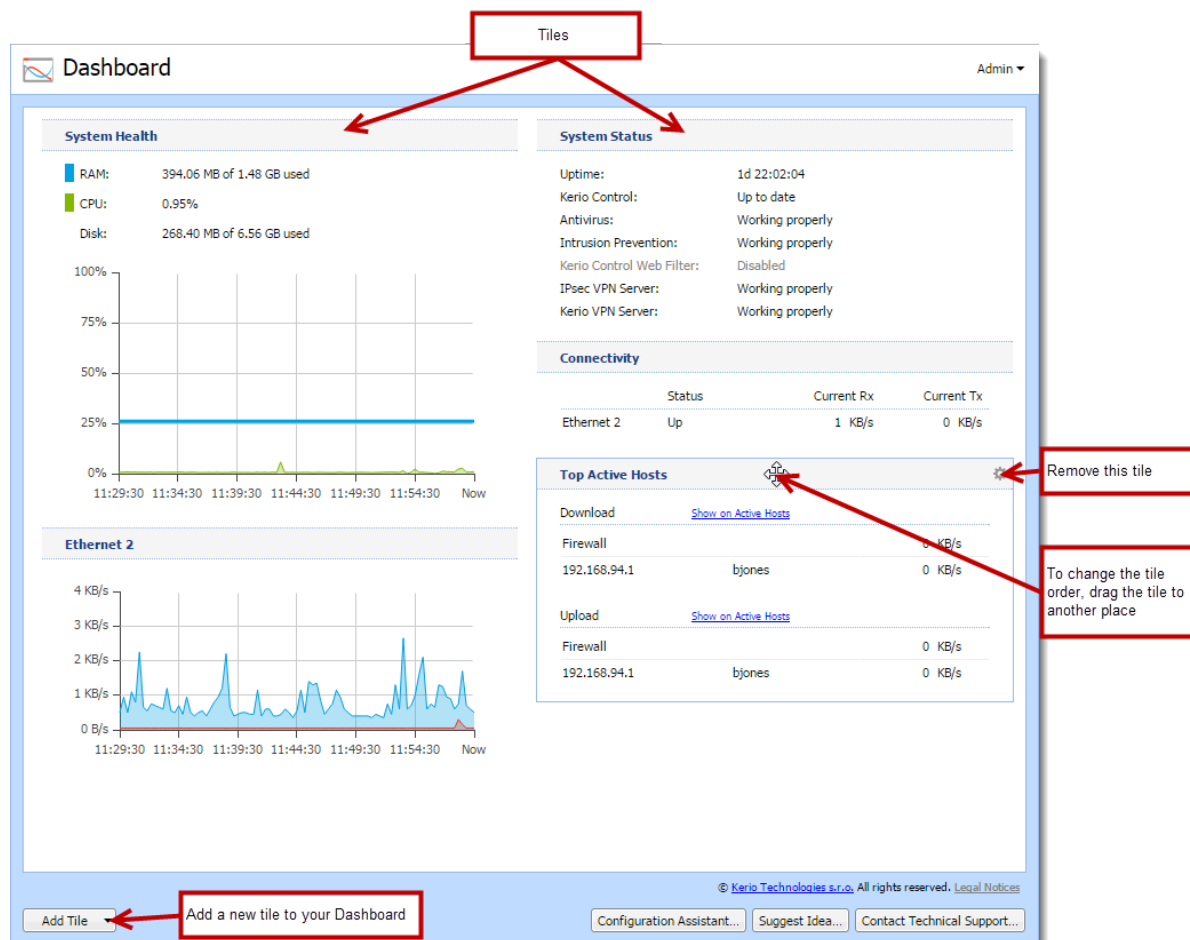
Using Dashboard in Kerio Control

Dashboard overview

Kerio Control includes a customizable Dashboard. Dashboard consists of tiles. Each tile displays a different type of information (graphs, statistics, Kerio News, etc.)

Dashboard is displayed in Kerio Control after each login.

To display Dashboard later, go to **Configuration** → **Dashboard**.



Configuring the Kerio Control web interface

Using HTTP for access to web interface

Kerio Control Web Interface is encrypted with SSL by default. If you need to switch to the HTTP connection:

1. Go to the administration interface.
2. In **Advanced Options** → **Web Interface**, uncheck **Force SSL secured connection**.



Unchecking of this option is a security risk.

3. Click **Apply**.

The screenshot shows the 'Advanced Options' window with the 'Web Interface' tab selected. Under the 'Web interface' section, the 'Force SSL secured connection (recommended)' checkbox is checked. The 'Use specified hostname' checkbox is also checked, with the text 'firewall.company.com' entered in the adjacent field. Below this, the 'Web Interface is accessible at:' is shown as 'https://firewall.company.com:4081/' and 'Administration is accessible at:' is shown as 'https://firewall.company.com:4081/admin'. Under the 'SSL certificate' section, the 'Certificate:' dropdown is set to 'Default' with an 'Edit...' button next to it. A blue information icon and text at the bottom state: 'If you change the certificate, you will need to login again to the Kerio Control Administration.'

Using a specified hostname

The default hostname of Kerio Control is `control`. If Kerio Control is a member of a domain (e.g. `example.com`), complete hostname will be `control.example.com`.

If Kerio Control is not a member of a domain, the hostname will be only `control`. In this case a problem could occur on older operating systems (e.g. Windows XP). Users cannot authenticate Kerio Control because the operating system is not able to read a one-word hostname. These operating systems need a hostname with at least two words separated by a dot (e.g. `control.mycompany`).

If you want to change the hostname, use the following steps:

1. In the administration interface, go to **Advanced Options** → **Web Interface**.
2. Select **Use specified hostname** and type a hostname (for example `firewall.mycompany.com`).
3. Click **Apply**.

Changing a SSL certificate

The principle of an encrypted Kerio Control web interface is based on the fact that all communication between the client and server is encrypted with SSL. For this reason you need a valid SSL certificate (see article [Configuring SSL certificates in Kerio Control](#)).

To change the current SSL certificate:

1. Go to the administration interface.
2. In the **Advanced Options** → **Web Interface**, select a certificate in the **Certificate** list.
3. Click **Apply**.

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,
- **IPsec and Kerio VPN interfaces** — virtual network interfaces (Kerio VPN, IPsec VPN),
- **Guest Interfaces** — interfaces which can be used for Guest LANs. See [Configuring guest networks](#), for more information.
- **Other interfaces** — interfaces which do not belong to any of the groups listed above (i.e. dial-like links).

Adding a new interface to the Interfaces section

Interfaces in Kerio Control represents:

- **Network adapter** — Each new network adapter in the Kerio Control computer displays as an interface in the **Interfaces** section.

If you use a Kerio Control Software Appliance, you must put a new network adapter (NIC) to the Kerio Control computer.

If you use a Kerio Control Virtual Appliance, you must create a new network adapter in your Hyper-V or VMware environment.
- **Port in Kerio Control Box** — In the **Interfaces** section displays LAN switch interface. You can take a port from the switch and [make it a standalone interface from the port](#).
- **VLAN** — If your network architecture is built on VLANs, you can [add VLANs as interfaces](#).

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 the [Configuration Assistant](#) article.

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:
 - **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 tunnels

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.
- L2TP — 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**.
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.

Configuring L2TP tunnel

This procedure is described in the [Configuring L2TP tunnel](#) article.

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 L2TP tunnel

L2TP tunnel overview

Kerio Control supports L2TP (Layer 2 Tunneling Protocol). Internet providers may use L2TP for creating tunnel for connecting you to the Internet. Configure L2TP interface when your provider requires this type of protocol.

Kerio Control also uses L2TP as a part of the [IPsec VPN solution](#). This article describes how the L2TP interface connects your company with the internet provider.

Prerequisites

You need the following information from your provider:

- L2TP server hostname
- username and password for L2TP server access

Configuring L2TP tunnel

You have to use L2TP interface when your provider uses L2TP for connecting you to the Internet.

1. In the administration interface, go to **Interfaces**.
2. Click **Add** → **L2TP**.
3. In the **L2TP Interface Properties** dialog, type a new interface name.
4. Leave the **Interface Group** as it is.
You can change it later.
5. On tab **Dialing Settings**, type the L2TP server hostname, username and password.
6. Set time intervals in which the connection should be established persistently and when it should be disconnected.

When the time interval is exceeded, the link demands manual dialing. The link can be hung up automatically after defined period of idleness.
7. Save the settings.

When the **Status** is **Up** in the **Interfaces** section, the L2TP tunnel is active.

Go to **Dial** log for more details about L2TP communications and dialing the line (see article [Using the Dial log](#)).

Configuring L2TP tunnel with public IP address

If your provider uses a public IP address in the L2TP interface, use additional steps:

1. In the administration interface, go to **Interfaces**.
2. Change **Internet connectivity** to **Multiple Internet Links - Load Balancing**.

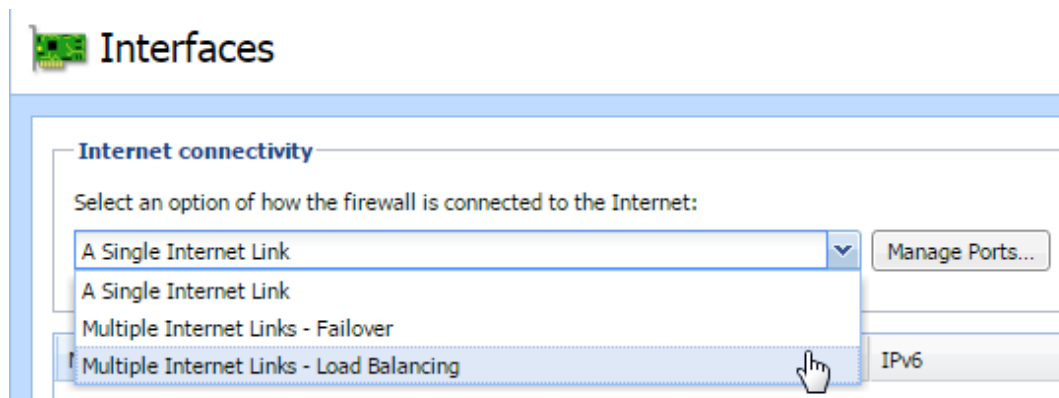


Figure 1 Load balancing configuration

3. Add L2TP tunnel (see above).
4. In **Interface Group**, select **Internet Interfaces**.
5. Enable **Use for Link Load Balancing** in the **L2TP Interface Properties** dialog.

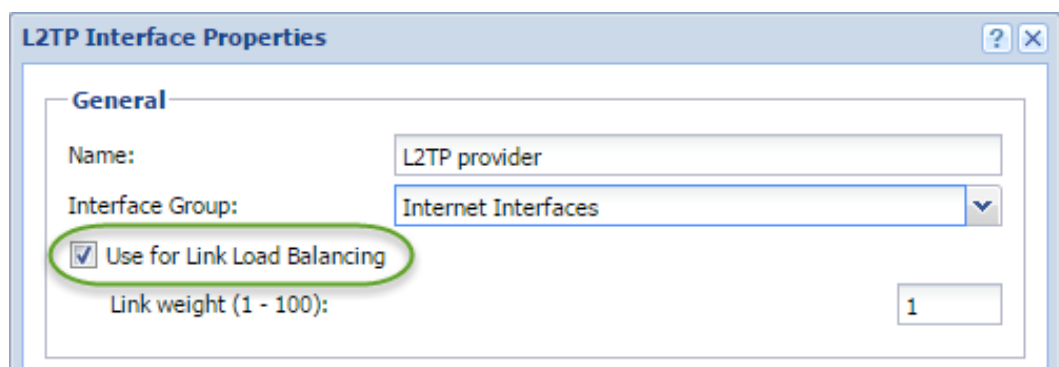


Figure 2 L2TP Interface Properties

Configuring L2TP tunnel

6. Disable **Use for Link Load Balancing** in the **Ethernet Interface Properties** dialog.

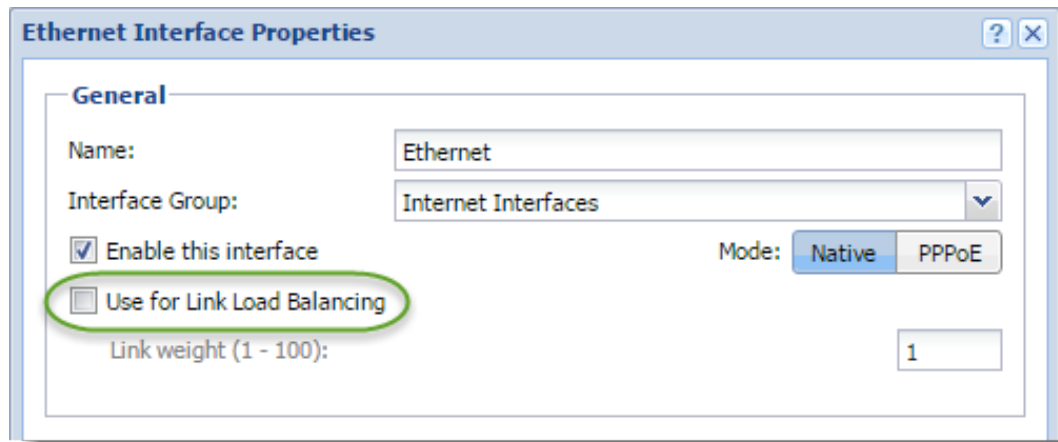


Figure 3 Ethernet Interface Properties

7. Save the settings.

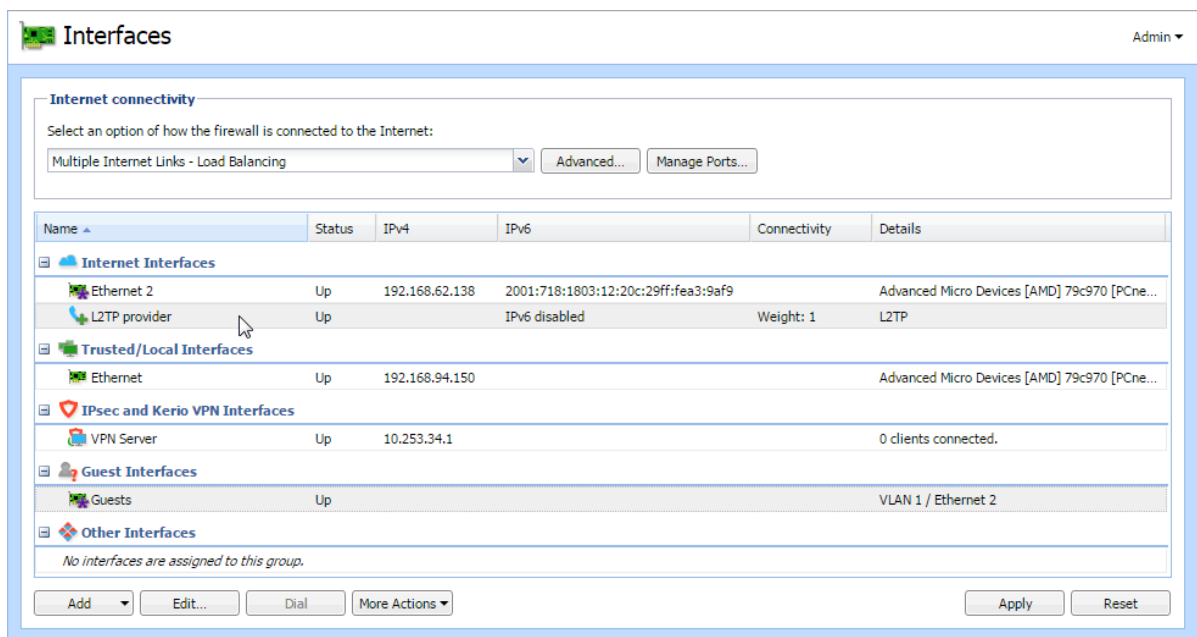


Figure 4 The result

When the **Status** is **Up** in the **Interfaces** section, the L2TP tunnel is active.

Go to **Dial** log for more details about L2TP communication and dialing the line (see article [Using the Dial log](#)).

Configuring the guest network

Guest network overview



Watch the [Configuring the guest network](#) video.

The guest network in Kerio Control offers your company's guests Internet access secured by Kerio Control.

- Guests can connect to your network without a Kerio Control username and password. Guests are not counted as licensed users.
- Kerio Control gathers statistics for the guest network under the built-in "Guest users" account.
- Users connect to the guest network from a [welcome page](#).
- You can set a [shared password](#) for accessing the Internet via a guest network. Guest users must type the shared password on the welcome page.
- Kerio Control redirects guest network users to the welcome page after 2 hours of inactivity.



Users connected through the guest network are fully secured by Kerio Control, except that Kerio Control Web Filter is disabled in the guest network.

Assigning guest interfaces

To create a guest network move an existing interface to the **Guest Interfaces** group.



To learn how to add a new interface to the **Interfaces** section, read [Configuring network interfaces](#).

To add one or more interfaces to the **Guest Interfaces** group:

1. In the administration interface, go to **Interfaces**.
2. Find the interface created for guests.
3. Drag that interfaces to the **Guest Interfaces** group.

Configuring the guest network

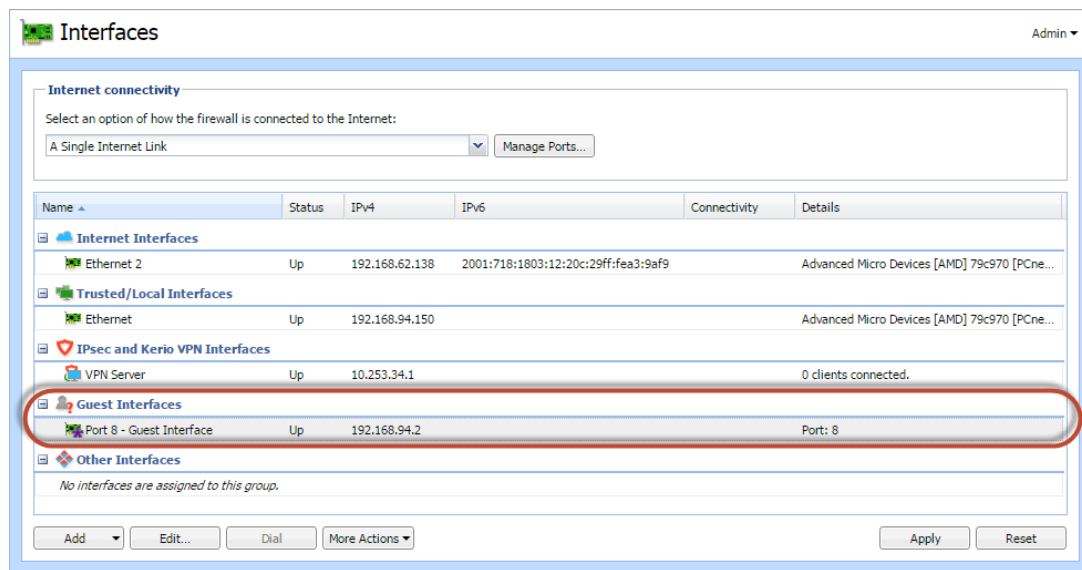


Figure 1 Section Interfaces

4. Click **Apply**.

Kerio Control creates the guest network and your guests can now connect to your company's Internet connection.

Setting DHCP scope

Interfaces from the **Guest Interfaces** group behave just like any interface from the **Trusted/Local Interfaces** or **Other Interfaces** group.

If the DHCP server in Kerio Control is enabled and you use automatic mode, the scope will be generated automatically. If you configure DHCP scopes manually, you must create a new one for each guest network.

Read more in [Using DHCP module](#).

Customizing the welcome page

When your guests access the Internet via the guest network, they see a welcome page. You can customize the page in Kerio Control, but you cannot disable it.

1. In the administration interface, go to **Domains and User Login**.
2. On the **Guest Interfaces** tab, type your own welcome text.



- You can format the message in [HTML](#).
- You can also add a custom logo in the **Advanced Options** → **Web Interface** section.

3. Click **Apply**.

Your guests now see this text on the welcome page.

Creating HTML content in your Welcome page

You can format the page in HTML.

You can also add links to external websites accessible via HTTP (for example: `HTTP link`). These web pages are accessible even without clicking on the **Continue** button. However, ensure that the linked pages do not require any external content (scripts, fonts, etc.), because this content will not be available.

Setting shared password for guest users

To set up a password guests can use to access the Internet via the guest network, customize it in Kerio Control:

1. In the Kerio Control administration, go to **Domains and User Login**.
2. On the **Guest Interfaces** tab, check the **Require users to enter password** option.
3. In the **Password** field, type the password.
All guests must use this password to access the Internet via guest network.
4. Click **Apply**.

Your guests must login with the password to access the Internet via guest network by typing the password on the [welcome page](#).

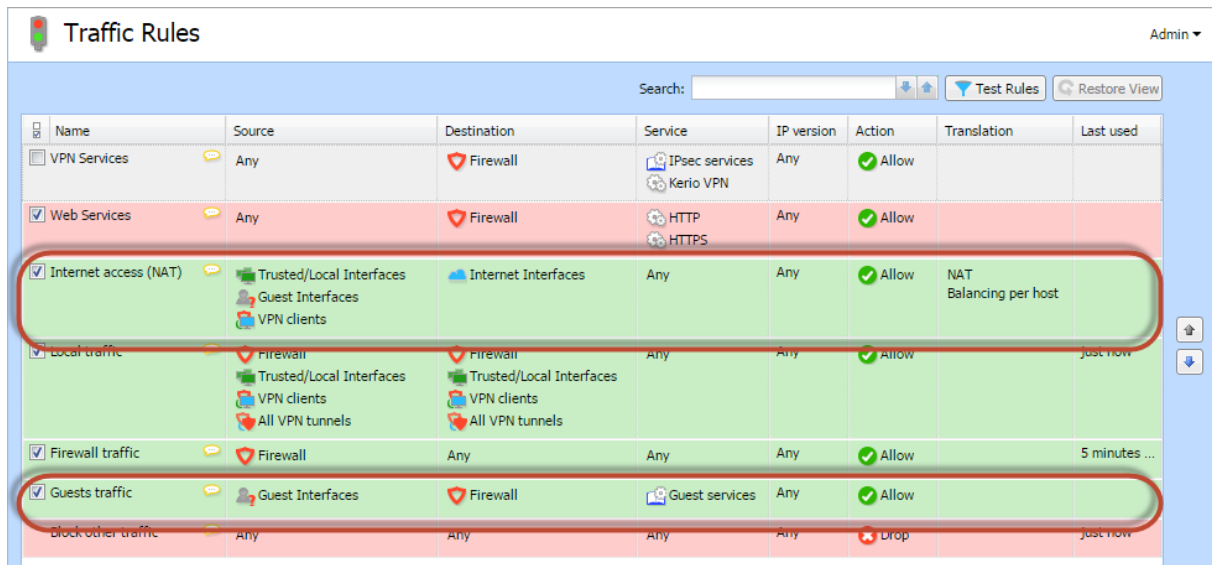
Traffic rules for the guest network

Traffic rules in Kerio Control include two rules that concern guest interfaces.

In the **Internet access (NAT)** outgoing rule, all guest interfaces are included.

The **Guests traffic** rule allows the traffic from all guest interfaces access to the firewall with a [Guest services group](#).

Configuring the guest network



Name	Source	Destination	Service	IP version	Action	Translation	Last used
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow		
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow		just now
Firewall traffic	Firewall	Any	Any	Any	Allow		5 minutes ...
Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow		
Block other traffic	Any	Any	Any	Any	Drop		just now

Figure 2 Traffic rules tab



Guests can access the firewall and Internet only. This is a hard-coded behavior. Traffic rules cannot override it.

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.

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. Type VLAN IDs separated by semicolons. VLAN ID is a number between 1 and 4094. To create multiple VLANs, add less than 90 VLANs at once.

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.

Configuring VLANs

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.

Changing MAC addresses of network interfaces

Overview



New in Kerio Control 8.5.0

A MAC address identifies devices on a network. Some routers or Internet service providers permit only specific MAC addresses. When you need to use a device or network adapter with a specific MAC address on your side, you can change the MAC address of a network interface in Kerio Control.

Changing MAC addresses

To override the MAC address:

1. In the administration interface, go to **Interfaces**.
2. Double-click the interface.
The **Interface Properties** dialog box opens.
3. Click the **Advanced** button.
The **Advanced Interface Properties** dialog opens.
4. Select **Override MAC address** and type the address.
5. Save your settings.

The interface now uses the newly configured MAC address.

Changing MAC addresses of network interfaces

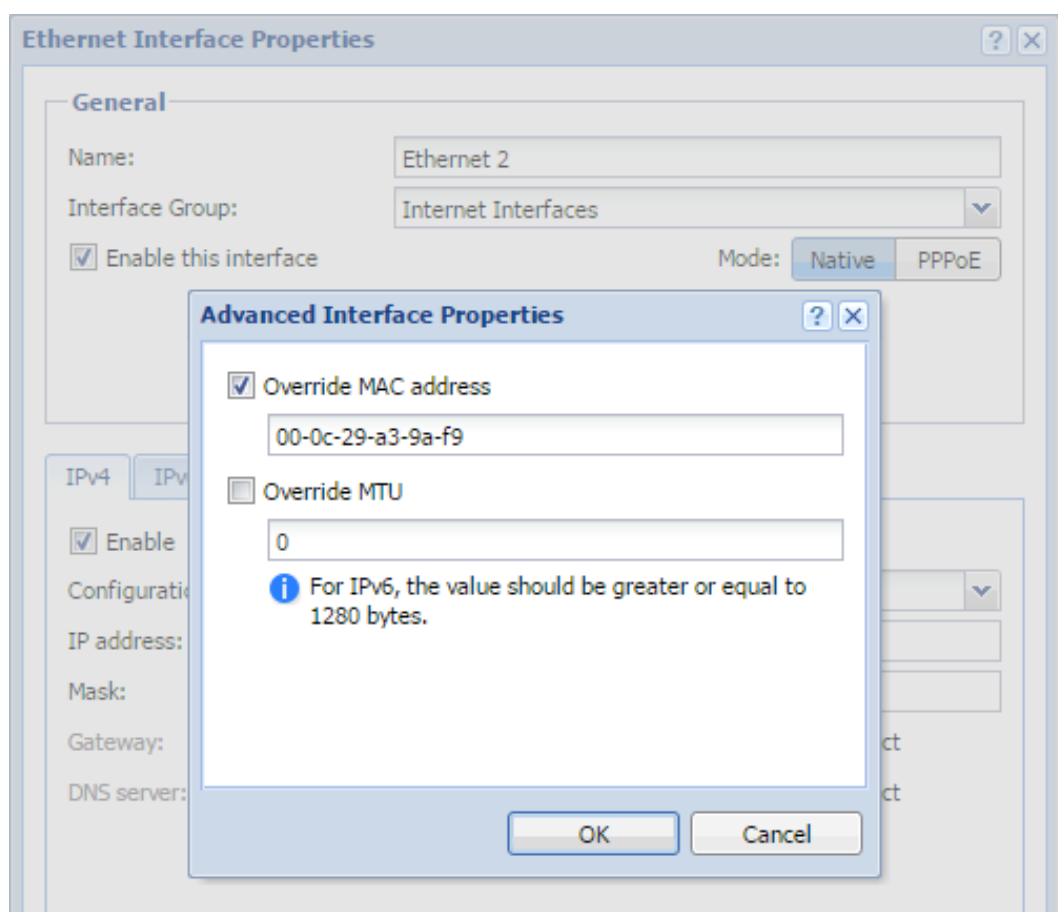


Figure 1 Ethernet Interface Properties dialog

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 **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.

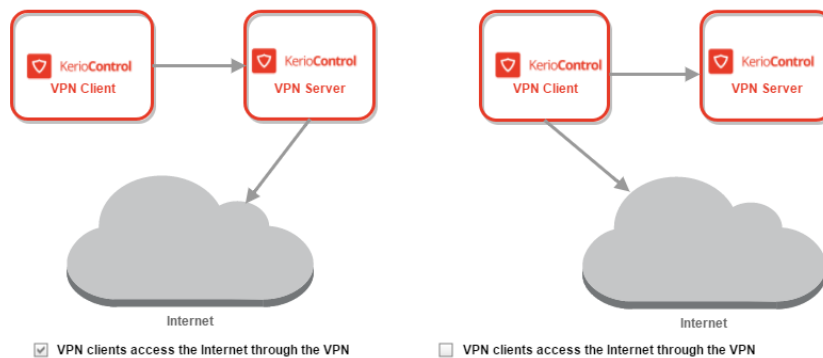


Do not switch to another port without a proper reason.

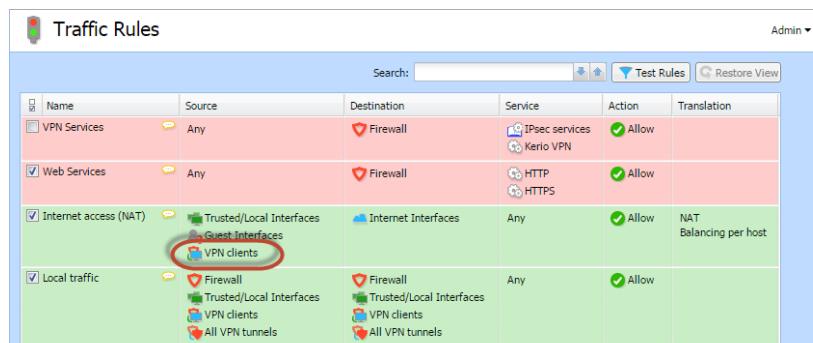
If it is not possible to run the VPN Server at the specified port (the port is used by another service), the error will be reported in the [Error log](#).

6. To specify a VPN route manually, read section [Configuring routing](#).
7. Kerio VPN Server directs the traffic from VPN clients in two ways:
 - Only traffic which ends in the Kerio Control network goes through the firewall — default mode. This type of connection is called [split tunneling](#).
 - All traffic goes through the firewall — select **VPN clients access the Internet through the VPN**.

Configuring Kerio VPN Server



Verify that your default **Internet access (NAT)** rule includes the **VPN clients** item.



8. 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 DNS

Using the Kerio Control DNS server

To use the [DNS server in Kerio Control](#) for Kerio Control VPN Clients:

1. In the administration interface, go to **Interfaces**.
2. Double-click **VPN Server**.
3. On the **DNS** tab, select **Use Kerio Control as DNS server**.
4. Select **Automatically select the domain suffix**.
5. Click **OK**.

Kerio Control uses its own DNS server for Kerio Control VPN Clients and uses the domain suffix specific for the Kerio Control network.

The screenshot shows the 'DNS' tab of the Kerio Control configuration interface. At the top, there are four tabs: 'IPsec VPN', 'Kerio VPN', 'DNS' (which is selected), and 'WINS'. Below the tabs, there are four radio button options: 'Use Kerio Control as DNS server' (selected), 'Use specific DNS servers', 'Automatically select the domain suffix' (selected), and 'Use specific domain suffix'. Under 'Use specific DNS servers', there are two text input fields labeled 'Primary DNS:' and 'Secondary DNS:'. Under 'Use specific domain suffix', there is a text input field labeled 'Domain suffix:'.

Configuring Kerio VPN Server

Using external DNS servers

To assign specific DNS servers to Kerio Control VPN Clients:

1. In the administration interface, go to **Interfaces**.
2. Double-click **VPN Server**.
3. On the **DNS** tab, select **Use specific DNS servers**.
4. In **Primary DNS**, type a fully qualified domain name.
5. (Optional) In **Secondary DNS**, type a fully qualified domain name of the backup DNS server.
6. If you want to use a different domain suffix, select **Use specific domain suffix**. Then type the domain suffix.
7. Click **OK**.

The DNS servers are assigned to all Kerio Control VPN Clients and the domain suffix is changed.



To use WINS to Kerio Control VPN Clients, select the **WINS** tab in the **VPN Server Properties** dialog box, and specify the WINS server.

Configuring Kerio Control 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 defined service for Kerio VPN (TCP/UDP 4090) in case you do not have this rule.

Hint:

Kerio Control VPN Clients connected to the firewall are monitored in the **Status** → **VPN Clients** section.

Assigning static IP addresses for Kerio Control VPN Clients

For details, read [Assigning static IP addresses for Kerio Control VPN Clients](#).

Kerio Control VPN Client for administrators

Overview

Kerio Control VPN Client enables an encrypted connection from individual systems (clients) to a remote private network via the Internet. The connection enables these clients to access the private network as if they were physically connected.

Three versions of Kerio Control VPN Client are available:

- Kerio Control VPN Client for Windows
- Kerio Control VPN Client for OS X
- Kerio Control VPN Client for Linux (read more in the [read-me file](#))

Kerio Control VPN Client connects to the VPN server in Kerio Control. Kerio Control user accounts are used to authenticate clients.

Users with administration rights to a computer can establish persistent connections. Persistent connections are reestablished whenever the user restarts their computer.



If users need to access services hosted on the Kerio Control VPN Client, you can assign a static IP address to Kerio Control VPN Client in Kerio Control. Read [Assigning static IP addresses for Kerio Control VPN Clients](#).

System requirements

For up-to-date system requirements, refer to:

<http://www.kerio.com/control/technical-specifications>

Licensing Policy

Kerio Control VPN Client does not require a special license.

Connecting to Kerio VPN Server

1. Configure [Kerio Control VPN Server in Kerio Control](#).
2. Install and configure Kerio Control VPN Client. For details, read [Installing and configuring Kerio Control VPN Client for users](#)



Kerio Control VPN Client for OS X uses a PackageMaker installer. You can deploy it to users' computers through Apple Remote Desktop or a similar application.

3. (Optional) Consider using 2-step verification. For more information, read [Configuring 2-step verification](#).

Troubleshooting SSL certificates

If Kerio Control VPN Client detects any certificate-related problems, a warning appears. If you consider the Kerio Control server trustworthy, confirm the warning. Kerio Control VPN Client saves the certificate.

Certificate-related problems are often caused by one of the following issues:

- The date of the certificate is not valid and you need to generate a new one in Kerio Control.
- The security certificate has been changed at the server since the last check.
- The certificate was issued by an untrusted authority.

Operating systems where Kerio Control VPN Clients are installed can have a problem with self-signed certificates or certificates issued by your local certification authority. If you use untrustworthy certificates, help users to get the root certificate to their computers.

- The name referred to the certificate does not match the server name.

The name of the server specified in the certificate does not correspond with the name of the server Kerio Control VPN Client is connecting to. This problem occurs when the server uses an invalid certificate or when the server name has changed. However, it can also suggest an intrusion attempt (a false DNS record with an invalid IP address has been used).



Certificates can be issued only for servers' DNS names, not for IP addresses.

Kerio Control VPN Client logs

This section is dedicated to Windows and OS X operating systems. If you need logs on Linux, read the following [read-me file](#).

Kerio Control VPN Client generates logs of its own activity and detected errors. The system service and the application's user interface work separately and separate logs are generated for each of these components. Use Log files for troubleshooting and for communication with Kerio Technologies technical support.

System service logs

The following log files are available for Kerio Control VPN Client:

- `error.log` contains critical errors, such as that the **Kerio VPN Client Service** failed to start, the VPN server is not available, or user authentication failed.
- `debug.log` contains detailed information on activities of the system service and detected errors.

By default, Kerio VPN Client Service saves the logs to the following locations:

- Windows: `C:\Program Files\Kerio\VPN Client\logs`
- OS X: `/usr/local/kerio/vpnclient/logs`

User interface logs

The following log files are available for Kerio Control VPN Client:

- `error.log`, which contains critical errors, such as failure to establish connection to Kerio VPN Client Service
- `debug.log`, which has detailed information on application activities and detected errors

Logs of the user interface are stored in the home folder of the user currently using the Kerio Control VPN Client. By default, the following path is used:

- Windows 7: `C:\Users\alexsmith\AppData\Roaming\Kerio\VpnClient\logs`
- OS X: `/Users/alexsmith/.kerio/vpnclient/logs`

Assigning static IP addresses for Kerio Control VPN Clients

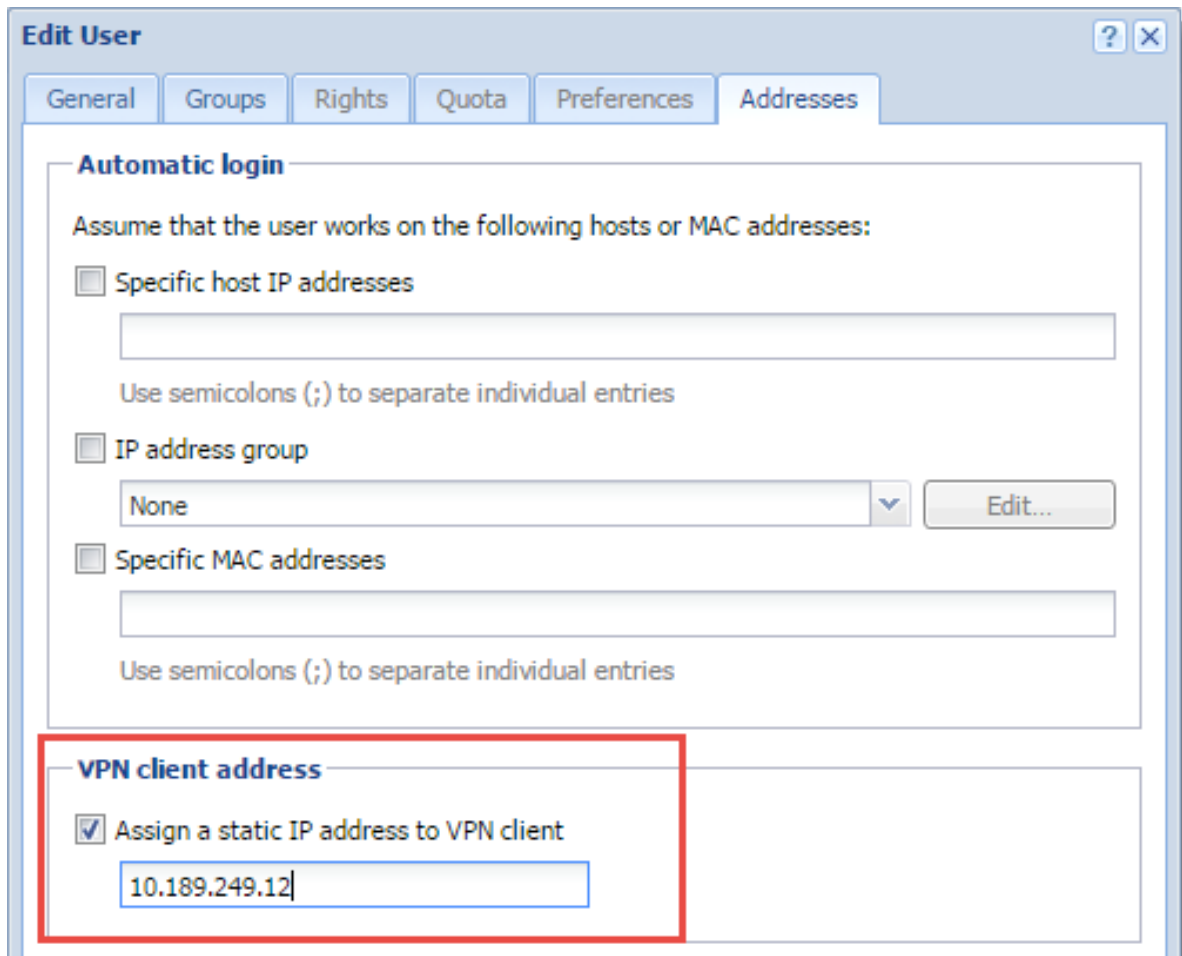
Overview

If Kerio Control user needs to access services hosted on the Kerio Control VPN Client, you can assign a static IP address to Kerio Control VPN Client.

For more information about Kerio Control VPN, read [Configuring Kerio Control VPN server](#)

1. In the administration interface, go to **Users and Groups** → **Users**.
2. Double-click the user to whom you want to assign a static IP address.
3. In the **Edit User** dialog box, go to the **Addresses** tab.
4. Select **Assign a static IP address to VPN client**.
5. Type the static IP address.
6. Click **OK**.

Assigning static IP addresses for Kerio Control VPN Clients



Edit User

General Groups Rights Quota Preferences **Addresses**

Automatic login

Assume that the user works on the following hosts or MAC addresses:

☐ Specific host IP addresses

Use semicolons (;) to separate individual entries

☐ IP address group

None Edit...

☐ Specific MAC addresses

Use semicolons (;) to separate individual entries

VPN client address

☒ Assign a static IP address to VPN client

10.189.249.12

From now on, Kerio Control assigns the IP address to user's Kerio Control VPN Client.

Do not set the same IP address to multiple users, Kerio Control will assign the address to the last edited user. All other users with the same IP address lose it and they get a dynamic address from the DHCP server.

Do not set the same IP address to multiple devices.

Configuring Kerio VPN tunnel

Kerio VPN overview

Kerio Control supports VPN (Virtual Private Network). Kerio Control includes a proprietary implementation called Kerio VPN. You can use Kerio VPN as:

- Kerio VPN tunnel to connect LANs
- [Kerio VPN server](#) to connect clients (for example, desktops, notebooks, mobile devices, and so on)

Configuring the Kerio VPN tunnel

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

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

4. Set the tunnel as:
 - **Active** to connect to a remote endpoint. Type the hostname of the remote VPN server. Specify also the port number if it differs from 4090 (for example, `server.company.com:4100`).
 - **Passive** if the local end of the tunnel has a fixed IP address and accept only incoming connections.
5. As **Type**, select **Kerio VPN**.
6. On the **Authentication** tab, specify the fingerprint for the local and remote VPN server certificates.

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**.

In the configuration at the remote server, specify the fingerprint of this local server.

7. Save your settings.



All local networks at each location must have unique IP subnets. Before connecting two sites using VPN Tunnel, make sure that their local network ranges are not the same, otherwise the routing does not work.

Configuring routing

By default, routes to all local subnets at the VPN server are defined. You can also specified other routes:

1. In the administration interface, go to **Interfaces**.
2. Double-click a VPN tunnel.
3. On the **Remote Networks** tab, select **Use custom routes**.

If **Use routes provided automatically by the remote endpoint** is also selected, custom routes are used instead in case of a collision.

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

Configuring VPN failover

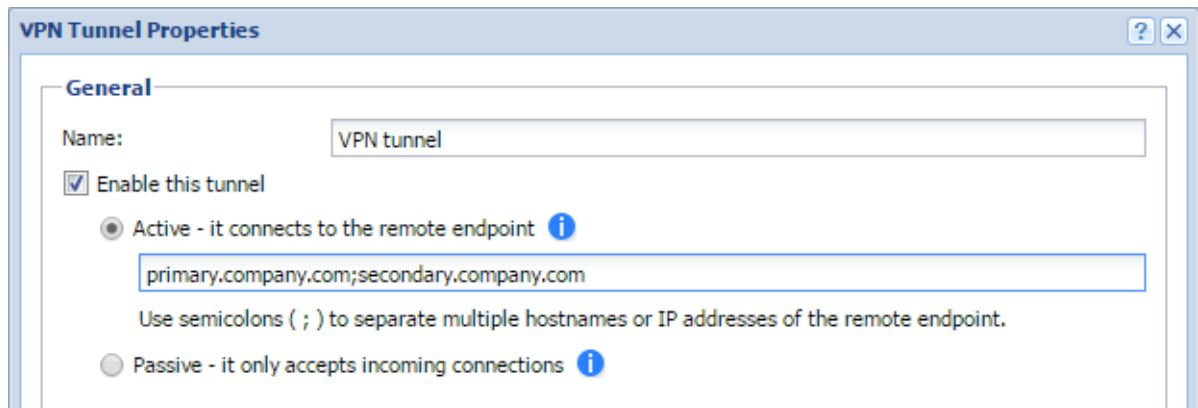
If Kerio Control uses load balancing between multiple Internet links, it is possible to use VPN failover.

VPN failover ensures that a VPN tunnel is re-established automatically in case the primary link used for VPN tunnelling becomes unavailable.

To configure failover, input all remote endpoints (by hostname or IP address), separated by semicolons, into the VPN tunnel properties (see the image below).



When attempting to establish the tunnel, Kerio Control will cycle through the list of the endpoints in the same order that they are listed in the VPN Tunnel Properties.



Examples of Kerio VPN tunnel configuration

Example 1 - Company with one branch office

This example describes how to connect two company local networks using the Kerio VPN tunnel.

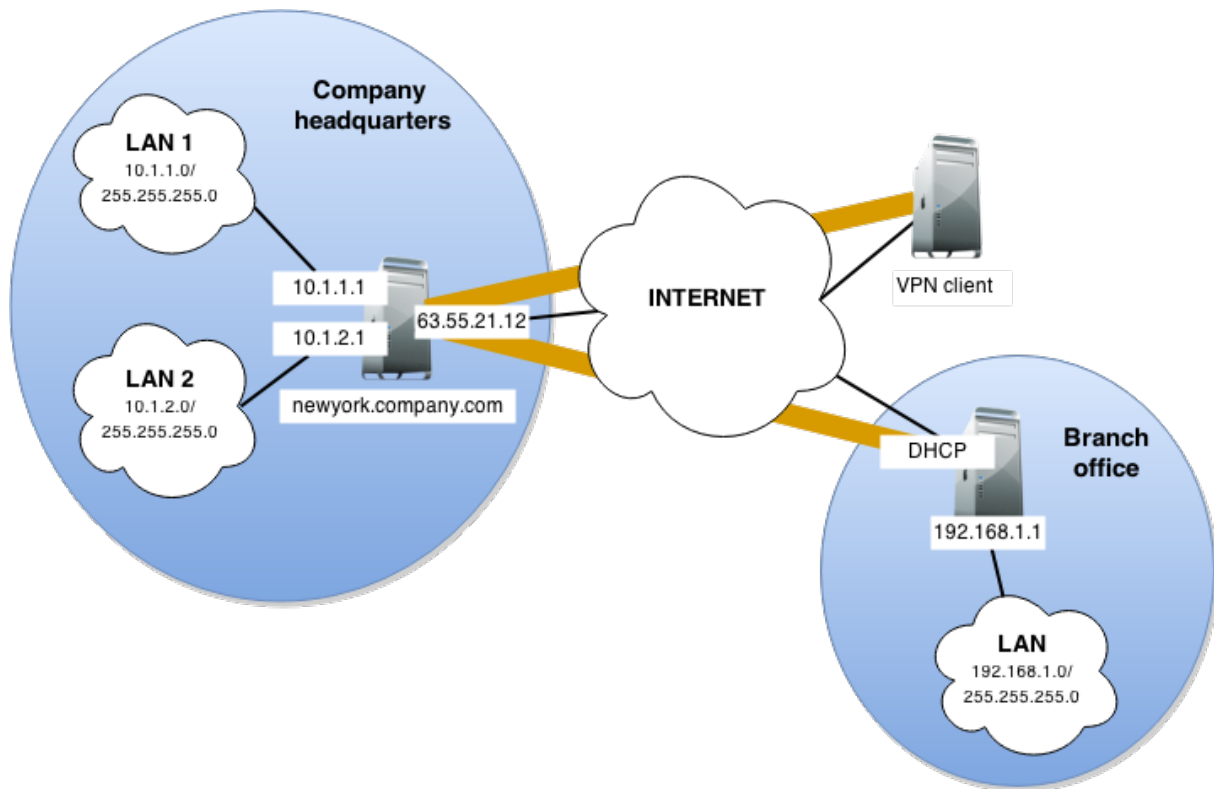
In this example:

- The headquarters office (the default gateway) uses the public IP address 85.17.210.230 with `newyork.company.com` as the DNS name
The branch office server uses a dynamic IP address assigned by DHCP
- The headquarters has two subnets, LAN1 and LAN2 with `company.com` as the DNS name
The branch office network has a single subnet, LAN, and uses `branch.company.com` as the DNS name

The traffic between both networks and VPN clients follows these rules:

- VPN clients can connect to LAN1 and the branch office network (LAN)
- Users cannot connect to VPN clients from any network
- From the branch office, users can connect only to the LAN1 network, and only the WWW, FTP, and Microsoft SQL services are available
- There are no restrictions for connections from the headquarters office to the branch office

Configuring Kerio VPN tunnel



You must configure the following settings:

1. In the headquarters Kerio Control administration, define the VPN tunnel.
The active endpoint is at the branch office (dynamic IP address).
The passive endpoint is at the headquarters server (public IP address).

VPN Tunnel Properties

General

Name:

☒ Enable this tunnel

☐ Active - it connects to the remote endpoint i

Remote endpoint hostname or IP address:

☒ Passive - it only accepts incoming connections i

Type: IPsec Kerio VPN

Authentication Remote Networks

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.

2. Verify the tunnel is created.

If not, refer to the [Error log](#), check the certificate fingerprints, and the availability of the remote server.

3. In [traffic rules](#), allow traffic between the local network, remote network, and VPN clients.

Name	Source	Destination	Service	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	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	Any	Allow		just now

4. Set traffic restrictions at the headquarter's server.

On the branch office server, only traffic between the local network and the VPN tunnel is enabled.

Configuring Kerio VPN tunnel

Name	Source	Destination	Service	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> Kerio VPN Server	Any	Firewall	Kerio VPN	Any	Allow		
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local Interfaces	Firewall Trusted/Local Interfac...	Any	Any	Allow		just now
<input checked="" type="checkbox"/> Kerio VPN Clients	VPN clients	LAN 1 Tunnel to branch office	Any	Any	Allow		
<input checked="" type="checkbox"/> Branch office	Tunnel to branch office	LAN 1	Any	Any	Allow		
<input checked="" type="checkbox"/> Company headquarters	Trusted/Local Interfaces	Tunnel to branch office	Any	Any	Allow		

5. Test the connection from each local network. Test availability both through the IP addresses and DNS names.

Use the `ping` and `tracert` (`traceroute`) system commands.

If the test through IP address does not respond, check the traffic rule configuration and verify that the subnets do not collide.

If IP address test is OK and the DNS test fails (Unknown host), check the DNS configuration.

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](#).

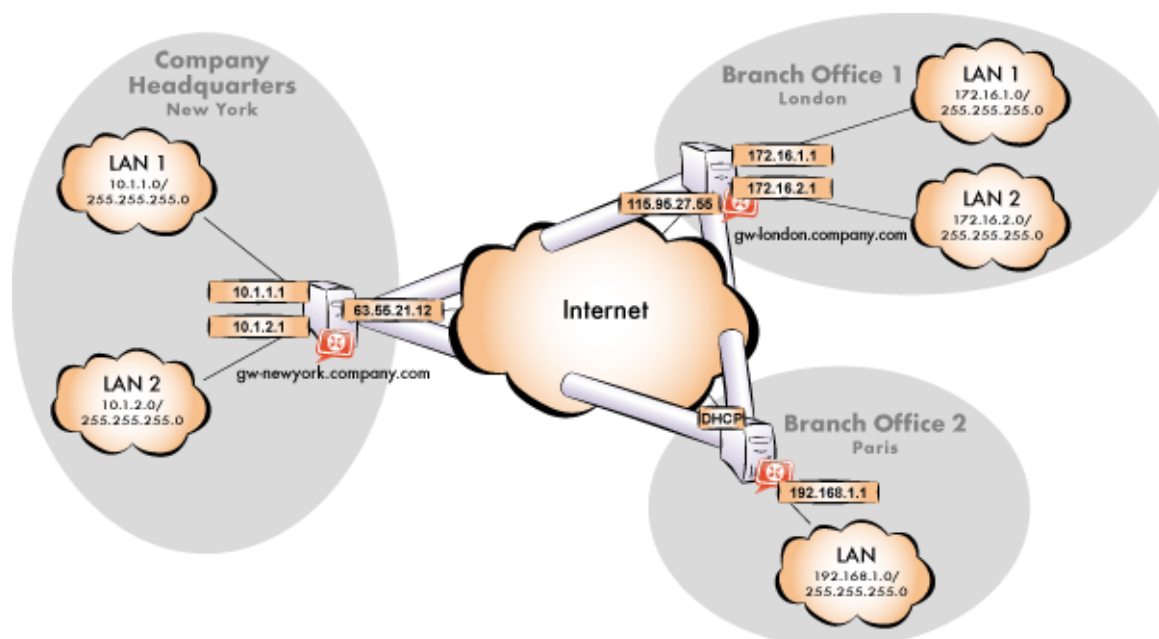


Figure 1 Example of a VPN configuration — a company with two filials

Example of Kerio VPN configuration: company with two filial offices

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.

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	IP version	Action	Translation	Last used
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		just now
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow		just now

Figure 2 Headquarter — default traffic rules for Kerio VPN

Example of Kerio VPN configuration: company with two filial offices

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.

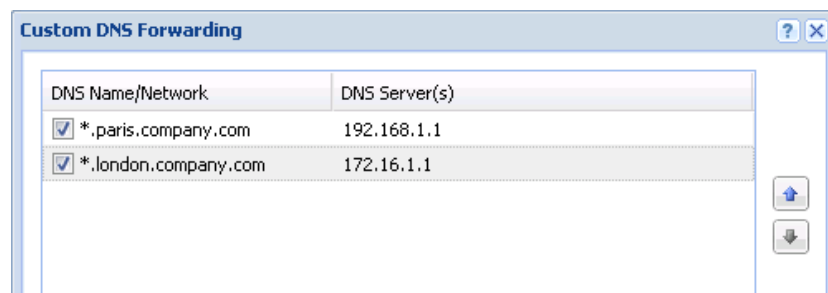


Figure 3 Headquarter — DNS forwarding settings

- 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.

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).

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 - 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).

Network	Mask	Description
<input checked="" type="checkbox"/> 192.168.1.0	255.255.255.0	Paris - LAN

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

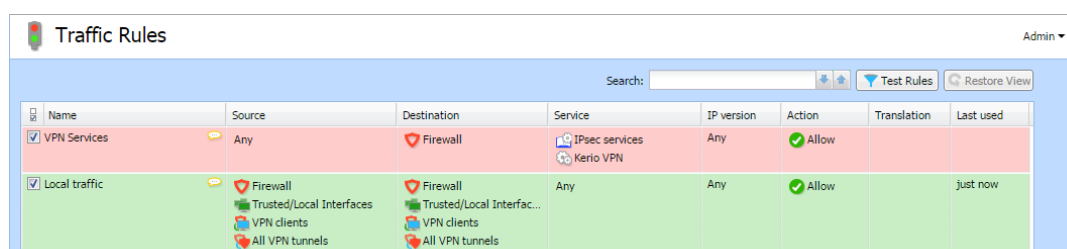
Configuration of the London filial

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).

Example of Kerio VPN configuration: company with two filial offices

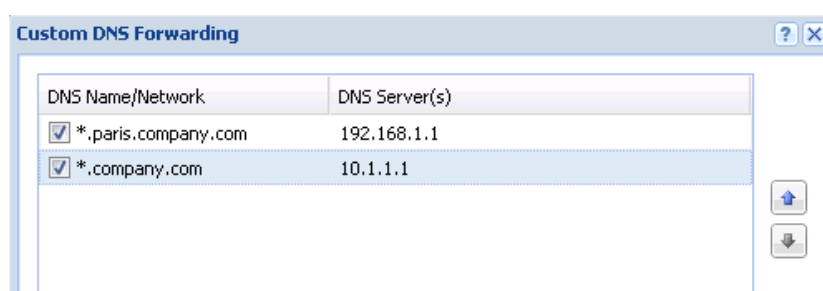


Name	Source	Destination	Service	IP version	Action	Translation	Last used
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow		just now

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.



DNS Name/Network	DNS Server(s)
*.paris.company.com	192.168.1.1
*.company.com	10.1.1.1

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.

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.

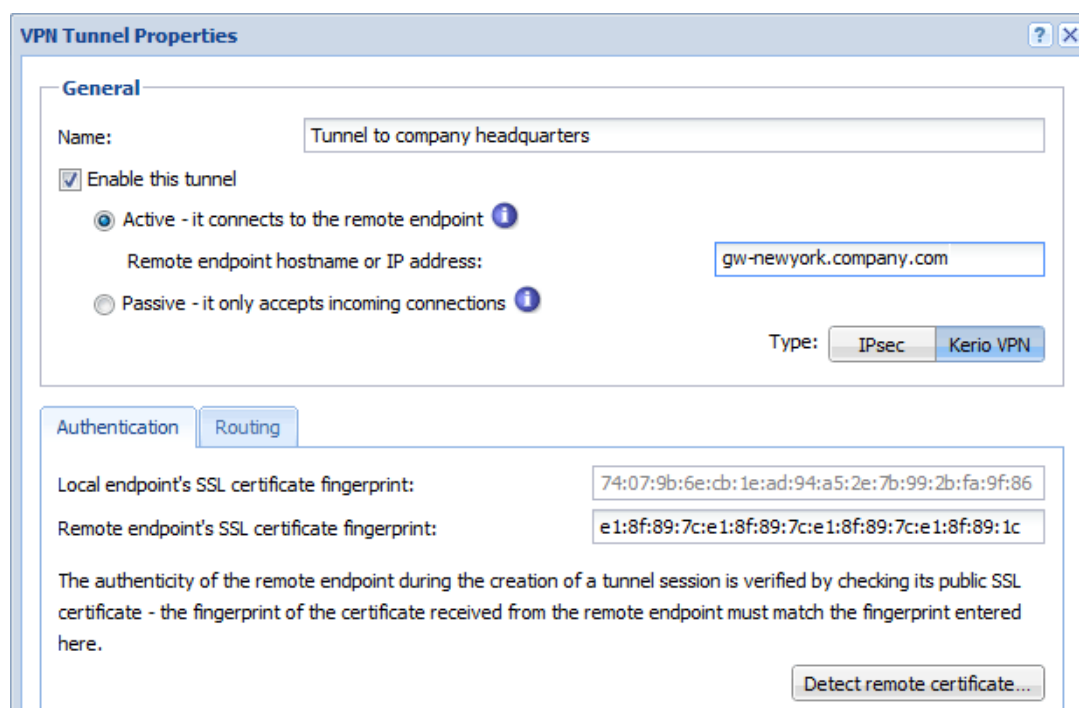


Figure 8 The London filial office — definition of VPN tunnel for the headquarters

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

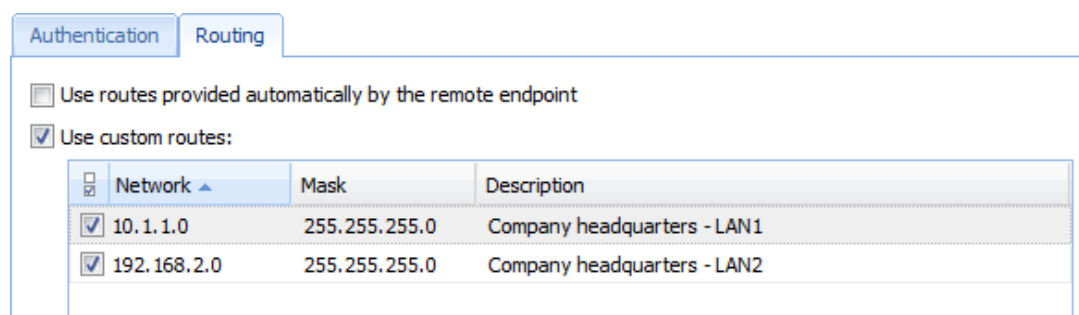


Figure 9 The London filial — routing configuration for the tunnel connected to the headquarters

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
```

Example of Kerio VPN configuration: company with two filial offices

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.

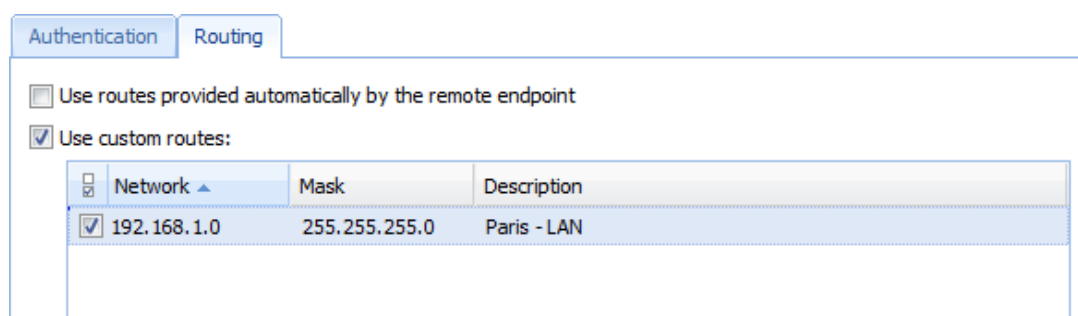


Figure 10 The London filial — routing configuration for the tunnel connected to the Paris branch office

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).

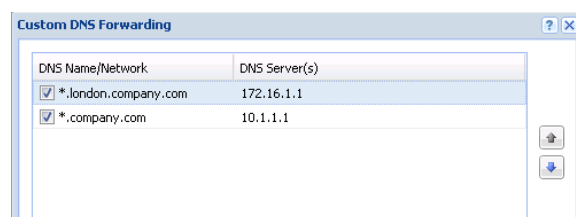


Figure 11 The Paris filial office
— DNS forwarding settings

- 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.

The screenshot shows the 'Routing' tab in the Kerio Control configuration interface. Under the 'Use custom routes' section, there is a table with the following data:

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.

Example of Kerio VPN configuration: company with two filial offices

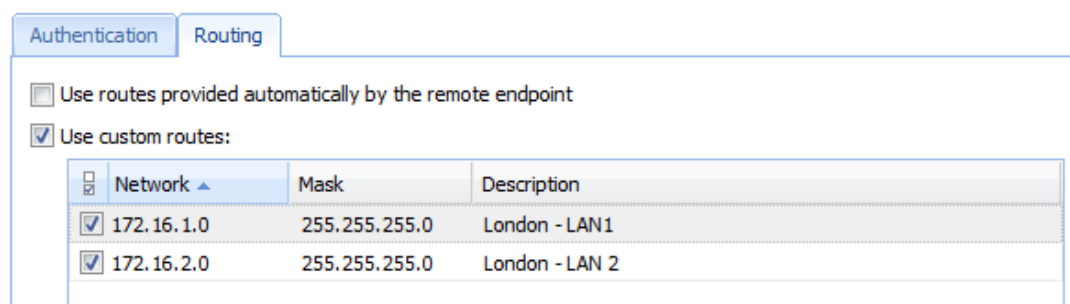


Figure 13 The Paris filial — routing configuration for the tunnel connected to the London branch office

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**.

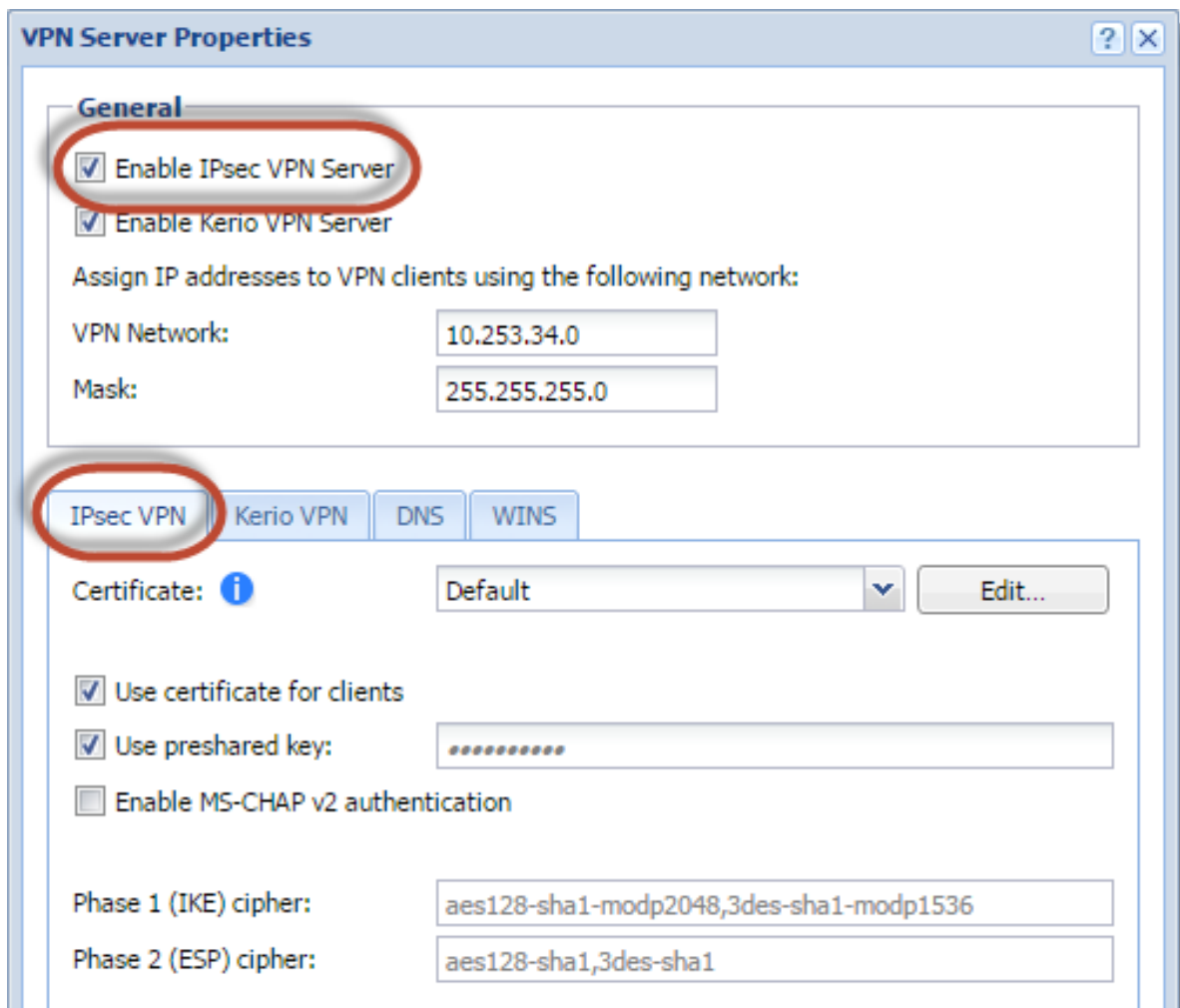


Figure 1 VPN Server Properties



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. Save the settings.

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. 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

Configuring IPsec VPN

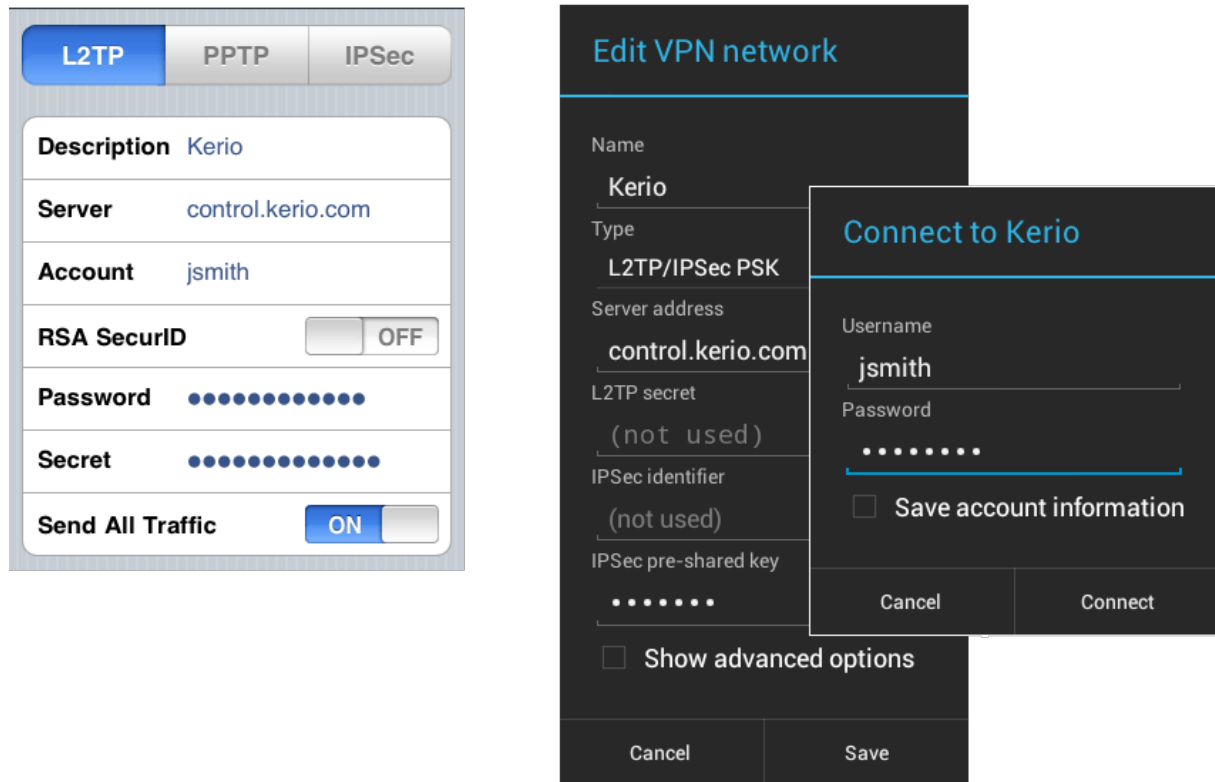


Figure 2 Examples of Apple iPhone and Android settings

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.



If you can connect two or more Kerio Controls via VPN tunnel, use [Kerio VPN](#). Kerio VPN tunnel is able to seek routes in remote networks.

Before you start

Prepare the following list:

- [Enable the VPN Services pre-configured traffic rule](#) on both tunnel endpoints.
- ID of the remote endpoint (in the most of servers it is called **Local ID**).
- You must prepare a list of all routes behind the remote endpoint.
- If you want to use a SSL certificate, prepare the SSL certificate of the remote endpoint, or an authority + ID of the remote SSL certificate. [You must import the certificate or the authority to Kerio Control](#).

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.

Configuring IPsec VPN tunnel

4. Set the tunnel as active (and type the hostname of the remote endpoint) or passive.

One Kerio Control must be set as active and the other as passive. The active endpoint establishes and maintains a connection to the passive endpoint.

5. Select **Type**: IPsec.
6. Select **Preshared key** and type the key.
7. Copy the value of the **Local ID** field from Kerio Control to the **Remote ID** of the remote endpoint and vice versa.

Predefined Local ID is the hostname of Kerio Control. If you change the Kerio Control hostname, Local ID will be changed too.

8. On tab **Remote Networks**, you must define all remote networks including subnet for VPN clients.

IPsec VPN is not able to seek remote networks. You must enter them manually.

9. Save the settings.



IKE ciphers displayed in the **VPN Server Properties** dialog are recommended. However, Kerio Control is able to work with ciphers described in [this article](#).

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 (Distinguished name) of the remote certificate.

When 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.
One endpoint must be set as active and the other as passive. The active endpoint establishes and maintains a connection to the passive endpoint.

5. Select **Type**: IPsec.
6. Select **Remote certificate**:
 - **Not in local store** — only an authority was imported to Kerio Control. Copy the remote SSL certificate ID to the **Remote ID** field and vice versa: import the Kerio Control authority to the remote endpoint and copy the **Local ID** somewhere in the remote endpoint.
 - Select the remote SSL certificate
Export the certificate from Kerio Control and import it to the remote endpoint.
7. On tab **Remote Networks**, you must define all remote networks including subnet for VPN clients.
IPsec VPN is not able to seek remote routes. You must enter them manually.
8. Save the settings.



IKE ciphers displayed in the **VPN Server Properties** dialog are recommended. However, Kerio Control is able to work with ciphers described in [this article](#).

Configuring local networks

Kerio Control IPsec tunnel is able to detect most of its local networks. To enable the automatic detection:

1. Go to **Interfaces** in the Kerio Control Administration.
2. Select the IPsec VPN tunnel and click **Edit**.
3. In the **VPN Tunnel Properties** dialog box, select **Use automatically determined local networks**.

Automatically determined local networks are:

- All non-internet interfaces networks with no default route.
- Static networks.
- Remote networks of other IPsec tunnels.
- Manually specified custom remote networks of Kerio VPN tunnels.
- VPN subnet.

Configuring IPsec VPN tunnel

4. If you define custom routes, select **Use custom networks** too.



To setup Kerio Control VPN — IPsec VPN interoperability, add also networks connected via Kerio Control VPN which are not defined manually in the Kerio Control VPN tunnel configuration.

5. Click **OK**.

VPN Tunnel Properties

General

Name:

☒ Enable this tunnel

☐ Active - it connects to the remote endpoint i

Use semicolons (;) to separate multiple hostnames or IP addresses of the remote endpoint.

☒ Passive - it only accepts incoming connections i

Type: IPsec Kerio VPN

Local Networks

☒ Use automatically determined local networks

☒ Use custom networks:

<input checked="" type="checkbox"/> Network ▲	Mask	Description
<input checked="" type="checkbox"/> 192.168.22.0	255.255.255.0	LAN 22

Networks from the following interfaces are not detected automatically:

- Interfaces from the **Internet Interfaces** group
- Interfaces with a default route
- Networks dynamically discovered by Kerio VPN

Configuring VPN failover

If Kerio Control is load balancing between multiple Internet links, it is possible to use VPN failover. This will ensure that a VPN tunnel is re-established automatically in case the primary link used for VPN tunnelling becomes unavailable.

To configure failover, input all remote endpoints (by hostname or IP address), separated by semicolons, into the VPN tunnel properties.



When attempting to establish the tunnel, Kerio Control will cycle through the list of the endpoints in the same order that they are listed in the **VPN Tunnel Properties**.

The screenshot shows the 'VPN Tunnel Properties' dialog box with the 'General' tab selected. The 'Name' field contains 'VPN tunnel'. The 'Enable this tunnel' checkbox is checked. Under the 'Active' radio button, the text 'primary.company.com;secondary.company.com' is entered in the endpoint field. A note below the field states: 'Use semicolons (;) to separate multiple hostnames or IP addresses of the remote endpoint.' The 'Passive' radio button is also visible but not selected.

Configuring IPsec VPN tunnel (Kerio Control and another device)

IPsec tunnel overview

You can create a secure tunnel between two LANs secured by a firewall.

This article describes creating a IPsec VPN tunnel between Kerio Control and another device.

Before you start, read article: [Configuring IPsec VPN tunnel](#) which describes Kerio Control settings.

Default values in Kerio Control

This section includes default and supported values for IPsec implemented in Kerio Control.

Both endpoints should be able to communicate automatically. If a problem occurs and you have to set the values manually, consult the following tables for default and supported values in Kerio Control.

The default values are used by Kerio Control. Remote endpoints of the tunnel can also use the supported values.

Phase 1 (IKE):

	Default values (in bold), supported values	Unsupported values
mode	main	aggressive
remote ID type	hostname , IP address	
NAT traversal	enabled	
ciphersuite (policies)	aes128-sha1-modp2048 , 3des-sha1-modp1536 , see the list of Supported ciphers	
version	IKEv1	IKEv2
DPD timeouts	enabled (150 sec)	
lifetime	3 hours	

Table 1 Phase 1 (IKE)

Phase 2 (ESP):

	Default values (in bold), supported values	Unsupported values
mode	tunnel	transport
protocol	ESP	AH
ciphersuite (policies)	aes128-sha1,3des-sha1 , see the list of Supported ciphers	
PFS	off	
lifetime	60 mins	

Table 2 Phase 2 (ESP)

Supported ciphers

Each cipher consists of three parts:

- Encryption Algorithm — aes128
- Integrity Algorithm — sha1
- Diffie Hellman Groups — modp2048

Kerio Control supports the following ciphers:

Phase 1 (IKE) - supported ciphers

Encryption Algorithms	Integrity Algorithms	Diffie Hellman Groups
aes128 or aes (128 bit AES-CBC)	md5 (MD5 HMAC)	2 (modp1024)
aes192 (192 bit AES-CBC)	sha1 or sha (SHA1 HMAC)	5 (modp1536)
aes256 (256 bit AES-CBC)	sha2_256 or sha256 (SHA2_256_128 HMAC)	14 (modp2048)
3des (168 bit 3DES-EDE-CBC)	sha2_384 or sha384 (SHA2_384_192 HMAC)	15 (modp3072)
	sha2_512 or sha512 (SHA2_512_256 HMAC)	16 (modp4096)
		18 (modp8192)
		22 (modp1024s160)
		23 (modp2048s224)
		24 (modp2048s256)

Table 3 Phase 1 (IKE) - supported ciphers

Phase 2 (ESP) - supported ciphers

Configuring IPsec VPN tunnel (Kerio Control and another device)

Encryption Algorithms	Integrity Algorithms	Diffie Hellman Groups
aes128 or aes (128 bit AES-CBC)	md5 (MD5 HMAC)	none (no PFS)
aes192 (192 bit AES-CBC)	sha1 or sha (SHA1 HMAC)	
aes256 (256 bit AES-CBC)	aesxcbc (AES XCBC)	
3des (168 bit 3DES-EDE-CBC)		
blowfish256 (256 bit Blowfish-CBC)		

Table 4 Phase 2 (ESP) - supported ciphers

Configuring traffic rules

How traffic rules work



Watch the [Configuring traffic rules](#) video.

The traffic policy consists of rules ordered by their priority. The rules 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.



To control user connections to WWW or FTP servers and filter contents, use the content filter available in Kerio Control for these purposes rather than traffic rules. Read more in the [Configuring the Content Filter](#) article.

Configuring traffic rules

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

To create your own rules, look at the following examples:

Configuring traffic rules

The screenshot shows the 'Traffic Rules' administration window. It features a search bar at the top, a 'Test Rules' button, and a 'Restore View' button. A table lists various rules with columns for Name, Source, Destination, Service, IP version, Action, Translation, and Last used. The rules are color-coded: red for inbound rules and green for outbound rules. Annotations highlight key features: a search bar for finding rules, a 'Test Rules' button for verification, a 'Last used' column for connection timing, a red highlight for inbound rules, a green highlight for outbound rules, a checkbox for enabling/disabling rules, and a default rule denying all traffic.

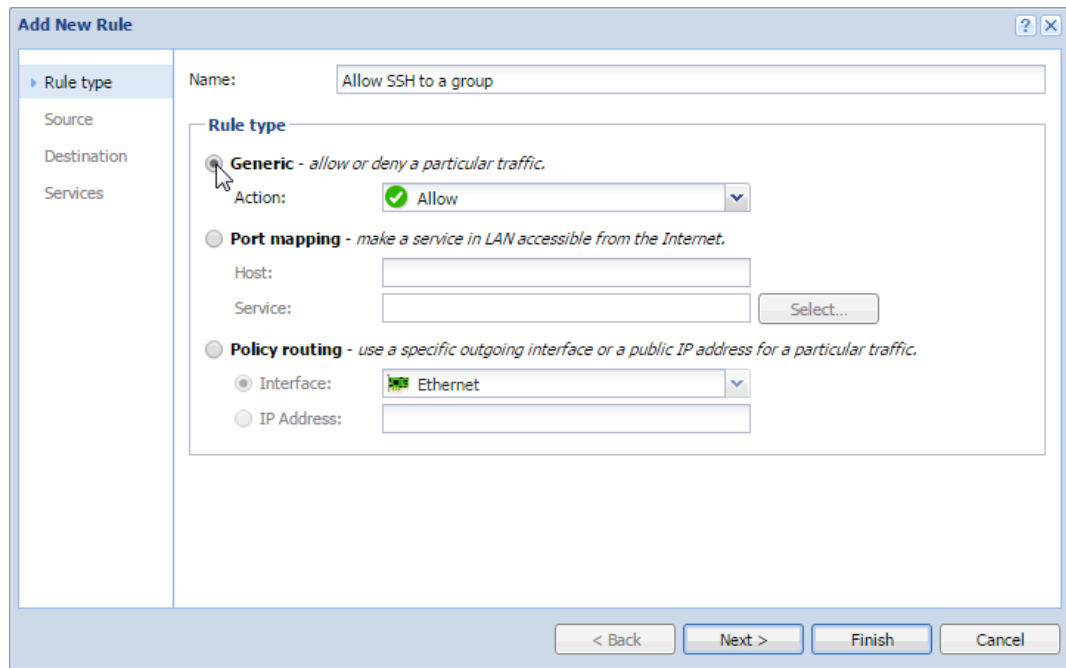
Name	Source	Destination	Service	IP version	Action	Translation	Last used
Trusted/Local Interface...	Internet Interfaces	HTTP	Any	Allow	NAT Balancing per host		
Trusted/Local Interface...	Internet Interfaces	Any	Any	Allow	NAT Balancing per host		
Guest Interfaces							
VPN clients							
asmith							
VPN Services	Any	Firewall	IPsec ser...	Any	Allow		
Web Services	Any	Firewall	HTTP	Any	Allow		
Local traffic	Firewall	Firewall	Any	Any	Allow	just now	
Firewall traffic	Firewall	Any	Any	Any	Allow	just now	
Guests traffic	Guest Interfaces	Firewall	Guest se...	Any	Allow	just now	
Block other traffic	Any	Any	Any	Any	Drop	just now	

Figure 1 Basic traffic rules configured by Wizard

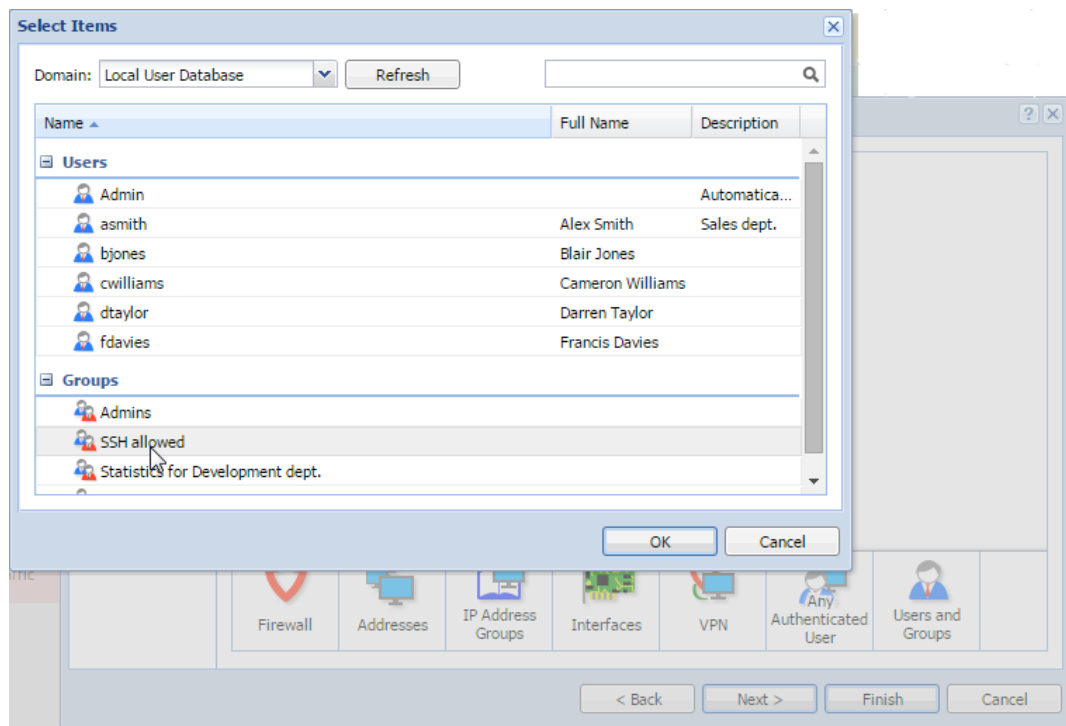
Generic rule

In the default state, Kerio Control denies communication for all services. To create an allowing rule for a service, for example, to allow a user group to use SSH for access to servers in the Internet:

1. Go to **Traffic Rules** in the administration interface.
2. Click **Add**.
3. In the **Add New Rule** dialog box, type a name for the rule (for example, Allow SSH to a group).
4. As a rule type, select **Generic**.



5. Click **Next**.
6. Click **Users and Groups**.
7. In the **Select Items** dialog box, double-click a group (**SSH allowed** in our case).



Configuring traffic rules

8. Click **Next**.
9. Select **Interfaces**.
10. In the **Select Items** dialog box, select **Internet Interfaces**.
11. Click **Next**.
12. Click **Services**.
13. In the **Select Items** dialog box, double-click **SSH**.

The rule allows your users to use SSH to access servers in the Internet.

<input checked="" type="checkbox"/> Allow SSH to a group	SSH allowed	Internet Interfaces	SSH	Any	Allow		
Block other traffic	Any	Any	Any	Any	Drop		just now

Port mapping

To enable all services for Kerio Connect placed in your local network protected by Kerio Control, follow these step:

1. In the administration interface, go to **Traffic Rules**.
2. Click **Add**.
3. In the **Add New Rule** wizard, type a name of the rule.
4. Select **Port mapping**.
5. In the **Host** field, type the hostname or IP address of the SMTP server placed in your local network.
6. Next to the **Service** field, click **Select**.
7. In the **Select Items** dialog, check the **Kerio Connect services** group (see figure [2](#)).
8. Click **Finish**.
9. Move the rule to the top of the table of traffic rules.

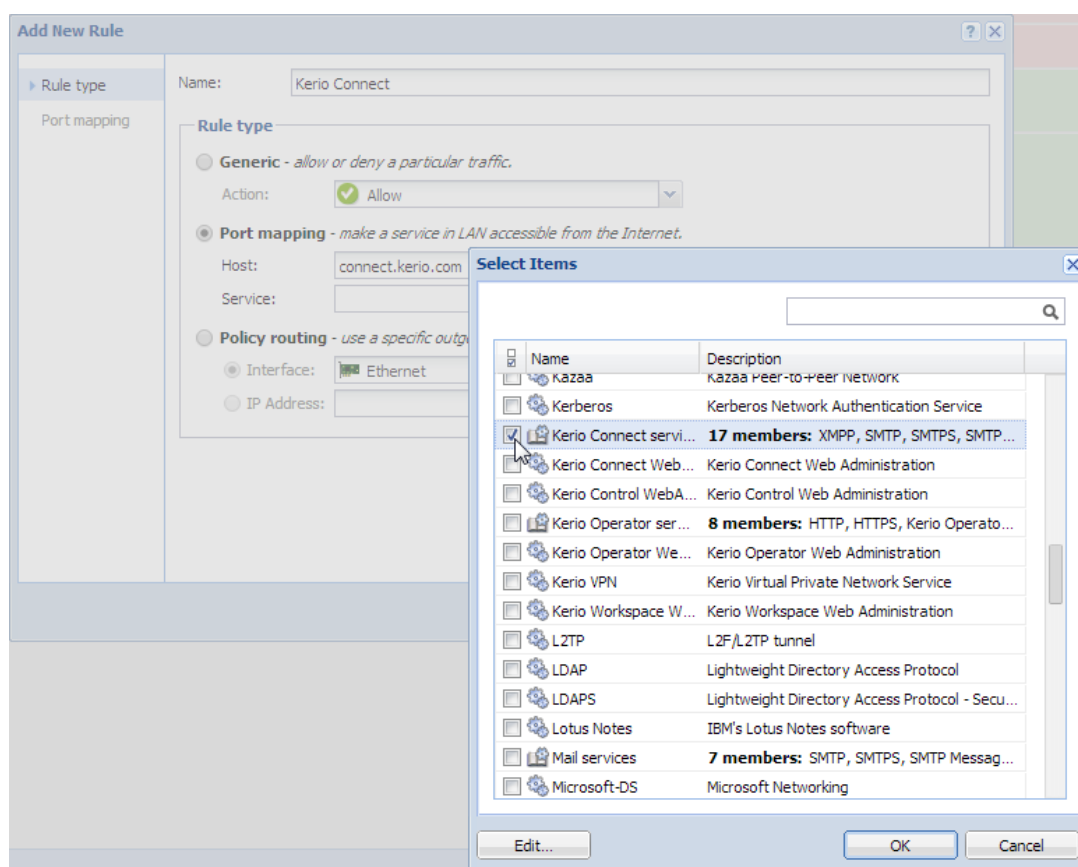


Figure 2 Adding a service group

Other examples

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

User accounts and groups in traffic rules

In traffic rules, source/destination can be specified also by user accounts and/or 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):

Configuring traffic rules

Enabling certain users to access the Internet

In a private network and with the Internet connection performed through NAT, you can specify which users can access the Internet in the **Source** item in the NAT rule.

Name	Source	Destination	Service	IP version	Action	Translation
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients asmith	Internet Interfaces	Any	Any	Allow	NAT Balancing per host

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

Such rules enable the specified users to connect to the Internet if they authenticate. They need to open the Kerio Control interface's login page manually and authenticate.



With the rule defined, all methods of automatic authentication are ineffective (i.e. redirecting to the login page, NTLM authentication and automatic authentication from defined hosts).

Automatic authentication (redirection to the login page) is performed when the connection to the Internet is established. This NAT rule blocks any connection unless the user is authenticated.

Enabling automatic authentication

The automatic user authentication issue can be solved as follows:

1. Add a rule allowing an unlimited access to the HTTP service and place it before the NAT rule.

Traffic Rules							Admin ▾
Search: <input type="text"/>							Test Rules Restore View
Name	Source	Destination	Service	IP version	Action	Translation	
<input checked="" type="checkbox"/> WWW without authentica...	Trusted/Local Interfaces	Internet Interfaces	HTTP	Any	Allow	NAT Balancing per host	
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients asmith	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	

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

2. In [Content Rules](#), allow specific users to access any web site and deny any access to other users.

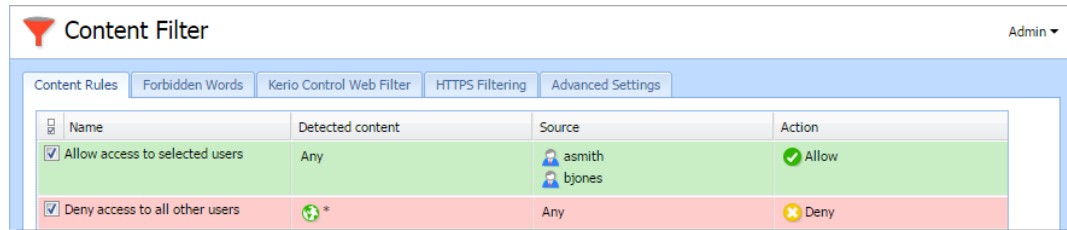


Figure 5 These URL rules enable specified users to access any Web site

Users who are not yet authenticated and attempt to open a web site are 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 other Internet services. Users not specified in the rules will be disallowed to access any web site or/and other Internet services.



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 the client stations use a DNS server in the Internet, you must 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](#).

Enabling protocol inspection on traffic rules

Kerio Control includes protocol inspectors that monitor all traffic on application protocols, such as HTTP, FTP. The inspectors filter the communication or adapt the firewall's behavior according to the protocol type. For more details, read [Protocol inspection in Kerio Control](#).

1. In the administration interface, go to **Traffic Rules**.
2. Right-click a table header and select **Columns** → **Inspector**.
3. In a particular rule, double-click the **Inspector** column and select the appropriate protocol inspector.

Configuring traffic rules



Each inspector should be used for the appropriate service only. Functionality of the service might be affected by using an inappropriate inspector.

4. Click **Apply**.

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

Traffic Rules Admin ▾							
Search: <input type="text"/> Test Rules Restore View							
<input type="checkbox"/>	Name	Source	Destination	Service	IP version	Action	Translation
<input checked="" type="checkbox"/>	Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	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**.

Interfaces are described in the [Configuring network interfaces](#) article.



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 (see the [Configuring a routing table in Kerio Control](#) article).

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	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> Firewall traffic	 Firewall	Any	Any	Any	 Allow		just now

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

Configuring traffic rules - multihoming

Multihoming overview

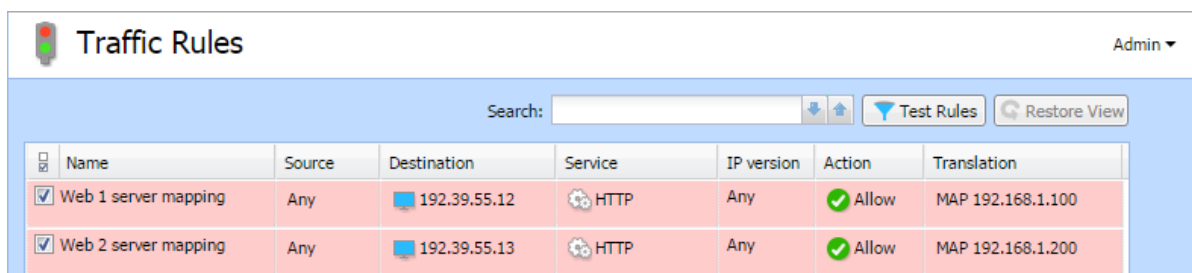
Multihoming is a term used for situations when one network interface connected to the Internet uses multiple public IP addresses. Typically, multiple services are available through individual IP addresses (this implies that the services are mutually independent).

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:



<input type="checkbox"/>	Name	Source	Destination	Service	IP version	Action	Translation
<input checked="" type="checkbox"/>	Web 1 server mapping	Any	192.39.55.12	HTTP	Any	Allow	MAP 192.168.1.100
<input checked="" type="checkbox"/>	Web 2 server mapping	Any	192.39.55.13	HTTP	Any	Allow	MAP 192.168.1.200

However, you must add the public IP addresses to the interface first.

Adding IP addresses to an interface

To add the public IP addresses to the interface settings:

1. In the administration interface, go to **Interfaces**.
2. Select an interface and click **Edit**.
3. Click **Define Additional IP Addresses**.
4. In the **Additional IP Addresses** dialog box, click **Add**.
5. Type the IP address and the mask.
Add as many addresses as you need.

Configuring traffic rules - multihoming

6. Save all the dialogs.
7. Click **Apply**.

Configuring traffic rules for multihoming

1. In the administration interface, go to **Traffic Rules**.
2. Click **Add**.
3. In the **Add New Rule** dialog, type a name for the rule (in our example: Web1 server mapping) and click **Next**.

The screenshot shows the 'Add New Rule' dialog box. On the left, there is a sidebar with 'Rule type' selected. The main area has a 'Name' field with the text 'Web 1 server mapping'. Below this, the 'Rule type' section contains three radio buttons: 'Generic' (selected), 'Port mapping', and 'Policy routing'. The 'Generic' option has an 'Action' dropdown set to 'Allow'. The 'Port mapping' option has 'Host' and 'Service' fields, with a 'Select...' button next to the 'Service' field. The 'Policy routing' option has an 'Interface' dropdown set to 'Ethernet' and an 'IP Address' field. At the bottom, there are four buttons: '< Back', 'Next >' (highlighted with a mouse cursor), 'Finish', and 'Cancel'.

4. In the **Source** section, leave **Any sources** and click **Next**.
5. In the **Destination** section, click **Addresses**.
The IP address of the interface connected to the Internet must be added
6. Add the IP address of the interface connected to the Internet.
Our example: 195.39.55.12.
7. Click **Next**.
8. In the **Service** section, select **HTTP**.
9. Click **Finish**.

10. In the `Web1 server mapping` rule, double-click in the column **Translation**.
11. In the **Traffic Rule - Translation** dialog, select the **Enable destination NAT** option and type the IP address of the corresponding Web server (`web1`) to the **Translate to the following host** field.
12. Repeat steps 1-8 for Web2 server.

Limiting Internet access with traffic rules

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 the [Configuring IP address translation](#) 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	IP version	Action	Translation	Last used
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients asmith	Internet Interfaces	CardDAV DNS FTP FTPS HTTP HTTPS SSH	Any	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	IP version	Action	Translation	Last used
Internet access (NAT)	Internet access	Internet Interfaces	Any	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	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> Internet access (NAT)	Internet access	Internet Interfaces	Any	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	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> Internet access (NAT)	Authenticated users	Internet Interfaces	Any	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](#).

Troubleshooting traffic rules

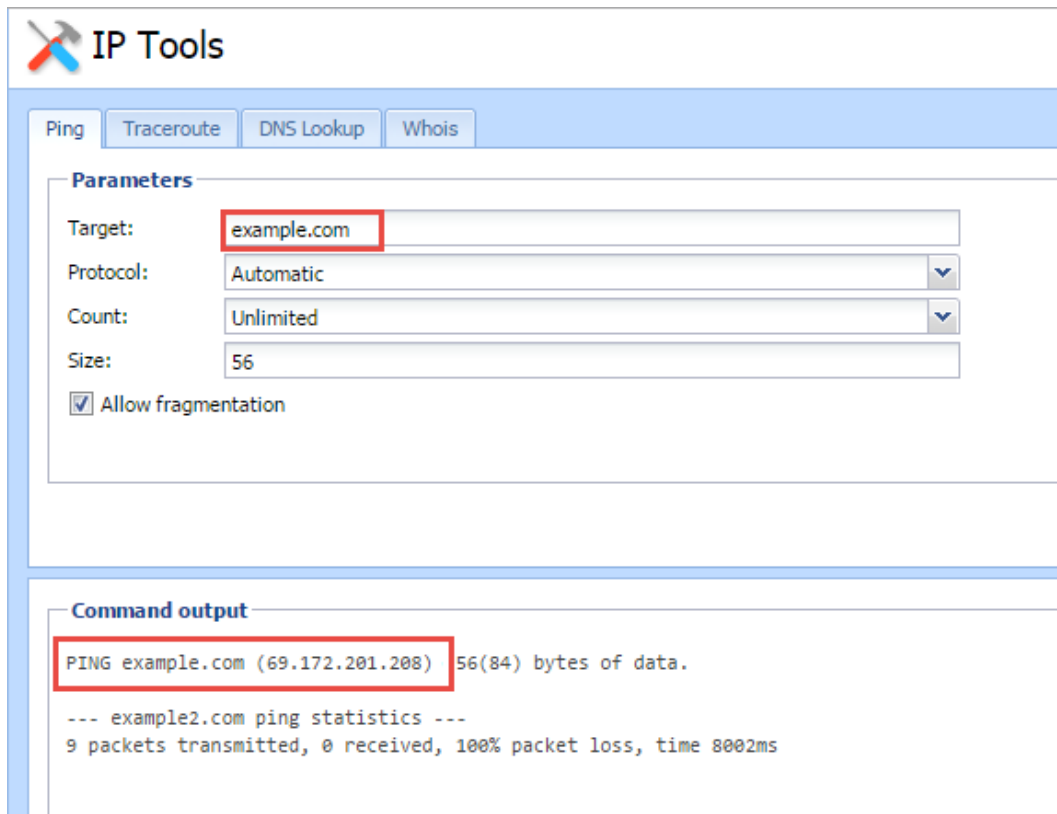
Overview

If a particular communication is broken (for example, your users cannot access the server example.com), your traffic rules may be blocking the communication. This article describes how to find packets dropped by a traffic rule and how to determine the traffic rule causing the problem.

Detecting IP addresses

Before you start, you must find out the IP address of dropped packets. You can use, for example, the **Ping** tool in Kerio Control:

1. In the administration interface, go to **Status** → **IP Tools**.
2. On the **Ping** tab, type the name of the server you cannot reach (example.com).
3. Click **Start**.
4. After a few seconds, type **Stop**.
5. If the server name has a DNS record, you can see the IP address of the server in the **Command output** section.



Now you have two options for discovering the traffic rule blocking the server:

- Look for dropped packets in the **Debug** log.
- Test the rules in the **Traffic Rules** section.

Looking for dropped packets

Once you know the IP address, switch to the **Debug** log:

1. In the administration interface, go to **Logs** → **Debug**.
2. Right-click the **Debug** window.
3. In the context menu, click **Messages**.
4. In the **Filtering** section, select **Packets dropped for some reason**.
5. In the **Debug** log, find the dropped packets using the IP address of the server.

Example:

```
[22/Dec/2015 15:32:40] {pktdrop} packet dropped:
Traffic rule: Example traffic rule (to WAN, proto:ICMP, len:84,
212.212.62.103 -> 69.172.201.208, type:8 code:0 id:12380 seq:1 ttl:64)
```

This tells you the following:

Troubleshooting traffic rules

[22/Dec/2015 15:32:40]	Date and time of the dropped packet
{pktdrop}	All packets caught by the Packets dropped for some reason message
packet dropped: Traffic rule: Example traffic rule	Reason Kerio Control dropped the packet: The cause is Traffic rule and Kerio Control adds the name of the rule
212.212.62.103 -> 69.172.201.208	Source and target IP addresses

Testing traffic rules

The **Test Rules** feature shows all rules that match a particular packet description.

1. In the administration interface, go to **Traffic Rules**.
2. Click the **Test Rules** button.
3. Type the source IP address of your firewall (212.212.62.103 in the example).
4. Type the destination IP address of the server you cannot access (69.172.201.208 in the example).

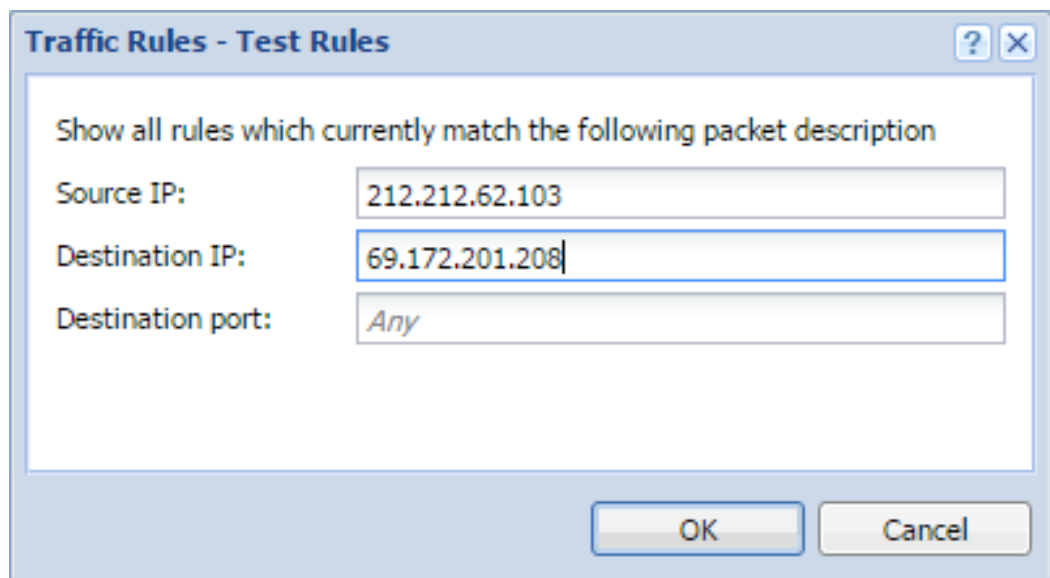
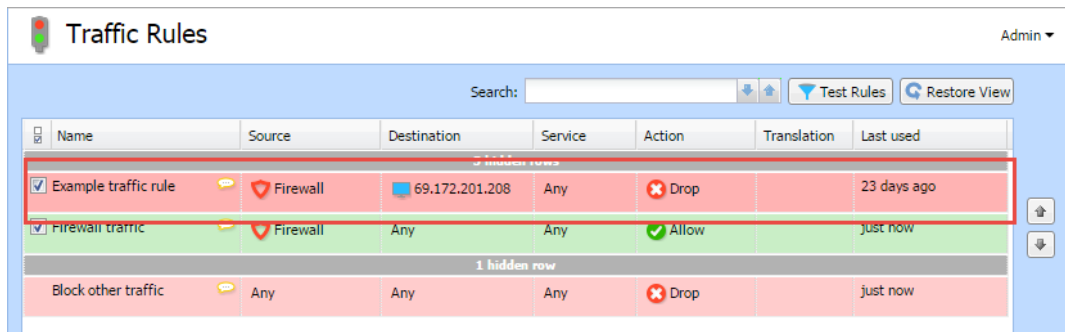
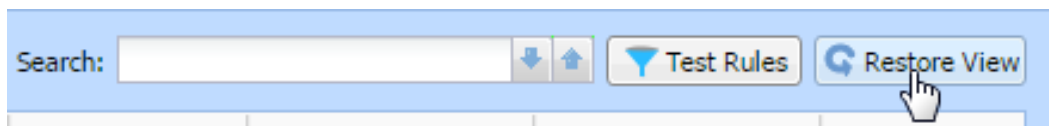


Figure 1 The Test rules dialog

5. Click **OK**.
6. The traffic rules list displays only rules matching the packet description. You can identify the corrupt rule and fix it.



7. After fixing the rule, click the **Restore View** button.



Now, you can again see all traffic rules.

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).

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

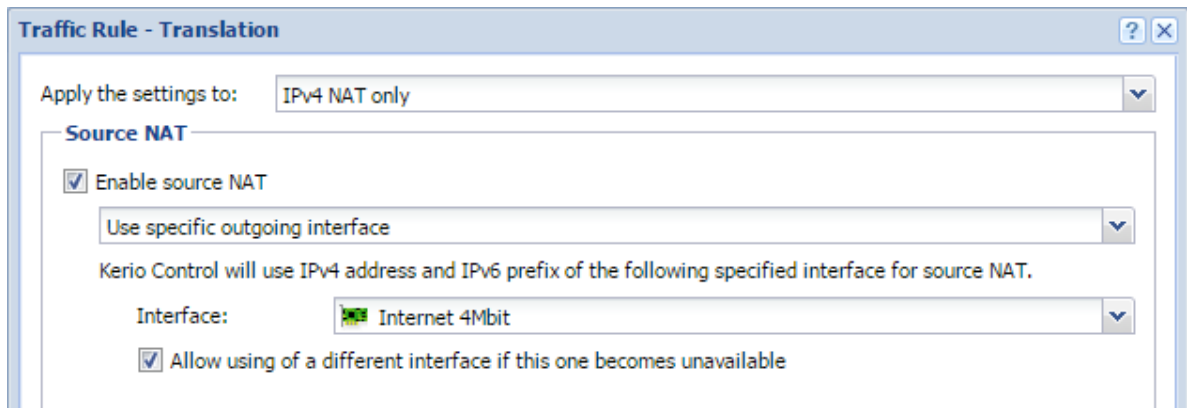
The firewall is connected to the Internet by two links with load balancing with speed values of 4 Mbit/s and 8 Mbit/s. One of the links is connected to the provider where the mailserver is also hosted. Therefore, all email traffic (SMTP, IMAP and POP3) is routed through this link.

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.

Name	Source	Destination	Service	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> NAT - preferred link for email	Trusted/Local Interfaces	Internet Interfaces	Kerio Connect services	Any	<input checked="" type="checkbox"/> Allow	NAT (Internet 4Mbit)	
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	<input checked="" type="checkbox"/> Allow	NAT Balancing per host	

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



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.

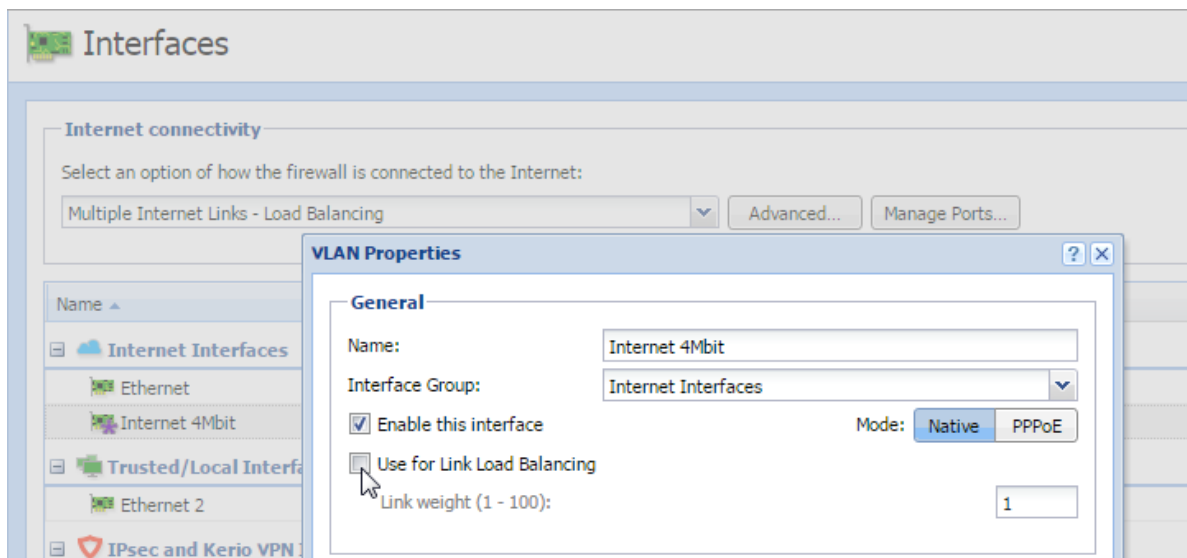


Figure 1 Interfaces — Uncheck the Use for Link Load Balancing option

Configuring an optimization of network traffic load balancing

Kerio Control provides two options of network traffic load balancing:

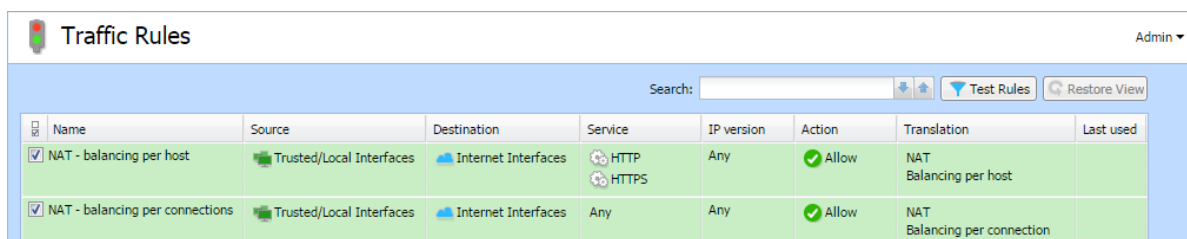
- per host (clients)
- per connection

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	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/>	NAT - balancing per host	Trusted/Local Interfaces	Internet Interfaces	HTTP HTTPS	Any	Allow	NAT Balancing per host	
<input checked="" type="checkbox"/>	NAT - balancing per connections	Trusted/Local Interfaces	Internet Interfaces	Any	Any	Allow	NAT Balancing per connection	

Figure 2 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 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](#) for IPv4.
- Intrusion detection is performed before the [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 of a malicious intrusion attempt is very high (e.g. Trojan horse network activity).
- **Medium severity** — Activity which is considered as suspicious (for example, traffic by a non-standard protocol on the standard port of another protocol).
- **Low severity** — Network activity which does not indicate immediate security threat (for example, port scanning).

Configuring intrusion prevention system

4. Click the **On the Kerio website, you can test these settings** link to test the intrusion prevention system for both IPv4 and IPv6.

During the test, three fake harmless intrusions of high, middle, and low severity are sent to the IP address of your firewall.

5. Click **Apply**.

The Security log will report when the firewall identifies and blocks an intrusion.

Configuring ignored intrusions

In some cases, legitimate traffic may be detected as an intrusion. If this happens, 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.
8. Click **OK** and **Apply**.

The legitimate traffic is 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 and uses any of the listed protocols on a non-standard port (for example, HTTP on port 10000), add this port to list of ports on which protocol-specific intrusions are 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 add the port (10000 in our example).
5. Click **OK** and **Apply**.

The service running on the non-standard port is now protected by the protocol-specific intrusions.

IP blacklists

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 the individual intrusion types. However, there are also disadvantages. Blacklists cannot include IP addresses of all possible intruders. Blacklists may also 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, 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 the **MAC Filter** tab, select **Enable MAC Filter**.
3. Select the network interface where the MAC filter will be applied (usually LAN).
4. Select the filter mode:
 - **Prevent listed computers from accessing the network** — The filter blocks only MAC addresses included in the list.
This mode can be used to block known MAC addresses, but does not filter traffic of new, unknown devices.
 - **Permit only listed computers to access the network** — The filter allows only MAC addresses included in the list, any other address is blocked.
Select the **Also permit MAC addresses used in DHCP reservations or automatic user login** option if you use [automatic user login](#) and [DHCP reservation by MAC](#). MAC addresses allowed by automatic user login and DHCP reservations are not visible in the MAC addresses list (see below).
5. Add MAC addresses to the list.

You can use the following separator in the MAC addresses:

- colons (e.g.: a0:de:bf:33:ce:12)
- dashes (e.g.: a0-de-bf-33-ce-12)
- no separators (a0debf33ce12)

6. Double check that listed addresses are correct.
7. Click **Apply**.

Your filter is fully configured and active.

Support for IPv6 protocol

Support for IPv6 protocol

- [IPv6 prefix delegation](#),
- [Configuring IPv6 parameters on network interfaces](#),
- Routing between individual interfaces and [IPv6 routing table](#),
- Kerio Web Filter,
- Antivirus on HTTP connections,
- Content filter on HTTP connections,
- [Stateless address auto-configuration of hosts and devices in the LAN \(SLAAC\)](#),
- Basic firewall with configuration options ([IPv6 filtering](#)),
- 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,
- Monitoring IP traffic in Kerio Control statistics,
- IP address groups,
- [Traffic Rules](#),
- Intrusion and prevention system (IPS),
- IP tools,
- MAC filter,
- Overview of an active host activities (only the port-based activities are recognized, such as Remote access, Instant messaging, Mail, Web pages, Streams),
- Configuration backup to [Samepage.io](#) or an FTP server,

- Reverse proxy,
- Kerio Control applies [host connection limits](#) to IPv6.

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

IPv6 filtering

Kerio Control supports allowing 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.

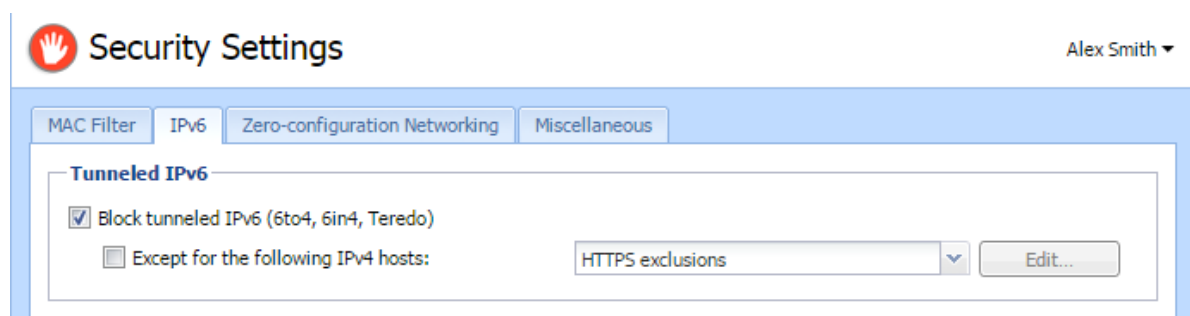
For security reasons, any incoming native and tunneled IPv6 traffic is disabled by default.

Allowing IPv6 for particular computers or prefixes

To allow incoming traffic through IPv6 protocol from the particular prefix or computer:

1. In the administration interface, go to **Traffic Rules**.
2. Prepare rules for incoming and outgoing traffic. Read more in the [Configuring traffic rules for IPv6 network](#) article.
3. Click **Apply**.

Blocking IPv6 tunneling



Support for IPv6 protocol

1. In the administration interface, go to **Security Settings** → **IPv6**.
2. Select option **Block tunneled IPv6 (6to4, 6in4, Teredo)**.
3. (Optional) 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.
6. Click **Apply**.

Configuring IPv6 networking in Kerio Control

Overview



New in Kerio Control 8.6!

To run the IPv6 network in Kerio Control:

- Enable IPv6 on WAN interfaces (IPv6 prefix delegation)
- Enable IPv6 on local interfaces
- Enable router advertisements

To see all the Kerio Control IPv6 features, see [Support for IPv6 protocol](#).



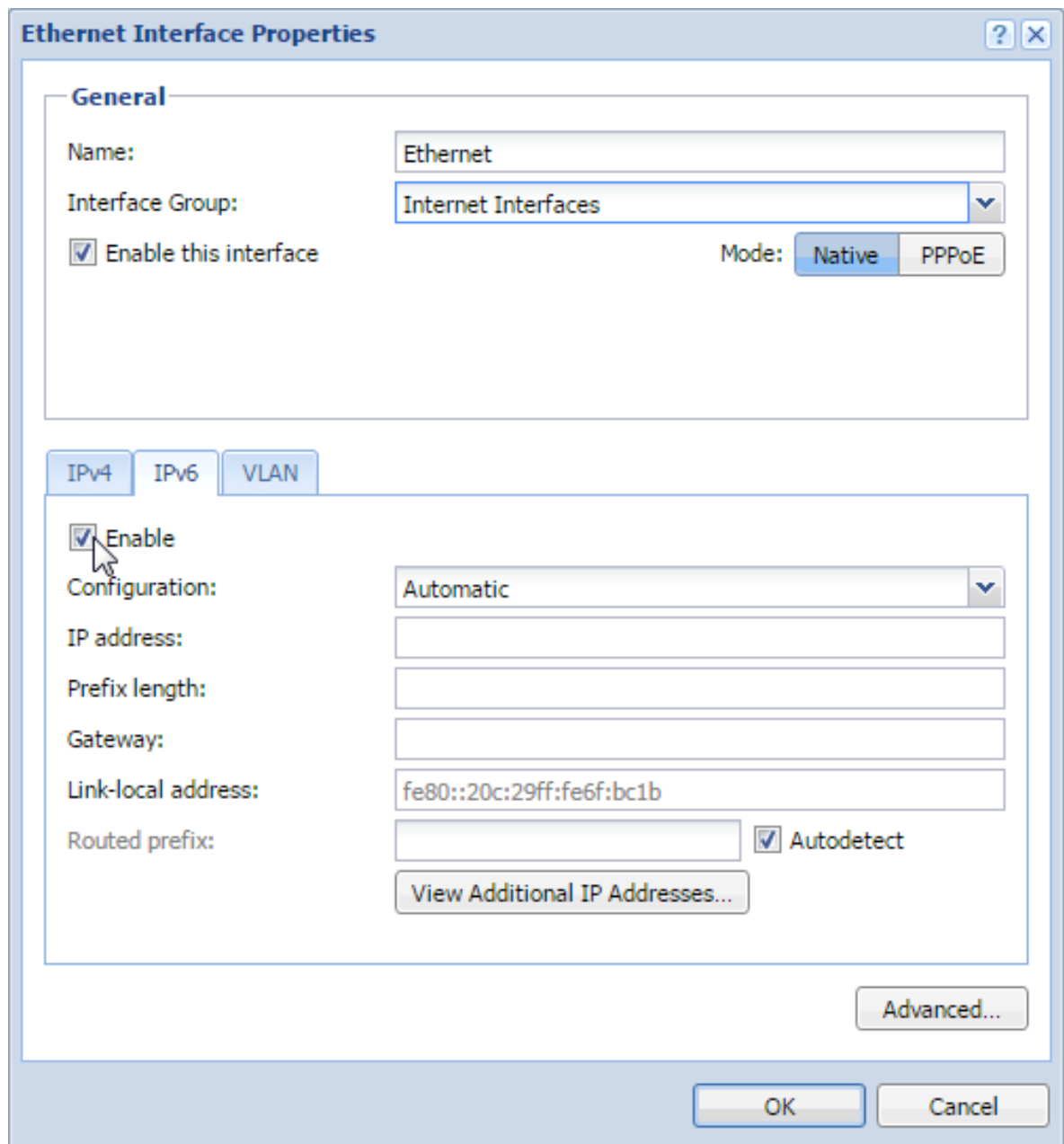
Kerio Control does not support DNS on IPv6, so you also need the IPv4 network.

Obtaining an IPv6 prefix from your ISP

Kerio Control supports the IPv6 prefix delegation. Your ISP assigns you an IPv6 prefix and you must enable it on a network interface in Kerio Control. Kerio Control then becomes a DHCPv6 client and obtains the prefix from your ISP.

If you get the IPv6 prefix from your ISP and your ISP uses a DHCPv6 server:

1. In the administration interface, go to **Interfaces**.
2. Double-click the Internet interface where you want to run IPv6.
3. In the **Interface Properties** dialog box, go to the **IPv6** tab.
4. Select **Enable**.
Autodetection of the routed prefix is selected by default.
5. Save your settings.



From now on, Kerio Control behaves as a DHCPv6 client and automatically obtains the routed prefix from your ISP. Kerio Control automatically records the routed prefix in the IPv6 router advertisements table and the IPv6 routing table.

Running IPv6 in the Kerio Control network

To run IPv6 in your local network, you must enable IPv6 on your local interfaces:

1. In the administration interface, go to **Interfaces**.
2. Double-click an interface in **Trusted/Local Interfaces**, **Guest Interfaces**, or **Other Inter-**

faces.

3. Go to the **IPv6** tab.
4. Select **Enable**.
5. Click **Apply**.

IPv6 now runs on the selected interface in the Kerio Control network.

Enabling the IPv6 router advertisements

Kerio Control uses the IPv6 router advertisements for stateless auto-configuration of IPv6 devices in the LAN (SLAAC). Kerio Control adds a record for every network in which it advertises as a default router.

1. In the administration interface, go to **IPv6 Router Advertisements**.
2. Enable the **Enable IPv6 Router Advertisements** option.
3. Click **Apply**.

All IPv6 devices now get the IPv6 address.

Manual configuration

Kerio Control generates advertisements automatically. However, if you need to make some changes, you can do it manually:

1. In the administration interface, go to **IPv6 Router Advertisements**
2. Click the link **Click to configure manually**.
3. Click **Add**.
4. Select an interface connected to the network where the router should advertise.
5. Double-click in the **Prefix** column and type the IPv6 prefix (subnet address).
6. Double-click in the **Prefix length** column and type the number of bits of IPv6 address that defines the prefix.
7. Click **Apply**.

Configuring Service Discovery forwarding in the Kerio Control network

Service Discovery forwarding overview



New in Kerio Control 8.5!

Kerio Control forwards [Service Discovery protocols](#) between networks. This allows remote users across VPN tunnels or other networks to locate and reach devices (printers, Apple TV, and so on) that host services behind the firewall.

If you have more Kerio Controls connected through the Kerio VPN tunnel, all Kerio Controls must have enabled Service Discovery forwarding. Also, all network devices in your network (switches, routers, and modems) must support multicast forwarding.

Examples of Service Discovery protocols include:

- mDNS, which is used by Apple Bonjour for locating Apple services, or devices such as printers (Bonjour Gateway)
- NetBIOS Name service, which is used to identify Microsoft Windows workstations, servers, and services
- SSDP, which is used by devices and applications supporting UPnP



Kerio Control supports Service Discovery forwarding only for Kerio VPN. IPsec VPN is not supported.

Configuring Service Discovery forwarding

To enable Service Discovery forwarding and to select subnets:

1. In the administration interface, go to **Security Settings** → **Zero-configuration Networking**.
2. Select **Enable Service Discovery forwarding**.
3. Select the interfaces (subnets) for which you want to enable Service Discovery forwarding.
4. Click **Apply**.

Kerio Control makes zero-configuration devices accessible in the selected interfaces.

Troubleshooting

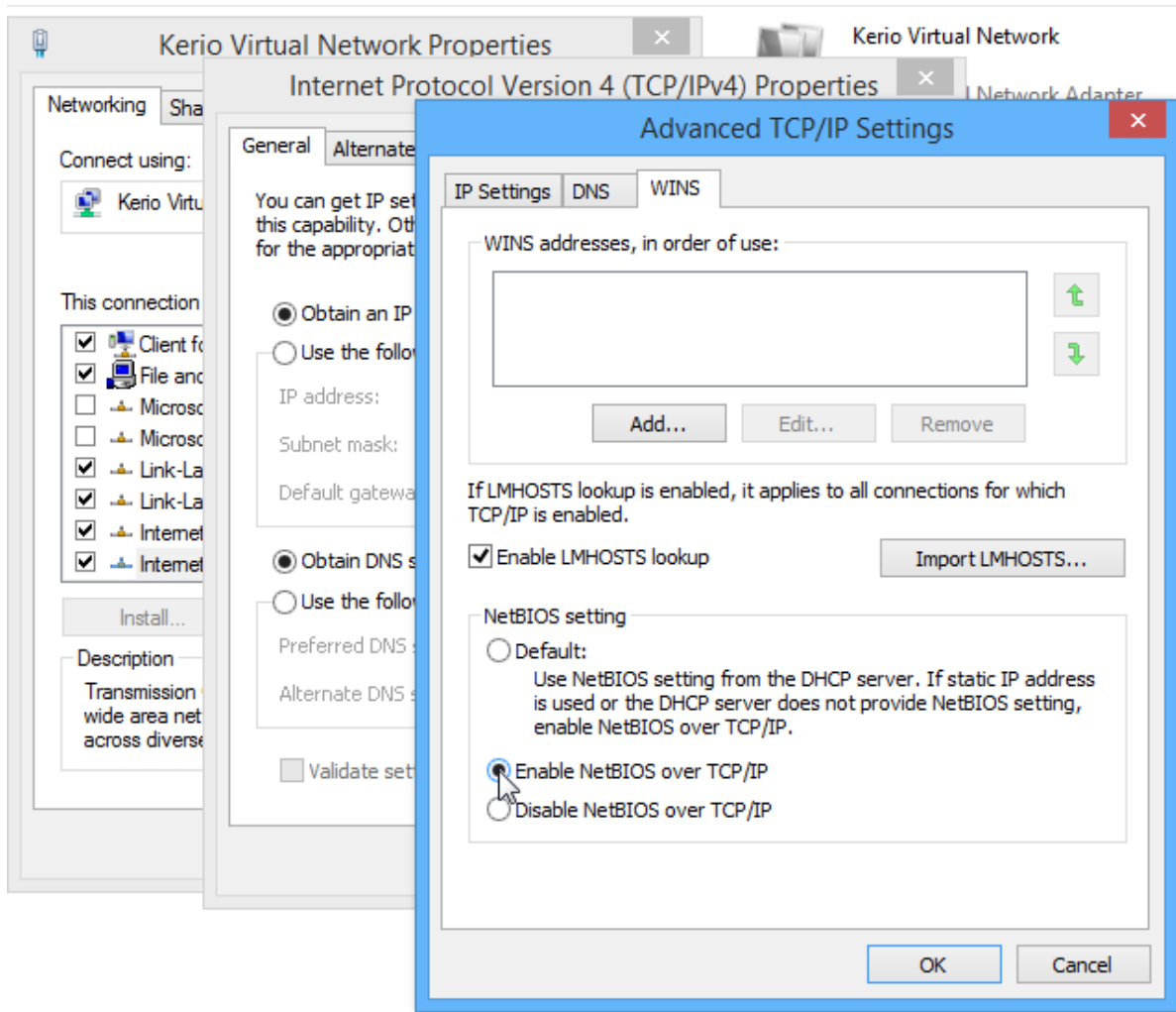
If you have trouble with Service Discovery forwarding, verify that the firewall is set properly on the client computers.

In Windows Firewall, we recommend creating inbound and outbound rules to allow traffic on ports 137 and 138 for any remote interface even if you disable Windows Firewall.

If you use Kerio Control VPN Client, the NetBIOS interface is disabled by default. To enable NetBIOS:

1. In your network connections, right-click **Kerio Virtual Network** and click **Properties**.
2. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
3. Click **Advanced**.
4. On the **WINS** tab, select option **Enable NetBIOS over TCP/IP**.
5. Save your settings.

Configuring Service Discovery forwarding in the Kerio Control network



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

1. In the administration interface, go to **Security Settings** → **Zero-configuration Networking**
2. Click **Enable UPnP service**.
3. If you want to log all packets passing through ports mapped with UPnP, click **Log packets**.
Kerio Control logs the communication to the **Filter** log.
4. If you want to log all connections, click **Log connections**
Kerio Control logs the communication to the **Connection** log.
5. Click **Apply**.

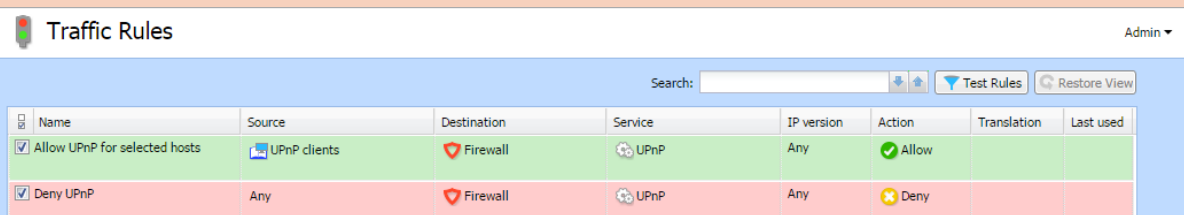
Configuring Universal Plug-and-Play (UPnP)



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	IP version	Action	Translation	Last used
<input checked="" type="checkbox"/> Allow UPnP for selected hosts	UPnP clients	Firewall	UPnP	Any	Allow		
<input checked="" type="checkbox"/> Deny UPnP	Any	Firewall	UPnP	Any	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 connection limits

Host connection limits in Kerio Control 9.0 and later

Overview

Limiting the number of TCP and UDP connections within your network helps protect your business against denial of service (DoS) attacks.

You can set connection limits based on:

- A source IP address (the host initiating the connection)
- A destination IP address (the host the connection is made to)

Kerio Control lets you create exceptions to change the limits or disable limits for specific address groups.

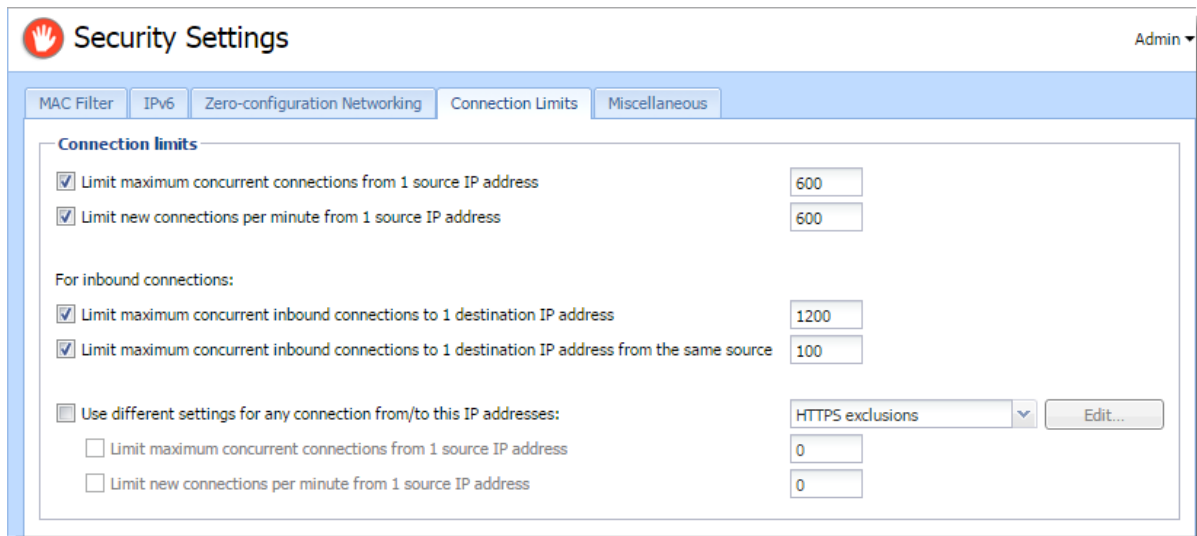
Kerio Control keeps track of the number of connections made from, or to, each [active host](#) in the network. It also blocks connections from malicious hosts.

Kerio Control connection limits apply to both IPv4 and IPv6 IP addresses.

The connection limits are enabled and set to the values shown here by default:

- Limit maximum concurrent connections from 1 source IP address: 600
- Limit new connections per minute from 1 source IP address: 600
- Limit maximum concurrent inbound connections to 1 destination IP address: 1200
- Limit maximum concurrent inbound connections to 1 destination IP address from the same source: 100

Configuring connection limits



The screenshot shows the 'Security Settings' window with the 'Connection Limits' tab selected. The 'Connection limits' section contains the following settings:

- ☒ Limit maximum concurrent connections from 1 source IP address: 600
- ☒ Limit new connections per minute from 1 source IP address: 600
- For inbound connections:
 - ☒ Limit maximum concurrent inbound connections to 1 destination IP address: 1200
 - ☒ Limit maximum concurrent inbound connections to 1 destination IP address from the same source: 100
- ☐ Use different settings for any connection from/to this IP addresses:
 - Dropdown menu: HTTPS exclusions
 - ☐ Limit maximum concurrent connections from 1 source IP address: 0
 - ☐ Limit new connections per minute from 1 source IP address: 0
 - Buttons: Edit...

After reaching the connection limit, Kerio Control breaks other connections to/from the host and creates an entry in the warning log.



Kerio Control can send system alerts to your email address if a host reaches a connection limit. Learn more in the [Using alert messages](#) article.

Changing default values

1. In the administration interface, go to **Security Settings** → **Connection Limits**.
2. Change the limits as needed.
3. Click **Apply**.



To return to the default state, click **Reset**.

Disabling connection limits

1. In the administration interface, go to **Security Settings** → **Connection Limits**
2. Clear all check boxes.
3. Click **Apply**.

Kerio Control disables host connection limits.

Excluding an IP address group from all connection limits

To remove connection limits for a specified group of IP addresses, add an exception:

1. In the administration interface, go to **Definitions → IP Address Groups**.
2. Add a new group with all the hosts for which you want different connection limits.
3. Go to **Security Settings → Connection Limits**.
4. Select **Use different settings for any connection from/to this IP address**.
5. Select the new IP address group from the drop-down list.
6. Click **Apply**.

Kerio Control excludes the IP address group from connection limits.

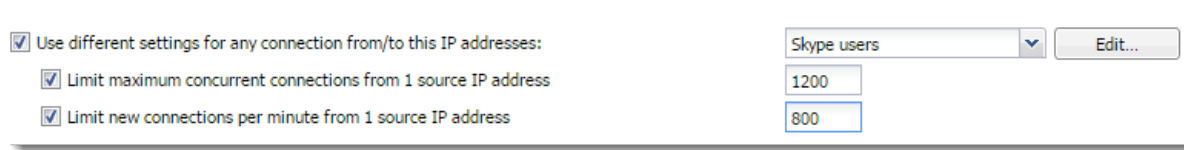
Setting different limits for specific IP address groups

To set different limits for any connection from/to a specific IP address group:

1. In the administration interface, go to **Definitions → IP Address Groups**.
2. Add a new group with all the hosts you want to exclude from counting connection limits.
3. Go to **Security Settings → Connection Limits**.
4. Select **Use different settings for any connection from/to this IP address**.
5. Select the new IP address group from the drop-down list.
6. Select **Limit maximum concurrent connections from 1 source IP address** and set a new limit.
7. Select **Limit new connections per minute from 1 source IP address** and set a new limit.
8. Click **Apply**.

Kerio Control changes the limits for the excluded IP addresses.

Configuring connection limits



The screenshot shows a configuration window with the following elements:

- A checked checkbox: "Use different settings for any connection from/to this IP addresses:"
- A dropdown menu set to "Skype users" with a downward arrow.
- An "Edit..." button.
- A checked checkbox: "Limit maximum concurrent connections from 1 source IP address" with a text input field containing "1200".
- A checked checkbox: "Limit new connections per minute from 1 source IP address" with a text input field containing "800".

Host connection limits in Kerio Control 8.6.2 and earlier

Overview

Kerio Control counts the number of connections for each [active host](#) and its peers in the Kerio Control network.



In this article:

- “Host” means any active host in Kerio Control.
- “Peer” means the computer communicating with any active host in the Kerio Control network.

Kerio Control blocks connections from infected hosts or peers. All connections to infected hosts and peers are allowed.

After reaching the connection limit, Kerio Control breaks other connections to/from the host and creates an entry in the warning log.



Kerio Control can send system alerts to your email address if a host reaches a connection limit. Learn more in the [Using alert messages](#) article.

Kerio Control applies connection limits to both IPv4 and IPv6 addresses.

The following connection limits are set by default:

- Single peer (to/from): 100 connections.
- All peers (to/from): 600 connections.
- All peers per minute (to/from): disabled.

Changing default values

1. In the administration interface, go to **Security Settings** → **Miscellaneous**.
2. Change the limits as needed.



Incoming and outgoing connections are counted separately.

3. Click **Apply**.

Security Settings

MAC Filter IPv6 Zero-configuration Networking **Miscellaneous**

Anti-spoofing

☒ Enable anti-spoofing

☒ Log

Connection limit

☒ Enable connection limit per host

For a single peer:

For all peers:

☐ New connections per minute:

☒ Apply different limits for:

For a single peer:

For all peers:

☐ New connections per minute:

Figure 1 Connection limits

Disabling connection limits

1. In the administration interface, go to **Security Settings** → **Miscellaneous**
2. Deselect **Enable connection limit per host**.
3. Click **Apply**.

Kerio Control disables host connection limits.

Excluding hosts from restrictions

If you have servers placed behind Kerio Control, you may need to increase or decrease their limits.

Specify exceptions using an IP address group:

1. In the administration interface, go to **Definitions** → **IP Address Groups**.
2. Add a new group with all the hosts you want to exclude from counting connection limits.

Configuring connection limits

3. Go to **Security Settings** → **Miscellaneous**.
4. Select **Apply different limits for**, and then select the new IP address group.
5. Set the limit for a single peer to **50**.
6. Set the limit for all peers to **1000**.
7. Click **Apply**.

Kerio Control excludes the hosts in the group from connection limits.

Configuring bandwidth management

Overview

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

How bandwidth management works

The bandwidth management feature provides two basic functions:

- **Limiting bandwidth for data transfers** is designed to reduce congestion caused by non-essential traffic (for example, large data transfers, video streaming, and so on).
- **Reserving bandwidth for specific services** reserves 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.

Internet links speed

For correct bandwidth management, you need to assign a link speed to each Internet interface. to ensure effective bandwidth management to be most effective, a conservative link speed estimate is best: approximately 80% of the actual speed.

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

Configuring bandwidth management

Suppose you want to restrict user John Smith to 50% of the link for download in all interfaces during his working hours:

1. In the administration interface, go to **Bandwidth Management and QoS**.
2. To create a new rule, click **Add**.
3. Type a name for the rule (John Smith).
4. Double-click **Traffic**.
5. In the **Traffic** dialog box, click **Users Groups**, select users or groups, and click save.
6. Double-click **Download**, check **Do not exceed**, and set the limit as shown here:

Configuring bandwidth management

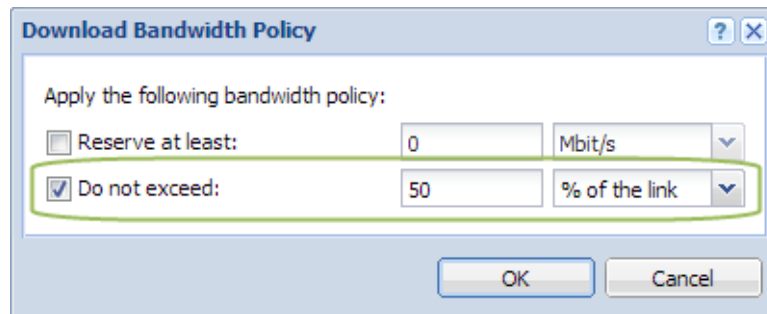


Figure 1 The Download Bandwidth Policy dialog

7. Leave **Upload** as it is (No limit).
8. Leave **Interface** 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. Select **Chart**.

The timeline for traffic matching the rule can be viewed under **Status** → **Traffic Charts** (for the previous 24 hours). The chart shows how much the particular traffic loads the link and helps you optimize bandwidth management rules. Local traffic is not counted.

11. Click **Apply** to save the new rule.



The order of rules is important. Rules are processed from the top down.

Bandwidth Management and QoS

Alex Smith ▾

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

	Name	Traffic	Download	Upload	Interface	Valid Time		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"/>	VPN	VPN	Reserve: 32 KB/s	Reserve: 32 KB/s	WAN 1		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Remote Access	Remote Ac...	Reserve: 20% ...	Reserve: 20% ...	WAN 2		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Alex Smith	alex	Reserve: 50% ...	No limit	All	Working hours	<input checked="" type="checkbox"/>	
	Other traffic	Any	No limit	No limit	All			

Figure 2 Bandwidth Management and QoS

Traffic types used in bandwidth management

You can apply limiting or reserving bandwidth to different types of traffic. You can select them in the **Traffic** column:

1. The **Applications and Web Categories** section requires the Kerio Control Web Filter license. For more information, read [Application awareness in Kerio Control](#) and [Using Kerio Control Web Filter](#).
2. The **Traffic Type** section includes predefined traffic types such as web, email, multimedia.
3. The **Large Data Transfers** section includes two parameters: volume of transferred data and duration of the longest idle interval. If the specified data volume is reached without the idleness interval having been thresholded, the connection is considered as a transfer of large data volume and corresponding limits.
4. The **QoS DSCP Value** can be set by using traffic rules, but it can be set by other routers on the way, the client or/and the server.

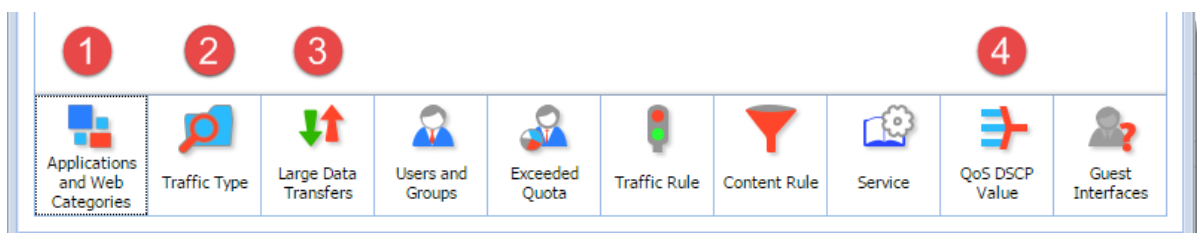


Figure 3 The Traffic dialog

Bandwidth management and VPN tunnels

When you are using bandwidth management and VPN tunnels at the same time, select **Use rules for VPN tunnels before encrypting**. Otherwise your VPN tunnel encrypts the communication, and bandwidth management rules are not applied.

Configuring bandwidth management

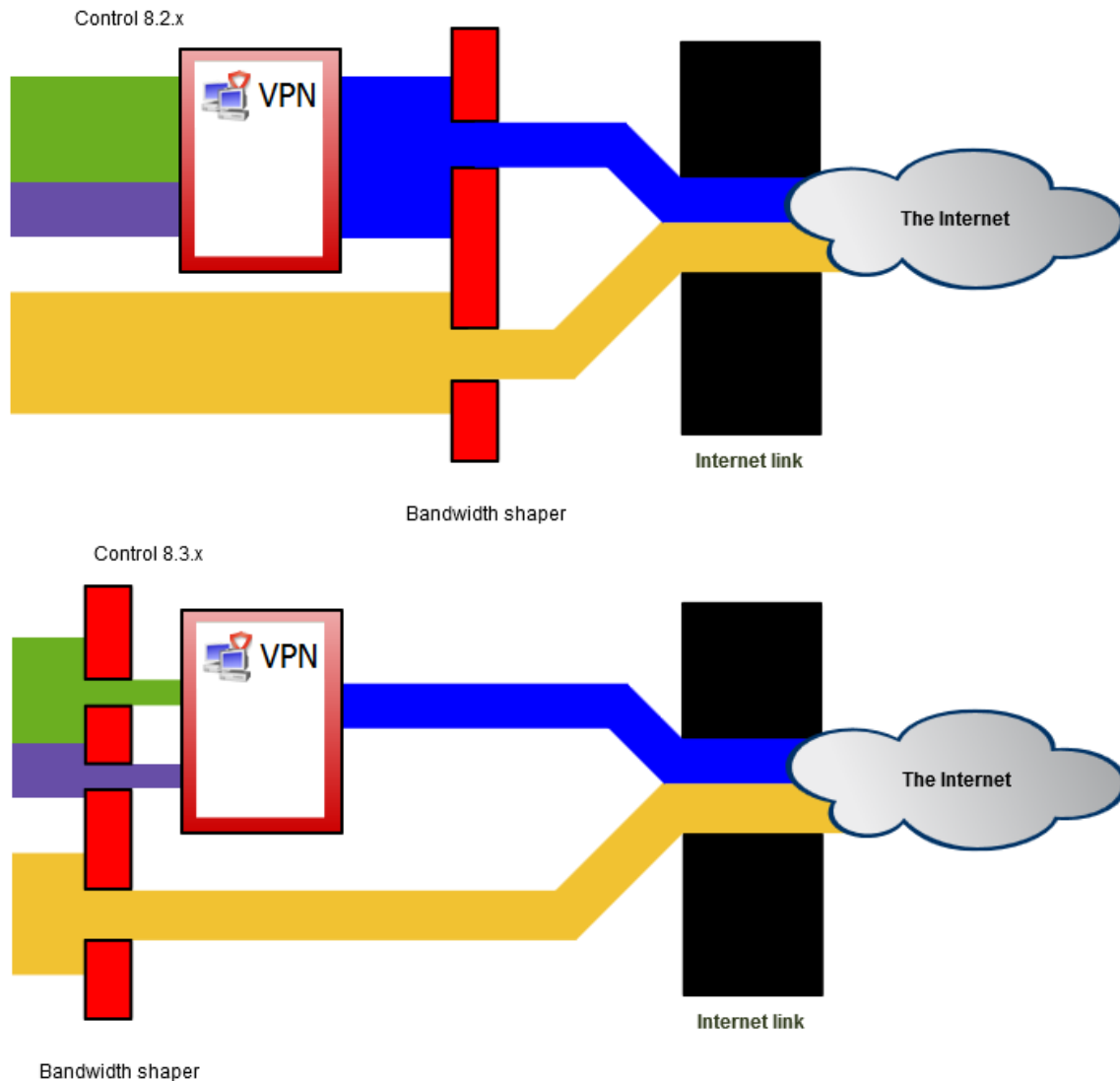


Figure 4 Bandwidth management and VPN tunnels



This option is available in Kerio Control 8.3 and newer. In a new installation, the option is selected by default. If you do not have a good reason to do so, do not change the settings. In an upgrade installation, the option is not selected and you can check it. However, bandwidth management of your Kerio Control will be influenced by that change.

Configuring the Content Filter

Content filter overview



Watch the [Configuring the content filter](#) video.

In the content filter, Kerio Control defines the types of web activities that are allowed by users on your network. The content filter blocks:

- [Kerio Control Web Filter](#)
- [Applications](#)

This filtering on different network layers is easily configured by a single set of rules.

Here are the main purposes of content filtering:

- Access limitations according to URL (substrings contained in URL addresses)
- Filtering based on classification by the [Kerio Control Web Filter](#) module (worldwide website classification database)
- Filtering based on classification by the [Application awareness](#)
- Limitations based on occurrence of [Forbidden words](#)
- [Enforcing SafeSearch in supported search engines](#)
- Access to certain FTP servers
- Limitations based on filenames
- [Elimination of P2P networks](#)

Prerequisites

- Traffic must be controlled by the HTTP / FTP / POP3 protocol inspector.
The HTTP, FTP and POP3 protocol inspectors are activated automatically unless their use is denied by traffic rules.
- Kerio Control performs URL based filtering for encrypted traffic (HTTPS protocol).

Configuring the Content Filter

Learn more in a special article [HTTPS filtering specifics](#).

- Secured FTP traffic (FTPS, SFTP) cannot be filtered.
- Content rules are also applied when the Kerio Control's proxy server is used. However, FTP protocol cannot be filtered if the parent proxy server is used. In such case, content rules are not applied.



Kerio Control does not apply content rules to the [reverse proxy traffic](#).

Configuring content rules

The **Content Rules** table includes several predefined rules.

Each rule is compound from several parts. Each part is represented with a column in the **Content Rules** table. Here there are the most important parts of each rule:

- **Detected content** defines what types of content to filter.
- **Source** is a person or IP address to which the rule applies.
- **Action** describes what to do with the selected content.

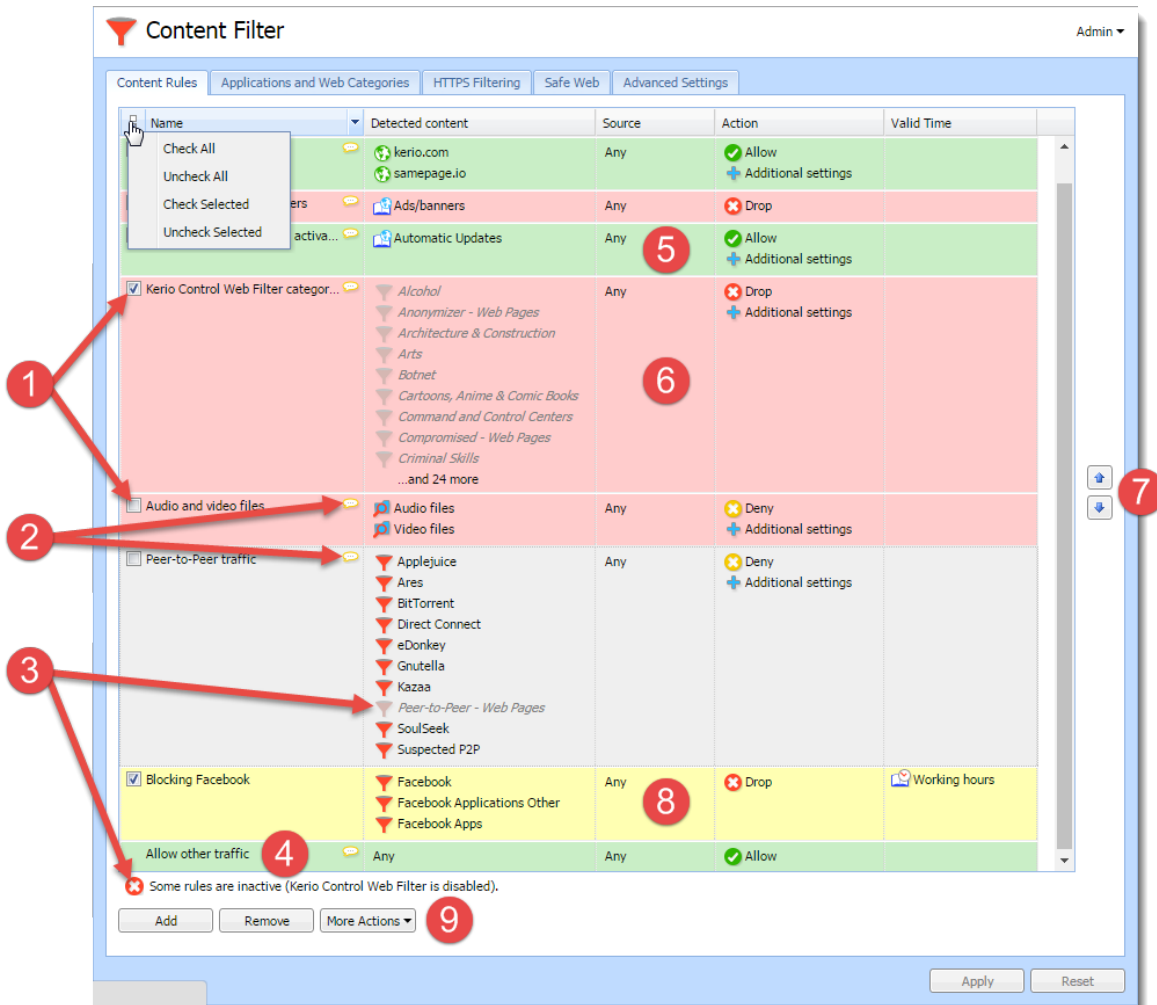
In the **Content Filter** table, you can see:

- Checkboxes which enable/disable rules (1)
- Short descriptions of each rule (2)
- Rules are greyed out when they are inactive(3)

Kerio Control Web Filter or the application awareness feature is inactive on the **Content Filter** → **Applications and Web Categories** tab.

- The default rule allows all content (4)
- Green color highlights allowing rules (5)
- Red color highlights denying and dropping rules (6)
- The order is important. Order rules from general to specific (7)
- Color your own rules for clear arrangement (8)
- **More Actions** (9) allows you to:

- Duplicate the highlighted rule
- Change color of the highlighted rule
- Change the description the highlighted rule
- Edit the time range of the highlighted rule

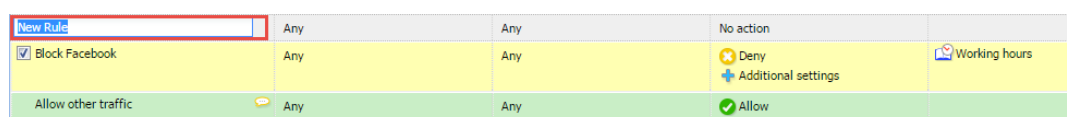


Duplicating content rules

If you want to create a new content rule, try to find a similar one and duplicate it first. Duplicating a rule and adjusting some parameters is quicker than creating the new rule.

Adding new rules

1. In the administration interface, go to **Content Filter**.
2. On tab **Content Rules**, click **Add**.
3. In table, type a name of the rule in the newly created line.



New Rule	Any	Any	No action	
<input checked="" type="checkbox"/> Block Facebook	Any	Any	Deny Additional settings	Working hours
Allow other traffic	Any	Any	Allow	

4. Double-click the **Detected content** column and select what type of the content should be filtered (see details in [Detecting content](#)).
5. Double-click the **Source** column and select users and/or IP addresses.
6. Double-click the **Action** column and fill in the dialog box (see details in [Setting actions](#)).
7. (Optional) Set the valid time — you can set a time interval for applying the rule.
Create time intervals in **Definitions** → **Time Ranges** (see article [Creating time ranges in Kerio Control](#)) then you can select the time interval in the **Content Rules** table.
8. Click **Apply**.

Detecting content

In the **Content Rule - Detected Content** dialog box, click:

- Applications and Web Categories — for pages sorted in the selected categories by the [Kerio Control Web Filter](#) and [the application awareness](#) for pages sorted in the selected categories by the application detection.
- File Name — to allow/disable the transfer of the defined file types.
- URL and Hostname — to type any URL starting with the specified string. It is possible to use wildcards * (asterisk) and ? (question mark).
- URL Groups — to allow/disable access to a group of web pages.

For more details, read article [Configuring URL groups](#).

Setting actions



To log all traffic matched with the rule, check **Log the traffic**. Each log will be written to the [Filter log](#).

The **Content Rule - Action** dialog varies depending on selected action:

Allow

Traffic allowed. With the allow rule you can create the following types of rules:

- Skip Antivirus scanning for selected users, IP addresses or host names.
- Skip Forbidden words filtering for selected users, IP addresses or host names.
- Do not require authentication for selected users, IP addresses or host names.

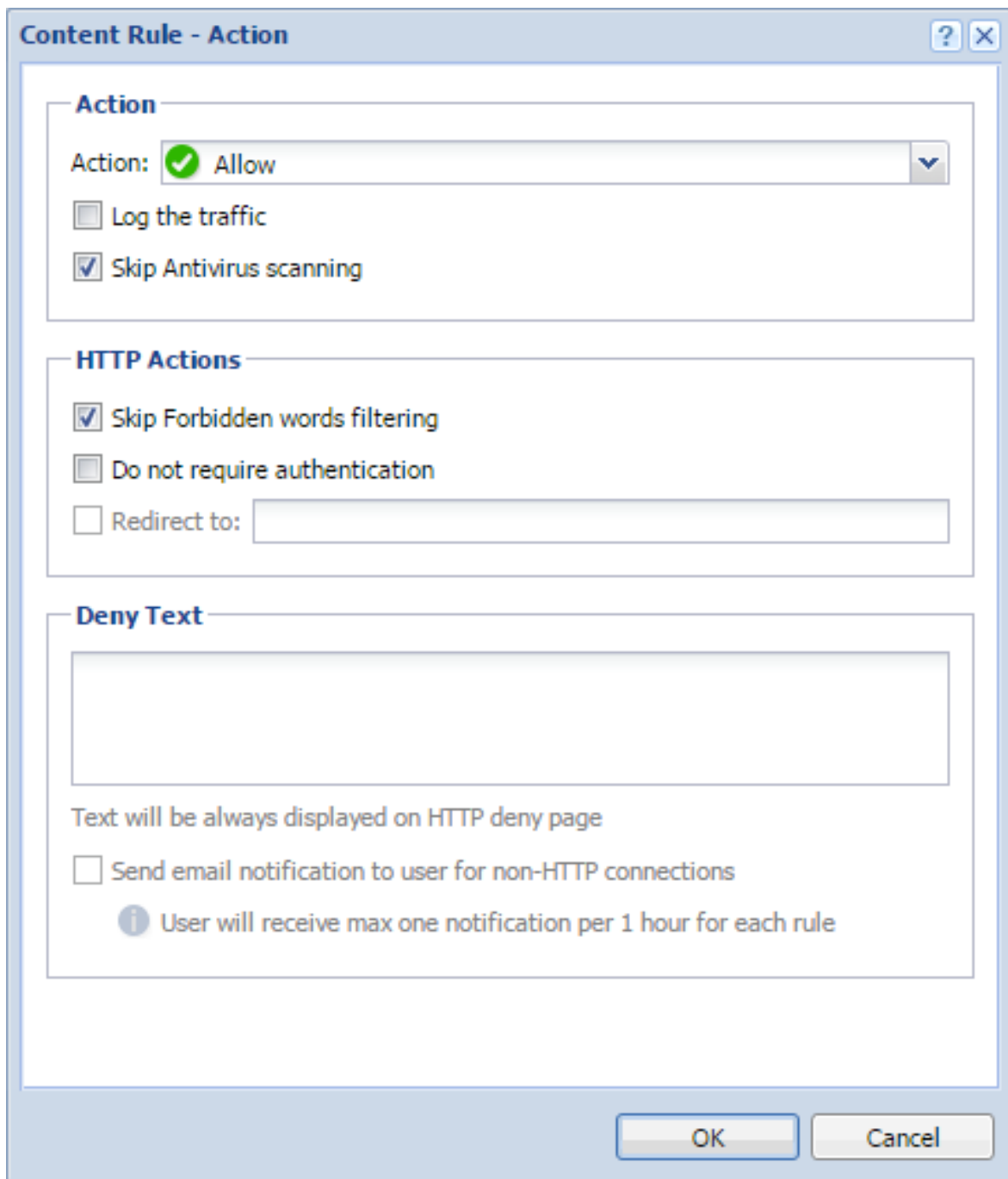


Figure 1 The allowing rule

Deny

User will be redirected to the firewall page with information that access is denied. You can:

- redirect a user to another page

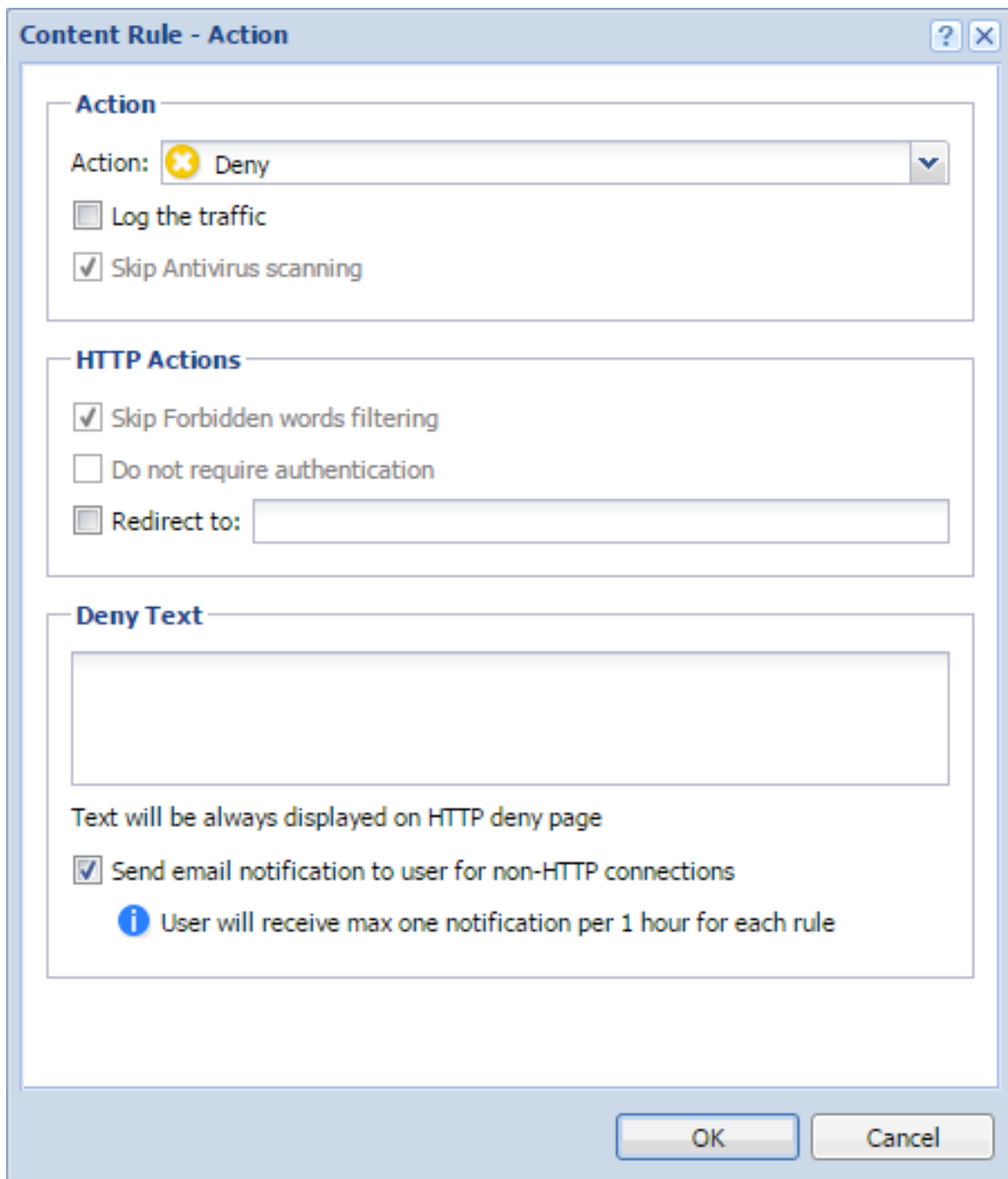


It works only for HTTP sites. Blocked HTTPS sites cannot be redirected to another URL, or to the custom denial page. The page will time out for the user.

- type a deny text
- send email notification

The user must have e-mail address configured in Kerio Control

The user must be authenticated to Kerio Control.



The image shows a Windows-style dialog box titled "Content Rule - Action". It has a standard title bar with a question mark and a close button. The dialog is divided into three main sections: "Action", "HTTP Actions", and "Deny Text".

- Action:** A dropdown menu is set to "Deny" (indicated by a yellow 'X' icon). Below it are two checkboxes: "Log the traffic" (unchecked) and "Skip Antivirus scanning" (checked).
- HTTP Actions:** Contains three checkboxes: "Skip Forbidden words filtering" (checked), "Do not require authentication" (unchecked), and "Redirect to:" (unchecked) followed by an empty text input field.
- Deny Text:** Features a large empty text area for custom denial messages. Below the text area is the text "Text will be always displayed on HTTP deny page". There is a checked checkbox for "Send email notification to user for non-HTTP connections". Below this is an information icon (i) followed by the text "User will receive max one notification per 1 hour for each rule".

At the bottom right of the dialog are "OK" and "Cancel" buttons.

Figure 2 The denying rule

Drop

Access is denied and the user will see the page as unavailable.

Unlocking rules

Privileged users can continue to filtered websites if you enable this right for them. Read [Setting access rights in Kerio Control](#) for detailed information.

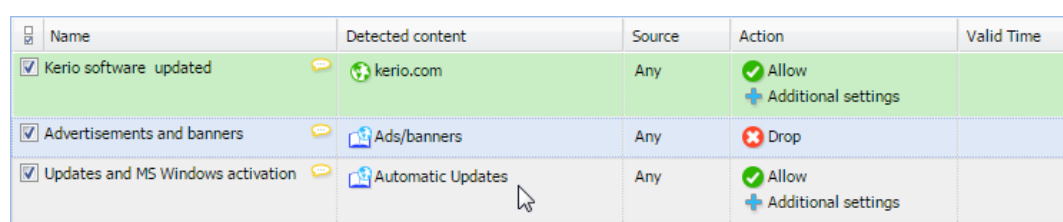
Examples

Adding new URLs for automatic updates

If you start to use a new software with the automatic updates option, you must add a new URL to the content filter:

1. Go to **Content Filter** and enable rule **Allow automatic updates and MS Windows activation**.

The rule is based on the **Automatic Updates** URL group.











Name	Detected content	Source	Action	Valid Time
<input checked="" type="checkbox"/> Kerio software updated	 kerio.com	Any	 Allow  Additional settings	
<input checked="" type="checkbox"/> Advertisements and banners	 Ads/banners	Any	 Drop	
<input checked="" type="checkbox"/> Updates and MS Windows activation	 Automatic Updates	Any	 Allow  Additional settings	

Figure 3 The Content Rules tab

2. Go to **Definitions** → **URL Groups**.
3. Click **Add**.
4. In the **Add URL** dialog, select **Select existing** → **Automatic Updates**.
5. Type the URL for automatic update.

You can use *, ? or select **Use regular expression** and type the URL as regular expression.

Blocking Facebook



If you have a Kerio Control Web Filter license, block Facebook or other social media with the [Application awareness](#).

To deny Facebook, add the following rule:

1. On the **Content Rules** tab, click **Add**.
2. Type a name of the new rule.

Configuring the Content Filter

3. Double-click **Detected Content**.
4. In the **Content Rule - Detected Content** dialog, click **Add** → **URL and Hostname**.
5. Type `facebook.com` into the **Site** field.
6. Check option **Also apply to secured connections (HTTPS)**.

This option has exceptions written in the [HTTPS filtering specifics](#) article.

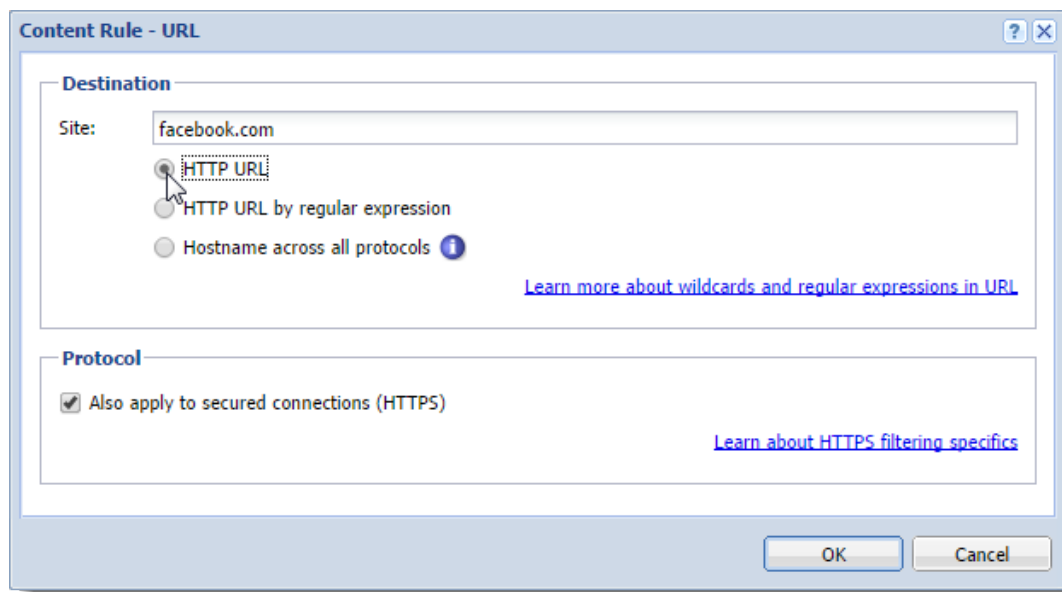


Figure 4 The first part of the Detected Content settings

7. Click **OK**.
8. In the **Content Rule - Detected Content** dialog, click **Add** → **URL and Hostname** again.
9. Type `www.facebook.com` into the **Site** field.
10. Select option **Hostname across all protocols**.

Kerio Control sends DNS query and ensures that all IP addresses used by Facebook will be identified.

11. Click **OK**.
12. Double-click **Action**.
13. In the **Content Rule - Action** dialog, select **Deny** in the **Action** drop-down menu.
14. Save the settings.

Test the rule by login to Facebook.

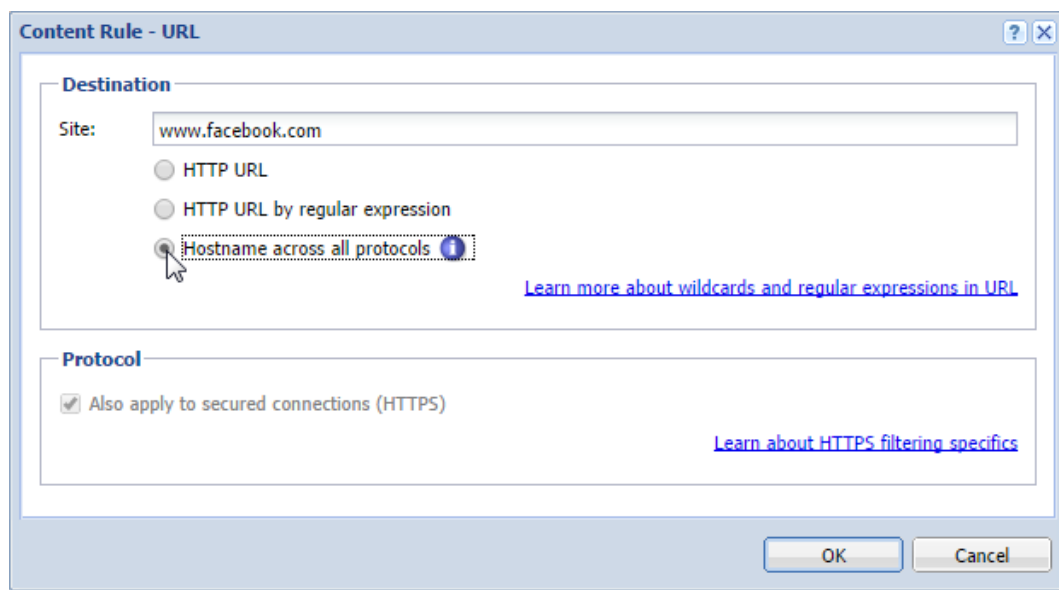


Figure 5 The second part of the Detected Content settings

Allowing all content from Samepage.io

If you want to:

- skip antivirus scanning,
- skip forbidden words filtering,
- do not require authentication,

for samepage.io (or another cloud service), follow the next steps:

1. On the **Content Rules** tab, click **Add**.
2. Type a name of the new rule (All for Samepage).
3. Double-click **Detected Content**.
4. In the **Content Rule - Detected Content** dialog, click **Add** → **URL and Hostname**.
5. Type samepage.io into the **Site** field.
6. Select **Also apply to secured connections (HTTPS)**.
This option has exceptions written in the [HTTPS filtering specifics](#) article.
7. Click **OK**.
8. Double-click **Action**.

Configuring the Content Filter

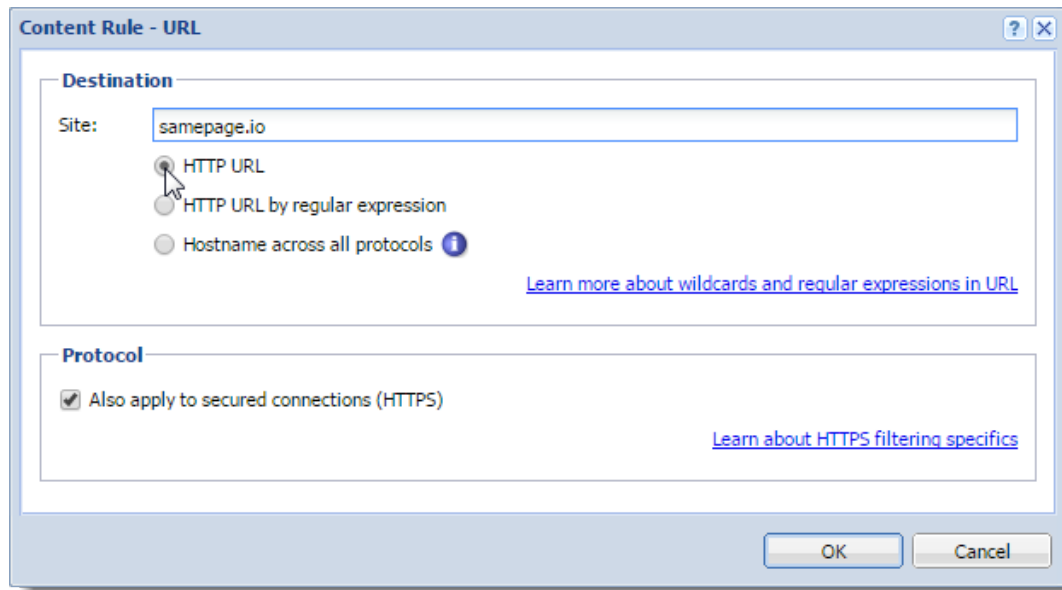


Figure 6 The first part of the Detected Content settings

9. In the **Content Rule - Action** dialog, select **Allow** in the **Action** drop-down menu.
10. Select **Skip Antivirus scanning**.
11. Select **Skip Forbidden words filtering**.
12. Select **Do not require authentication**.
13. Save the settings.

Related articles

[Application awareness in Kerio Control](#)

[Using Kerio Control Web Filter](#)

[Blocking inappropriate or explicit content in search results](#)

[Eliminating Peer-to-Peer traffic](#)

[Filtering web content by word occurrence](#)

[Filtering HTTPS connections](#)

Eliminating Peer-to-Peer traffic

Peer-to-Peer (P2P) networks

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).

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. However, using various methods (such as known ports, established connections, etc.), the P2P Eliminator is able to detect whether users connect to one or multiple P2P networks.

Configuring/Adding the P2P traffic rule

1. In the administration interface, go to **Content Filter**.
2. Select **Peer-to-Peer traffic**.
3. Click **Apply**.

If your **Content Filter** does not include the **Peer-to-Peer traffic** rule, you can add one:

1. Click **Add**.
2. Type a name of the new rule (for example Peer-to-Peer traffic).
3. Double-click **Detected content**.
4. In the **Content Rule - Detected Content** dialog, click **Add** → **Applications and Web Categories**.
5. In the **Selected items** dialog, select **Downloads** → **Peer-to-Peer**.
6. Double-click **Action**.
7. In the **Content Rule - Action** dialog, select **Deny** in the **Action** list.

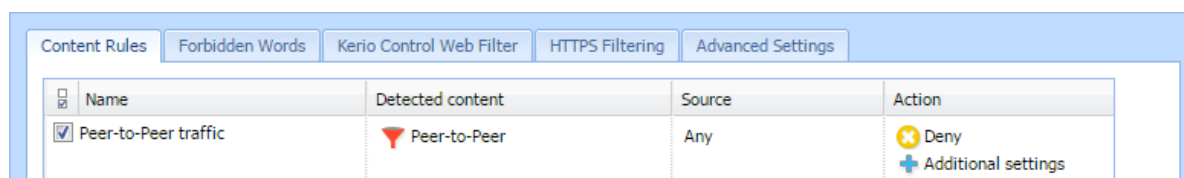
Eliminating Peer-to-Peer traffic

8. (Optional) Select **Send email notification to user for non-HTTP connections**.

Kerio Control informs users about denying P2P traffic.

9. Click Apply.

The result is displayed on figure below.



Information about P2P detection and blocked traffic can be viewed in the **Status → Active Hosts** section.



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 and Monitoring** section.

Configuring parameters for detection of P2P networks

P2P networks are detected automatically (the P2P Eliminator module keeps running). To set the P2P Eliminator module's parameters, go to **Content Filter → Advanced Settings**.

It is not possible to block connections to particular P2P networks. P2P Eliminator allows to permit such services where it is guaranteed that they do not use P2P networks.

Consider the following TCP/UDP port numbers as suspicious

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 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.



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).

Application awareness in Kerio Control

Overview



New in Kerio Control 9.1!

Application awareness has two parts:

- Application control
- Application visibility

Application control allows Kerio Control to recognize thousands of applications in the Kerio Control network. You can then:

- Reserve or limit bandwidth for certain applications
- Allow, deny, or block traffic from or to those applications

Application visibility allows you to review used applications in [Kerio Control Statistics](#) and [Active Connections](#).

The application awareness is available under the Kerio Control Web Filter license. For details, read [Changes in licensing](#).

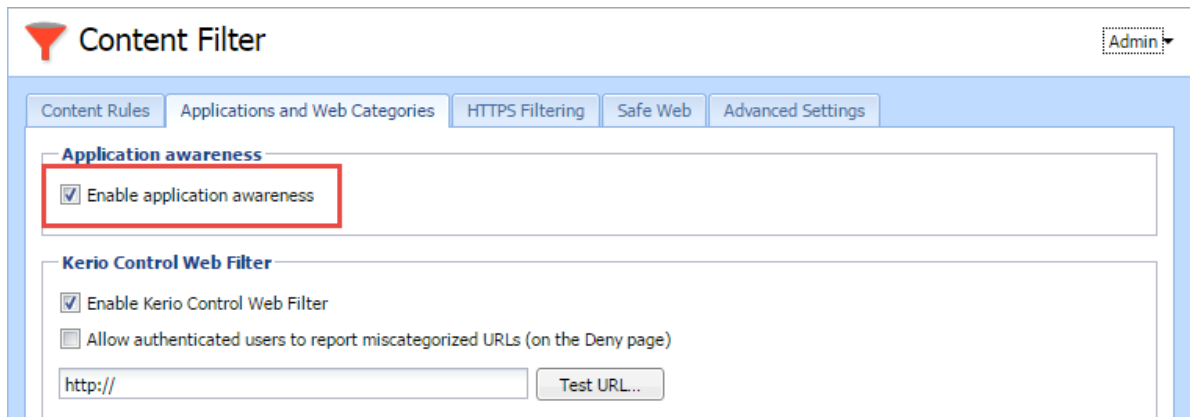
The new application awareness means that the behavior of content filtering and bandwidth management in Kerio Control changes. Rules may become more strict and can be applied to more applications or connections that they match.

To set up and use application awareness, you first [enable application awareness in Kerio Control](#). Then you can select and use applications in the [Content Filter](#) and [Bandwidth Management](#) rules.

Enabling application awareness

Application awareness does not work in combination with [Kerio Control non-transparent proxy server](#) enabled.

1. In the administration interface, go to **Content Filter**.
2. Click the **Applications and Web Categories** tab, and select **Enable application awareness**.
3. Click **Apply**.

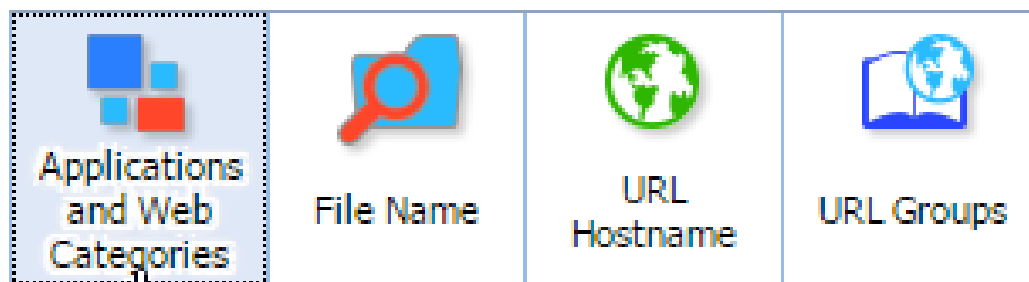


Setting content rules

Example: Social networks

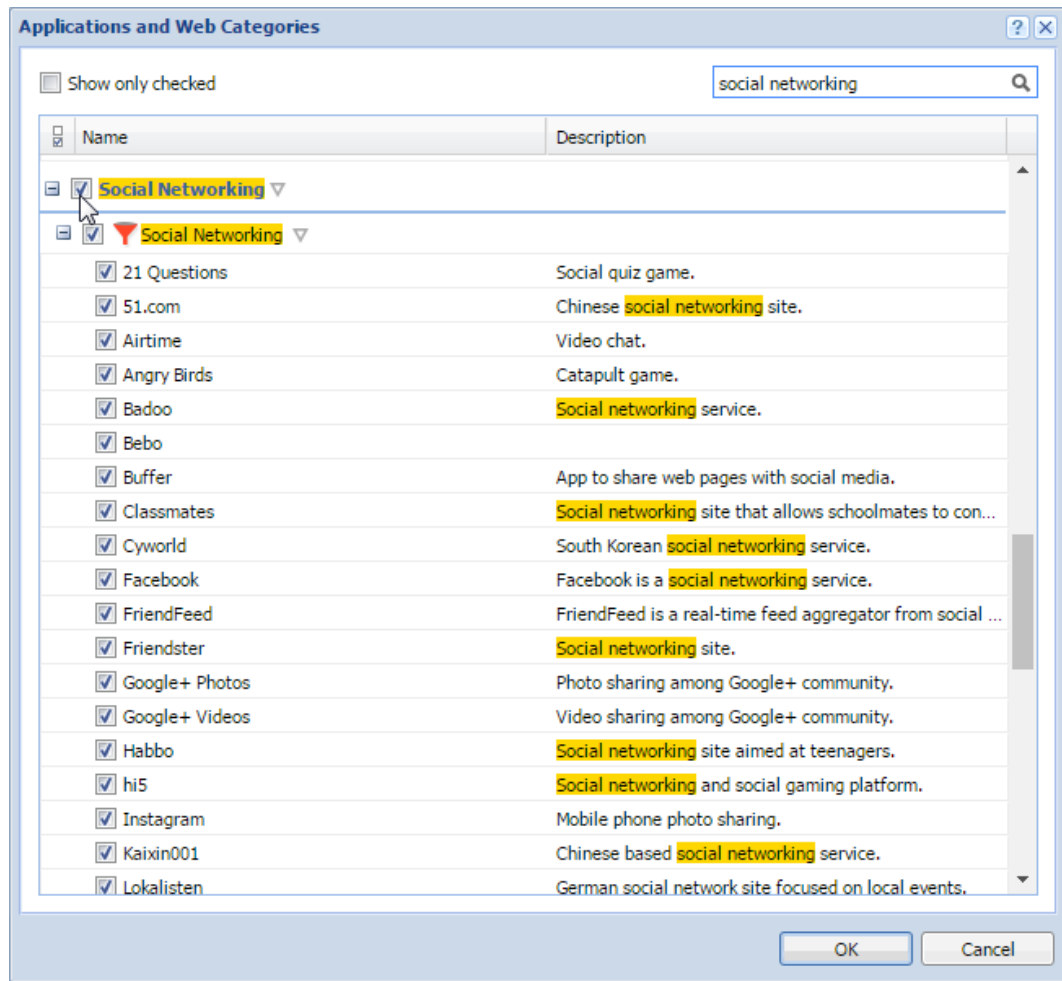
Whenever Kerio Control processes a rule that includes applications and web categories, application awareness is activated. This example shows how to set up a rule that denies all users access to social networks.

1. In the administration interface, go to **Content Filter**.
2. Click the **Content Rules** tab, and click **Add**.
3. In the table, type a name for the rule.
4. Double-click in the **Detected content** column.
5. In the **Content Rule - Detected Content** dialog box, click **Applications and Web Categories**.



Application awareness in Kerio Control

6. In the **Applications and Web Categories** dialog box, select **Social Networking**.



7. Click OK twice.
8. Do not change the **Source** column.
9. Double-click in the **Action** column.
10. In the **Content Rule - Action** dialog box, select **Deny**.

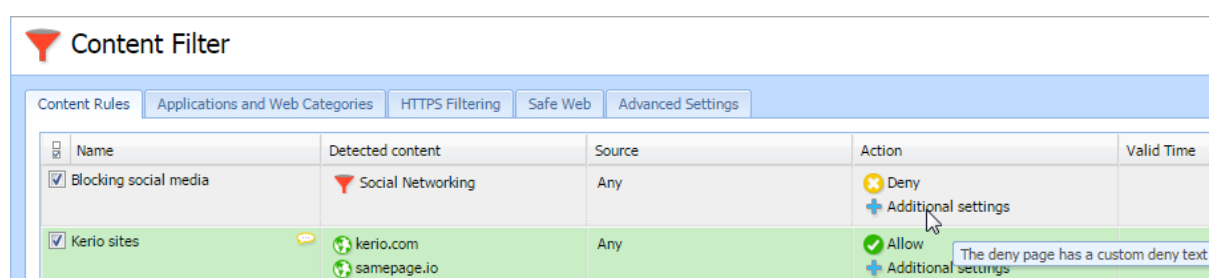


11. Type a deny text that appears to users in their browsers when the rule is matched.

12. Click OK.

13. Click the **Content Rules** tab, and then click **Apply**.

From now on, Kerio Control refuses all attempts to use social media like Facebook or Twitter.



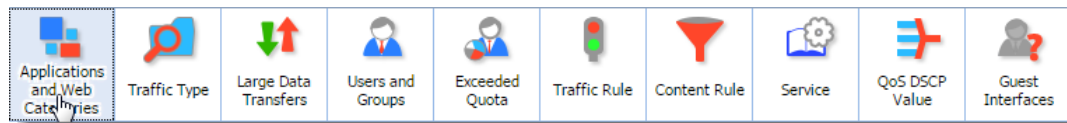
Setting bandwidth rules

Example: Limiting music access

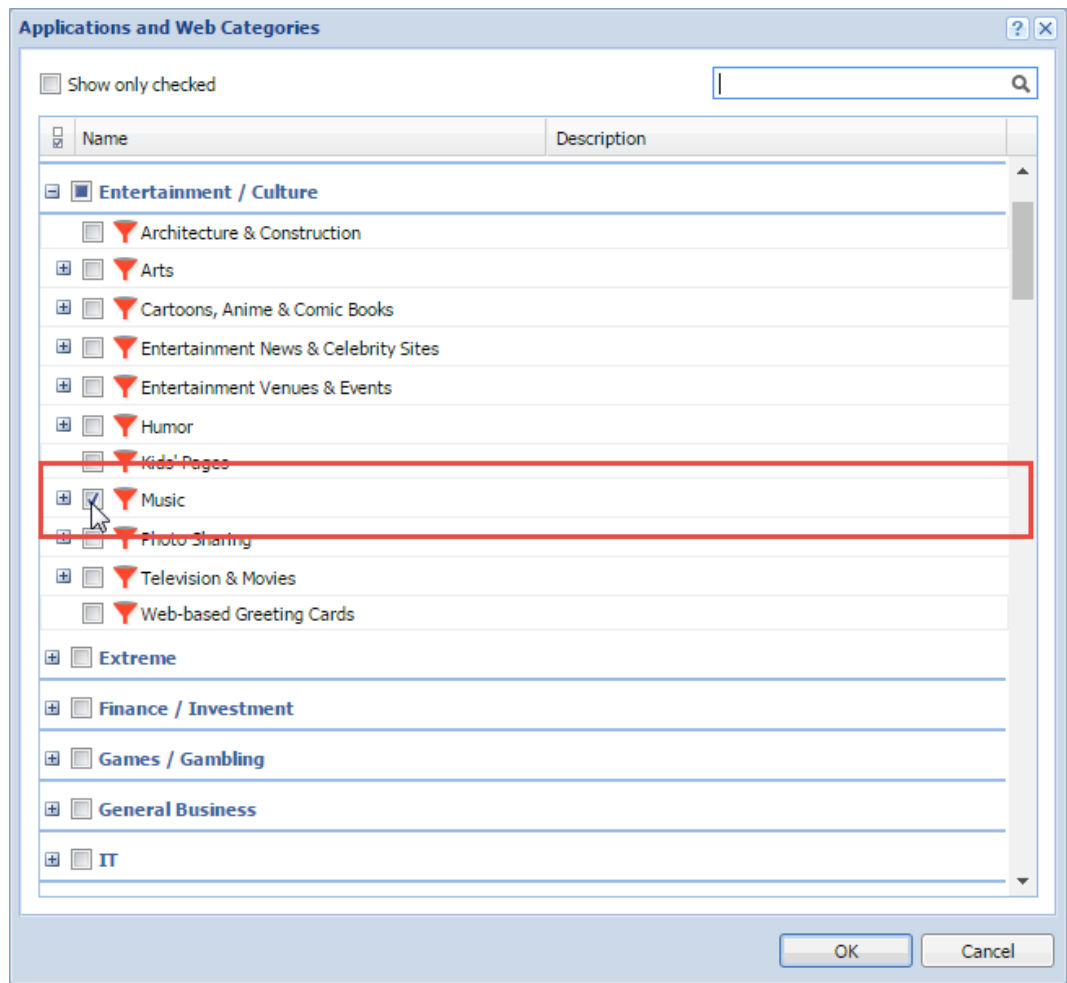
Whenever Kerio Control processes a rule that includes applications and web categories, application awareness is activated. This example describes how to set up a rule limiting access to music for all users:

1. In the administration interface, go to **Bandwidth Management and QoS**.
2. Click **Add**.
3. In the table, type a name for the rule.
4. Double-click in the **Traffic** column.
5. In the **Traffic** dialog box, click **Applications and Web Categories**.

Application awareness in Kerio Control



6. In the **Applications and Web Categories** dialog box, under **Entertainment / Culture**, select **Music**.



7. Click OK twice.
8. In the **Download** column, limit the bandwidth.
In our example, the Ethernet line is limited to 400 KB/s for music.
9. Click **Apply**.

After applying the rule, Kerio Control limits all users who listen to music with applications like Spotify or Internet radiostations.

Bandwidth Management and QoS

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

Name	Traffic	Download	Upload	Interface	Valid Time	Chart
<input checked="" type="checkbox"/> Exceeded quota	Exceeded quota	Limit: 100 KB/s	Limit: 100 KB/s	All	Working hours	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Limit music	Music	Limit: 400 KB/s	No limit	All		<input type="checkbox"/>
<input checked="" type="checkbox"/> SIP VoIP	SIP VoIP	Reserve: 240 KB/s	Reserve: 240 KB/s	All	Working hours	<input type="checkbox"/>
Other traffic	Any	No limit	No limit	All		

Application visibility in Active Connections

In the **Active Connections** section, you can see all applications detected on active connections:

1. In the administration interface, go to **Status** → **Active Connections**.

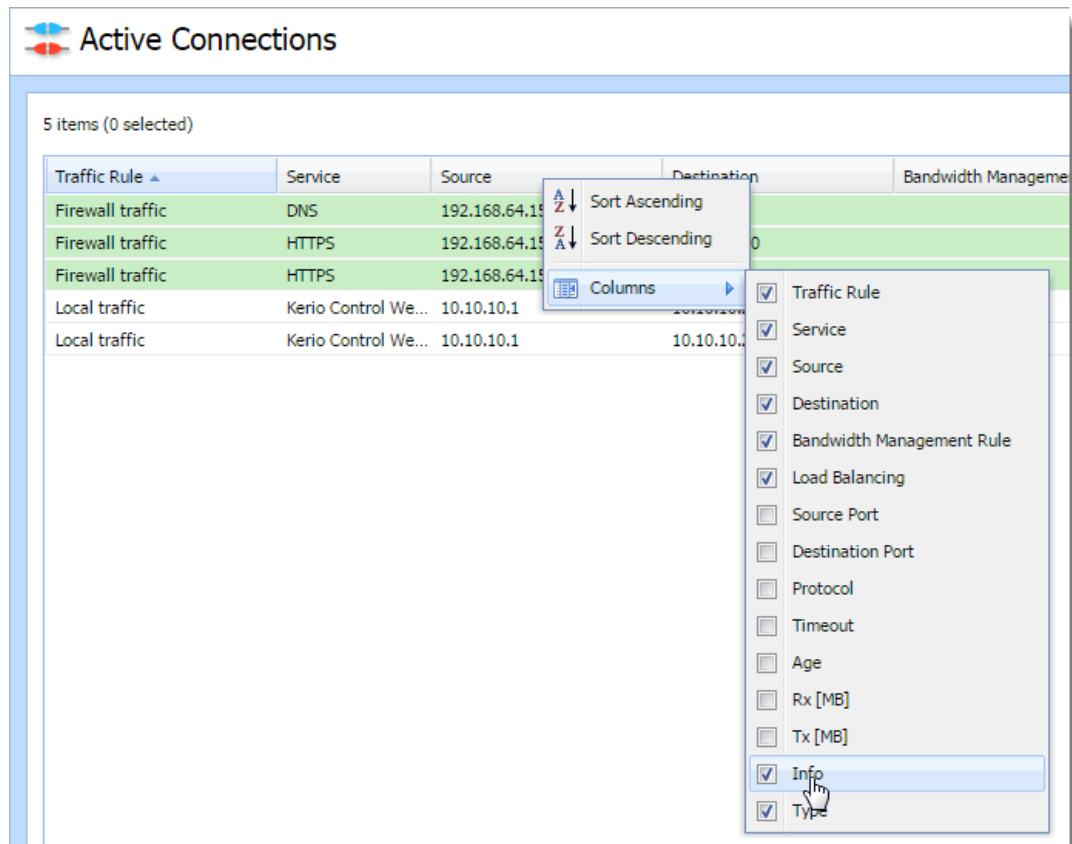
Active Connections

5 items (0 selected)

Traffic Rule	Service
Firewall traffic	DNS
Firewall traffic	HTTPS
Firewall traffic	HTTPS
Local traffic	Kerio Control V
Local traffic	Kerio Control V

2. Right-click the column header.
3. In the context menu, click **Columns**.
4. Select **Info**.

Application awareness in Kerio Control



From now on, the **Info** column displays applications detected by the application awareness.

Debugging application awareness

To run logging for the application awareness:

1. In the administration interface, go to **Logs** → **Debug**.
2. Right-click in the log window.
3. In the context menu, select **Messages**.
4. In the **Logging Messages** window, select:
 - Application awareness
 - Intrusion Prevention System
 - General protocol inspection messages
5. Click OK.

From now on, the log is running.

If you have all necessary data gathered, unselect all three log options. Logging too much information slows Kerio Control's performance.

Changes in licensing



This section is for users upgrading from previous versions to Kerio Control 9.1.

In Kerio Control 9.1 and later, you need a Kerio Control Web Filter license if you have existing rules that you want to continue to use for the following web categories:

- Peer-to-Peer
- Streaming & Downloadable Audio
- Streaming & Downloadable Video
- Email
- Internet Phone & VOIP
- ICQ/AIM
- IRC
- Jabber
- MSN
- Yahoo
- IPsec
- Kerio VPN
- L2TP
- Open VPN
- PPTP
- RDP
- SSH
- Telnet
- VNC

Using 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 users attempt to access a web page, Kerio Control sends a request on the page rating. According to the classification of the page users are either allowed or denied to access the page.



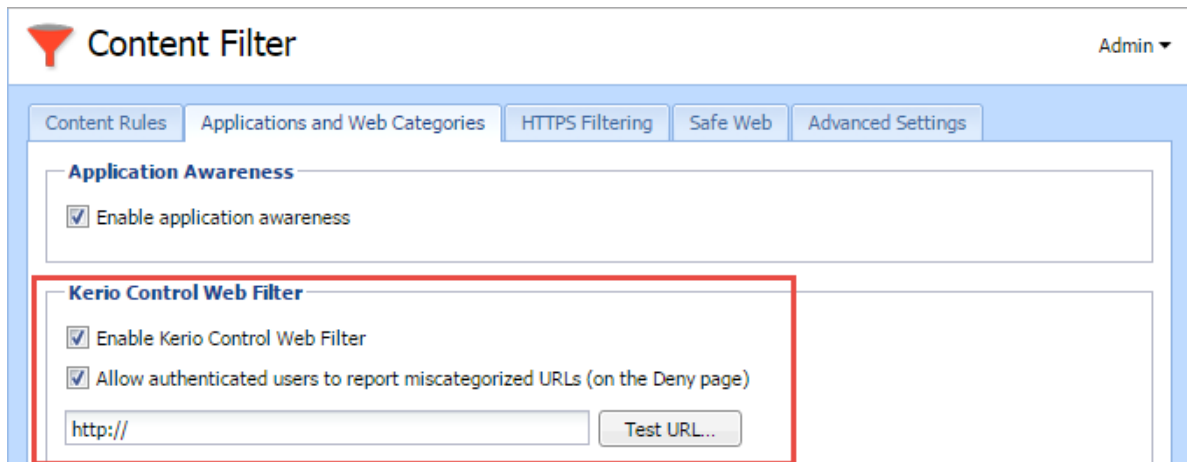
Kerio Control Web Filter requires a special license. Unless Kerio Control includes this module, it behaves as a trial version only (this means that it is automatically disabled after 30 days from the Kerio Control installation and options in the Kerio Control Web Filter tab will not be available).

Enabling Kerio Control Web Filter

1. In the administration interface, go to **Content Filter** → **Applications and Web Categories**.
2. Select **Enable Kerio Control Web Filter**.
3. Select **Allow authenticated users to report miscategorized URLs**

If the user believes that the page is in a wrong category (which makes Kerio Control block access to the page), they can suggest a change to the developers. All suggestions are logged in the **Security** log. If a page is still blocked after couple of days, add the page to the [URL whitelist](#).

4. 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 **Content Filter**, go to **Kerio Control Web Filter**.
2. Type in the URL 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 **Content Filter**, 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 **Content Filter**.
2. On the **Content Rules** tab, enable the predefined rule **Kerio Control Web Filter categories and applications**.
3. Double-click the **Detected content** column and click **Add** → **Applications and Web Categories**.
4. Select the **Job Search** rating category.
5. Click OK twice.
6. On the **Content Rules** tab, click **Apply**.

URL rules are described in more details in a special article: [Configuring the Content Filter](#).

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](#). Also you can use it for [Kerio Control reverse proxy](#). 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 HTTP cache

1. In the administration interface, go to **Proxy Server** → **HTTP 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. If you are using reverse proxy, check **Enable cache for Kerio Control reverse proxy**.
5. 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 **HTTP Cache**, set HTTP protocol TTL (default value: 1 day).
This setting applies to all objects where no extra cache period is specified.
2. Click **URL Specific Settings** for objects on specific servers or pages.

Configuring HTTP cache

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.

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 **HTTP 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). 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.

Blocking inappropriate or explicit content in search results

Overview



New in Kerio Control 9.1!

Kerio Control enables a [SafeSearch](#) module in search engines. SafeSearch blocks inappropriate or explicit content in search results of Kerio Control users.

Kerio Control supports SafeSearch in the following engines:

- Google Search
- YouTube
- Bing
- Yandex

How it works

The SafeSearch feature is based on DNS. If user's computer asks for the IP address of [www.google.com](#), Kerio Control modifies the DNS request to [forcesafesearch.google.com](#). Therefore, SafeSearch does not work in combination with [Kerio Control non-transparent proxy server](#) enabled.

Kerio Control uses the SafeSearch implemented in search engines. Each search engine implements SafeSearch differently, so search results may differ across the supported engines.

Enabling SafeSearch

Firstly, you must [use the Kerio Control DNS server](#). Then follow the steps:

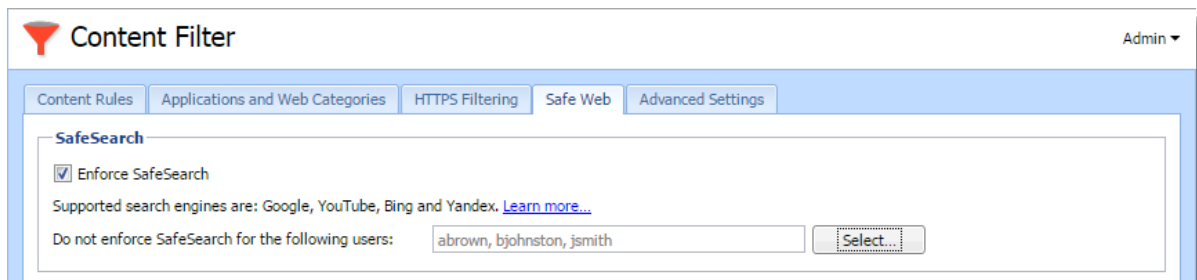
1. In the administration interface, go to **Content Filter** → **Safe Web**.
2. Click **Enforce SafeSearch**.
3. Click **Apply**.

With SafeSearch enabled, Kerio Control users should not see any sexually explicit or inappropriate content in the search results.

Blocking inappropriate or explicit content in search results



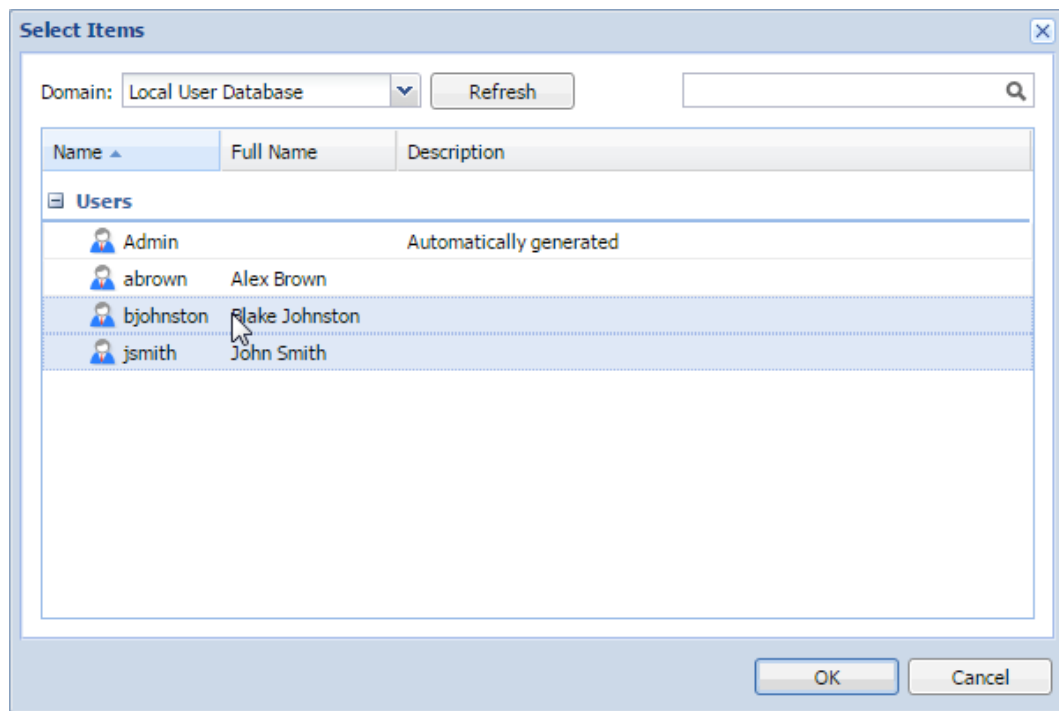
Because of DNS limitations, SafeSearch does not block content cached in browsers and user computers before enabling SafeSearch. You can flush caches in your browser and computer or wait for rewriting the caches. It may take up to 24 hours.



Excluding users from SafeSearch

Users can have problems with SafeSearch enabled. For example, SafeSearch can block an important web page with harmless content. If this happens, you can exclude users from the SafeSearch blocking:

1. In the administration interface, go to **Content Filter** → **Safe Web**.
2. In the **Do not enforce SafeSearch for the following users** field, click **Select**.
3. In the **Select Items** dialog box, click **Add**.
4. In another **Select Items** dialog box, select users.



5. Click **OK** twice.

6. Click **Apply**.

Kerio Control excludes the selected users from the SafeSearch blocking.

Filtering web content by word occurrence

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.

The feature Forbidden Words is disabled by default. To enable it, select **Enable Forbidden words filtering** in the **Content Filter** → **Forbidden Words** tab.

Adding a new forbidden word

1. In the administration interface, go to **Content Filter** → **Safe Web**.

2. Click **Add**.

3. In the **Add Group Item** dialog box, select an existing group or create a new one.

Words are sorted into groups. All groups have the same priority and Kerio Control tests all of the groups.

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 web sites 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 Kerio Control does not block legitimate web pages.

Add Group Item

Add to a group

☐ Select existing: Pornography

☒ Create new: Job opportunities

Properties

Keyword: job

Weight: 20

Description: Word job got 20 points to increase its weight

OK Cancel

6. Click **OK**.
7. On the **Safe Web** tab, click **Apply**.

Filtering HTTPS connections

Overview



New in Kerio Control 8.4!

Kerio Control decrypts and filters HTTPS connections. Filtering is the same as for the HTTP protocol. Kerio Control can apply the same filters and methods to the content of HTTPS connections, such as:

- filtering URLs
- Kerio Control Web Filter
- antivirus check

You can see the filtering results in **User Statistics and Reporting**.

When a user accesses a site secured by HTTPS, an SSL certificate warning appears because Kerio Control uses its own certificate for reencrypting HTTPS communication. Therefore it is important to [distribute the Kerio Control certificate to your users' web browsers as a root certificate authority](#).



HTTPS protocol filtering provides an HTTPS inspector. You can switch off the inspector for a particular rule in the **Traffic Rules** section or for a particular protocol in the **Definitions** → **Services** section. Read more in the [Disabling protocol inspectors](#) article.



If you use [a non-transparent proxy server](#), the HTTPS filtering does not work.

Configuring HTTPS filtering

To start HTTPS filtering:

1. Go to **Content Filter** → **HTTPS Filtering** in the administration interface.
2. Select **Decrypt and filter HTTPS traffic**.

3. Select **Show Legal Notice to users**, if it is necessary in your country.

Contact your legal advisor if it is necessary to select this option. When users open a HTTPS site, Kerio Control warns them that the connection is decrypted by Kerio Control. The disclaimer appears each logged-in user once per session and might be annoying to users.

4. Click **Apply**.

Kerio Control decrypts and filters all HTTPS communication.

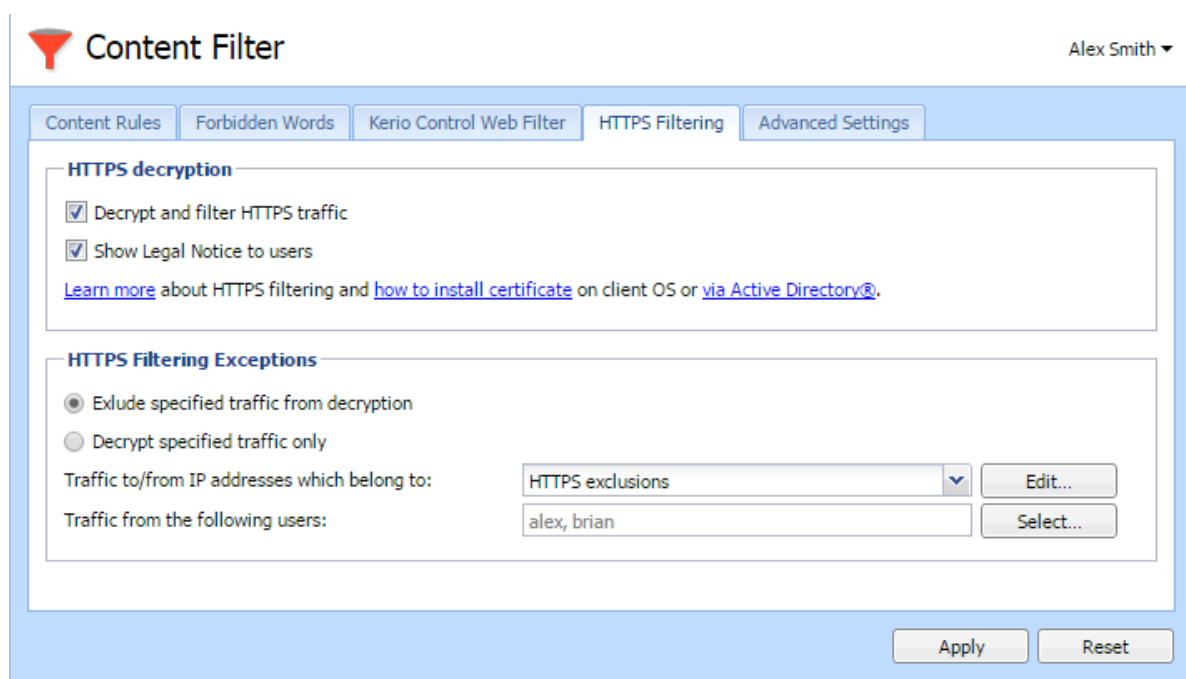


Figure 1 HTTPS Filtering

Setting HTTPS filtering exceptions

Kerio Control allows you to add exceptions from HTTPS filtering. There are two types of exceptions. You can:

- **Exclude specified traffic from decryption**
- **Decrypt specified traffic only** use it when you need to decrypt only certain servers or users.

You can set exceptions for:

- [web applications](#)
- [users](#)

Excluding traffic to/from web applications

Some web applications cannot use the Kerio Control certification authority (for example web access to banks, dropbox.com, microsoft.com) or use a non-HTTPS service on port 443. You must exclude these web applications from the HTTPS filtering.

To set exceptions for an web application, you must know its IP address, domain name, or hostname:

1. On the **HTTPS Filtering** tab, select **Exclude specified traffic from decryption**.
2. Next to the **Traffic to/from IP addresses which belong to** field, click **Edit**.
3. In the **IP Address Groups** dialog box, click **Add**.
4. In the **Add IP Address** dialog box, click **Select existing**.
5. In the **Select existing** menu, select **HTTPS exclusions**.
6. Select **Addresses** and type the IP address, host name or domain name of the web application.



If you add a domain name, you must use the [Kerio Control DNS server and enable the DNS cache](#).

If you use IP address or a host name you can use any DNS server.

7. Save your settings.
8. On the **HTTPS Filtering** tab, click **Apply**.

All web applications in this list are excluded from the HTTPS filtering.

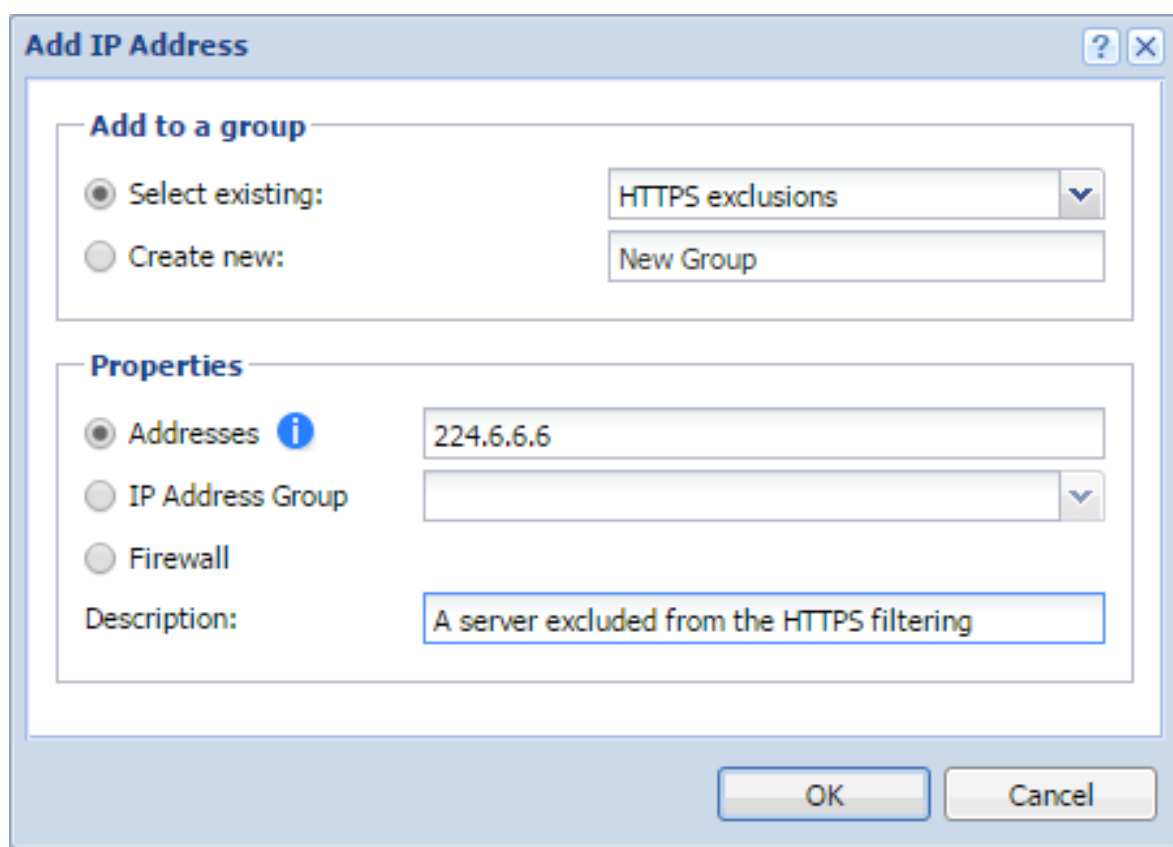


Figure 2 HTTPS Filtering - preconfigured exception for Dropbox.com



To change or delete an exclusion, go to the **Definitions** → **IP address groups** section.

Excluding users from the HTTPS filtering

If there are Kerio Control users, which cannot use HTTPS filtering (for example because of legal reasons), you can exclude them:

1. On the **HTTPS Filtering** tab, click **Exclude specified traffic from decryption**.
2. Next to the **Traffic from the following users** field, click **Select**.
3. In the **Select Items** dialog box, click **Add**.
4. In the new **Select Items** dialog box, select the domain of users which should be excluded.
5. Select users and click **OK**.

Kerio Control adds users to the list.

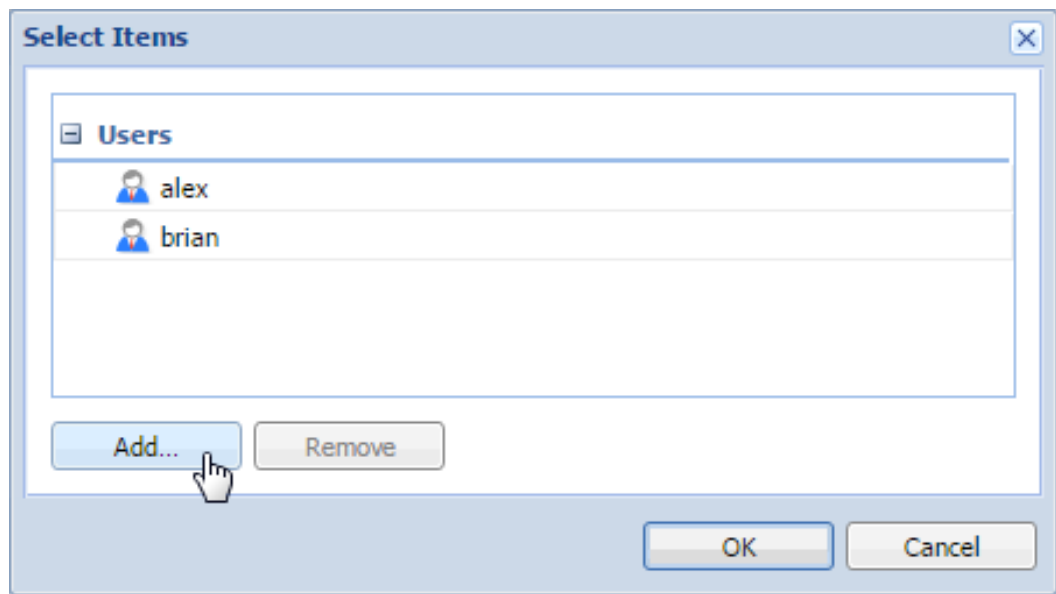


Figure 3 HTTPS Filtering exceptions for users

6. Click **OK**.
7. On the **HTTPS Filtering** tab, click **Apply**.

Kerio Control displays the list of excluded user in the **Exclude traffic from the following users** field. These users are excluded from the HTTPS filtering.

Importing a certificate for an untrusted web applications into Kerio Control

Sometimes you or your users need to go to servers with a self-signed certificate. Such certificates are untrusted, so Kerio Control needs the certificate for authentication. You can:

- [add the server to a list of excluded applications](#)
- [install the certificate of the server to Kerio Control](#)

Installing certificates to Kerio Control

1. In the administration interface, go to **Definitions** → **SSL Certificates**.
2. Click the **More actions** → **Import** → **Import New Certificate** button.
3. The **Import Certificate** dialog box opens.
4. In the **Import Certificate** dialog box, select **Certificate without private key**.

5. Type the URL of the web application
or
if you have the certificate, select the certificate file.
6. Click **Import**.

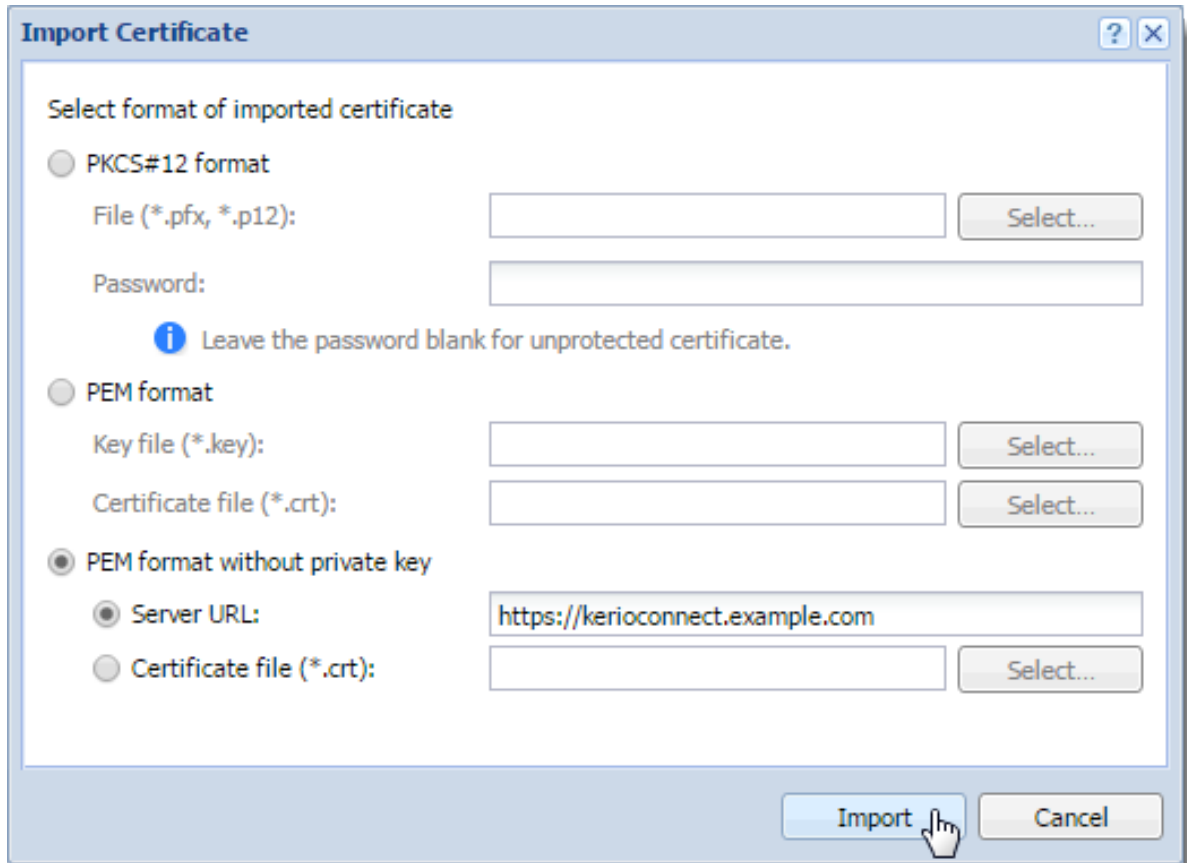


Figure 4 Kerio Control client login page

New certificate appears in the **SSL Certificates** section. Now your users can go to the untrusted page.

Configuring 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 non-transparent proxy server.

You can use it, for example, when Kerio Control is deployed within a network with many hosts where proxy server has been used. Thus, the Internet connection is kept if proxy server is used, and you don't have to re-configure all the host (or only some hosts require re-configuration).



The proxy server can be used for HTTP, HTTPS and FTP protocols. Proxy server does not support the SOCKS protocol.



If you use a non-transparent proxy server, [the filtering of HTTPS connections](#) does not work.

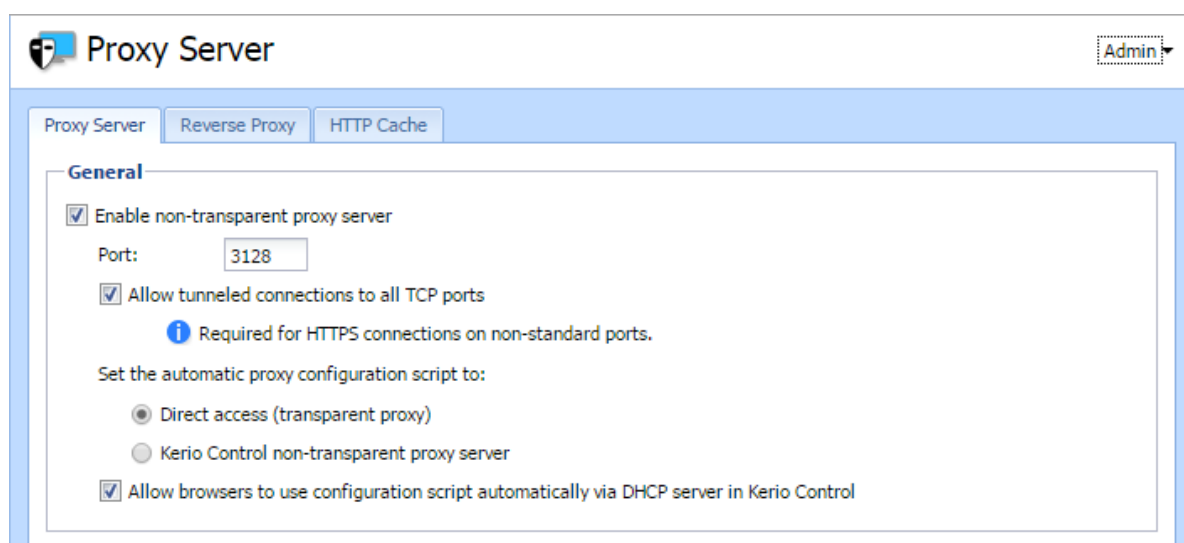
Configuring the proxy server

1. In the administration interface, go to **Proxy Server**.
2. Select option **Enable non-transparent proxy server**.
This option enables the HTTP proxy server in Kerio Control on the port in the **Port** entry (3128 port is set by the default).
3. To enable a tunnelled connection on non-standard TCP ports (for example, connecting to remote Kerio Control administration placed in the Internet from your local network), select option **Allow tunnelled connections to all TCP ports**.



This option affects HTTPS traffic only. You can always access HTTP on any port via non-transparent proxy.

4. Click **Apply**.



Configuring browsers

To communicate through non-transparent proxy server, you must configure web browsers on client hosts. You have several options for this configuration:

- Configure browsers manually: type the IP address or DNS name of the proxy server and port (3128 is the default port for Kerio Control) in the proxy server settings in the browser
- In the Kerio Control administration in the **Proxy Server** section, switch the mode for automatic proxy configuration script to **Kerio Control non-transparent proxy server**, and add the following address to the browsers settings:

`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).

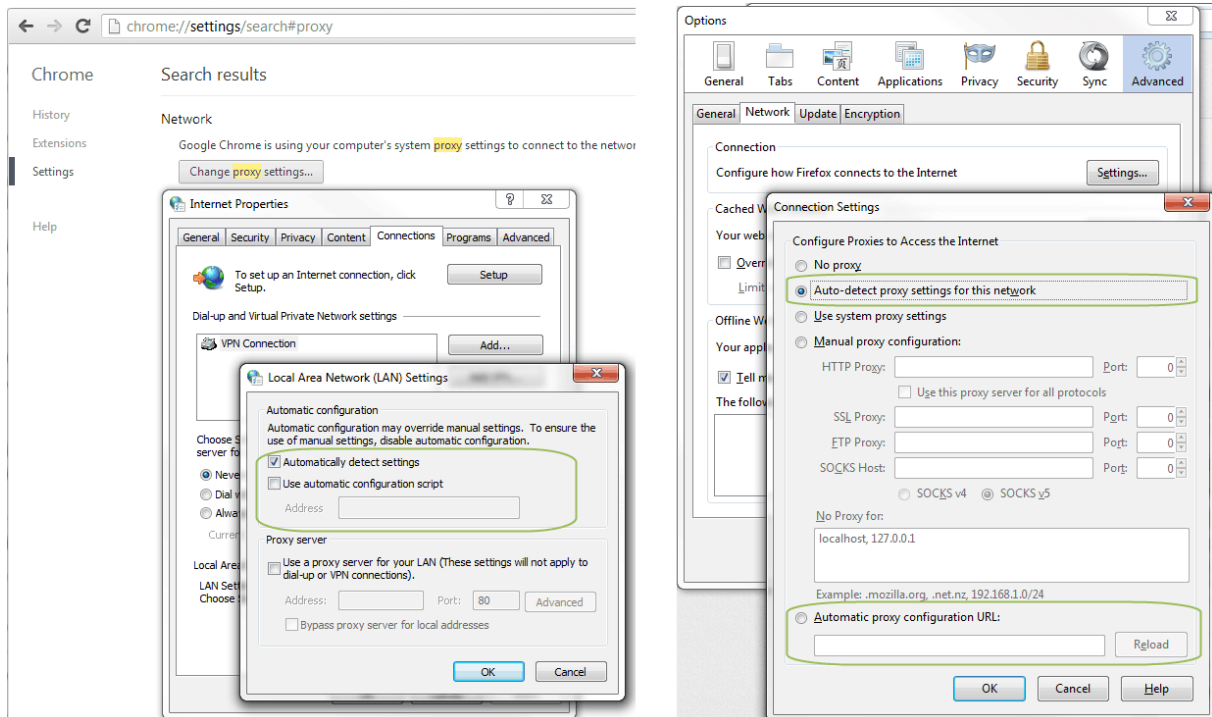
- In the Kerio Control administration in the **Proxy Server** section, switch the mode for automatic proxy configuration script to **Allow browsers to use configuration script automatically via DHCP server in Kerio Control**

All browsers must select **Automatically detect settings** in the proxy server settings.



The automatic configuration of browsers may take several hours. Browsers must ask for a new configuration.

Configuring proxy server



Forwarding to parent proxy server

You can use a parent proxy server for non-transparent proxy traffic, update checks, Sophos updates downloads, and for connecting to the online Kerio Control Web Filter databases.

1. In the administration interface, go to **Proxy Server**.
2. Select **Use parent proxy server**.
3. Type the IP address or the DNS name of the parent proxy server to the **Server** field.
4. Type a port number behind the colon.
5. If your provider gives you credentials for authentication, select option **Parent proxy server requires authentication** and type the credentials.



Credentials are sent with each HTTP request. Only Basic authentication is supported.

Parent proxy server

☒ Use parent proxy server

Server: :

☒ Parent proxy server requires authentication

Username:

Password:

Configuring the reverse proxy

Why use the reverse proxy server in Kerio Control



New in Kerio Control 8.3!

With the reverse proxy, you can provision more than one web server placed behind Kerio Control. A single public IP address is used on a default port (80 for HTTP and 443 for HTTPS). Kerio Control forwards traffic to different servers based on the hostname. Kerio Control does not support directories.



[Content Filter rules](#) are not applied to the reverse proxy traffic in Kerio Control.

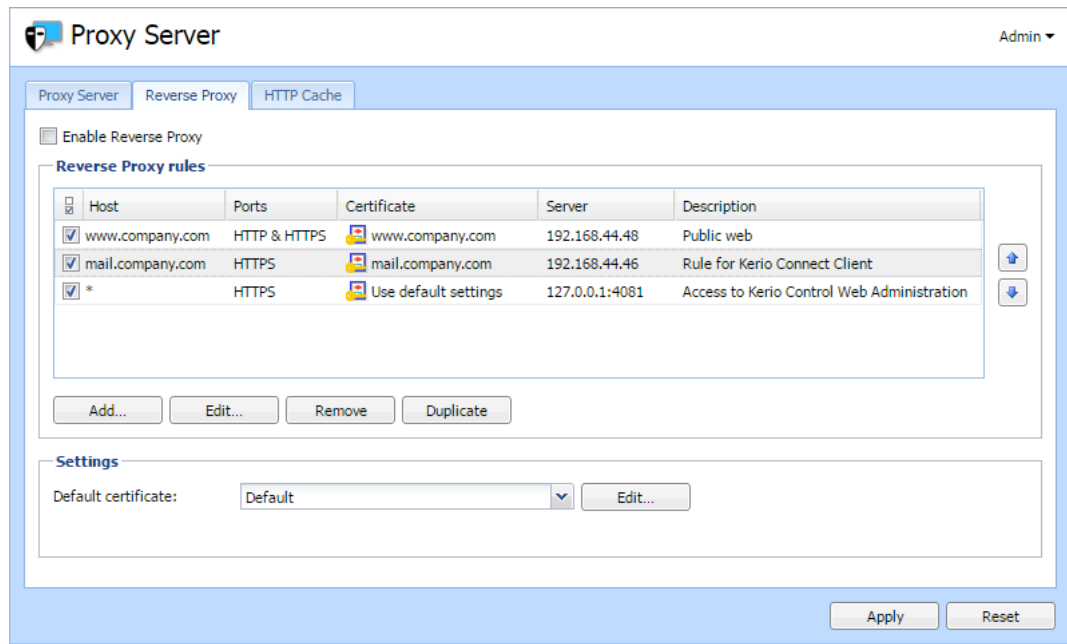
Configuring the reverse proxy



First, you must [configure a traffic rule to allow HTTP/HTTPS to the firewall](#).

To configure the reverse proxy, enable it in Kerio Control and add rules for particular web servers:

1. In the administration interface, go to **Proxy Server** → **Reverse Proxy**.
2. Select **Enable Reverse Proxy**.



3. Click **Add** and [create new rules for your servers](#), as described below.

4. Arrange your rules using the arrows on the right side of the main window.

Kerio Control examines rules from the top down. The last asterisk rule directs other traffic to the 4081 port (Kerio Control Web Administration).

5. In **Settings**, select a valid SSL certificate. You need the certificate for proper authentication of Kerio Control when using HTTPS protocol in rules.

To avoid problems with browsers, use [one SSL certificate with alternative DNS names](#) as a default certificate, as described below.



The SSL certificate must be created with a proper Kerio Control DNS name as a hostname.

Adding new rules

Each rule represents one web server behind Kerio Control.

1. In the administration interface, go to **Proxy Server** → **Reverse Proxy**.

2. Click **Add**.

3. In the **Reverse Proxy Rule** dialog box, type the DNS name of the web server in the **Host** field.

Configuring the reverse proxy



Asterisk notation is allowed.

4. Select the protocol of the server. You can select HTTP, HTTPS, or both.

If you are using the HTTPS protocol, select a valid SSL certificate. You need the certificate for proper authentication of Kerio Control when using HTTPS protocol.



The SSL certificate must be created with a proper web server DNS name as a hostname.

5. In the **Server** field, type the server's private IP address.

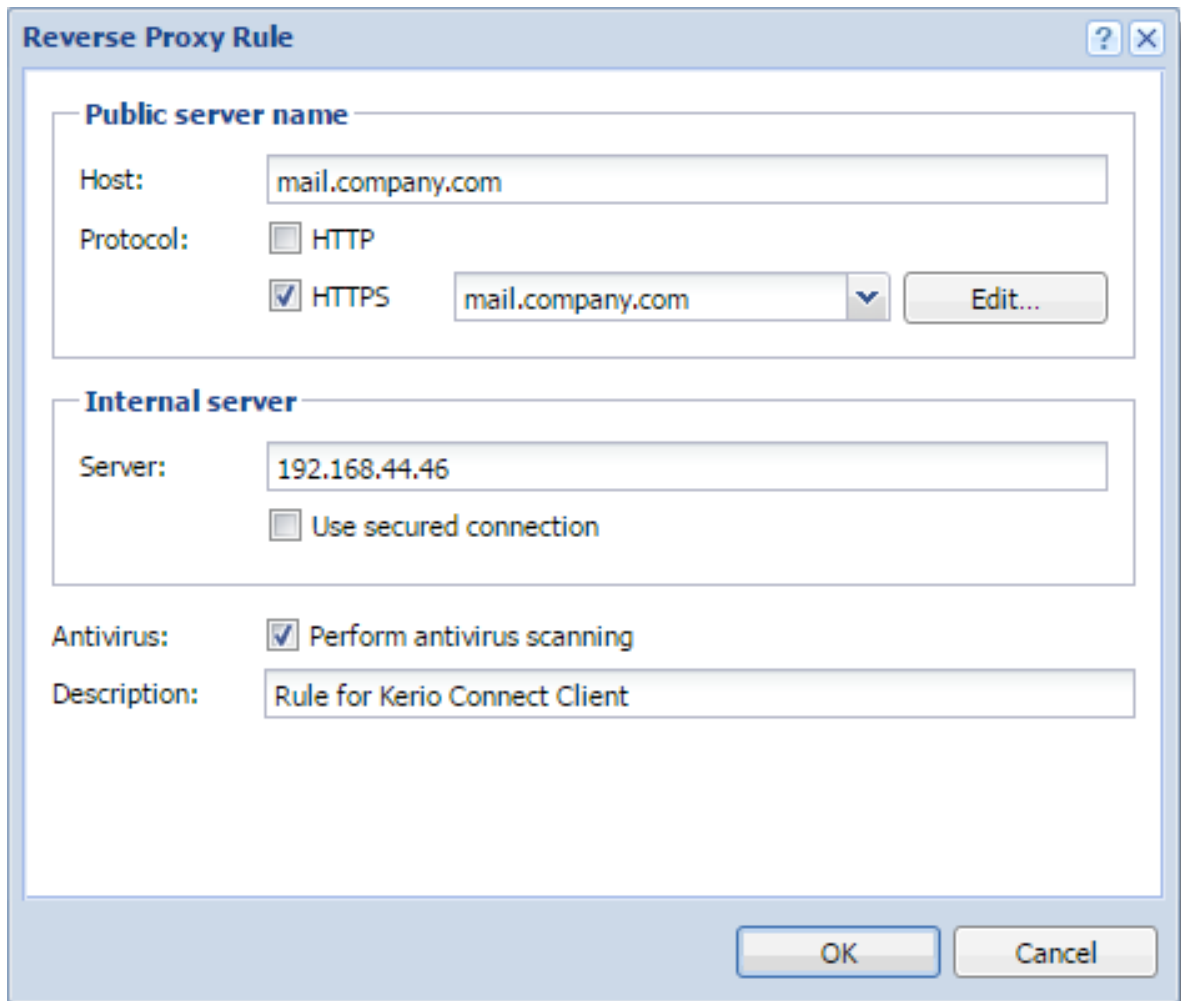
To secure the connection from Kerio Control to the web server (in the local network), select **Use secured connection**.

6. (Optional) To use antivirus scanning on files uploaded to the web server, select **Perform antivirus scanning**.

7. Click **OK**.

8. In the main window, click **Apply**.

Kerio Control can now use the new rule for your web server.

The image shows a 'Reverse Proxy Rule' dialog box with a light blue border and standard window controls (minimize, maximize, close) in the top right. The dialog is divided into several sections. The 'Public server name' section contains a 'Host:' field with 'mail.company.com', a 'Protocol:' section with radio buttons for 'HTTP' (unchecked) and 'HTTPS' (checked), a dropdown menu showing 'mail.company.com', and an 'Edit...' button. The 'Internal server' section contains a 'Server:' field with '192.168.44.46' and a 'Use secured connection' checkbox (unchecked). Below these sections is an 'Antivirus:' section with a checked checkbox for 'Perform antivirus scanning'. At the bottom is a 'Description:' field containing 'Rule for Kerio Connect Client'. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Reverse Proxy Rule

Public server name

Host: mail.company.com

Protocol: ☐ HTTP ☒ HTTPS mail.company.com Edit...

Internal server

Server: 192.168.44.46 ☐ Use secured connection

Antivirus: ☒ Perform antivirus scanning

Description: Rule for Kerio Connect Client

OK Cancel

Figure 1 Reverse Proxy Rule dialog

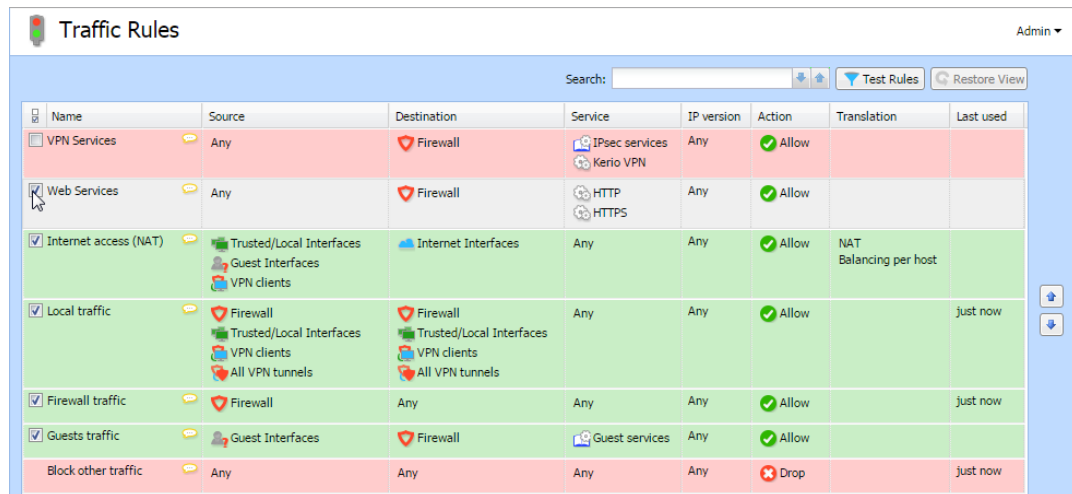
Configuring a traffic rule

To allow HTTP or HTTPS to the firewall, you must configure traffic rules:

1. In the administration interface, go to **Traffic Rules**.
2. Select the **Web Services** rule.

If the rule is not available, create the rule to allow HTTP or HTTPS to the firewall, as shown in the figure below.

Configuring the reverse proxy



Name	Source	Destination	Service	IP version	Action	Translation	Last used
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow		
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow		just now
Firewall traffic	Firewall	Any	Any	Any	Allow		just now
Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow		
Block other traffic	Any	Any	Any	Any	Drop		just now

3. Click **Apply**.

HTTP/HTTPS traffic is allowed.

Creating SSL certificates with alternative DNS names

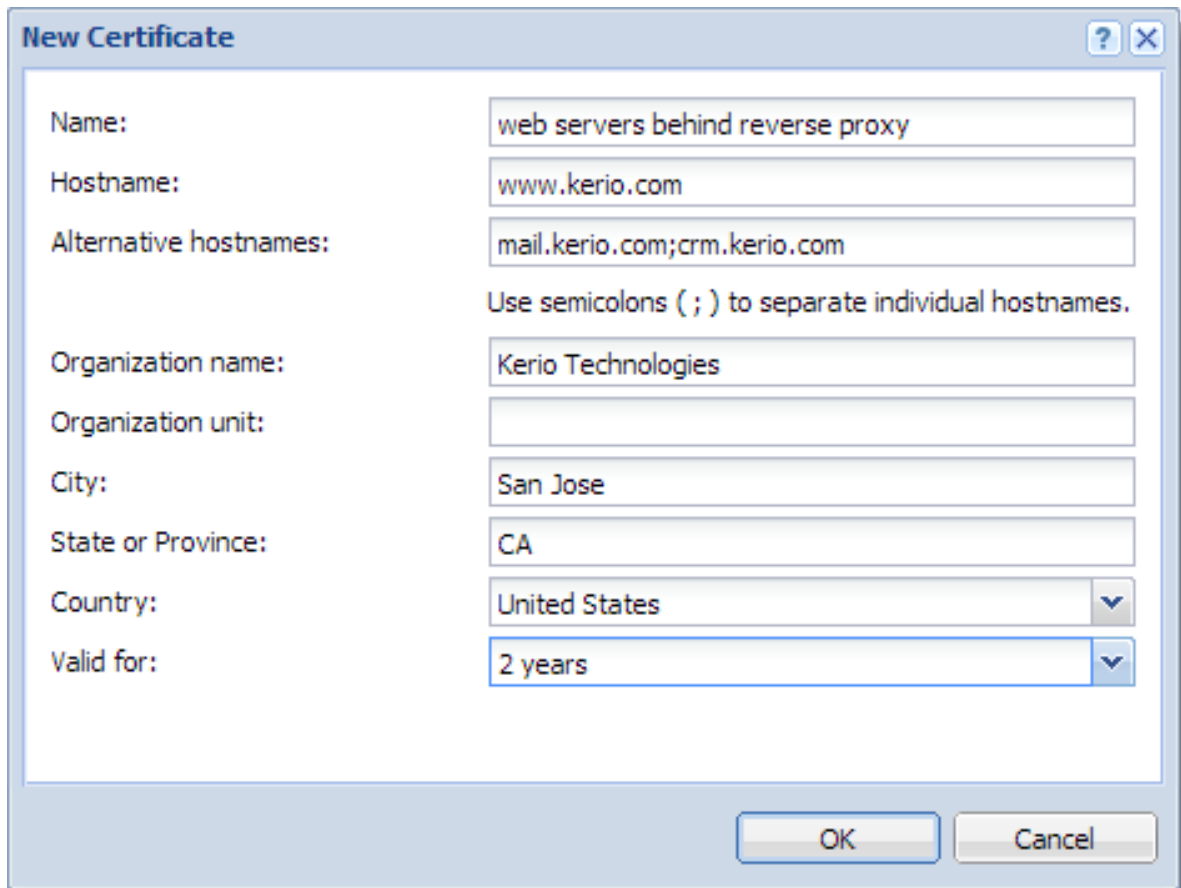
If you configure the reverse proxy for your web servers, you can use just one certificate for all the web servers placed behind the reverse proxy.



You can use this for [self-signed certificates](#) and certificates [signed by a certification authority](#).

To create an SSL certificate with alternative DNS names:

1. In the administration interface, go to **Definitions** → **SSL Certificates**.
2. Click **Add** → **New Certificate** or **Add** → **New Certificate Request**.
3. In the **New Certificate** or **New Certificate Request** dialog box, type the name for the certificate.
4. In the **Hostname** field, type the hostname of any of your web servers placed behind the reverse proxy.
5. In the **Alternative hostnames** field, type the other web server hostnames.
Use semicolon (;) to separate the hostnames.
6. You may type the **City**, **State or Province**, and select **Country** and **Validity** of the certificate.
7. Click **OK**.
8. In the main window, click **Apply**.



New Certificate

Name:

Hostname:

Alternative hostnames:

Use semicolons (;) to separate individual hostnames.

Organization name:

Organization unit:

City:

State or Province:

Country: ▼

Valid for: ▼

OK Cancel



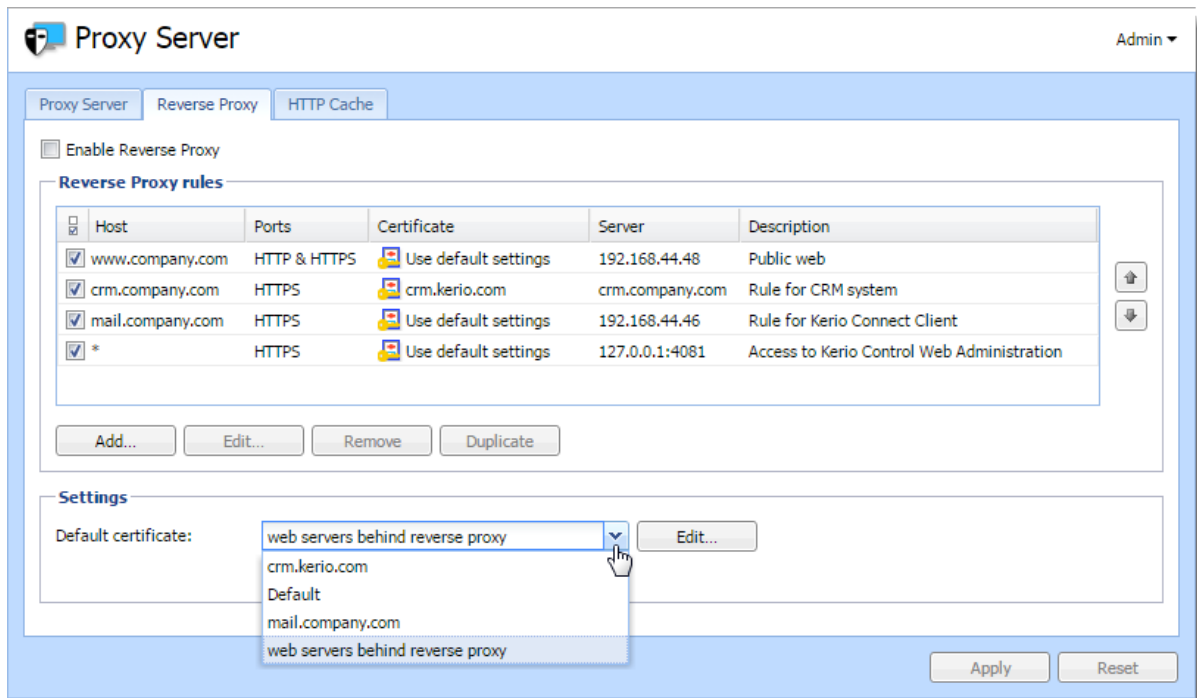
If you want to use a certificate signed by a certification authority, you must [export the certificate request from Kerio Control](#) and send it to the certification authority.

Once you've created the SSL certificate with alternative DNS names, you can use it as a default certificate:

1. In the administration interface, go to **Proxy Server** → **Reverse Proxy**.
2. Change **Default certificate** to the certificate with alternative DNS names.

Your result should be similar to what is shown below.

Configuring the reverse proxy



Configuring HTTP cache for the reverse proxy

1. In the administration interface, go to **Proxy Server** → **HTTP Cache**.
2. Check **Enable cache for Kerio Control reverse proxy**.
3. Click **Apply**.

For more details about HTTP cache in Kerio Control, read the [Configuring HTTP cache](#) article.

Configuring antivirus protection

Antivirus protection 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, 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). Check of outgoing traffic causes problems with temporarily undeliverable email.

- If a substandard port is used for the traffic, corresponding [protocol inspector](#) will not be applied automatically. In that case, define a service which will allow this traffic using a protocol inspector.

Configuring antivirus protection

1. In the administration interface, go to **Antivirus**.
2. On tab **Antivirus Engine**, select option **Use the integrated antivirus engine**

This option is available if the license key for Kerio Control includes a license for the Sophos antivirus module or in trial versions.

3. Select option **Check for update every ... hours**.

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

Configuring antivirus protection



If the update attempt fails, detailed information will be logged into the Error log.

4. Check protocols HTTP, FTP and POP3 in the **Protocols** section.

For advanced options, go to the following tabs:

- HTTP, FTP Scanning — see article [Configuring HTTP and FTP scanning](#)
 - Email Scanning — see article [Configuring email scanning](#)
5. SMTP scanning is disabled by default. You can enable it for inbound connections. However, if you use [Kerio Connect with greylisting](#), do not enable SMTP scanning.
 6. 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. It might happen that the connection over which the file is transferred is interrupted when the time limit is exceeded.



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.

7. Click **Apply**.

Using DHCP module

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.

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 groups **Trusted/Local Interfaces**, **Guest Interfaces** and **Other Interfaces**. This implies that the only thing to do is actually to run the DHCP server.

Automatic configuration of scopes

By default, the DHCP server works in the mode of automatic configuration of scopes.

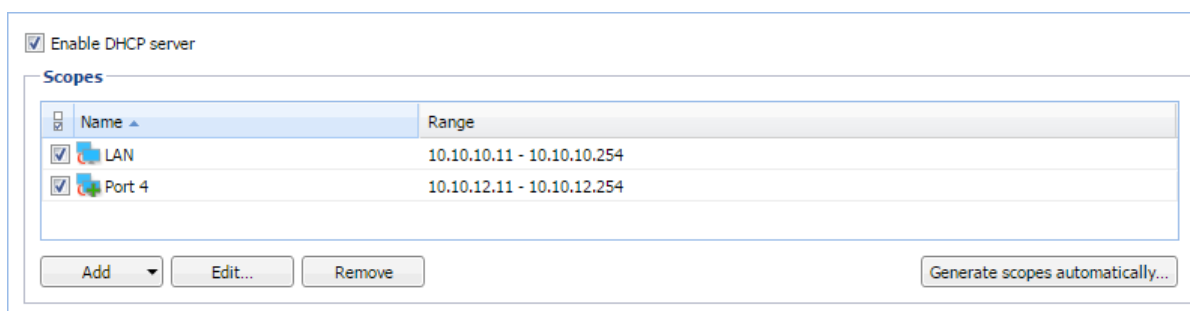


Figure 1 Section DHCP — Automatic configuration of scopes

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**, **Guest Interfaces** and **Other 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 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 respond 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 within each subnet. To create exclusions from this scope (for example for a group of servers with static IP addresses), follow these instructions:

1. In the **Edit Scope** dialog, click **Exclusions**.
2. In the **Exclusions** dialog, click **Add**.
3. Add **From** and **To** IP addresses.

Example

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

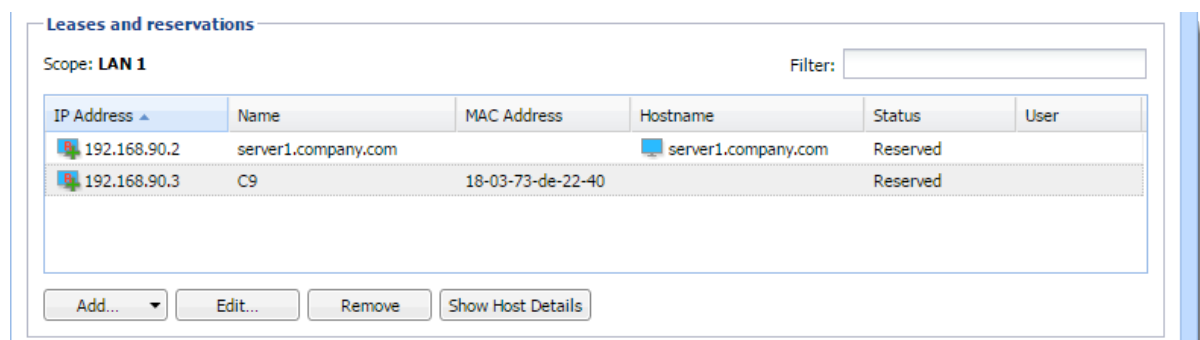
Scopes can be viewed in the **Leases and reservations** table.

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.



IP Address	Name	MAC Address	Hostname	Status	User
192.168.90.2	server1.company.com		server1.company.com	Reserved	
192.168.90.3	C9	18-03-73-de-22-40		Reserved	

Figure 2 Section DHCP — Leases and reservations

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.

Making a DHCP reservation in Active Hosts

You can reserve an IP address for a MAC address without typing it, if [Kerio Control is able to see the MAC address of the host](#):

1. In the administration interface, go to **Status → Active Hosts**.
2. Select a host.
3. Right-click on the selected user and click **Make DHCP Reservation by MAC**.
Kerio Control opens a window with information about the new configuration.
4. Click OK.

DHCP server of Kerio Control reserves the MAC address, if the DHCP server in Kerio Control is enabled and a scope of IP addresses is created on the interface.



If you use [Kerio Control MAC Filter](#), check the **Also permit MAC addresses used in DHCP reservations or automatic user login** option.

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

Kerio Control includes a [DNS](#) server. We recommend to configure the DNS server module with DHCP server module in Kerio Control together. Configuration and administration is simple and responses to repeated DNS queries will be fast.



In case of Active Directory environments, Kerio Control will forward DNS queries to the internal Domain Name Server if Kerio Control is joined to 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 hostnames found in the DHCP lease table.
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.
There are two reasons for that:

- DNS names in the [Hosts table](#) can be specified without the local domain (for example `jsmith-pc`). The DNS module can complete the query with the local domain.
- A host can send the DNS query in the `jsmith-pc.example.com` format. If the DNS module knows the local domain `example.com`, the name is divided and read: host: `jsmith-pc` and local domain: `example.com`

6. Click **Apply**.

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.

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:

```
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:

```
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.

Using the DNS module

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:

- Common DNS queries (A queries),
- Reverse queries (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.
 6. Save the settings and create another rule if it is needed.

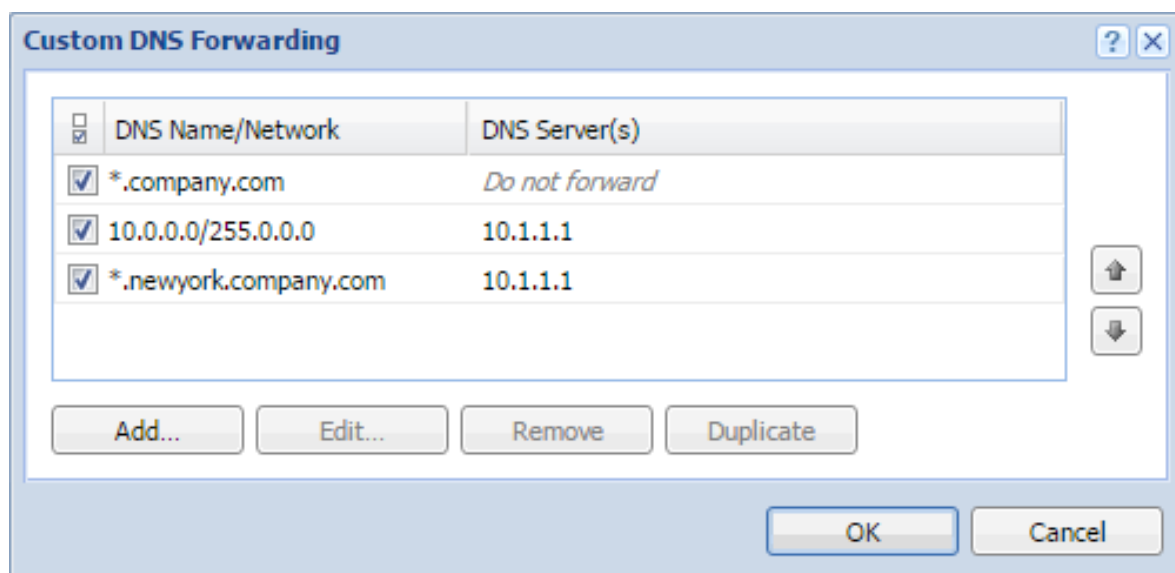


Figure 1 Custom DNS forwarding

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 in Kerio Control

Overview

Kerio Control allows you to view and edit the IPv4 and IPv6 routing tables. Kerio Control works with the operating system's routing table as well as with the static routes created in Kerio Control.

To modify the routing table, in the administration interface, go to the **Routing Table** section. Note separate tabs for IPv4 and IPv6.



If multiple Internet links are in network load balancing mode, Kerio Control displays only a single default route which is routed through the link with the highest link weight.

Routing Table Admin ▾

IPv4 Routing Table IPv6 Routing Table

Active routing table

Name	Network ▴	Mask	Gateway	Interface	Metric
System route	0.0.0.0	0.0.0.0	192.168.62.1	Ethernet	0
VPN route	172.26.27.0	255.255.255.0		VPN Server	0
VPN tunnel in CISCO router to San Jose division	192.168.61.0	255.255.255.0	192.168.94.1	Ethernet 2	1
System route	192.168.62.0	255.255.255.0		Ethernet	0
System route	192.168.94.0	255.255.255.0		Ethernet 2	0

Static routes

Name	Network ▴	Mask	Gateway	Interface	Metric
<input checked="" type="checkbox"/> VPN tunnel in CISCO router to San Jose division	192.168.61.0	255.255.255.0	192.168.94.1	Ethernet 2	1

Add... Edit... Remove

Apply Reset

Figure 1 Routing Table

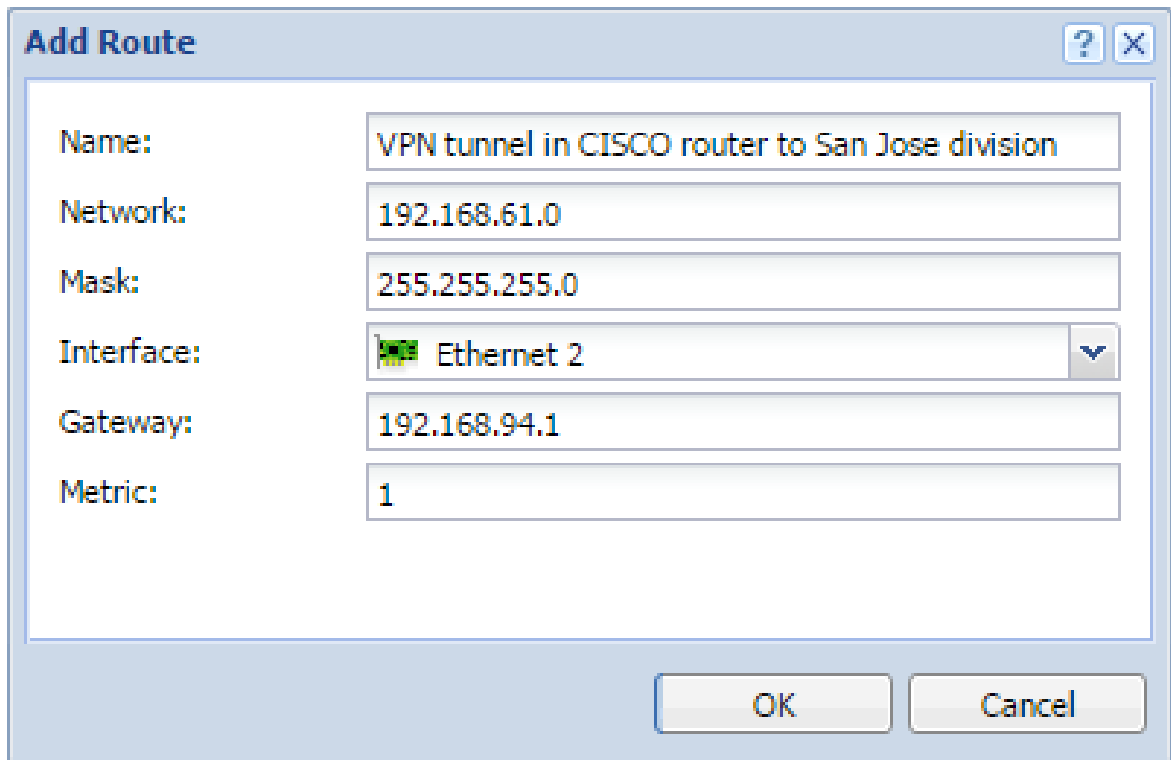
Route types

The following route types are available:

- **System routes** — These routes are downloaded from the operating system's routing table. You cannot edit or remove the system routes.
- **VPN routes** — These routes are visible in the table in the **Interfaces** column when tunnels are in the Up state. Kerio Control shows all routes configured in IPsec VPN tunnel settings and all routes accessible behind the Kerio VPN tunnel. To create VPN routes, go to the **Interfaces** section, (See the articles [Configuring IPsec VPN tunnel](#) and [Configuring Kerio VPN tunnel](#).).
- **Static routes** — Kerio Control saves static routes to the configuration file and adds them to the system routing table. You can add, modify, remove or temporarily disable these routes.

Modifying static routes in the IPv4 routing table

1. In the administration interface, go to **Routing Table** → **IPv4 Routing Table**.
2. Click **Add**.
3. In the **Name** field, type the route name.
4. In the **Network** field, type an IP subnet.
5. In the **Mask** field, type a mask defining the subnet.
6. In the **Interface** menu, select the interface.
7. In the **Gateway** field, type the IP address of the gateway (if necessary).
8. In the **Metric** field, type the number that defines the route's priority.



Add Route

Name: VPN tunnel in CISCO router to San Jose division

Network: 192.168.61.0

Mask: 255.255.255.0

Interface: Ethernet 2

Gateway: 192.168.94.1

Metric: 1

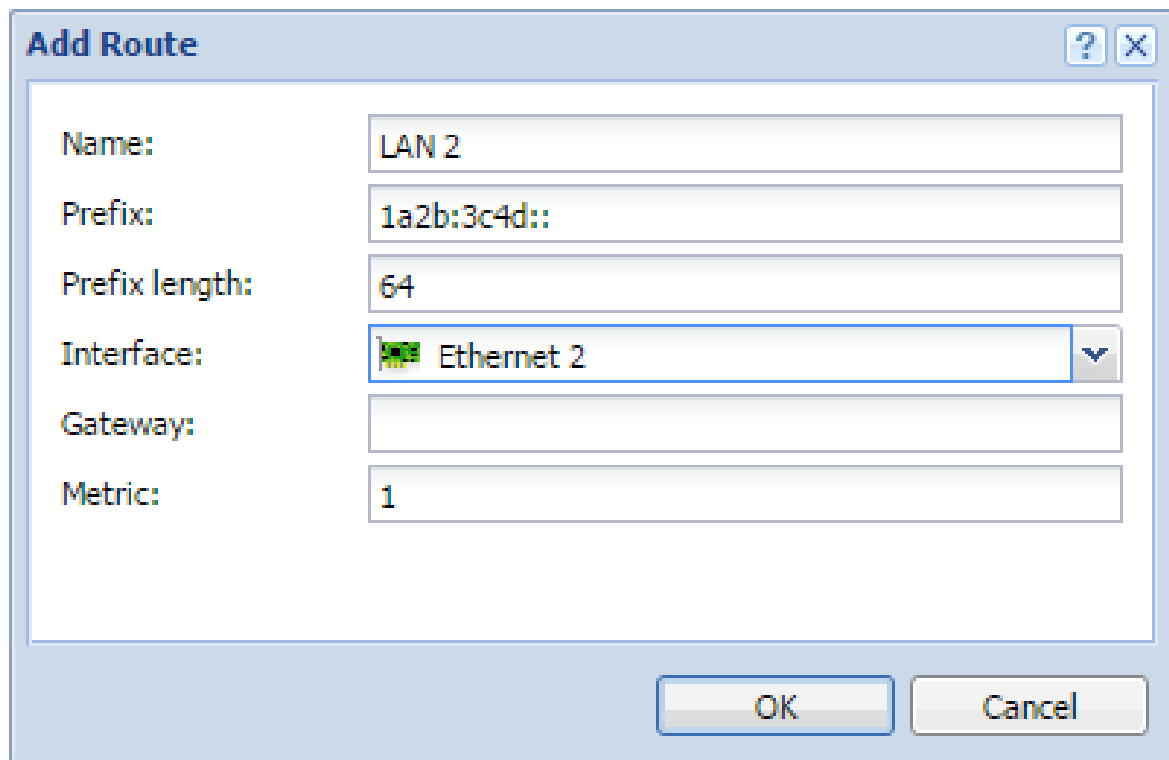
OK Cancel

Modifying routes in the IPv6 routing table




New in Kerio Control 8.6!

1. In the administration interface, go to **Routing Table** → **IPv6 Routing Table**.
2. Click **Add**.
3. In the **Name** field, type the route name.
4. In the **Prefix** field, type an IP subnet.
5. In the **Prefix length** field, type a prefix.
6. In the **Interface** menu, select the interface.
7. In the **Gateway** field, type the IP address of the gateway (if it is necessary).
8. In the **Metric** field, type the number that defines the route's priority.



The image shows a 'Add Route' dialog box with a light blue border and a title bar containing a question mark and a close button. The dialog contains several input fields for configuring a route. The 'Name' field is labeled 'Name:' and contains the text 'LAN 2'. The 'Prefix' field is labeled 'Prefix:' and contains the text '1a2b:3c4d::'. The 'Prefix length' field is labeled 'Prefix length:' and contains the text '64'. The 'Interface' field is labeled 'Interface:' and is a dropdown menu showing 'Ethernet 2' with a small icon to its left and a downward arrow to its right. The 'Gateway' field is labeled 'Gateway:' and is currently empty. The 'Metric' field is labeled 'Metric:' and contains the text '1'. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

Name:	LAN 2
Prefix:	1a2b:3c4d::
Prefix length:	64
Interface:	 Ethernet 2 ▼
Gateway:	
Metric:	1

OK Cancel

Using alert messages

Overview

Kerio Control can send automatic email messages (alerts) about important events. You can specify:

- Default alert language
- Recipients
- Alert types
- Timing



Ensure your Kerio Control is connected to an SMTP server for sending alerts.

Configuring alerts

1. In the administration interface, go to **Advanced Options** and [connect Kerio Control to your SMTP server](#).
2. Go to **Accounting and Monitoring** → **Alert Settings**.
3. Select a default language for alerts.
4. Click **Add**.
5. In the **Add Alert** dialog box, select a Kerio Control user or type an email address.
6. Select the type of alert you want to create:
 - [System alert](#) — You can choose from many types of system alerts, as described below.
 - Traffic rule alert — You can create alerts for traffic rules.
 - Content rule alert — You can create alerts for content rules.
 - [Log message alert](#) — You can create custom log message alerts for administrators, as described below.

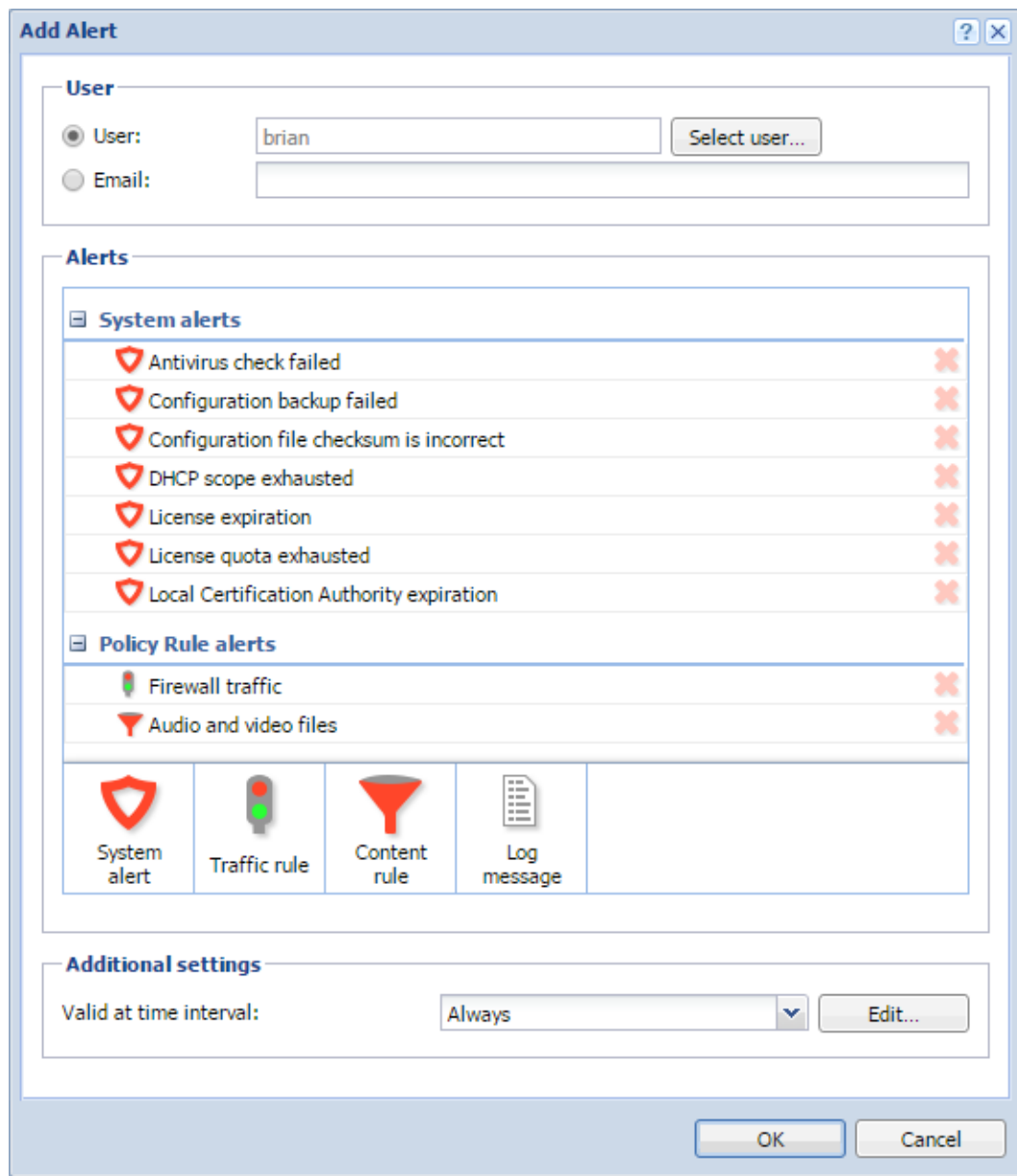


Figure 1 Add Alert dialog

7. Configure the alert and click **OK**.

The **Add Alert** dialog displays the list of active alerts, grouped by type.

You can add more particular alerts for a selected recipient.

8. When you have finished adding alerts, select a [time interval](#) in which Kerio Control sends the alerts.

See [Creating time ranges in Kerio Control](#).

9. Save your settings.

Kerio Control sends alerts to the selected user. If you need to set up alerts for other users, you can do it in the same way, as shown below.

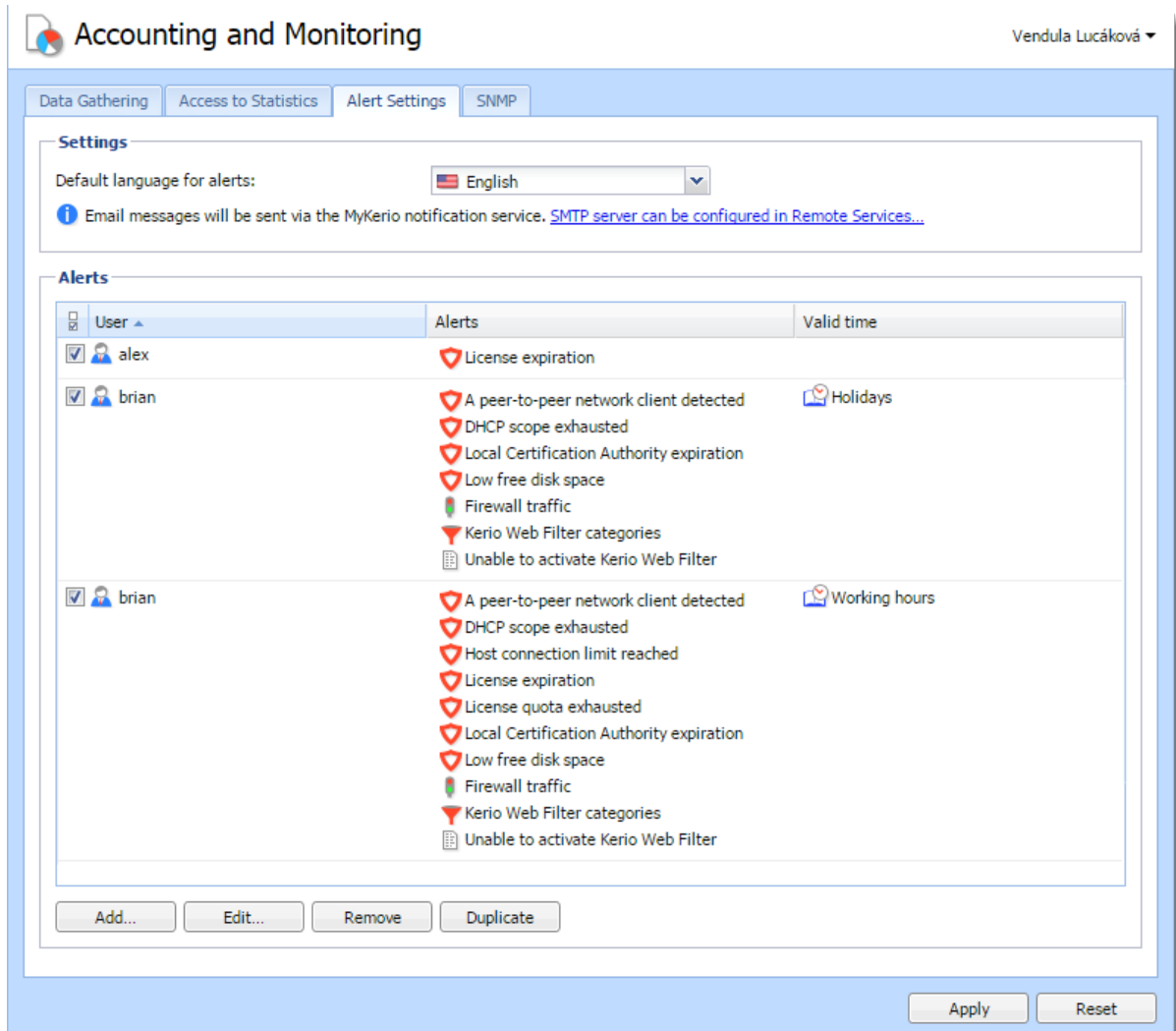


Figure 2 Alert Settings dialog

System alerts

You can add the following system alerts:

- **A peer-to-peer network client detected** — Kerio Control sends this alert when users start using P2P. The alert includes information about IP address, resolution (P2P was blocked or traffic was slowed down), and so on.
- **Antivirus check failed** — Kerio Control sends this alert when the antivirus engine fails to check files (typical for password-protected or damaged files).

- **Configuration backup failed** — Kerio Control sends this alert when configuration backup to Samepage or an FTP server fails. For details, see [Saving configuration to Samepage](#) and [Saving configuration to FTP server](#).
- **Configuration file checksum is incorrect** — Kerio Control sends this alert when someone changes any configuration file.
- **DHCP scope exhausted** — Kerio Control sends this alert when there are no free IP addresses in the DHCP scope. For more details, see [Using DHCP module](#).
- **Host connection limit reached** — Kerio Control sends this alert when hosts in the local network reach the connection limit (typical when a Trojan horse or spyware has infected the host).
- **Internet connectivity changed** — Kerio Control sends this alert when the Internet connection fails and the system switches to a secondary line, or vice versa.
- **License expiration** — Kerio Control sends this alert 7 days before the expiration of your Kerio Control license, Kerio Control Software Maintenance, Kerio Control Web Filter, or Sophos Antivirus software. The alert is sent daily until you renew the license.
- **License quota exhausted** — Kerio Control sends two alerts. The first email is sent when 90% of the quota is exhausted. The second email is sent when the quota is fully exhausted.
- **Local Certification Authority expiration** — Kerio Control sends this alert 7 days before expiration of the local certification authority (CA). You should check the expiration date, create a new local CA, and distribute it to users' browsers.

Select this option, if your users use HTTPS filtering because they have a local CA installed in their browsers. For more information, see [Filtering HTTPS connections](#).

- **Low free disk space/memory warning** — Kerio Control sends this alert when the Kerio Control host has less than 300 MB of free disk space and less than 200 MB of free memory available.

Kerio Control needs enough disk space to be able to save logs, statistics, configuration settings, temporary files (e.g. an installation archive of a new version or a file that is currently scanned by an antivirus engine) and other information. Whenever the Kerio Control administrator receives such an alert message, they should immediately take appropriate action.

- **New version available** — A new version of Kerio Control has been detected on the Kerio Technologies server during an update check.
- **RAS line status changed** — This alert is sent when a line (PPPoE, PPTP or L2TP interface) is dialed or hung up. The alert message includes a name of the line and type

of dialing (manually from the administration interface, automatically in the configured time range, etc.).

- **User transfer quota exceeded** — A user has reached their daily, weekly or monthly user transfer quota, and Kerio Control has responded by taking the designated action.



If you want to send an alert to the user, edit the quota settings of the corresponding user or domain template.

- **VPN tunnel status changed** — This alert works for the Kerio Control VPN tunnel and the IPsec VPN tunnel. Kerio Control sends the alert when status of the tunnel is changed from **Up** to **Down** or from **Down** to **Up**.
- **Virus detected** — The antivirus engine has detected a virus in a file transmitted by HTTP, FTP, SMTP, or POP3.



If you want to send an alert to the user, go to **Antivirus** → **HTTP, FTP scanning**, and select **Alert the client**.

Sending log message alerts

For information on log message alerts, read the article [Sending log message alerts](#)

Viewing alerts

To view all generated Kerio Control system alerts, go to **Status** → **Alert Messages**. Alerts are displayed in the language chosen for the administration interface.

The left side of the **Alerts** section lists all alerts sorted by date and time. Each line provides information on one alert:

- **Date** — Date and time of the event,
- **Alert** — Event type.

Alert log

All system alert messages are recorded in the **Alert** log.

The **Alert** log provides a complete history of system alerts generated by Kerio Control: 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 the alert type (in capitals). The other information varies by alert type.

Sending log message alerts

Overview

Kerio Control can send alerts to predefined email addresses when a condition you have defined matches the text in a particular log.

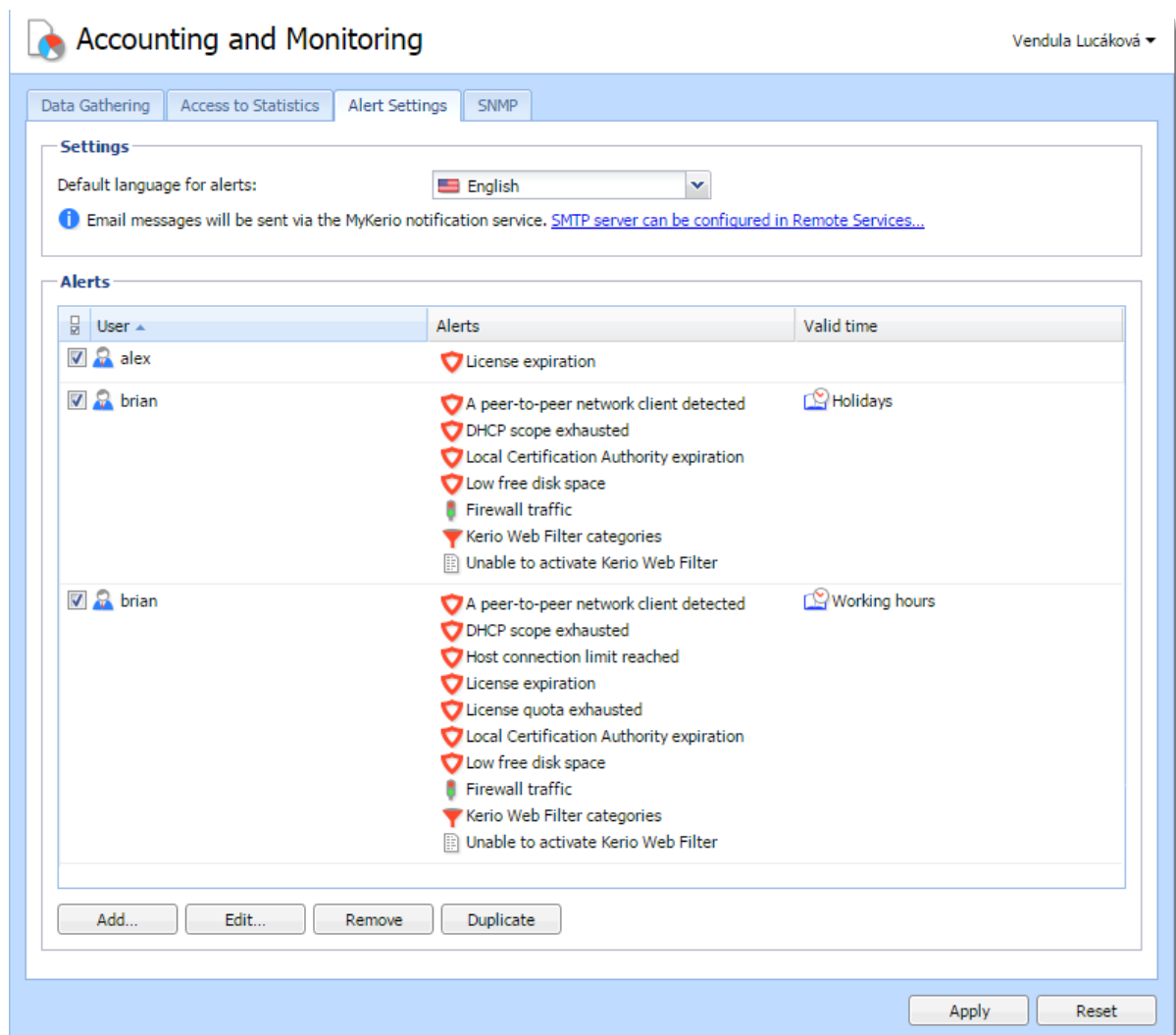
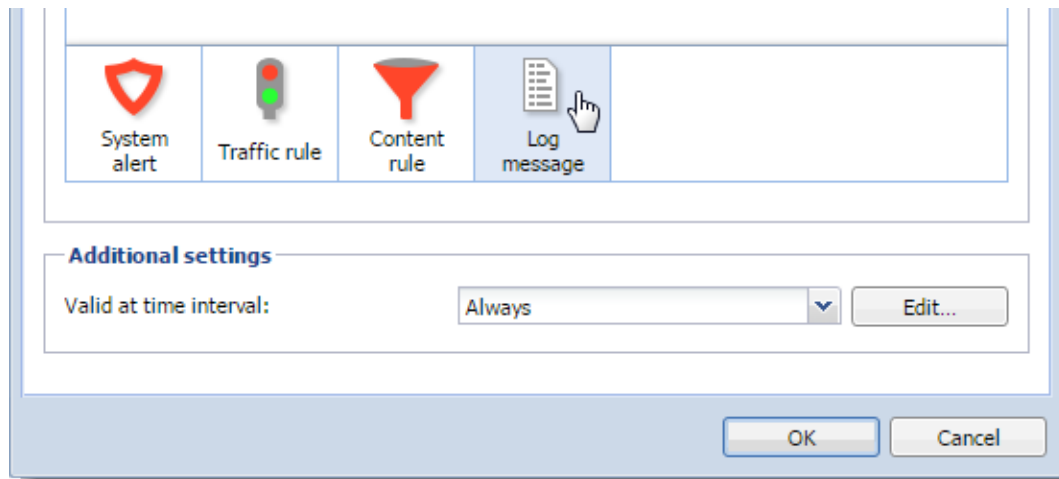


Figure 1 Add Alert dialog

Adding rules for log message alerts

1. In the administration interface, go to **Accounting and Monitoring** → **Alert Settings** and click **Add**.
2. In the **Add Alert** dialog, click **Log message**.

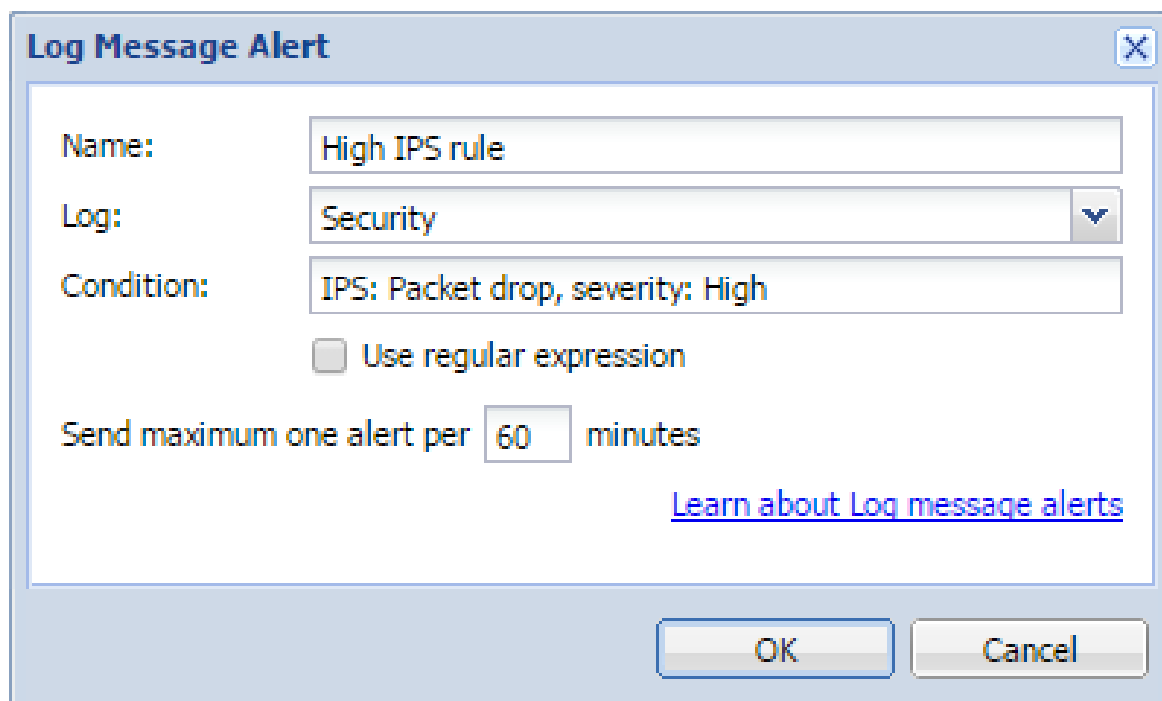


3. In the **Log Message Alert** dialog box, type a name for the alert.
The name appears in the subject line of the email message the alert sends.
4. From the **Log** menu, select the log type.
5. In the **Condition** field, type the text string you want Kerio Control to search for.
Kerio Control compares the string to the text in the log, and when it finds a match, sends the alert to the designated email address.
6. Select **Use regular expression** if the string in the **Condition** field is a regular expression.
Kerio Control uses Perl regular expression syntax. For the complete specification, go to <http://www.boost.org>.
7. Set a time interval for sending the alert.
Some events in Kerio Control happen often. Limit the interval to once per hour or per day to avoid getting too many messages in your mailbox.
8. Click **OK**.

Kerio Control sends the alert whenever the condition matches a text string in the log.

Examples of log alerts

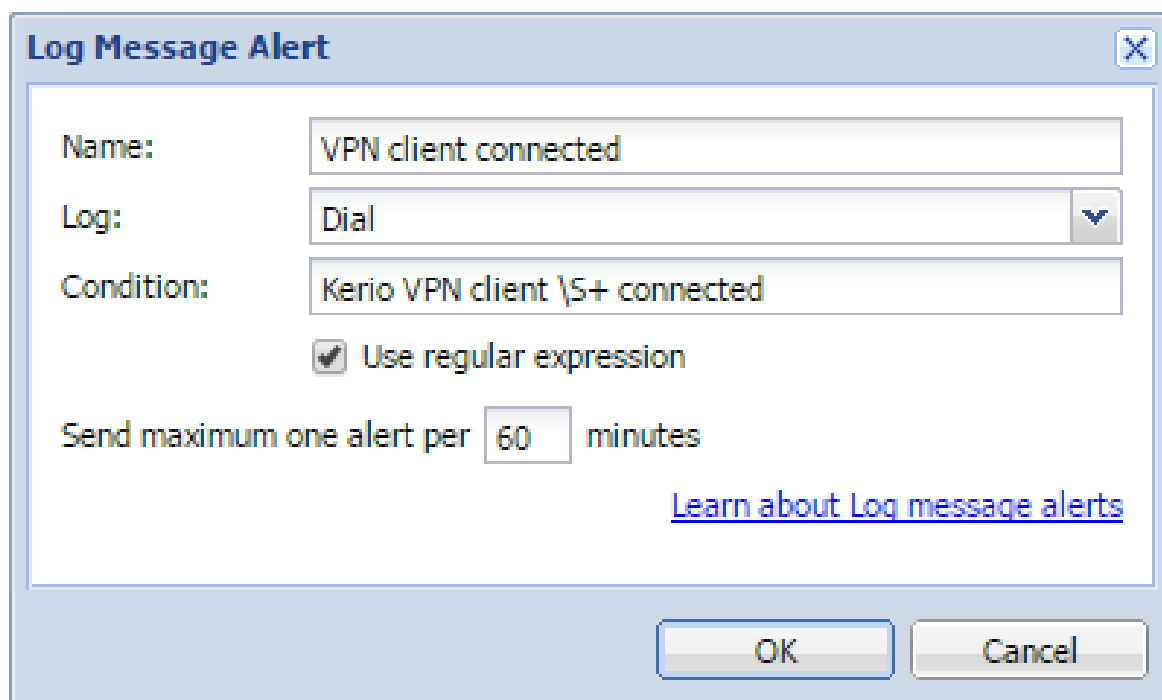
High severity IPS events



The dialog box is titled "Log Message Alert" and has a close button (X) in the top right corner. It contains the following fields and controls:

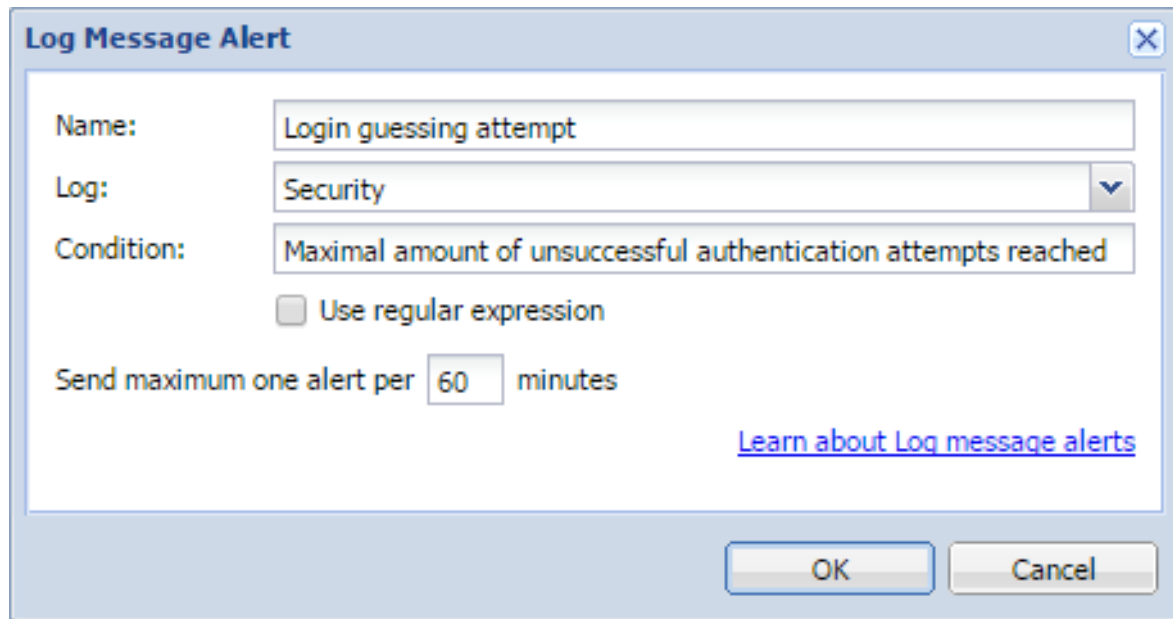
- Name:** A text box containing "High IPS rule".
- Log:** A dropdown menu with "Security" selected and a downward arrow.
- Condition:** A text box containing "IPS: Packet drop, severity: High".
- ☐ Use regular expression
- Send maximum one alert per** **minutes**
- [Learn about Log message alerts](#)
- OK** and **Cancel** buttons at the bottom right.

VPN client connected (regular expressions)



The dialog box is titled "Log Message Alert" and has a close button (X) in the top right corner. It contains the following fields and controls:

- Name:** A text box containing "VPN client connected".
- Log:** A dropdown menu with "Dial" selected and a downward arrow.
- Condition:** A text box containing "Kerio VPN client \\S+ connected".
- ☒ Use regular expression
- Send maximum one alert per** **minutes**
- [Learn about Log message alerts](#)
- OK** and **Cancel** buttons at the bottom right.

Login guessing attempt

The image shows a 'Log Message Alert' dialog box with a light blue border and a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing 'Login guessing attempt'.
- Log:** A dropdown menu with 'Security' selected and a downward arrow on the right.
- Condition:** A text input field containing 'Maximal amount of unsuccessful authentication attempts reached'.
- ☐ Use regular expression
- Send maximum one alert per** **minutes**
- A blue hyperlink: [Learn about Log message alerts](#)
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Configuring statistics and reports

Overview

Kerio Control provides detailed statistics on user activity, volume of transferred data, visited websites and web categories. This information helps you understand the browsing activities and habits of individual users. You can choose from the following options:

- Each user can access their personal statistics through the Kerio Control Statistics interface.
- Managers can access the statistics of their subordinates.
- Kerio Control can send automated statistics reports to users and/or managers.
- Kerio Control can gather statistics for communications between local networks and the Internet.

This article discusses the configuration in the Kerio Control administration interface.

Prerequisites

- The firewall requires user authentication. You can set user authentication in **Domains and User Login** → **Authentication Options**.
- The HTTP protocol inspector applies to any HTTP traffic. Kerio Control sets this condition by default, but you can disable the protocol inspector for specific traffic rules.

To gather statistics from secure traffic, configure the [filtering of HTTPS connections](#).

- Kerio Control includes web categories when using [the Kerio Control Web Filter module](#). To ensure all sites are categorized, select the **Categorize each page regardless of URL rules** option in the **Content Filter** → **Kerio Control Web Filter** section.

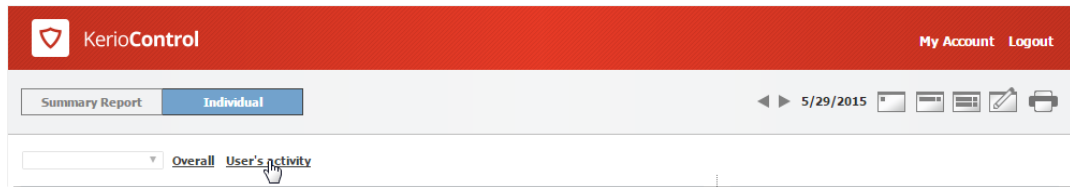
Settings for statistics, reports and quota

1. In the administration interface, go to **Accounting and Monitoring** → **Data Gathering**.
2. Enable **Gather internet usage statistics**.

Statistics settings also affect the monitoring of the volume of transferred data against user quotas. If you deselect the **Gather internet usage statistics** option, Kerio Control cannot count the transferred data against user quotas.

3. Enable or disable **Gather user's activity records**.

The option enables monitoring and logging of browsing activity of individual users (the **User's activity** tab in the Kerio Control Statistics web interface).



Please note that whether it is legal to gather users' activities varies by country. Before setting this option, be sure the laws in your jurisdiction permit it.

Disable this option to reduce demands on the firewall and save server disk space.

4. Use the **Delete statistics older than** parameter to specify how long the data will be kept. To save disk space, keep statistics only as long as necessary.



Kerio Control tries to optimize size of the statistic database and volume of processed data. The greatest volume of data is generated by statistics of visited websites. Therefore, Kerio Control keeps daily statistics of visited websites only for the last 40 days. Weekly and monthly statistics are available for the entire data storage period as set in the configuration (2 years by default).

5. To gather statistics data for one or more user group, select them in the **Gather group statistics for these groups** field. See the [Using group statistics](#) section.
6. Set the first day of the week and month in the **Accounting periods for statistics and quota** section.

For example, a month can start on day 15 of the calendar month and end on day 14 of the following month.

The first day of the month also sets when the monthly transferred data counter of individual users is set to zero.

Configuring statistics and reports

The screenshot shows the 'Accounting and Monitoring' window with the 'Data Gathering' tab selected. The 'Admin' user is logged in. The 'Data Gathering' tab contains several sections:

- Gather internet usage statistics:** A checkbox is checked.
- Statistics:**
 - Gather user's activity records:** A checkbox is checked.
 - Delete statistics older than:** A text box contains '24' and a dropdown shows 'month(s)'.
 - Gather group statistics for these groups:** A text box contains 'Statistics for Development dept., Statistics for Sales d' and a 'Select...' button.
 - Delete all statistics data...:** A button.
- Accounting periods for statistics and quota:**
 - First day of week:** A dropdown shows 'Monday'.
 - First day of month:** A text box contains '1'.
- Accounting exceptions:**
 - Account traffic only in the given time interval:** A dropdown shows 'Working hours' and an 'Edit...' button.
 - Exclude website statistics for URLs which belong to:** A dropdown shows 'Automatic Updates' and an 'Edit...' button.
 - Exclude traffic to/from IP addresses which belong to:** A dropdown shows 'Web servers' and an 'Edit...' button.
 - Exclude the following users from statistics:** A text box contains 'asmith, fdavies' and a 'Select...' button.

At the bottom right, there are 'Apply' and 'Reset' buttons.

Figure 1 Accounting and Monitoring section — Data Gathering tab

Using group statistics

Kerio Control can gather and display collective Internet usage statistics for groups of users. To do this:

1. Create groups in the **Users and Groups** → **Groups** section.
2. On the **Accounting and Monitoring** → **Data Gathering** tab, add these groups to the **Gather group statistics for these groups**.
3. On the **Accounting and Monitoring** → **Access to Statistics** tab, add access rights for displaying data.

Accounting exceptions

You can configure Kerio Control to exclude certain types of data from the statistics that are gathered:

- **Account traffic only in the given interval** — defines a time period for gathering statistics and quota (for example, during working hours).
- **Exclude website statistics for URLs which belong to** — defines a URL group (for example, you might want to exclude your own web servers from the statistics).

Use wildcards in URL groups items to define exceptions for particular pages or for all pages on a particular server, all web servers in a domain, etc.

Kerio Control applies URL exceptions only to unsecured web pages. If you want apply it also to secured web pages, configure the [filtering of HTTPS connections](#).

- **Exclude traffic to/from IP addresses which belong to** — defines IP addresses of hosts which are excluded from the statistics and to which quota is not applied.
- **Exclude the following users from statistics** — turns off data collection for the specified users. This setting takes priority over any other quota settings in user or group preferences.

Setting access rights and email reports

Users can see their own statistics in their Kerio Control Statistics accounts. For more information, see [Using the Kerio Control Statistics interface](#).

To access the Kerio Control Statistics login page, use the URL from the **Accounting and Monitoring** → **Access to Statistics** tab.

In the **Accounting and Monitoring** → **Access to Statistics** section, you also have these options:

- **Show user names in this format** , which sets the format for user names in Kerio Control Statistics.
- **Default email report language**, which enables you to select the language to use for email reports.



Kerio Control allows you to send statistics by email. To send email reports, set a server for outgoing email messages under **Remote Services** → **SMTP Relay**.

Configuring statistics and reports

The screenshot shows the 'Accounting and Monitoring' administration interface. The 'Access to Statistics' tab is selected. The 'Settings' section includes a URL for internet usage statistics, a dropdown for user names format, and a dropdown for default email report language. The 'Access rights and email reports' section contains a table with columns for User, Online access, Data, and Regular email reports. The 'User access' section has checkboxes for online statistics access and email report intervals.

Accounting and Monitoring Admin ▾

Data Gathering Access to Statistics Alert Settings SNMP

Settings

Internet usage statistics are available at <https://192.168.94.149:4081/>

Show user names in this format:

Default email report language:

❗ Email messages will be sent via the MyKerio mail service. [SMTP server can be configured in Remote Services...](#)

Access rights and email reports

User	Online access	Data	Regular email reports
<input checked="" type="checkbox"/> Admin	Allowed	All Data	
<input checked="" type="checkbox"/> asmith	Allowed	Group statistics: Statistics for Sales dept.	Weekly

Add... Edit... Remove More Actions ▾

User access

☒ Users can access their own statistics online

Users receive their own individual email reports:

☐ Daily ☒ Weekly ☐ Monthly

Apply Reset

Allowing users to see their own statistics

1. In the administration interface, go to **Accounting and Monitoring** → **Access to Statistics**.
2. Select **Users can access their own statistics online**.
3. (Optional) To send statistics to users by email, select the appropriate interval: **Daily**, **Weekly** or **Monthly**.
4. Click **Apply**.

Allowing managers to see other users and group statistics

1. In the administration interface, go to **Accounting and Monitoring** → **Access to Statistics**.
2. In the **Access rights and email reports** section, click **Add**.

3. In the **Access Rights and Email Reports** dialog box, select the manager you want to grant the rights to.

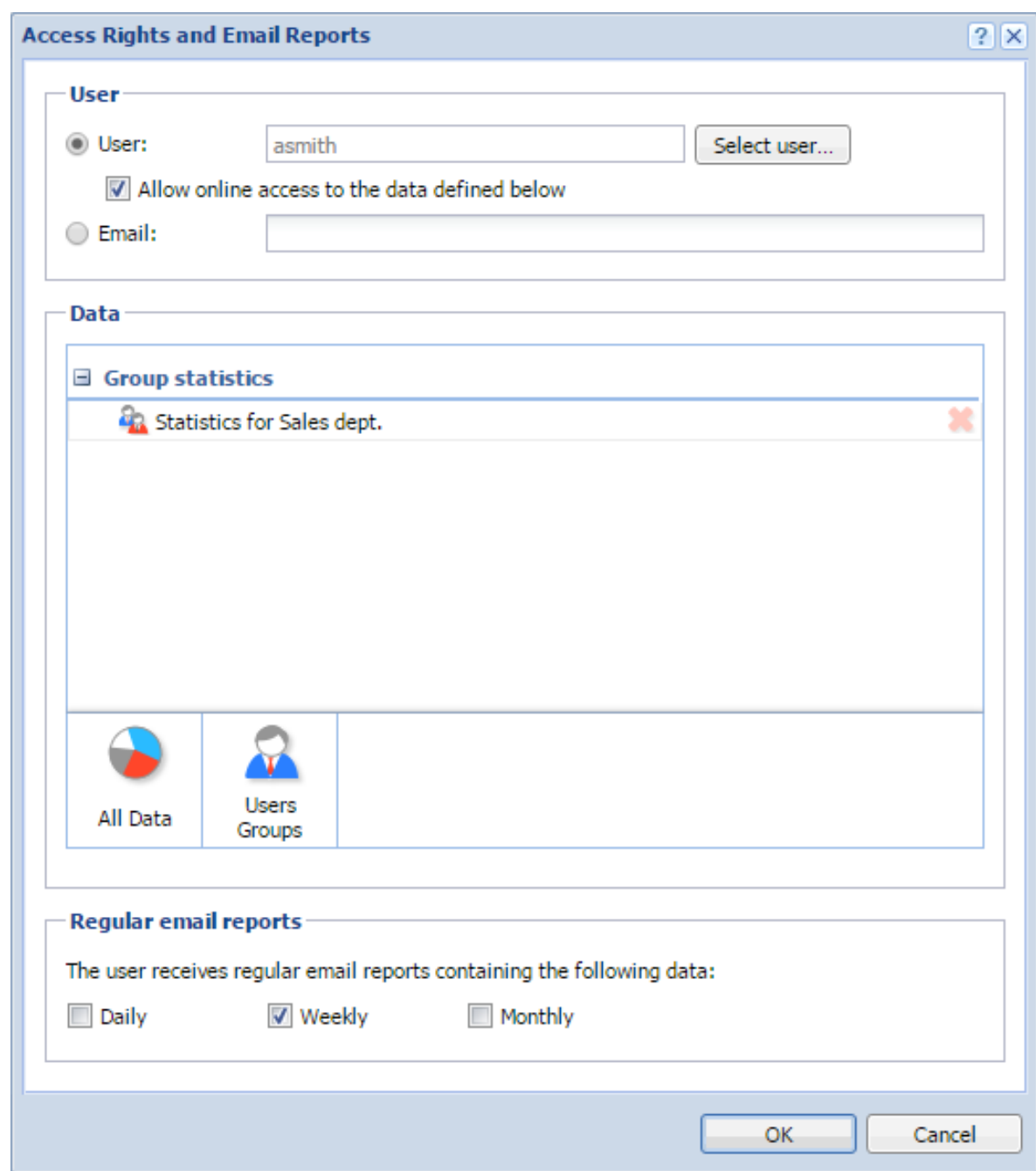
Alternatively, you can add their email address if they do not have an account in Kerio Control.

4. Select **Allow online access to the data defined below** to display data in the manager's Kerio Control account.
5. In the **Data** section, select whose data the manager can see:
 - **All data** — The manager can display statistics of all authenticated, unauthenticated and guest users from all guest interfaces.
 - **Users/Groups** — The manager can display statistics of only individual users or user groups.
6. In the **Regular email reports** section, you can have a daily, weekly or monthly report sent from Kerio Control Statistics.



In the administration interface, go to **Users and groups** → **Users** and verify that the user has a valid email address set.

7. Save your settings.



The dialog box is titled "Access Rights and Email Reports" and contains three main sections: "User", "Data", and "Regular email reports".

User



☒ **User:**



☒ Allow online access to the data defined below

☐ **Email:**

Data

☒ **Group statistics**

 Statistics for Sales dept. 

All Data Users Groups

Regular email reports

The user receives regular email reports containing the following data:

☐ Daily ☒ Weekly ☐ Monthly

Configuring system settings date, time, time zone and server name

System Configuration overview

The Kerio Control administration console allows setting of a few basic parameters of the firewall's operating system.

Configuring date and time

Many Kerio Control features (user authentication, logs, statistics, etc.) require correct setting of date, time and time zone on the firewall. Kerio Control allows manual settings or synchronization with an NTP server (recommended).

1. In the administration interface, go to **Advanced Options → System Configuration**.

2. Select option **Keep synchronized with NTP server**.

Date and time can be set manually but it is better to use an NTP server which provides information about the current time and allows automatic management of the firewall's system time.

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.

3. Click **Apply**.

Configuring time zone

1. In the administration interface, go to **Advanced Options → System Configuration**.

2. Select a time zone from the **Server time zone** list.

3. Click **Apply**.

The current date and time will be changed according to the new time zone.

Configuring the server name

The default Kerio Control hostname is `control`. To change the hostname [connect to a directory service](#) or change the web interface URL in the **Advanced Options** → **Web Interface** tab.

Upgrading Kerio Control

Using update checker

Once you purchase Kerio Control or extend your [Software Maintenance](#), you are eligible to receive new versions of Kerio Control and its components as soon as they are available.

To get notified about new versions of Kerio Control, [configure Alert Settings](#).

Checking new versions

For immediate check of new versions, click **Check Now**. If you want to configure automatic checking new versions, read the following steps:

1. In the administration interface, go to section **Advanced Options** → **Software Update**.
2. Select option **Periodically check for new versions**.

Kerio Control checks for updates every 24 hours.

Once a new version is available, the **Software Update** tab will display a link to the download page.

3. You can also select the **Check also for beta versions** option.

If Kerio Control is used in production, we do not recommend enabling this option.

4. Click **Apply**.

From now on, Kerio Control checks new versions.

Automatic upgrade of Kerio Control



New in Kerio Control 9.1!

Kerio Control allows you to set automatic downloads and upgrades to a new version.

The Kerio Control upgrade workflow starts with checking for updates. If a new version is available, Kerio Control downloads it. Then Kerio Control waits for the **Upgrade window** time range. By default, the time range is set on Friday night. During this interval, Kerio Control upgrades to the new version.

Upgrading Kerio Control

To enable and configure automatic upgrade:

1. In the administration interface, go to **Advanced Options** → **Software Update**.

2. Select option **Periodically check for new versions**.

Kerio Control checks for updates every 24 hours.

Once a new version is available, the **Software Update** tab will display a link to the download page.

3. Select **Download and upgrade to new versions automatically in given time interval** for automatic upgrade.

The time interval is set in **Time Ranges** and you can adjust it to your schedule. For more information, read [Creating time ranges in Kerio Control](#).

4. You can also select the **Check also for beta versions** option.

Kerio Control downloads and upgrades to new beta versions automatically.

If Kerio Control is used in production, we do not recommend enabling this option.

5. Click **Apply**.

From now on, Kerio Control downloads new versions of Kerio Control and in the given interval upgrades to the new version.

Configuring email alerts

Kerio Control allows you to set email alert when a new version is available. For more information, read [Using alert messages](#).

When a new version is available, email alert

go to **Accounting and Monitoring** → **Alert Settings**. Select the **New version available** check box.

Manually uploading a binary image file

This procedure might be useful for the following situations:

- downgrade of Kerio Control
- upgrade to a custom version (e.g. beta version)

If you have prepared the upgrade image file, you can upload it manually:

1. In the administration interface, go to section **Advanced Options** → **Software Update**.
2. Click the **Select File** button.

3. Select the upgrade image file (`kerio-control-upgrade.img`).
4. Wait for uploading the file.
5. Click the **Start Upgrade** button.

Wait for the upgrade and restart of Kerio Control.

When the restart is finished, your Kerio Control is up-to-date.

Upgrade with USB tools

In case that it is not possible to update Kerio Control via the administration interface, Kerio Control Box can be updated from a USB flash drive. For more information, read the [Kerio Control Box - USB Tools](#) article.

Troubleshooting

If any problems regarding updates occur, check the **Debug** log — right-click the **Debug** log area and check **Messages** → **Update checker**.

Configuring the SMTP server

Configuring the SMTP Relay

Kerio Control does not provide any built-in SMTP server. If you want to get alerts, notifications, statistics and reports to your mailbox, use [MyKerio notification service](#) or configure an SMTP Relay Server.

By default, MyKerio notification service sends all emails from Kerio Control, but the amount of emails this service can send is limited per 24 hours. If you expect a large amount of emails from your appliance, use SMTP Relay instead.

If you want to use a common SMTP relay:

1. In the administration interface, go to **Remote Services** → **SMTP Relay**.
2. Select **SMTP server**.
3. In the **Server** field, type DNS name or IP address of the server.
If available, use an SMTP server within the local network (messages are often addressed to local users).
4. Select **Require SSL-secured connection**.
Kerio Control selects the best method available with this option enabled.
5. If the SMTP server requires authentication, type username and password at the specified SMTP server.
6. Specify an email address in the **Specify sender email address in the "From:" header** field.
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).
Preset From header does not apply to messages forwarded during antivirus check.
7. Click **Test**.
8. In the **Email Address** dialog, type your email address for testing the connection and click OK.
9. Click **Apply**.

Dynamic DNS for public IP address of the firewall

Overview

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 (DynDNS, no-ip.com or ChangeIP.com) and select a free host name for the domain (e.g. company.no-ip.com).
- 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.

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. 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.
2. 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.

Configuring DDNS

1. Create an account at the following DDNS provider:
 - *ChangeIP* (<http://www.changeip.com/>),
 - *DynDNS* (<http://www.dyndns.org/>),
 - *No-IP* (<http://www.no-ip.com/>).
2. In the administration interface, go to **Remote Services** → **Dynamic DNS**.

Dynamic DNS for public IP address of the firewall

3. Select option **Automatically update dynamic DNS service records with the firewall's IP address**.
4. Select a DDNS provider.
5. In the **Update hostname** field, type a DNS name.
If DDNS supports wildcards, they can be used in the host name.
6. Set username and password for access to updates of the dynamic record.
- 7.



New in Kerio Control 8.3!

If Kerio Control uses the multiple internet links mode (load ballancing or failover) you can choose how to identify IP addresses for your DDNS provider:

- **IP address configured on outgoing Internet interface** — Kerio Control always sends the IP address from the Internet interface to the DDNS provider.
- **Detected public IP address** — before sending the IP address to the DDNS provider, Kerio Control detects which IP address is used for access to the Internet.
- **IP address configured on interface** — Kerio Control sends the IP address from the chosen interface to the DDNS provider.



If you don't know which option is the best, switch to **Detected public IP address**.

8. Click **Apply**.

Saving configuration to MyKerio

Overview



New in Kerio Control 9.1!

Kerio Control can automatically back up and upload the configuration files to [MyKerio](#) every day.

Each backup includes:

- Configuration files
- SSL certificates
- DHCP leases

To configure backup to an FTP server instead, read the [Saving configuration to FTP server](#) article.

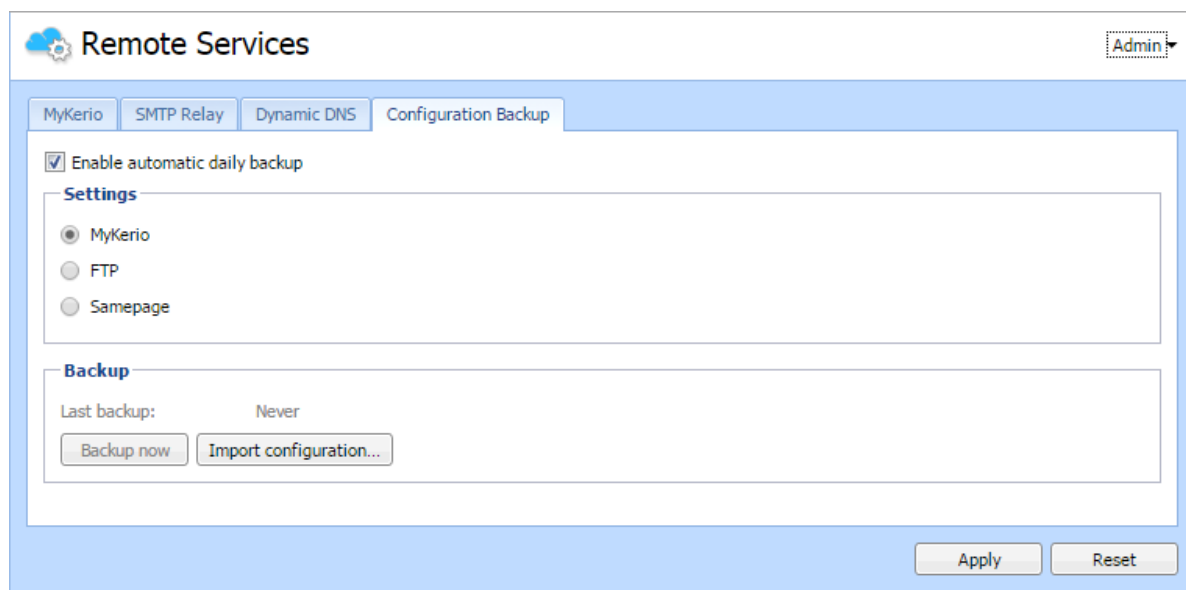
Saving configuration to MyKerio

Before you start, connect your Kerio Control to MyKerio. For details, read [Adding Kerio Control to MyKerio](#).

Once Kerio Control is connected to MyKerio:

1. In the administration interface, go to **Remote Services** → **Configuration Backup**.
2. Select **Enable automatic daily backup**.
3. In **Settings**, select **MyKerio**.
4. Click **Apply**.

Saving configuration to MyKerio



The screenshot shows the 'Remote Services' configuration window with the 'Configuration Backup' tab selected. At the top right is an 'Admin' link with a dropdown arrow. Below the tabs, there is a checkbox labeled 'Enable automatic daily backup' which is checked. Under the 'Settings' section, three radio buttons are present: 'MyKerio' (selected), 'FTP', and 'Samepage'. The 'Backup' section shows 'Last backup:' followed by 'Never'. At the bottom of this section are two buttons: 'Backup now' and 'Import configuration...'. At the very bottom of the window are 'Apply' and 'Reset' buttons.

Kerio Control uploads configuration files once a day.

Restoring configuration from a backup

To learn how to restore your configuration from a backup, read the [Backups in MyKerio](#) article.

Saving configuration to Samepage

Saving configuration to Samepage



Support of Samepage backups in Kerio Control ends soon and works only for Samepage accounts created before March 2016. Newer accounts can no longer upload backups to Samepage.

You can upload your configuration to [MyKerio](#) instead. For more details, read [Saving configuration to MyKerio](#).

Kerio Control can automatically backup and upload the configuration files to [Samepage.io](#) every day.

Each backup includes:

- Configuration files
- SSL certificates
- DHCP leases



To configure backup to an FTP server, read [Saving configuration to FTP server](#) article.

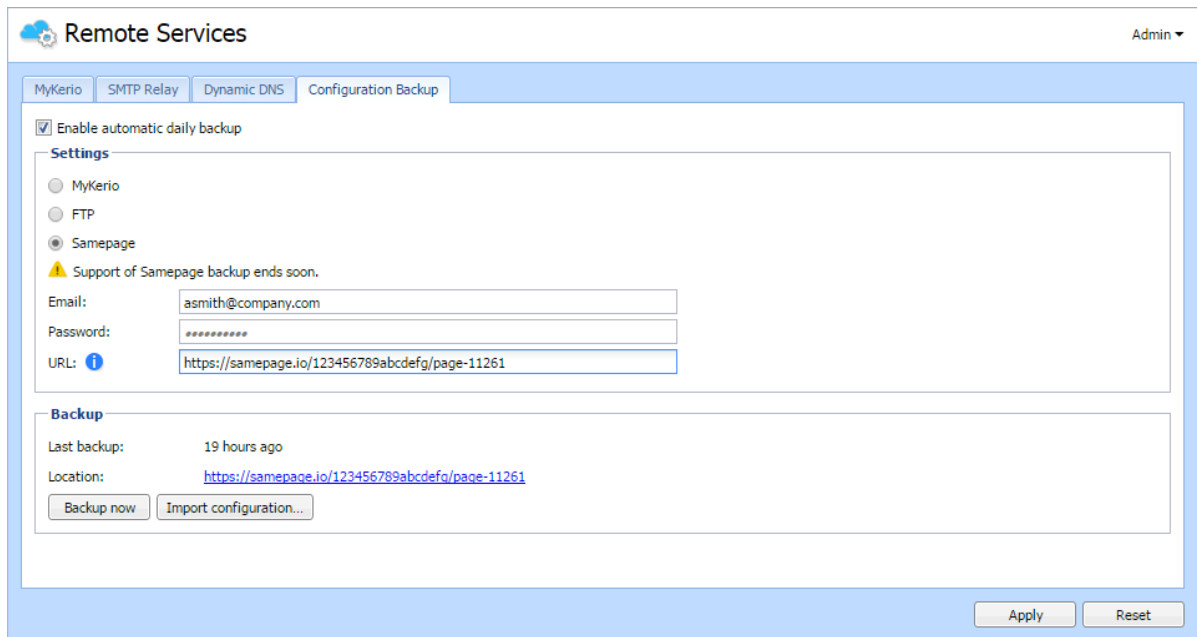
1. Sign-up to [Samepage](#) for free (or use your existing Samepage account).
2. Create a new page for the backup and copy the URL of the page.



Samepage.io includes two types of pages. [Team pages](#) do not support saving Kerio Control backups. For saving the backups, create a new page according to steps in the [Creating a Page](#) article.

3. In the Kerio Control Administration, go to **Remote Services** → **Configuration Backup**.
4. Select the **Enable automatic daily backup** option.
5. In the **Service** menu, select **Samepage**.
6. Type the username and password of your Samepage account.
7. In the URL field, paste the URL of the Samepage backup page you created in step 2.
8. Click **Apply**.

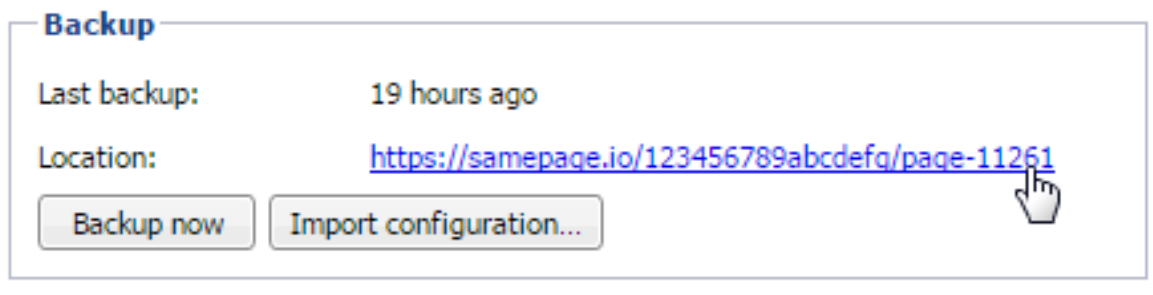
Saving configuration to Samepage



The screenshot shows the 'Remote Services' configuration window with the 'Configuration Backup' tab selected. At the top, there are tabs for 'MyKerio', 'SMTP Relay', 'Dynamic DNS', and 'Configuration Backup'. Below the tabs, there is a checkbox labeled 'Enable automatic daily backup' which is checked. Under the 'Settings' section, three radio buttons are present: 'MyKerio', 'FTP', and 'Samepage', with 'Samepage' being selected. A warning icon and text state 'Support of Samepage backup ends soon.' Below this, there are input fields for 'Email' (containing 'asmith@company.com'), 'Password' (containing '*****'), and 'URL' (containing 'https://samepage.io/123456789abcdefg/page-11261'). The 'Backup' section shows 'Last backup:' as '19 hours ago' and 'Location:' as the same URL. At the bottom of the backup section are two buttons: 'Backup now' and 'Import configuration...'. The bottom of the window has 'Apply' and 'Reset' buttons.

Kerio Control uploads configuration files once a day.

Only the specified user has access to this page. The section backup displays the link to the Samepage backup page.



This is a close-up of the 'Backup' section from the previous screenshot. It shows the 'Last backup:' status as '19 hours ago' and the 'Location:' as a blue hyperlink: 'https://samepage.io/123456789abcdefg/page-11261'. A mouse cursor is pointing at the end of this link. Below the link are two buttons: 'Backup now' and 'Import configuration...'.

For immediate configuration backups to the FTP server, click **Backup now**.

Restoring configuration from backup

To import the files back to Kerio Control, click the **Import configuration** button, or use the [Configuration Assistant](#).

Saving configuration to FTP server

Configuring backup to an FTP server

Kerio Control can automatically backup and upload the configuration files to your FTP server every day.

Each backup includes:

- Configuration files
- SSL certificates
- DHCP leases



To configure backup to [MyKerio](#), read [Saving configuration to MyKerio](#) article.

1. In the administration interface, go to **Remote Services** → **Configuration Backup**.
2. Select the **Enable automatic daily backup** option.
3. In the **Service** menu, select **FTP**.
4. Type the username and password of your FTP server.
5. In the URL field, [type the location for backups](#) of your Kerio Control.
6. Click **Apply**.

Kerio Control uploads configuration files once a day.

For immediate configuration backups to the FTP server, click **Backup Now**.

Saving configuration to FTP server

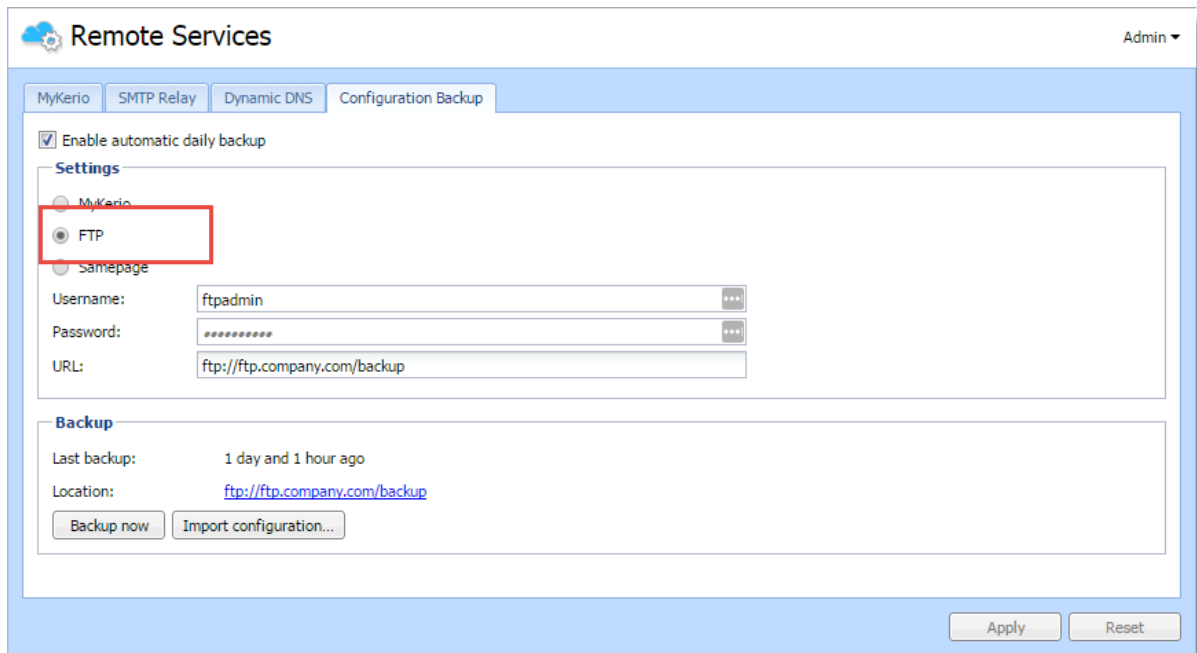


Figure 1 Configuring backup to FTP

Restoring configuration from backup

To import the files back to Kerio Control, click the **Import configuration** button, or use the [Configuration Assistant](#).

Composing FTP URLs

You can use the following FTP address formats:

- Domain name
`ftp://server.domain`
- Custom port on server side
`ftp://server.domain:port`
- Path relative to a user's home directory
`ftp://server.domain/path`
- Absolute path
`ftp://server.domain/%2Fdirectory-in-root/other-directory`
- IPv4/IPv6 address
`ftp://IPv4-address`

`ftp://[IPv6-address]`

Example

- FTP server has no DNS name (AAAA record) and is accessible via an IPv6 address only (2002:1234:4567:89ab:250:56ff:feb8:5e)
- FTP server runs on a custom port 1234
- User home directory on the FTP server is `/home/user`
- Backup directory on the FTP server is `/backup/control`

The result is:

`ftp://[2002:1234:4567:89ab:250:56ff:feb8:5e]:1234/%2Fbackup/control`

Managing user accounts

User accounts overview

User accounts are used to:

- Authenticate users
- Gather reporting data in Kerio Control Statistics
- Set access rights for Kerio Control administration
- Control user access to the Internet from local networks

Users are managed in the **Users** section of the administration interface.

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 **Accounting and Monitoring** → **Data Gathering**.
2. Verify that the **Gather internet usage statistics** option is selected.

Managing user accounts

For more information, go to the [Configuring statistics and reports](#) article.

3. In the administration interface, go to **Users**.
4. Select a user (or a template) and click **Edit**.
5. 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).

6. 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.

7. 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 the **General** tab, clear the **Account is enabled** option.
3. Save your settings.

Deleting users permanently

1. In the administration interface, go to **Users**.
2. Select the user, and click **Remove**.
3. In the **Confirm Action** dialog, click **Yes**.

Kerio Control deletes the user.

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 unlock HTTP content 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.

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).

Setting access rights to internet usage statistics and user's activity records

For detailed information, go to the [Configuring statistics and reports](#) article.

Configuring automatic user login

Automatic login overview

If users work at reserved workstations (i.e. their computers are not used by any other user), they can use automatic login to Kerio Control. Their computers are identified with [Media Access Control address](#) (MAC address) or IP address (static or reserved by DHCP).



Watch the [Configuring automatic user login](#) video.

Configuring automatic login on MAC address



You can use automatic login on MAC address if [Kerio Control is able to see the MAC address of the host](#).

To configure automatic login on MAC address, follow these steps:

1. In the administration interface, go to **Users**.
2. Select a user and click **Edit**.
3. In the **Edit User** dialog, go to the **Addresses** tab.
4. Check the **Specific MAC addresses** option.
5. Type the MAC address of the selected user.
6. To save, click OK.

The user does not have to use their credentials for the Kerio Control login.



If you use [Kerio Control MAC Filter](#), check the **Also permit MAC addresses used in DHCP reservations or automatic user login** option.

Configuring automatic user login

Configuring automatic login in the Active Hosts section

If a user is logged in to Kerio Control, you can assign a MAC address and configure automatic login without typing the MAC address:

1. In the administration interface, go to **Status** → **Active Hosts**.
2. Select a user.
3. Right-click on the selected user and click **Login User Automatically by MAC**.
Kerio Control opens a window with information about the new configuration.
4. Click OK.

The user does not have to use their credentials for the Kerio Control login.

Configuring automatic login on static IP addresses

If a user works at a reserved workstation with a fixed IP address (static or reserved at the DHCP server), the user can use an automatic login from this 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 the **Addresses** tab.
4. You have several options:
 - For one or several IP address: Check the **Specific host IP addresses** option.
 - For more IP addresses: click **Edit** and [create a new group of IP addresses](#) for automated login and check the **IP address group** option.
5. To save, click OK.

The user does not have to use their credentials for the Kerio Control login.

Why Kerio Control does not know the MAC address

Kerio Control does not know the MAC address in the following cases:

- You use a routed network and the computer is placed behind a router.
- The host is connected to the network via a VPN client (either Kerio VPN or IPsec).
- The browser on the host is set to use a non-transparent proxy.

Assigning static IP addresses for Kerio Control VPN Clients

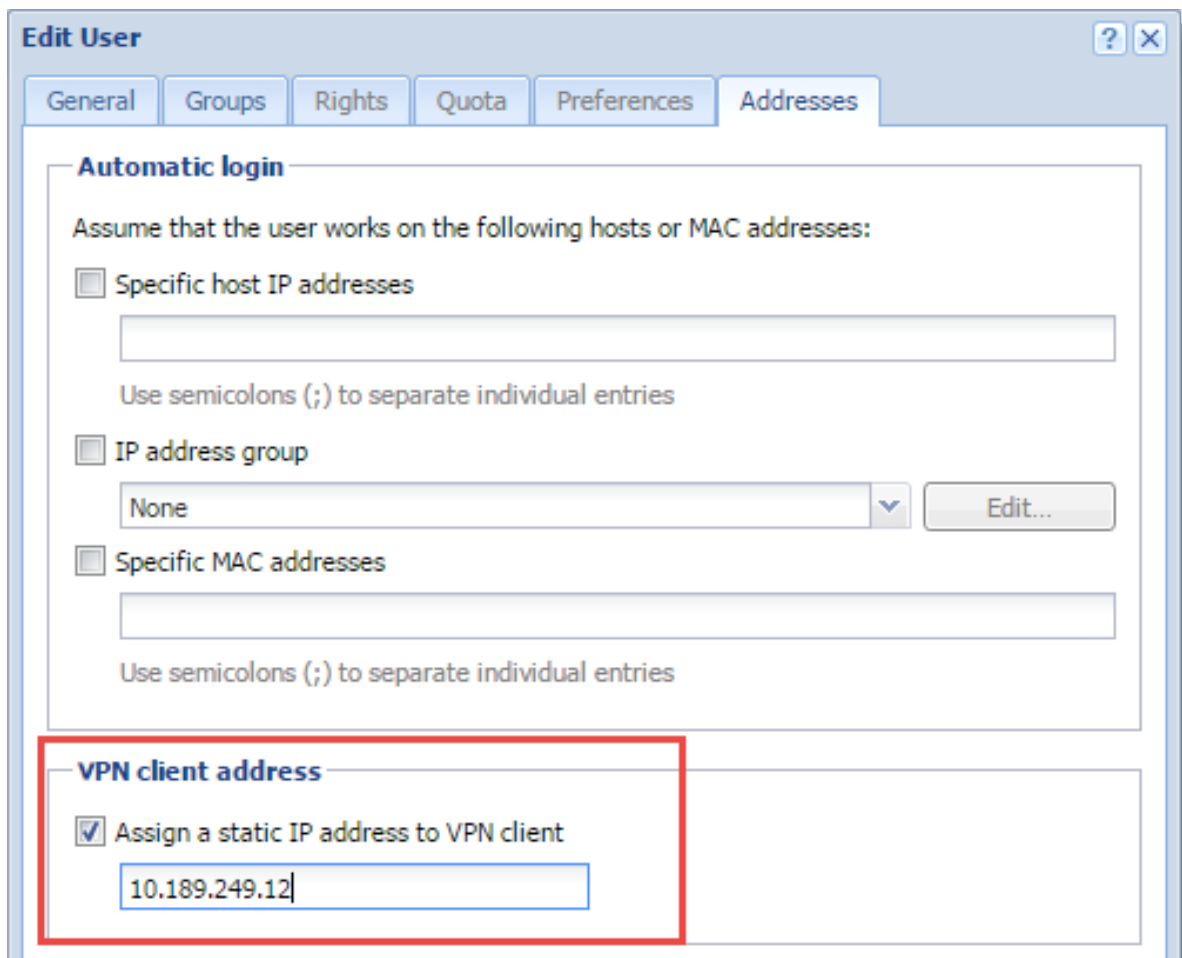
Overview

If Kerio Control user needs to access services hosted on the Kerio Control VPN Client, you can assign a static IP address to Kerio Control VPN Client.

For more information about Kerio Control VPN, read [Configuring Kerio Control VPN server](#)

1. In the administration interface, go to **Users and Groups** → **Users**.
2. Double-click the user to whom you want to assign a static IP address.
3. In the **Edit User** dialog box, go to the **Addresses** tab.
4. Select **Assign a static IP address to VPN client**.
5. Type the static IP address.
6. Click **OK**.

Assigning static IP addresses for Kerio Control VPN Clients



Edit User

General Groups Rights Quota Preferences **Addresses**

Automatic login

Assume that the user works on the following hosts or MAC addresses:

☐ Specific host IP addresses

☐ IP address group

☐ Specific MAC addresses

Use semicolons (;) to separate individual entries

None Edit...

VPN client address

☒ Assign a static IP address to VPN client

10.189.249.12

From now on, Kerio Control assigns the IP address to user's Kerio Control VPN Client.

Do not set the same IP address to multiple users, Kerio Control will assign the address to the last edited user. All other users with the same IP address lose it and they get a dynamic address from the DHCP server.

Do not set the same IP address to multiple devices.

Configuring 2-step verification

Overview



Watch the [2-step verification](#) video.

The 2-step verification adds an extra layer of security to your account by using an application on the user's smartphone to confirm their identity.

This type of verification protects access to Kerio Control and your LAN from the Internet with two independent steps. Users must use their credentials to authenticate and also type a special time-limited code generated by an authentication application on their phones or computers that supports RFC 6238, such as

- Google Authenticator — Available for iOS, Android and Windows Phone
- FreeOTP Authenticator — Available for iOS and Android (<https://fedorahosted.org/>)
- Authenticator for iOS (<http://matrubin.me/>)
- Authenticator for Windows Phone (<http://www.windowsphone.com/>)
- WinAuth for Windows OS (<https://winauth.com/>)

The 2-step verification protects all interfaces accessible from the Internet:

- Kerio Control VPN Client/IPsec VPN client
- Kerio Control Statistics
- Kerio Control Administration

Users must use the verification code every time they try to connect to the Kerio Control network from the Internet. If they select **Remember me on this device**, their browser remembers the connection for the next 30 days from the last connection.

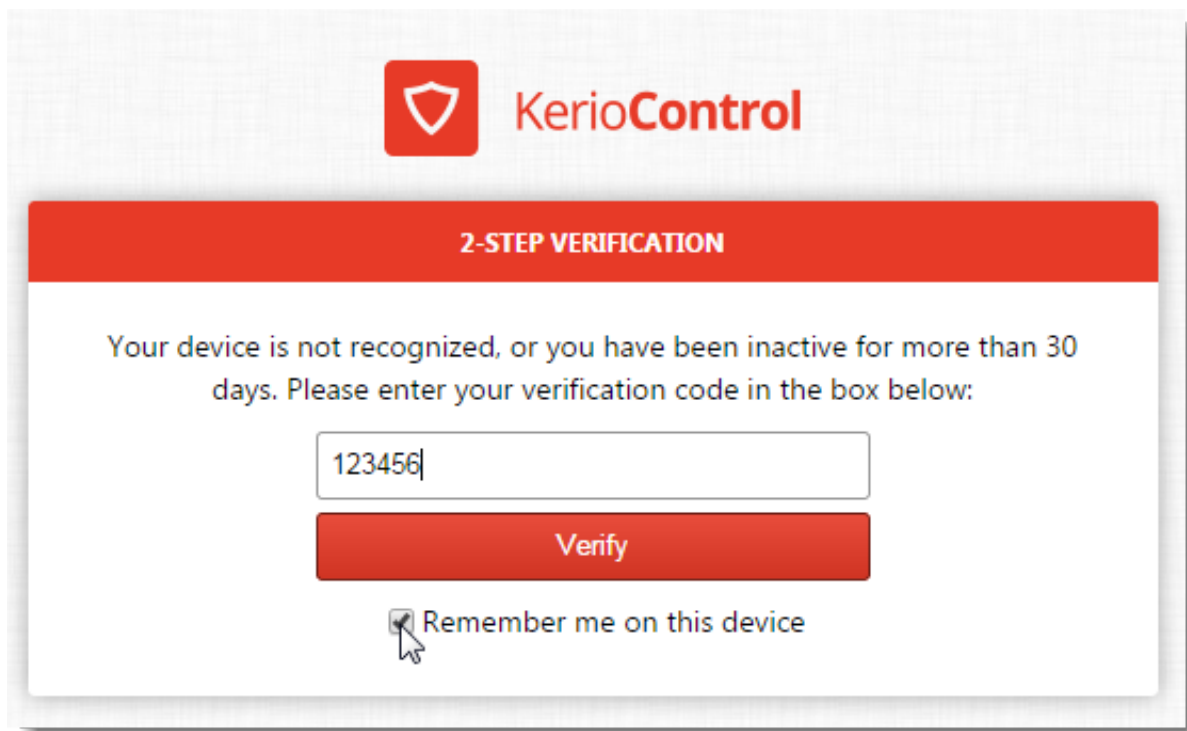


Figure 1 The 2-Step Verification tab

Configuring the 2-step verification in Kerio Control Administration

Users can set up their 2-step verification in Kerio Control Statistics themselves. For instructions, refer to [Authenticating to firewall with 2-step verification](#).

As administrator, you can also require the use of 2-step verification:

1. In the administration interface, go to **Domains and User Login** → **Security Options**.
2. Select **Require 2-step verification**.
3. Select **Allow remote configuration** to allow users to pair their mobile device with their Kerio Control account remotely.



If you disable this option, users must pair their devices from the local network only.

4. Click **Apply**.

Kerio Control now starts to require the 2-step verification. Users must pair their mobile devices with their Kerio Control account. They authenticate to the Kerio Control network with their credentials and a verification code.

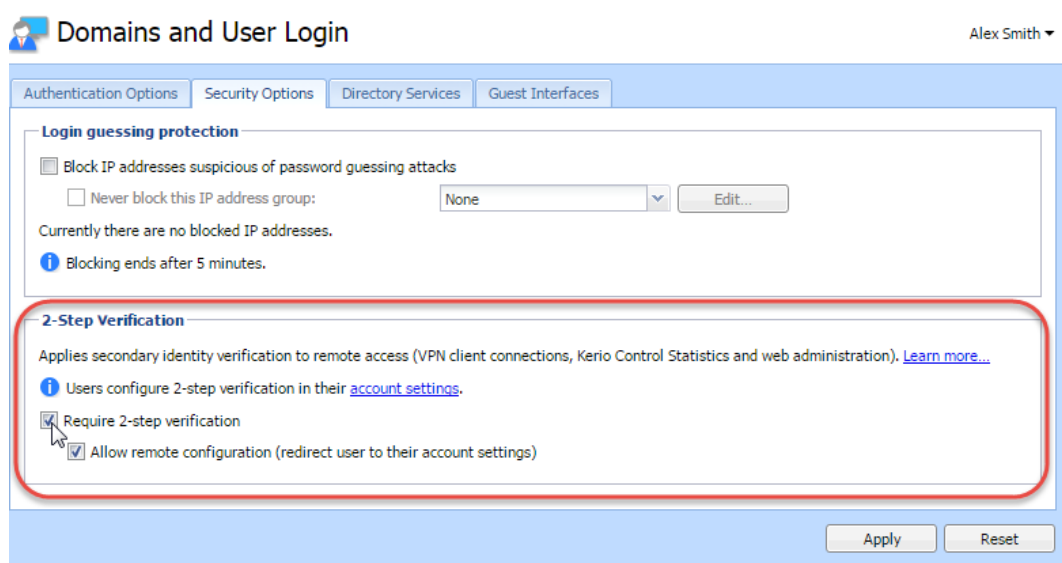


Figure 2 The 2-Step Verification tab

Disabling the 2-step verification for a particular user

If a user loses their mobile device, you must disable the 2-step verification for that person. Otherwise the user cannot access the Kerio Control network from the Internet.

1. In the Kerio Control Administration, go to **Users and Groups** → **Users**.
2. Right-click the user whose access you need to change.
3. In the context menu, click **Reset 2-step verification**.

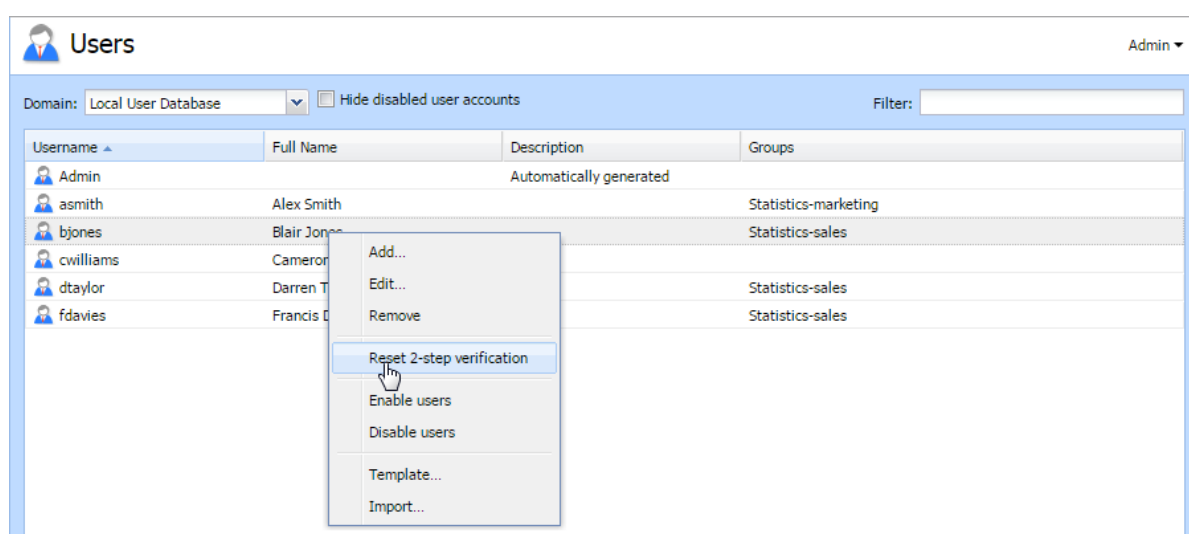


Figure 3 The 2-Step Verification tab

Configuring 2-step verification

The user can now enable the 2-step verification in Kerio Control Statistics with a new mobile device.

Enabling the 2-step verification in Kerio Control Statistics

Users can enable the 2-step verification in their account in Kerio Control Statistics. For more information, see [Authenticating to firewall with 2-step verification](#).

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.

Authenticating users to Kerio Control

Overview

Kerio Control can authenticate users on the network. By authenticating users, Kerio Control can associate people with devices. This allows you to create policies and monitor activities of identifiable people rather than anonymous devices.

Kerio Control can authenticate users via:

- Kerio Control web interface — See [Requiring user authentication when accessing web pages](#) for details.
- Automatic login — Kerio Control permanently associates a user to a device based on the device IP or MAC address. See [Configuring automatic user login](#) for details.
- RADIUS — See [Using RADIUS server in Kerio Control](#) for details.
- VPN — See [Configuring Kerio VPN server](#) and [Configuring IPsec VPN](#) for details.

Requiring user authentication when accessing web pages

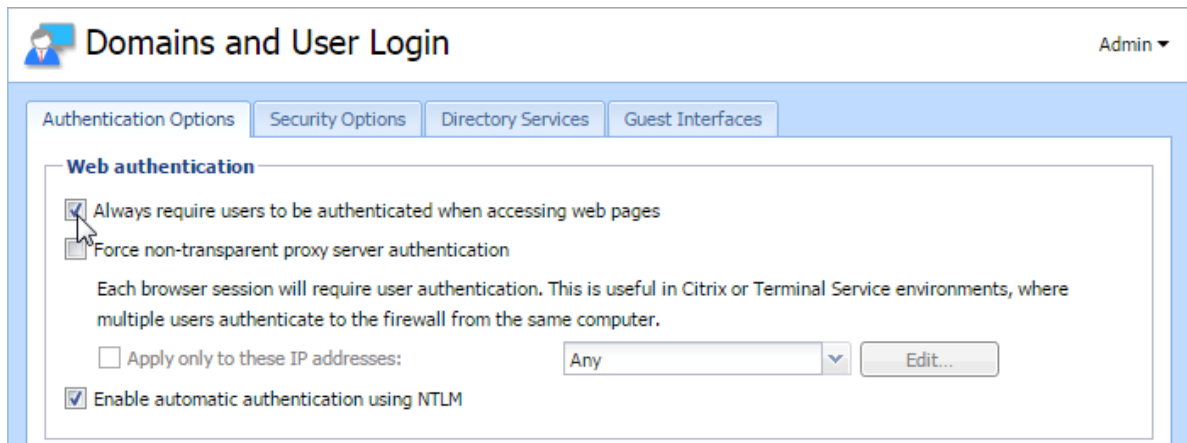
Kerio Control can require users to authenticate before they can browse the web. When an unauthenticated user open a non secure website in their browser, Kerio Control redirects the user to the firewall login page. After the user successfully logs in, Kerio Control permits the user to the originally requested page.



Before enabling this option, make sure you properly configure the Kerio Control web interface. Refer to [Configuring the Kerio Control web interface](#) for details.

To enable requiring user authentication:

1. In the administration interface, go to **Domains and User Login** → **Authentication Options**.
2. Select **Always require users to be authenticated when accessing web pages**.
3. (Optional) If Kerio Control connects to Active Directory, you can select **Enable automatic authentication using NTLM**. In this case, the web browser automatically authenticates the user via NTLM. See [Configuring NTLM authentication to work with Kerio Control](#) for details.
4. Click **Apply**.



Requiring user authentication when multiple users use one computer



This option is useful only in Citrix or Terminal Service environments, where multiple users authenticate to the firewall from the same computer.

If you have computers in the Kerio Control network that two or more users access simultaneously, you can require user authentication for each browser session. This allows Kerio Control to uniquely identify the web requests of each user on the computer.

Prerequisites:

- Configure non-transparent proxy server in Kerio Control.
- Configure non-transparent proxy server settings in browsers on computers shared with two or more users.

See [Configuring proxy server](#) for details.

To enable this option:

1. In the administration interface, go to **Domains and User Login** → **Authentication Options**.
2. Select **Force non-transparent proxy server authentication**.
3. Select **Apply only to these IP addresses**.
4. Add a new IP address group for computers shared with two and more users.
5. Click **Apply**.

Kerio Control requires authentication every time when a browser opens.

If you run Terminal Server on Windows Server 2008 R2 and newer, you can use Remote Desktop IP Virtualization instead of proxy servers. For more information, see [Using Remote Desktop IP Virtualization](#).

User logout

By default, Kerio Control automatically logs out authenticated users after 120 minutes of inactivity. You can disable or adjust this timeout.

1. In the administration interface, go to **Domains and User Login** → **Authentication Options**.
2. Select **Automatically logout users if they are inactive**.
3. Specify a timeout.
4. Click **Apply**.

If you want to manually override the timeout and force user logout, you can perform this action in the **Active Hosts**. See [Monitoring active hosts](#) for details.

Troubleshooting user authentication

If users have problems authenticating to Kerio Control, you can use the **Debug** or **Error** logs to view messages related to the web interface and user authentication. See [Using the Debug log](#) and [Using the Error log](#) for details.

Troubleshooting examples:

- Cannot reach the Kerio Control web interface due to invalid hostname or SSL certificate.
- Login failure due to unsupported or untrusted NTLM authentication method.

Using RADIUS server in Kerio Control

RADIUS server overview

RADIUS (Remote Authentication Dial In User Service) is a protocol used for access to a computer network.

Kerio Control implements a RADIUS server for user authentication with your Wi-Fi access point. This allows users to use their Kerio Control username and password to access your Wi-Fi.



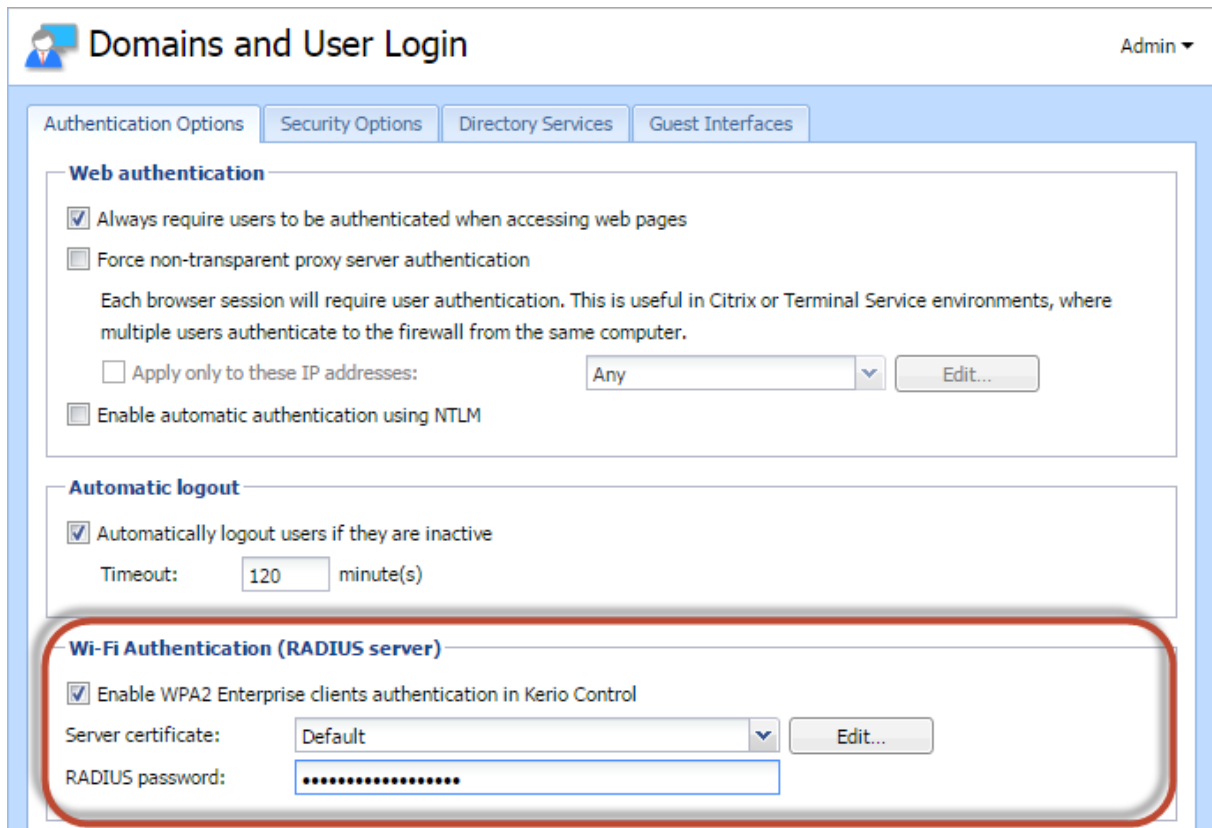
There is a known issue with Windows 7 clients: Windows 7 do not accept untrustworthy certificates. If you Windows 7 clients cannot connect through RADIUS, read the [Configuring Windows 7 clients](#) section.

Configuring Kerio Control

1. In the administration interface, go to **Domains and User Login**.
2. In **Wi-Fi Authentication**, select **Enable WPA2 Enterprise clients authentication in Kerio Control** in **Wi-Fi Authentication**.
3. Select the **Server certificate**.
If you have one, use the certificate signed by a certification authority, because some devices connecting to Wi-Fi access point have problems reading self-signed certificates.
4. Type the RADIUS password.
You must type the same password used in the access point configuration. This might be called the “shared key” or “shared secret” in the Wi-Fi access point configuration.
5. Click the **Apply** button.



Kerio Control does not support MS-CHAPv2 with Apple Open Directory. Kerio Control supports only Microsoft Active Directory.



Domains and User Login Admin ▾

Authentication Options Security Options Directory Services Guest Interfaces

Web authentication

☒ Always require users to be authenticated when accessing web pages

☐ Force non-transparent proxy server authentication

Each browser session will require user authentication. This is useful in Citrix or Terminal Service environments, where multiple users authenticate to the firewall from the same computer.

☐ Apply only to these IP addresses: Any Edit...

☐ Enable automatic authentication using NTLM

Automatic logout

☒ Automatically logout users if they are inactive

Timeout: 120 minute(s)

Wi-Fi Authentication (RADIUS server)

☒ Enable WPA2 Enterprise clients authentication in Kerio Control

Server certificate: Default Edit...

RADIUS password:

Figure 1 Wi-Fi Authentication

Users authentication in Microsoft Active Directory

The Wi-Fi authentication works without any additional settings.

Configuring your Wi-Fi access point

Each type of access point has a different configuration for connecting to a RADIUS server. Find and configure these items (note that terminology may differ slightly):

- Authentication method for the RADIUS server: IEEE 802.1x or WPA/WPA2 Enterprise.
- RADIUS server: IP address where Kerio Control is running.
- Port: 1812. It is the default port for the RADIUS protocol.
- Shared key, shared secret, or RADIUS password: Entered above, in the [Configuring Kerio Control](#) section.

Configuring Windows 7 clients

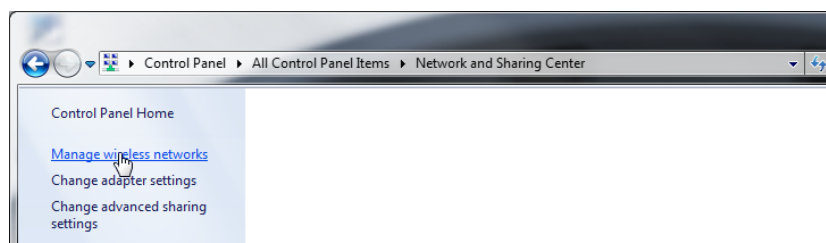
If your users with Windows 7 cannot connect through RADIUS:

- Your Windows 7 clients are connected to your network through Wi-Fi without RADIUS or through the Ethernet cable: Import a Kerio Control local authority as root certificate to Windows 7 clients. You can:
 - If you use Active Directory, import certificate of your domain controller into Kerio Control.
 - [Deploy root certificate via Active Directory.](#)
 - [Import root certificate to each client individually.](#)



Although Windows 7 knows the SSL certificate, the **The connection attempt cannot be completed** warning appears at users's clients during the first connection attempt. Users must click **Connect** in this window.

- Your clients are not connected to your network: Create a profile in the **Manage Network Center** on each Windows 7 client manually. Windows 7 clients do not validate the Kerio Control SSL certificate:
 1. In **Windows 7**, click the **Start** menu.
 2. Go to **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Manage wireless networks**.



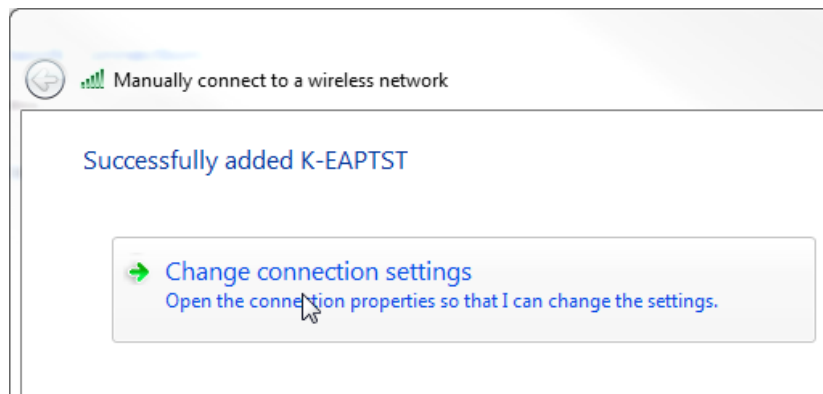
3. Click **Add**.
The **Manually connect to a wireless network** dialog opens.
4. Select **Manually create a network profile**.
5. In the next step, type the SSID name in the **Network name** field.
6. In **Security type**, select WPA2-Enterprise.

7. In **Encryption type**, select AES.
8. Select **Start this connection automatically**.
9. Select **Connect even if the network is not broadcasting**.
10. Click **Next**.

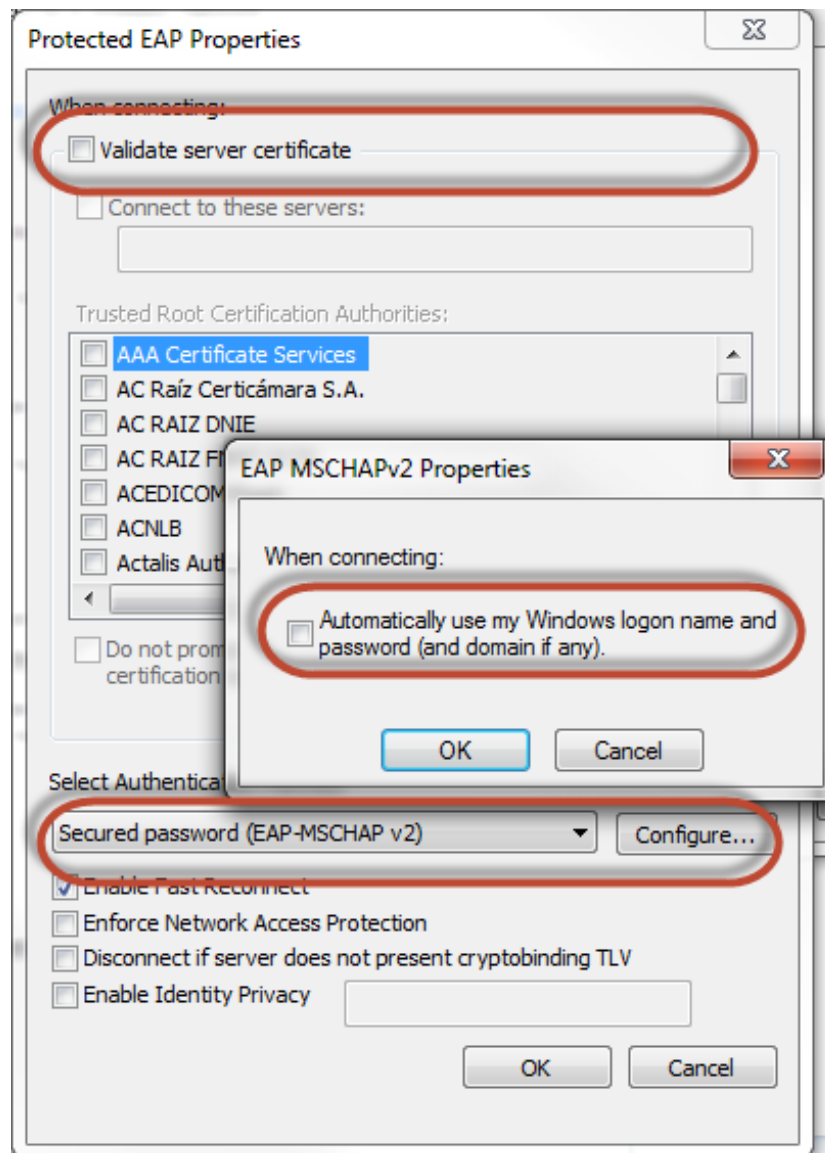
The **Successfully added** page appears.

Now, you must unselect validation of a server certificate:

1. Click **Change connection settings**.



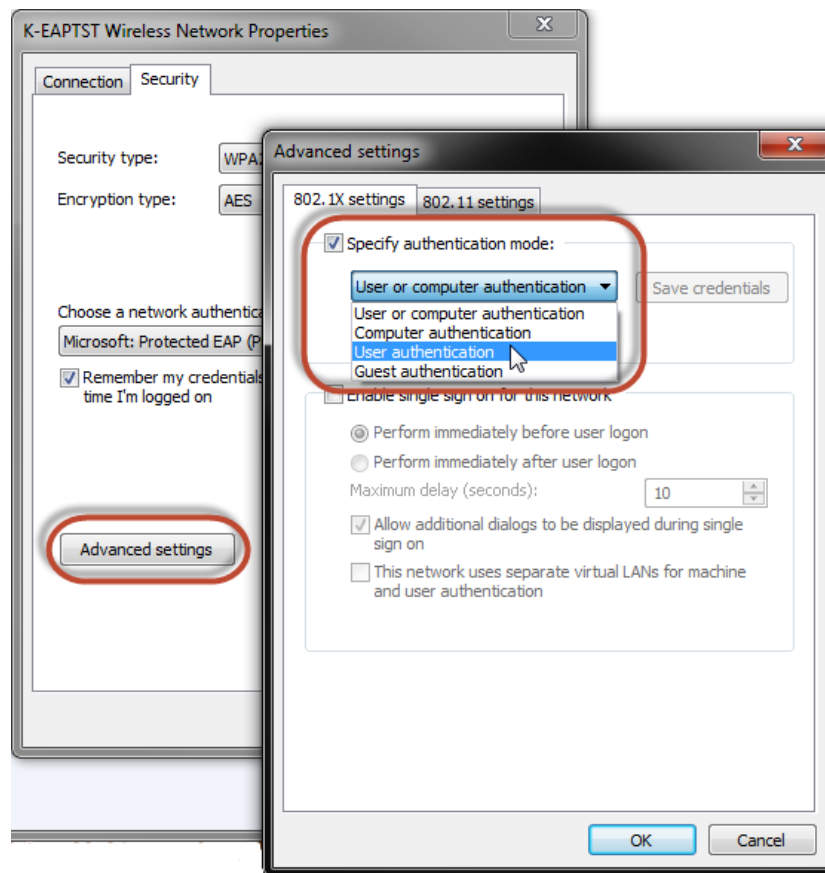
2. On the **Security** tab, click **Settings**.
The **Protected EAP Properties** opens.
3. Unselect **Validate server certificate**.
4. In **Authentication Method**, select **Secured password (EAP-MSCHAP v2)**.
5. Click **Configure**.
The **EAP-MSCHAP v2 Properties** opens.
6. Unselect **Automatically use my Windows logon on name and password**.



7. Click OK.

Now, you must specify the computer authentication:

1. On the **Security** tab, click **Advanced settings**.
2. Select the **802.1X settings** tab.
3. Select **Specify authentication mode**.
4. Select **User authentication**.



5. Click OK.

Windows 7 does not validate the SSL certificate and users can connect through your Wi-Fi to the network.

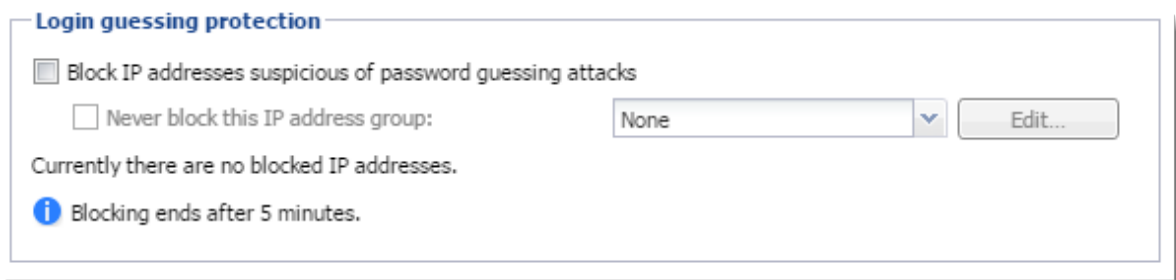
Protecting users against password guessing attacks

Protecting against password guessing attacks

Kerio Control can block IP addresses suspicious of password guessing attacks.

If an attacker tries to log in unsuccessfully 5 times (through various services), Kerio Control blocks the IP address.

1. Go to section **Configuration** → **Domains and User Login** → tab **Security Options**.
2. Select the **Block IP addresses suspicious of password guessing attacks** option.
3. You can select a group of trustworthy [IP addresses](#).
4. Save the settings.



When an account is blocked, user cannot log in. Kerio Control unlocks the blocked IP addresses after 5 minutes.

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 an 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 installation. The server can use this certificate.

However, to avoid users seeing a confirmation message that suggests the site is not secure, 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 formats:

- Certificate (public key) — X.509 Base64 in text format (PEM). The file has the extension `.crt`.
- Private key — The file is in RSA format and it has the extension `.key` with 4KB max. Passphrase is supported.
- Certificate + private key in one file — The format is PKCS#12. The file has the extension `.pfx` or `.p12`.

Creating a new Local Authority

Local Authority is generated automatically during Kerio Control installation. However, the hostname and other data are incorrect, so you need to generate a new certificate for the Local Authority.

To create and use a certificate for the Local Authority:

1. Go to **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, the official name of your company, the city and country of your company, and the period for which the certificate should be valid.

The new Local Authority will be available and visible in **Definitions** → **SSL Certificates**. The old one is:

- Changed from **Local Authority** to **Authority**
- Renamed to **Obsolete Local Authority**
- Available as a trusted authority for IPsec

If you need to know how to export the local authority and import it as root certificate to a browser, read the [Exporting and importing Kerio Control local authority as root certificate](#) article.

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.



Hostname 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.



Hostname 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.

Configuring SSL certificates in Kerio Control

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**.

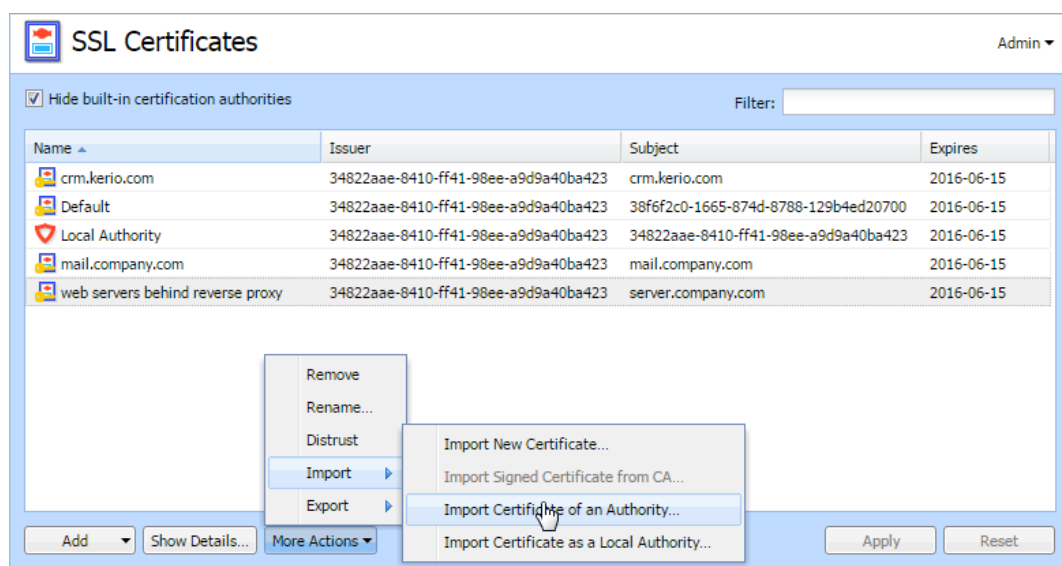
The certificate replaces the certificate request. You can use this certificate. Using the certificate means that you have to select it in the specific settings (for example SSL certificate for VPN server you have to select in **Interfaces** → **VPN Server**).

Importing intermediate certificates

Kerio Control allows authentication by **intermediate** certificates.

To add an intermediate certificate to Kerio Control, follow these steps:

1. In the administration interface, go to section **Configuration** → **SSL Certificates**.
2. Import certificates by clicking on **Import** → **Import Certificate of an Authority**.



3. Save the settings.



If you have multiple intermediate certificates, add them all in the same way.

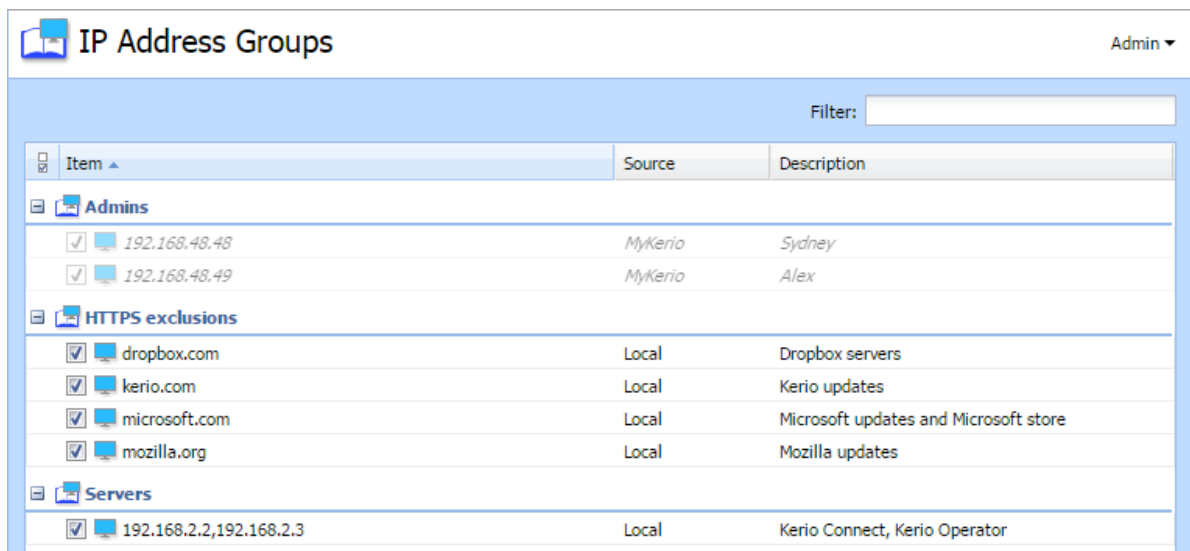
Configuring IP address groups

Using IP address groups

In IP address groups, you can define:

- single IPv4 or IPv6 address
- groups of IPv4 or IPv6 addresses
- hostnames
- IP address ranges for IPv4 or IPv6
- IPv4 subnet with mask
- IPv6 prefix

Kerio Control uses predefined IP address groups in other configuration dialogs such as the traffic and URL rules.



Item	Source	Description
Admins		
<input checked="" type="checkbox"/> 192.168.48.48	MyKerio	Sydney
<input checked="" type="checkbox"/> 192.168.48.49	MyKerio	Alex
HTTPS exclusions		
<input checked="" type="checkbox"/> dropbox.com	Local	Dropbox servers
<input checked="" type="checkbox"/> kerio.com	Local	Kerio updates
<input checked="" type="checkbox"/> microsoft.com	Local	Microsoft updates and Microsoft store
<input checked="" type="checkbox"/> mozilla.org	Local	Mozilla updates
Servers		
<input checked="" type="checkbox"/> 192.168.2.2,192.168.2.3	Local	Kerio Connect, Kerio Operator

Figure 1 Section IP Address Groups

Configuring IP address groups



If you have multiple Kerio Control appliances, you can manage them in MyKerio and use shared IP address groups across all your appliances. All shared IP address groups are labeled as **MyKerio** and all groups added in the appliance are labeled as **Local** in the **Source** column. For more details, read [Sharing definitions across Kerio Control appliances with MyKerio](#).

Adding a new IP address group

1. In the administration interface, go to **Definitions** → **IP Address Groups**.

2. Click **Add**.

Add IP Address dialog opens.

3. Select **Create new** and type a name of the IP address group.

4. Select:

- **Addresses**

Type the IP address, range, network, subnet or prefix.

In the **Properties** part of the window, move the cursor above the information point.

Help displays all patterns accepted by Kerio Control (see the screenshot below).

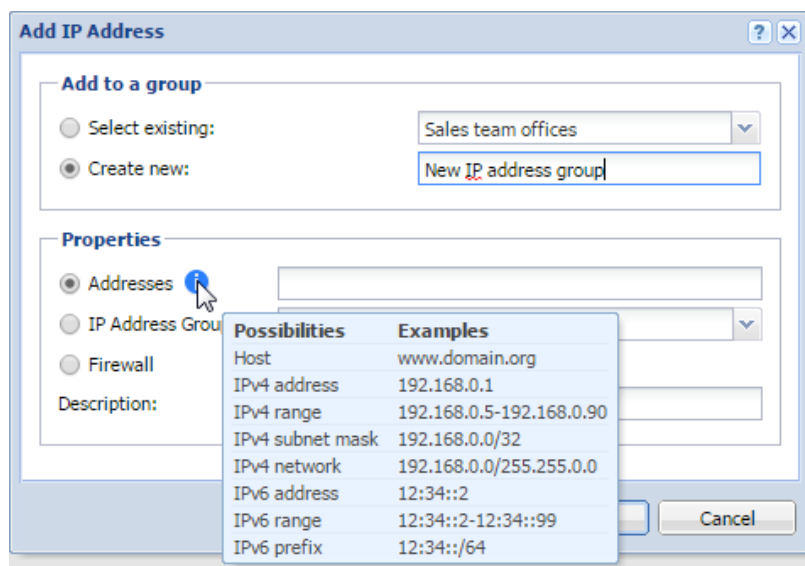


Figure 2 Section IP Address Groups



If you add a domain name, you must use the [Kerio Control DNS server and enable the DNS cache](#).

If you use IP address or a host name you can use any DNS server.

- 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.

5. You can add a description for better reference.

6. Click **OK**.

Adding item into existing address group

If you wish to add items to an existing IP address group:

1. In the administration interface, go to **Definitions** → **IP Address Groups**.

2. Click **Add**.

Add IP Address dialog opens.

3. Choose **Select existing** and specify the desired IP address group from the selection menu.

4. In the **Properties** part of the dialog, define addresses, IP address group or firewall (see step 4 and 5 in section [Adding a new IP address group](#))

5. Click **OK**.



You can edit only individual items within an IP address group. You cannot edit or remove the IP address group itself. If you want to remove the IP address group, you must remove all items or [move them to another IP address group](#).

Moving items from one IP address group to another

If you add a new item to wrong IP address group, you can move it to the right one:

1. In the administration interface, go to **Definitions** → **IP Address Groups**.

2. Right-click the item.

Configuring IP address groups

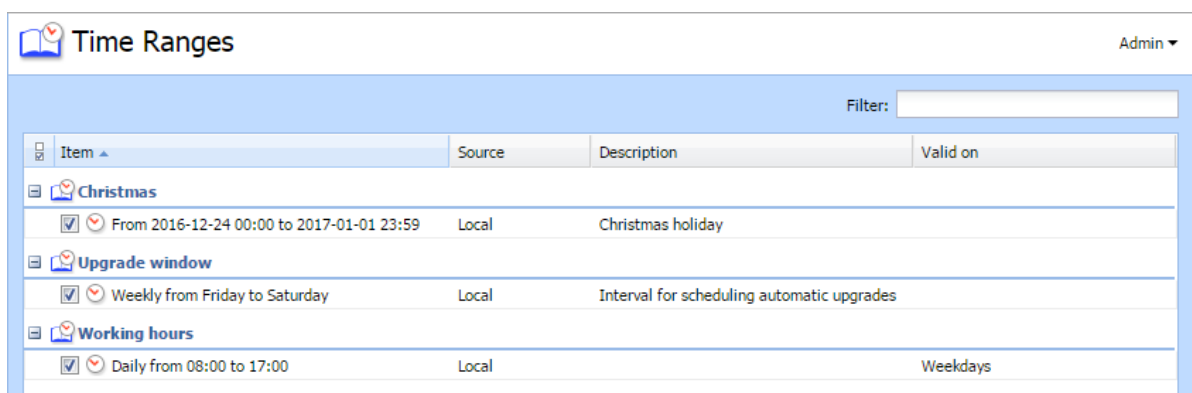
3. In the context menu, click **Edit**.
Edit IP Address dialog opens.
4. Select **Move to existing** and specify the desired IP address group from the selection menu.
5. Click OK.

Creating time ranges in Kerio Control

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.



Item	Source	Description	Valid on
Christmas			
<input checked="" type="checkbox"/> From 2016-12-24 00:00 to 2017-01-01 23:59	Local	Christmas holiday	
Upgrade window			
<input checked="" type="checkbox"/> Weekly from Friday to Saturday	Local	Interval for scheduling automatic upgrades	
Working hours			
<input checked="" type="checkbox"/> Daily from 08:00 to 17:00	Local		Weekdays



If you have multiple Kerio Control appliances, you can manage them in MyKerio and use shared time ranges across all your appliances. All shared time ranges are labeled as **MyKerio** and all time ranges added in the appliance are labeled as **Local** in the **Source** column. For more details, read [Sharing definitions across Kerio Control appliances with MyKerio](#).

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.

Configuring URL groups

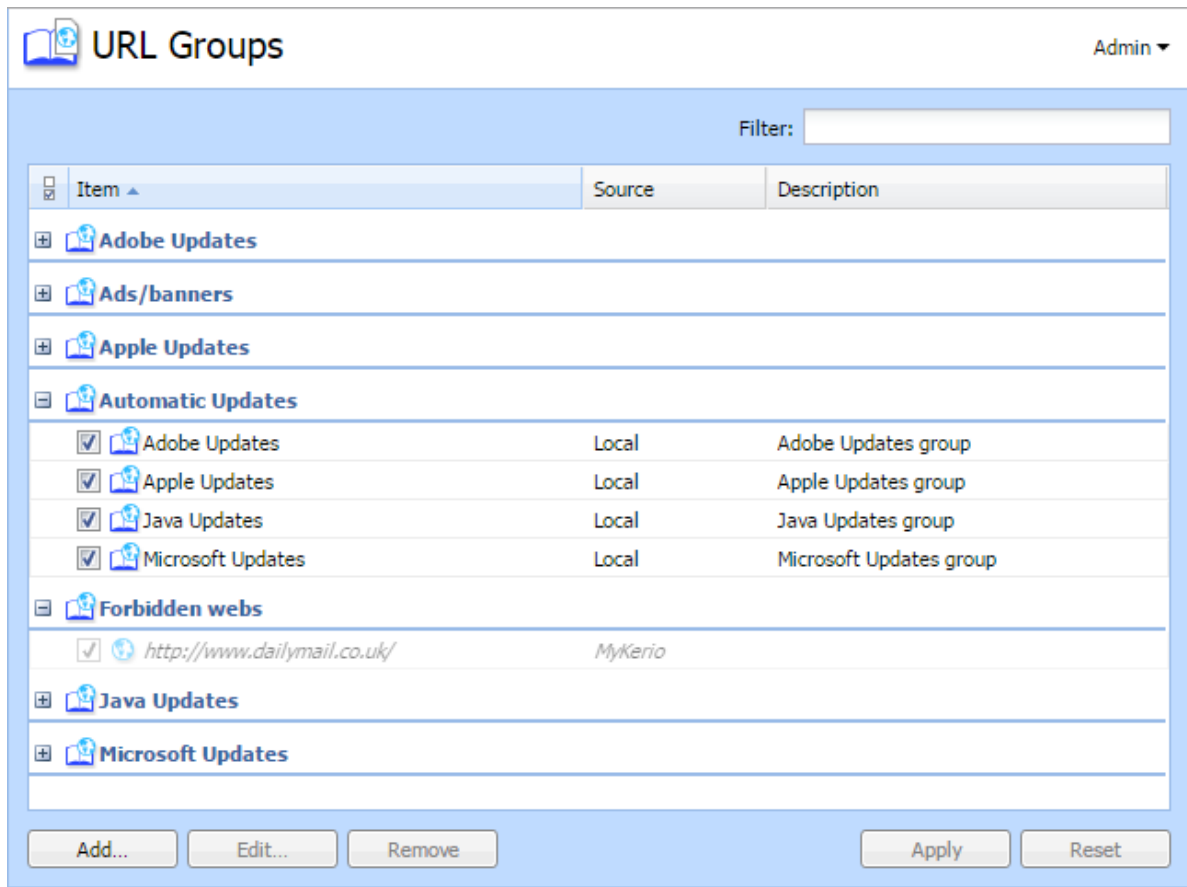
Using URL groups

URL groups enable the administrator to define content 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 content 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:

- **Adobe Updates** — URL of pages requested for automatic updates of Adobe products.
- **Ads/banners** — URLs of pages that contain advertisements, banners, etc.
- **Apple Updates** — URL of pages requested for automatic updates of Apple products.
- **Automatic Updates** — URL of pages requested for automatic updates.
- **Java Updates** — URL of pages requested for automatic updates of Java.
- **Microsoft Updates** — URL of pages requested for automatic updates of Windows.

Configuring URL groups



If you have multiple Kerio Control appliances, you can manage them in MyKerio and use shared URL groups across all your appliances. All shared URL groups are labeled as **MyKerio** and all groups added in the appliance are labeled as **Local** in the **Source** column. For more details, read [Sharing definitions across Kerio Control appliances with MyKerio](#).

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 special characters — * and ?. An asterisk (*) stands for any number of characters, a question mark (?) represents one character.
- Regular expressions.

For details, read article [Wildcards and regular expressions in URL](#).

5. Save the settings.

Services in Kerio Cotrol

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 create groups of services which simplifies creating traffic rules.

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 — HTTP 8080.
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.
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
- **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.

Creating service groups



New in Kerio Control 8.3!

Creating service groups simplifies [creating traffic rules](#) because you do not have to use all the services in your traffic rules. If you need a rule for more services, create a group of all these services and work with the group during creating the traffic rule.

A good example for creating group of services is Kerio Connect — mail server from Kerio Technologies (see figure [1](#)).

1. In the administration interface, go to **Definitions** → **Services**.
2. Click **Add** → **Add Service Group**.
3. In the **Add Service Group** dialog, type a name of the new group.
4. Click **Add**.
5. In the **Select items** dialog, select required service and click **OK**.
6. Repeat step 5 for other services.
7. When the new service group is ready, click **OK**.

The service group is finished and you can use it for [creating a traffic rule](#).

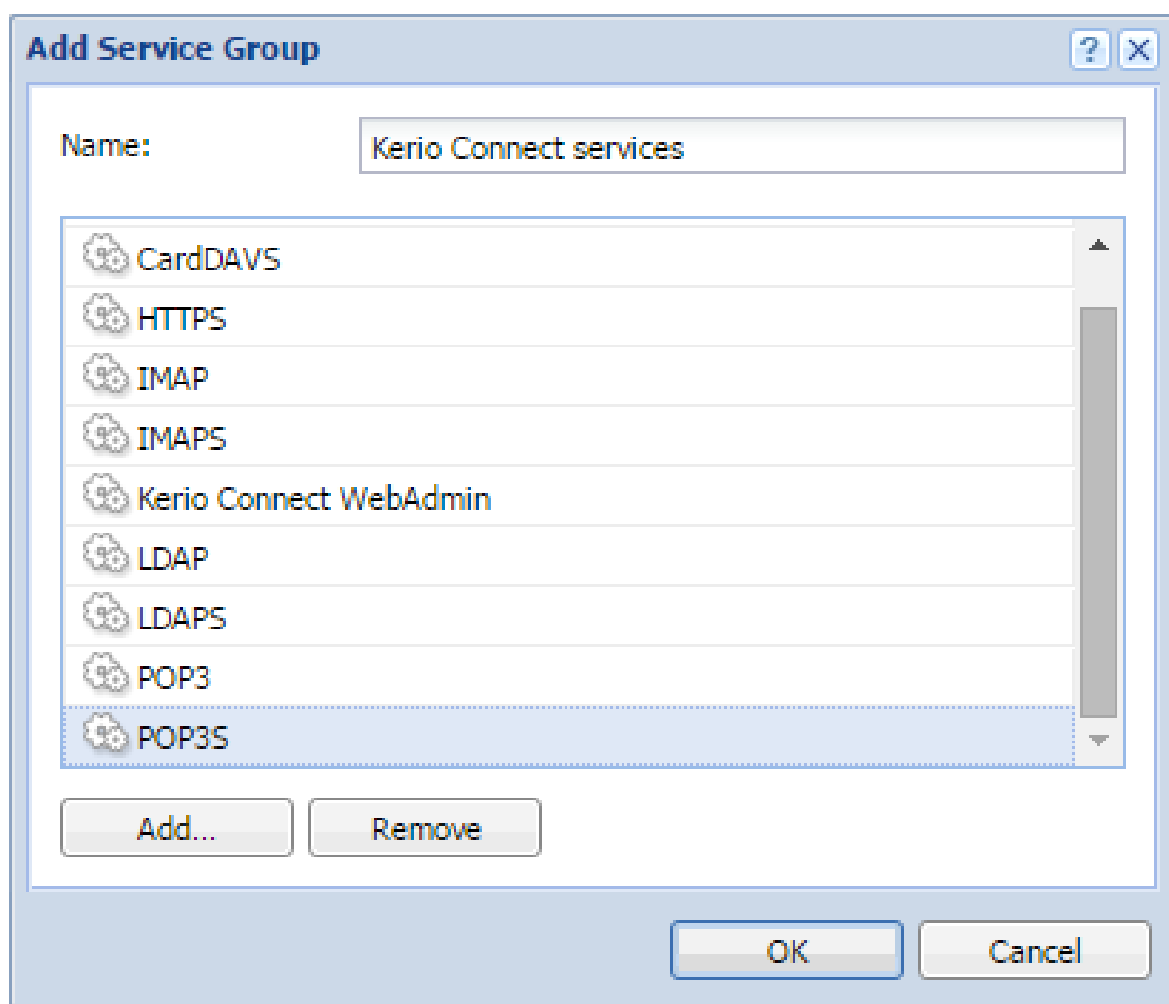


Figure 1 Edit Service Group dialog

Protocol inspection in Kerio Control

Overview

Kerio Control includes protocol inspectors, which monitor all traffic on application protocols, such as HTTP and FTP. The inspectors filter the communication or adapt the firewall's behavior according to the protocol type.

For example, the **HTTP protocol inspector** monitors traffic between browsers and web servers. The protocol inspector blocks connections to particular pages or downloads of particular types of content (for example, images or pop-ups).

Each protocol inspector applies to a specific protocol and service. By default, all available protocol inspectors are used in definitions of corresponding services. (They are applied to matching traffic automatically.)

To apply a protocol inspector explicitly to other traffic, you must edit or add a new service where this inspector is to be used.

Applying protocol inspection to a non standard port

As an example, if you connect to a remote FTP server on the non standard port 2101, you must create a new service for TCP 2101 that uses the FTP inspector:

1. In the administration interface, go to **Definitions** → **Services**.
2. Click **Add** → **Add Service**.
3. In the **Add Service** dialog box, type the name and description of the service.
4. In the **Protocol** drop-down list, select **TCP**.
5. In the **Protocol inspector** drop-down list, select **FTP**.
6. In the **Destination port** section, select the **Equal to** condition and type the port number (2101 in our example).
7. Click **OK**.

Add Service

General

Name: FTP 2101

Description: FTP server on a non-standard port 2101

Protocol: TCP

Protocol inspector: FTP

Source port

Condition: Any

Destination port

Condition: Equal to

Port number: 2101

OK Cancel

From now on, Kerio Control applies the FTP protocol on the non-standard port 2101.

Disabling a protocol inspector



Disable protocol inspectors only for troubleshooting purposes. Disabling a protocol inspector may break the functionality within the protocol or prevent content from being scanned. If you disable SIP or FTP protocol inspectors, their communication fails.

There are two ways to disable protocol inspectors:

- In the **Services** section, to disable protocol inspection for all traffic
- In the **Traffic Rules** section, to disable protocol inspection for traffic meeting the condition of the rule

Disabling protocol inspectors in services

Supposed that a communication to an Internet server does not work correctly. The HTTP protocol inspector stops the communication because it appears to be malicious. To troubleshoot, you can disable the HTTP protocol inspector to see if that solves the problem.

1. In the administration interface, go to **Definitions** → **Services**.
2. Double-click the HTTP service.
3. In the **Edit Service** dialog box, in the **Protocol inspector** drop-down list select **None**.
4. Save your settings.

Now try to access the HTTP server from the Internet. If it is accessible, you have your answer. Enable the HTTP protocol inspector for the service and disable it in the particular traffic rule, as described below.

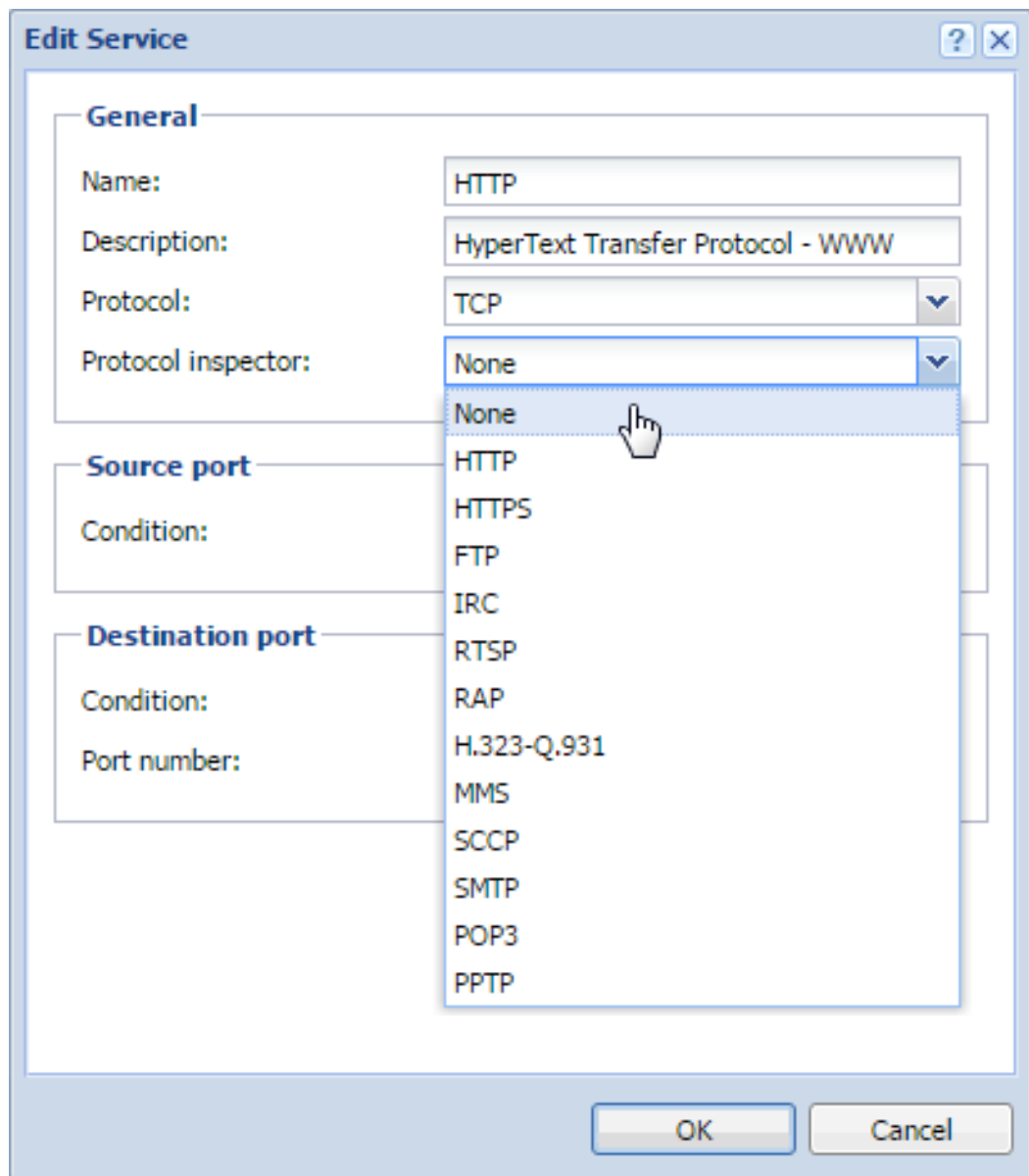


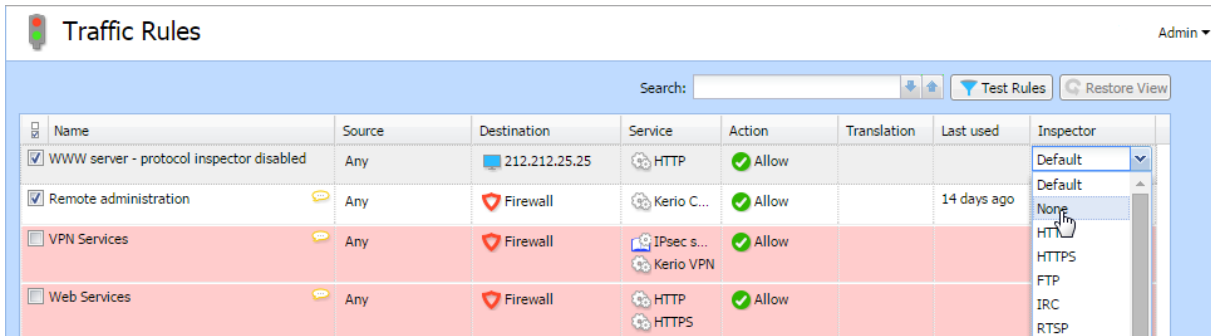
Figure 1 Disabling a protocol inspector

Disabling protocol inspectors in traffic rules

In **Traffic Rules**, you can disable protocol inspectors for a particular traffic rule. For our example we will use the HTTP server placed in the Internet:

1. In the administration interface, go to **Traffic Rules**.
2. Right-click a table header and select **Columns** → **Inspector**.
3. In any single rule, double-click the **Inspector** column and select **None**.
4. Click **Apply**.

Kerio Control disables the protocol inspector for that traffic rule.



The screenshot shows the 'Traffic Rules' management interface in Kerio Control. At the top, there is a search bar and buttons for 'Test Rules' and 'Restore View'. Below this is a table with columns: Name, Source, Destination, Service, Action, Translation, Last used, and Inspector. The table contains four rules. The 'Inspector' column for the first rule is open, showing a dropdown menu with options: Default, None, HTTP, HTTPS, FTP, IRC, and RTSP. The 'None' option is highlighted, indicating it is being selected to disable the protocol inspector for that rule.

Name	Source	Destination	Service	Action	Translation	Last used	Inspector
<input checked="" type="checkbox"/> WWW server - protocol inspector disabled	Any	212.212.25.25	HTTP	Allow			Default
<input checked="" type="checkbox"/> Remote administration	Any	Firewall	Kerio C...	Allow		14 days ago	Default
<input type="checkbox"/> VPN Services	Any	Firewall	IPsec s... Kerio VPN	Allow			None
<input type="checkbox"/> Web Services	Any	Firewall	HTTP HTTPS	Allow			HTTP

Figure 2 Disable a protocol inspector

Monitoring active hosts

Overview

Kerio Control displays the hosts within the local network, or active users using Kerio Control for communication with the Internet in **Status** → **Active Hosts**.

Look at the upper window to view information on individual hosts, connected users, data size/speed, etc.

The section can, for example, displays:

- The current traffic speed for incoming data (**Rx**) and outgoing data (**Tx**) (1)
- The date and time of the active host' registration in the Kerio Control (2)
- The total size of the data received and transmitted since the **Start time** (3)
- The total number of connections from/to the host (4)

You can display the details in the **Connections** tab.

- The IP address of the host from which is the user connecting (5)
- The duration of the time with zero data traffic (6)

You can set the firewall to logout users automatically after the inactivity exceeds the allowed time.

Clicking the right mouse button in the **Active Hosts** window (or on the record selected) displays a context menu that provides the following options:

View in Users

This option is available if the user is logged in.

Kerio Control redirects you to the **Configuration** → **Users** section (the user's account is automatically highlighted) and you can change the details of the account.

For example: in the **Active Hosts** section, you find out that one of the Kerio Control users have huge download. Click **View in Users** and you are immediately in the **Users** section, the user is highlighted and you can set a quota for them.

View in Statistics

This option is available if the user is logged in.

Kerio Control redirects you to the **Status** → **User Statistics** section (the user is automatically highlighted) and you can check user's statistics.

For example: in the **Active Hosts** section, you find out that one of the Kerio Control users have huge download. Click **View in Statistics** and you are immediately in the **User**

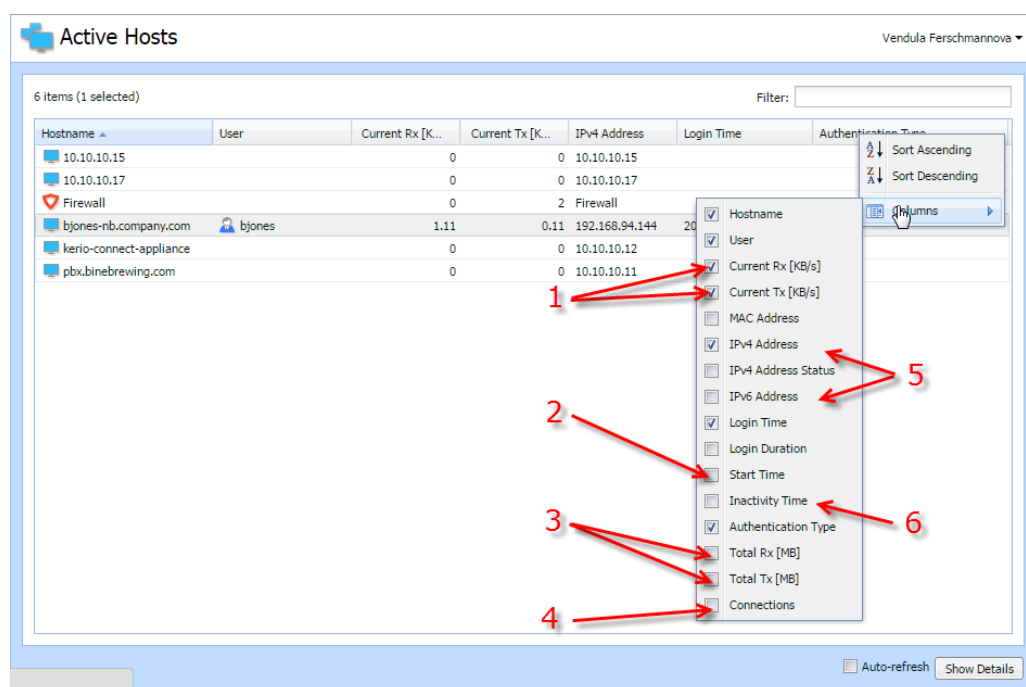


Figure 1 Active Hosts tab

Statistics section, the user is highlighted and you can check if the user's download is often so high.

Make DHCP reservation by MAC

If Kerio Control knows the MAC address, you can make a DHCP reservation by MAC. Read more in the [Using DHCP module](#) article.

Login user automatically by MAC

This option is available if the user is logged in and Kerio Control knows the MAC address of the host.

If users work at reserved workstations (i.e. their computers are not used by any other user), they can use automatic login to Kerio Control. Their computers are identified with Media Access Control address (MAC address). Read more in the [Configuring automatic user login](#) article.

Logout User

Immediate logout of a selected user from the selected active host or hosts.

Logout All Users

Immediate logout of all firewall users.

The Active Hosts section provides detailed information on a selected host and connected user in the [bottom window](#). If you cannot see the details, click the **Show details** button (see figure 1):

Monitoring active hosts

General

Open the **General** tab to view and copy&paste information on user's login, size/speed of transmitted data and information on the activities of the user.

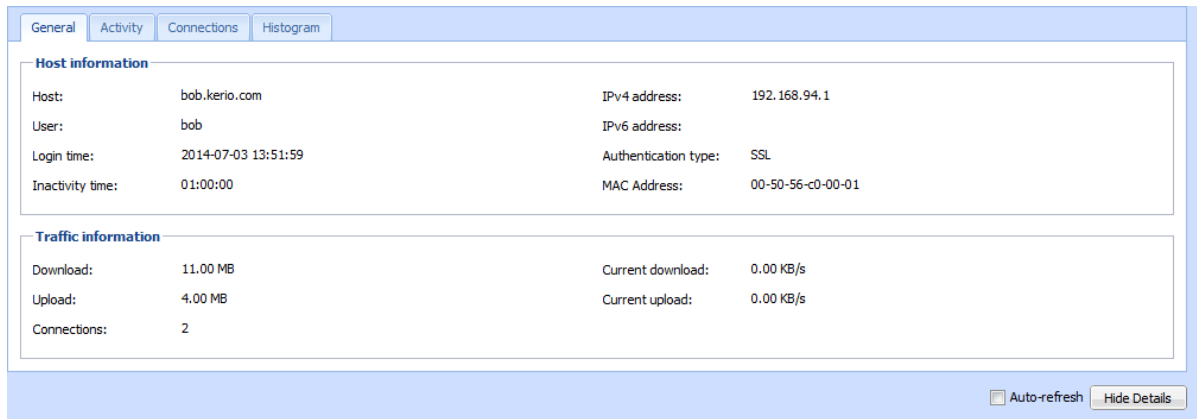


Figure 2 Detailed information for each host or user

Host information

- **Host** — DNS name (if available) or IPv4 address of the host
- **User** — Kerio Control username of the user
- **Login time** — date and time when a user logged-in.
- **Inactivity time** — time for which no packet is sent
- **IPv4 address** — IPv4 address of the host
- **IPv6 address** — IPv6 address of the host
- **Authentication type** — this is displayed if the host uses an authentication.
- **MAC address** — the MAC address is displayed if [Kerio Control knows the MAC address of the host](#).

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.

The **Connections** item means the number of TCP/UDP connections.

Activity

Active since

Time (in minutes and seconds) when the activity was detected.

Event Type

Type of detected activity (network communication). Kerio Control distinguishes many activities, for example SMTP, POP3, WWW (HTTP traffic), FTP, Streams (real-time transmission of audio and video streams), VPN, etc.

Description

Detailed information on an activity. For example:

- **WWW** — title of a Web page to which the user is connected (if no title is available, URL will be displayed instead).



For better transparency, only the first visited page of each web server, to which the user connected, is displayed.

- **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).
- **P2P** — information that the client is probably using Peer-To-Peer network.

Connections

The **Connections** tab displays all active connections to the Internet. Information about each connection includes the processed traffic rule, transfer rate, protocol, outgoing interface, remote host and more.

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.



1. To kill a connection between the LAN and the Internet immediately, right-click the connection and select **Kill connection**.
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.

Monitoring active hosts

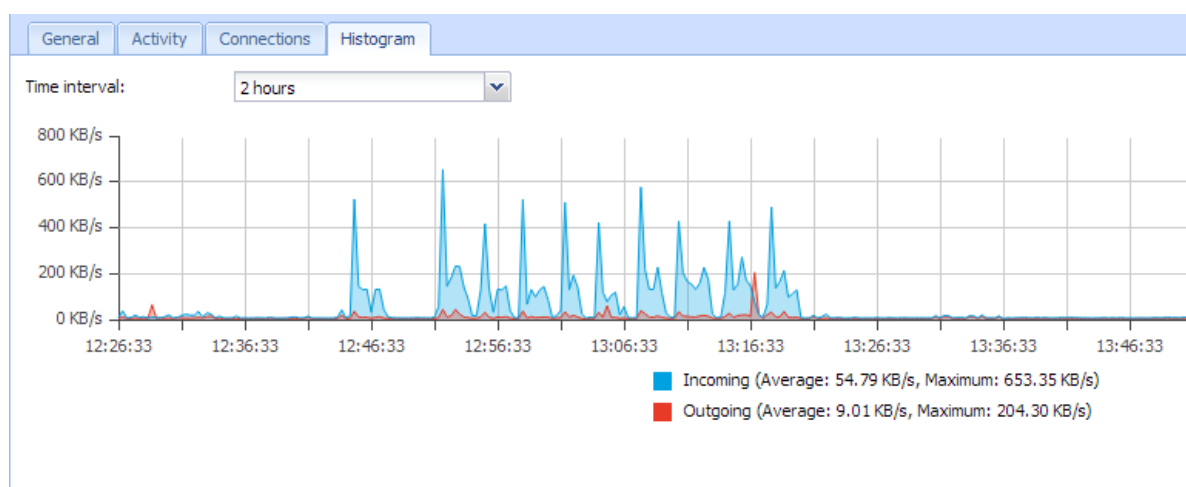


Figure 3 Histogram tab

Monitoring VPN clients

Overview

This article describes a monitoring of all clients connected to Kerio Control through VPN. There are two types of VPN:

- Kerio VPN
- IPsec VPN

Monitoring of VPN clients you can find in the **Status** → **VPN clients** section. The section can, for example, display:

- The DNS name or the public IP address of the host (1)
- The status of the connection (2):
 - Connecting
 - Authenticating — Kerio Control verifies the username and the password
 - Authenticated — Kerio Control configures the client
 - Connected — The client communicates with hosts
- The type of the tunnel (Kerio VPN or IPsec VPN) (3)
- The version and the build number of the Kerio VPN Client (4)

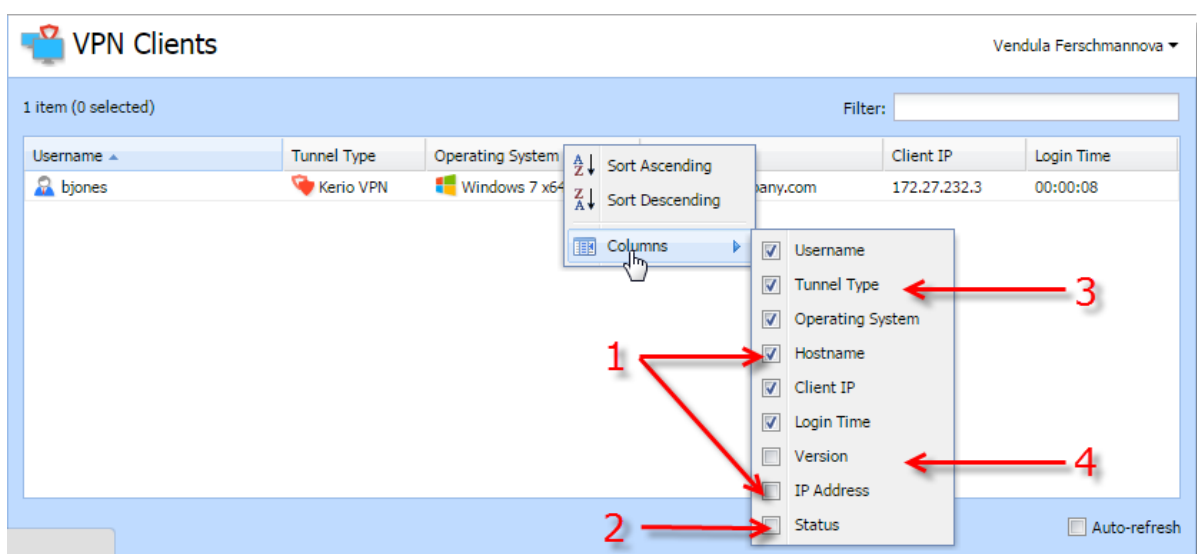


Figure 1 VPN Clients

Monitoring VPN clients



Disconnected clients are removed from the list automatically.

Disconnecting a VPN client

You are allowed to close any of the VPN connections. Right-click to a connection and click **Disconnect**.

Monitoring 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**.

Section **Status** → **Alert Messages** displays all alerts sent to users since startup of Kerio Control. On the left side of the **Alert Messages** 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 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).

Configuring alerts

For more details, read the [Using alert messages](#) article.

Alert log

All alert messages are recorded into the **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.

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).

Monitoring user statistics

Overview

Kerio Control monitors users' traffic and their quota.

To display the monitoring, go to **Status** → **User Statistics**. The section displays:

- A list of Kerio Control users (1)
- A counter for all users (2)
- A counter for not logged in users (3)
- A counter for guest users (4)
- A column indicating the percentage of spent quota per user (5)
- Columns with traffic by day, week, month, and in total (6)

You can also display traffic separately for incoming and outgoing traffic in total and by time period. To do so, select from the IN and OUT options (for example, **Today IN [MB]**, **Month OUT [MB]**, and so on).

The screenshot shows the 'User Statistics' interface. Red arrows point to specific features: 1 points to the 'Username' column header, 2 points to the 'all users' row, 3 points to the 'not logged in' row, 4 points to the 'guest users' row, 5 points to the 'Quota' column, and 6 points to the traffic columns (Today [MB], Week [MB], Month [MB], Total [MB]). A 'Columns' dropdown menu is open, showing options for displaying various traffic metrics.

Username	Full Name	Quota	Today [MB]	Week [MB]	Month [MB]	Total [MB]
all users	all users		15	1 324	1 963	44 988
Admin	Admin		0	0	0	5 026
Admin	Admin		0	0	0	0
amontoya	Adam Montoya	0%	880	1 208	3 087	
cmoore	Cindy Moore	0%	0	0	0	0
cparker	Carl Parker	0%	2	2	722	
hyoung	Harry Young	0%	0	0	0	0
jkeaton	James Keaton	0%	0	0	0	0
mhall	Michael Hall	0%	0	0	0	0
rsmall	Michael Small	0%	0	0	0	0
sbond	Sarah Bond	0%	0	0	0	18
tbond	Tracy Bond	0%	0	0	0	14
vgruber	Vicky Gruber	0%	0	0	0	0
vpntestuser	VPN Testuser	0%	0	0	0	1
wsmith	Wendy Smith	0%	0	0	0	0
not logged in	not logged in		442	753	35 226	
guest users	guest users		0	0	0	0

Kerio Control Statistics

To display the user statistics in Kerio Control Statistics, right-click a users' name and click **View in Kerio Control Statistics**.

For more information about Kerio Control Statistics, visit the [Kerio Control Statistics](#) section in our Knowledge Base.

Monitoring System Health in Kerio Control

Overview

System Health shows current usage of CPU, RAM and the disk space of the computer or device where Kerio Control is running.

Time Interval

Selection of time period for which CPU load and RAM usage is displayed.

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 usage

Currently used and free space on the disk space or a memory card.

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.

Reboot

Restart of the system or shutdown of the device.

Lack of system resources may seriously affect functionality of Kerio Control. If these resources are permanently overloaded, it is recommended to restart Kerio Control and then check system resources usage once again.

Power Off

Shutdown of the device.

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 and configuring 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.

Optionally, records of each log may be recorded in files on the local disk 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 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 common context menu will be displayed:

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.

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 with the following parameters:

Using and configuring logs

- **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. 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 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.

1. Use the **Highlighting** option in the context pop-up menu 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.

2. Click on **Add** and define a rule or double-click the existing rule and redefine it.
3. 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 regular expression (all lines containing one or multiple strings matching the regular expression will be highlighted).



Kerio Control accepts all [regular expressions in accordance with the POSIX standard](#).

4. Click **OK**.

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.

1. Select **Enable logging to file**.

This option enables/disables saving to a file.

If the log is not saved in a file on the disk, only records generated since the last login to Kerio Control will be shown. After logout (or closing of the window with the administration interface), the records will be lost.

2. Select a type of rotation:

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).

3. Type a number of rotated log files to keep.

Maximal count of log files that will be stored. Whenever the threshold is reached, the oldest file will be deleted.

4. Click **OK**.



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

The **External Logging** tab allows sending of individual log records to the Syslog server. Simply enter the DNS name or the IP address of the Syslog server. If you are using default port, type the server name only. If you are using non default port, customize it as `server:port` in the **Syslog server** field.

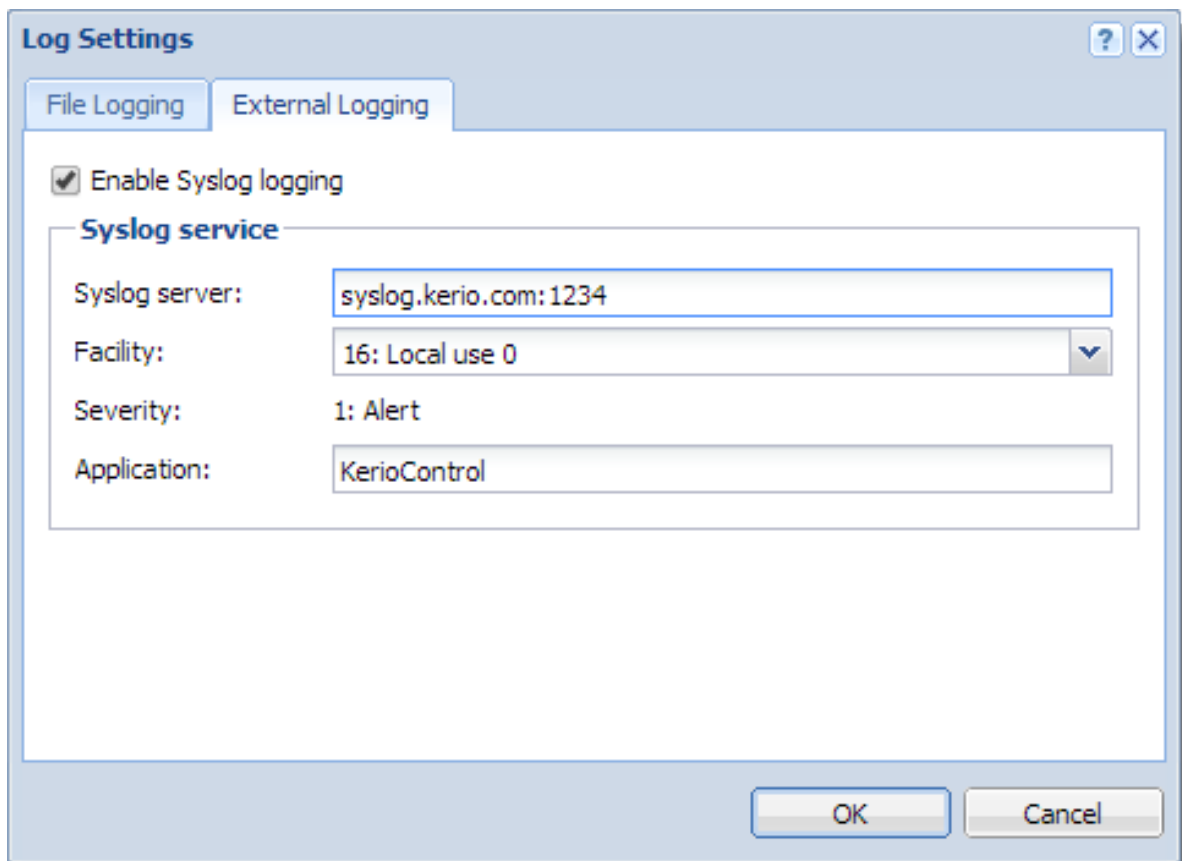


Figure 1 Syslog settings for the Alert log

The Syslog server distinguishes logs by **Facility** and **Severity**.

- **Facility** — The default value is 16: Local use 0, but you can change it as you need.
- **Severity** — The value is fixed for each log. **Severity** values are provided in table [1](#).

In the **Application** field, you can type a description displayed in the Syslog server.

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>Host</i>	6: Informational
<i>Http</i>	6: Informational
<i>Security</i>	5: Notice
<i>Warning</i>	4: Warning
<i>Web</i>	6: Informational

Table 1 Severity of Kerio Control logs

Detailed articles

Log	Article
Alert	Using Alert Messages
Config	Using the Config log
Connection	Using the Connection log
Debug	Using the Debug log
Dial	Using the Dial log
Error	Using the Error log
Filter	Using the Filter log
Host	Using the Host log
Http	Using the Http log
Security	Using the Security log
Warning	Using the Warning log
Web	Using the Web log

Logging packets

Packet logging

This function enables monitoring of IPv4 or IPv6 packets according to a user-defined log expression. The expression must be defined using special symbols.

Packet logging can be cancelled by removing the expression entry.



Kerio Control also offers a packet dump. The packet dump saves the wanted traffic to file which can be downloaded and opened by Wireshark.

Configuring packet logging

1. In the administration interface, go to **Logs** → **Debug**.
2. In the context menu, click **Packet Logging**.
3. Type an expression.
4. Click **OK**.

Logical Expression

Packets can be described by logical expressions following this pattern:

`variable1 = value1 & variable2 = value2 | variable3 = value3`

where:

- `variable1 ... variableN` are characteristic information about the packet (see below)
- `&` is the logical operator **and**
- `|` is the logical operator **or**

Interpretation of logical expressions

Expressions are parsed according to the priority of the individual operators: the `&` operator is parsed before `|`. If multiple conditions are connected by the same operator, the expression is

parsed from left to right. If necessary, parentheses can be used to determine the priority of conditions:

```
variable1 = value1 & (variable2 = value2 | variable3 = value3)
```

Variables

The following variables can be used in logical expressions defining packets:

any

All IP packets are logged (the condition is always met). It would be meaningless to combine the any option with other condition(s).

addr

Source or destination IP address of the packet.

saddr

Source IP address.

daddr

Destination IP address.

Define conditions for addr, saddr, daddr as follows:

Condition	Description
= 1.2.3.4	IPv4 address of the host
= 1.2.3.4/255.255.255.0	subnet defined by the network IPv4 address and a corresponding subnet mask
= 1.2.3.4/24	subnet defined by the network IPv4 address and number of bits of the corresponding subnet mask
= 1.2.3.4-1.2.3.10	IPv4 range (inclusive)
= 2001:abcd:1234::1	IPv6 address of the host
= list:"name of IP group"	IP address group
= user:"user1,user2,[group1],user3,[group2]"	IP addresses of hosts from which the users are connected

For IPv6 protocol, you can enter only host addresses. It is not possible to specify a subnet by the prefix and its length or by an address range.

port

Number of source or destination port (TCP or UDP).

Logging packets

sport

Source port number.

dport

Destination port number.

if

Interface (in any direction).

iif

Incoming interface.

oif

Outgoing interface.

Allowed conditions:

Condition	Description
= "interface name"	Interface name used by Kerio Control
= vpnclient	Any VPN client
= vpn	Any VPN client
= vpn:"name of VPN connection"	Name of VPN connection

direc

Packet direction:

- = in — incoming packet
- = out — outgoing packet

tcpfl

Flags in TCP header.

Options: FIN SYN RST PSH ACK URG NONE (none) ALL (all).

Any TCP packet containing specified flags (their value is 1) meet the condition. Flags not used in the specification are ignored.

Individual flags of the tcpfl variable can be marked either by the + symbol (the flag is enabled) or by the - symbol (the flag is disabled). All conditions are flagged by default unless one of these symbols is used.

Example: The tcpfl = SYN +ACK -RST expression is met by any packet flagged by SYN and ACK that has a disabled RST flag.

Examples

This logical expression defines Microsoft Networking service packets at the Internet interface:

```
if = "Internet" & (port >= 137 & port <= 139 | port = 445)
```

This expression defines packets going out through the Internet interface and directed to the WWW server with IP address 123.32.45.67 at port 80 or 8080:

```
oif = "Internet" & daddr = 123.32.45.67 & (dport = 80 | dport = 8080)
```

This expression defines incoming TCP packets flagged by SYN (TCP connection establishment):

```
direc = in & tcpfl = SYN
```

Creating and downloading packet dumps

1. In the administration interface, go to **Logs** → **Debug**.
2. In the context menu, click **Packet Dump To File**.
3. Type an expression.
4. To create the packet dump and start logging, click **Start**.
5. Do you have enough information? Click **Stop**.
6. Click **Download** and save the file to your computer.

Log packet formatting

Log packet formatting

Log packet formatting in the debug and filter logs allows further customization of the output to make the logs easier for you to read. This article explains these customization options and how to use them.

1. In the administration interface, go to **Logs** → **Debug/Filter**.
2. In the context menu, click **Format of logged packets**.
3. [Type an expression](#).
4. Click OK.

Creating expressions

Format of logged packets is defined by special expressions (a template). You can edit this template to get transparent and relevant information.

Default template

The default template for packet logging follows this pattern:

`%DIRECTION%, %IF%, proto:%PROTO%, len:%PKTLEN%, %SRC% - %DST%, %PAYLOAD%`

Expressions introduced with % are variables. Other characters and symbols represent static text as printed in the log.

Variables

The following variables can be used in packet logging templates:

- `%DIRECTION%` — traffic direction in respect of the particular network interface of the firewall (incoming / outgoing)
- `%IF%` — interface name
- `%PROTO%` — protocol type (TCP, UDP, etc.)
- `%PKTLEN%` — packet size
- `%SRC%` — source IP address and port (depending on the protocol attribute Raw)

- %DST% — destination IP address and port (depending on the protocol attribute Raw)
- %SRCMAC% — source MAC address
- %DSTMAC% — destination MAC address
- %PAYLOAD% — size of the data part of the packet with details provided (depending on the protocol and attribute Raw)
- %PAYLOADLEN% — size of the data part of the packet
- %DSCP% — DSCP value in the IP header

If you wanted to track the direction on an interface, the source and destination and size of the packet:

```
%DIRECTION% %IF%, %SRC% >> %DST%, length %PKTLEN%
```

Which would result in the following:

```
[08/Sep/2012 11:47:39] PERMIT "Firewall traffic" packet from WAN,  
192.168.52.2:53 >> 192.168.52.128:1035, length 96
```

```
[08/Sep/2012 11:47:39] PERMIT "Firewall traffic" packet to WAN,  
192.168.52.128:1035 >> 192.168.52.2:53, length 63
```

If you wanted to also show the protocol that was being used the following would display this:

```
%DIRECTION% %IF% %PROTO% (%SRC% >> %DST%)
```

Which would result in the following:

```
[08/Sep/2012 16:12:33] PERMIT "Firewall traffic" packet to  
WAN UDP (192.168.52.128:1121 >> 192.168.52.2:53)
```

```
[08/Sep/2012 16:12:33] PERMIT "Firewall traffic" packet from  
WAN UDP (192.168.52.2:53 >> 192.168.52.128:1121)
```



After this change has been applied the logs will update with the new view. This change is not retroactive and will not alter the previous format of your log data. This change will be applied to both the **Filter** and **Debug** log at the same time, it is not possible to set different customizations for each log.

Using the Config log

Config log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

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.

Reading the Config log

The Config window contains three log types:

1. *Information about logging in to Kerio Control administration*

Example

```
[18/Apr/2013 10:25:02] winston - session opened
for host 192.168.32.100. User-Agent: Mozilla/5.0 (Windows NT
6.1; WOW64; rv:22.0)
Gecko/20100101 Firefox/22.0.
[18/Apr/2013 10:32:56] winston - session closed
for host 192.168.32.100
```

- [18/Apr/2013 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
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0. — information about the used browser
- 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/2013 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/2013 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)

Using the Connection log

Connection log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

The Connection log gathers:

- traffic matching traffic rules with the **Log connections** enabled (see screenshot [1](#)),

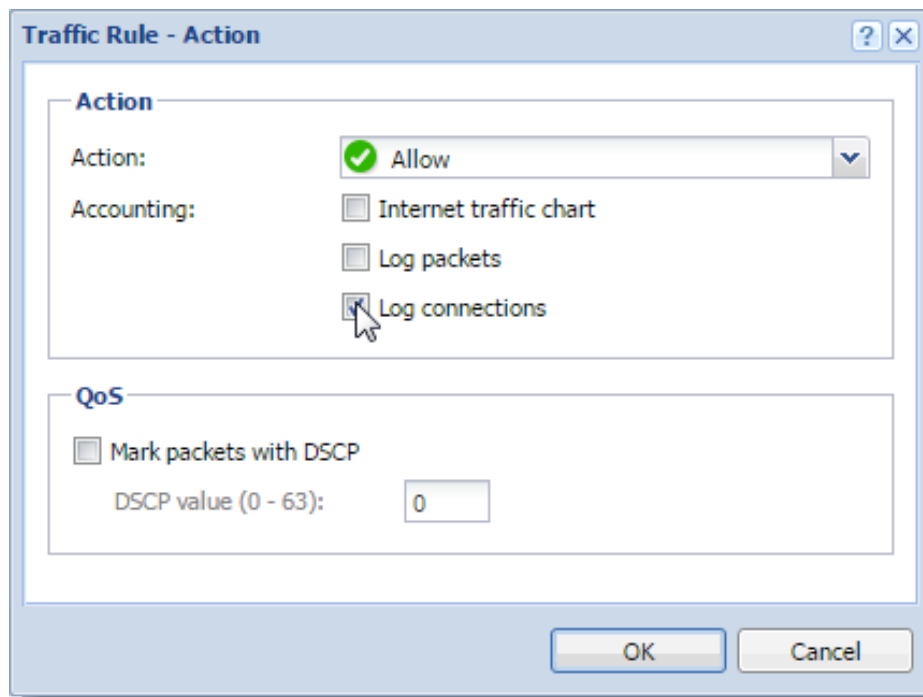


Figure 1 Traffic Rules → Action

- log of UPnP traffic with the **Log connections** enabled (**Security Settings** → **Zero-configuration Networking**),
- information on IPv6 connections with the **Log connections** enabled (**Security Settings** → **IPv6**).

Reading the Connection log

[18/Apr/2013 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/2013 10:22:47] — date and time when the event was logged (Note: Connection logs are saved immediately after a 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.
- [User] winston 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).

Using the Debug log

Debug log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

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.

Using the Debug log

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.

For more details, see article [Log packet formatting](#).

Packet Logging

This function enables monitoring of IPv4 or IPv6 packets according to the user defined log expression.

Logging of IP traffic can be cancelled by leaving or setting the **Expression** entry blank.

For more details, see article [Logging packets](#).

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.

Packet Dump To File

This function enables monitoring of IPv4 or IPv6 packets according to the user defined log expression and saving the Debug log to the special file. The packet dump can be downloaded and saved in your computer and opened by Wireshark.

For more details, see article [Logging packets](#).



If the expression is too general, the packet dump file gets large and exhausts free disk space. The network traffic is continuously dumped, even after the administrator logs out of the administration. For those reasons, some time after the recording starts a warning notification appears in the administration interface.

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),
- **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),
- **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.),
- **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 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, etc.
- **IPsec** — detailed information about IPsec traffic:
 - Select **General** for general information about IPsec tunnel.
 - Select **Charon output** for solving problems with ciphers (the same cipher must be used on both endpoints).
 - Select **L2TPD output/PPPD output** for solving problems with L2TP/PPP tunnels.

Using the Dial log

Dial log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

The Dial log displays data about dialing and hanging up the dial-up lines, and about time spent on-line.

Reading the Dial log

1. Manual connection (from Kerio Control administration or Kerio Control client interface)

[31/Jul/2013 11:41:48] Line "Connection" dialing manually from IP 10.10.10.60, user admin.

[31/Jul/2013 11:42:04] Line "Connection" connected

The first log item is reported upon initialization of dialing. The log provides information about line name, IP address and username.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

2. Automatic connections

Automatic dialing due to time range is logged as:

[10/Jul/2013 14:19:22] Line "Kerio PPPoE" dialing due to configured connect time.

Automatic dialing due to configured connectivity options (e.g. Link Load Balancing) is logged as:

[10/Jul/2013 14:34:44] Line "Kerio PPPoE" dialing, required by internet connectivity.

3. Line disconnection (manual or automatic, performed after a certain period of idleness)

15/Mar/2013 15:29:18] Line "Connection" hanging up, manually from IP 10.10.10.60, user Admin.

[15/Mar/2013 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`).

4. Disconnection caused by an error (connection is dropped)

```
[15/Mar/2013 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).

5. Dial of the link on respond to a packet from local network

```
[15/Mar/2013 15:53:42] Packet  
TCP 192.168.1.3:8580 -> 212.20.100.40:80  
initiated dialing of line "Connection"
```

```
[15/Mar/2013 15:53:53] Line "Connection" successfully connected
```

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.).

Using the Error log

Error log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

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.

Reading the Error log

Pattern of Error logs

`[15/Apr/2013 15:00:51] (6) Automatic update error: Update failed.`

- `[15/Apr/2013 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, the number of users would break license limit, unable to find license file, Software Maintenance expiration, etc.),
- Internal errors (unable to read routing table or interface IP addresses, etc.),
- Configuration errors (unable to read configuration file, detected aloop in the configuration of the DNS module or the Proxy server, etc.),
- Network (socket) errors,

- Errors while starting or stopping the Kerio Control (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.),
- VPN errors,
- HTTP cache errors (errors when reading/writing cache files, not enough space for cache, etc.),
- 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 administration 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.

Using the Filter log

Filter log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

The Filter 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 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.

Selection of information monitored by the Filter log

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. To configure the template:

1. In the administration interface, go to **Logs** → **Filter**.
2. In the context menu, click **Format of logged packets**.
3. Type an expression.
4. Click OK.

For more information, see article [Log packet formatting](#).

Reading the Filter log

Example of a URL rule log message

```
[18/Apr/2013 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/2013 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/2013 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/2013 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

Using the Filter log

- **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)

Using the Host log

Host log overview



New in Kerio Control 8.3!

Logs keep information records of selected events occurred in, or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

This log gives you information on who, when and which address and machine accesses the Kerio Control network.

Reading the Host log

An example of user registration

```
[02/Mar/2014 13:36:49] [IPv4] 192.168.40.131
[MAC] 00-10-18-a1-c1-de (Apple) - Host registered

[02/Mar/2014 13:37:56] [IPv4] 192.168.40.131
[MAC] 00-10-18-a1-c1-de (Apple) [User] jsmith@company.com - User logged
in

[02/Mar/2014 16:48:52] [IPv4] 192.168.40.131
[MAC] 00-10-18-a1-c1-de (Apple) - User jsmith@company.com logged out

[02/Mar/2014 16:48:52] [IPv4] 192.168.40.131
[MAC] 00-10-18-a1-c1-de (Apple) - Host removed
```

- [02/Mar/2014 13:36:49] — date and time when the action was happen
- [IPv4] 192.168.40.131 — IPv4 address of the client host
- [MAC] 00-10-18-a1-c1-de (Apple) — MAC address of the host. If the MAC address is not displayed, [Kerio Control is not able to see the MAC address of the host](#).
- jsmith@company.com —username authenticated through the firewall

An example of IP address leased from DHCP

```
[04/Mar/2014 12:07:28] [IPv4] 10.10.30.81 [MAC] 00-0c-29-1d-cc-bd (Apple)
[Hostname] jsmith-cp - IP address leased from DHCP
```

- [04/Mar/2014 12:07:28] — date and time when the action was happen
- [IPv4] 10.10.30.81 — IPv4 address of the client host
- [MAC] 00-0c-29-1d-cc-bd (Apple) — MAC address of the host. If the MAC address is not displayed, [Kerio Control is not able to see the MAC address of the host](#).
- [Hostname] jsmith-cp — computer hostname

An example of registering and removing an IPv6 address

IPv6 addresses are changed in time by the operating system of the host. See below an example of registering and removing such an IPv6 address on Kerio Control:

```
[04/Mar/2014 16:05:28] [IPv4] 10.10.30.81
[IPv6] 2001:718:1803:3513:b4c6:82b3:e0f5:309e [MAC] 00-0c-29-1d-cc-bd
(Apple)
[Hostname] jsmith-cp - IPv6 address 2001:718:1803:3513:b4c6:82b3:e0f5:309e
registered
```

```
[04/Mar/2014 16:23:25] [IPv4] 10.10.30.81
[MAC] 00-0c-29-1d-cc-bd (Apple) [Hostname] jsmith-cp -
IPv6 address 2001:718:1803:3513:b4c6:82b3:e0f5:309e removed
```

- [04/Mar/2014 16:05:28] — date and time when the action was happen
- [IPv4] 10.10.30.81 — IPv4 address of the client host
- [IPv6] 2001:718:1803:3513:b4c6:82b3:e0f5:309e — IPv4 address of the client host
- [MAC] 00-0c-29-1d-cc-bd (Apple) — MAC address of the host. If the MAC address is not displayed, [Kerio Control is not able to see the MAC address of the host](#).
- [Hostname] jsmith-cp — computer hostname

Using the Http log

Http log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

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 content 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 is better suited to be viewed by the Kerio Control administrator.

Reading the Http log

An example of an Http log record in the Apache format

```
192.168.64.64 - jsmith  
[18/Apr/2013:15:07:17 +0200]  
"GET http://www.kerio.com/ HTTP/1.1" 304 0 +4
```

- 192.168.64.64 — IP address of the client host
- jsmith — name of the user authenticated through the firewall (a dash is displayed if no user is authenticated through the client)
- [18/Apr/2013:15:07:17 +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).

Using the Http log

- 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

Using the Security log

Security log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

The Security log is a log for security-related messages.

Reading the Security log

Records of the following types may appear in the log:

Intrusion prevention system logs

Records of detected intrusions or traffic from IP addresses included in web databases of known intruders (blacklists).

```
[02/Mar/2013 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

Using the Security log

name of the particular host (if identifiable) or name of the user connected to the firewall from the particular local host

Anti-spoofing log records

Messages about packets that were captured by the *Anti-spoofing* module (packets with invalid source IP address).

```
[17/Jul/2013 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)

FTP protocol parser log records

Example 1

```
[17/Jul/2013 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/2013 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)

Failed user authentication log records

Message format:

Authentication: Service: Client: IP address: reason

- service — the Kerio Control service to which the client connects:
 - WebAdmin — web administration interface,
 - WebInterface — client interface,
 - HTTP Proxy — user authentication on the proxy server,
 - VPN Client — encapsulates both Kerio VPN and IPsec VPN ,
 - Admin — messages from the Console,
- IP address — IP address of the computer from which the user attempted to authenticate
- reason — reason of the authentication failure (nonexistent user/ wrong password)

Information about the start and shutdown of the Kerio Control Engine and some Kerio Control components

Start and shutdown of the Kerio Control Engine:

[17/Jun/2013 12:11:33] Engine: Startup

[17/Jun/2013 12:22:43] Engine: Shutdown

Start and shutdown of the Intrusion Prevention Engine:

[28/Jun/2013 10:58:58] Intrusion Prevention engine: Startup

[28/Jun/2013 11:18:52] Intrusion Prevention engine: Shutdown

Updating components

Kerio Control uses components (antivirus engine and signatures, Intrusion Prevention signatures and blacklists). Updates of these components are logged in the **Security** log:

[09/Jul/2013 17:00:58] IPS: Basic rules successfully updated to version 1.176

[10/Jul/2013 11:56:18] Antivirus update: Sophos database has been successfully updated. Sophos Scanning Engine (4.90.5198110/3.43.0.0) is now active.

Using the Warning log

Warning log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

The Warning log displays warning messages about errors of little significance. Warnings can display for example 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
- Kerio Control configuration issues (invalid values retrieved from the configuration file),
- Warnings of Kerio Control 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),
- Bandwidth Management warnings,
- Kerio Control Web Filter alerts,
- Crashdumps after failure of the application.

Reading the Warning log

The connection limit configured in **Security Settings** → **Miscellaneous** was exceeded:

[18/Jan/2013 11:22:44] Connection limit of 500 inbound connections reached for host 192.168.42.192.

Kerio Control could not be authorized to Kerio Web Filter. Kerio Web Filter is not working and users can open all web pages:

[02/Jan/2013 13:45:37] Unable to categorize 'example.com' by Kerio Web Filter. DNS response 'FAILURE: Invalid authorization' to query 'example.com.f836.ko-34554.v3.url.zvelo.com' is invalid.

Kerio Control was not able to contact registration server. You have to update your license manually:

[02/Jan/2012 15:54:20] License update failed: Automatic license update failed. User interaction is required by registration server

Using the Web log

Web log overview

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information about configuring and using logs, see article [Configuring and using logs in Kerio Control](#).

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.

Reading the Web Log

[24/Apr/2013 10:29:51] 192.168.44.128 james
"Kerio Technologies" http://www.kerio.com/

- [24/Apr/2013 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)
- http://www.kerio.com/ — URL pages

Using IP tools in Kerio Control

About IP tools

Kerio Control includes several tools you can use to troubleshoot connectivity issues, or to obtain information about a particular host or IP address. These tools are located under **Status** → **IP Tools**.

To use an IP tool:

1. In the administration interface, go to Status → IP Tools and click the tool's tab.
2. Type parameters into the appropriate fields.
3. Click the **Start** button.
4. Refer to the **Command output** window for the tool's output.
5. When you have enough data for analysis, click the **Stop** button.

Ping

The **Ping** tool is used to test connectivity between two hosts.

For example, if you believe a web site may be down, you can ping the server address to verify connectivity to that host.



Some hosts filter ping requests. In that case, the ping command cannot accurately test connectivity to that host.

Parameters for Ping

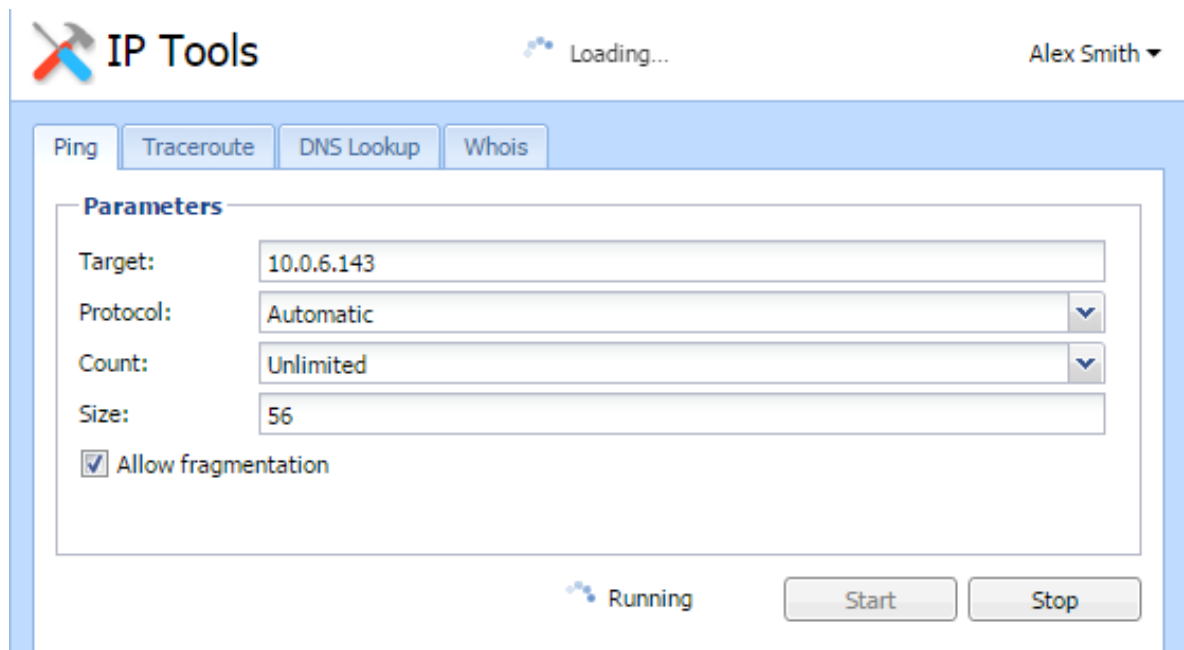
Target — IP address or hostname of the remote host.

Protocol — IPv4 or IPv6.

Count — The number of ping attempts.

Size — Default value is 56.

Allow fragmentation — enable this option to allow the ping request to be broken into smaller packets by other routers, if necessary.



Traceroute

The **Traceroute** tool is used to check the route (path) between two hosts.

For example, if you cannot ping a remote host, or if the response time is very slow, you can use **Traceroute** to determine where the problem may be occurring.

Parameters for Traceroute

Target — IP address or hostname of the remote host.

Protocol — IPv4 or IPv6.

Resolve addresses to hostnames — Enable this option to display the reverse lookup name (if available) for each IP host in the path.

DNS Lookup

A DNS lookup is a process that queries a domain name server to resolve the IP address of a given hostname.

For example, if an application such as a web browser reports errors resolving a hostname, you can perform a DNS lookup to verify the response from a given DNS server.

Parameters for DNS Lookup

Name — The hostname or IP address to query, such as `www.kerio.com`.

Tool — Specifies the tool used and the output format (`nslookup` or `dig`).

Server — Specifies the DNS server to query. The server list is populated from DNS servers assigned to each network interface.

Type — Specifies the type of the DNS query, such as A, TXT, SRV.

Command output

```
Server:          10.0.0.254
Address: 10.0.0.254#53

Name:   kerio.com
Address: 166.78.1.97
```

Whois

The Whois tool is used to obtain ownership information for an Internet resource, such as a domain name or IP address.

For example, if you would like to obtain ownership information about a suspicious intrusion attempt, you can perform a `whois` lookup for the offending host.

Input an IP address or hostname into the **Host** field to perform a whois query.

SNMP monitoring

Configuring Kerio Control

SNMP is a protocol which allows you to monitor Kerio Control status.

1. In the administration interface, go to **Configuration** → **Accounting and Monitoring** → **SNMP**.
2. Check **Enable SNMP monitoring**.
3. In the **Location** field, type any text which will help you recognize the server and its location.
4. In the **Contact** field, type your contact information which will help you recognize the server and its location.
5. Select which version to use — 2c or 3 (both versions are read-only).

Version 2c supports passwords as plain text only (community string), version 3 supports encryption (SHA-1). Some monitoring tools, however, do not support version 3.



Use the [snmpwalk](#) command to list all available object identifiers.

Cacti

Cacti is a monitoring tool which can handle the SNMP protocol.

In the web administration of Cacti, go to the **Devices** section, add a new device, provide a description, then enter the hostname or IP address of Kerio Control. Specify the SNMP version (usually version 2) and the community previously defined in the Kerio Control administration. Leave the other values as default.

Devices [new]	
General Host Options	
Description Give this host a meaningful description.	<input type="text" value="Kerio Control"/>
Hostname Fully qualified hostname or IP address for this device.	<input type="text" value="gw.company.com"/>
Host Template Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.	<input type="text" value="None"/>
Number of Collection Threads The number of concurrent threads to use for polling this device. This applies to the Spine poller only.	<input type="text" value="1 Thread (default)"/>
Disable Host Check this box to disable all checks for this host.	<input type="checkbox"/> Disable Host
Availability/Reachability Options	
Downed Device Detection The method Cacti will use to determine if a host is available for polling. <i>NOTE: It is recommended that, at a minimum, SNMP always be selected.</i>	<input type="text" value="SNMP Uptime"/>
Ping Timeout Value The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.	<input type="text" value="400"/>
Ping Retry Count After an initial failure, the number of ping retries Cacti will attempt before failing.	<input type="text" value="1"/>
SNMP Options	
SNMP Version Choose the SNMP version for this device.	<input type="text" value="Version 2"/>
SNMP Community SNMP read community for this device.	<input type="text" value="public"/>
SNMP Port Enter the UDP port number to use for SNMP (default is 161).	<input type="text" value="161"/>
SNMP Timeout The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).	<input type="text" value="500"/>
Maximum OID's Per Get Request Specified the number of OID's that can be obtained in a single SNMP Get request.	<input type="text" value="10"/>
Additional Options	
Notes Enter notes to this host.	<div></div>
<div>Cancel Create</div>	

Generating a bootable USB flash drive for Kerio Control software appliances

Overview

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 drive.



All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.

Please follow the instructions according to your operating system:

Windows

1. Insert the USB flash drive into a USB port on your computer.
2. Download the `kerio-control-installer.iso` file.
3. Download and unpack [Image Writer](#) (it does not require installation).
4. In Image Writer, find the `kerio-control-installer.iso` file, select your flash drive and click **Write**.
5. Eject the flash drive securely and remove it from your computer.

Linux

1. Insert the USB flash drive into a USB port on your computer.
2. Run the terminal (console) in the super-user mode (e.g. using commands `su` or `sudo -s` — depending on your Linux distribution).
3. Use the command `fdisk -l` to detect the USB flash drive name (e.g. `/dev/sdb`).
4. Save the drive image to the USB flash drive using this command:

```
dd if=kerio-control-installer.iso of=/dev/sdx bs=1M
```

replace `kerio-control-installer.iso` by the real file name and `/dev/sdx` with the actual device name. 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 drive operations.

- 6.

Eject the USB drive safely and remove it from the USB port.

OS X

1. Insert the USB flash drive into a USB port on your computer.
2. Run the terminal (**Applications** → **Utilities** → **Terminal**).
3. Use the command `sudo diskutil list` to detect the USB flash drive name (e.g. `/dev/diskX` or `/dev/DiskY` — mind the letter case).
4. Use the command `sudo diskutil unmountDisk /dev/diskX` to unmount the flash drive.



This is case sensitive.

5. Save the drive image file to the USB flash drive by using this command:

```
sudo dd if=kerio-control-installer.iso of=/dev/disk1 bs=1m
```

replace `kerio-control-installer.iso` by the real file name and `/dev/diskX` with the actual device name.
6. Eject the flash drive securely and remove it 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).
5. A SSL Certificate must be installed and configured correctly for Kerio Control.

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.

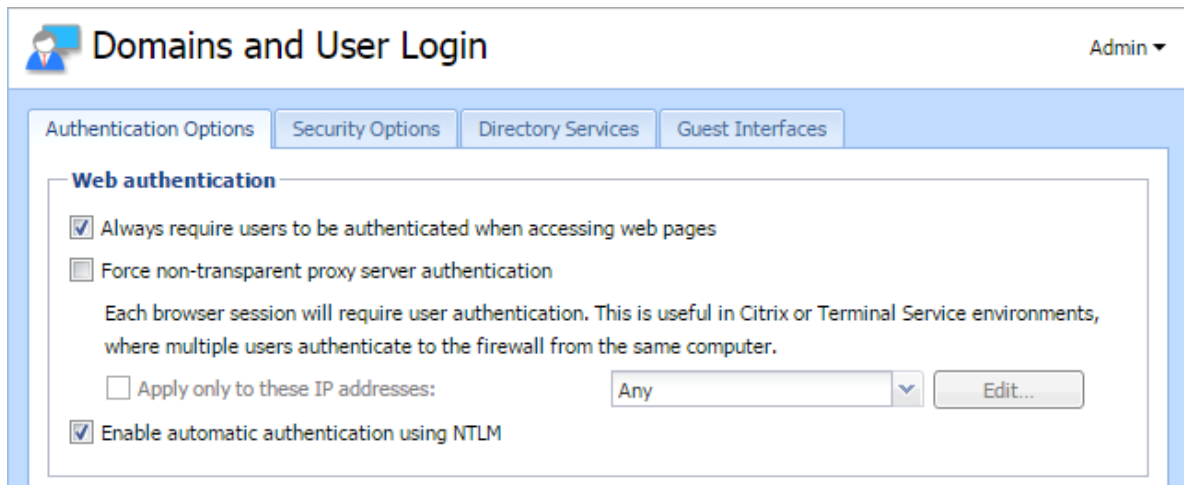


Figure 1 NTLM — user authentication options

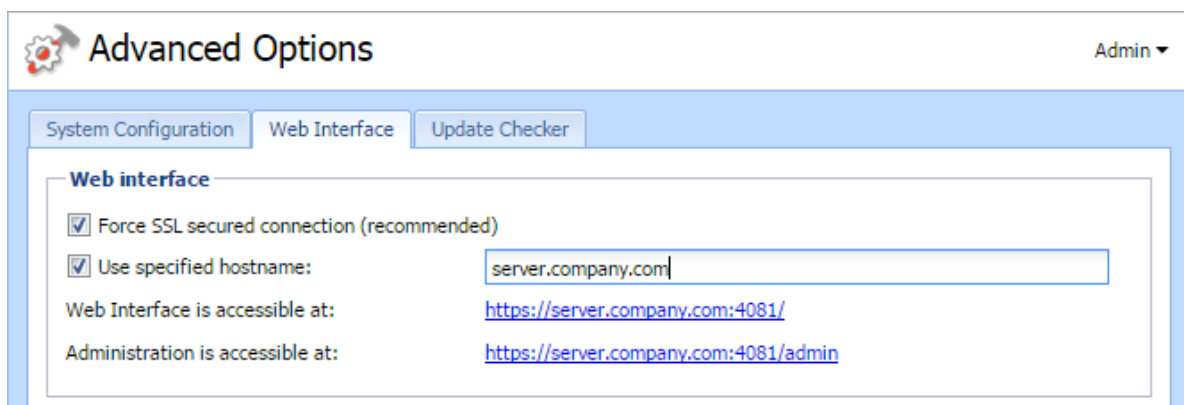


Figure 2 Kerio Control's Web interface configuration

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.

Automatic user authentication using NTLM

- 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.

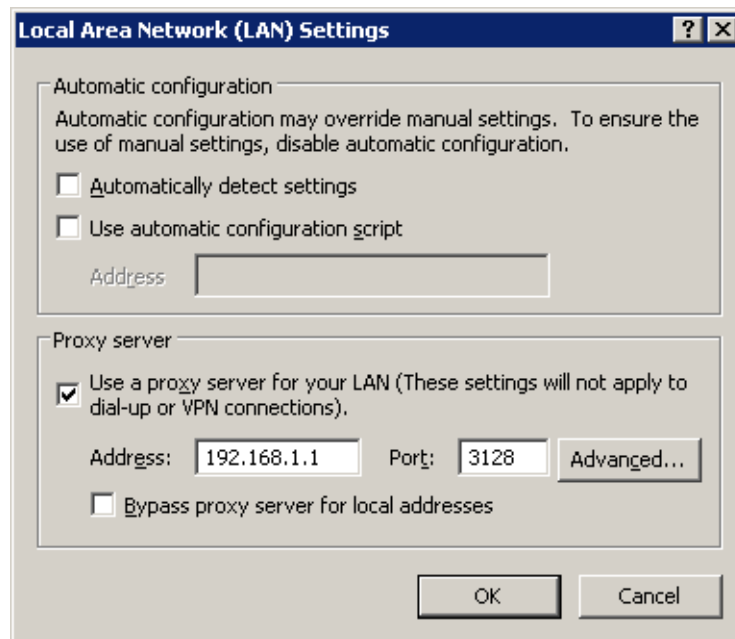


Figure 1 Configuring proxy server in Internet Explorer

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).

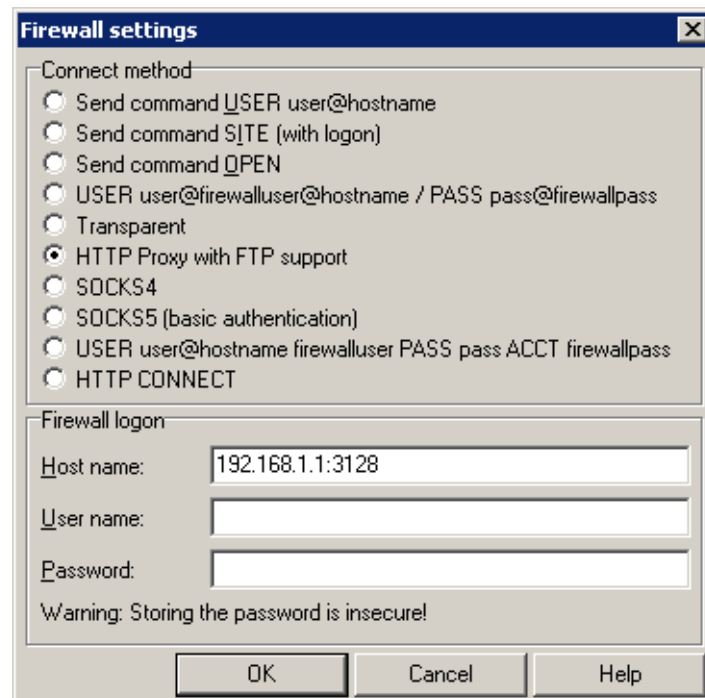


Figure 2 Setting proxy server for FTP in Total Commander

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.

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.

Navigation bar

Tap an icon in the left menu and a navigation bar appears.

Tap the main window and the navigation bar disappears.

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®, OS X®, 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/>

Heimdal Kerberos

Heimdal is an implementation of Kerberos 5, largely written in Sweden. It is freely available under a three clause BSD style license (but note that the tar balls include parts of Eric Young's libdes, which has a different license). Other free implementations include the one from MIT, and Shishi. Also Microsoft Windows and Sun's Java come with implementations of Kerberos.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Copyright ©1995-1997 Eric Young. All rights reserved.

Copyright ©1990 by the Massachusetts Institute of Technology

Copyright ©1988, 1990, 1993 The Regents of the University of California. All rights reserved.

Copyright ©1992 Simmule Turner and Rich Salz. All rights reserved.

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.

Net-SNMP

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment (eg. routers), computer equipment and even devices like UPSs. Net-SNMP is a suite of applications used to implement SNMP v1, SNMP v2c and SNMP v3 using both IPv4 and IPv6.

Copyright 1989, 1991, 1992 by Carnegie Mellon University

All Rights Reserved

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Copyright © 2001-2003, Networks Associates Technology, Inc

All Rights Reserved

Portions of this code are copyright © 2001-2003, Cambridge Broadband Ltd.

All Rights Reserved

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

All Rights Reserved

Copyright © 2003-2010, Sparta, Inc

All Rights Reserved

Copyright © 2004, Cisco, Inc and Information Network

All Rights Reserved

Center of Beijing University of Posts and Telecommunications.

All Rights Reserved

Copyright © Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

All Rights Reserved

OpenLDAP

Freely distributable LDAP (Lightweight Directory Access Protocol) implementation.

Copyright © 1998-2007 The OpenLDAP Foundation

Copyright ©1999, Juan C. Gomez, All rights reserved

Copyright ©2001 Computing Research Labs, New Mexico State University

Portions Copyright©1999, 2000 Novell, Inc. All Rights Reserved

Portions Copyright ©PADL Software Pty Ltd. 1999

Portions Copyright ©1990, 1991, 1993, 1994, 1995, 1996 Regents of the University of Michigan

Portions Copyright ©The Internet Society (1997)

Portions Copyright ©1998-2003 Kurt D. Zeilenga

Portions Copyright ©1998 A. Hartgers

Portions Copyright ©1999 Lars Uffmann

Portions Copyright ©2003 IBM Corporation

Portions Copyright ©2004 Hewlett-Packard Company

Portions Copyright ©2004 Howard Chu, Symas Corp.

Legal Notices

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.

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/>

Qt

Qt is a cross-platform application framework. It is released under LGPL license version 2.1.

Copyright © 2008 Nokia Corporation and/or its subsidiary(-ies)

Source code is available at

<http://download.kerio.com/archive/>

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 prevention and detection system (IDS/IPS). The package consists of snort itself, pcre, daq and dnet libraries. The package is distributed as a whole and licensed under GNU General Public License version 2.

Copyright © Kerio Technologies s.r.o.

Copyright © 2001-2013 Sourcefire Inc.

Copyright © 1998-2001 Martin Roesch

Copyright © 1997-2009 University of Cambridge

Copyright © 2007-2008, Google Inc.

Copyright © 2000-2006 Dug Song <dugsong@monkey.org>

Complete source code 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 developed 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.