



KerioControl

ADMINISTRATOR GUIDE

Find out how to install and configure Kerio Control in different environments and how to set up advanced features



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and Kerio Control are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

Kerio Control is copyright of Kerio. - 1999-2019 Kerio. All rights reserved.

Document Version: 9.2.8

Last updated (month/day/year): 02/09/2019

Contents

1 Introduction	8
2 Getting started	9
2.1 System requirements for Kerio Control	10
2.2 Configuration Assistant	10
2.2.1 Configure Internet connection and the local network	10
2.2.2 Define traffic policy	13
2.2.3 Export your configuration	14
2.2.4 Import configuration files	14
2.2.5 Register product	15
2.3 Logging to Kerio Control	15
2.4 Adding Kerio Control to MyKerio	16
2.4.1 Adding Kerio Control to MyKerio through Kerio Control Administration	16
2.4.2 Adding Kerio Control to MyKerio during the Kerio Control installation	17
2.5 Upgrading Kerio Control	18
2.5.1 Checking new versions	18
2.5.2 Automatic upgrade of Kerio Control	19
2.5.3 Configuring email alerts	19
2.5.4 Upgrade with USB tools	19
2.5.5 Troubleshooting	19
2.5.6 Upgrading to the latest version from Kerio Control 9.1 and newer	19
2.5.7 Upgrading to the latest version from Kerio Control 8 & 9.0	20
2.5.8 Upgrading to the latest version from Kerio Control 7	20
2.6 Installation	21
2.6.1 Installing Kerio Control	22
2.6.2 Configuring the Activation Wizard	23
2.6.3 Generating a bootable USB flash drive for Kerio Control software appliances	30
2.6.4 Increasing the number of supported network interfaces in the Kerio Control VMware Virtual Appliance	31
2.6.5 Migrating from Kerio Control (Windows Edition) to the Appliance Editions (Software/Virtual/Hardware)	31
2.6.6 Kerio Control Virtual Appliance for Hyper-V	33
2.6.7 Kerio Control VMware Virtual Appliance	35
2.7 Licenses and registration	37
2.7.1 Licensing and registering Kerio Control	38
2.7.2 Transferring the configuration and license from the Windows version of Kerio Control to the Software or Virtual Appliance edition	40
2.7.3 How do I apply renewals or add-ons to my Kerio product?	40
2.8 Hardware appliance	41
2.8.1 Kerio Control NG series installation guide	41
2.8.2 End of life of Kerio Control Box 1110	43
2.8.3 Configuring Ethernet ports in Kerio Control hardware appliances	44
2.8.4 Migrating configuration from one Kerio Control hardware appliance to another	47
2.8.5 Connecting to Kerio hardware appliances with a serial console	52
2.8.6 WiFi	57
2.9 Kerio Control API	66
3 Using	67
3.1 Using Dashboard in Kerio Control	67
3.2 Tips for tablets	68
3.3 Antivirus	69
3.3.1 Configuring antivirus protection	69

3.3.2 Configuring email scanning	70
3.3.3 Configuring HTTP and FTP scanning	71
3.3.4 Using an external antivirus with Kerio products	72
3.4 Backup	73
3.4.1 Saving configuration to FTP server	73
3.4.2 Saving configuration to MyKerio	75
3.4.3 Saving configuration to Samepage	76
3.5 Accounts	77
3.5.1 Managing user accounts in Kerio Control	78
3.5.2 Setting access rights in Kerio Control	81
3.5.3 Managing user quotas in Kerio Control	81
3.5.4 Blocking web object elements for particular users	84
3.5.5 Configuring automatic user login	85
3.5.6 Creating user groups in Kerio Control	86
3.5.7 Authenticating users to Kerio Control	87
3.6 Directory services	89
3.6.1 Connecting Kerio Control to directory service	89
3.6.2 Automatic user authentication using NTLM	92
3.6.3 How do I force users to log out of the firewall?	95
3.6.4 How to use a Windows Active Directory Group Policy Object (GPO) to logon and logout users automatically from Kerio Control	96
3.6.5 Optimizing the communication between Kerio Control and Active Directory	109
3.7 Monitoring	110
3.7.1 Monitoring active hosts	110
3.7.2 Monitoring active connections	114
3.7.3 Monitoring System Health in Kerio Control	116
3.7.4 Monitoring traffic in Kerio Control	116
3.7.5 Monitoring user statistics	119
3.7.6 Monitoring VPN clients	121
3.7.7 SNMP monitoring	122
3.8 Logs	123
3.8.1 Using and configuring logs	124
3.8.2 Using the Config log	128
3.8.3 Using the Connection log	129
3.8.4 Using the Debug log	130
3.8.5 Using the Dial log	132
3.8.6 Using the Error log	133
3.8.7 Using the Filter log	134
3.8.8 Using the Host log	135
3.8.9 Using the Http log	137
3.8.10 Using the Security log	138
3.8.11 Using the Warning log	140
3.8.12 Using the Web log	141
3.8.13 Logging packets	141
3.8.14 Log packet formatting	144
3.9 VPN	145
3.9.1 Configuring Kerio VPN	145
3.9.2 Configuring IPsec VPN Server	154
3.9.3 Routing all traffic through Kerio VPN Tunnel	172
3.9.4 Connecting multiple offices via Kerio VPN and IPsec VPN tunnels	176
3.9.5 Assigning static IP addresses for Kerio Control VPN Clients	181
3.9.6 Kerio Control VPN Client for administrators	182

3.9.7 Using Logs to troubleshoot VPN Client issues	182
4 Settings	184
4.1 Interfaces	184
4.1.1 Configuring network interfaces	184
4.1.2 Configuring the guest network	187
4.1.3 Configuring PPPoE connections	190
4.1.4 Configuring PPTP tunnel	191
4.1.5 Configuring TCP/IP settings in Kerio Control interfaces	192
4.1.6 Configuring L2TP tunnel	194
4.1.7 Configuring multiple WAN IPs with PPPoE	196
4.1.8 Configuring VLANs	199
4.1.9 Changing MAC addresses of network interfaces	200
4.1.10 Changing the MTU of network interfaces	201
4.1.11 Changing the speed and duplex settings of Ethernet interfaces	202
4.1.12 Using alert messages	204
4.1.13 Sending log message alerts	208
4.1.14 Using IP Tools	210
4.2 Security	212
4.2.1 Configuring 2-step verification	212
4.2.2 Blocking all incoming connections from specified countries in Kerio Control	215
4.2.3 Configuring connection limits	217
4.2.4 Configuring intrusion prevention system	221
4.2.5 Filtering MAC addresses	222
4.2.6 Protecting users against password guessing attacks	223
4.2.7 Protocol inspection in Kerio Control	224
4.2.8 Encrypting User Data	227
4.3 IPv6	228
4.3.1 Configuring IPv6 networking in Kerio Control	228
4.3.2 Support for IPv6 protocol	230
4.3.3 Configuring traffic rules for IPv6 network	231
4.4 Traffic rules	235
4.4.1 Configuring traffic rules	236
4.4.2 Configuring IP address translation	241
4.4.3 Configuring Demilitarized Zone (DMZ)	244
4.4.4 Configuring traffic rules - exclusions	245
4.4.5 Configuring traffic rules - multihoming	245
4.4.6 Limiting Internet access with traffic rules	247
4.4.7 Troubleshooting traffic rules	248
4.5 Content filtering	251
4.5.1 Configuring the Content Filter	251
4.5.2 Application awareness in Kerio Control	258
4.5.3 Configuring FTP policy	267
4.5.4 Configuring HTTP policy	268
4.5.5 Filtering web content by word occurrence	272
4.5.6 Blocking inappropriate or explicit content in search results	273
4.5.7 Filtering HTTPS connections	275
4.5.8 HTTPS filtering specifics	279
4.5.9 Using Kerio Control Web Filter	279
4.5.10 Slow Internet connection with activated Kerio WebFilter	281
4.5.11 Eliminating Peer-to-Peer traffic	282
4.6 Bandwidth optimization	284
4.6.1 Configuring bandwidth management	284

4.6.2 Configuring policy routing	289
4.6.3 Setting limit per host	292
4.6.4 Detecting large data transfers	293
4.6.5 Bandwidth management - setting the speed of the link	294
4.7 Proxy server	294
4.7.1 Configuring proxy server	294
4.7.2 Configuring the reverse proxy	297
4.8 Server configuration	302
4.8.1 Configuring a routing table in Kerio Control	303
4.8.2 Configuring HTTP cache	306
4.8.3 Configuring Service Discovery forwarding in the Kerio Control network	307
4.8.4 Configuring the Kerio Control web interface	308
4.8.5 Configuring system settings date, time, time zone and server name	309
4.8.6 Customizing logo on Kerio Control login page, denial pages and user alerts	312
4.8.7 Customizing the language used in Kerio Control interfaces	312
4.8.8 Configuring statistics and reports	313
4.8.9 Configuring the SMTP server	318
4.8.10 DHCP server in Kerio Control	319
4.8.11 DNS forwarding service in Kerio Control	323
4.8.12 Modifying parameters in Kerio Control configuration	325
4.8.13 Optimizing performance with large segment offload	326
4.8.14 Using RADIUS server in Kerio Control	327
4.8.15 Configuring IP address groups	332
4.8.16 Configuring URL groups	335
4.8.17 Services in Kerio Control	337
4.8.18 Creating time ranges in Kerio Control	338
4.8.19 Configuring Universal Plug-and-Play (UPnP)	340
4.8.20 Using Remote Desktop IP Virtualization	341
4.8.21 Wildcards and regular expressions in URL	342
4.8.22 Dynamic DNS for public IP address of the firewall	342
4.9 SSL certificates	343
4.9.1 Configuring SSL certificates in Kerio Control	343
4.9.2 Exporting and importing Kerio Control local authority as root certificate	346
4.9.3 Changing SSL certificates in Kerio Control	347
4.9.4 Deploying Kerio Control certificate via Microsoft Active Directory	347
5 Troubleshooting	349
5.1 How do I generate a network trace (packet dump) for Kerio technical support?	349
5.1.1 Discussion	349
5.1.2 Windows and MacOSX	349
5.1.3 Linux	349
5.2 Common issues	350
5.2.1 Authenticating iPhone 5 (iOS6) device to WiFi fails	350
5.2.2 Dshield Identified Top Attackers blocks access from LAN	351
5.2.3 I have a page that is miscategorized by Kerio Web Filter	351
5.2.4 Redirecting users to the authentication page does not work, the page cannot be displayed.	352
5.2.5 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded) ..	352
5.2.6 Browser extensions or add-ons may interfere with Kerio products	352
5.2.7 User is prompted for credentials	353
5.2.8 Troubleshooting SSL certificates	354
5.3 Wifi issues	355
5.3.1 WiFi connection is slow	355
5.3.2 Wireless devices cannot connect to WiFi	356

5.4 USB tools	356
5.4.1 Recovering your Kerio Control Box NG series password using a USB flash drive	357
5.4.2 Recovering your Kerio Control password using a USB flash drive	357
5.4.3 Restoring the Kerio Control Box NG series default configuration using a USB flash drive	358
5.4.4 Restoring the Kerio Control default configuration using a USB flash drive	362
5.4.5 Updating Kerio Control Box NG series using a USB flash drive	365
5.4.6 Updating Kerio Control using a USB flash drive	365
5.4.7 Diagnostic tool for Kerio Control Box	367
5.4.8 Diagnostic tool for Kerio Control Box NG series	368
5.5 Vulnerabilities	369
6 Glossary	371
7 Legal Notices	378
7.1 Trademarks and registered trademarks	378
7.2 Open source software	378
7.2.1 bindlib	378
7.2.2 Clearsilver	378
7.2.3 Firebird	378
7.2.4 Heimdal Kerberos	379
7.2.5 h323plus	379
7.2.6 KIPF — driver	379
7.2.7 KIPF — API	379
7.2.8 KVNET — driver	379
7.2.9 KVNET — API	380
7.2.10 libcurl	380
7.2.11 libiconv	380
7.2.12 libmbfl	380
7.2.13 libxml2	380
7.2.14 Net-SNMP	380
7.2.15 OpenLDAP	381
7.2.16 OpenSSL	381
7.2.17 Operating system	381
7.2.18 PHP	381
7.2.19 Prototype	382
7.2.20 ptlib	382
7.2.21 Qt	382
7.2.22 ScoopyNG	382
7.2.23 Snort	382
7.2.24 strongSwan	382
7.2.25 zlib	383

1 Introduction

Kerio Control provides a combination of Unified Threat Management and Next-Generation firewall which helps you to protect, manage and monitor your network and users' behavior.

Kerio Control, as a Unified Threat Management solution, preserves the integrity of your servers with deep packet inspection and advanced network routing capabilities, including simultaneous IPv4 and IPv6 support. You can create inbound and outbound traffic policies, restrict communication by specific URL, application, traffic type, content category and time of day.

IPS adds a transparent layer of network protection, with Snort-based behavior analysis, and a regularly updated database of rules and blacklisted IP addresses from Emerging Threats.

The optional anti-virus service scans all web and FTP traffic, email attachments and downloads, automatically updating itself with the latest virus definitions. Kerio Antivirus allows you to keep viruses, worms, trojans and spyware from infesting your network.

The optional Kerio Control Web Filter with application awareness limits legal liability, protects your network and boosts user productivity by limiting user access to dangerous or inappropriate sites or those that just plain waste time.

You can easily prioritize and monitor network traffic to guarantee high-speed transmission for the most important traffic types. Internet Link Load Balancing optimizes Internet access by distributing traffic across multiple links. Kerio Control monitors link availability.

Kerio Control QoS gives you control over how much bandwidth each type of network traffic can consume.

You can get detailed usage reporting with Kerio Control Statistics. This component lets managers and admins view the Internet and application activities of individual users.

With Kerio Control VPN or industry-standard IPsec/L2TP, you can link headquarters to remote users and branch offices.

The Kerio Control web based administration is clean and simple, and you can upgrade to the latest version automatically or manually with just one click.

Kerio Control supports flexible deployment. You can opt for a software appliance, a virtual machine, or a performance-optimized hardware appliance. Remote deployment of hardware appliances is easier and faster than ever before with self-provisioning through [MyKerio](#).

2 Getting started

Would you like to try out Kerio Control? This topic provides a quick list of actions to help you get started with Kerio Control.

1 Choose deployment method

Kerio Control is available as a Software, Virtual, or Hardware appliance. The product features and functionality are nearly identical across all versions.

If the Virtual or Software Appliances, make sure your hardware meets the [system requirements](#). These appliances also require two Ethernet cards - one for the Internet interface and one or more cards for the local network (it depends on the topology of your network).

2 Install Kerio Control

To install the Software or Virtual Appliances, download the appropriate image files first. For more information, refer to [Installing Kerio Control](#) (page 22).

If you purchased Kerio Control Hardware Appliance, Kerio Control is already installed. Connect Ethernet cables to the Ethernet ports and run the Kerio Control Hardware Device. Read more: [NG series](#) or [NG-Wifi series](#).

After installation, Kerio Control automatically detects your Internet and local interfaces.

3 Access the user interface

It is recommended to access the Kerio Control user interface using MyKerio, which is a cloud service that enables you to administer numerous Kerio Control appliances from a single dashboard. To do this, add your Kerio Control instance to MyKerio first. For more information, refer to [Adding Kerio Control to MyKerio](#) (page 16).

Alternatively you can access the administration console from a web browser using the IP address of the firewall. Note that the computer from where you want to manage Kerio Control must be in the same IP subnet as the firewall.

4 Activate Kerio Control

When launching the administration interface the first time, run through the a configuration wizard to activate essential settings. For more information, refer to [Configuring the Activation Wizard](#) (page 23).

5 Define network interfaces and connectivity

Network interfaces in Kerio Control provide routing between local networks and the Internet. Configure networking parameters and define your Internet connectivity before any other types of firewall configuration. For more information, refer to [Configuring network interfaces](#) (page 184).

6 Assign parameters to local networks

Kerio Control simplifies management of the network by acting as a Dynamic Host Configuration Protocol (DHCP) server. DHCP automatically assigns networking parameters to connected devices. For more information, refer to [DHCP server in Kerio Control](#) (page 319).

7 Add user accounts

Specify the users to monitor and protect and configure users with permissions to manage the Kerio Control network. You can either create local user accounts or map the users from a directory service. For more information, refer to [Managing user accounts in Kerio Control](#) (page 78).

8 Enforce security and access policies

Kerio Control enforces security through Intrusion Prevention, Traffic Rules, Content Rules and Kerio Antivirus. These features are automatically configured to ensure that the firewall allows only legitimate network communications.

Read more about [Traffic rules](#), the [Content Filter](#), [Application awareness](#) and [Antivirus protection](#).

9 Enable remote access

You can use Virtual Private Networking (VPN) to allow remote users or entire networks to access services inside the local network. Kerio Control implements IPsec for mobile device access and tunneling with third-party VPN gateways. You can also use the proprietary Kerio VPN implementation for remote access from desktop operating systems, and for tunneling to other Kerio Control firewalls.

For more information refer to [Kerio VPN tunnel](#), [IPsec VPN](#) and [SSL certificates](#).

10 Manage bandwidth

Kerio Control gives you control over how much bandwidth each type of network traffic can consume. You can administer one or more lines to the Internet and at the same time prioritize traffic based on a variety of conditions such as services, interfaces, users. For more information, refer to [Configuring bandwidth management](#) (page 284).

11 Generate reports

The [Kerio Control Statistics](#) feature records the activities of authenticated users to a local database on the firewall. Privileged users can access statistics information on demand through a special web interface or by email.

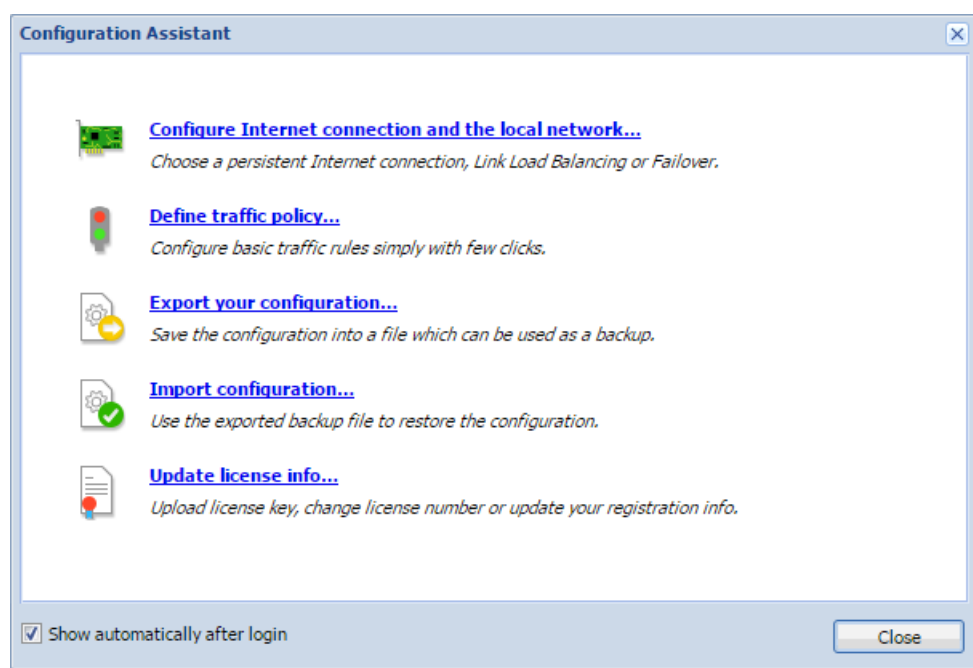
2.1 System requirements for Kerio Control

You can find detailed and always up-to-date system requirements for Kerio Control on our website:

[Kerio Control System Requirements](#)

2.2 Configuration Assistant

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



NOTE

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:

2.2.1 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.

NOTE

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).

NOTE

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

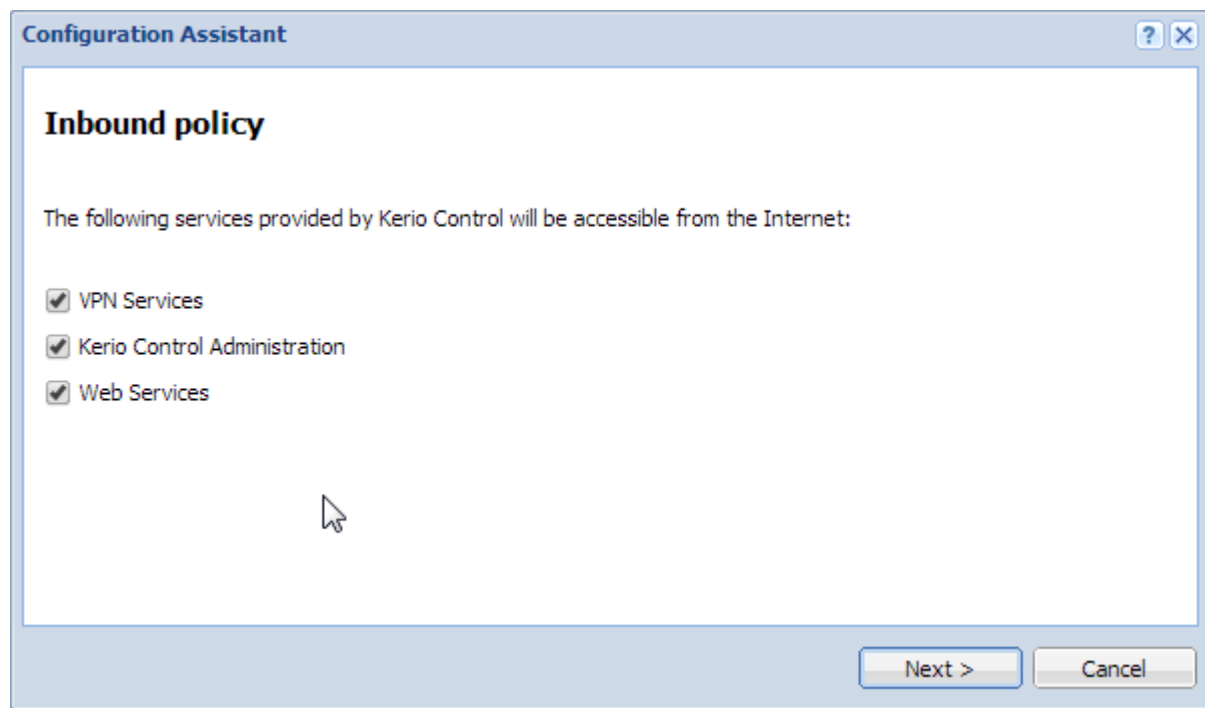
General notes

- » 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**).

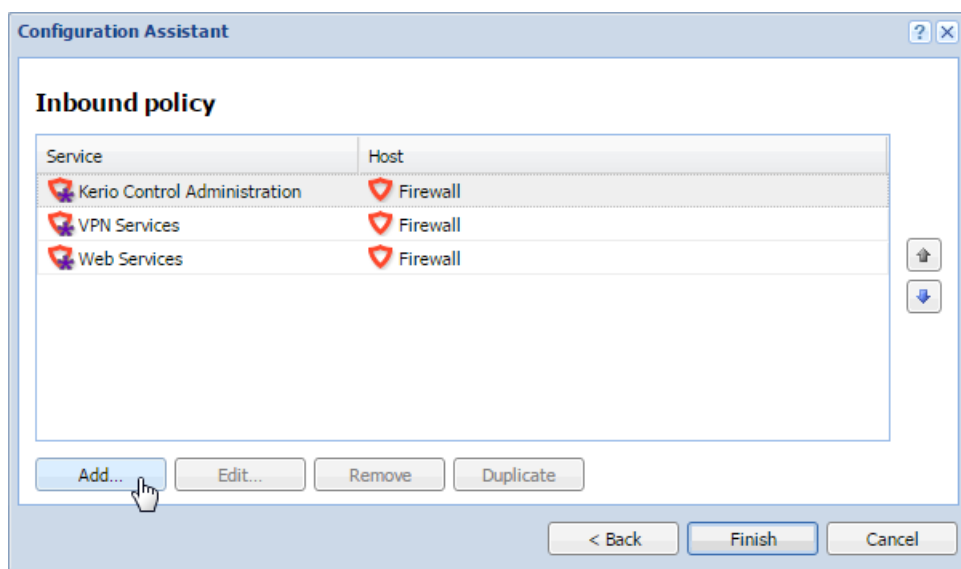
2.2.2 Define traffic policy

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.).



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**.



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. For more information, refer to [Services in Kerio Control](#) (page 337).
- **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. For more information, refer to [Configuring traffic rules](#) (page 236).

2.2.3 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 the Kerio Control license key.

NOTE

Kerio Control can automatically upload configuration files to MyKerio or FTP (see [Saving configuration to MyKerio](#) and [Saving configuration to FTP server](#)).

2.2.4 Import configuration files

1. Download the configuration file from the [FTP server](#), [MyKerio](#), or [Samepage](#).
2. In the administration interface, click **Configuration Assistant**.
3. In **Configuration Assistant**, click **Import configuration**.
4. Click **Upload Configuration File**.
5. Select a method for the import:

- Restore from backup — Kerio Control rewrites everything including basic TCP/IP settings.
- Transfer configuration from another Kerio Control installation — TCP/IP settings as IP addresses stays unchanged.

6. Click **Finish**.

Kerio Control restarts and applies the configuration.

If network interfaces have been changed since the export took place (for example, in case of exchange of a defective network adapter) or if the configuration is imported from another computer, Kerio Control attempts to pair the imported network interfaces with the real interfaces in the appliance. 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, review the **Interfaces** section.

2.2.5 Register product

For more information, refer to [Configuring the Activation Wizard](#) (page 23).

2.3 Logging to Kerio Control

Log in to Kerio Control to manage, configure and use the system.

After running the configuration and activation wizard, the system is ready to be used. The administrator and other users that were given the required permissions can log in to the various interface available.

Logging in as Administrators

There are three types of interfaces that an administrator of Kerio Control can access:

- » **Direct access:** The administrator can access directly the machine where Kerio Control is installed.
- » **Remote access via MyKerio:** [MyKerio](#) is a cloud service which enables the administrator to configure and manage numerous Kerio Control appliances from a single dashboard.
- » **Kerio Control Statistics:** Kerio Control Statistics is a web interface where the administrator can have an overview of the domain browsing statistics. For more information refer to [Kerio Control Statistics](#).

To login in Kerio Control Statistics:

Launch your web browser and type your Kerio Control address. The address has this pattern:

`https://server:4081/` where `server` refers to the name or IP address of Kerio Control, and `4081` represents a web interface port.

Logging in as a user

Kerio Control Statistics is a web interface where users can view their own browsing statistics.

To login as a user:

Launch your web browser and type your Kerio Control address. The address has this pattern:

`https://server:4081/` where `server` refers to the name or IP address of Kerio Control, and `4081` represents a web interface port.

2.4 Adding Kerio Control to MyKerio

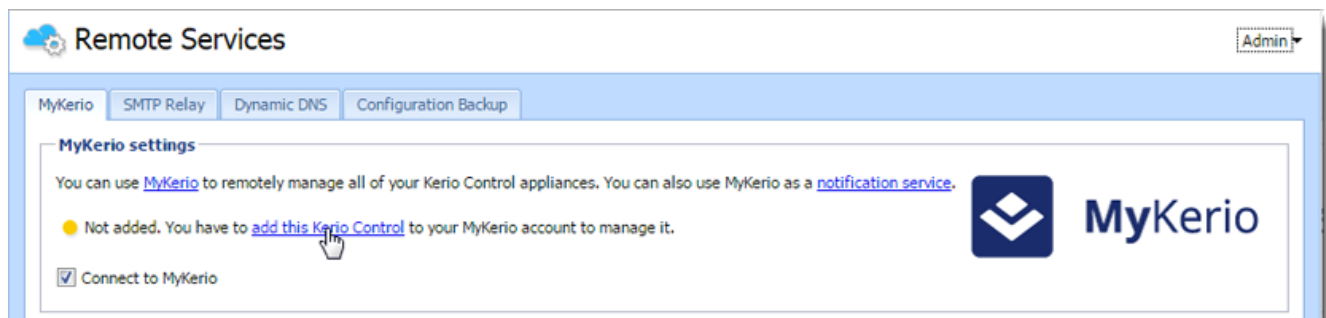
MyKerio is a cloud service that enables you to administer numerous Kerio Control appliances from a single dashboard. This article describes a process for adding Kerio Control to MyKerio. There are two ways how to accomplish it:

- » Adding Kerio Control to MyKerio through Kerio Control Administration
- » Adding Kerio Control to MyKerio during the Kerio Control installation

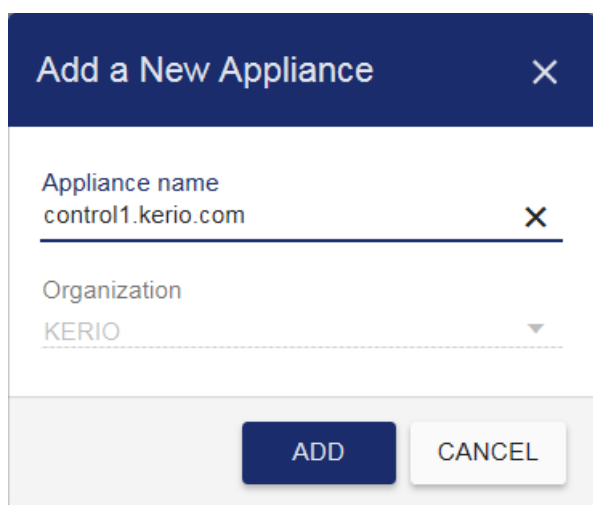
2.4.1 Adding Kerio Control to MyKerio through Kerio Control Administration

To link Kerio Control to MyKerio you must enable access to MyKerio in Kerio Control and sign up for MyKerio.

1. In the Kerio Control administration interface, go to **Remote Services**.

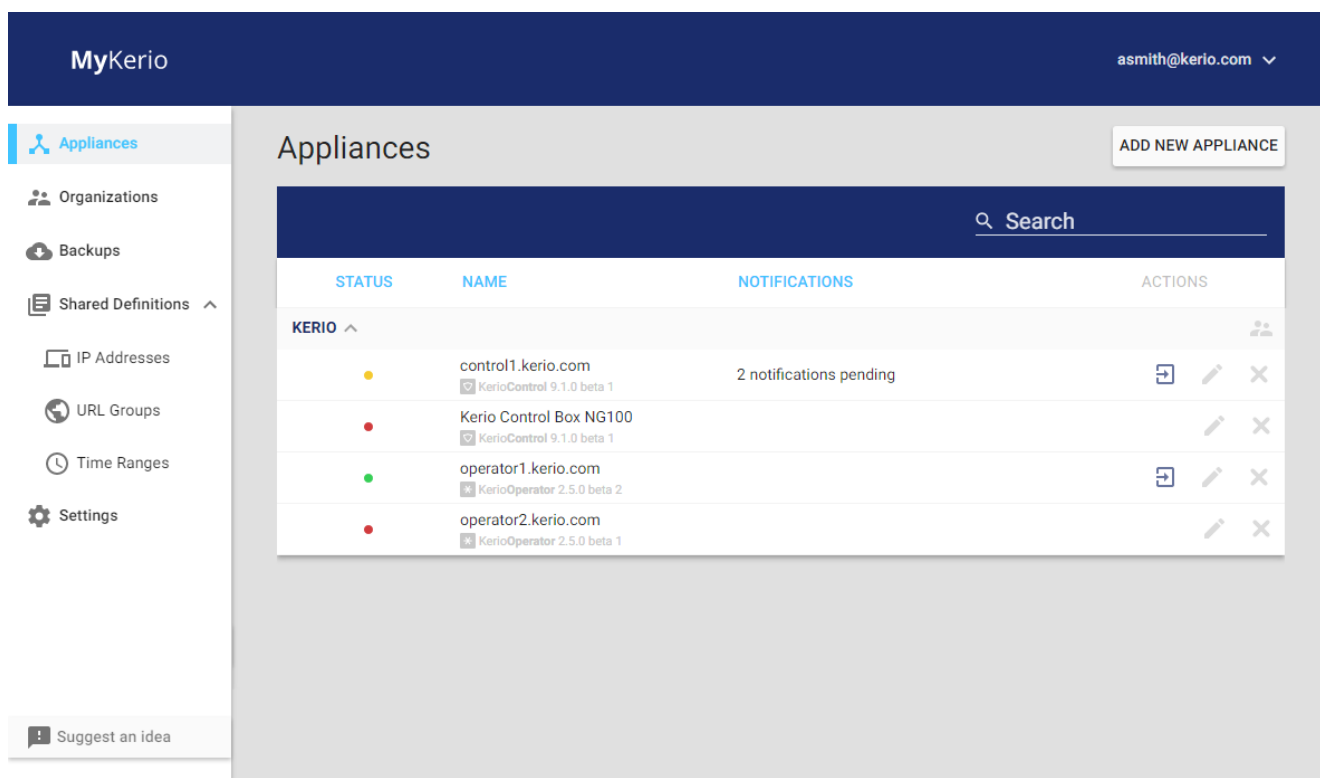


2. Ensure that **Connect to MyKerio** is selected.
3. Click the link **add this Kerio Control**. Your web browser opens <https://my.kerio.com/>, where you can register or log in if you are already registered.
4. After successful login, MyKerio displays the **Add a New Appliance** dialog box.
5. Type the name of the Kerio Control appliance (for example, your company name). If you have more organizations created in MyKerio, select also the organization. For more information refer to http://go.gfi.com/?pageid=mykerio_help#csid=1935.



6. Click **Add**.

You are now connected to MyKerio and you can see the Kerio Control appliance in the MyKerio dashboard.



2.4.2 Adding Kerio Control to MyKerio during the Kerio Control installation

When you install a new Kerio Control appliance, you can add it to MyKerio during the installation process. In the last installation dialog in the Kerio Control console, you can find a link to MyKerio (see figure below):



1. Type the link to your browser. Your web browser opens <https://my.kerio.com/login>, where you can register or log in if you are already registered. MyKerio with the **Add a New Appliance** dialog box opens.

2. Type the name of the newly installed appliance.

3. Click **Add**.

The MyKerio dashboard appears, the appliance is displayed and its status is **Up** (status bullet is green).

If you miss the correct link during the installation, you can [add](#) Kerio Control to MyKerio later in the Kerio Control Administration.

2.5 Upgrading Kerio Control

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. For more information, refer to [Configuring email alerts](#) (page 19).

Choose your current Kerio Control version for notes and instructions on how to upgrade to the latest version while retaining all settings:

- » [Versions 9.1 and newer](#)
- » [Versions 8 and 9.0](#)
- » [Version 7](#)

2.5.1 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 displays 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.

2.5.2 Automatic upgrade of Kerio Control

NOTE

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.

You can also enable and configure automatic upgrade. For more information, refer to [Upgrading to the latest version from Kerio Control 9.1 and newer](#) (page 19).

2.5.3 Configuring email alerts

Kerio Control allows you to set email alert when a new version is available. For more information, refer to [Using alert messages](#) (page 204).

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 and wait for the upgrade and restart of Kerio Control.

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

2.5.4 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 details, see [Updating Kerio Control using a USB flash drive](#) or [Updating Kerio Control Box NG series using a USB flash drive](#).

2.5.5 Troubleshooting

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

2.5.6 Upgrading to the latest version from Kerio Control 9.1 and newer

This topic describes how to upgrade a Kerio Control version 9.1 or newer installation to the latest version while retaining all settings.

Important notes when upgrading

- » 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**. For more information, refer to [Using alert messages](#) (page 204).

Upgrade procedure

1. In the administration interface, go to section **Advanced Options > Software Update**.
2. Select option **Periodically check for new versions**. When a new version is available, the **Software Update** tab displays a link to the download page.
3. Select **Download and upgrade to new versions automatically in given time interval** for automatic upgrade.
4. Select **Upgrade window time interval**. The time interval is set in **Time Ranges** and you can adjust it to your schedule. For more information, refer to [Creating time ranges in Kerio Control](#) (page 338).
5. Click **Apply**. Kerio Control now downloads new versions of Kerio Control and in the given interval upgrades to the new version

2.5.7 Upgrading to the latest version from Kerio Control 8 & 9.0

This topic describes how to upgrade a Kerio Control version 8.x or 9.0 installation to the latest version while retaining all settings.

Important notes when upgrading

- » 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**. For more information, refer to [Using alert messages](#) (page 204).

Upgrade procedure

1. In the administration interface, go to section **Advanced Options > Software Update**.
2. For immediate check of new versions, click **Check Now**.
3. When a new version is available, click **Download** in the **Upgrade to new version** section.
4. Click **Upgrade Now** when it appears.
5. In the **Confirm Restart** dialog box, click **Yes**. Upgrade can take a couple of minutes, then the log in dialog appears.
6. When upgrade is complete, log in to Kerio Control Administration and verify in **Dashboard** (tile **System**) that the new version has been installed successfully. If any problems regarding updates occur, check the debug logs. To do this, right-click the **Debug log** area and check **Messages > Update checker**.

2.5.8 Upgrading to the latest version from Kerio Control 7

This topic describes how to upgrade a Kerio Control version 7 installation to the latest version while retaining all settings.

Important notes when upgrading

- » You must first upgrade to Kerio Control 8.0 and then perform the upgrade to the latest version.

- » When purchasing Kerio Control or extending your Software Maintenance, you are automatically 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**. For more information, refer to [Using alert messages](#) (page 204).

Upgrade procedure

1. Go to <http://download.kerio.com> and download Kerio Control 8.0 (released on 2013-03-12). In **Select a product**, choose **Kerio Control**. In **Select a version**, choose **8.0.0 (released on 2013-03-12)**. Click **Show files**.
2. Select the installation image according to your appliance type.
3. Download the image.
4. Run the installation image. The installation program automatically closes the Kerio Control Engine and Kerio Control Engine Monitor. The installation program detects the directory with the former version and updates it by replacing appropriate files with the new ones automatically. The license, all log files and user defined settings are maintained.
5. Log in to the Kerio Control Administration.
6. In the administration interface of Kerio Control 8, go to section **Advanced Options > Software Update**.
7. Click **Check Now**.
8. When a new version is available, click **Download**.
9. Click **Upgrade Now** when it appears.
10. In the **Confirm Restart** dialog box, click **Yes**. Upgrade can take a couple of minutes.
11. When upgrade is complete, log in to Kerio Control Administration and verify in the **Dashboard** that the new version has been installed successfully. If any upgrade issues occur, right-click the **Debug log** area and check **Messages > Update checker**.

2.6 Installation

Kerio Control is available as:

- » VMware Virtual Appliance
- » Hyper-V Virtual Appliance
- » Software Appliance
- » KHardware Appliance

2.6.1 Installing Kerio Control	22
2.6.2 Configuring the Activation Wizard	23
2.6.3 Generating a bootable USB flash drive for Kerio Control software appliances	30
2.6.4 Increasing the number of supported network interfaces in the Kerio Control VMware Virtual Appliance ...	31
2.6.5 Migrating from Kerio Control (Windows Edition) to the Appliance Editions (Software/Virtual/Hardware) ..	31
2.6.6 Kerio Control Virtual Appliance for Hyper-V	33
2.6.7 Kerio Control VMware Virtual Appliance	35

2.6.1 Installing Kerio Control

Kerio Control can be installed in three different ways:

- » Software Appliance
- » Virtual Appliance
- » Hardware appliance

NOTE

From version 9.3 onwards 32-bit hardware is no longer supported.

Product editions

Edition	Description
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 information, refer to Kerio Control NG series installation guide (page 41).

Installing Software Appliance edition

The below information explains how to install the software appliance edition on a machine without an operating system. Watch [this](#) video for more information.

WARNING

Any existing operating system 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.

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.

To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**. For more information, refer to [Configuring network interfaces](#) (page 184).

Installing Virtual Appliance

Kerio Control Virtual Appliance is a UTM solution distributed as a virtual appliance for VMware and Hyper-V. The software provides a complex set of features for security of local networks, control of user access to the Internet and monitoring of user activity.

Solution	Information
Kerio Control VMware Virtual Appliance	For more information, refer to Kerio Control VMware Virtual Appliance (page 35).
Kerio Control Hyper-V Virtual Appliance	For more information, refer to Kerio Control Virtual Appliance for Hyper-V (page 33).

Hardware appliance

Kerio Control can be acquired as a dedicated hardware device that can be installed inside your network as an unified threat management firewall that features intrusion prevention, content filtering, activity reporting, bandwidth management, and virtual private networking.

For more information, refer to [Kerio Control NG series installation guide](#) (page 41).

The hardware appliance comes with three options:

Appliance	Description
Hardware Appliance NG100	Desktop appliance. 3x Gb ports. 1.3 GHz Dual Core Intel Bay Trail, 4 GB RAM, 32 GB SSD.
Hardware Appliance NG300	Sub-1U table-mountable appliance. 4x Gb ports . 2.4 GHz quad core Intel Atom, 4 GB RAM, 32 GB SSD.
Hardware Appliance NG500	1U rack-mountable appliance. 6x Gb ports. 3.6 GHz quad-core Intel Core i5, 4 GB RAM, 32 GB SSD.

2.6.2 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 is set as a default language after the first logon to the administration interface. You can change the language settings later.

Step 2: Setup connection

NOTE

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.

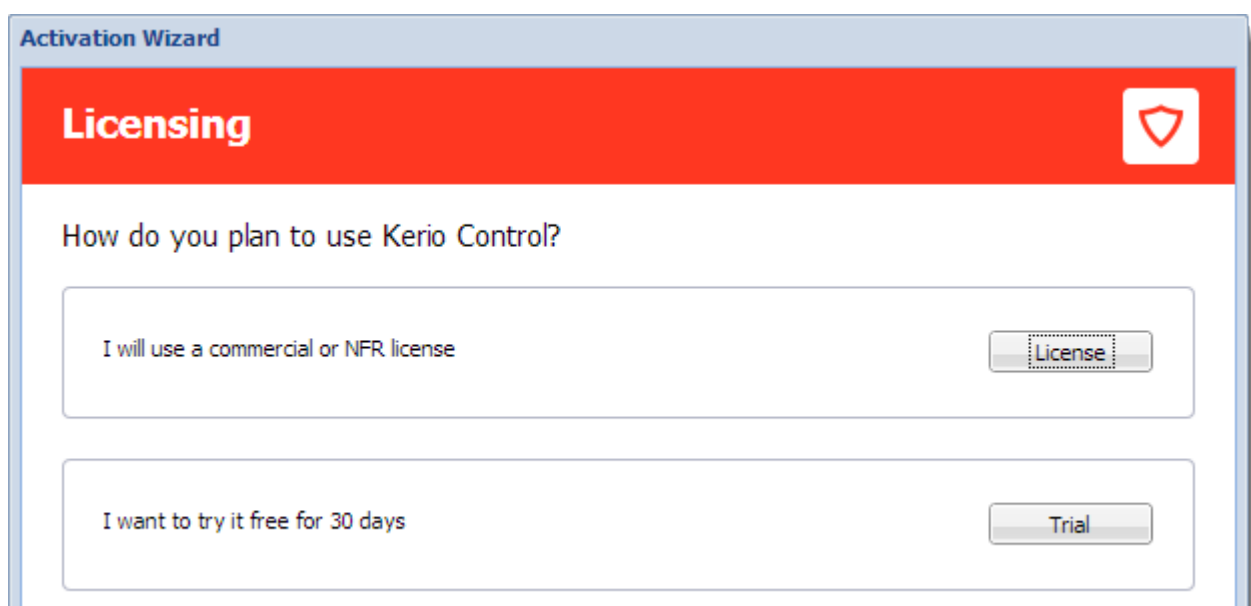
Select your time zone and verify the date and time settings.

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](#)



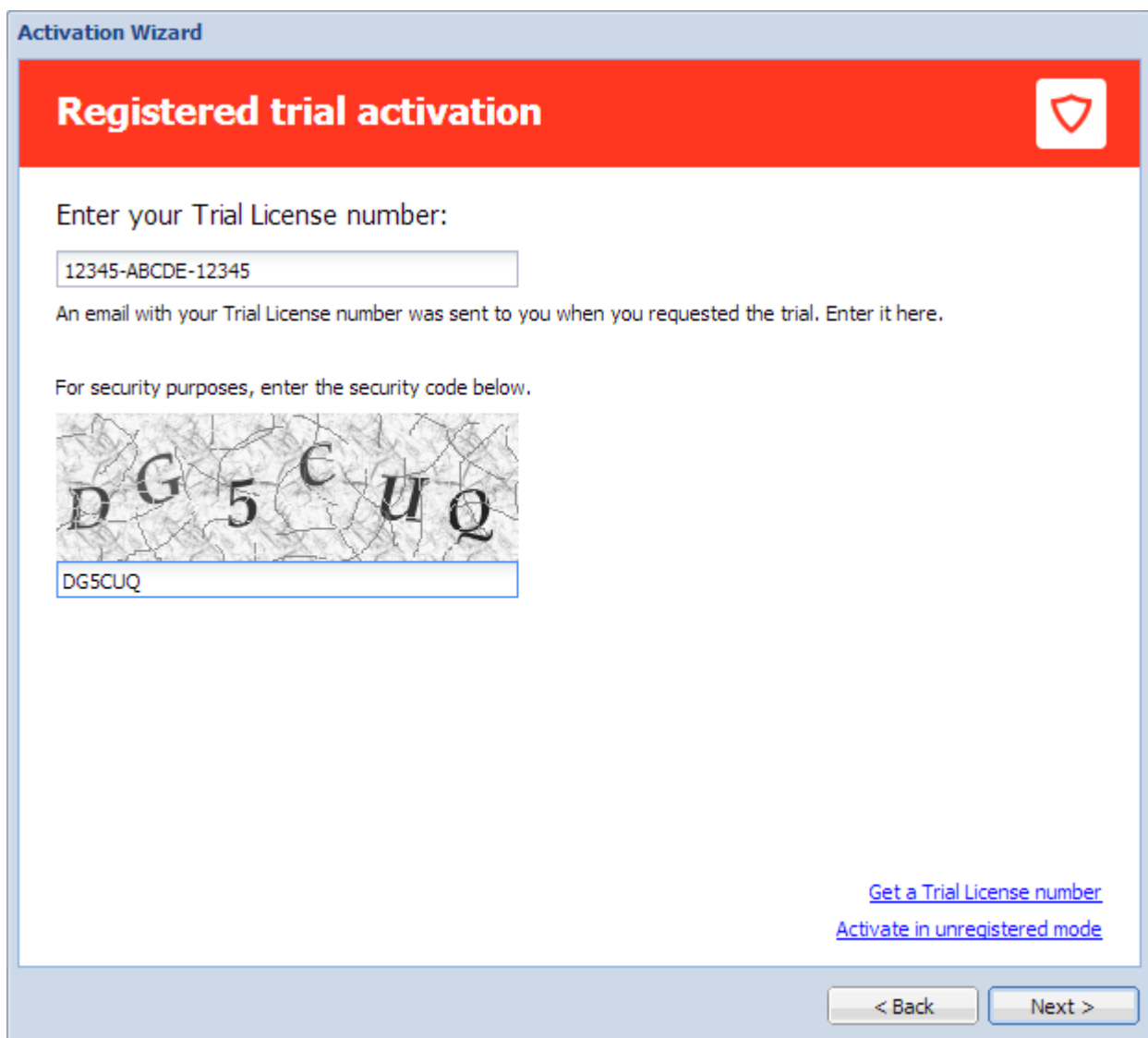
Screenshot 1: The Activation Wizard displays the licensing dialog.

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. 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**.



Activation Wizard

Registered trial activation

Enter your Trial License number:

12345-ABCDE-12345

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.

D G 5 € U Q

DG5CUQ

[Get a Trial License number](#)
[Activate in unregistered mode](#)

< Back Next >

Screenshot 2: The Activation Wizard displays the registered trial activation dialog.

4. Click the **Finish** button.

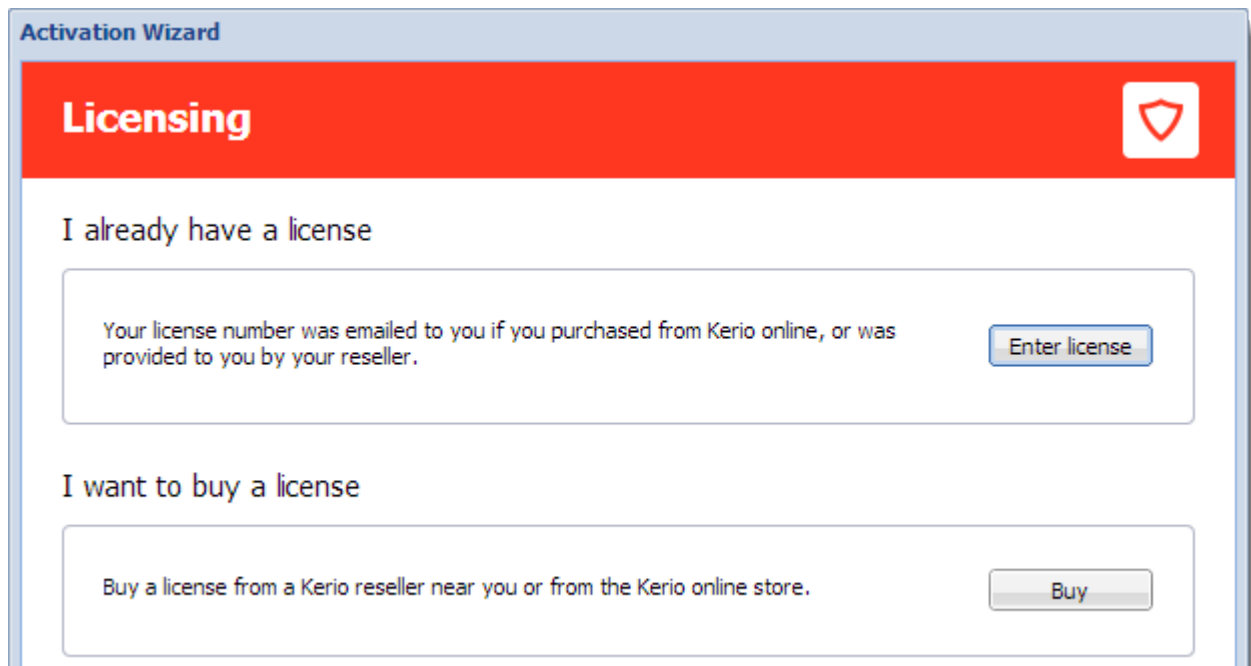
NOTE

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

Insert Kerio Control license number

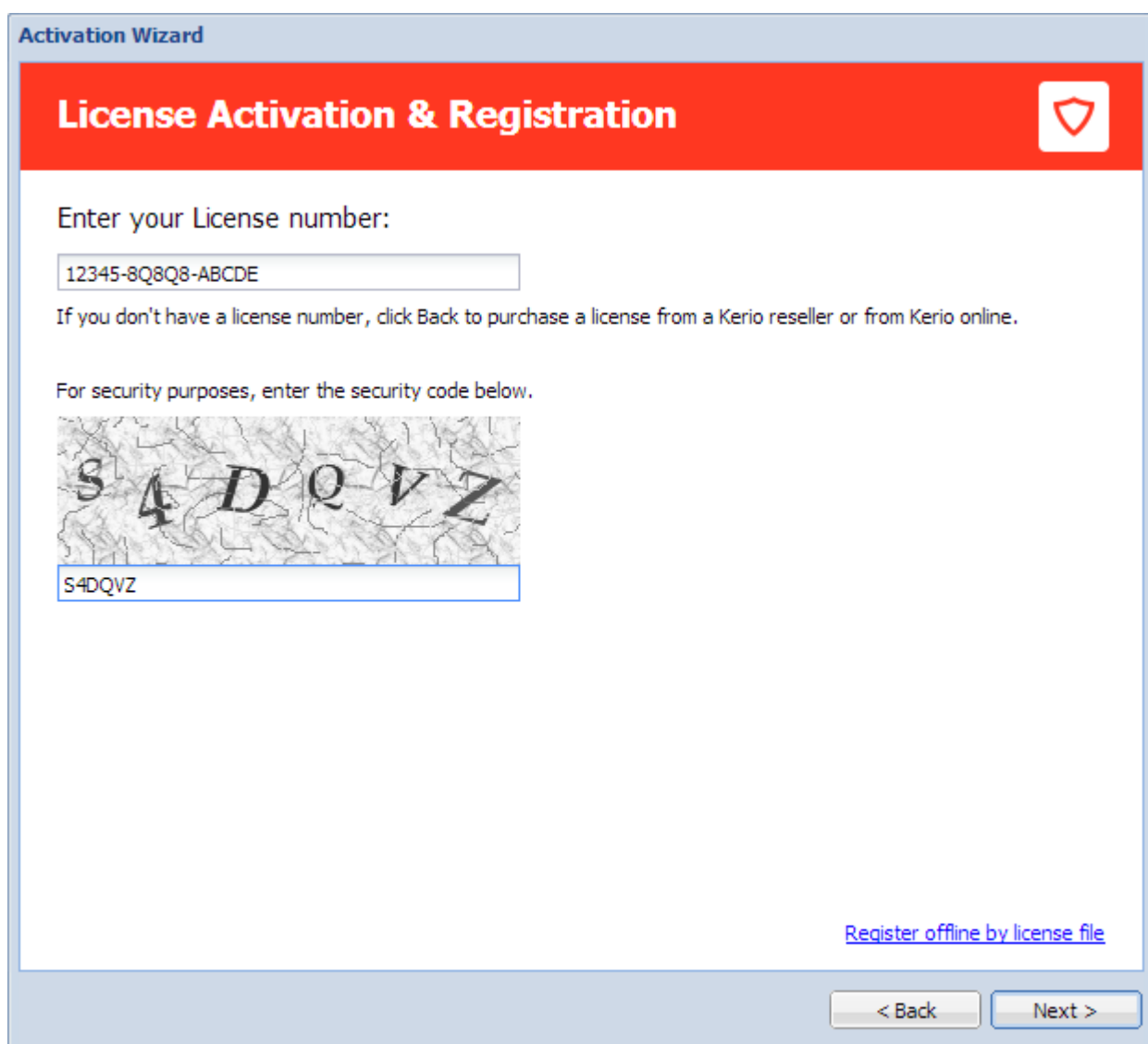
For registration, you need a license number for the purchased product.

1. Click **License** in the Licensing dialog.
2. In the next step, click **Enter license**.



Screenshot 3: The Activation Wizard displays the licensing dialog.

3. Insert the license number and enter the security code displayed in the picture.



Screenshot 4: The Activation Wizard displays the license activation and registration 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.

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 license 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**.

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.

IMPORTANT

Remember this password and keep it from anyone else!

Registration Wizard

Administrator account

Username: Admin

Password: [masked]

Conferma password: [masked]

☒ Do you want to receive alerts?

Indirizzo email: sos@naonis.it

☒ 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 >

Screenshot 5: The Activation Wizard displays the administrator account dialog.

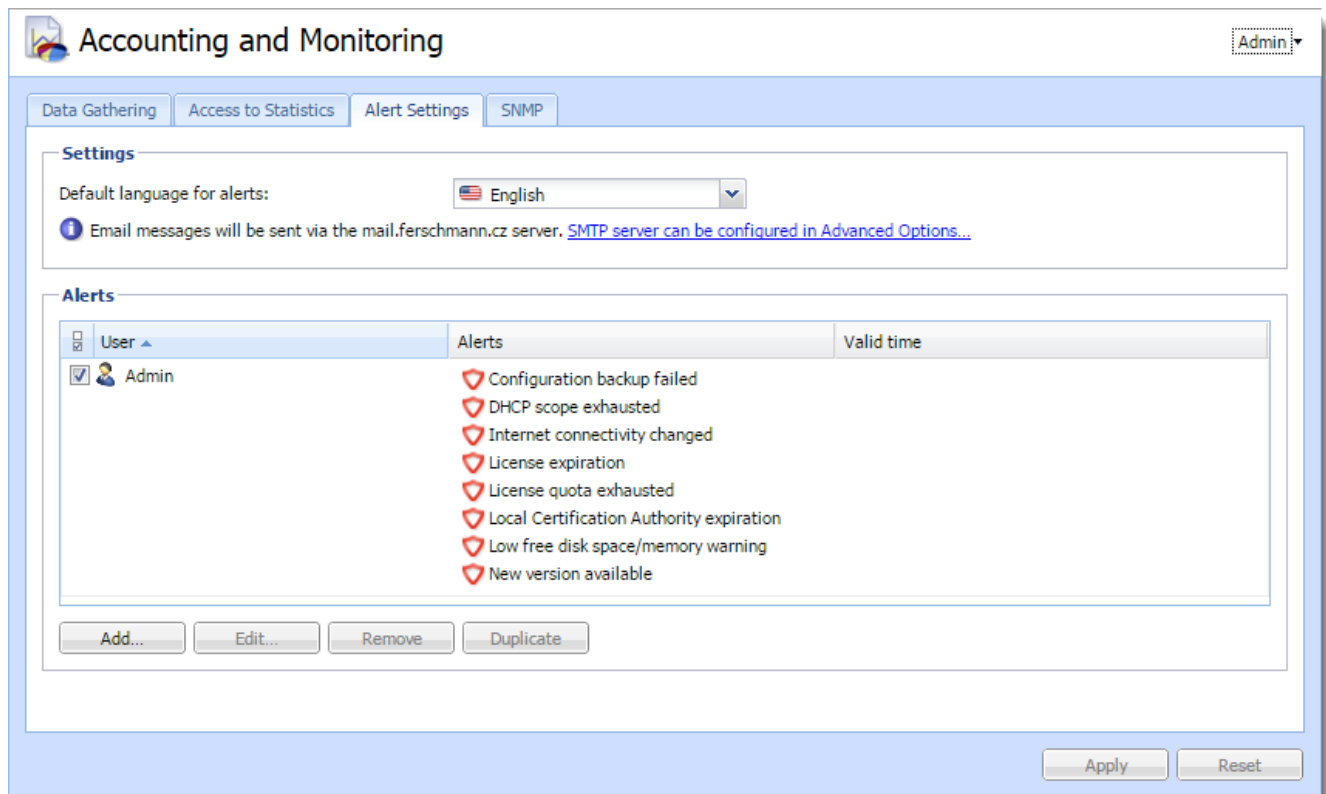
Sending default alerts

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).



For more information, refer to [System alerts](#) (page 206).

NOTE

Ensure your Kerio Control is connected to an SMTP server for sending alerts. For more information, refer to [Configuring the SMTP server](#) (page 318).

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**.

2.6.3 Generating a bootable USB flash drive for Kerio Control software appliances

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.

NOTE

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` and replace `kerio-control-installer.iso` with 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` and replace `kerio-control-installer.iso` with the real file name and `/dev/diskX` with the actual device name.
6. Eject the flash drive securely and remove it from your computer.

2.6.4 Increasing the number of supported network interfaces in the Kerio Control VMware Virtual Appliance

Kerio Control Virtual Appliance does not limit the number of network interfaces. However, based on the default virtual hardware version of the Kerio Control Virtual Appliance, the maximum number of allowed interfaces is 4.

Upgrading the virtual hardware

You can increase the number of supported interfaces by upgrading the virtual hardware. Refer to [upgrading a virtual machine to the latest hardware version](#) located in VMware's knowledge base.

Hardware limits based on VMware vSphere 5.0 are available [here](#).

2.6.5 Migrating from Kerio Control (Windows Edition) to the Appliance Editions (Software/Virtual/Hardware)

This article covers details regarding the Appliance Editions of Kerio Control, and provides guidance regarding the migration from the Windows Edition of Kerio Control to the various Appliance Editions.

As of version 8.0, Kerio Control will be available only as a Software, Virtual, or Hardware appliance. This means that customers running the Windows version are advised to migrate to one of the Appliance Editions. There is no cost to transfer the license to the Software or Virtual Appliance, and in most cases, you can continue using the same hardware. If you would like to migrate to one of the hardware box editions, the prorated value of your software license can be applied as a credit.

NOTE

The following answers should address some of the common questions regarding the migration:

What is the Kerio Control Appliance Edition?

The Kerio Control Software is packaged with a minimal (Linux based) operating system, which can be easily installed onto most computers. The Software Appliance Edition can be installed via an installation disk that is created by burning an ISO image onto a CD or USB disk. The Virtual Appliance is a specially packaged version of the Software Appliance, which can be easily deployed on ESX/ESXi or Microsoft Hyper-V. The Hardware Appliance consists of two models, which ship with a pre-configured version of the Software Appliance.

Do I need to know Linux?

No, all management of Kerio Control Appliance Edition is done through the web interface. There is no interaction with the operating system.

How is the Appliance Edition different than the Windows Edition?

Many of the recently added features, such as IPv6 routing, VLANs, and IPsec support are implemented only in the Appliance Editions. Administrative tasks such as TCP/IP changes, Upgrades, or Reboots are all performed from the web administration. Otherwise, the administration is identical.

What are the benefits of the Appliance Edition?

- » Additional features (IPv6, VLANs, IPsec)
- » Easier administration and maintenance

- » Lower system requirements
- » Better performance

Can the Software Appliance be installed on the same hardware as my current Kerio Control Windows installation?

Yes, in most cases the software appliance can be installed onto the same hardware.

How long will the migration take?

The Software Appliance installation and configuration import should take only a few minutes. Additional prior steps must be performed, which involve exporting the Windows configuration, downloading the Kerio Control Software Appliance, and burning the ISO image onto an installation CD or USB drive.

How do I install the Software Appliance?

You can download the ISO from the Kerio website. You will need burning software to image the file onto a CD-ROM or USB drive. You can then boot a computer from the CD or USB, and the display will guide you through the installation. Similar to how you would install any other operating system.

For instructions, refer to [Installing Kerio Control](#)

Can I deploy the Virtual Appliance under Windows Server Hyper-V?

Yes, you may choose to continue using Windows and Kerio Control, however you will need to have a Windows Server with the Hyper-V role.

NOTE

Watch the [Migrating from the Windows version of Kerio Control to the Hyper-V appliance](#) tutorial video.

Can I deploy the Virtual Appliance under VMware ESXi?

Yes, you can deploy Kerio Control virtual appliance in VMware ESXi.

NOTE

Watch the [Migrating from the Windows version of Kerio Control to the VMware appliance](#) tutorial video.

How do I transfer the license from my Windows installation to the Appliance Edition?

You can use the same server license on the Appliance Edition. During the installation of the software or virtual appliance, you will be asked to provide your server license. Otherwise, you can register the license any time from the web administration.

How do I transfer my configuration from the Windows installation?

This is done by exporting and importing your configuration through the web administration. Additional steps are provided in [Transferring the configuration and license from the Windows version of Kerio Control to the Software or Virtual Appliance edition](#)

2.6.6 Kerio Control Virtual Appliance for Hyper-V

This topic provides detailed description on installation and basic configuration of the Kerio Control Virtual Appliance for Hyper-V, version 8. All additional modifications and updates reserved.

Kerio Control Virtual Appliance for Hyper-V is a UTM solution distributed as a virtual appliance for Hyper-V. The software provides a complex set of features for security of local networks, control of user access to the Internet and monitoring of user activity. It also includes tools for secure interconnection of company's offices and connection of remote clients to the LAN via the Internet (VPN).

To keep this document simple and easy to read, Kerio Control Virtual Appliance for Hyper-V will be referred to as firewall.

System requirements and licensing

System requirements

For up-to-date system requirements, please refer to: <http://www.kerio.com/control/technical-specifications>

Licensing Policy

Kerio Control Virtual Appliance for Hyper-V can be used for free for 30 days from installation (trial version).

Upon the trial version expiration, you will need to purchase.

Upon the trial version expiration, you will need to purchase a corresponding license for further use of the product. Then simply register the trial version with a valid license key. This process makes the trial version full version automatically.

The license is defined by:

- » The base product license,
- » Kerio Control Web Filter license (optional component used for classification of web content),
- » License for the integrated Kerio Antivirus (optional component).

For detailed information about license options, pricing and license purchase, refer to <http://www.kerio.com/control>.

Installation and basic configuration of the firewall

Importing the virtual appliance into Hyper-V

Kerio Control Virtual Appliance for Hyper-V is distributed in the form of virtual harddisk.

1. Unpack the distribution Zip package into the desired target location (e.g. C:\KerioControl). After importing the appliance into Hyper-V, the location cannot be changed anymore!
2. The server needs to have the Hyper-V role set. You can add the role in the Server Manager control panel (**Roles > Add Roles**).
3. Open the Hyper-V Manager control panel and choose the local Hyper-V server.
4. Run the New virtual machine wizard (**New > Virtual machine**).
5. As a virtual machine location, choose the directory with the unpacked virtual harddisk (see above). Assign at least 1,5 GB RAM and virtual network adapters.
6. In the next step, choose the **existing virtual harddisk** option. Select the virtual harddisk unpacked from the distribution package.
7. After finishing the wizard, connect to the virtual appliance and start it.

Installation and basic configuration

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.

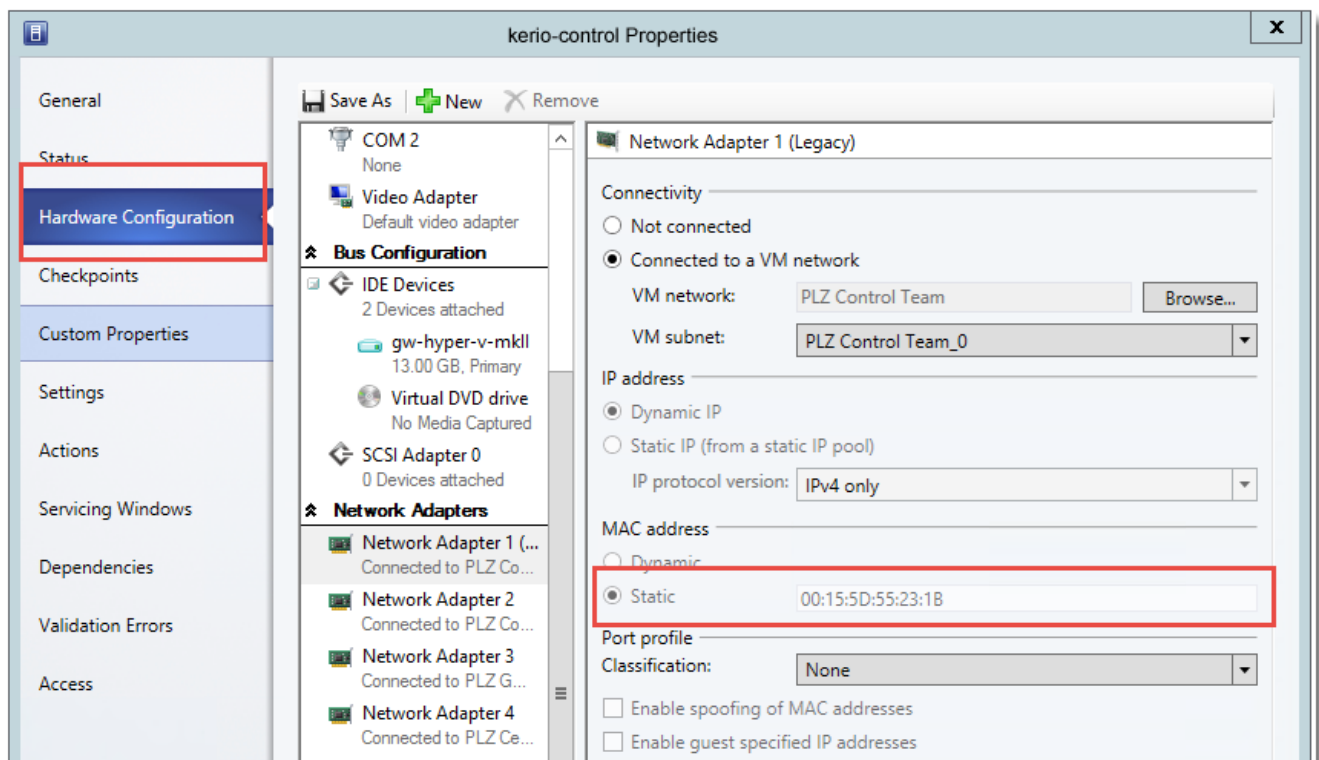
To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**.

Login to the Kerio Control Administration web interface and configure the product as necessary.

Setting a static MAC address for the Kerio Control appliance

Hyper-V assigns dynamic MAC addresses by default. Kerio Control needs a static MAC address:

1. In **Virtual Machine Manager**, go to properties of the Kerio Control appliance.
2. In **Properties**, go to **Hardware Configuration**.
3. In **Hardware Configuration**, select **Static** in the **MAC address** section.



Screenshot 6: Hardware configuration in the properties of Kerio Control

Hyper-V assigns the static MAC address to your Kerio Control appliance.

Firewall administration

The Kerio Control Administration web interface allows full remote administration of the firewall and viewing of status information and logs.

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.

Authenticate with username `Admin` and the password set within the product activation.

NOTE

Remote administration via the Internet must be enabled explicitly by the firewall's traffic rules.

The firewall's console

On the console of the virtual computer where Kerio Control Virtual Appliance for Hyper-V is installed, information about the firewall remote administration options is displayed. Upon authenticating by the administration password (see above), this console allows to change some basic settings of the firewall, restore default settings after installation and shut down or restart the computer.

The firewall's console allows:

- » to change configuration of network interfaces (e.g. if network configuration changes or if an incorrect interface was chosen for the local network during the firewall installation).
- » to change traffic policy of the firewall so that remote administration is not blocked (if connection to the administration fails).
- » to shut down or restart the firewall.
- » to recover default configuration.

This option restores the firewall settings as applied upon the first startup on Hyper-V. All configuration parameters and other data will be removed and the initial configuration wizard is started again. Restoration of default configuration is useful especially if the firewall does not work correctly and you cannot easily fix the configuration.

2.6.7 Kerio Control VMware Virtual Appliance

This topic provides detailed description on installation and basic configuration of the Kerio Control VMware Virtual Appliance, version 8. All additional modifications and updates reserved.

Kerio Control VMware Virtual Appliance is a UTM solution distributed as a virtual appliance for VMware. The software provides a complex set of features for security of local networks, control of user access to the Internet and monitoring of user activity. It also includes tools for secure interconnection of company's offices and connection of remote clients to the LAN via the Internet (VPN).

To keep this document simple and easy to read, Kerio Control VMware Virtual Appliance will be referred to as firewall.

System requirements and licensing

For up-to-date system requirements, please refer to: <http://www.kerio.com/control/technical-specifications>

Kerio Control VMware Virtual Appliance can be used for free for 30 days from installation (trial version).

Upon the trial version expiration, you will need to purchase a corresponding license for further use of the product. Then simply register the trial version with a valid license key. This process makes the trial version full version automatically.

The license is defined by:

- » The base product license,
- » Kerio Control Web Filter license (optional component used for classification of web content),

- » License for the integrated Kerio Antivirus (optional component).

For detailed information about license options, pricing and license purchase, refer to <http://www.kerio.com/control>.

Installation and basic configuration of the firewall

Kerio Control VMware Virtual Appliance (referred simply as “the firewall” in the document) is distributed in two types of packages:

- » In the OVF format (Open Virtualization Format) — for VMware ESX/ESXi,
- » In the proprietary VMX format for “hosted” VMware products — VMware Server, Workstation, Fusion and Player.

Importing virtual appliance to VMware product

Use an installation package in accordance with the type of your VMware product (see above):

- » In case of products VMware Server, Workstation, Player and Fusion, download the compressed VMX distribution file (*.zip), unpack it and open the .vmx file.
- » You can import a virtual appliance directly to VMware ESX/ESXi from the URL of the OVF file — for example: <http://www.kerio.com/control/download/vmware-ovf>

VMware ESX/ESXi automatically downloads the OVF configuration file and a corresponding disk image (.vmdk).

If your ESXi does not support deployment using URL. Download the required OVF files from <http://download.kerio.com/archive/>.

Then, follow these steps:

1. Select your **Product** and **Version** and click **Show Files**.
2. Download Kerio Control VMware Virtual Appliance (OVF) and Kerio Control VMware Virtual Appliance (OVF) – disk image on your local computer.
3. Browse and attach both the OVF files in the ESXi Host.
4. Wait for the deployment and the file transfer to fully complete on the ESXi Host.

If you import virtual appliance in the OVF format, bear in mind the following specifics:

- » In the imported virtual appliance, time synchronization between the host and the virtual appliance is disabled. However, Kerio Control features a proprietary mechanism for synchronization of time with public Internet time servers. Therefore, it is not necessary to enable synchronization with the host.
- » Tasks for shutdown or restart of the virtual machine will be set to default values after the import. These values can be set to “hard” shutdown or “hard” reset. However, this may cause loss of data on the virtual appliance. Kerio Control VMware Virtual Appliance supports so called Soft Power Operations which allow to shutdown or restart hosted operating system properly. Therefore, it is recommended to set shutdown or restart of the hosted operating system as the value.

Installation and basic configuration

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**.
Login to the Kerio Control Administration web interface and configure the product as necessary.

Firewall administration

The Kerio Control Administration web interface allows full remote administration of the firewall and viewing of status information and logs.

The web administration interface is available at: *https://<IP address of the firewall>:4081/admin*
for example, *https://10.10.10.1:4081/admin*, which is the IP address where Kerio Control is accessible from your LAN.

Authenticate with username `Admin` and the password set within the product activation.

NOTE

Remote administration via the Internet must be enabled explicitly by the firewall's traffic rules.

The firewall's console

On the console of the virtual computer where Kerio Control VMware Virtual Appliance is installed, information about the firewall remote administration options is displayed. Upon authenticating by the administration password (see above), this console allows to change some basic settings of the firewall, restore default settings after installation and shut down or restart the computer.

The firewall's console allows:

- » to change configuration of network interfaces (e.g. if network configuration changes or if an incorrect interface was chosen for the local network during the firewall installation).
- » to change traffic policy of the firewall so that remote administration is not blocked (if connection to the administration fails).
- » to shut down or restart the firewall.
- » to recover default configuration.

This option restores the firewall settings as applied upon the first start up on VMware. All configuration parameters any other data will be removed and the initial configuration wizard is started again (see, [Installation and basic configuration of the firewall](#)). Restoration of default configuration is useful especially if the firewall does not work correctly and you cannot easily fix the configuration.

2.7 Licenses and registration

This section provides information about Kerio Control licenses and registrations.

2.7.1 Licensing and registering Kerio Control	38
2.7.2 Transferring the configuration and license from the Windows version of Kerio Control to the Software or Virtual Appliance edition	40
2.7.3 How do I apply renewals or add-ons to my Kerio product?	40

2.7.1 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. For more information, refer to [Configuring the guest network](#) (page 187).

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**.

IMPORTANT

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:

- » Kerio 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

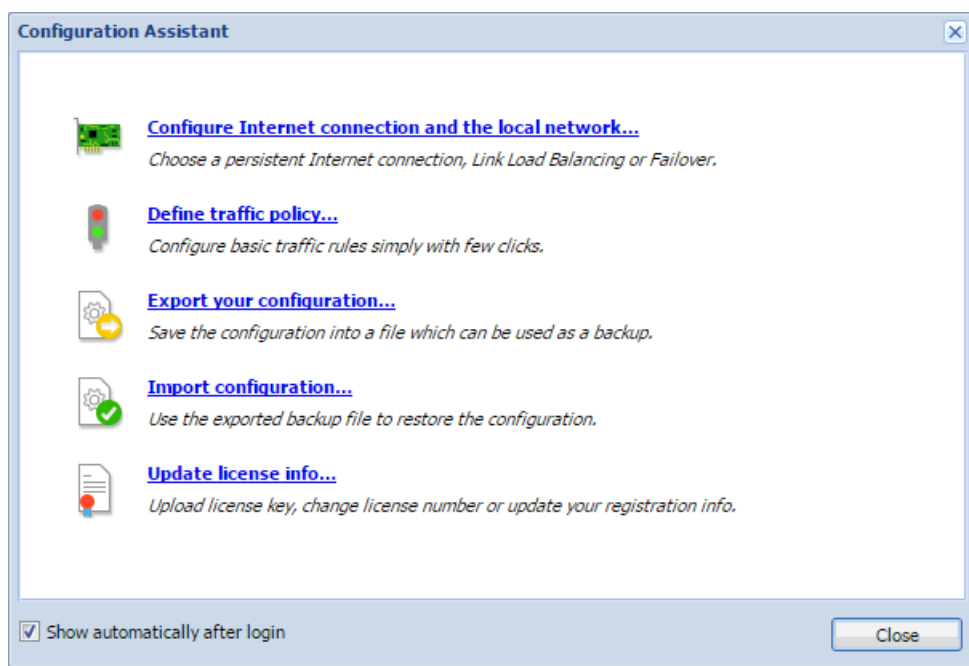
If you skip the registration in the [Activation Wizard](#), you can register Kerio Control from the **Dashboard** in the administration interface (displayed after each login).

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**.



3. In the **Configuration Assistant** dialog box, click **Register product**. For more information, refer to [Configuring the Activation Wizard](#) (page 23).

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**. For more information, refer to [Configuring the Activation Wizard](#) (page 23).

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)

IMPORTANT

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. For more information, refer to [Configuration Assistant](#) (page 10).

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

IMPORTANT

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

2.7.2 Transferring the configuration and license from the Windows version of Kerio Control to the Software or Virtual Appliance edition

You can transfer the configuration and license of the Microsoft Windows version of Kerio Control to the Software or Virtual Appliance edition. This article describes the details of license and configuration transfer between the various editions of Kerio Control.

Details

For details regarding the installation of the Kerio Control appliance, refer to [Installing Kerio Control](#).

Configuration transfer

You can transfer the configuration using the built-in export and import feature.

1. Log in to your Kerio Control installation running on the Windows based system
2. Export your configuration using the [Configuration Assistant](#)
3. Log in to your Kerio Control software or virtual appliance
4. Import your configuration using the [Configuration Assistant](#)

License transfer

Licenses of the Windows version of Kerio Control are transferrable to the software or virtual appliance. During the installation of the software or virtual appliance, register the same license number using the [Activation Wizard](#). After registering the license on the software or virtual appliance, uninstall the Kerio Control software from the Microsoft Windows system.

2.7.3 How do I apply renewals or add-ons to my Kerio product?

When you purchase renewals or add-ons for a Kerio Product, License changes are applied automatically by the product within 24 hours. You can force an immediate update from the administration dashboard using the **update registration info** link in the **License Details** tile.

2.8 Hardware appliance

This section describes deployment and configuration for hardware appliances.

2.8.1 Kerio Control NG series installation guide	41
2.8.2 End of life of Kerio Control Box 1110	43
2.8.3 Configuring Ethernet ports in Kerio Control hardware appliances	44
2.8.4 Migrating configuration from one Kerio Control hardware appliance to another	47
2.8.5 Connecting to Kerio hardware appliances with a serial console	52
2.8.6 WiFi	57

2.8.1 Kerio Control NG series installation guide

Use this quick install guide to find information about safely installing and implementing Kerio Control Box NG series UTM appliances.

NOTE

From version 9.3 onwards 32-bit hardware is no longer supported.

General Safety Instructions

During installation follow these security instructions:

- » The appliance should be placed on a flat surface or securely mounted horizontally in rack enclosure.
- » The NG500 Series are intended primarily for server rooms due to noisy performance.
- » Do not attempt to open or disassemble the appliance for any reason.
- » Strictly follow the [installation instructions](#).
- » Do not place the appliance near a heat source.
- » Place the appliance in a ventilated space, making sure that the appliance fans and vents are unobstructed at all times.
- » Do not expose the appliance to liquids of any kind. In the event of liquid intrusion, unplug the appliance immediately.
- » Verify that the voltage and frequency of the power socket match the values printed on the power adapter before plugging in the appliance. Use only the power adapter supplied with the appliance.
- » Do not place any items on top of the power cable; keep the power cable away from walkways or other areas where it could pose a tripping hazard.

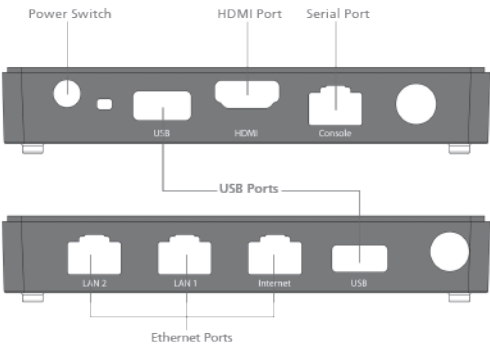
Appliance description

Kerio Control Box types:

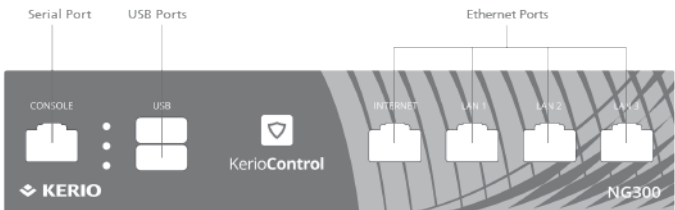
- » Kerio Control Box NG100 — Desktop appliance
- » Kerio Control Box NG300 — Sub-1U table mountable appliance

» Kerio Control Box NG500 — 1U rack mountable appliance

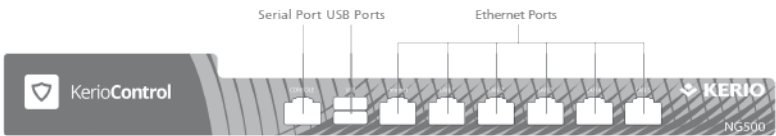
Feature	Description
Serial port	Used for connecting to a console with a serial cable
USB ports	Input for USB devices
Ethernet network ports	Used for connecting to the Internet and the LAN with an Ethernet cable



Screenshot 7: Kerio Control Box NG100 (front + back)



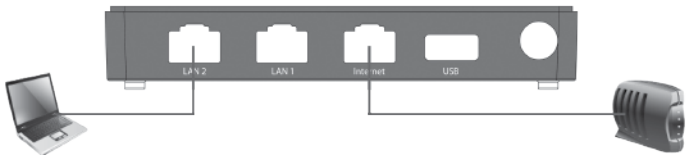
Screenshot 8: Kerio Control Box NG300 (front + back)



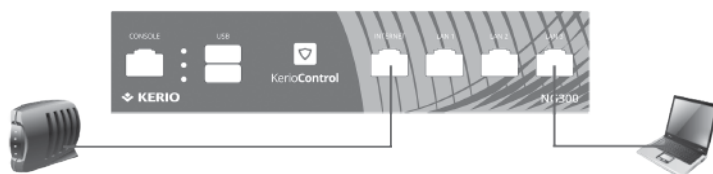
Screenshot 9: Kerio Control Box NG500 (front + back)

Kerio Control Box Installation and Configuration

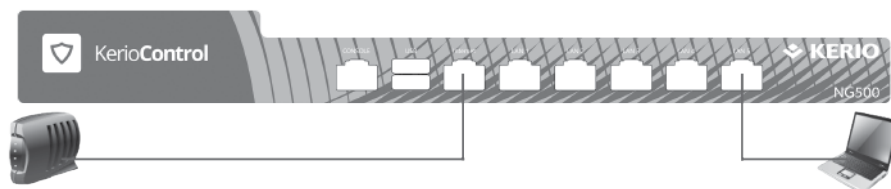
Once a suitable place has been located for the appliance and it has been plugged into a power outlet according to the safety instructions, it is time to connect it to the network and configure settings.



Screenshot 10: Connecting Kerio Control Box NG100 to the network



Screenshot 11: Connecting Kerio Control Box NG300 to the network



Screenshot 12: Connecting Kerio Control Box NG500 to the network

To configure the appliance:

1. Connect the Internet port to the Internet (e.g. DSL or Cable modem) using an Ethernet cable.
2. Connect the LAN port to the computer that is used to configure the appliance (see the figures above).
3. Turn on the appliance.

Now you have two options:

- » Add and manage the appliance through MyKerio (see [Installing Kerio Control Box through MyKerio](#))
- » Access the Kerio Control Administration through a browser (see below):
 - a. Set the networking preferences for Ethernet on the connected computer to **Automatic DHCP configuration**. (You can change it later after the configuration is complete).
 - b. Renew the DHCP lease on the computer and confirm it has an IP address of 10.10.10.11.
 - c. Open a web browser and connect to the Kerio Control Administration web interface using the following URL: **https://10.10.10.1/admin**
 - d. Ignore the SSL certificate warnings and proceed to the configuration wizard.
 - e. Follow the instructions provided by the wizard and configure the appliance.

NOTE

For troubleshooting purposes, you can use the serial port to connect the console to the device. See [Connecting to Kerio hardware appliances with a serial console](#).

Additional Information

2.8.2 End of life of Kerio Control Box 1110

Kerio announces the end-of-life dates for Kerio Control Box 1110. The last major supported version for Kerio Control Box 1110 is Kerio Control 9.2. The last day to order the affected product was September 2013.

Support is available under the terms and conditions of customers' service contract. Customers with active software maintenance contracts receive support from the Kerio Technical Support as shown below.

Milestone	Definition	Date
End-of-software maintenance releases date	The last day that Kerio Engineering may release any final software maintenance releases or bug fixes. After this date, Kerio Technologies will no longer develop, repair, or maintain the appliance.	November 30, 2017
Last day of software maintenance	The last day of software maintenance. After this date, software maintenance will no longer be available. All software maintenance renewals will be prorated to end on this date.	December 31, 2017
Last day of technical support	The last day that Kerio Technical Support will provide technical assistance for the product.	December 31, 2018

Product migration options

You can upgrade to [NG Series](#) or [NG Wifi Series](#). For details, go to [Kerio Control NG Series](#).

2.8.3 Configuring Ethernet ports in Kerio Control hardware appliances

You can configure Ethernet ports in Kerio Control hardware devices as standalone or in a LAN bridge:

- » **Standalone interface** maintains its own network with a separate IP subnet and optional DHCP scope. You can apply policies such as bandwidth and traffic rules to standalone interfaces.
- » **LAN Switch** is a virtual network interface that shares its TCP/IP configuration with all associated ports. All Kerio Control policies apply to all Ethernet ports in the LAN switch. All local network ports belong to the LAN switch by default and you can manually exclude a port as standalone.

Configuring ports

WARNING

Do not try to administer the appliance through the port you want to switch to standalone mode. If you do, Kerio Control will not apply the configuration.

To change from LAN Switch to Standalone:

1. In the administration interface, go to **Interfaces** or **Interfaces and WiFi**.
2. Right-click the interface.
3. In the context menu, select **Manage Ports**.

Interfaces

Internet connectivity

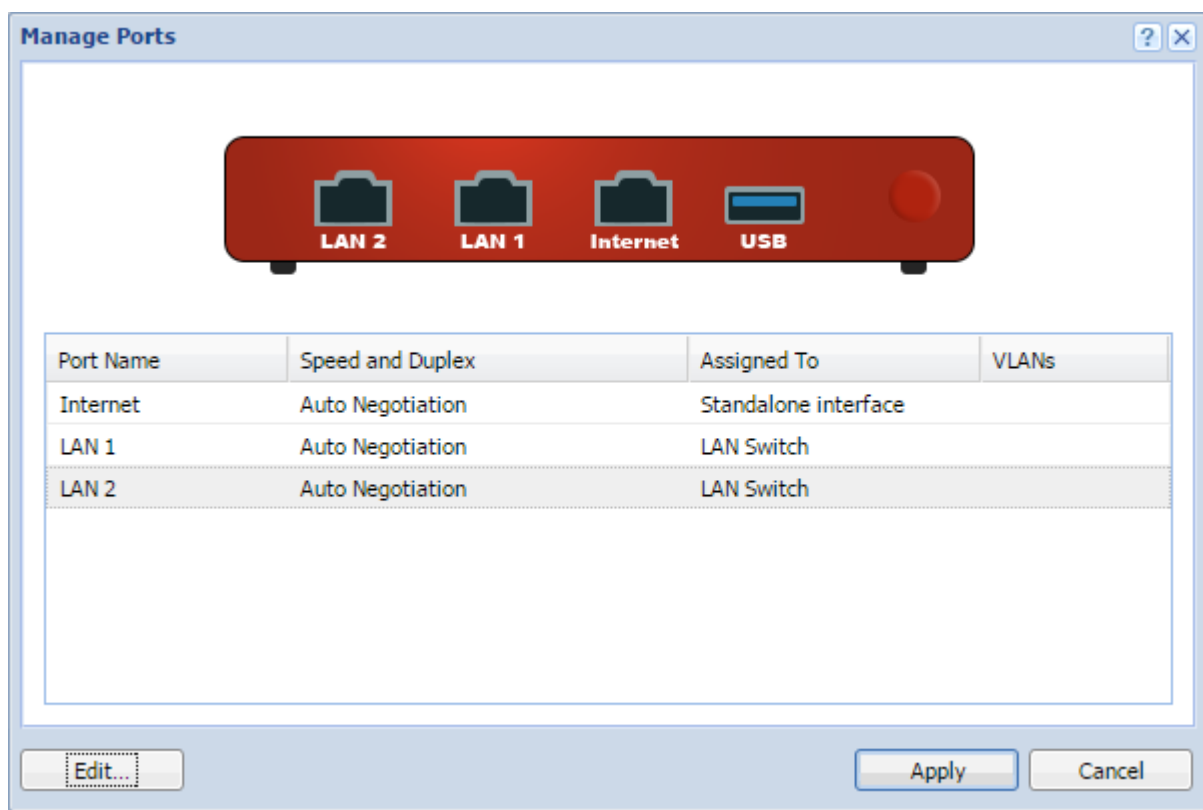
Select an option of how the firewall is connected to the Internet:

A Single Internet Link Ports...

Name	Status	IPv4	IPv6
Internet Interfaces			
WAN	Up	192.168.64.150	2001:718:1803:64:290:bff:fe41:40f0
Trusted/Local Interfaces			
LAN Switch	Up	10.10.10.1	
IPsec and Kerio VPN Interfaces			
VPN Server		10.189.177.1	
Guest Interfaces			
No interfaces are assigned to this category			
Other Interfaces			
No interfaces are assigned to this category			

Add
Edit...
Remove
Dial
Disable
Manage Ports...
Show Traffic Chart
Configure in Wizard...

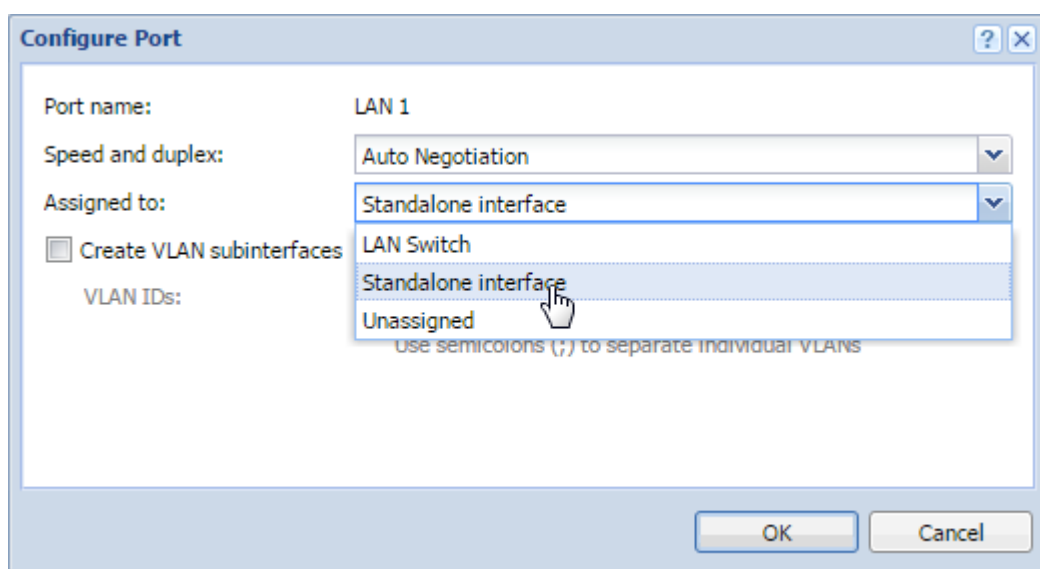
4. In the **Manage Ports** dialog box, select a port and click **Edit**. The **Manage Ports** dialog box shows the scheme of your hardware device with a port description to help you identify which port to configure.



5. In the **Configure Port** dialog box, select **Standalone interface**.

NOTE

You can add virtual LAN sub-interfaces for standalone interfaces. For more information, refer to [Configuring VLANs](#) (page 199).



6. Click **OK**

7. Click **Apply**. Kerio Control verifies your configuration changes. However, if you are physically connected through the port you want to change, Kerio Control does not apply the changes and the port stays assigned to the LAN switch.

If Kerio Control accepts your configuration, the interface runs as standalone.

Configuring the new interface

1. In the administration interface, go to **Interfaces** or **Interfaces and WiFi**.
2. (Optional) Move the standalone interface to another interface group. For more information, refer to [Configuring network interfaces](#) (page 184).
3. Configure the TCP/IP settings. For more information, refer to [Configuring TCP/IP settings in Kerio Control interfaces](#) (page 192).
4. (Optional) Enable the DHCP scope. For more information, refer to [DHCP server in Kerio Control](#) (page 319).

2.8.4 Migrating configuration from one Kerio Control hardware appliance to another

This article describes hardware device replacement. There are two basic scenarios:

- » Your original hardware device is broken and you received a new hardware device of the same type.
- » Your original hardware device works well, but you want to upgrade your infrastructure with a new Kerio Control hardware device.

To switch from one Kerio Control hardware appliance to another, you need to configure and register the new Kerio Control and then switch off the original appliance.

If your original hardware appliance is still running, configure the new hardware appliance in advance in your office. If the original Kerio Control is broken, you can configure the new one in the production environment.

Use the following steps:

1. [Get the configuration files from a backup or the original Kerio Control installation.](#)
2. [Connect the new appliance to the Internet.](#)
3. [Activate the license.](#)
4. [Upgrade the new appliance to the latest version of Kerio Control.](#)
5. [Import the configuration to the new appliance.](#)
6. [Replace the hardware appliance.](#)

Before you start

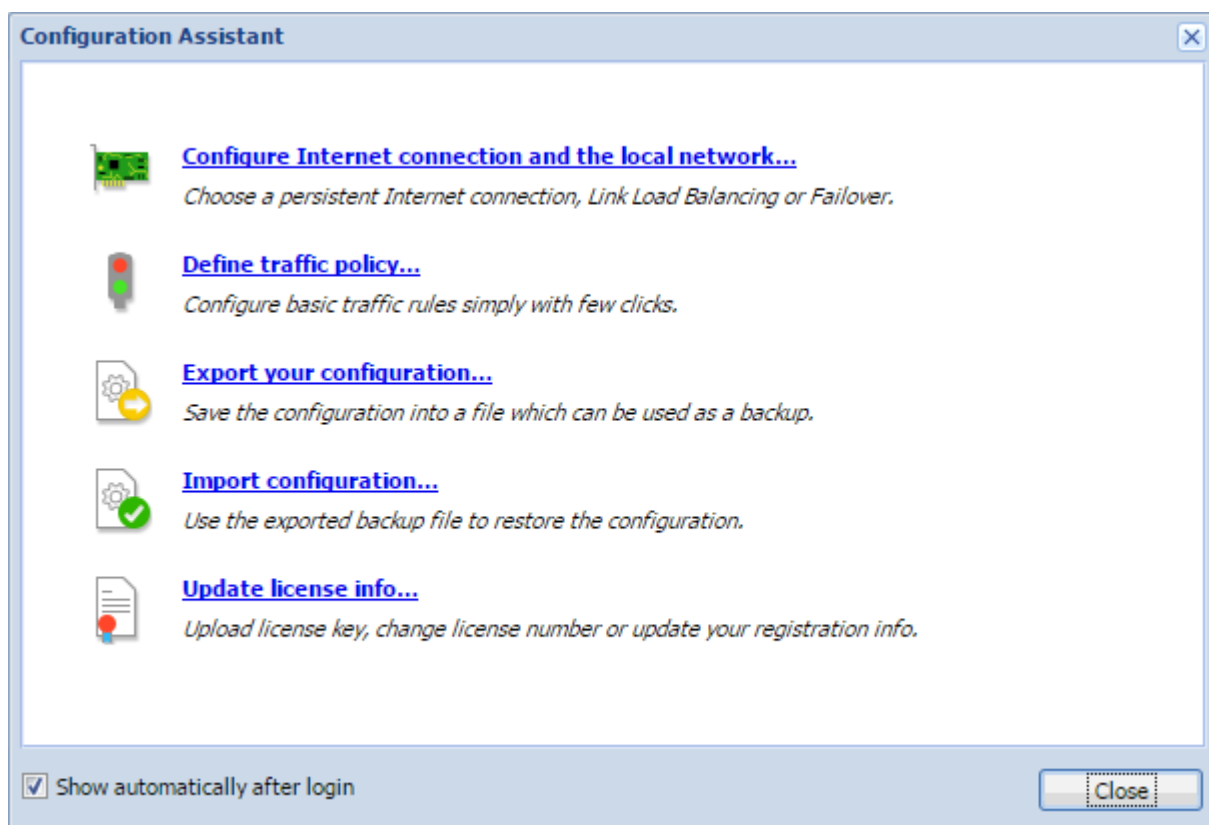
In the administration interface for the original hardware appliance, go to the **Interfaces** section and note all the interfaces and their type. You must ensure that the new hardware appliance has the same number of interfaces as the original.

IP addresses assigned to interfaces are imported to the new hardware appliance only if they are in manual mode. All interfaces with automatic mode get the new IP addresses from the DHCP server. This can be changed later in the **Interfaces** section.

Getting configuration files

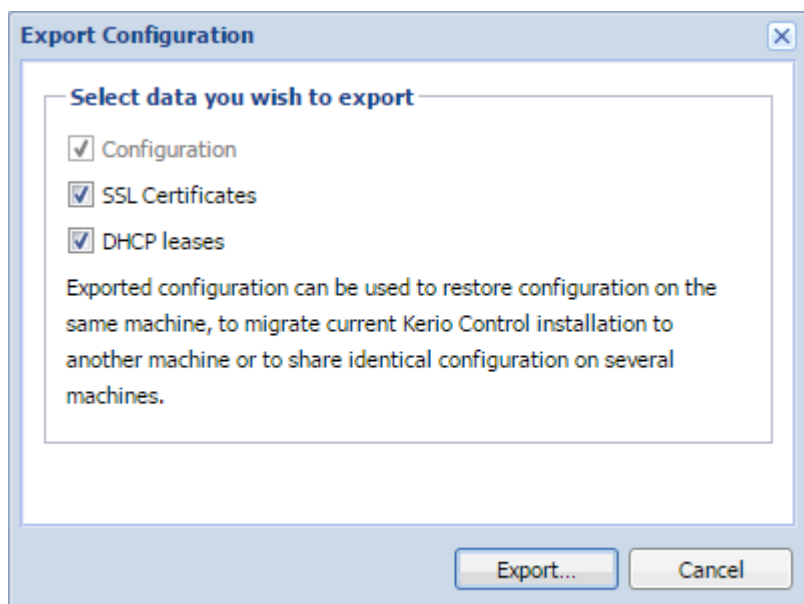
Exporting a configuration from the original Kerio Control appliance

1. In the administration interface, go to **Dashboard**.
2. Click **Configuration Assistant**.
3. In the **Configuration Assistant** dialog box, click **Export your configuration**.



4. In the **Export Configuration** dialog box, select all the items.

5. Click **Export**.



Your browser downloads the Kerio Control backup file with the configuration. The backup file has the following format: `ControlBackup_2016_03_03__14_44_45.tar.gz`.

Downloading a backup from FTP, MyKerio, or Samepage

If your original Kerio Control does not work, download the last backup from the [FTP server](#), [MyKerio](#), or [Samepage](#).

IMPORTANT

If your original Kerio Control does not work and you don't have a backup, configure the new Kerio Control manually.

Connecting the new Kerio Control to the Internet

The DHCP server in the Kerio Control hardware appliance is enabled by default. (For details, see the printed Installation Guide attached to the Kerio Control hardware appliance.)

Requirements:

- » The hardware appliance must be plugged into a socket.
- » At least one Internet cable must be connected.
- » At least one LAN cable must be connected.

At this point the hardware appliance is running and you can access the Internet from the local network. However, all users connected in the Kerio Control network will see the following page every 2 minutes until you activate your Kerio Control.

License Warning

There is no valid license for the product.

[Continue browsing](#)

Kerio Control

Registering a new Kerio Control

If the new hardware appliance is of the same type as the original one, you can use the same license. In all other cases, you need a new license. For details, contact your Kerio sales representative.

Registering the new Kerio Control hardware appliance is a part of the [Activation Wizard](#), which appears when you point your browser to `https://10.10.10.1/admin`.

NOTE

You can also register your new hardware appliance through MyKerio. For more details, see [Installing Kerio Control Box through MyKerio](#).

Upgrading the new Kerio Control hardware appliance

Before you import the configuration, you must have the same version of Kerio Control that was running on the original appliance (or a newer version) installed on the new hardware appliance:

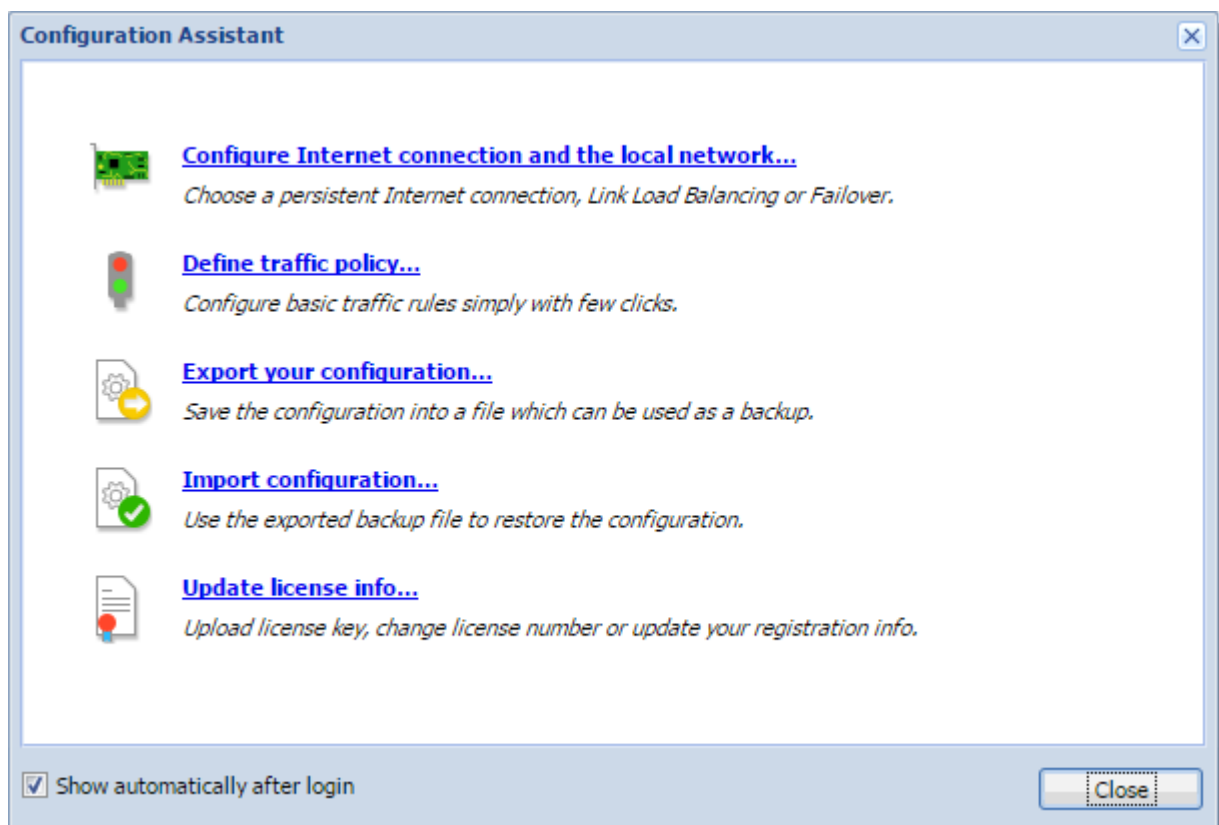
1. In the administration interface, go to **Advanced Options > Software Update**.
2. If a new version is available, click the **Download** button.
3. After the new version downloads, click **Upgrade Now** and wait for the server to restart.

Once the server has restarted your Kerio Control hardware appliance is up to date.

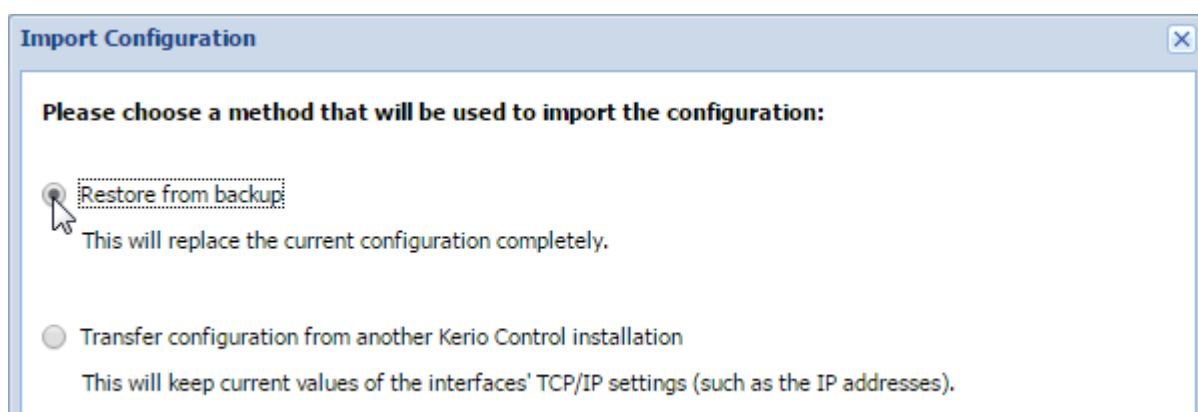
Importing a configuration to a new Kerio Control

At this point, you can import the Kerio Control configuration:

1. Open the administration interface. The **Configuration Assistant** should open automatically. If it does not, in the **Dashboard**, click **Configuration Assistant**.
2. In the **Configuration Assistant** dialog box, click **Import configuration**.



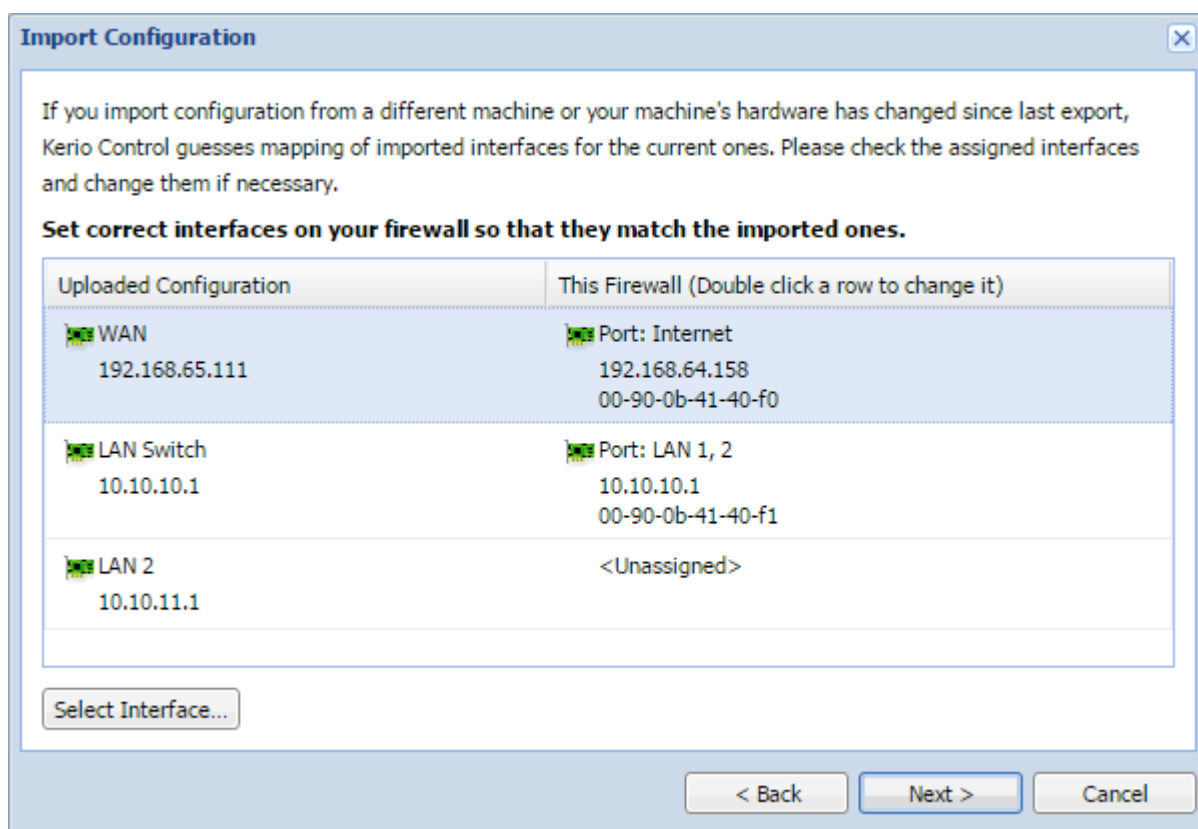
3. In the **Import Configuration** wizard, click **Upload configuration file**.
4. Select the file and click **Open**.
5. Select **Restore from backup** to completely replace all the configuration files.



6. Click **Next**.

7. Kerio Control pairs the imported network interfaces with the real interfaces on the appliance. To change the result:

- Double-click the interface you want to change.
- In the **Select Interface** dialog box, double-click the interface you want to pair. From now on, the interface from the original appliance is paired with the new one.



If you cannot pair the interfaces, edit them later in the **Interfaces** section of the administration interface.

8. Click **Next**.

9. Read the notes in the last step of the wizard and click **Finish**.

Kerio Control imports the configuration and restarts.

The new Kerio Control hardware appliance is now configured and ready to replace the original appliance.

Switching appliances

IMPORTANT

The following procedure requires Kerio Control to be taken offline.

1. Stop the original hardware appliance.
2. Disconnect all the cables.
3. Swap in the new appliance in place of the original one.
4. Connect all the cables.
5. Switch on the new appliance.
6. Open the web interface of the new appliance.
7. Go to the administration interface and in the **Interfaces** section check to see whether all the interfaces are configured properly. For example, standalone/LAN switch settings are not transferred, so you must set them up manually.

IMPORTANT

Connect to the administration interface from the local network. The Internet interface does not allow access by default.

2.8.5 Connecting to Kerio hardware appliances with a serial console

Connecting to the Kerio hardware appliance through a serial console can help you in the following cases:

- » Broken network access to the hardware appliance due to configuration mistakes or network hardware issues (both from the box and network switch sides)
- » Direct access to the Linux shell
- » You need to see the boot sequence from the hardware appliance
- » Access to BIOS

Setting a communication through a serial console

The connection uses these settings:

- » Speed: 9600
- » Data bits: 8
- » Stop bit: 1
- » Parity: none
- » Flow control: none

Use the instructions for your operating system to create these settings:

- » [Windows](#)
- » [Linux](#)
- » [OS X](#)

Accessing BIOS

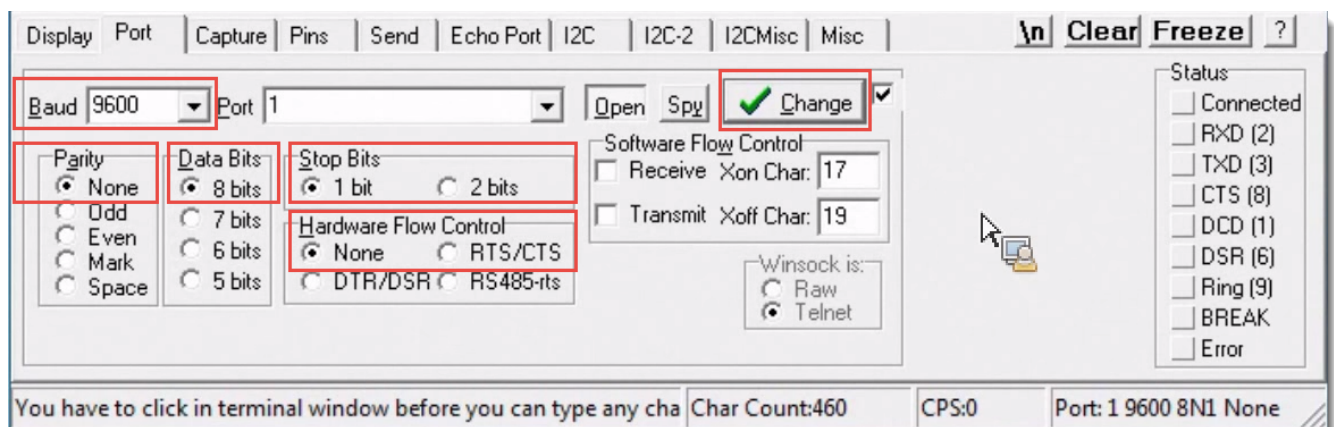
The connection uses these settings:

- » Speed: 115200
- » Data bits: 8
- » Stop bit: 1
- » Parity: none
- » Flow control: none

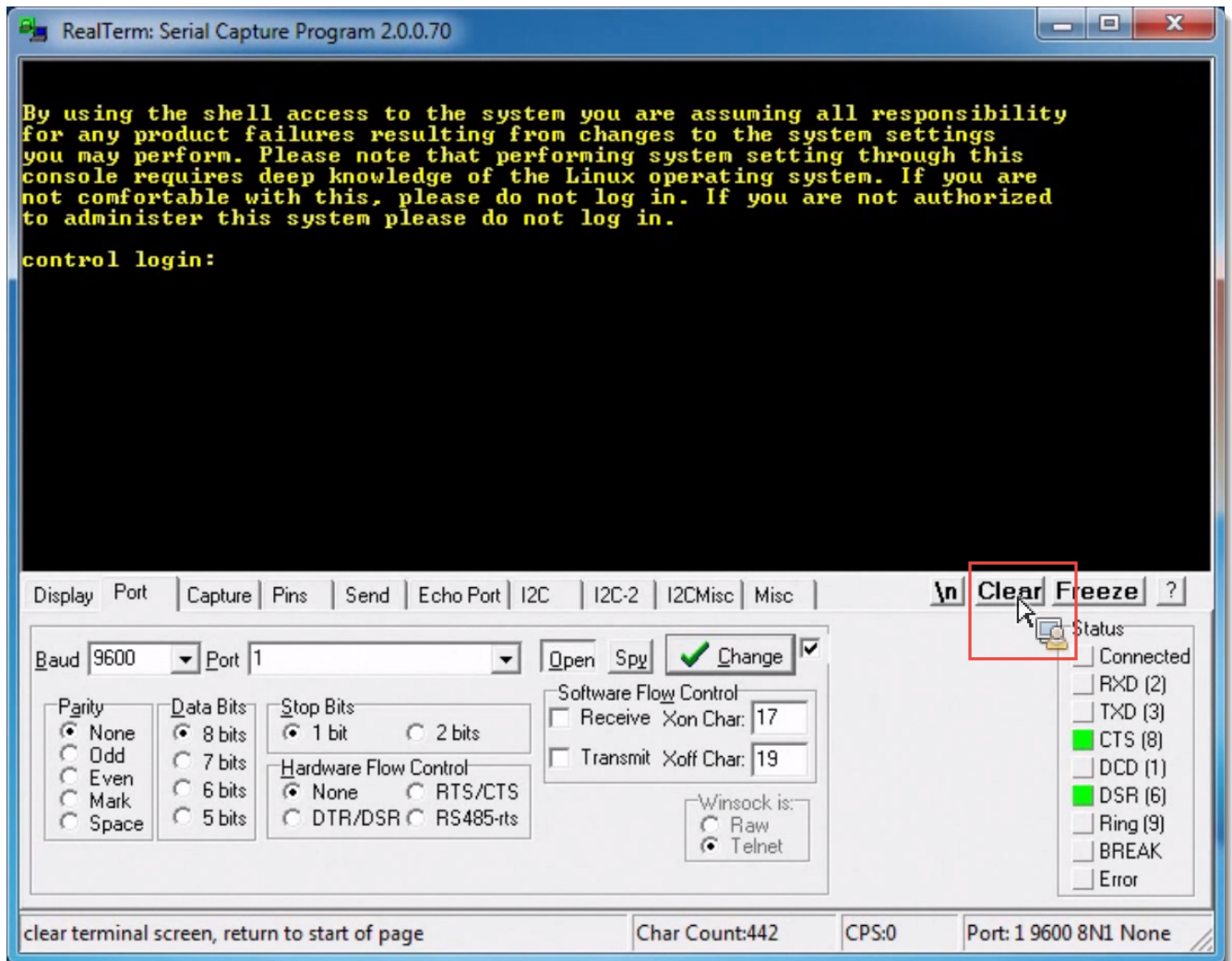
Windows

To connect to the hardware appliance, you need a special application such as PuTTY or RealTerm. Here are the steps for RealTerm:

1. Install RealTerm on your computer.
2. Attach the serial cable to the hardware appliance and to your PC.
3. Run RealTerm.
4. On the **Display** tab, select **ANSI**.
5. Click the **Port** tab and make the following selections there:
 - Baud: 9600
 - Parity: None
 - Data Bits: 8
 - Stop Bits: 1
 - Hardware Flow Control: None
6. Click **Change**.



Before logging on to your hardware device, click **Clear**.



Now, you can log in to your hardware device as root. Use the admin password for verification.

Linux

To connect to the hardware appliance, you need a special terminal software such as minicom. Here are the steps for minicom:

1. Install the minicom application.
2. Type the following command at the shell prompt: `$minicom -s`
3. In the menu, select **Serial port setup**.

```

+-----[configuration]-----+
| Filenames and paths      |
| File transfer protocols  |
| Serial port setup       |
| Modem and dialing        |
| Screen and keyboard      |
| Save setup as dfl        |
| Save setup as..         |
| Exit                     |
| Exit from Minicom        |
+-----+

```

4. Type **A**.
5. In the **A** section, type the interface: **TTYSO**. If you use an USB-to-serial adapter, select **USB** instead.
6. Press **Enter**.
7. Type **E**.
8. In the **E** section, type **CQ**: 9600 baud, Q: 8 bits, parity: none, stop bit: 1.

```

+-----+-----[Comm Parameters]-----+-----+
| A - Serial Del                               |
| B - Lockfile Locl      Current: 9600 8N1    |
| C - Callin Prol Speed      Parity          Data |
| D - Callout Prol A: <next>      L: None      S: 5 |
| E - Bps/Par/Bt B: <prev>      M: Even      T: 6 |
| F - Hardware Flo C: 9600      N: Odd       U: 7 |
| G - Software Flo D: 38400      O: Mark     V: 8 |
|                               P: Space        |
| Change which |                               |
+-----+-----+-----+-----+-----+
|                               Stopbits       |
| Screen al W: 1                Q: 8-N-1      |
| Save setl X: 2                R: 7-E-1      |
| Save setl                     |
| Exit |                       |
| Exit frol Choice, or <Enter> to exit? █    |
+-----+-----+-----+-----+-----+

```

9. Press **Enter**.
10. Type **F** and set it to **No**.
11. Press **Enter** to save the configuration.

```
+-----+
| A -   Serial Device   : /dev/ttyS0 |
| B - Lockfile Location : /var/lock  |
| C - Callin Program    :           |
| D - Callout Program   :           |
| E -   Bps/Par/Bits    : 9600 8N1  |
| F - Hardware Flow Control : No     |
| G - Software Flow Control : No     |
|                               |
|   Change which setting? █         |
+-----+
| Screen and keyboard |
| Save setup as dfl   |
| Save setup as..     |
| Exit                |
| Exit from Minicom   |
+-----+
```

12. Return to the main menu.

13. Select **Exit**.

```
+-----[configuration]-----+
| Filenames and paths |
| File transfer protocols |
| Serial port setup   |
| Modem and dialing   |
| Screen and keyboard |
| Save setup as dfl   |
| Save setup as..     |
| Exit                |
| Exit from Minicom   |
+-----+
```

Now, you can log in to your hardware device as root. Use the admin password for verification.

OS X

To connect to the hardware appliance, you need:

- » USB to Serial adapter with the FTDI chipset directly supported by OS X.
- » Special terminal software such as CoolTerm.

Here are the steps for CoolTerm:

1. Put the serial cable to the hardware appliance and also to your Mac with the USB to Serial adapter.
2. Open CoolTerm.
3. In the **Serial Port** section, select the USB adapter as port.
4. Baudrate: 9600.
5. Data Bits: 8.
6. Parity: none.

7. Stop Bits: 1.
8. Flow Control: no selection.
9. Click **Connect**.

Now you can log in to your hardware device as root. Use the admin password for verification.

2.8.6 WiFi

This topic describes deployment and configuration specific to Kerio Control hardware devices which contains embedded WiFi module.

Kerio Control NG100W and NG300W installation guide

Purpose

This document is a quick guide for safely installing and implementing Kerio Control NG100W and NG300W UTM appliances.

General Safety Instructions

During installation follow these security instructions:

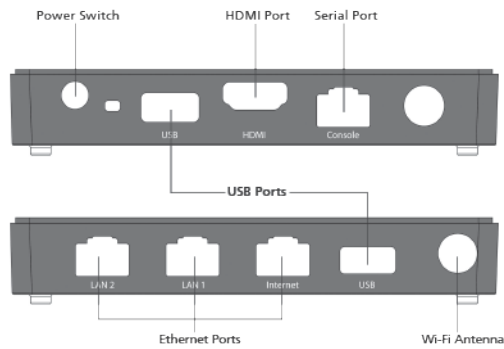
- » The appliance should be placed on a flat surface or securely mounted horizontally in rack enclosure.
- » Do not attempt to open or disassemble the appliance for any reason.
- » Strictly follow the installation instructions (see section 4).
- » Do not place the appliance near a heat source.
- » Place the appliance in a ventilated space, making sure that the appliance fans and vents are unobstructed at all times.
- » Do not expose the appliance to liquids of any kind. In the event of liquid intrusion, unplug the appliance immediately.
- » Verify that the voltage and frequency of the power socket matches the values printed on the power adapter before plugging in the appliance. Use only the power adapter supplied with the appliance.
- » Do not place any items on top of the power cable; keep the power cable away from walkways or other areas where it could pose a tripping hazard.

Appliance description

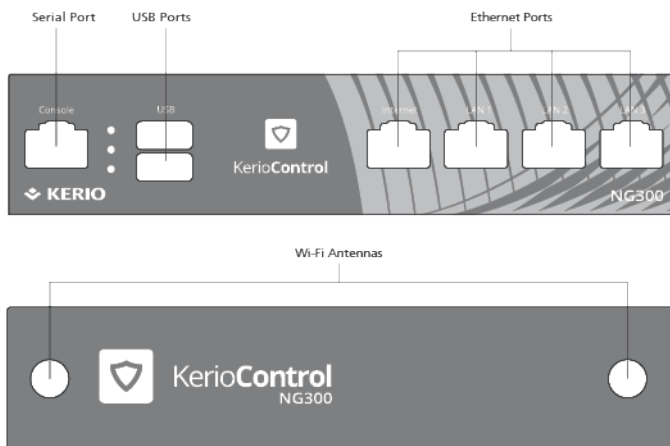
Kerio Control hardware appliance types:

- » Kerio Control Box NG100W — Desktop appliance
- » Kerio Control Box NG300W — Sub-1U table mountable appliance

Feature	Description
Serial port	Used for connecting to a console with a serial cable
USB ports	Input for USB devices
Ethernet network ports	Used for connecting to the Internet and the LAN with an Ethernet cable
Antenna(s)	Dual band antenna used for Wi-Fi



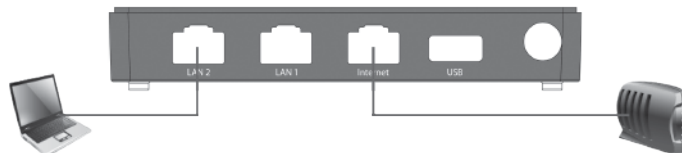
Screenshot 13: Kerio Control Box NG100W (front + back)



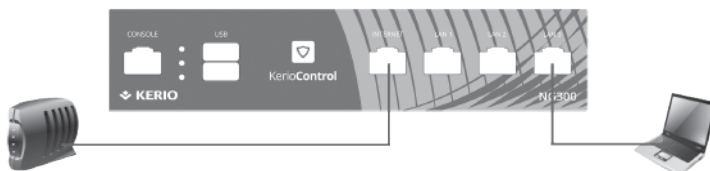
Screenshot 14: Kerio Control Box NG300W (front + back)

Kerio Control Box Installation and Configuration

Once a suitable place has been located for the appliance and it has been plugged into a power outlet according to the safety instructions, it is time to connect it to the network and configure settings.



Screenshot 15: Connecting Kerio Control Box NG100W to the network



Screenshot 16: Connecting Kerio Control Box NG300W to the network

To configure the appliance:

1. Connect the antenna(s) to the hardware appliance.
2. Connect the Internet port to the Internet (e.g. DSL or Cable modem) using an Ethernet cable.

3. Connect the LAN port to the computer that will be used to configure the appliance (see the figures below).
4. Turn on the appliance.

Now you have two options:

- » Add and manage the appliance through MyKerio (see [Installing Kerio Control Box through MyKerio](#))
- » Access the Kerio Control Administration through a browser (see below):
 - a. Set the networking preferences for Ethernet on the connected computer to **Automatic DHCP configuration**. (You can change it later after the configuration is complete).
 - b. Renew the DHCP lease on the computer and confirm it has an IP address of 10.10.10.11.
 - c. Open a web browser and connect to the Kerio Control Administration web interface using the following URL: **https://10.10.10.1/admin**
 - d. Ignore the SSL certificate warnings and proceed to the configuration wizard.
 - e. Follow the instructions provided by the wizard and configure the appliance.

NOTE

For troubleshooting purposes, you can use the serial port to connect the console to the device. See [Connecting to Kerio hardware appliances with a serial console](#).

Managing WiFi in Kerio Control NG100W and NG300W

NOTE

New in Kerio Control 9.2!

Kerio Control NG100W and Kerio Control NG300W include an embedded WiFi access point, which provides connectivity for wireless devices such as cell phones, tablets, and laptops.

The Kerio Control WiFi module supports:

- » Dual-band antenna, which provides 2.4 or 5 GHz
- » Wireless standards 802.11a, b, g, n, and ac
- » Authentication: none, WPA, WPA2 (PSK or Enterprise)
- » Up to eight wireless networks (SSIDs)

WiFi Parameters	Kerio NG100W	Kerio NG300W
MIMO	No	Yes
Antenna Type	1x 2dBi dipole dual-band external	2x2 dBi dipole dual-band external
Data Rate Max for 2.4 GHz	150 Mbps	300 Mbps
Data Rate Max for 5 GHz	433 Mbps	867 Mbps

NOTE

Kerio Control NG100W and Kerio Control NG300W do not include wireless client mode, so you cannot connect your Kerio Control to another WiFi access point.

Configuring the WiFi access point

To configure the WiFi access point in Kerio Control, select a country, band, and channel. The band and channel are preconfigured to the fastest options for the selected country.

1. In the administration interface, go to **Interfaces and WiFi**.
2. Click the **WiFi** button.
3. In the **Country** drop-down list, select the country where the hardware device is deployed. Each country has different legislative restrictions for bands and channels, and Kerio Control allows you to set only bands and channels that are permitted in the selected country.
4. In the **Band** drop down list, the fastest allowed band is selected by default. If your devices do not support the latest **ac (5 GHz)** standard, switch the band to another one (a, b, g, or n).
5. In the **Channel** drop down list, the fastest channel is selected by default. If your devices do not have a good signal, select a different channel.

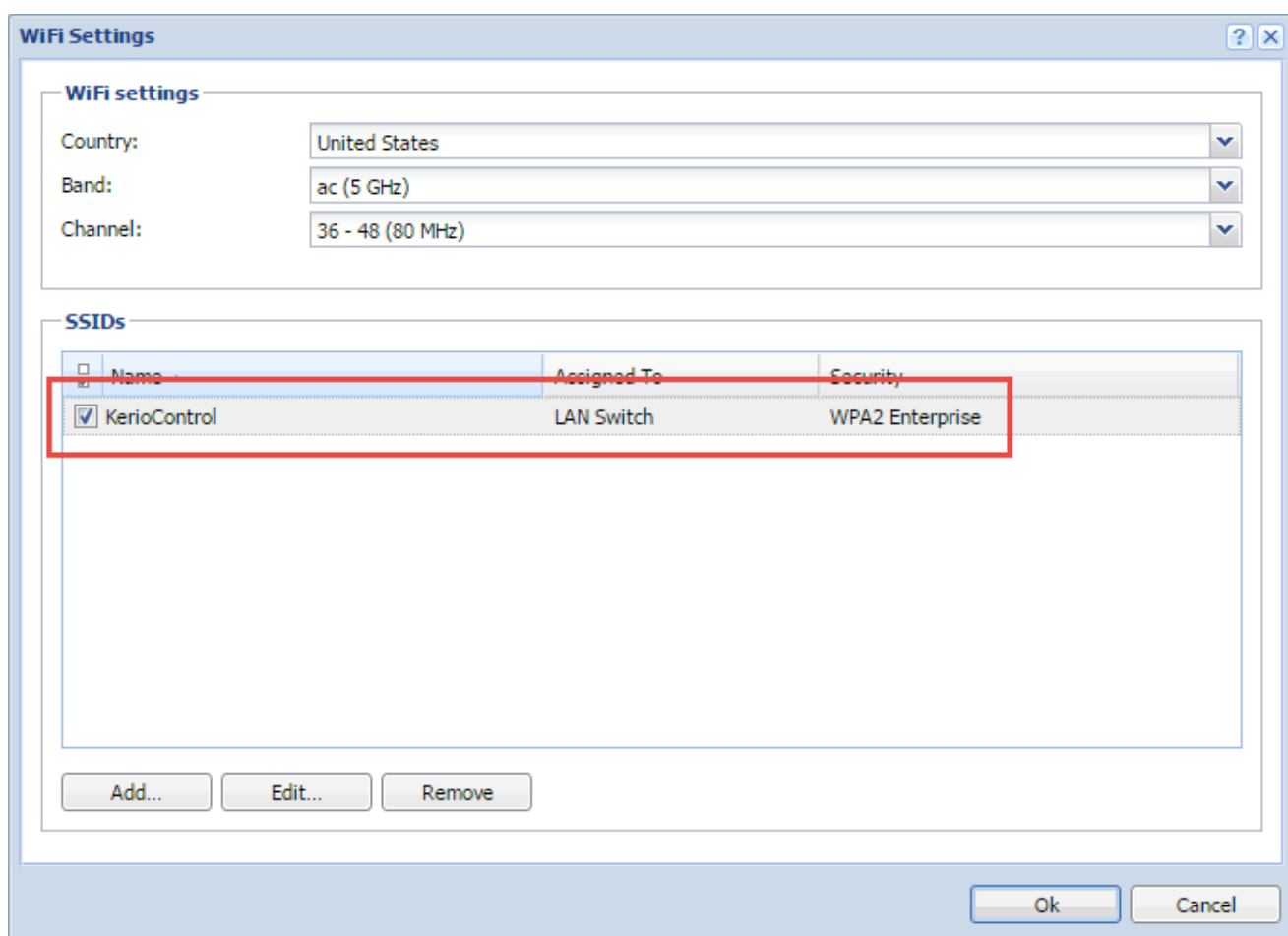
Now your WiFi is ready and the settings are common for all Kerio Control SSIDs.

Configuring WiFi networks

Service Set Identifier (SSID) allows you to create different WiFi networks. Because WiFi needs at least one SSID to work. The first SSID, `KerioControl`, is configured for you:

- » `SSID = KerioControl`
- » It is set up as a network bridge (LAN Switch), so that it is a part of your existing local network and users get IP addresses from the local network range.
- » It is set to use WPA2 Enterprise, so your users use their Kerio Control accounts for connecting to the WiFi network.

To use the `KerioControl` network, select the SSID and click **OK**

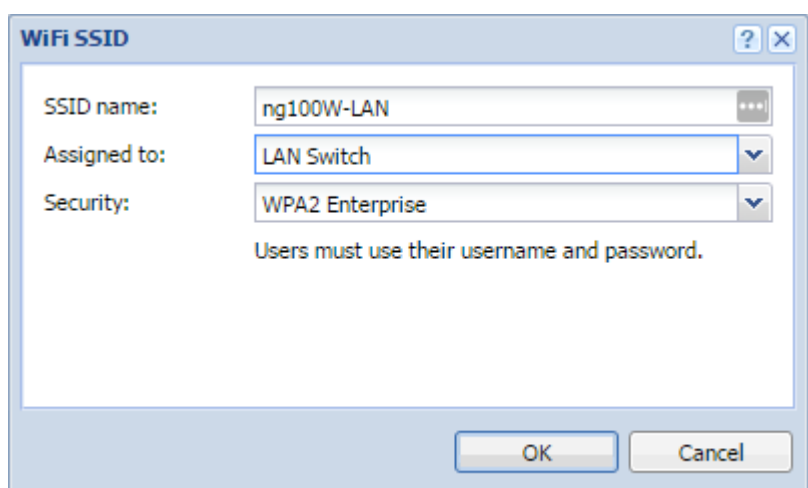


Creating new SSIDs

1. In the administration interface, go to **Interfaces and WiFi**.
2. Click the **WiFi** button.
3. In the **WiFi Settings** dialog box, click **Add**.
4. In **SSID name**, type a name for the network. The SSID identifies the WiFi network. It displays on users' devices, so the name should be short and easy to remember.
5. In the **Assigned to** drop down menu, select:
 - **LAN Switch** to add WiFi to an existing subnet. Your WiFi network runs in the wireless bridging mode. For more information, refer to [Wireless bridging on Kerio Control NG100W and NG300W](#) (page 63).
 - **Standalone** to add a different network subnet where users get IP addresses from a different range. For details, see [Configuring WiFi guest networks](#) and [Configuring Ethernet ports in Kerio Control hardware appliances](#). If you select this option, you must also configure the TCP/IP settings and DHCP. For details, see [Configuring TCP/IP settings in Kerio Control interfaces](#) and [DHCP server in Kerio Control](#).

Usually you need one SSID assigned to a LAN switch for your local users and one standalone SSID for a guest network. For details, see [Wireless bridging in Kerio Control](#) and [Configuring WiFi guest network](#).

6. In the **Security** drop down menu, select WPA2 Enterprise for local networks and WPA2 PSK for guest networks. For details, see [Supported authentication types](#).



WiFi SSID

SSID name:

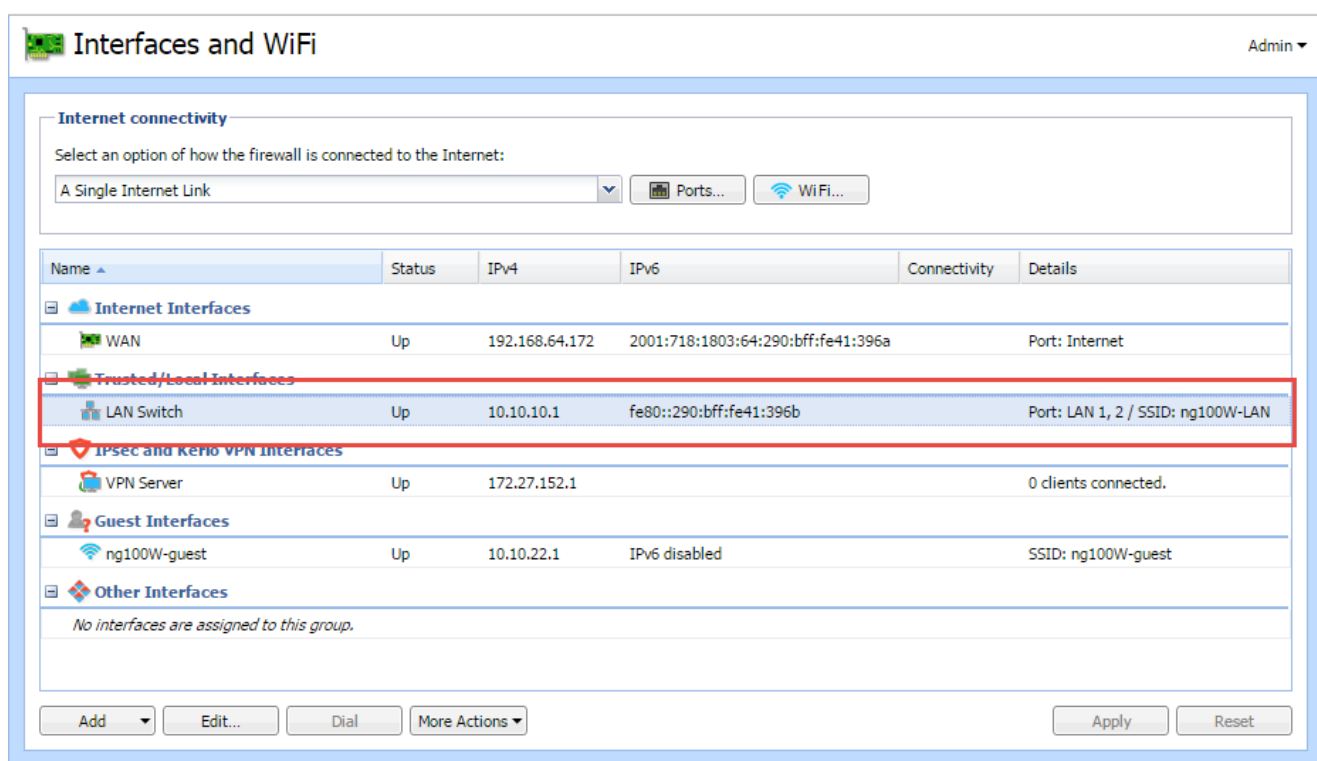
Assigned to:

Security:

Users must use their username and password.

OK Cancel

To verify that the WiFi network is up and running, go to the **Interfaces and WiFi** section and check the status in the **Trusted/Local Interfaces** group.



Interfaces and WiFi Admin

Internet connectivity

Select an option of how the firewall is connected to the Internet:

Name	Status	IPv4	IPv6	Connectivity	Details
Internet Interfaces					
WAN	Up	192.168.64.172	2001:718:1803:64:290:bff:fe41:396a		Port: Internet
Trusted/Local Interfaces					
LAN Switch	Up	10.10.10.1	fe80::290:bff:fe41:396b		Port: LAN 1, 2 / SSID: ng100W-LAN
IPsec and Kerio VPN Interfaces					
VPN Server	Up	172.27.152.1			0 clients connected.
Guest Interfaces					
ng100W-guest	Up	10.10.22.1	IPv6 disabled		SSID: ng100W-guest
Other Interfaces					
No interfaces are assigned to this group.					

Add Edit... Dial More Actions Apply Reset

Supported authentication types

Type	Description
None	WiFi connection is accessible for all WiFi clients. They do not need any type of password.
WPA PSK	Authentication requires a preshared key encrypted with WPA (WiFi Protected Access).
WPA Enterprise	Authentication requires Kerio Control usernames and passwords. Kerio Control uses embedded RADIUS authentication. Do not use WPA Enterprise for a guest network.
WPA2 PSK	The most secure and recommended authentication with a preshared key applicable to your guest network.
WPA2 Enterprise	The most secure and recommended authentication requires Kerio Control usernames and passwords. Kerio Control uses embedded RADIUS authentication. Do not use WPA2 Enterprise for a guest network.

Troubleshooting

Users from Germany, Netherlands, and Bulgaria should use channels less than 140 for optimal power performance. For further information refer to <https://www.gfi.com/support/products/Using-Wifi-channels-above-140-in-Kerio-Control-NG100W-and-NG300W>.

For more information, refer to [Wifi issues](#) (page 355).

Wireless bridging on Kerio Control NG100W and NG300W

NOTE

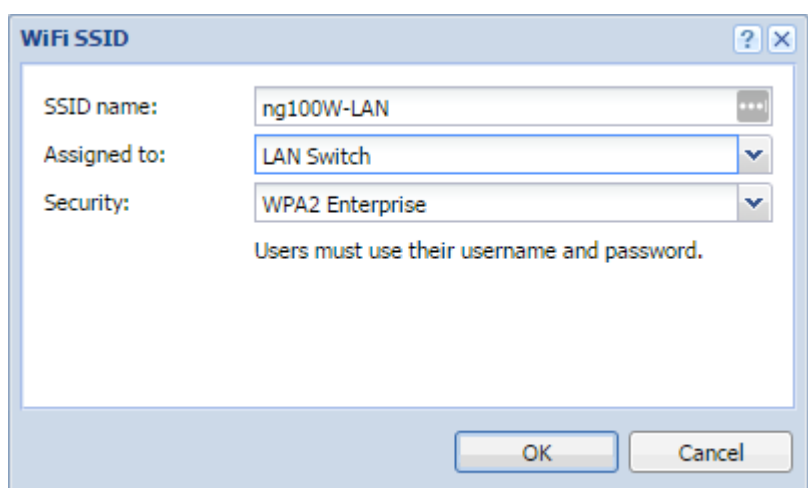
New in Kerio Control 9.2!

Kerio Control includes the embedded WiFi access point. For more information, refer to [Managing WiFi in Kerio Control NG100W and NG300W](#) (page 59). This article describes how to run WiFi interfaces in an existing subnet so that your internal WiFi users share the same LAN and get IP addresses from the same subnet as users connected through the Ethernet.

You can also configure the WiFi network as a guest network. For more information, refer to [Configuring WiFi guest networks on Kerio Control NG100W and NG300W](#) (page 64).

Configuring WiFi for Kerio Control users

1. Verify that WiFi settings are configured properly. For more information, refer to [Managing WiFi in Kerio Control NG100W and NG300W](#) (page 59).
2. In the administration interface, go to **Interfaces and WiFi**.
3. Click the **WiFi** button.
4. In the **WiFi Settings** dialog box, select an existing SSID or add a new one.
5. In the **Assigned to** drop down menu, select **LAN Switch** to add WiFi to an existing subnet. Your WiFi network runs in wireless bridging mode. For more information, refer to [Configuring Ethernet ports in Kerio Control hardware appliances](#) (page 44). In the **Security** drop down list, select **WPA2 Enterprise**. WPA2 Enterprise is the most secure and recommended authentication. WPA2 Enterprise uses embedded RADIUS authentication, therefore, requires Kerio Control usernames and passwords for connecting to the WiFi network.
6. Click **OK** twice.



WiFi SSID

SSID name:

Assigned to:

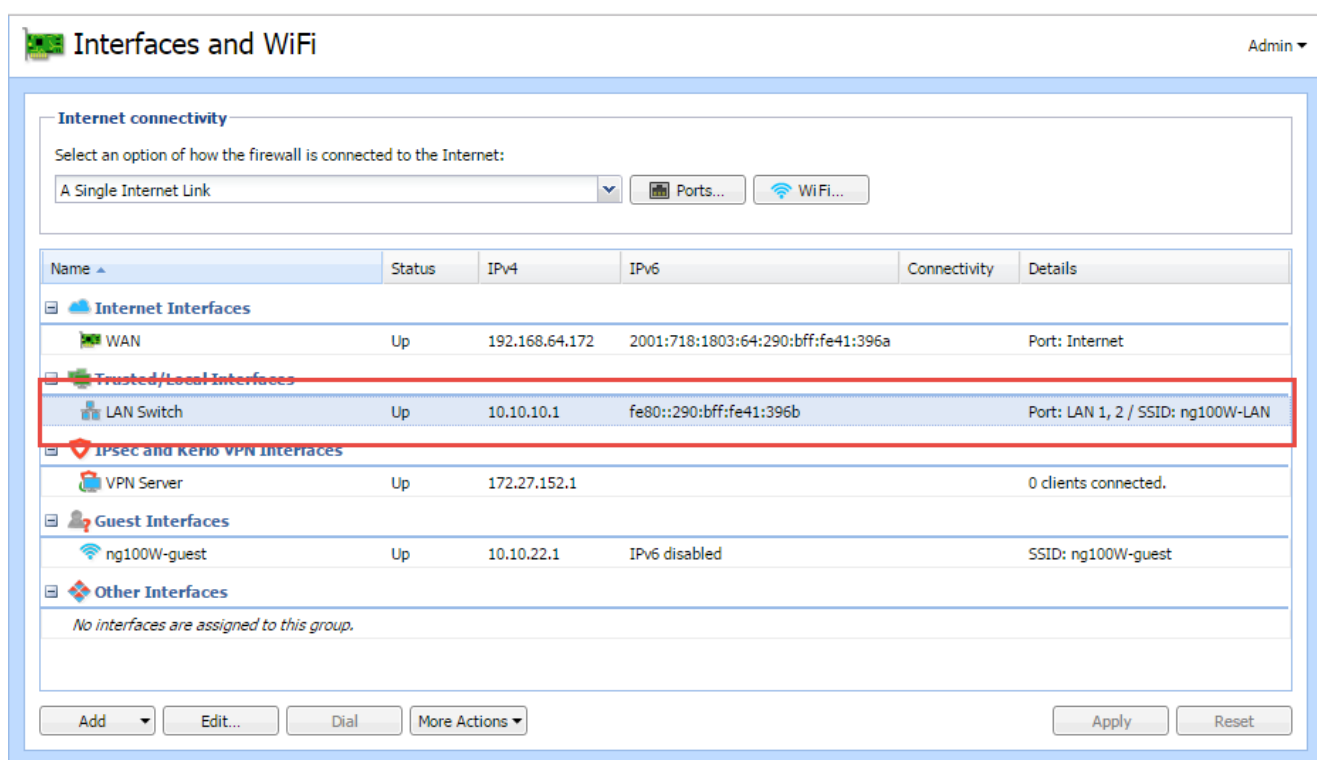
Security:

Users must use their username and password.

OK Cancel

To verify that the WiFi network is up and running, go to the **Interfaces and WiFi** section and check the status in the **Trusted/Local Interfaces** group.

The WiFi interface is now bridged, so users connected through WiFi are placed in the same network segment as users connected through Ethernet interfaces assigned to the LAN switch.



Interfaces and WiFi Admin

Internet connectivity

Select an option of how the firewall is connected to the Internet:

Name	Status	IPv4	IPv6	Connectivity	Details
Internet Interfaces					
WAN	Up	192.168.64.172	2001:718:1803:64:290:bff:fe41:396a		Port: Internet
Trusted/Local Interfaces					
LAN Switch	Up	10.10.10.1	fe80::290:bff:fe41:396b		Port: LAN 1, 2 / SSID: ng100W-LAN
IPsec and Kerio VPN Interfaces					
VPN Server	Up	172.27.152.1			0 clients connected.
Guest Interfaces					
ng100W-guest	Up	10.10.22.1	IPv6 disabled		SSID: ng100W-guest
Other Interfaces					
No interfaces are assigned to this group.					

Add Edit... Dial More Actions

Apply Reset

Configuring WiFi guest networks on Kerio Control NG100W and NG300W

NOTE

New in Kerio Control 9.2!

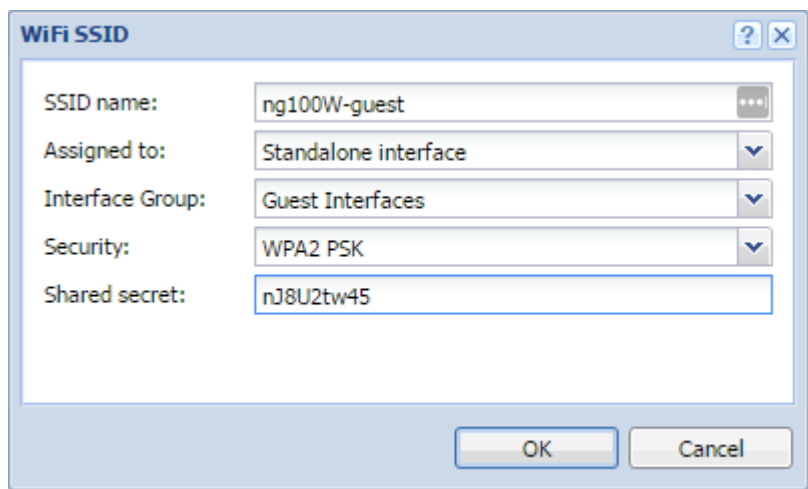
Kerio Control includes the embedded WiFi access point. For more information, refer to [Managing WiFi in Kerio Control NG100W and NG300W](#) (page 59). This article describes how to run a WiFi guest network as a separate network with a shared password so that guests can use WiFi without accessing your local network.

You can also configure WiFi as a network bridge. For more information, refer to [Wireless bridging on Kerio Control NG100W and NG300W](#) (page 63).

Configuring WiFi for guests

To set up a guest WiFi network:

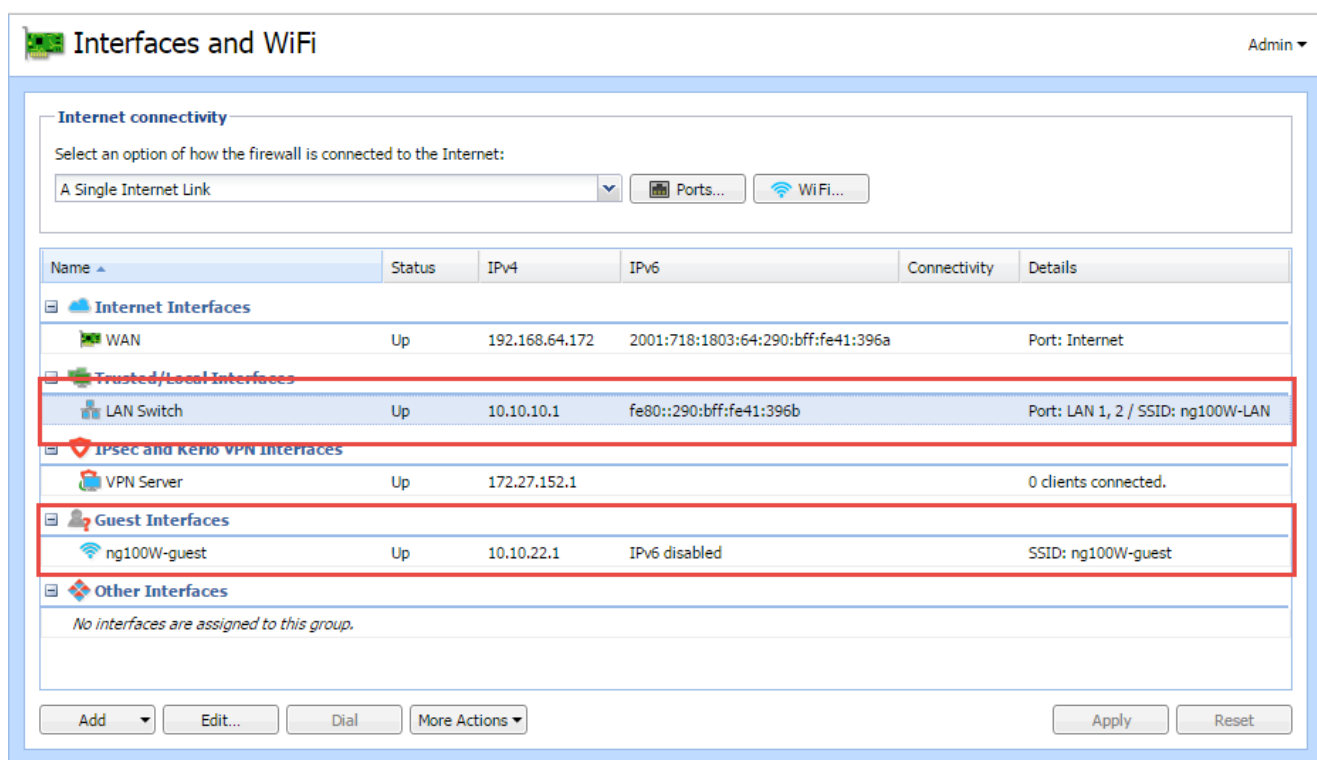
1. Verify that the WiFi settings are configured properly. For more information, refer to [Configuring WiFi networks](#) (page 60).
2. In the administration interface, go to **Interfaces and WiFi**.
3. Click the **WiFi** button.
4. Click **Add** to create a new SSID.
5. In the **WiFi SSID** dialog box, type a name for the SSID. The SSID identifies the WiFi network. It displays on users' devices, so the name should be short and easy to remember.
6. In the **Assigned to** drop down menu, select **Standalone interface** to create a new subnet in your network. For more information, refer to [Configuring Ethernet ports in Kerio Control hardware appliances](#) (page 44).
7. In the **Interface Group** drop down list, select **Guest Interfaces**.
8. In the **Security** drop down list, select **WPA2 PSK**.
9. In the **Shared secret** field, type a password. The password must be at least eight characters long.
10. Click **OK** twice.



The screenshot shows a dialog box titled "WiFi SSID" with a light blue header and standard window controls (minimize, maximize, close). Inside the dialog, there are five configuration fields, each with a label on the left and a corresponding input field on the right. The fields are: "SSID name:" with the value "ng100W-guest" and a small "show/hide" icon; "Assigned to:" with a dropdown menu showing "Standalone interface"; "Interface Group:" with a dropdown menu showing "Guest Interfaces"; "Security:" with a dropdown menu showing "WPA2 PSK"; and "Shared secret:" with the value "nJ8U2tw45". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Give the password and SSID name to all guests who want to use this WiFi guest network. They need it for authentication to the network.

The new guest network is placed under the **Guest Interfaces** group in the **Interfaces** section. The WiFi interface is standalone, so all users connected through this WiFi are placed in a separate network segment.



Verify on your mobile device or laptop that you can see the new WiFi network and that you can connect your device to the new network. The WiFi requires the password you created.

2.9 Kerio Control API

The Kerio Control API enables you to programmatically access your Kerio Control server to integrate with third-party solutions or write scripts to automate specific tasks. The API provides all actions available in the client and administration interfaces of the product. For example, you can add/remove users, update IP address groups, read logs, manage time ranges, and much more.

For more information about Kerio Control API, go to http://go.gfi.com/?pageid=control_help#cshid=api

3 Using

This topic contains information about:

3.1 Using Dashboard in Kerio Control	67
3.2 Tips for tablets	68
3.3 Antivirus	69
3.4 Backup	73
3.5 Accounts	77
3.6 Directory services	89
3.7 Monitoring	110
3.8 Logs	123
3.9 VPN	145

3.1 Using Dashboard in Kerio Control

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**.

The screenshot shows the Kerio Control Dashboard interface. A red box labeled "Tiles" points to the top of the dashboard area. Another red box labeled "Add a new tile to your Dashboard" points to the "Add Tile" button at the bottom left. A red box labeled "Remove this tile" points to a minus icon in the top right corner of the "Top Active Hosts" tile. A red box labeled "To change the tile order, drag the tile to another place" points to a four-way arrow icon in the top left corner of the "Top Active Hosts" tile.

Dashboard Admin ▾

System Health

- RAM: 394.06 MB of 1.48 GB used
- CPU: 0.95%
- Disk: 268.40 MB of 6.56 GB used

Ethernet 2

System Status

- Uptime: 1d 22:02:04
- Kerio Control: Up to date
- Antivirus: Working properly
- Intrusion Prevention: Working properly
- Kerio Control Web Filter: Disabled
- IPsec VPN Server: Working properly
- Kerio VPN Server: Working properly

Connectivity

	Status	Current Rx	Current Tx
Ethernet 2	Up	1 KB/s	0 KB/s

Top Active Hosts

Download [Show on Active Hosts](#)

Firewall		0 KB/s
192.168.94.1	bjones	0 KB/s

Upload [Show on Active Hosts](#)

Firewall		0 KB/s
192.168.94.1	bjones	0 KB/s

© Kerio Technologies s.r.o. All rights reserved. [Legal Notices](#)

Add Tile Add a new tile to your Dashboard Configuration Assistant... Suggest Idea... Contact Technical Support...

3.2 Tips for tablets

This article provides a few useful tips for a better administration user experience on tablet devices.

Tip	Description
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. If you have Multi-Touch allowed on iOS 5, you can use up to three fingers for log scrolling.

3.3 Antivirus

Kerio Control protects your network against viruses, Trojans, and malware.

3.3.1 Configuring antivirus protection	69
3.3.2 Configuring email scanning	70
3.3.3 Configuring HTTP and FTP scanning	71
3.3.4 Using an external antivirus with Kerio products	72

3.3.1 Configuring antivirus protection

Kerio Control provides integrated Kerio Antivirus powered by the Bitdefender antivirus engine, which check 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 are scanned.

NOTE

Use of Kerio 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.

If you set a strict content filtering policy, ensure that Kerio Antivirus can reach the following URLs:

- » bupdate.kerio.com
- » bupdate-cdn.kerio.com

For details about creating content rules, see [Configuring the Content Filter](#).

Configuring antivirus protection

1. In the administration interface, go to **Antivirus**.
2. On tab **Kerio Antivirus**, select option **Use Kerio Antivirus** This option is available if the license key for Kerio Control includes a license for the Kerio Antivirus module or in trial versions.
3. Select option **Check for update every ... hours**. If any new update is available, it is downloaded automatically. If the update attempt fails, detailed information are logged into the [Error log](#).


Updates

☒ Check for update every hours

Last update check: 4 minutes ago

Current virus database updated: less than a minute ago

Threat definitions count: 8528221



NOTE

If the update attempt fails, detailed information are 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.

WARNING

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**.

3.3.2 Configuring email scanning

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

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

WARNING

1. Within antivirus scanning, it is possible to remove only infected attachments, entire email messages cannot be dropped.
2. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network). To check also outgoing traffic (e.g. when local clients connect to an SMTP server without the local network), define a corresponding [traffic rule](#) using the SMTP protocol inspector.

Configuring email scanning

1. In the administration interface, go to **Antivirus**.
2. On tab **Antivirus Engine**, check that antivirus control is enabled and select options **Enable SMTP scanning** and **Enable POP3 scanning**.
3. On tab **Email Scanning**, select option **Prepend subject message with text**. This text informs the recipient of the message and it can be also used for automatic message filtering.

NOTE

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

4. Use the **TLS connections** section to set firewall behavior for cases where both mail client and the server support TLS-secured SMTP or POP3 traffic. In case that TLS protocol is used, unencrypted connection is established first. Then, client and server agree on switching to the secure mode (encrypted connection). If the client or the server does not support TLS, encrypted connection is not used and the traffic is performed in a non-secured way. If the connection is encrypted, firewall cannot analyze it and perform antivirus check for transmitted messages.
5. The **If an attachment cannot be scanned** section defines actions to be taken if one or multiple files attached to a message cannot be scanned for any reason (e.g. password-protected archives, damaged files, etc.):
 - **Remove the attachment from the email message** — Kerio Control reacts in the same way as when a virus was detected (including all the actions described above).
 - **Allow delivery of the attachment** — Kerio Control behaves as if password-protected or damaged files were not infected. Generally, this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files (typically password-protected archives) and the antivirus is installed on the workstations.
6. Click **Apply**.

3.3.3 Configuring HTTP and FTP scanning

In HTTP and FTP traffic, Kerio Control can scanned the selected types of files.

The transmitted file is saved in a temporary file on the local disk of the firewall. Kerio Control caches the last part of the transmitted file (segment of the data transferred) and performs an antivirus scan of the temporary file.

If it detects a virus, the last segment of the data is dropped. The client then receives an incomplete (damaged) file which cannot be executed and the virus cannot be activated. If no virus is found, Kerio Control sends also the rest of the file and the transmission is completed successfully.

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

Configuring scanning

1. In the administration interface, go to **Antivirus > Antivirus Engine**.
2. Verify that antivirus control is enabled and select options **Enable HTTP scanning** and **Enable FTP scanning**.

3. On the **HTTP, FTP Scanning** tab, select **Alert the client**. Kerio Control sends an email messages warning to the user who attempts to download the file that a virus was detected and download was stopped for security reasons. Kerio Control sends alert messages when:

- The user is authenticated and connected to the firewall
- A valid email address is set in a corresponding user account
- The SMTP server used for mail sending is configured

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

- **Deny transmission of the file** — Kerio Control considers the file as infected and denies the transmission.
- **Allow transmission of the file** — Kerio Control treats the file as not infected. Use this option only if, for example, users transmit a big volume of compressed password-protected files and the antivirus is installed on the workstations.

HTTP and FTP scanning rules

Kerio Control contains a set of predefined rules for HTTP and FTP scanning. The firewall administrator can change the default configuration.

Scanning rules are ordered and processed from the top. When Kerio Control finds a rule which matches the object, the appropriate action is taken and other rules are stopped.

If the object does not match any rule, Kerio Control does not scan the object. If you want to scan object types other than in the predefined rules, add a rule which enables scanning of any URL or MIME type to list.

To add new rules, follow these instructions:

1. On the **HTTP, FTP Scanning** tab, click **Add**.

2. Select **Condition type**:

- **HTTP URL** — URL of the object (for example, `www.kerio.com/img/logo.gif`), a string specified by a wildcard matching (for example, `*.exe`) or a server name (for example, `www.kerio.com`). Server names represent any URL at a corresponding server (`www.kerio.com/*`).
- **HTTP MIME type** — MIME types can be specified either by complete expressions (e.g. `image/jpeg`) or using a wildcard matching (for example, `application/*`).
- **Filename** — this option filters out certain filenames (not entire URLs) transmitted by FTP or HTTP (for example, `*.exe`, `*.zip`, and so on). If only an asterisk is used, the rule applies to any file transmitted by HTTP or FTP.
- **File type** — select a group of predefined file extensions.

NOTE

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

3. Select **Action** to scan the objects for viruses.

4. Type a description.

5. Save the settings.

3.3.4 Using an external antivirus with Kerio products

Kerio Control and Kerio Connect include Kerio Antivirus that provides an integrated protection against malicious viruses.

However, you can use alternative antivirus solutions by using the **Kerio Antivirus SDK for Kerio Connect and Kerio Control**. The Antivirus SDK includes a public API that can be used to write plugins for alternative antivirus solutions. Get the [SDK](#) and read our [blog](#) to get detailed information.

3.4 Backup

This section provides information about server backup and data recovery.

3.4.1 Saving configuration to FTP server	73
3.4.2 Saving configuration to MyKerio	75
3.4.3 Saving configuration to Samepage	76

3.4.1 Saving configuration to 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

NOTE

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**.

Remote Services Admin ▾

MyKerio SMTP Relay Dynamic DNS **Configuration Backup**

☒ Enable automatic daily backup

Settings

☐ MyKerio
☒ **FTP**
☐ Samepage

Username: ...
 Password: ...
 URL:

Backup

Last backup: 1 day and 1 hour ago
 Location: <ftp://ftp.company.com/backup>

Kerio Control uploads configuration files once a day.

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](#).

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` or `ftp://[IPv6-address]`

Example

- » FTP server has no DNS name (AAAA record) and is accessible via an IPv6 address only (`2002:1234:4567:89-ab: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`

3.4.2 Saving configuration to MyKerio

NOTE

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

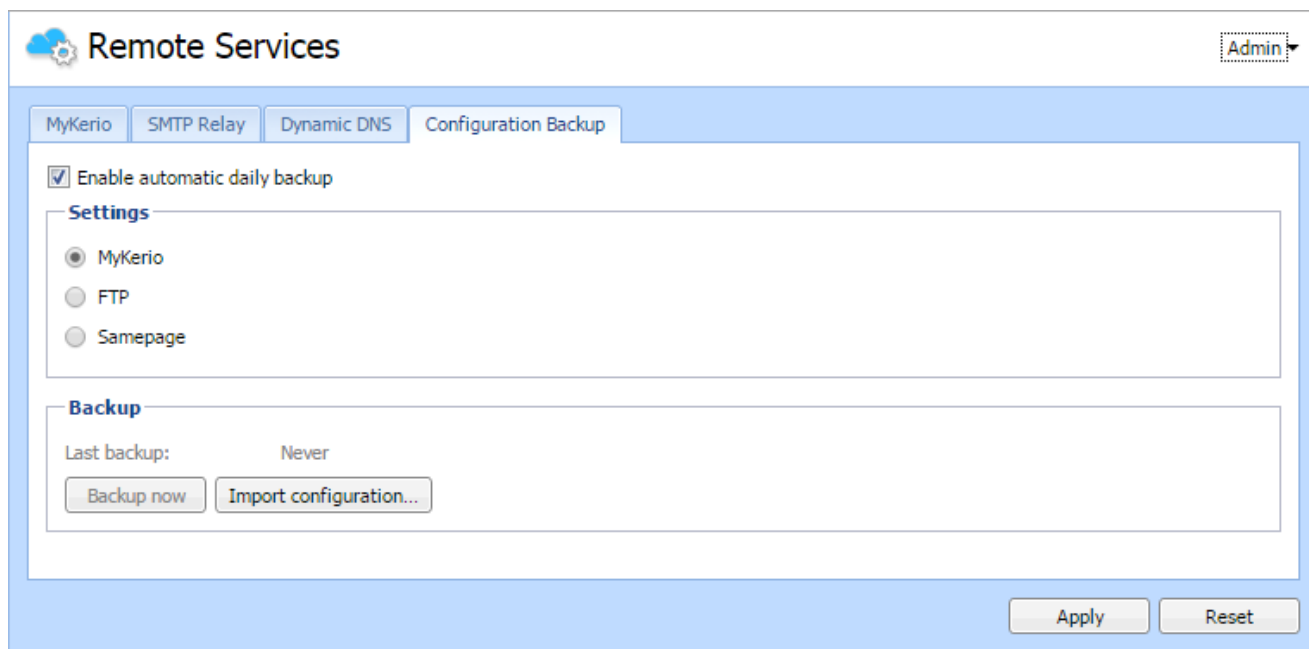
To configure backup to an FTP server instead, see the [Saving configuration to FTP server](#) article.

Saving configuration to MyKerio

Before you start, connect your Kerio Control to MyKerio. For more information, refer to [Adding Kerio Control to MyKerio](#) (page 16).

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**.



The screenshot shows the 'Remote Services' configuration window in Kerio Control. The 'Configuration Backup' tab is selected. The 'Enable automatic daily backup' checkbox is checked. Under the 'Settings' section, the 'MyKerio' radio button is selected. Under the 'Backup' section, the 'Last backup' status is 'Never'. There are buttons for 'Backup now' and 'Import configuration...'. At the bottom right, there are 'Apply' and 'Reset' buttons. An 'Admin' link with a right arrow is in the top right corner.

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](#).

3.4.3 Saving configuration to Samepage

IMPORTANT

Support of Samepage backups in Kerio Control ends soon and works only for Samepage accounts created before July 2016. Newer accounts can no longer upload backups to Samepage.

You can upload your configuration backups to [MyKerio](#) instead. For more information, refer to [Saving configuration to MyKerio](#) (page 75).

Kerio Control can automatically backup and upload the configuration files to [Samepage.io](#) every day.

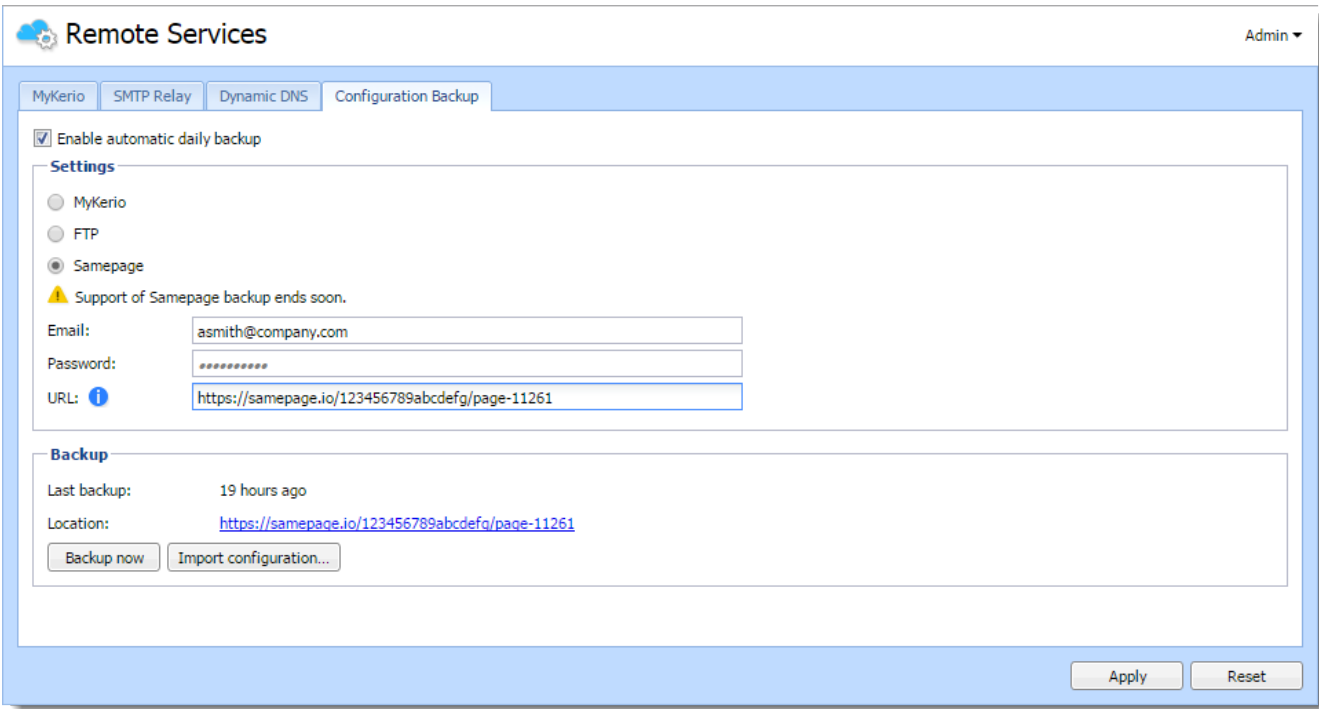
Each backup includes:

- » Configuration files
- » SSL certificates
- » DHCP leases

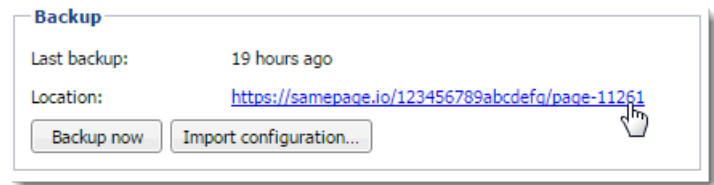
NOTE

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.
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**.



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.



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](#).

3.5 Accounts

This section helps you to create and edit user accounts, setting access rights and maintain user groups.

3.5.1 Managing user accounts in Kerio Control	78
3.5.2 Setting access rights in Kerio Control	81
3.5.3 Managing user quotas in Kerio Control	81
3.5.4 Blocking web object elements for particular users	84
3.5.5 Configuring automatic user login	85
3.5.6 Creating user groups in Kerio Control	86

3.5.1 Managing user accounts in Kerio Control

User accounts are used to:

- » Authenticate users with their username and password, optionally with 2-step verification. For more information, refer to [Configuring 2-step verification](#) (page 212).
- » Gather reporting data in Kerio Control Statistics. For more information go to http://go.gfi.com/?pageid=control_help#cshid=1806
- » Set access rights for Kerio Control administration. For more information, refer to [Setting access rights in Kerio Control](#) (page 81).
- » Add users to groups. For more information, refer to [Creating user groups in Kerio Control](#) (page 86).
- » Automatic user login. For more information, refer to [Configuring automatic user login](#) (page 85).
- » Set quotas for users. For more information, refer to [Managing user quotas in Kerio Control](#) (page 81).
- » Set a language for users. For more information, refer to [Customizing the language used in Kerio Control interfaces](#) (page 312).
- » Set web content rules. For more information, refer to [Blocking web object elements for particular users](#) (page 84).
- » Control user access to the Internet from local networks. See [Monitoring active connections](#) and [Monitoring active hosts](#).

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 local administration accounts. For more information, refer to [Adding a local administration account](#) (page 79).

To create a local account:

1. In the administration interface, go to the **Users** section.
2. Click **Add**.
3. In the **Add User** dialog box, type the username and password (other items are optional). Usernames are not case-sensitive.
4. Click **OK**

NOTE

If you plan to create numerous local accounts with similar settings, use a template. For more information, refer to [Using templates](#) (page 80).

Adding a local administration account

The advantage of local administrator accounts is that such users can authenticate locally even if the network communication fails.

1. In the administration interface, go to the **Users** section.
2. Click **Add**.
3. In the **Add User** dialog box, type the username and password and confirm password. Usernames are not case-sensitive.
4. In the **Authentication** drop-down list, select **Internal user database**.
5. In the **Domain template** part, select **This user has a separate configuration**.

The screenshot shows the 'Add User' dialog box with the following details:

- Username:** local admin
- Full name:** Blake Johnston
- Description:** local administrator
- Email address:** bjohnston@company.com
- Authentication:** Internal user database
- Password:** [masked]
- Confirm password:** [masked]
- ☒ **Account is enabled**
- Domain template:**
 - ☐ This user's configuration is defined by the domain template
 - ☒ This user has a separate configuration

Now, you can edit the **Rights** tab independently of other users.

6. Go to the **Rights** tab.
7. Select **Full access to administration**.
8. (Optional) Select also additional rights **Users can unlock HTTP content rule**, **Users can control dial-up lines**, and **Users can connect using VPN**. For more information, refer to [Setting access rights in Kerio Control](#) (page 81).
9. Click **OK**

From now on, the local administrator account works and the user can access Kerio Control Administration with it.

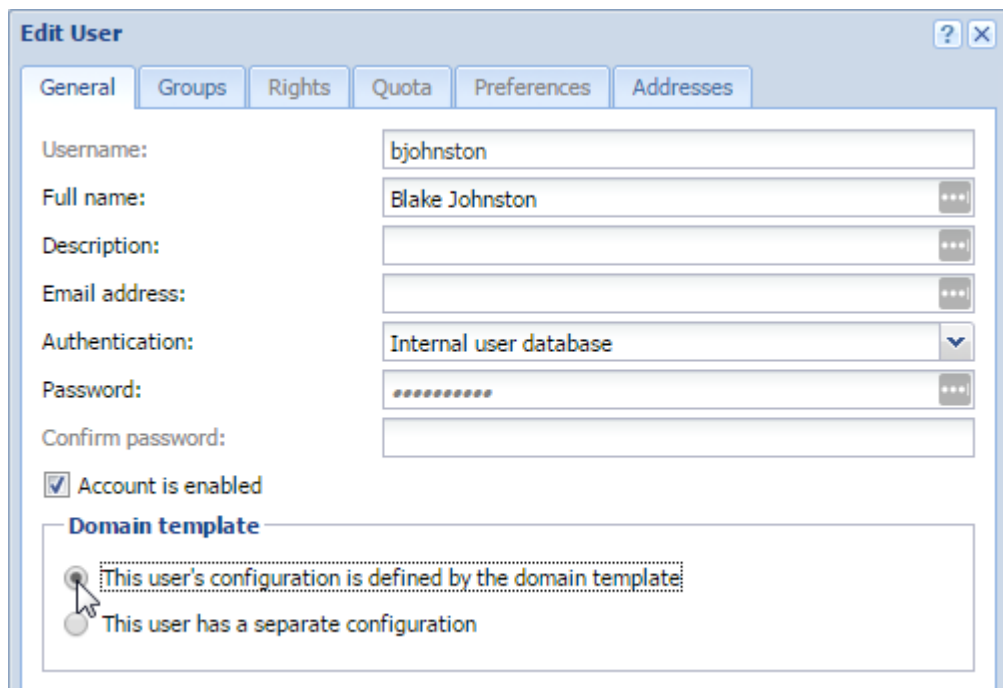
Adding accounts from a directory service

For more information, refer to [Connecting Kerio Control to directory service](#) (page 89).

Using templates

Each domain in Kerio Control includes a template. If you are planning to create numerous accounts with similar settings, or change one item for all users in the domain, use the template for it:

1. In the administration interface, go to **Users** section.
2. Click **Template**.
3. In the template, specify all the settings which are common for all users from this domain.
4. Save the settings.
5. In the **Users** section, click **Add/Edit** a user.
6. In the **Add/Edit user** dialog, select **This user's configuration is defined by the domain template**.



The screenshot shows the 'Edit User' dialog box with the following details:

- General** tab is active.
- Username:** bjohnston
- Full name:** Blake Johnston
- Description:** (empty)
- Email address:** (empty)
- Authentication:** Internal user database
- Password:** (masked with dots)
- Confirm password:** (empty)
- ☒ **Account is enabled**
- Domain template** section:
 - ☒ This user's configuration is defined by the domain template
 - ☐ This user has a separate configuration

Deleting user accounts

User accounts can be suspended temporarily or deleted permanently.

You cannot disable/delete the following users:

- » You, if you are logged in Kerio Control Administration.
- » 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.

3.5.2 Setting access rights in Kerio Control

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:

Option	Description
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 more information, refer to [Configuring statistics and reports](#) (page 313).

3.5.3 Managing user quotas in Kerio Control

Kerio Control enables you to configure a limit for the volume of data a user can transfer, as well what happens when that quota is exceeded.

Configuring user quotas

1. In the administration interface, go to **Accounting and Monitoring > Data Gathering**.
2. Select **Gather internet usage statistics**. For more information, refer to [Settings for statistics, reports and quota](#) (page 314).
3. In the administration interface, go to **Users**.

4. Select a user (or a template) and click **Edit**. For more information, refer to [Managing user accounts in Kerio Control](#) (page 78).
5. Select one or more of the **Enable ... limit** options: **daily**, **weekly** and/or **monthly**. Use the **Direction** drop-down list to select which transfer direction to control:
 - **download** = incoming data
 - **upload** = outgoing data
 - **all traffic** = both incoming and outgoing data
6. Type the quotas and select the units from the drop-down list.
7. Choose one of the **Exceeded quota action** options.
 - **Block any further traffic** allows the user to continue using the open connections. However, no new connections can be established, such as connecting to another server or downloading a file through FTP. If users exceed their quotas and Kerio Control blocks the traffic, the restriction is applied until the end of the quota period (day, week, month). To cancel these restrictions, temporarily disable the limit, raise its value, turn off the block, or delete the data volume counter of the user in the **Status > User Statistics** section.
 - **Don't block further traffic** limits the Internet connection speed for the user. Traffic is not blocked but the user may notice that the connection is slower. For more information, refer to [Configuring a bandwidth rule for exceeded quotas](#) (page 83).
8. (Optional) Select **Notify user by email when quota is exceeded** and specify an email address in the **Edit User** dialog box. For more information, refer to [Configuring the SMTP server](#) (page 318).

NOTE

The Kerio Control administrator can also be notified when any user quota is exceeded. For more information, refer to [Using alert messages](#) (page 204).

Edit User

General Groups Rights **Quota** Preferences Addresses

Transfer quota

☒ Enable daily limit
 Direction: all traffic
 Quota: 1 GB

☒ Enable weekly limit
 Direction: all traffic
 Quota: 5 GB

☒ Enable monthly limit
 Direction: all traffic
 Quota: 20 GB

Quota exceed action

☐ Block any further traffic
☒ Don't block further traffic
 (Limit bandwidth according to the Bandwidth Management settings only.)
☒ Notify user by email when quota is exceeded

OK Cancel

Configuring a bandwidth rule for exceeded quotas

If you don't want to block the traffic when users exceed their quotas, you can limit bandwidth for all users who exceed a certain limit. In the following example, the bandwidth is limited to 2 Mbit/s.

1. In the administration interface, go to **Bandwidth management and QoS**.
2. Click **Add**.
3. Type a name for the rule (for example, `Exceeded quota`).
4. Double-click in the **Traffic** column.
5. In the **Traffic** dialog box, select **Exceeded Quota**.
6. Click **OK**.
7. Double-click in the **Download** column.
8. In the **Download Bandwidth Policy** dialog box, select **Do not exceed** and type the value (for example, 2 Mbit/s).
9. Double-click in the **Upload** column.
10. In the **Upload Bandwidth Policy** dialog box, select **Do not exceed** and type the value (for example, 2 Mbit/s).

From now on, all users who exceed their quotas have their Internet connection slowed down to 2 Mbit/s.

NOTE

If you want to release the limit for a particular user, delete the data volume counter of the user in the **Status > User Statistics** section. For more information, refer to [Monitoring user statistics](#) (page 119).

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						
<input type="checkbox"/>	Name	Traffic	Download	Upload	Interface	Valid Time
<input checked="" type="checkbox"/>	Exceeded quota	Exceeded quota	Limit: 2 Mbit/s	Limit: 2 Mbit/s	All	Working hours
<input checked="" type="checkbox"/>	Limit music	Music	Limit: 400 KB/s	No limit	All	
<input checked="" type="checkbox"/>	SIP VoIP	SIP VoIP	Reserve: 240 KB/s	Reserve: 240 KB/s	All	Working hours
	Other traffic	Any	No limit	No limit	All	

3.5.4 Blocking web object elements for particular users

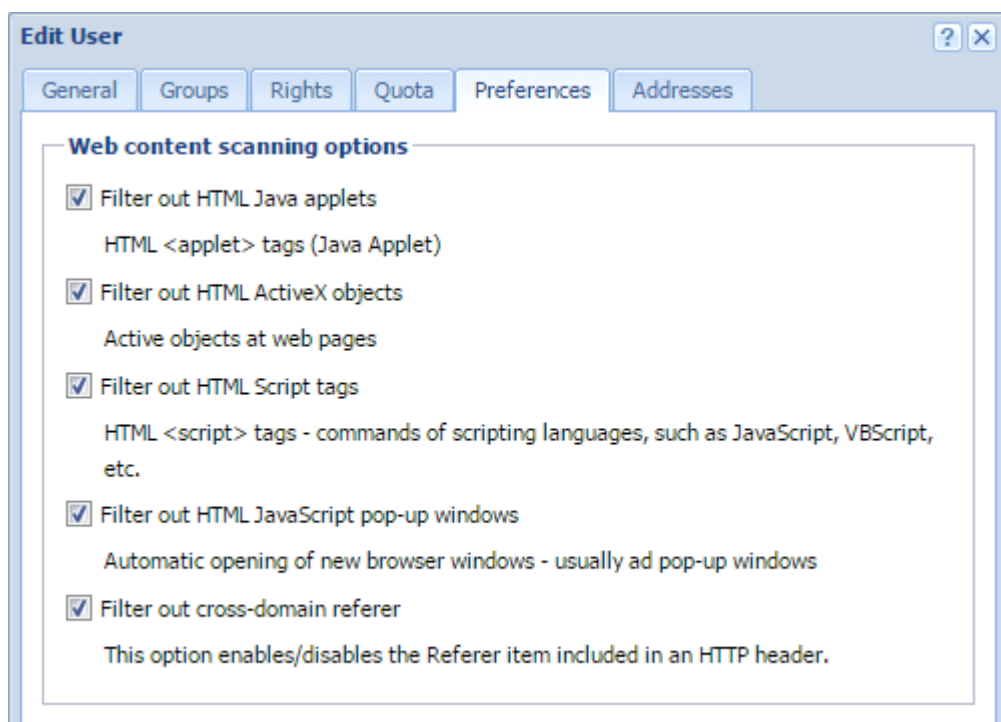
You can define a filter to protect Kerio Control users from potentially harmful objects in web pages.

By default, Kerio Control does not block any web elements.

Blocking web elements

1. In the administration interface, go to the **Users** section.
2. Double-click a user's name, or click **Template** to apply the filter to all users in the domain.
3. In the **Edit User** or **Edit User Template** dialog box, go to **Preferences**.
4. Select the type of objects you want to block:
 - **Filter out HTML Java applets** blocks applets in Java.
 - **Filter out HTML ActiveX objects** allows or blocks object and embedded HTML tags. Active objects at web pages.
 - **Filter out HTML Script tags** blocks the executive code in JavaScript, VBScript, and so on.
 - **Filter out HTML JavaScript pop-up windows** allows or blocks the window.open() method in JavaScript. Automatic opening of new browser windows, usually pop-up windows with advertisements.
 - **Filter out cross-domain referrer** enables or disables the HTTP referrer item in headers.
5. Click **OK**

If users complain about functionality of important web pages after the filter is enabled, deselect some options on the **Preferences** tab.



3.5.5 Configuring automatic user login

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).

Configuring automatic login on MAC address

IMPORTANT

You can use automatic login on MAC address if Kerio Control is able to see the MAC address of the host. For more information, refer to [Why Kerio Control does not know the MAC address](#) (page 86).

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.

IMPORTANT

If you use Kerio Control MAC Filter, check the **Also permit MAC addresses used in DHCP reservations or automatic user login** option. For more information, refer to [Filtering MAC addresses](#) (page 222).

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. For more information, refer to [Configuring IP address groups](#) (page 332).
5. 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.

3.5.6 Creating user groups in Kerio Control

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. For more information, refer to [Connecting Kerio Control to directory service](#) (page 89).

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.

NOTE

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. For more information, refer to [Setting access rights in Kerio Control](#) (page 81).

8. Save the settings.

3.5.7 Authenticating users to Kerio Control

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. For more information, refer to [Authenticating users to Kerio Control](#) (page 87).
- » Automatic login — Kerio Control permanently associates a user to a device based on the device IP or MAC address. For more information, refer to [Configuring automatic user login](#) (page 85).
- » RADIUS — For more information, refer to [Using RADIUS server in Kerio Control](#) (page 327).
- » VPN — See [Configuring Kerio VPN server](#) and [Configuring IPsec VPN](#) 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.

See also:

Requiring user authentication when accessing web pages

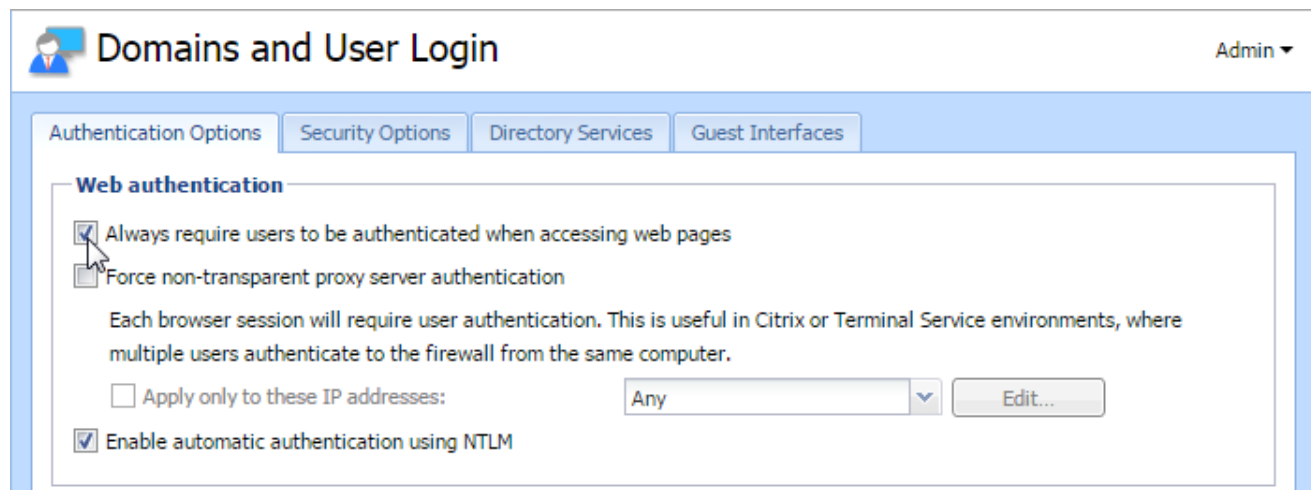
Kerio Control can require users to authenticate before they can browse the web. When this options is enabled and an unauthenticated user opens a non-secure website in their browser, Kerio Control redirects the user to the firewall login page. After the user successfully logs in, Kerio Control permits the user to access the originally requested page.

NOTE

Before enabling this option, make sure you configured the Kerio Control web interface. For more information, refer to [Configuring the Kerio Control web interface](#) (page 308).

To require user authentication:

1. In the administration interface, go to **Domains and User Login > Authentication Options**.



Screenshot 17: Configuring user authentication

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. For more information, refer to [Automatic user authentication using NTLM](#) (page 92).
4. Click **Apply**.

Requiring user authentication when multiple users use one 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.

NOTE

This option is useful only in Citrix or Terminal Service environments, where multiple users authenticate to the firewall from the same 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.

For more information, refer to [Configuring proxy server](#) (page 294).

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 whenever 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, refer to [Using Remote Desktop IP Virtualization](#) (page 341).

User logout options

Kerio Control is configured by default to logout authenticated users automatically after 120 minutes of inactivity. You can disable or adjust this timeout.

To configure log out options:

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**.

To override the timeout and force user logout manually, you can use the **Active Hosts**. For more information, refer to [Monitoring active hosts](#) (page 110).

3.6 Directory services

This section provides information how to connect to Microsoft Active Directory and Apple Open Directory.

3.6.1 Connecting Kerio Control to directory service	89
3.6.2 Automatic user authentication using NTLM	92
3.6.3 How do I force users to log out of the firewall?	95
3.6.4 How to use a Windows Active Directory Group Policy Object (GPO) to logon and logout users automatically from Kerio Control	96
3.6.5 Optimizing the communication between Kerio Control and Active Directory	109

3.6.1 Connecting Kerio Control to directory service

Which directory services are supported

- » Microsoft Active Directory
- » Apple Open Directory

What is the connection used for

Advantages	Description
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.

Advantages	Description
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.

IMPORTANT

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 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.

NOTE

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.

WARNING

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.

3.6.2 Automatic user authentication using NTLM

Kerio Control supports automatic user authentication by the NTLM method (authentication from web browsers). Once they are authenticated for the domain, users do not need to type their usernames and passwords.

This article provides detailed conditions and configuration settings for correct functioning of NTLM.

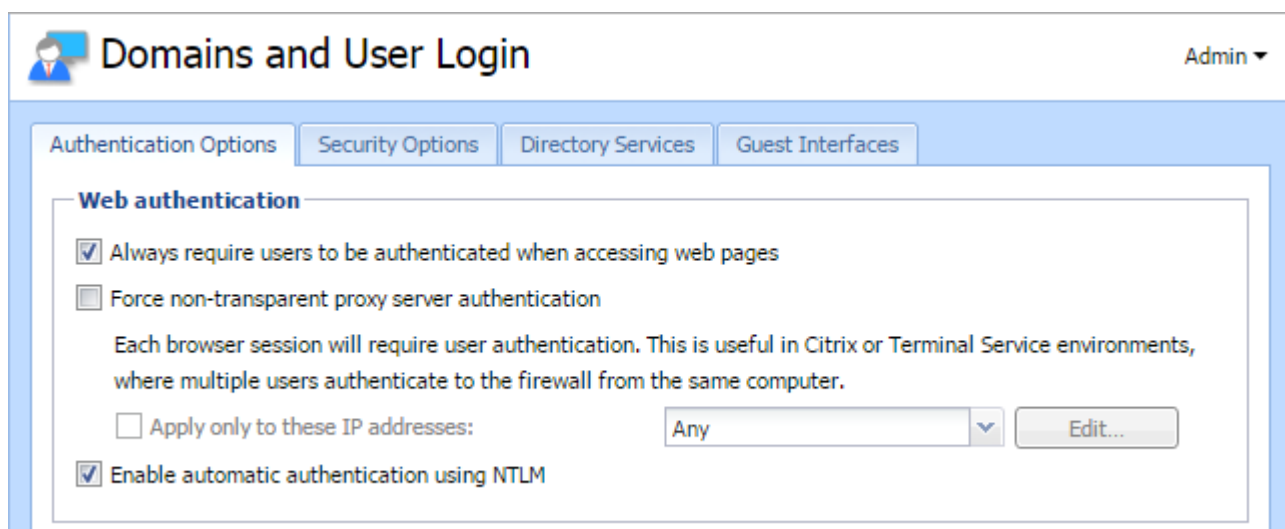
Prerequisites

- » Join Kerio Control to the Microsoft Active Directory domain with a valid DNS name as a Kerio Control server name. For more information, refer to [Connecting Kerio Control to directory service](#) (page 89).
- » Join client hosts to the domain.
- » Install a valid SSL certificate for the web interface and configure it correctly in Kerio Control. For more information, refer to [Configuring SSL certificates in Kerio Control](#) (page 343). SSL certificates can be configured and distributed using Group Policy Settings. For more information, refer to [Deploying Kerio Control certificate via Microsoft Active Directory](#) (page 347).
- » Configure browsers to trust the Kerio Control hostname, if necessary. See [Configuring web browsers](#) below.

Configuring NTLM in Kerio Control

For successful configuration, enable NTLM authentication and a DNS name in the Kerio Control settings:

1. In the administration interface, go to **Domains and User Login**.
2. (Optional) On the **Authentication Options** tab, select **Always require users to be authenticated when accessing web pages**.
3. Select **Enable automatic authentication using NTLM**.



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

4. Click **Apply**.

Kerio Control is now configured properly to use the NTLM authentication.

Next, you need to configure browsers on client hosts.

Configuring web browsers

For proper functioning of NTLM, only use browsers that support this method:

- » [Microsoft Internet Explorer](#)
- » [Mozilla Firefox](#)
- » [Google Chrome](#)

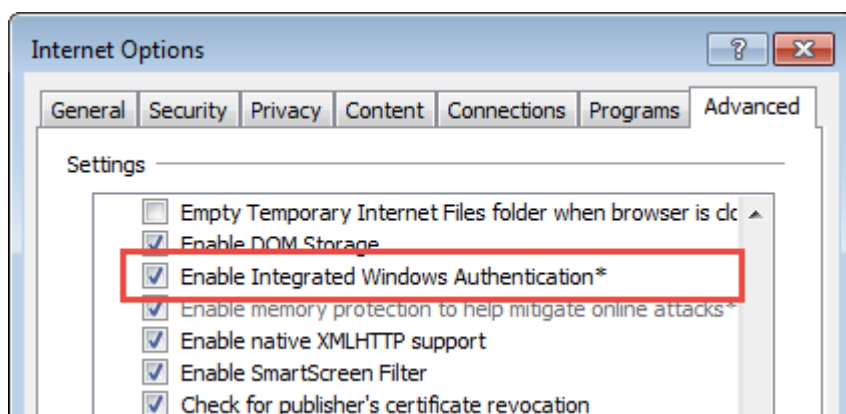
NOTE

Edge does not support NTLM yet.

Setting Microsoft Internet Explorer

In Internet Explorer, you must enable integrated Windows authentication and add the Kerio Control server name to trusted servers in its security settings:

1. Open Internet Explorer
2. Click **Tools > Internet Options**.
3. Click the **Advanced** tab.



4. Select **Enable integrated Windows Authentication**.

5. Restart Internet Explorer.

Internet Explorer is now properly configured and NTLM authentication should work. Users do not have to authenticate with Kerio Control credentials.

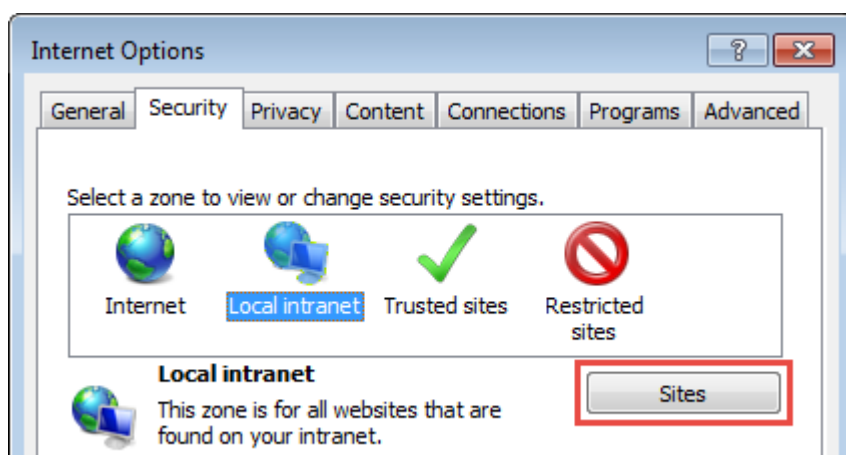
If NTLM does not work, you may have problems with Kerio Control server name. In this case:

1. Go to **Tools > Internet Options**.

2. Click the **Security** tab

3. Select **Local intranet**.

4. Click **Sites**



5. In the **Local Intranet** dialog box, click **Advanced**.

6. Add the Kerio Control server name to the list of trusted servers. For increased security, type the server name in this format: `https://server.company.com`

Setting Mozilla Firefox

1. Open Mozilla Firefox.

2. Type `about:config` in the address bar.

3. Use the filter to search for `network.automatic-ntlm-auth.trusted-uris`

4. Double-click the item.

5. In the dialog box, add the Kerio Control server name. For increased security, type the server name in this format:
`https://server.company.com`

Mozilla Firefox is now properly configured and NTLM authentication works. Users do not need to authenticate with Kerio Control credentials.

Setting Google Chrome

Chrome uses [Internet Explorer's security configuration](#), so one way to configure Chrome's settings is to configure Internet Explorer. Google Chrome adopts the same settings, so NTLM authentication will work.

Troubleshooting

When

3.6.3 How do I force users to log out of the firewall?

Kerio Control can use NTLM authentication to allow users to automatically log onto the firewall when they are logged onto an ActiveDirectory or NT domain. However if the user does not manually logout from **Kerio Control**, his session remains active until the session timeout period expires. This timeout period is set to 2 hours by default.

If user logs out from Windows, he does not logout from **Kerio Control**. Once again the timeout is 2 hours. The consequence of this is that a user license will continue to be in use. If you have more users than licenses this may prevent a new user from being able to connect through **Kerio Control**. Furthermore the next user on that computer will appear to be the previous user. This may lead to incorrect logging of user activity.

It is possible to create a logout link and store it as a bookmark in order to logout from Kerio Control, or alternatively it is possible to use some logout script to logout user automatically.

`https://firewall_ip:4081/internal/logout`

`http://firewall_ip:4080/internal/logout`

Details

It is possible to automate the **Kerio Control** logout process by using a script which is called during the logout from Windows. This method will be useable for any number of users who are sharing the same machine.

In Active Directory, the Directory Controller will allow to run a script during the user's logout. This script will perform the logout automatically for the user by calling a utility which makes the necessary HTTP request to the Kerio Control's webserver for logout.

The script needs to open this URL: **`http://firewall_ip:4080/internal/logout`**

Here is an example script which uses the freely available wget program.

1. Download [wget for Microsoft Windows](#).
2. Copy the wget.exe file to each client computers.
3. Using Active Directory, set a Group Policy to apply the wget.exe file during the logout procedure.
 - a. Open Group policy settings: **Active Directory Users and Groups > [your domain] > Properties > Group Policy** tab, and select the "Open" button.
 - b. In the Group Policy Management console, select your domain from the left-hand menu bar. Then select "Default Domain Policy" under the "Linked Group Policy Objects" tab. Right click and select "Edit".
 - c. In the Group Policy Object editor, select **User Configuration > Windows Settings > Scripts** (Logon/Logoff).

d. Create a new Logoff script by double clicking on "Logoff" and pressing the "Add" button.

e. Use the following settings for your script - Program name: `c:\wget.exe`

- Program parameters (http): `-q http://firewall_ip:4080/internal/logout`
- Program parameters for https logout (server certificate is trusted): `-q https://firewall_ip:4081/internal/logout`
- Program parameters for https logout (server certificate is not trusted, eg. in case of self signed certificate): `--no-check-certificate -q https://firewall_ip:4081/internal/logout`

f. Save the script and exit all folders

g. **Under "Default Domain Policy" > Properties, you must enable "Enforced".**

4. Test the logoff script by logging a user out of windows and then checking **Kerio Control** to confirm the user has logged out. You can see this under **Status > Hosts/Users**.

3.6.4 How to use a Windows Active Directory Group Policy Object (GPO) to logon and logout users automatically from Kerio Control

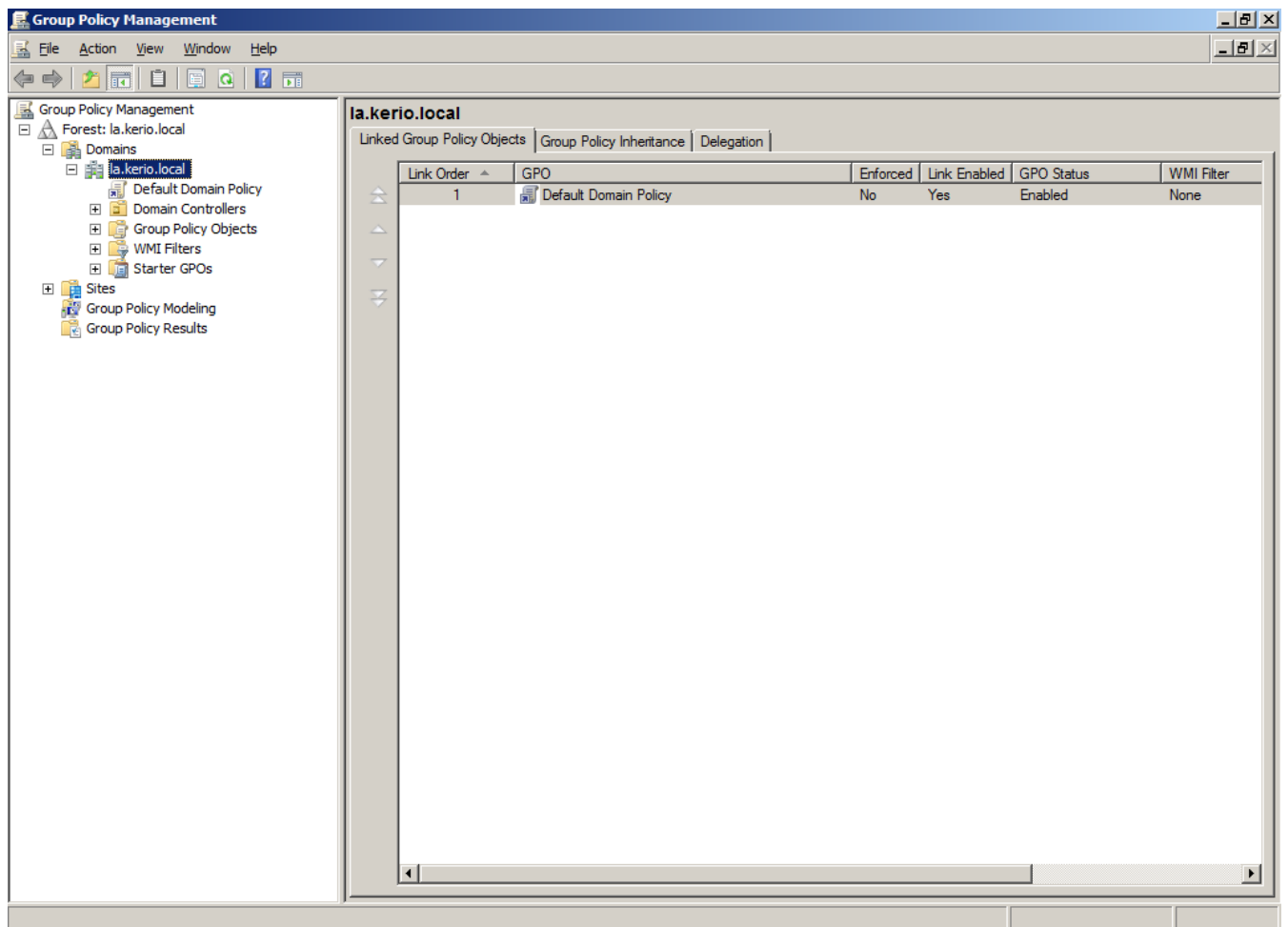
Kerio Control can use NTLM authentication to allow users to automatically log onto the firewall when they are logged onto a Windows Active Directory. It is possible to create a Group Policy object containing scripts to logon and logout users from Kerio Control.

NOTE

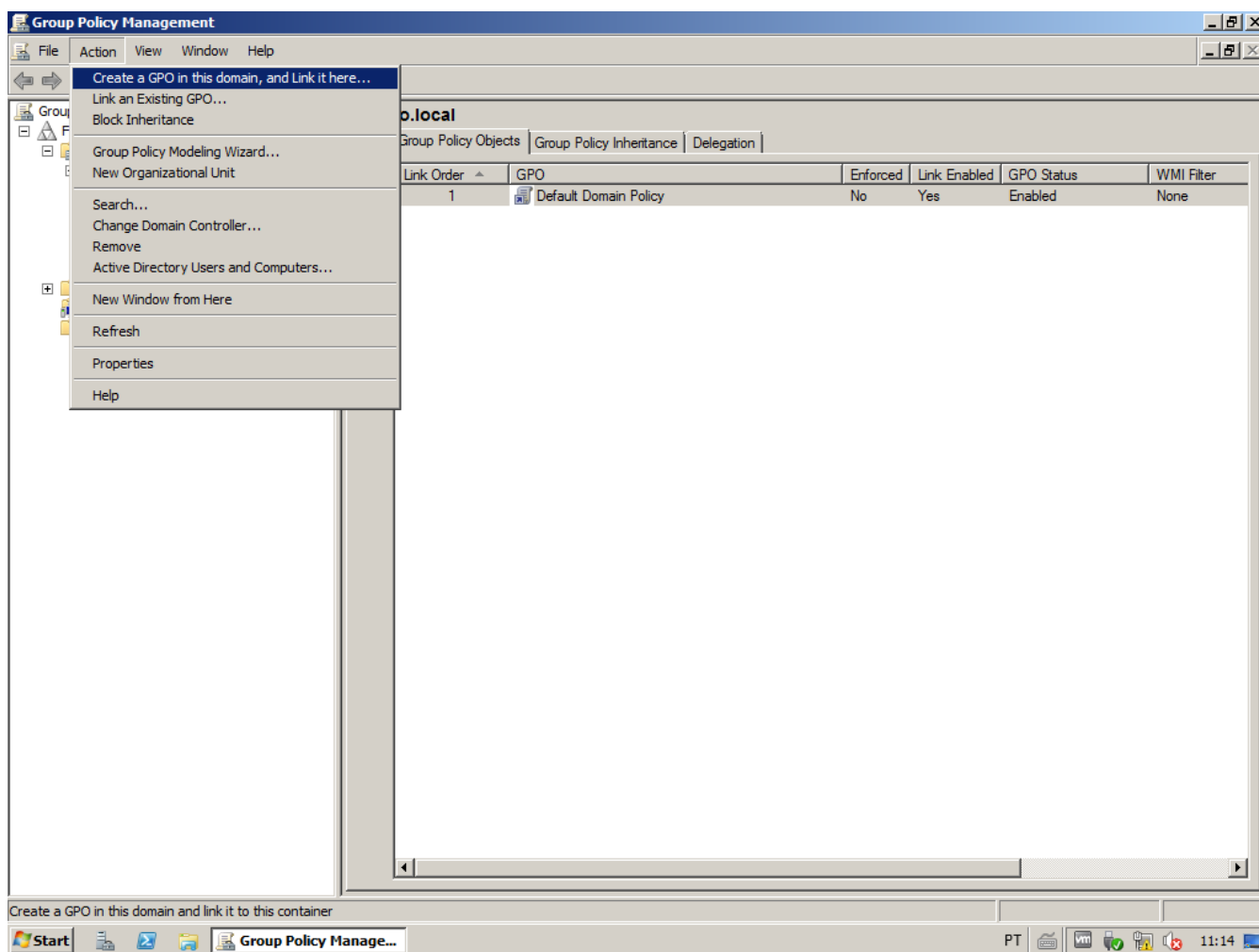
This article was based on Active Directory running on Microsoft Windows Server 2008 Domain Controller.

Details

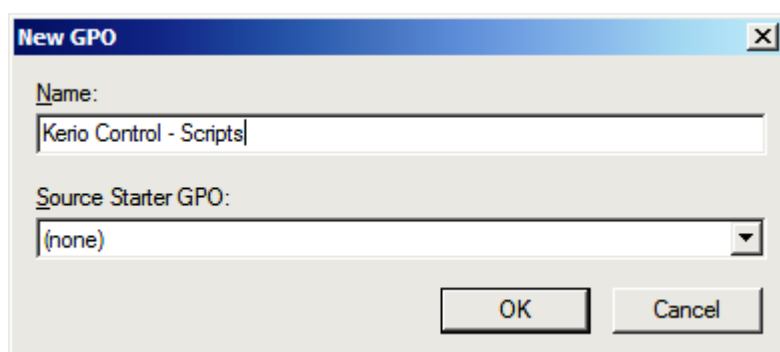
1. Connect to your domain controller. Go to **Start > Administrative Tools > Group Policy Management**.



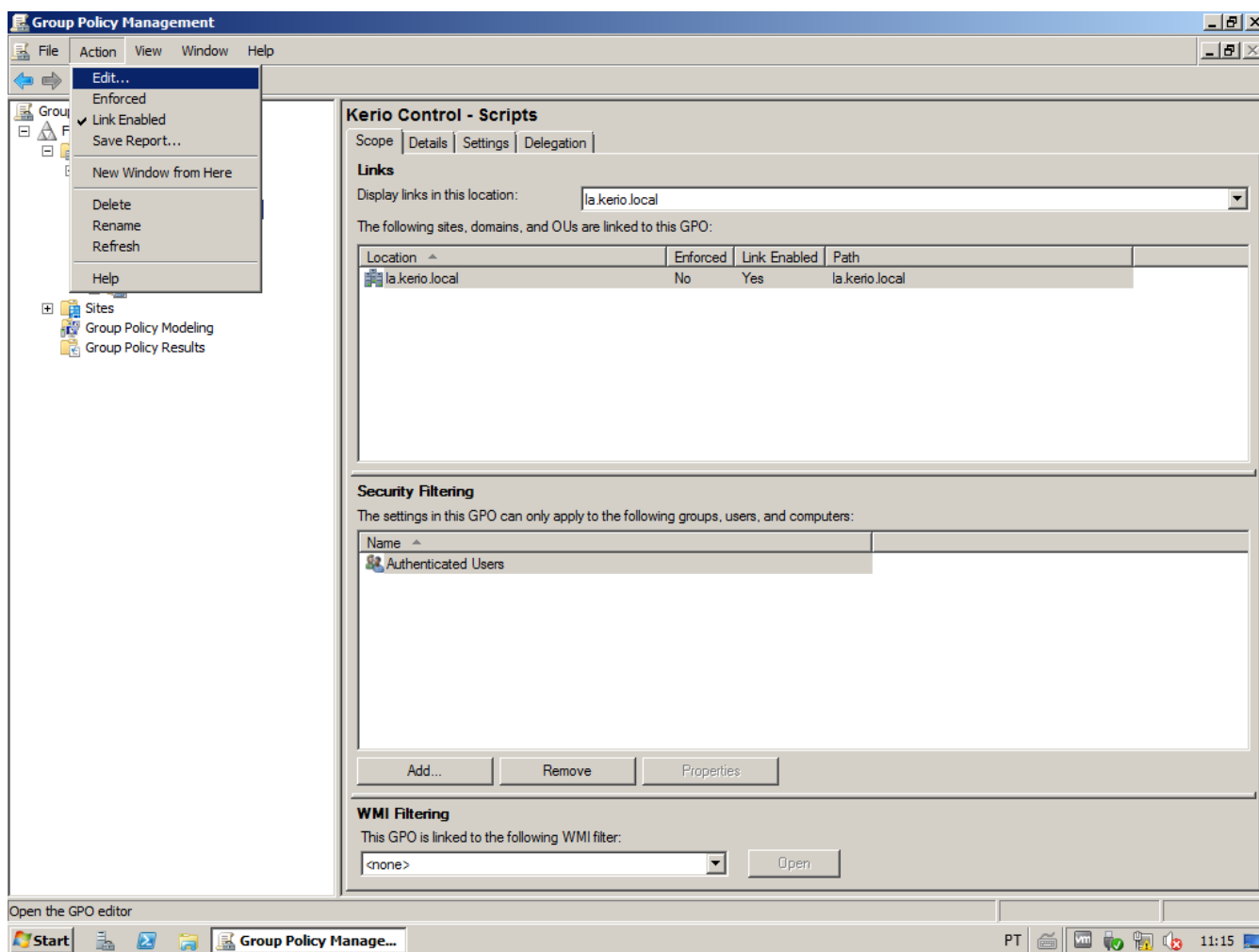
2. Select the domain. After that, select **Action > Create a GPO in this domain, and Link it here....**



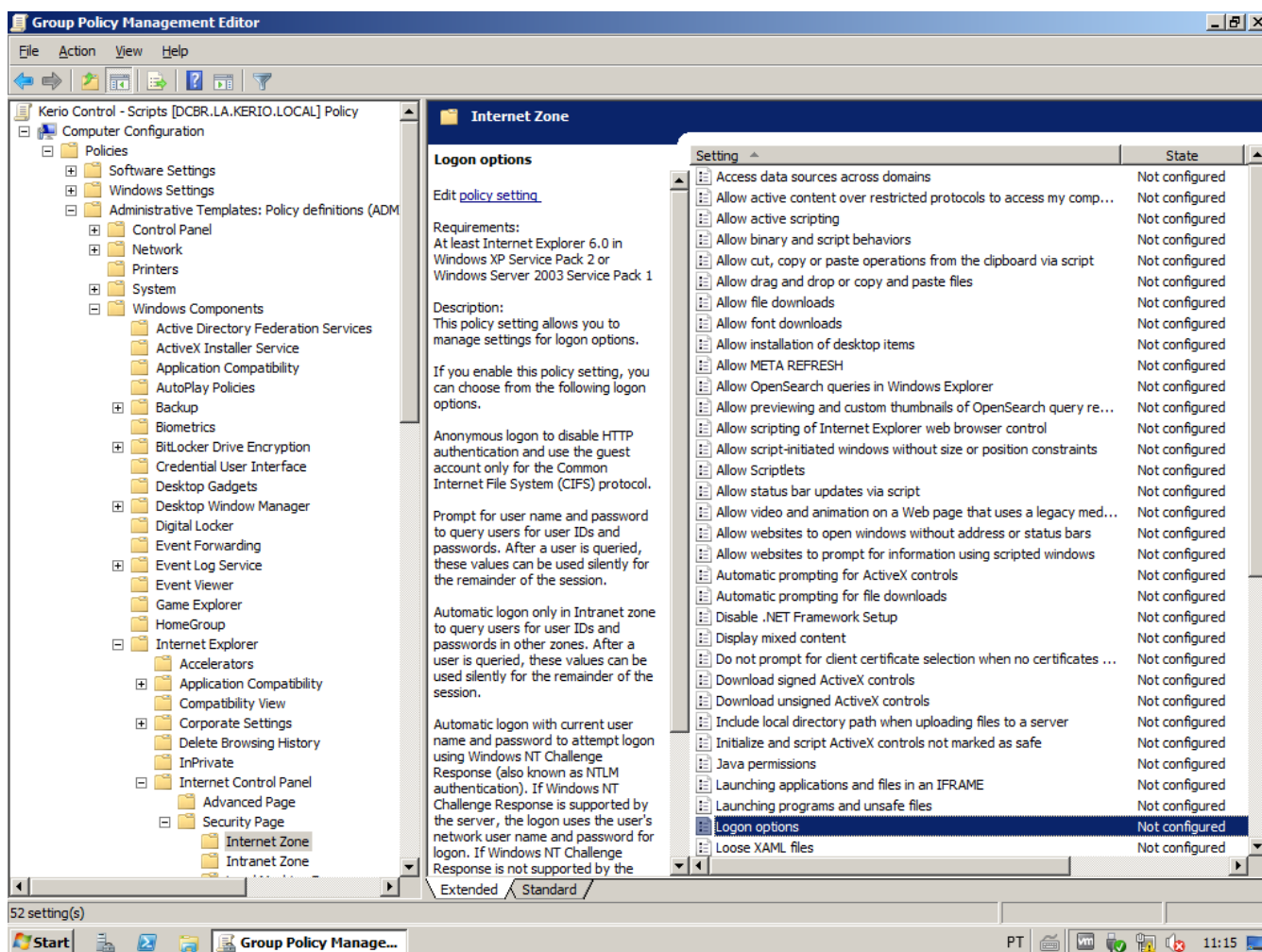
3. Give an appropriated name to this object.



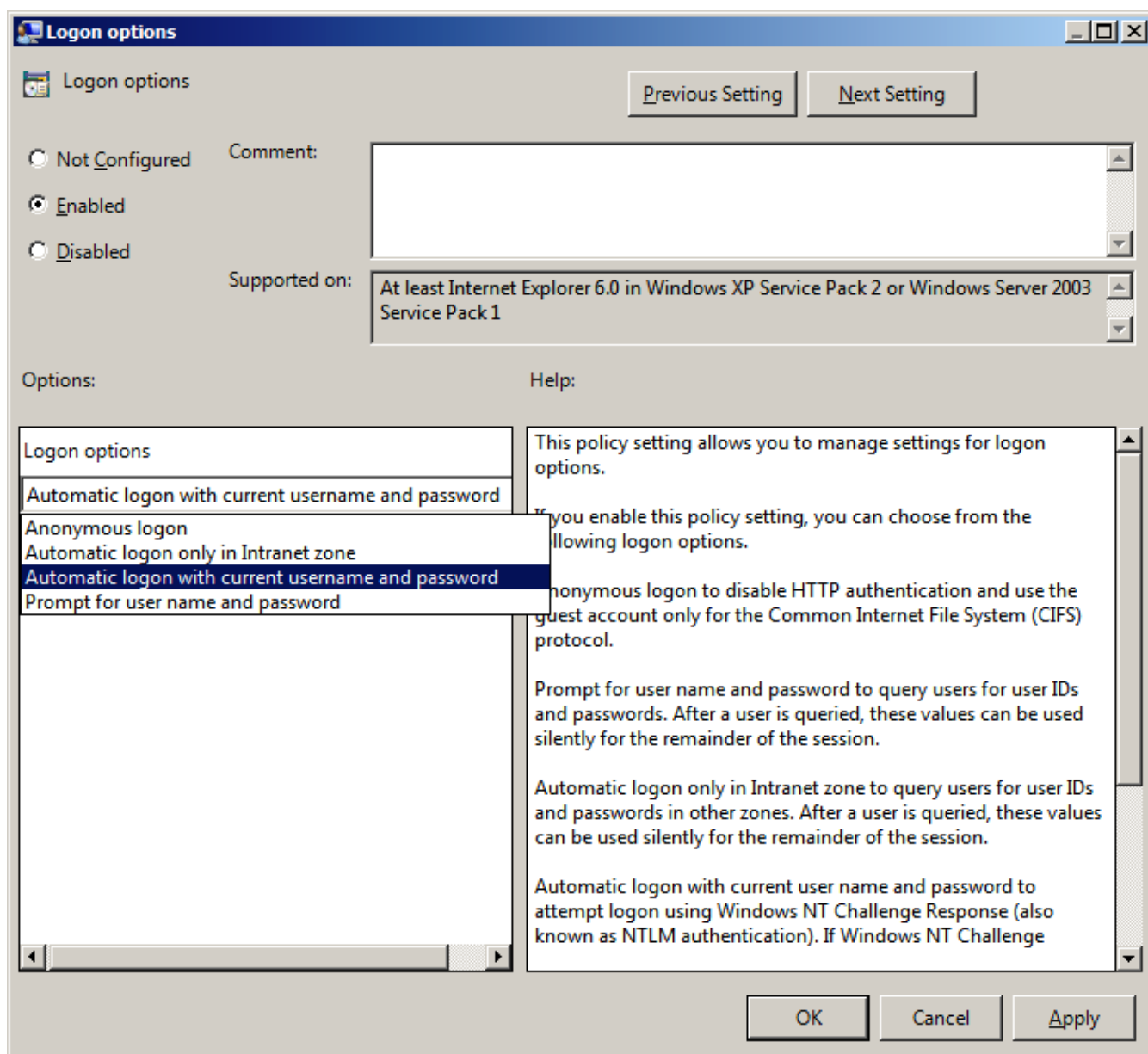
4. After creating the object, select **Action > Edit...**



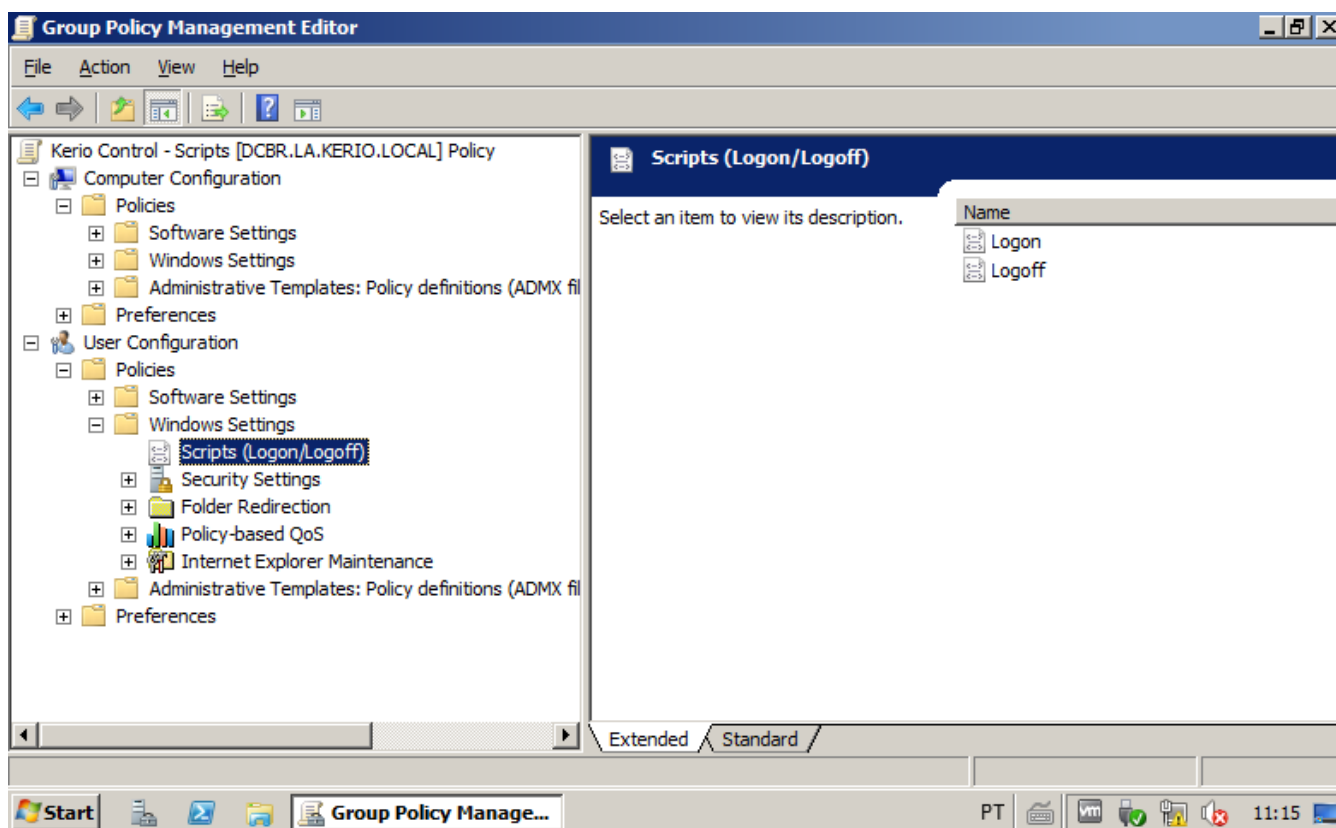
5. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone**.



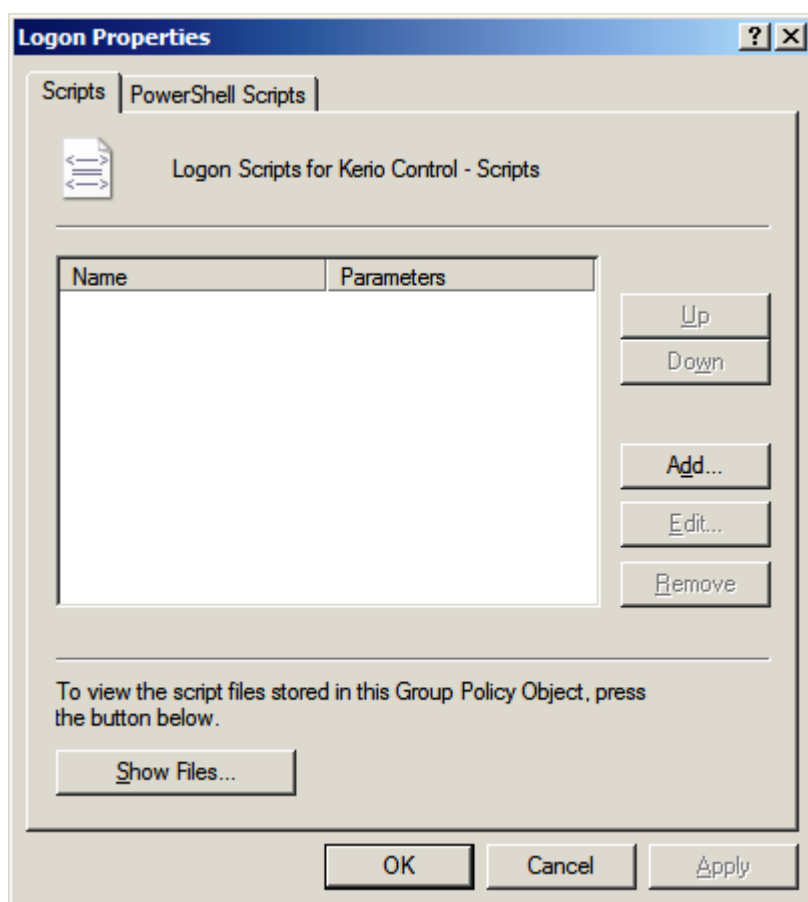
6. Select **Logon options** with a double-click, enable it and change the option to **Automatic logon with current user-name and password**. Apply these changes.



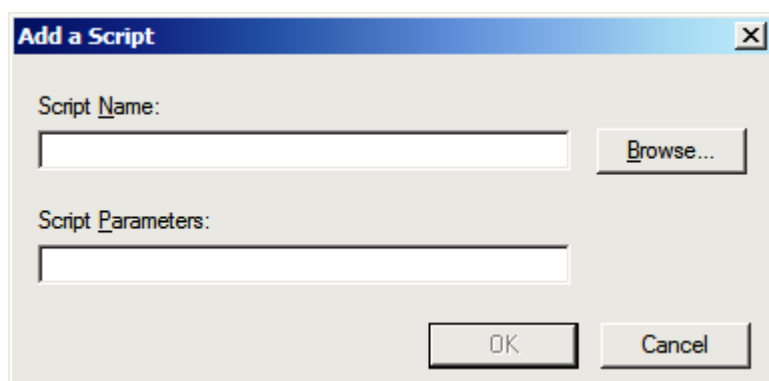
7. Select **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.



8. Select **Logon** with a double-click and click **Add...**



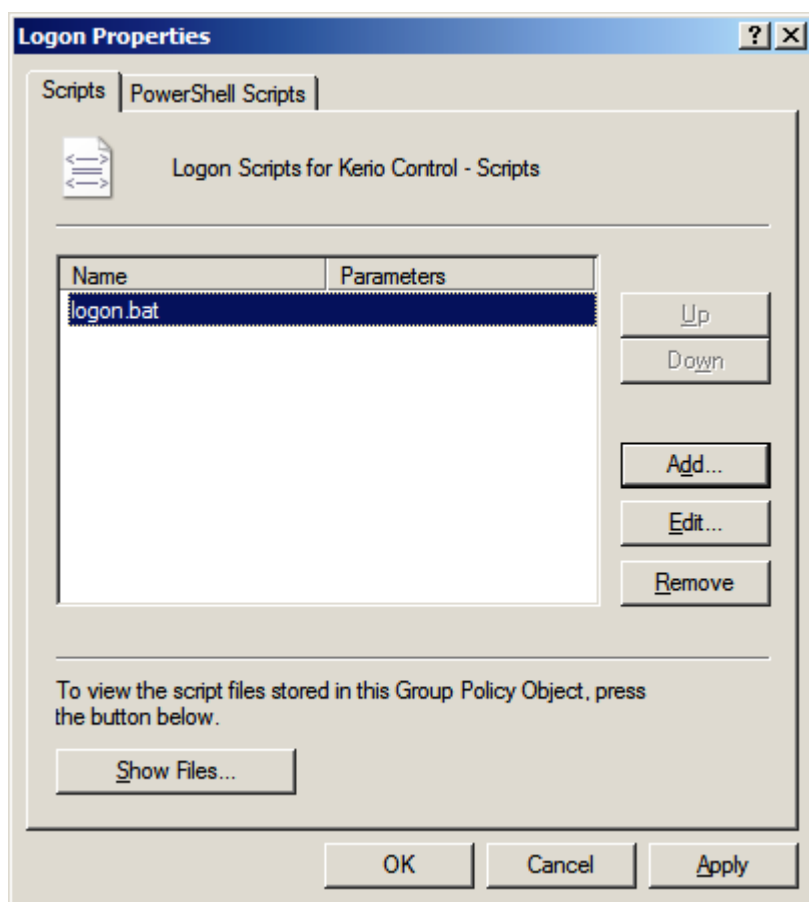
9. Click **Browse...**



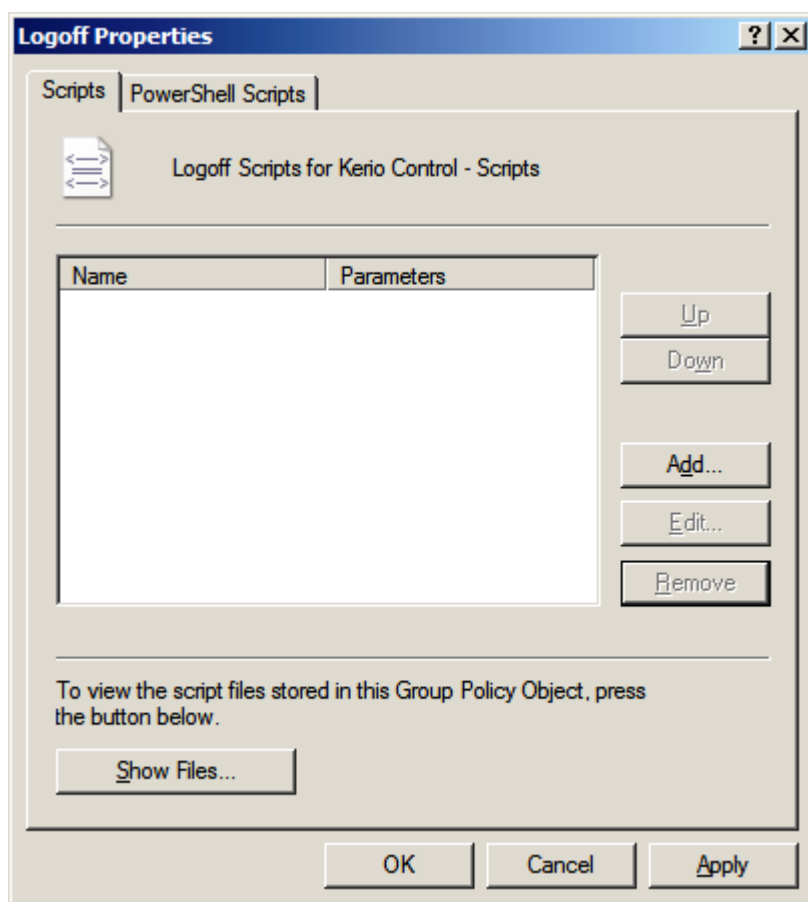
10. Create two files: **logon.vbs** and **logon.bat**. Use the sample code in the table below for reference, changing the logon script path:

File	Code
logon.vbs	<pre>Dim oIE Set oIE = CreateObject("InternetExplorer.Application") oIE.Visible = False oIE.Fullscreen = False oIE.Toolbar = True oIE.Statusbar = True oIE.Navigate("http://www.google.com/") WScript.Sleep(30000) oIE.quit</pre>
logon.bat	<pre>cscript //nologo \\domain\systool\..\logon.vbs</pre>

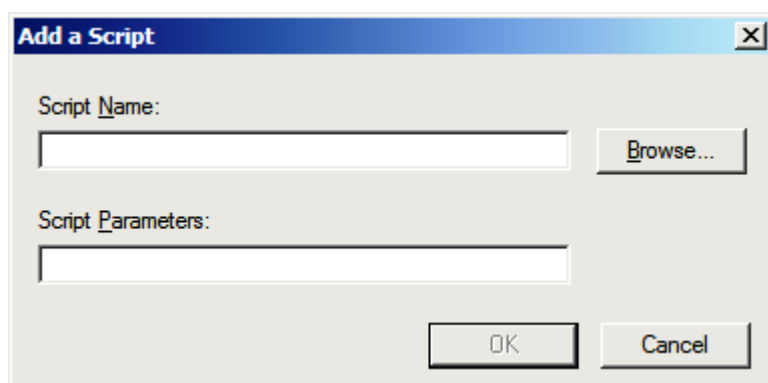
11. Select **logon.bat** with a double-click and click **OK**



12. Select **Logoff** with a double-click and click **Add...**



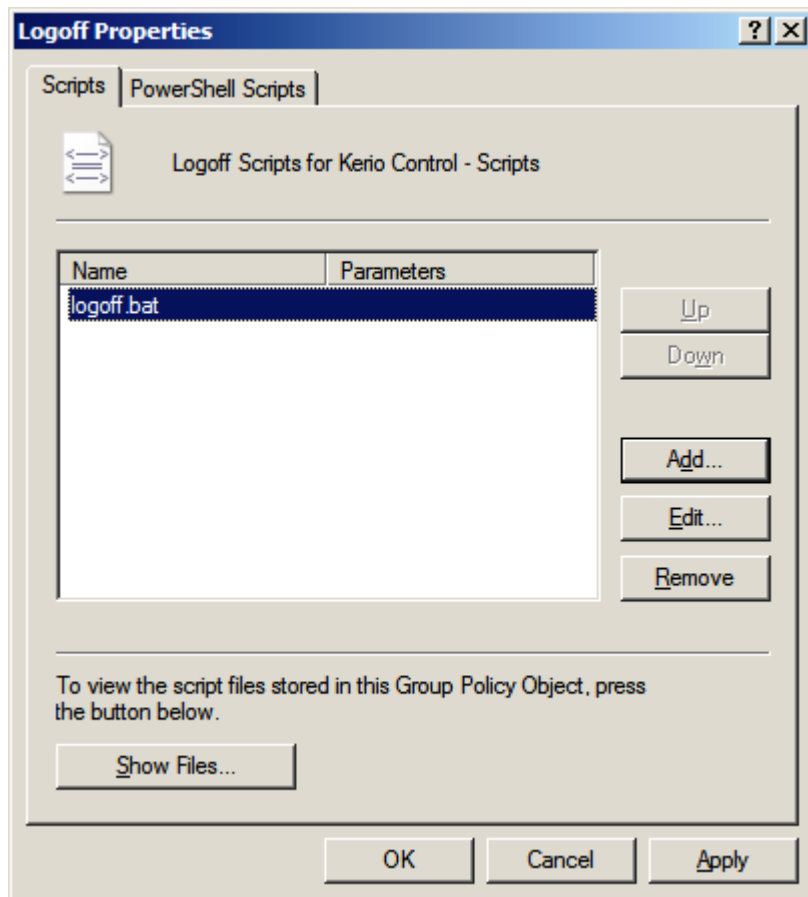
13. Click **Browse...**



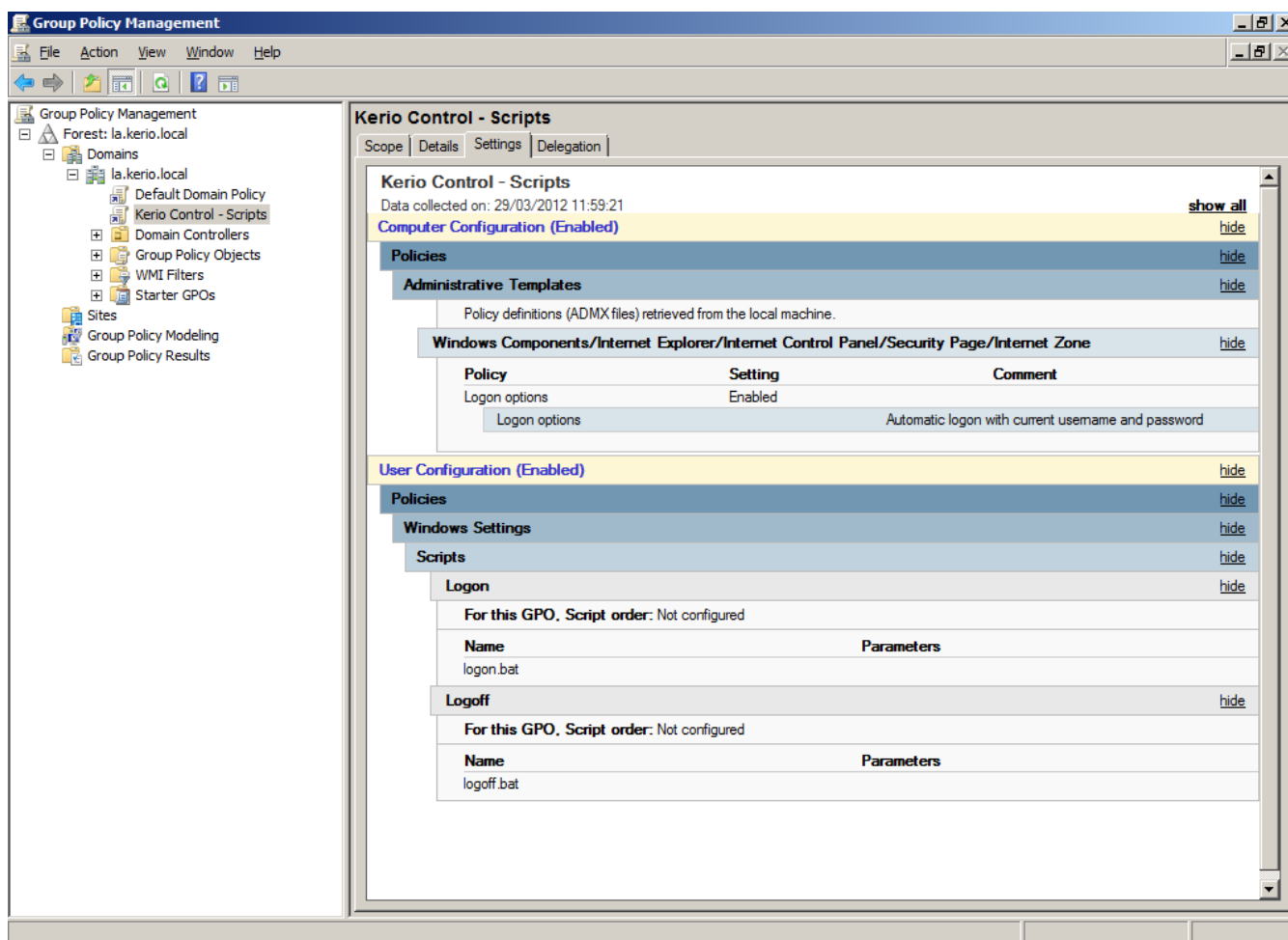
14. Create two files: **logoff.vbs** and **logoff.bat**. Use the sample code in the table below for reference, changing the logoff script path:

File	Code
logoff.vbs	<pre>Dim oIE Set oIE = CreateObject("InternetExplorer.Application") oIE.Visible = False oIE.Fullscreen = False oIE.Toolbar = True oIE.Statusbar = True oIE.Navigate("http://<Kerio Control Server IP address>:4081/internal/logout") WScript.Sleep(30000) oIE.quit</pre>
logoff.bat	<pre>cscript //nologo \\domain\sysvol\.. \logout.vbs</pre>

15. Select **logoff.bat** with a double-click and click **OK**



16. Double-check GPO settings and close **Group Policy Management**.

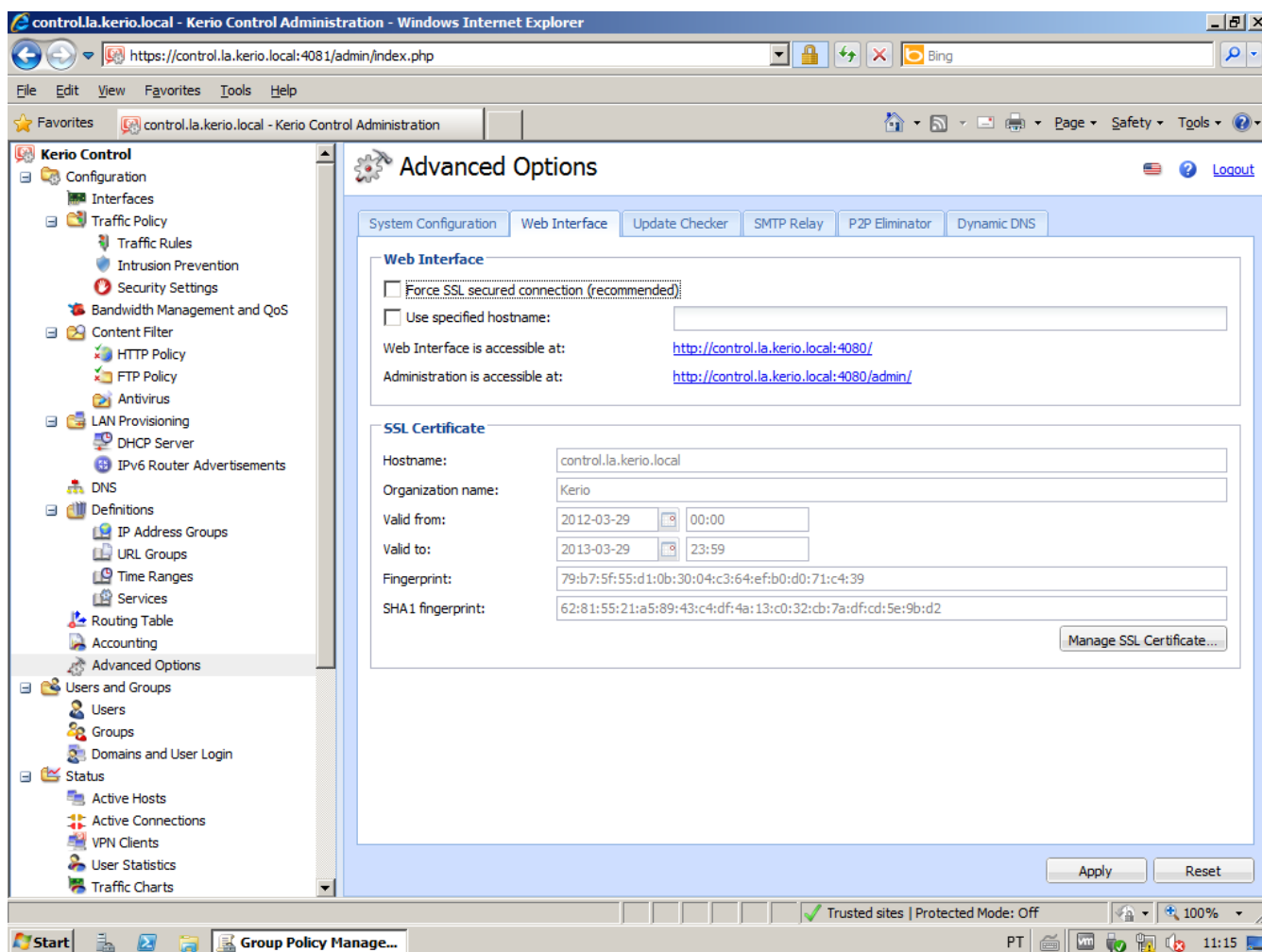


17. Open **Kerio Control Web Administration Interface**. Go to **Advanced Options** and disable **Force SSL secured connection (recommended)**. Apply this change.

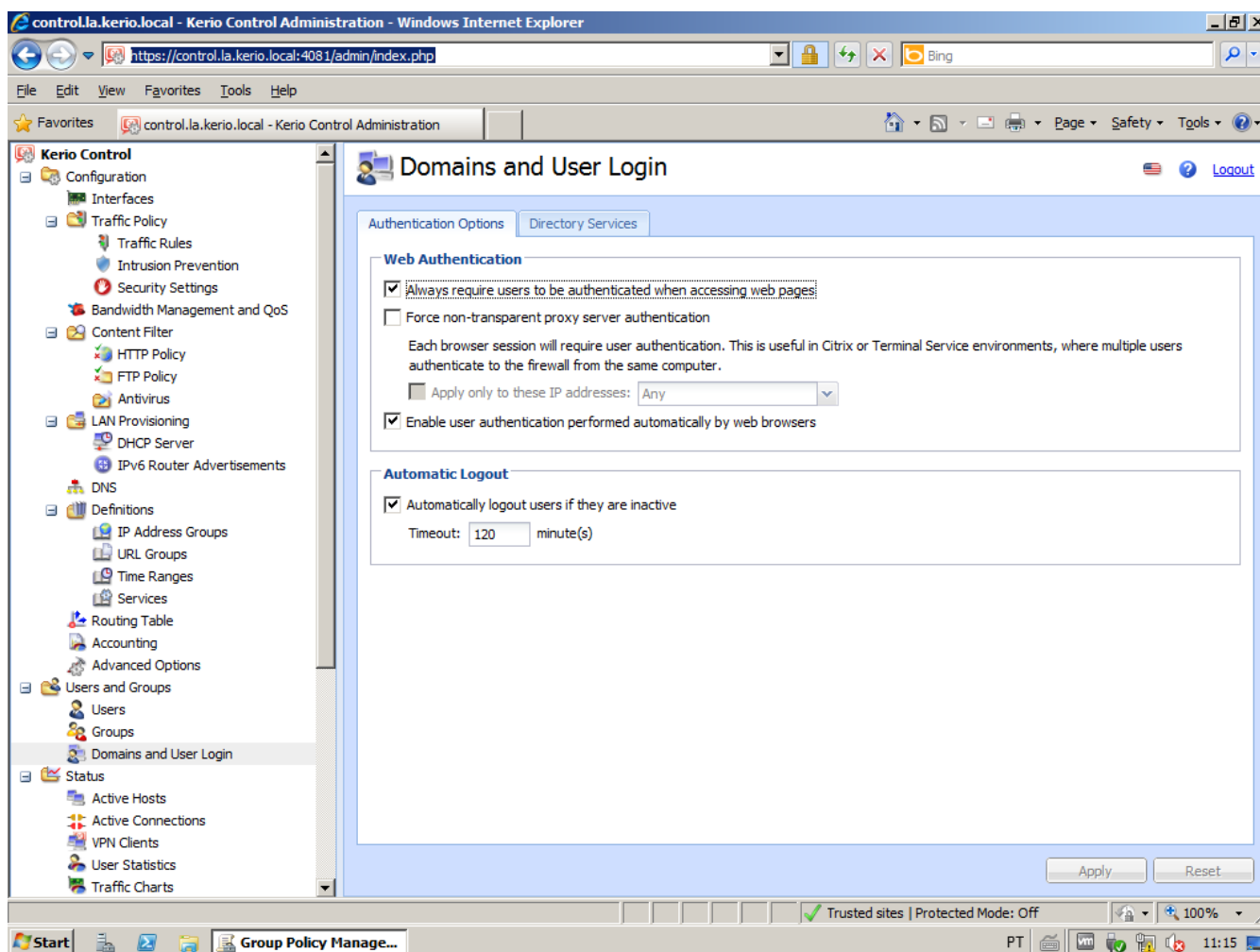
IMPORTANT DISCLAIMER:

Disabling this option will ignore the browser message: website's security certificate contains invalid information and it will allow Kerio Control authentication using NTLM authentication even the SSL certificate is not trusted on local machine (eg. in case of self signed SSL certificate). At the same time, this can be a security risk because users send their credentials to Kerio Control server using a plain-text format over unencrypted channel.

For correct encrypted communication it is required to have trusted signed SSL certificate for the URL of the Kerio Control web interface.



18. Go to **Users and Groups > Domains and User Login** and enable **Always require users to be authenticated when accessing web pages** and **Enable user authentication performed automatically by web browsers**. Apply these changes.



3.6.5 Optimizing the communication between Kerio Control and Active Directory

If you have a large or territory-distributed Active Directory, you can edit variables in the Kerio Control configuration files to speed up communication between Kerio Control and Active Directory.

Customizing the search suffix

You can define a specific search suffix for:

- » Geographically distributed Active Directory schemes
- » Active Directory with more than 10000 objects

This definition reduces:

- » Loading time and number of displayed domain controller users/groups in the Kerio Control Administration
- » Traffic between Kerio Control and hosts in the domain controller.

To customize the search suffix for searching in the LDAP database:

1. Log in to the operating system shell environment. For more information, refer to [Modifying parameters in Kerio Control configuration](#) (page 325).
2. Type `/opt/kerio/winroute/tinydbclient "update Domains set Cus-`

tomSearchSuffix='OU=Users,DC=example,DC=com' where Domain=example.com"

3. To apply the new configuration, type: `/etc/boxinit.d/60winroute restart`

Optimizing timeouts

You can optimize two timeouts:

» `ConnectionTimeout` determines for how long Kerio Control holds the connection open. The default value is 600 seconds. If Active Directory cuts the connection prematurely, you can decrease the number:

a. Log in to the operating system shell environment. For more information, refer to [Modifying parameters in Kerio Control configuration](#) (page 325).

b. Type `/opt/kerio/winroute/tinydbclient "update LdapAttributes set ConnectionTimeout=300 where Type=ADS"`

c. To apply the new configuration, type: `/etc/boxinit.d/60winroute restart`

» `OpTimeout` determines how long Kerio Control waits for a response when sending packets to the Active Directory controller. The default value is 5 seconds. To optimize the timeout, increase the number:

a. Log in to the operating system shell environment. For more information, refer to [Modifying parameters in Kerio Control configuration](#) (page 325).

b. Type `/opt/kerio/winroute/tinydbclient "update LdapAttributes set OpTimeout=60 where Type=ADS"`

c. To apply the new configuration, type: `/etc/boxinit.d/60winroute restart`

3.7 Monitoring

Kerio Control monitors network traffic, users, and system health.

3.7.1 Monitoring active hosts	110
3.7.2 Monitoring active connections	114
3.7.3 Monitoring System Health in Kerio Control	116
3.7.4 Monitoring traffic in Kerio Control	116
3.7.5 Monitoring user statistics	119
3.7.6 Monitoring VPN clients	121
3.7.7 SNMP monitoring	122

3.7.1 Monitoring active hosts

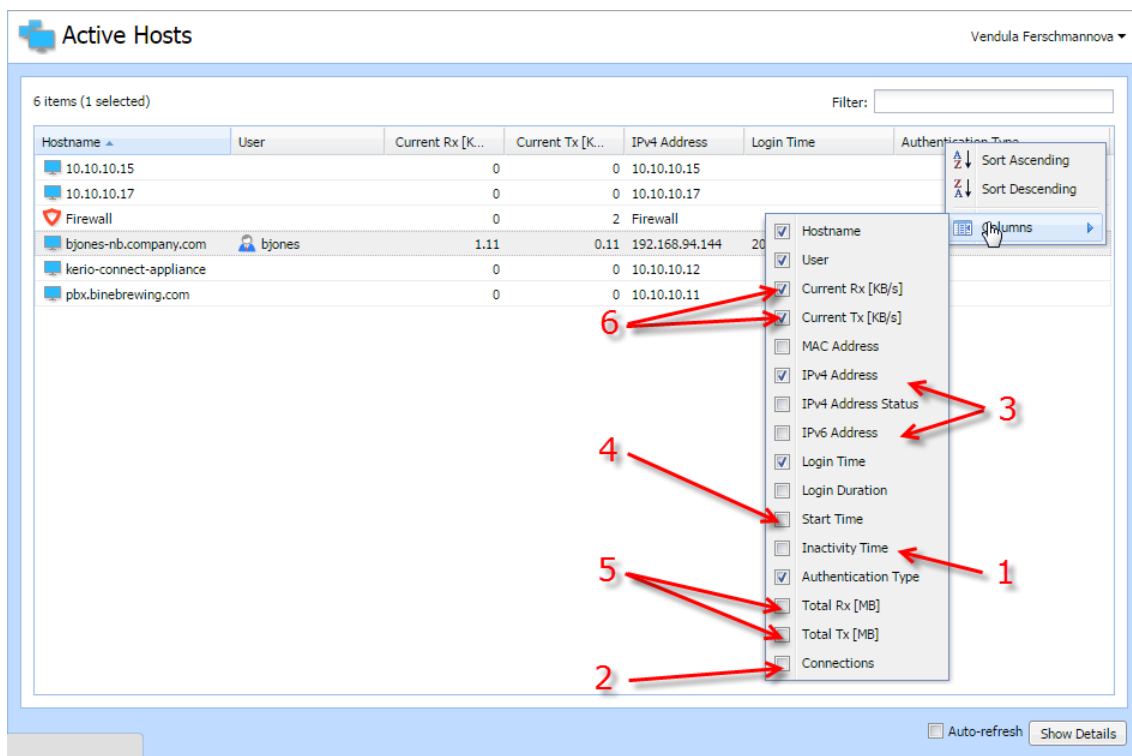
Kerio Control displays the hosts within the local network, or active users using Kerio Control for communication with the Internet in **Status > Active Hosts**.

Look at the upper window to view information on individual hosts, connected users, data size/speed, etc.

The section can, for example, display:

» The duration of the time with zero data traffic (1). You can set the firewall to logout users automatically after the inactivity exceeds the allowed time.

- » The total number of connections from/to the host (2). You can display the details in the **Connections** tab.
- » The IP address of the host from which is the user connecting (3)
- » The date and time of the active host' registration in the Kerio Control (4)
- » The total size of the data received and transmitted since the **Start time** (5)
- » The current traffic speed for incoming data (**Rx**) and outgoing data (**Tx**) (6)



Clicking the right mouse button in the **Active Hosts** window (or on the record selected) displays a context menu that provides the following options:

Option	Description
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 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. For more information, refer to Reserving an IP address (page 321). 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). For more information, refer to Configuring automatic user login (page 85).

Option	Description
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 . If you cannot see the details, click the **Show details** button:

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.

The screenshot shows a web interface with four tabs: General, Activity, Connections, and Histogram. The 'General' tab is selected. It contains two main sections: 'Host information' and 'Traffic information'. The 'Host information' section displays details for a user named 'bob' from 'bob.kerio.com', including login and inactivity times, and network addresses. The 'Traffic information' section shows data transfer statistics. At the bottom right, there are controls for 'Auto-refresh' and a 'Hide Details' button.

Host information

Option	Description
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

Option	Description
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.

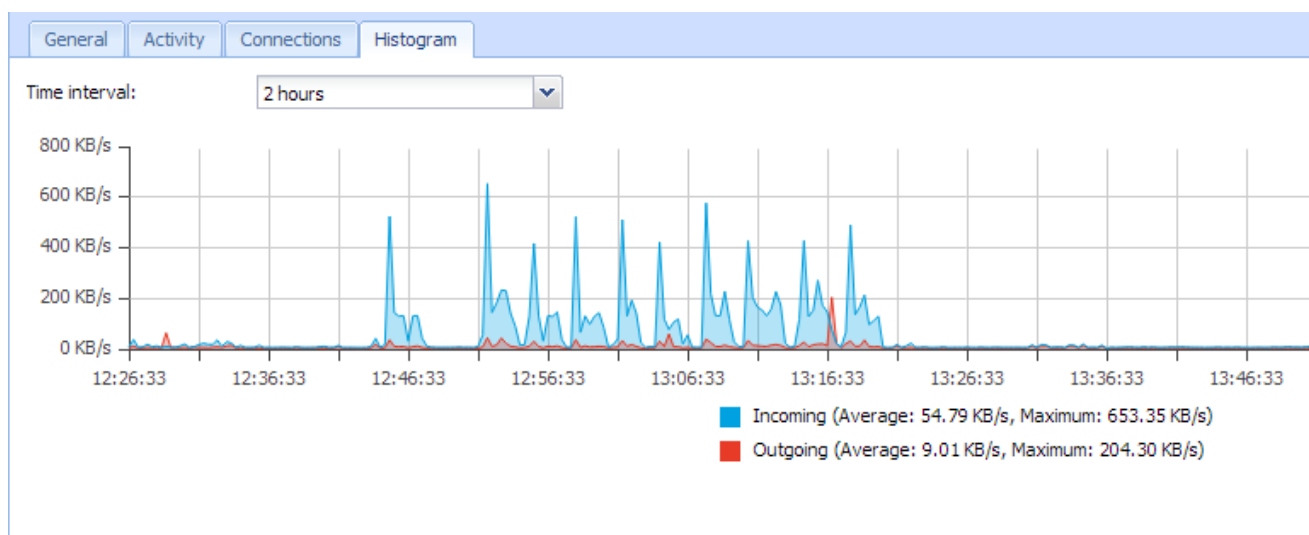
NOTE

To kill a connection between the LAN and the Internet immediately, right-click the connection and select **Kill connection**.

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.



3.7.2 Monitoring active connections

Kerio Control monitors the following network connections:

- » Client connections to the Internet through Kerio Control
- » Connections from the Kerio Control appliance
- » Connections from other hosts to services provided by Kerio Control
- » Connections performed by clients within the Internet that are mapped to services running in LAN
- » [Local connections which go through Kerio Control](#)

You can find monitoring of active connections in **Status > Active Connections**.

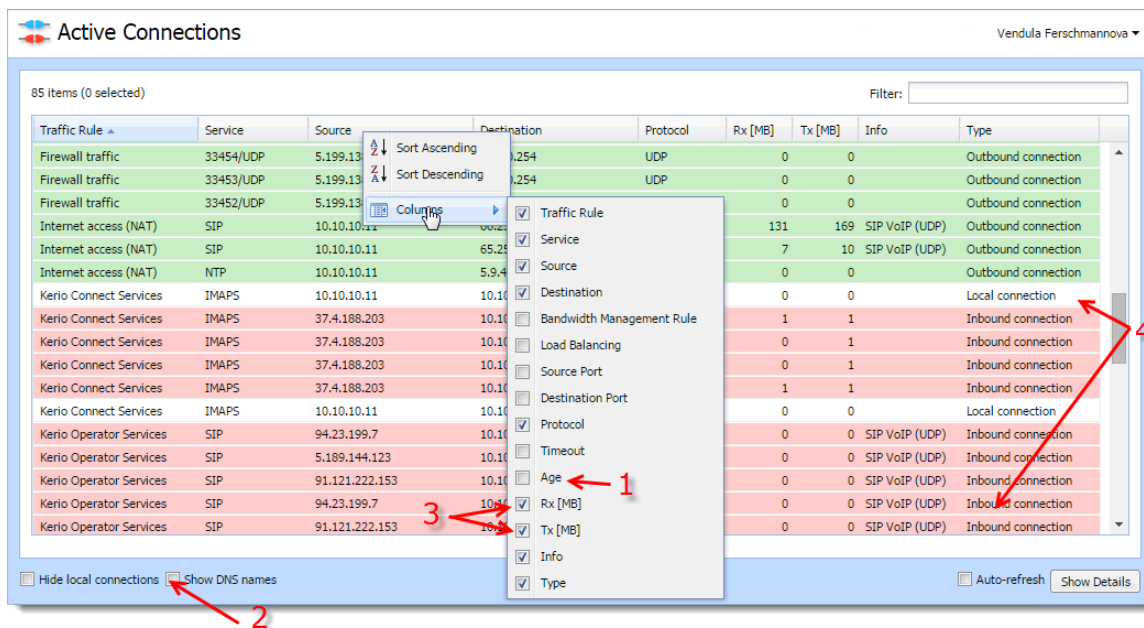
Each line of the **Active Connections** window represents one network connection. (Note that these are not user connections. Each client application can use multiple connections at any given moment).

The Active Connections section provides detailed information on a selected connection in the bottom window. If that information is not visible, click the **Show details** button. You can also copy IP addresses and hostnames in the bottom window.

The section can, for example, display:

- » The length of the connection (1)
- » Source and destination countries are classified by a GeoIP filter. Enable the filter for displaying countries. For more information, refer to [Blocking inappropriate or explicit content in search results](#) (page 273). (2)
- » The total size of data received (**Rx**) or transmitted (**Tx**) during the connection (3)

Kerio Control also distinguishes different types of connections by colours (4)



Screenshot 18: Active Connections

Killing connections

You can close any of the active connections. Right-click a connection and click **Kill Connection**.

Application visibility in Active Connections

If you want to see applications recognized by Application awareness in **Active Connections**, display the **Info** column. For more information, refer to [Application visibility in Active Connections](#) (page 265).

Local connections

A local connection is monitored if the communication goes through Kerio Control:

- » Trusted/Local Interfaces and Other Interfaces
- » IPsec and Kerio VPN Interfaces
- » Kerio Control interfaces



NOTE

Both directions are monitored.

Local connections between two computers from a single interface are not monitored by Kerio Control:



3.7.3 Monitoring System Health in Kerio Control

System Health shows current usage of CPU, RAM and the disk space of the computer or device where Kerio Control is running.

Option	Description
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 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).

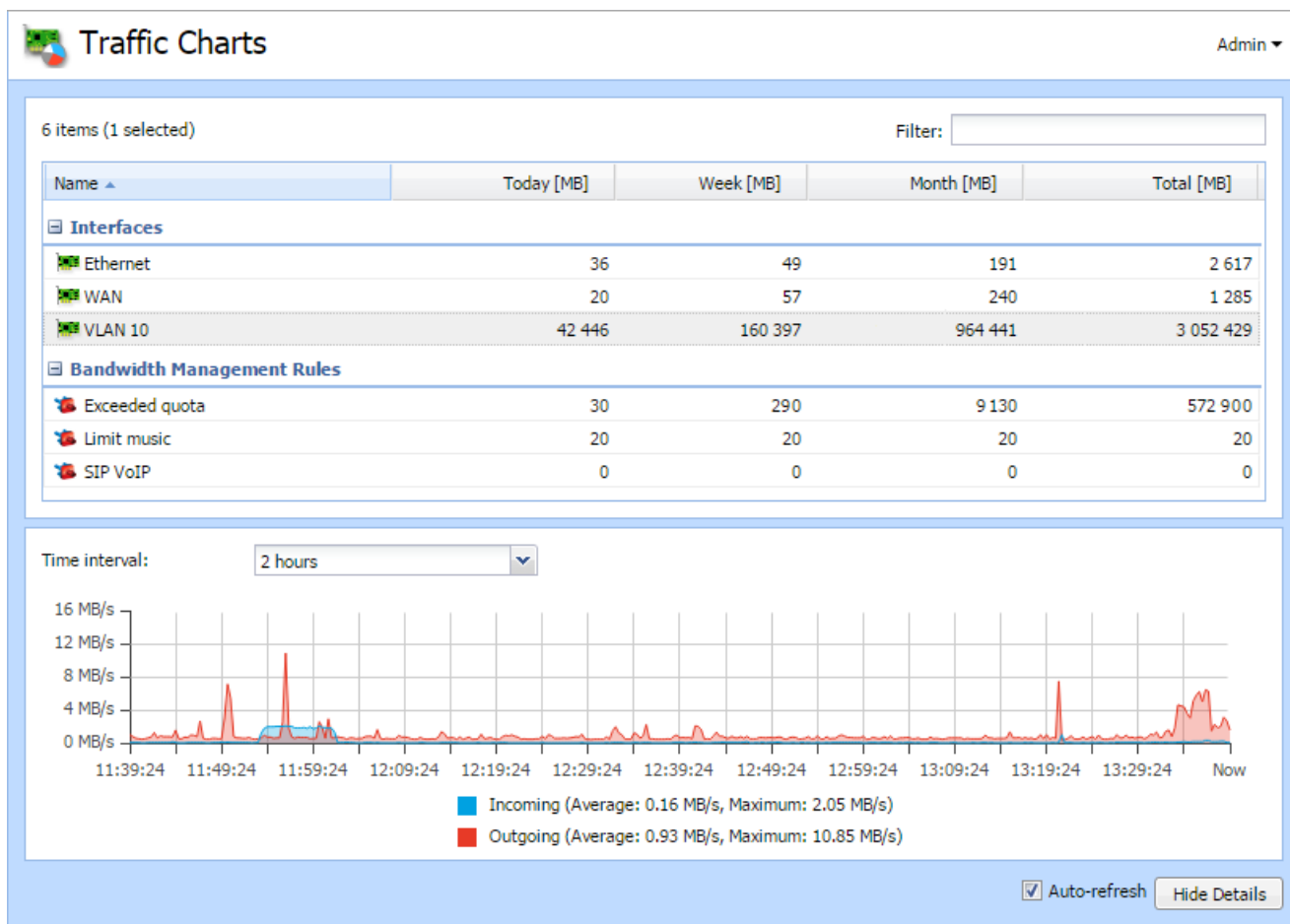
3.7.4 Monitoring traffic in Kerio Control

Kerio Control displays traffic charts in the **Status > Traffic Charts** section.

You can also view charts based on:

- » All Kerio Control interfaces, including VLANs and tunnels. Kerio Control displays charts as soon as data starts to flow through the interface.

- » Bandwidth rules.
- » Traffic rules.



Displaying charts for bandwidth rules

To display a chart for a bandwidth rule, you must first configure it in the particular rule:

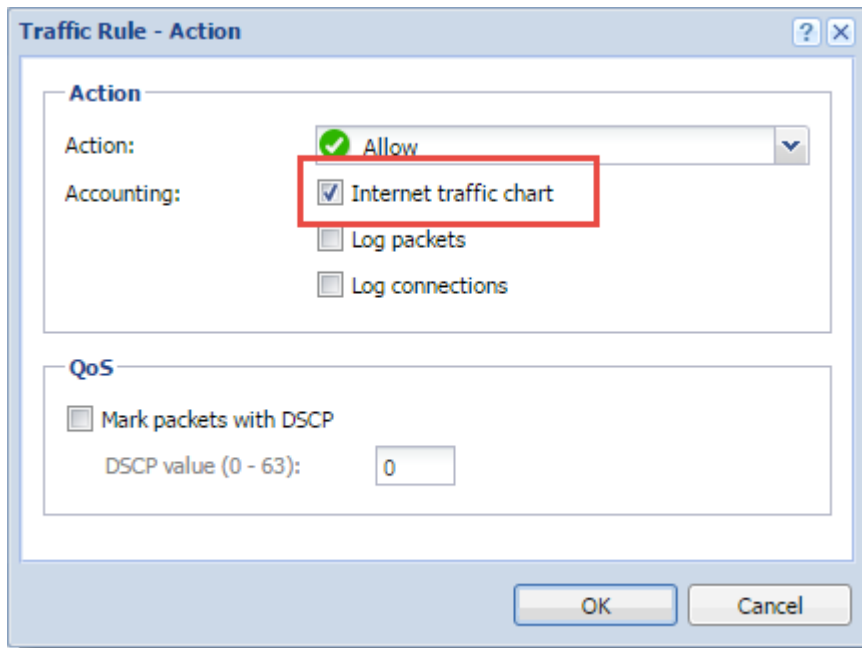
1. In the administration interface, go to **Bandwidth Management and QoS**.
2. In the **Bandwidth Management rules** table, in the **Chart** column, select the checkbox for a bandwidth rule you want to see in **Traffic Charts**. If you don't see the **Chart** column, click the table header and select **Columns > Chart**.
3. Click **Apply**.

From now on, you can view the chart for the selected bandwidth rules in the **Traffic Charts** section.

Displaying charts for traffic rules

To display a chart for a traffic rule, you must first configure it in the particular rule:

1. In the administration interface, go to **Traffic Rules**.
2. In the **Traffic Rules** table, double-click the **Action** column for a rule you want to see in **Traffic Charts**.
3. In the **Traffic Rule - Action** dialog box, select **Internet traffic chart**.



4. Click **OK**.

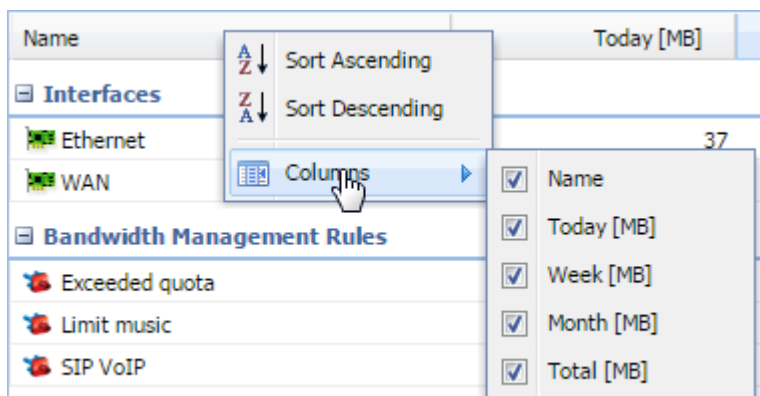
5. Click **Apply**.

From now on, you can view the chart for the selected traffic rules in the **Traffic Charts** section.

Customizing a Traffic Chart table

To add or remove a column in the **Traffic Chart** table:

1. Right-click the table header.
2. In the context menu, select **Columns**.
3. Select any item you need or deselect an item to remove it.

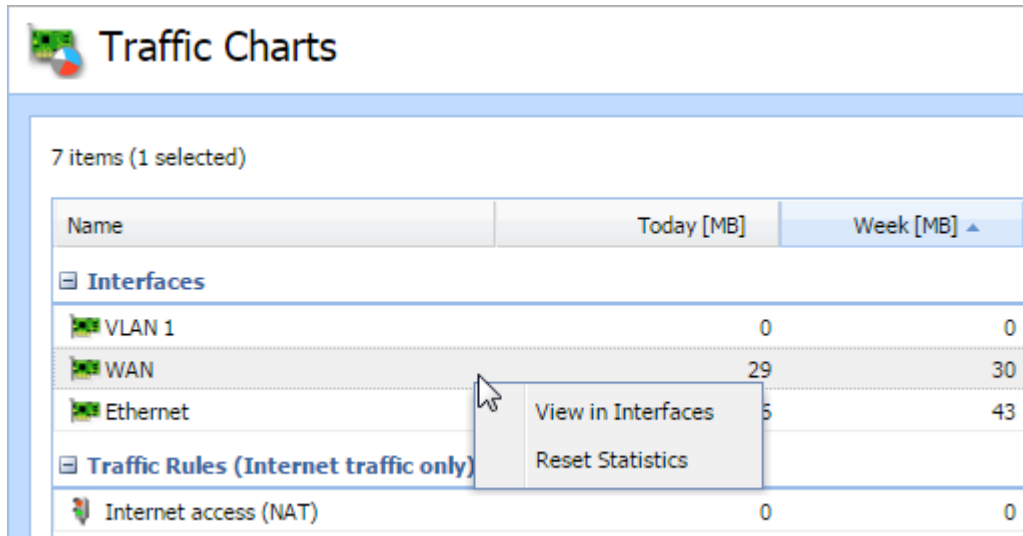


Switching from traffic charts to interfaces and rules

To move quickly from **Traffic Charts** to the **Interfaces**, **Traffic Rules**, or **Bandwidth Management and QoS** section:

1. In the administration interface, go to **Status > Traffic Charts**.
2. Right-click the interface or rule.

3. In the context menu, select **View in Interfaces** or **View in Traffic Rules** or **View in Bandwidth Management**.



Traffic Charts

7 items (1 selected)

Name	Today [MB]	Week [MB] ▲
Interfaces		
VLAN 1	0	0
WAN	29	30
Ethernet	5	43
Traffic Rules (Internet traffic only)		
Internet access (NAT)	0	0

View in Interfaces
Reset Statistics

Kerio Control displays the interface or rule in the corresponding section.

Resetting traffic chart statistics

1. In the administration interface, go to **Status > Traffic Charts**.
2. Right-click the interface or rule.
3. In the context menu, select **Reset Statistics**.

Kerio Control resets statistics for the particular rule or interface.

3.7.5 Monitoring user statistics

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).

User Statistics

17 items (1 selected)

Username	Full Name	Quota	Today [MB]	Week [MB]	Month [MB]	Total [MB]
all users	all users		15	1 324	1 963	44 988
Admin			0	0	0	5 026
Admin			0	0	0	0
amontoya	Adam Montoya			880	1 208	3 087
cmoore	Cindy Moore	0%		0	0	0
cparker	Carl Parker	0%		2	2	722
hyoung	Harry Young	0%		0	0	0
jkeaton	James Keaton	0%		0	0	0
mhall	Michael Hall	0%		0	0	0
msmall	Michael Small	0%		0	0	0
sbond	Sarah Bond	0%		0	0	18
tbond	Tracy Bond	0%		0	0	14
vgruber	Vicky Gruber	0%		0	0	0
vpntestuser	VPN Testuser	0%		0	0	1
wsmith	Wendy Smith	0%		0	0	0
not logged in	not logged in		442	753	35 226	
guest users	guest users			0	0	0

Auto-refresh

Deleting User Traffic Counters

Deleting user traffic counters ensures that the [exceeded quota](#) is released and the user can start using the Internet again.

1. In the administration interface, go to **Status > User Statistics**.

2. Right-click a user.

3. In the context menu, click **Delete User Traffic Counters**.

Kerio Control deletes all statistics and the user can start with browsing again.

User Statistics

7 items (1 selected)

Username	Full Name	Quota
all users	all users	
abrown	Alex Brown	8%
Admin		46%
bjohnston	Blake Johnston	
jsmith	John Smith	
not logged in	not logged in	
guest users	guest users	

View in Users
View in Kerio Control Statistics
Delete User Traffic Counters

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](#) help section.

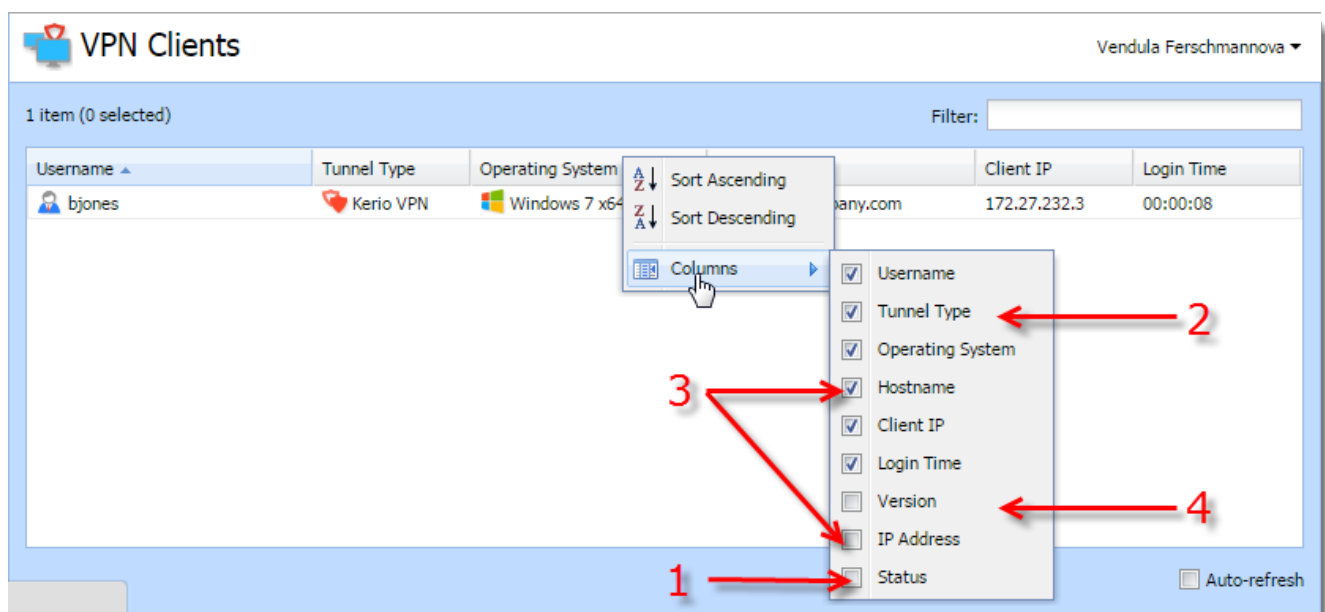
3.7.6 Monitoring VPN clients

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 status of the connection (1):
 - 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) (2)
- » The DNS name or the public IP address of the host (3)
- » The version and the build number of the Kerio VPN Client (4)



NOTE

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**.

3.7.7 SNMP monitoring

Configuring Kerio Control

Simple Network Management Protocol (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). Note that version 2c supports passwords as plain text only (community string), while version 3 supports encryption (SHA-1). Some monitoring tools, however, do not support version 3.

NOTE

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.

Kerio Control

Hostname

Fully qualified hostname or IP address for this device.

gw.company.com

Host Template

Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

None

Number of Collection Threads

The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

1 Thread (default)

Disable Host

Check this box to disable all checks for this host.

☐ Disable Host

Availability/Reachability Options

Downed Device Detection

The method Cacti will use to determine if a host is available for polling.

SNMP Uptime

NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Timeout Value

The timeout value to use for host ICMP and UDP ping. This host SNMP timeout value applies for SNMP pings.

400

Ping Retry Count

After an initial failure, the number of ping retries Cacti will attempt before failing.

1

SNMP Options

SNMP Version

Choose the SNMP version for this device.

Version 2

SNMP Community

SNMP read community for this device.

public

SNMP Port

Enter the UDP port number to use for SNMP (default is 161).

161

SNMP Timeout

The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

500

Maximum OID's Per Get Request

Specified the number of OID's that can be obtained in a single SNMP Get request.

10

Additional Options

Notes

Enter notes to this host.

Cancel

Create

3.8 Logs

This section provides information about consulting logs, filtering options, and debugging Kerio Control.

3.8.1 Using and configuring logs	124
3.8.2 Using the Config log	128
3.8.3 Using the Connection log	129
3.8.4 Using the Debug log	130
3.8.5 Using the Dial log	132
3.8.6 Using the Error log	133

3.8.7 Using the Filter log	134
3.8.8 Using the Host log	135
3.8.9 Using the Http log	137
3.8.10 Using the Security log	138
3.8.11 Using the Warning log	140
3.8.12 Using the Web log	141
3.8.13 Logging packets	141
3.8.14 Log packet formatting	144

3.8.1 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.

NOTE

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:

- » **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).

WARNING

Removed logs cannot be refreshed anymore.

NOTE

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).

NOTE

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.

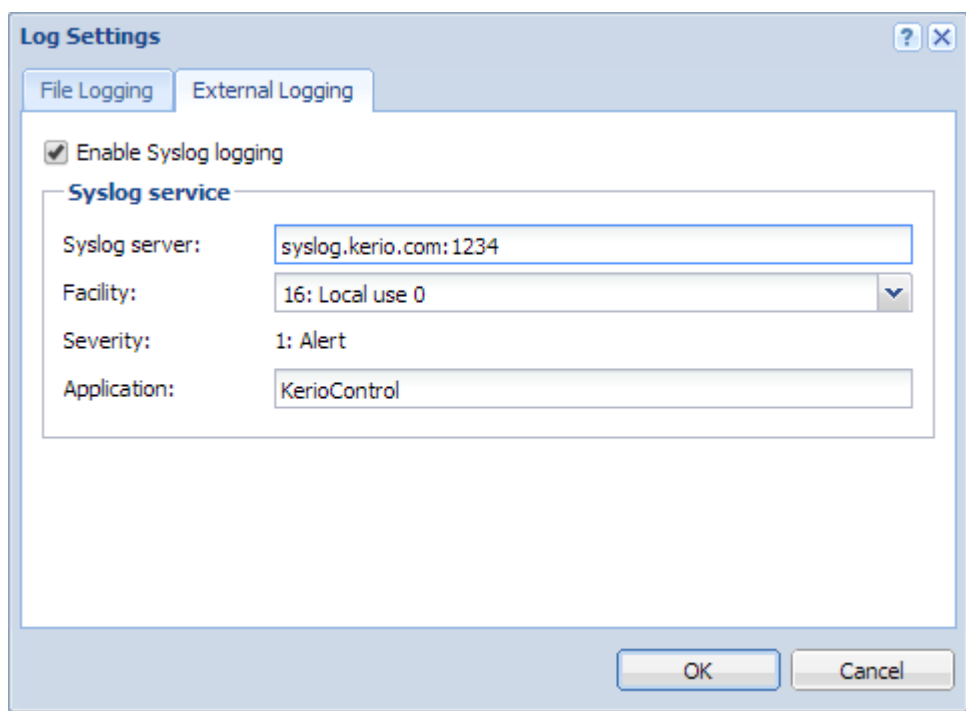
4. Click **OK**

NOTE

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.



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 below.

In the **Application** field, you can type a description displayed in the Syslog server.

Log	Severity
Alert	1: Alert
Config	6: Informational
Connection	6: Informational
Debug	7: Debug
Dial	5: Notice
Error	3: Error
Filter	6: Informational
Host	6: Informational
Http	6: Informational
Security	5: Notice
Warning	4: Warning
Web	6: Informational

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

3.8.2 Using the Config log

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information, refer to [Using and configuring logs](#) (page 124).

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:

Information about logging in to Kerio Control administration

Example 1

```
[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 Fire-
fox/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)

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 2

```
[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

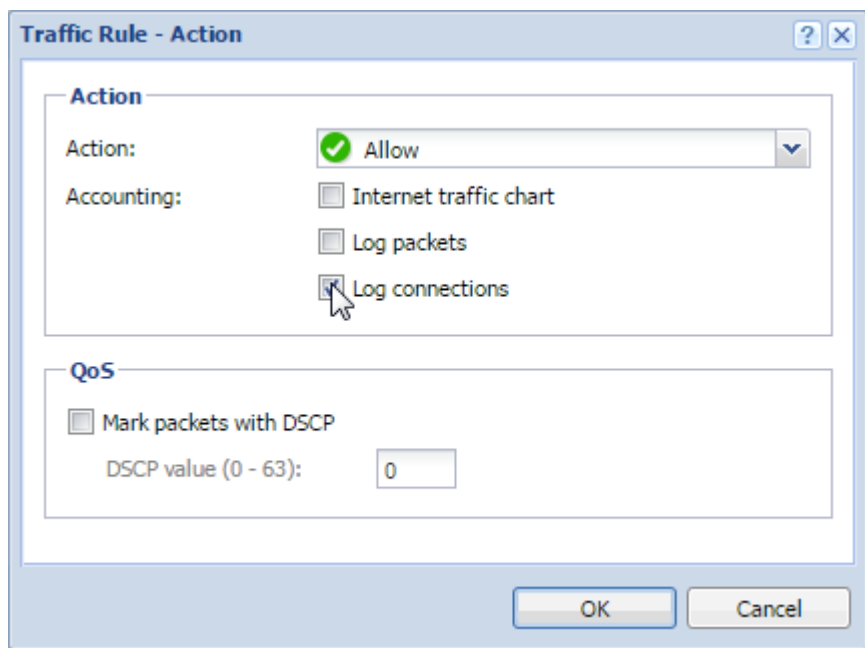
» insert StaticRoutes ... — the particular command used to modify the Kerio Control's configuration database (in this case, a static route was added to the routing table)

3.8.3 Using the Connection log

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,



» 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).

3.8.4 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 information, refer to [Log packet formatting](#) (page 144).

>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 information, refer to [Logging packets](#) (page 141).

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 information, refer to [Logging packets](#) (page 141).

WARNING

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 proving 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.

3.8.5 Using the Dial log

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.).

3.8.6 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 a loop in the configuration of the DNS module or the Proxy server, etc.),
- » Network (socket) errors,
- » Errors while starting or stopping the Kerio Control (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.

NOTE

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.

3.8.7 Using the Filter log

Logs keep information records of selected events occurred in or detected by Kerio Control. For more information, refer to [Using and configuring logs](#) (page 124).

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, refer to [Log packet formatting](#) (page 144).

Reading the Filter log

Example of a URL rule log message

```
[18/Apr/2013 13:39:45] ALLOW URL 'Kerio Antivirus 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)
- » 'Kerio Antivirus 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
- » flags: — TCP flags
- » seq: — sequence number of the packet (TCP only)
- » ack: — acknowledgement sequence number (TCP only)
- » win: — size of the receive window in bytes (it is used for data flow control TCP only)
- » tcplen: — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

3.8.8 Using the Host log

Host 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 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

3.8.9 Using the Http log

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).

NOTE

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 processes 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).
- » 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

3.8.10 Using the Security log

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 Binaryproto:TCP,
ip/port:95.211.98.71:80(hosted-by.example.com) > 192.168.48.131:49960
(wsmith-pc.company.com,user:wsmith)
```

- » `IPS: Packet drop` — the particular intrusion had the action set for **Log and drop** (in case of the **Log** action, `IPS: Alert`)
- » `severity: High` — severity level
- » `Rule ID: 1:2010575` — number identifier of the intrusion (this number can be used for definition of exceptions from the intrusion detection system, i.e. in the system's advanced settings)
- » `ET TROJAN ASProtect/ASPack...` — intrusion name and description (only available for some intrusions)
- » `proto:TCP` — traffic protocol used
- » `ip/port:95.211.98.71:80(hosted-by.example.com)` — source IP address and port of the detected packet; the brackets provide information of the DNS name of the particular computer, in case that it is identifiable
- » `> 192.168.48.131:49960(wsmith-pc.company.com,user:wsmith)` — destination IP address and port in the detected packet; the brackets provide DNS name of the particular host (if identifiable) or name of the user connected to the firewall from the particular local host

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: Kerio Antivirus database has been
successfully updated. Kerio Antivirus engine version/Signature count:
(AVCORE v2.1 Linux/x86_64 11.0.1.12 (Sep 29, 2016)/8528221) is now active.
```

3.8.11 Using the Warning log

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
```


3.8.12 Using the Web log

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

3.8.13 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.

NOTE

Kerio Control also offers a packet dump. The packet dump saves the wanted traffic to file which can be downloaded and opened by Wireshark. See the [Creating and downloading packet dumps](#) section.

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
<code>= 1.2.3.4</code>	IPv4 address of the host
<code>= 1.2.3.4/255.255.255.0</code>	subnet defined by the network IPv4 address and a corresponding subnet mask
<code>= 1.2.3.4/24</code>	subnet defined by the network IPv4 address and number of bits of the corresponding subnet mask
<code>= 1.2.3.4-1.2.3.10</code>	IPv4 range (inclusive)
<code>= 2001:abcd:1234::1</code>	IPv6 address of the host
<code>= list:"name of IP group"</code>	IP address group
<code>= user:"user1,user2,[group1],user3,[group2]"</code>	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).

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
= vpndclient	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.

3.8.14 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 attributeRaw)
- » %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)
```

NOTE

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.

3.9 VPN

This topic helps you create and configure Kerio Control VPN and IPsec VPN.

3.9.1 Configuring Kerio VPN	145
3.9.2 Configuring IPsec VPN Server	154
3.9.3 Routing all traffic through Kerio VPN Tunnel	172
3.9.4 Connecting multiple offices via Kerio VPN and IPsec VPN tunnels	176
3.9.5 Assigning static IP addresses for Kerio Control VPN Clients	181
3.9.6 Kerio Control VPN Client for administrators	182
3.9.7 Using Logs to troubleshoot VPN Client issues	182

3.9.1 Configuring Kerio VPN

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 such as desktops, notebooks, mobile devices, etc.
- » [Kerio VPN tunnel](#) for connecting LANs.

Configuring Kerio VPN Server

Kerio VPN Server offers clients such as desktops, notebooks, mobile devices, etc. a secure way to connect to the network.

NOTE

You must enable communication through VPN in Traffic Rules before start configuring the Kerio VPN Server. For more information, refer to [Configuring traffic rules](#) (page 236).

To configure Kerio VPN Server:

Configuring Interface

To configure Interface:

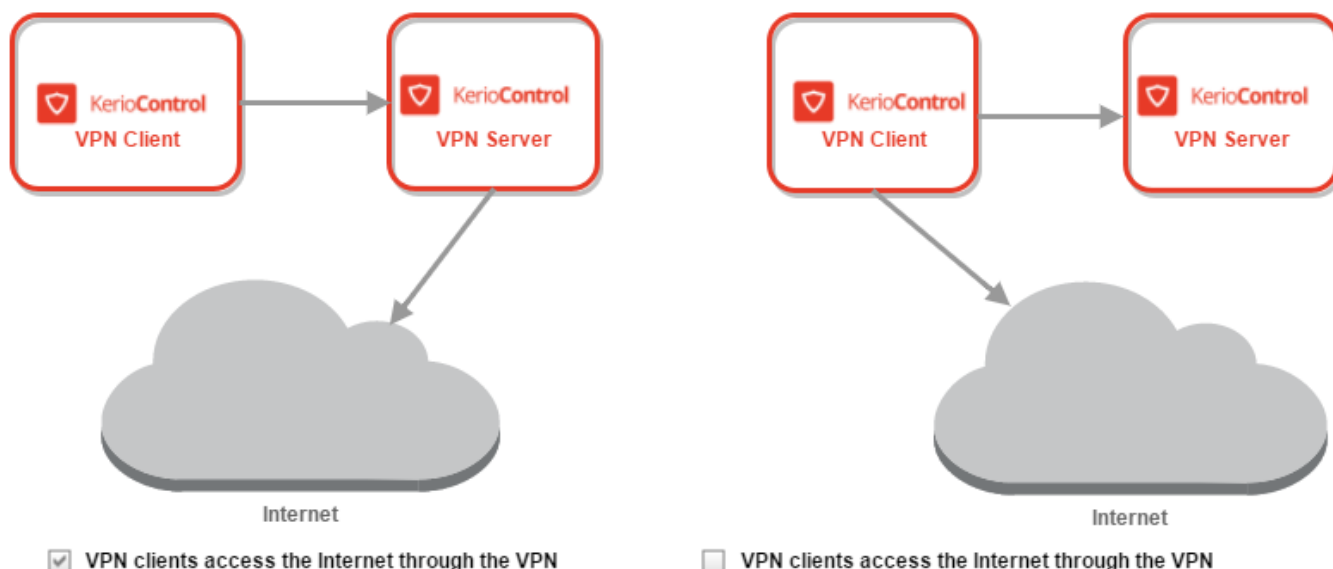
1. In the administration interface, go to **Interfaces**.
2. Double-click **VPN Server**.
3. In the **VPN Server Properties** dialog, check **Enable Kerio VPN Server**.
4. On tab **Kerio VPN**, select a valid certificate.
5. The port 4090 is set as default. Both TCP and UDP protocols are used.

NOTES

Do not switch to another port without a proper reason.

If it is not possible to run the VPN Server on the specified port, the error is 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**.



Screenshot 19: VPN diagrams

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

Traffic Rules							
Admin							
Search: <input type="text"/>							
<input type="button" value="Test Rules"/> <input type="button" value="Restore View"/>							
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"/> Web Services	Any	Firewall	HTTP HTTPS	Any	Allow		
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	
<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
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any	Any	Any	Allow		just now

Screenshot 20: Configuring Traffic Rules

9. 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 box, define a network, mask and description. In case of any collisions, custom routes are used instead.
6. Save the settings.

NOTE

Use the 255.255.255.255 network mask to define a route to a specific host. It can be helpful when adding a route to a host in the demilitarized zone at the VPN Server's side.

Configuring DNS

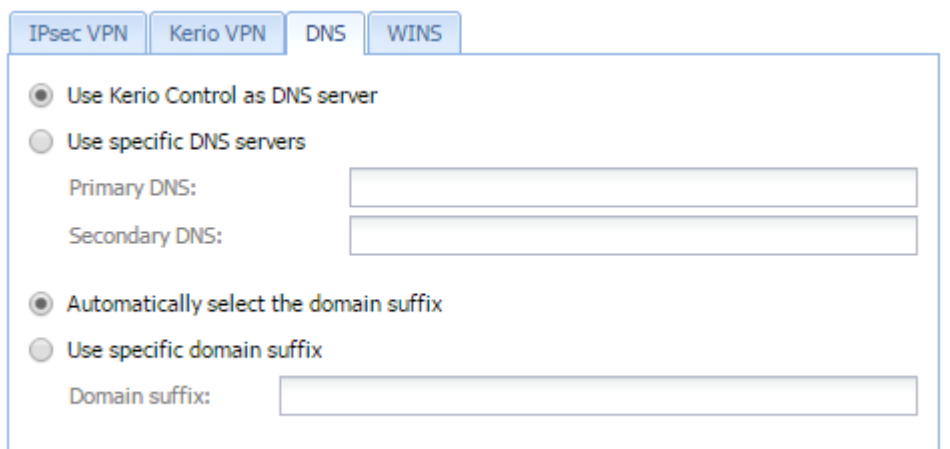
Kerio VPN Server needs a DNS Server to be used. There are two possible configuration options:

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.



Screenshot 21: Configuring which DNS to be used by Kerio Control VPN

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.

NOTE

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 on 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.

NOTE

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 more information, refer to [Assigning static IP addresses for Kerio Control VPN Clients](#) (page 181).

Configuring Kerio VPN tunnel

Kerio VPN tunnel allows the administrator to connect officers located on separated geographic areas into a single network.

Kerio VPN tunnel offers authentication and encryption to ensure a fast and secure connection.

To configure Kerio VPN tunnel:

Adding a new 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 Kerio 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 Kerio 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 Kerio 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 of the remote server, specify the fingerprint of this local server.

7. Save your settings.

NOTE

All local networks at each location must have unique IP subnets. Before connecting two sites using Kerio 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 Kerio VPN server are defined. You can also specify 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 multi-site tunnels

Kerio Control VPN automatically exchanges routing information based on the same order it establishes each tunnel. It does not implement prioritization or optimal path routing. For scenarios that involve more than two VPN tunnels, you can designate a central endpoint in a star topology.

For example, if you have four sites named A, B, C, and D and you designate D as the central endpoint. The tunnels configuration is done as follows:

A <-----> D

B <-----> D

C <-----> D

The star topology forces all VPN routing through a single endpoint. In case that endpoint is unavailable, all sites become unreachable. To improve the reliability of this topology, you can designate a secondary central endpoint using VPN failover configuration.

Configuring VPN failover

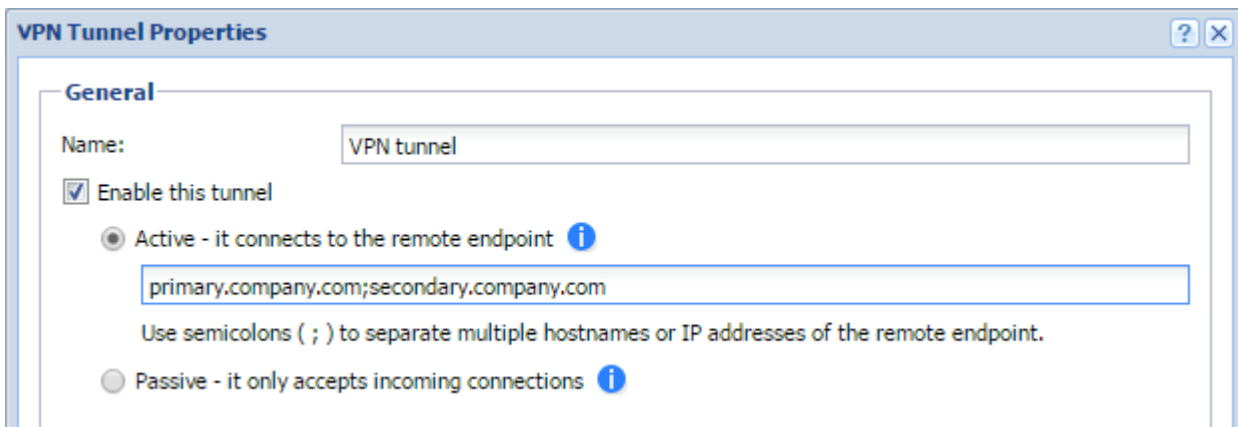
If Kerio Control uses load balancing between multiple Internet links, it is possible to use VPN failover.

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

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

NOTE

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



Screenshot 22: VPN tunnel properties

Example - Company with one branch office

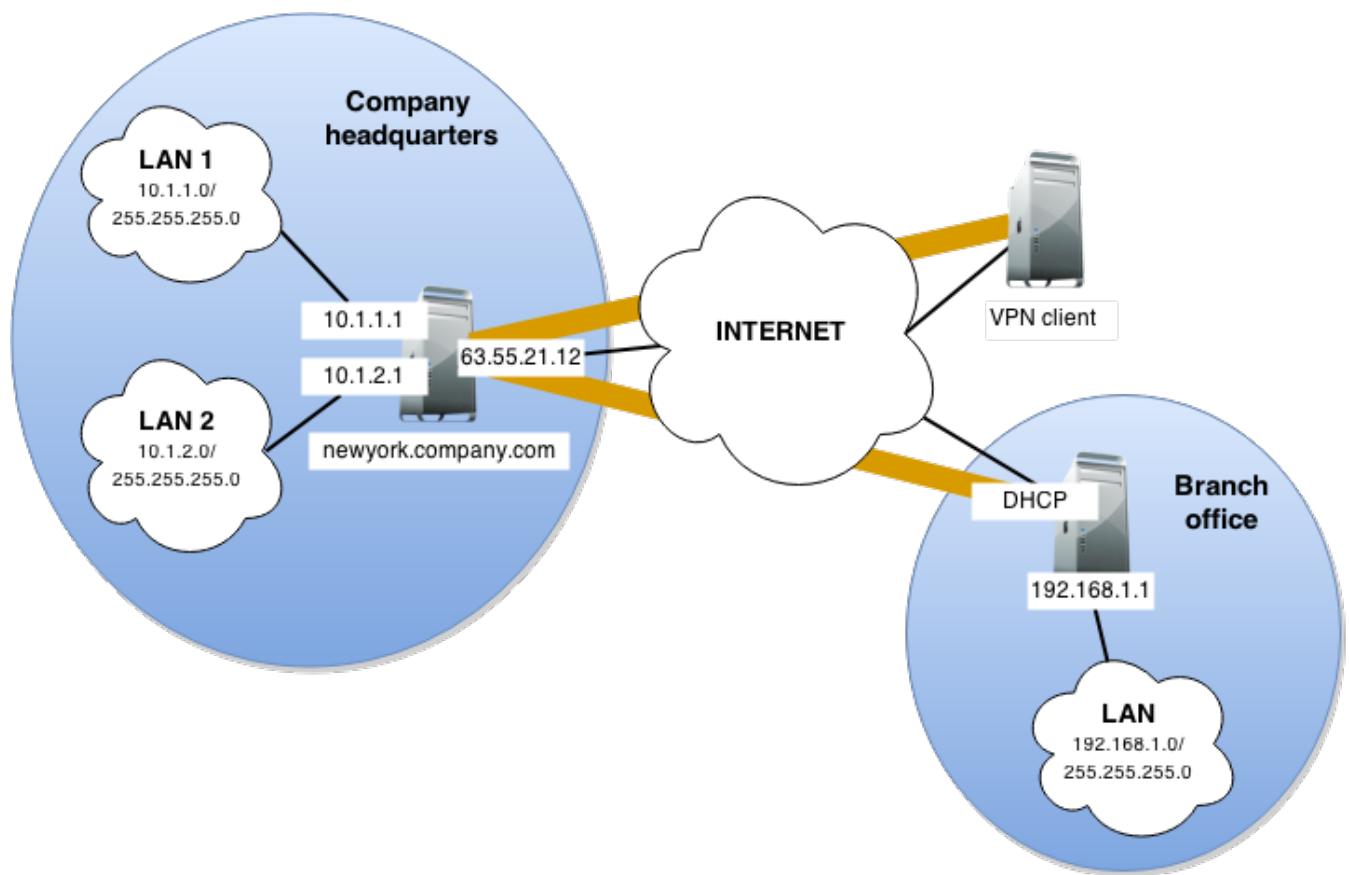
This example describes how to connect two company local networks using the Kerio VPN tunnel.

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.



Screenshot 23: VPN diagram

You must configure the following settings:

1. In the headquarters, Kerio Control administration, define the Kerio 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 [?] [X]

General

Name:

☒ Enable this tunnel

☐ Active - it connects to the remote endpoint ⓘ
 Remote endpoint hostname or IP address:

☒ Passive - it only accepts incoming connections ⓘ

Type:

Authentication **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.

Screenshot 24: VPN tunnel properties

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.

Traffic Rules Admin ▾

Search: [↑] [↓]

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 Interfac... VPN clients All VPN tunnels	Any	Any	✓ Allow		just now

Screenshot 25: Traffic Rules dashboard

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.

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 Interfaces	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		

Screenshot 26: Traffic rules details

5. Test the connection from each local network. Test availability both through the IP addresses and DNS names. Use the `ping` and **tracert (tracert)** 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.

3.9.2 Configuring IPsec VPN Server

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

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

Configuring IPsec VPN Server

Kerio IPsec VPN Server offer clients such desktops, notebooks, mobile devices, etc. a secure way to connect to the network.

To implement Kerio IPsec VPN Server you need to make changes in the configuration on the server side and also in the client side.

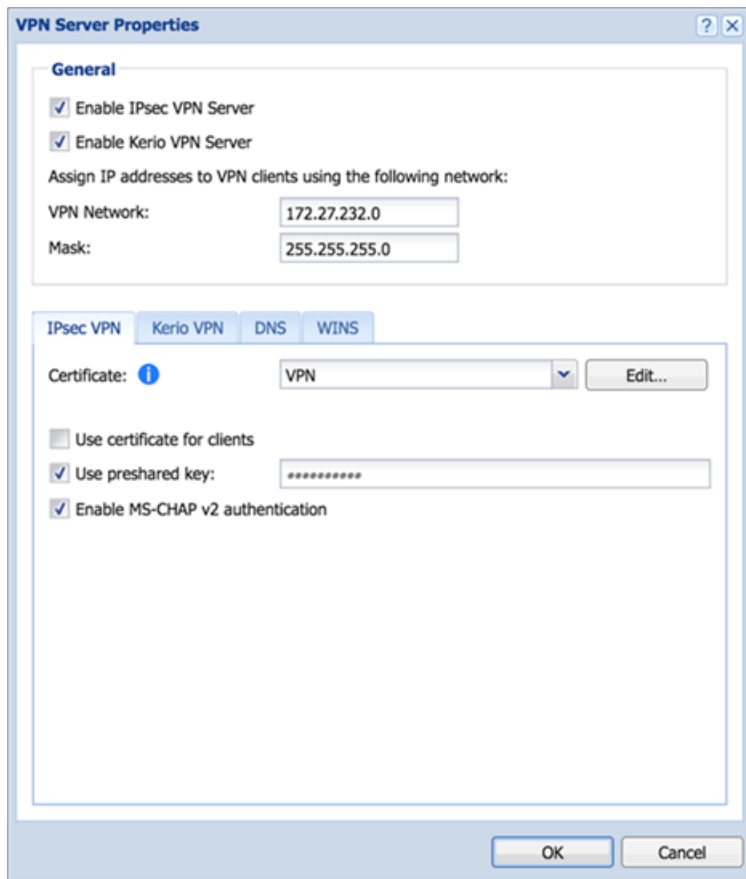
Configuring the Server side

For securing the communication on the server side you can use both or one of the methods below:

- » a preshared key (PSK, shared secret)
- » a SSL certificate

Configuring IPsec VPN server with a preshared key

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



Screenshot 27: VPN Server properties

1. In the administration interface, go to **Interfaces**.
2. Double-click on **VPN Server**.
3. In the **VPN Server Properties** dialog box, check **Enable IPsec VPN Server**. Note that Kerio Control can 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 **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 the client side

On the client side only one of the two methods can be available. Either a preshared key or a SSL Certificate. Each user must provide their credentials for authentication.

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

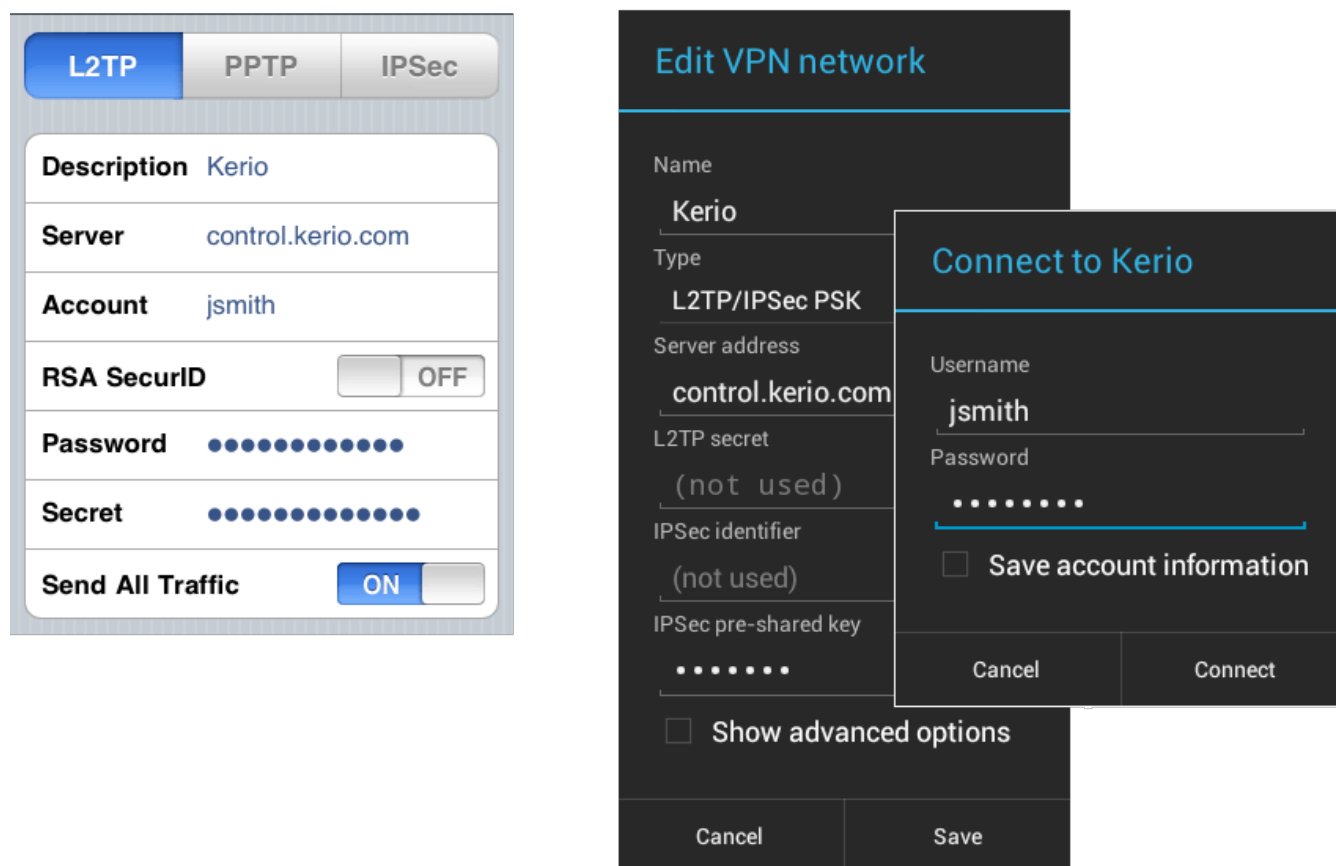
Configuring clients with a SSL certificate

All client machines need to have the certificated imported into the Certification Trusted store. Instruct your users to contact help desk in case of a message of invalid certificate.

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



Screenshot 28: Mobile settings for connection via VPN

Configuring IPsec VPN tunnel

Kerio IPsecVPN tunnel allows the administrator to connect officers located on separated geographic areas into a single network.

Kerio IPsec VPN tunnel offers authentication and encryption to ensure a fast and secure connection.

NOTE

To connect two or more Kerio Controls via VPN tunnel, use [Kerio VPN](#). Unlike Kerio IPsec VPN tunnel, Kerio VPN tunnel is able to seek routes in remote networks automatically.

To configure Kerio IPsec VPN tunnel:

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**.
- » 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 authentication method

You can select one of the following methods:

Preshared key authentication

This method is easier for set up. Both endpoints use the same password for authentication:

1. In the administration interface, go to **Interfaces**.
2. Click **Add > VPN Tunnel**.
3. Type a name of the new tunnel.
4. Set the tunnel as active and type the hostname of the remote endpoint. At least one endpoint must be set as active. 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. Pre-defined Local ID is the hostname of Kerio Control. If you change the Kerio Control hostname, Local ID is changed too.
8. (Optionally) In the **Phase 1 and 2 cipher**, click **Change** and configure ciphers manually. It can be necessary if you want to connect Kerio Control with the third party firewall. For details, see [Configuring IKE ciphers](#).
9. On tabs **Remote Networks** and **Local Networks**, you must [define all remote networks including subnet for VPN clients](#) and [all local networks which are not detected by Kerio Control](#).
10. Save the settings.

SSL certificate authentication

Authentication with a SSL certificate requires a valid SSL certificate on both endpoints.

- » [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. At least one endpoint must be set as active. 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. (Optionally) In the **Phase 1 and 2 cipher**, click **Change** and configure ciphers manually. It can be necessary if you want to connect Kerio Control with the third party firewall. For details, see [Configuring IKE ciphers](#).
8. Save the settings.

Configuring ciphers in key exchange (IKE)

NOTE

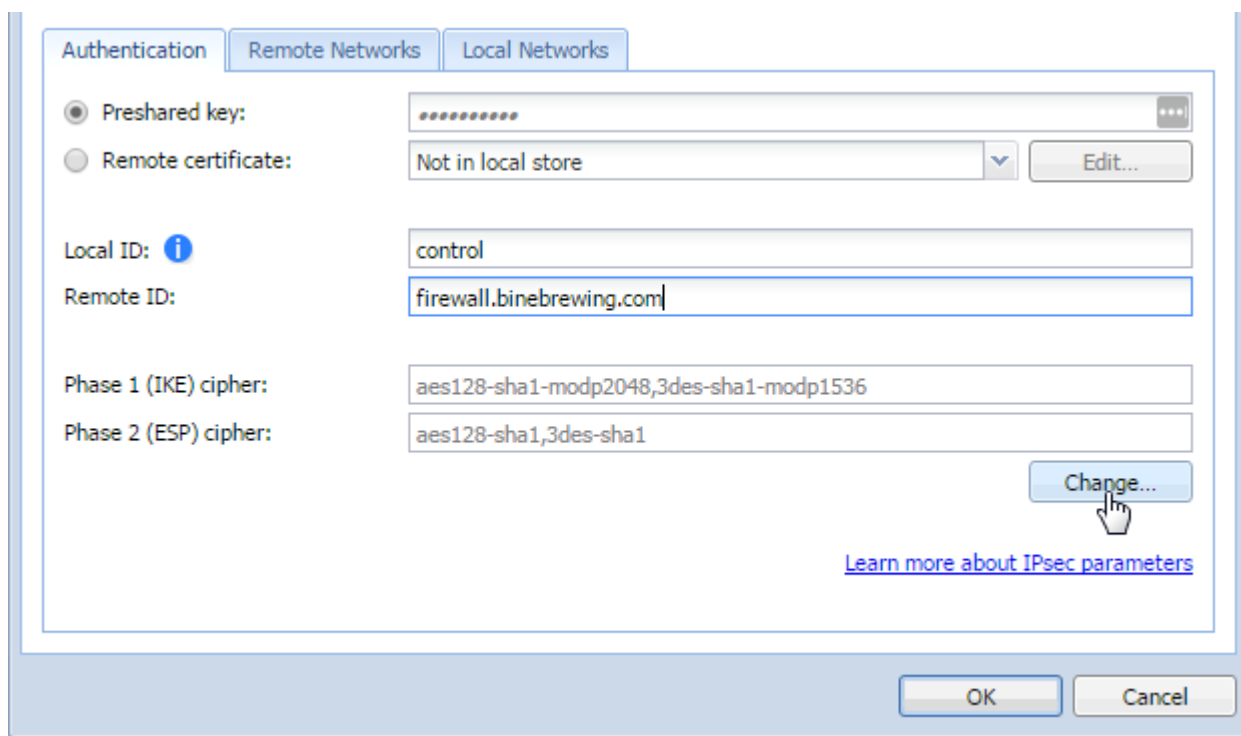
New in Kerio Control 9.2!

Kerio Control can use several IKE ciphers during the connecting and authorizing process of IPsec tunnel. In many cases, these ciphers are common between the endpoints and no custom configuration is necessary.

In other cases, you may need to assign custom ciphers. Therefore, you can configure IKE ciphers in Kerio Control manually:

Configuring authentication

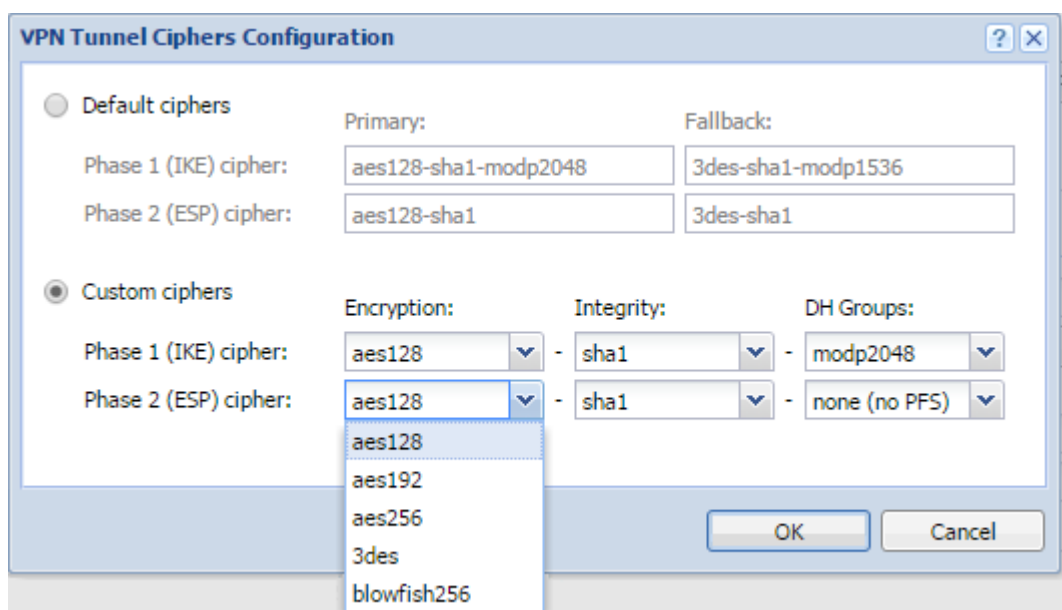
1. In the administration interface, go to **Interfaces**.
2. Select the IPsec VPN tunnel and click **Edit**.
3. In the **VPN Tunnel Properties** dialog box, click **Change** on the **Authentication** tab.



Screenshot 29: Configuring Authentication for the VPN tunnel

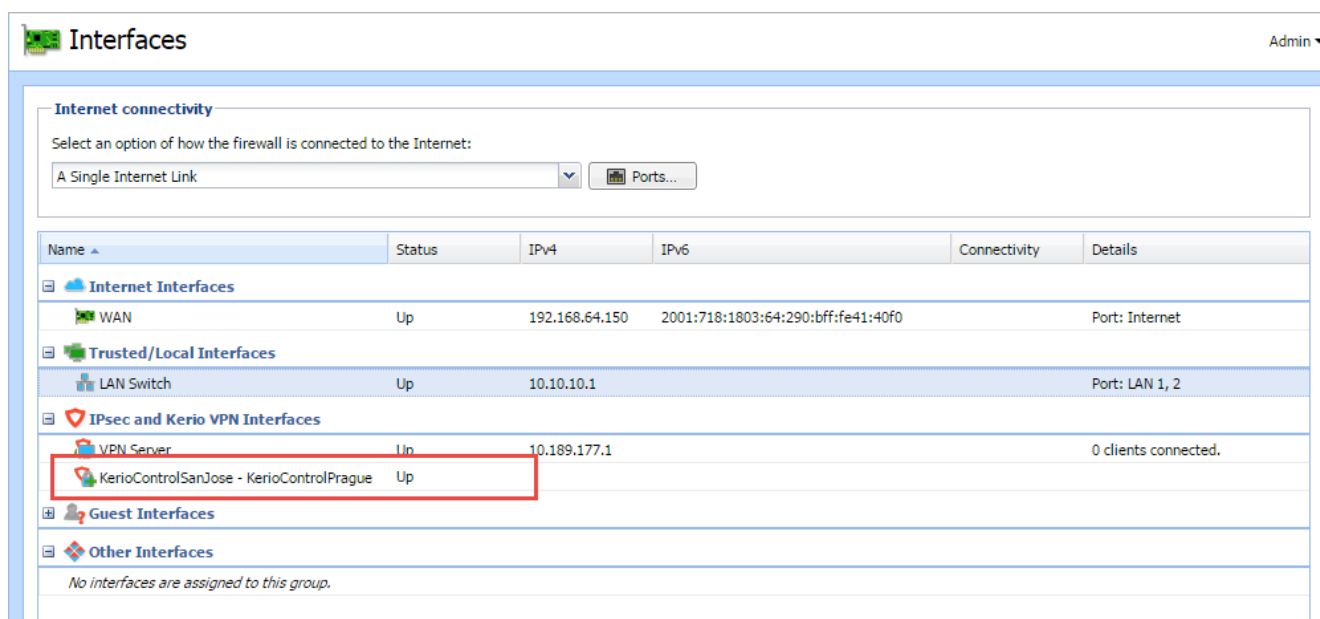
4. In the **VPN Tunnel Ciphers Configuration**, select **Custom ciphers**.

5. In drop down menus, change ciphers in the same way as they are set in the other firewall or device.



Screenshot 30: Configuring VPN Tunnel Ciphers

6. Click **OK** twice.



Screenshot 31: Interface node showing new VPN connection

Both endpoints should connect successfully and you can verify it in the **Interfaces** section. The IPsec tunnel is **Up**. For more information, refer to [Default values in Kerio Control](#) (page 162).

Configuring local networks

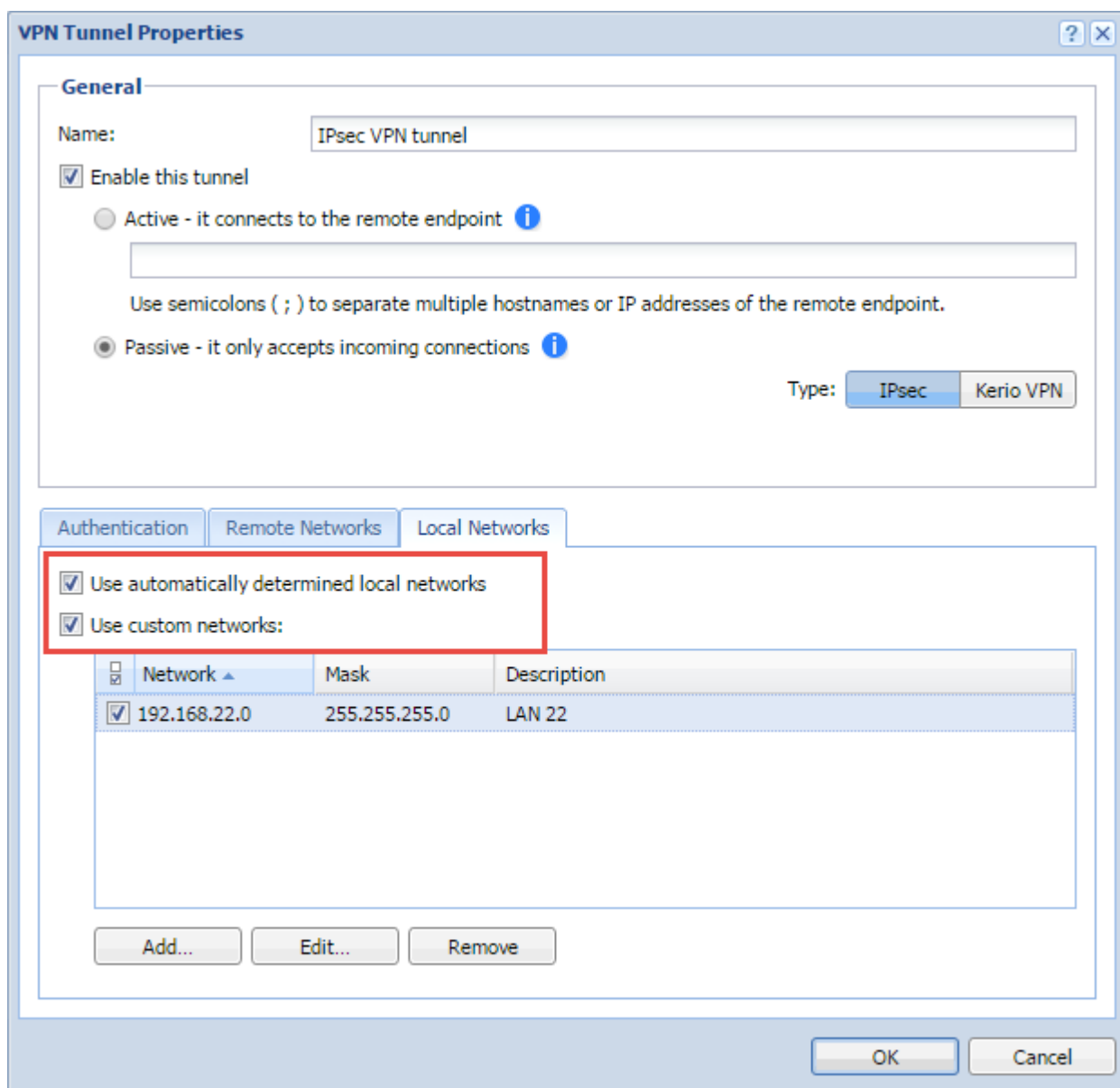
Kerio Control IPsec tunnel can detect most of its local networks. To enable the automatic detection:

1. In the administration interface, go to **Interfaces**.
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.
4. If you define custom routes, select **Use custom networks** too.

NOTE

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

5. Click **OK**



Screenshot 32: Configuring local networks

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 remote networks

IPsec VPN is not able to seek remote routes. You must enter them manually. For more information, refer to [Configuring the IPsec VPN tunnel](#) (page 176).

Configuring VPN failover

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

To configure failover:

1. In the administration interface, go to **Interfaces**.
2. Select the IPsec VPN tunnel and click **Edit**.

Screenshot 33: Configuring failover

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

NOTE

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

Configuring IPsec VPN tunnel with another device

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

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

Before you start, read the topic which describes Kerio Control settings. For more information, refer to [Configuring IPsec VPN tunnel](#) (page 156).

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.

For more information, refer to [Configuring ciphers in key exchange \(IKE\)](#) (page 158).

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

Phase 1 (IKE):

Variable	Default values	Supported values	Unsupported values
mode	main		aggressive
remote ID type	hostname	IP address	
NAT traversal	enabled		
ciphersuite (policies)	aes128-sha1-modp2048,3des-sha1-modp1536		
version	IKEv1		

Variable	Default values	Supported values	Unsupported values
DPD timeouts	enabled (150 sec)		
lifetime	3 hours		

Phase 2 (ESP):

Variable	Supported values	Unsupported values
mode	tunnel	transport
protocol	ESP	AH
ciphersuite (policies)	aes128-sha1, 3des-sha1	
PFS	off	
lifetime	60 mins	

Supported ciphers

Each cipher consists of three parts:

- » Encryption Algorithm — for example, `aes128`
- » Integrity Algorithm — for example, `sha1`
- » Diffie Hellman Groups — for example, `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)

Phase 2 (ESP) - supported ciphers

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)	2 (modp1024)
aes256 (256 bit AES-CBC)	aesxcbc (AES XCBC)	5 (modp1536)
3des (168 bit 3DES-EDE-CBC)		14 (modp2048)
blowfish256 (256 bit Blowfish-CBC)		15 (modp3072)
		16 (modp4096)
		18 (modp8192)
		22 (modp1024s160)
		23 (modp2048s224)
		24 (modp2048s256)

Configuring IPsec VPN client on Apple OS X

There are three steps to connect Apple OS X computer to your company network through IPsec VPN and authenticate with an SSL certificate:

1. Configure IPsec VPN server in Kerio Control.
2. Create SSL certificate and import the certificate to Keychain Access.
3. Configure VPN client as L2TP over IPsec.

Step 1: Configuring Kerio Control

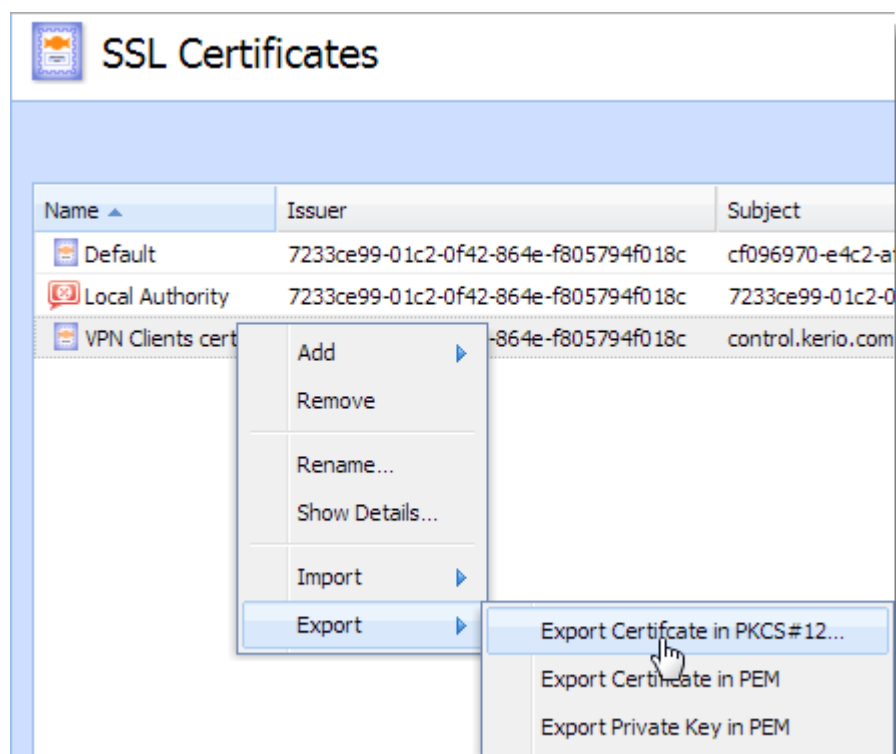
To configure Kerio Control Server:

1. Setup IPsec VPN server to use certificates issued by a Local Certification Authority. For more information, refer to [Configuring IPsec VPN Server](#) (page 154).
2. Go to **Definitions > SSL Certificates**.
3. Click **Add > New Certificate** and create a new certificate for VPN clients.

IMPORTANT

Do not use IP address instead of the Kerio Control hostname.

4. Click **Apply** in the **SSL Certificates** section.
5. Export this certificate in the PKCS#12 format.



Screenshot 34: SSL certificates section

6. In the **Export Certificate in PKCS#12 Format** dialog, use password without national characters.
7. Check **Include all certificates in the certification path if possible** and Kerio Control exports all higher certificates including the certification authority.
8. Click **OK**

Step 2: Importing the certificate

To import the SSL certificate to the Keychain Access utility in your Apple OS X:

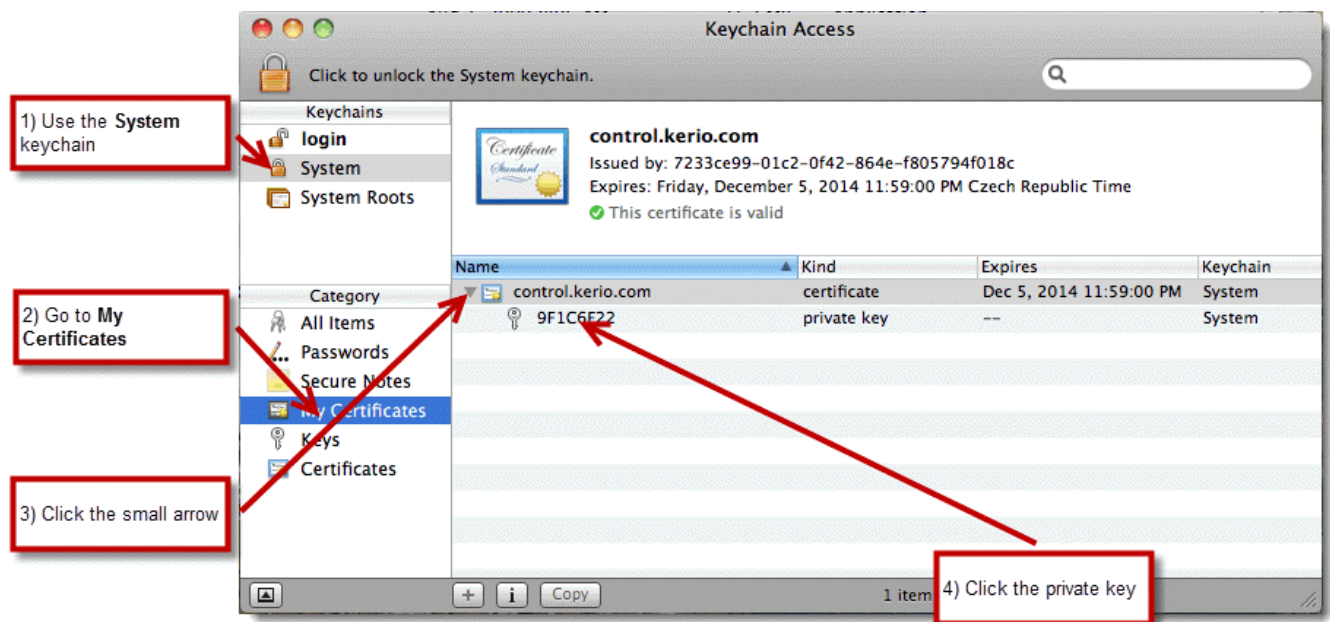
1. Go to **Applications > Utilities > Keychain Access**.
2. Switch view to **System** keychain and unlock the keychain.

IMPORTANT

Do not confuse keychains. Default **Login** keychain is unwanted in this case.

3. Drag the PKCS#12 file, drop it to the **System** keychain. There are at least two Kerio Control certificates — one or more certificates (blue certificate icon) and Certification Authority (gold certificate icon) in the Keychain Access.
4. Locate the imported Certification Authority (CA) in the **System** keychain.
5. Set the CA trust properties to **Always trusted**.
6. Locate the imported certificate and ensure the certificate is trusted.

Procedure for Mac OS X 7 and newer:



Screenshot 35: Keychain access configuration

1. In the **System** keychain, go to **My Certificates**.
2. Find your certificate and click the small arrow and a private key appears.
3. Double-click the private key and go to **Access Control**.
4. Click the + icon and add the following executable to the list: `/usr/sbin/racoon`

NOTE

If you don't see the `/usr` folder when browsing for the executable, use the **Show hidden files**.
The shortcut is `cmd-shift-.` (cmd-shift-dot).

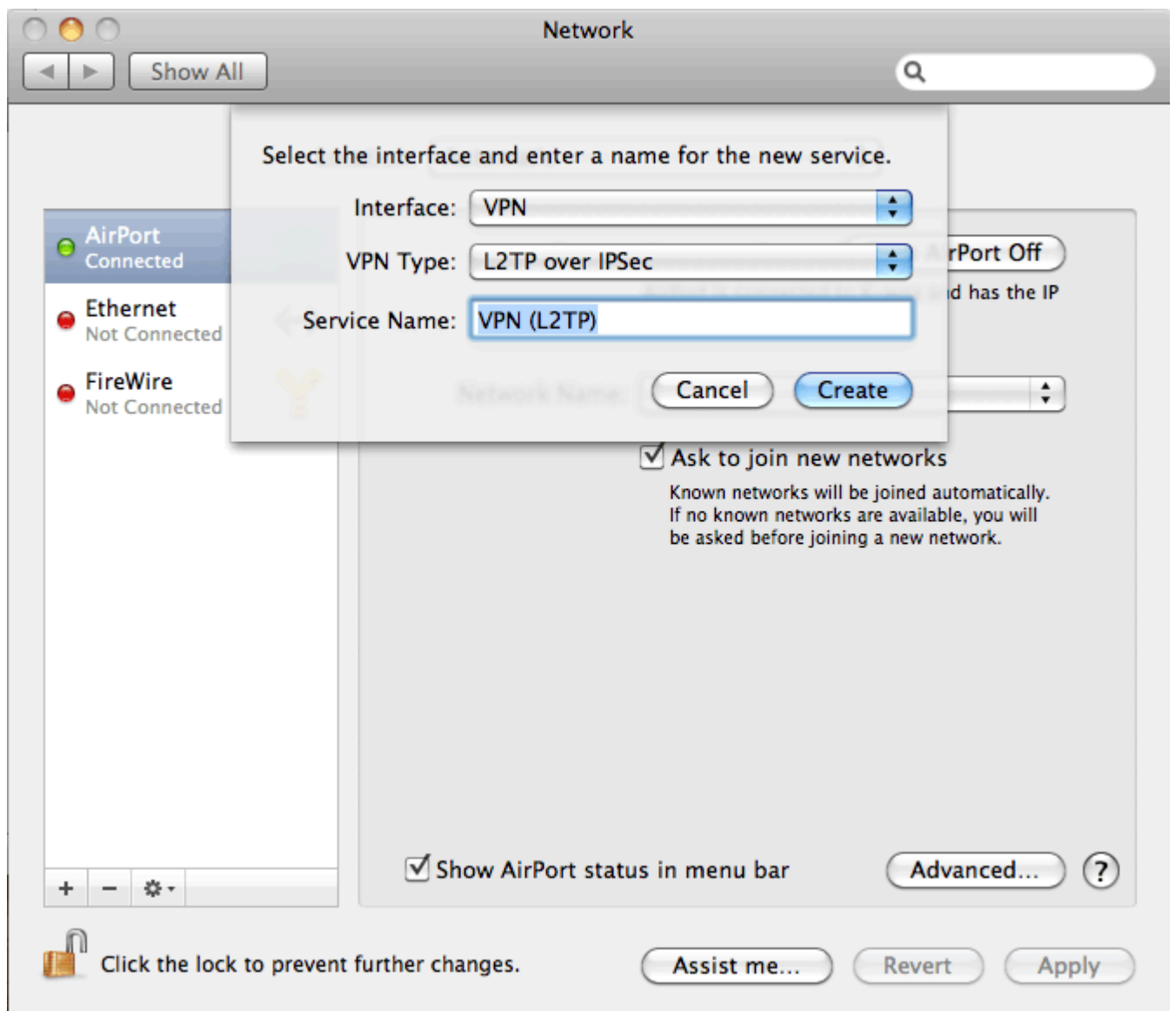
5. Click **Open**.

Keychain Access uses your SSL certificate.

Step 3: Creating VPN client on Apple OS X computer

You must create a VPN connection based on L2TP over IPsec:

1. Go to **System Preferences > Network**
2. In the **Network** dialog, click the **+** icon and add **VPN**.
3. Select the **L2TP over IPsec** mode.

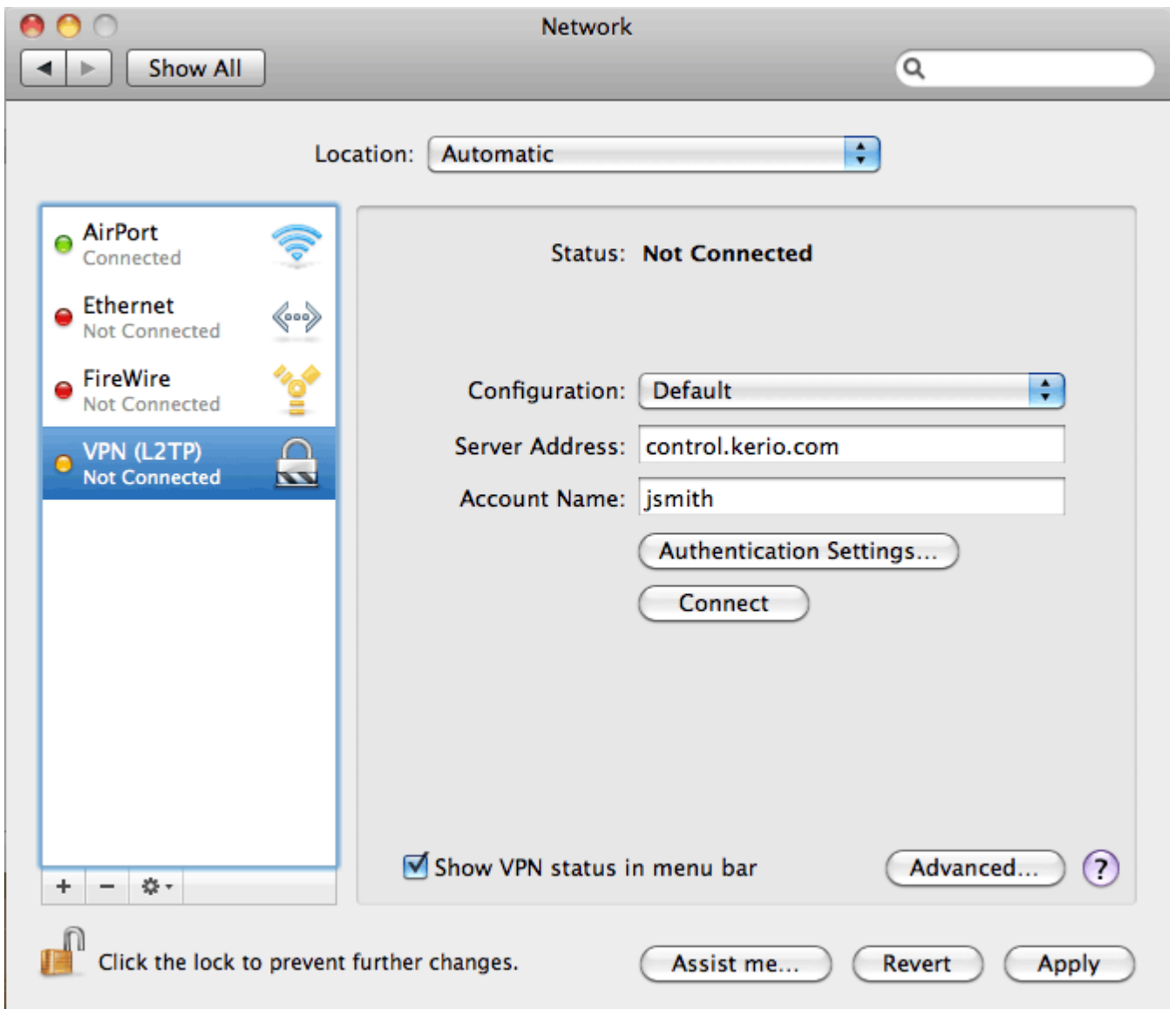


Screenshot 36: Creating VPN client

4. Type a hostname of Kerio Control to **Server Address** and your Control's username to **Account Name**.

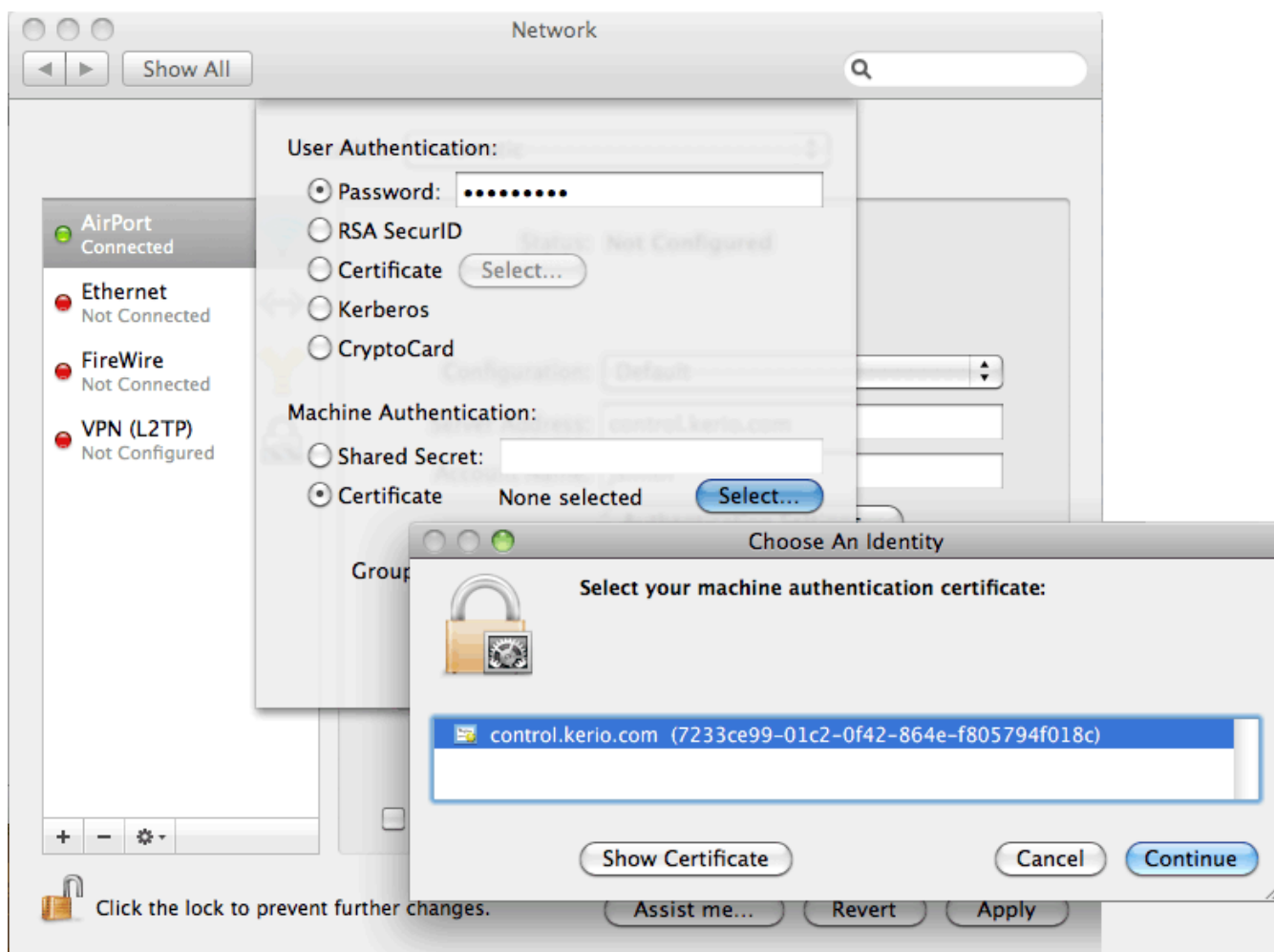
IMPORTANT

Do not use IP address instead of the Kerio Control hostname.



Screenshot 37: Selecting authentication settings

5. Click **Authentication Settings**.
6. Set user authentication by password and type your Kerio Control's password. MS-CHAPv2 might be needed.



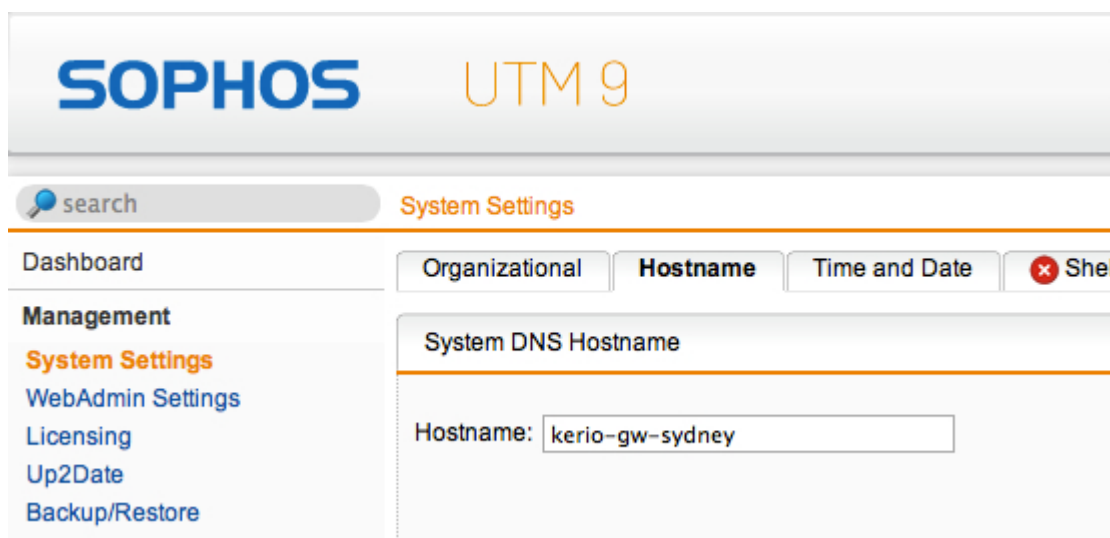
Screenshot 38: Selecting the certificate for authentication

7. Set **Machine Authentication** by a certificate, click **Select** and select the certificate from the previous step.

Configuring IPsec VPN tunnel with Astaro

This article covers the configuration details necessary to establish a site to site VPN tunnel between an Astaro firewall, and Kerio Control. The tested configuration involves IPsec with a pre-shared key.

Before configuring a new VPN tunnel, you will need the defined hostname of the Astaro system, located under **System Settings > Hostname**.



Screenshot 39: Configuring hostname in Astaro

There are two steps to connect Astaro firewall and Kerio Control IPsec VPN:

Step 1: Configuring Kerio Control

1. To configure Kerio Control:
2. Open the Kerio Control web administration.
3. Go to **Configuration > Interfaces**.
4. From the bottom, choose **Add > VPN Tunnel...** Make sure the tunnel type is set to **IPsec**.
5. Define the qualified hostname of the Astaro firewall as the Active endpoint.

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

Authentication Remote Networks Local Networks

☒ **Preshared key:**

☐ **Remote certificate:** Not in local store

Local ID: i

Remote ID:

[Learn more about IPsec parameters](#)

OK Cancel

Screenshot 40: Adding a preshared key

6. In the Authentication section, define a pre-shared key, and input the hostname of the Astaro gateway under the **Remote ID**. This should match exactly as it appeared in the Astaro configuration.
7. Take note of the **Local ID**. This value will be used when configuring the tunnel parameters in Astaro.
8. In the **Remote Networks** section, define all subnets which are located behind the Astaro gateway.

Step 2: Configuring Astaro firewall

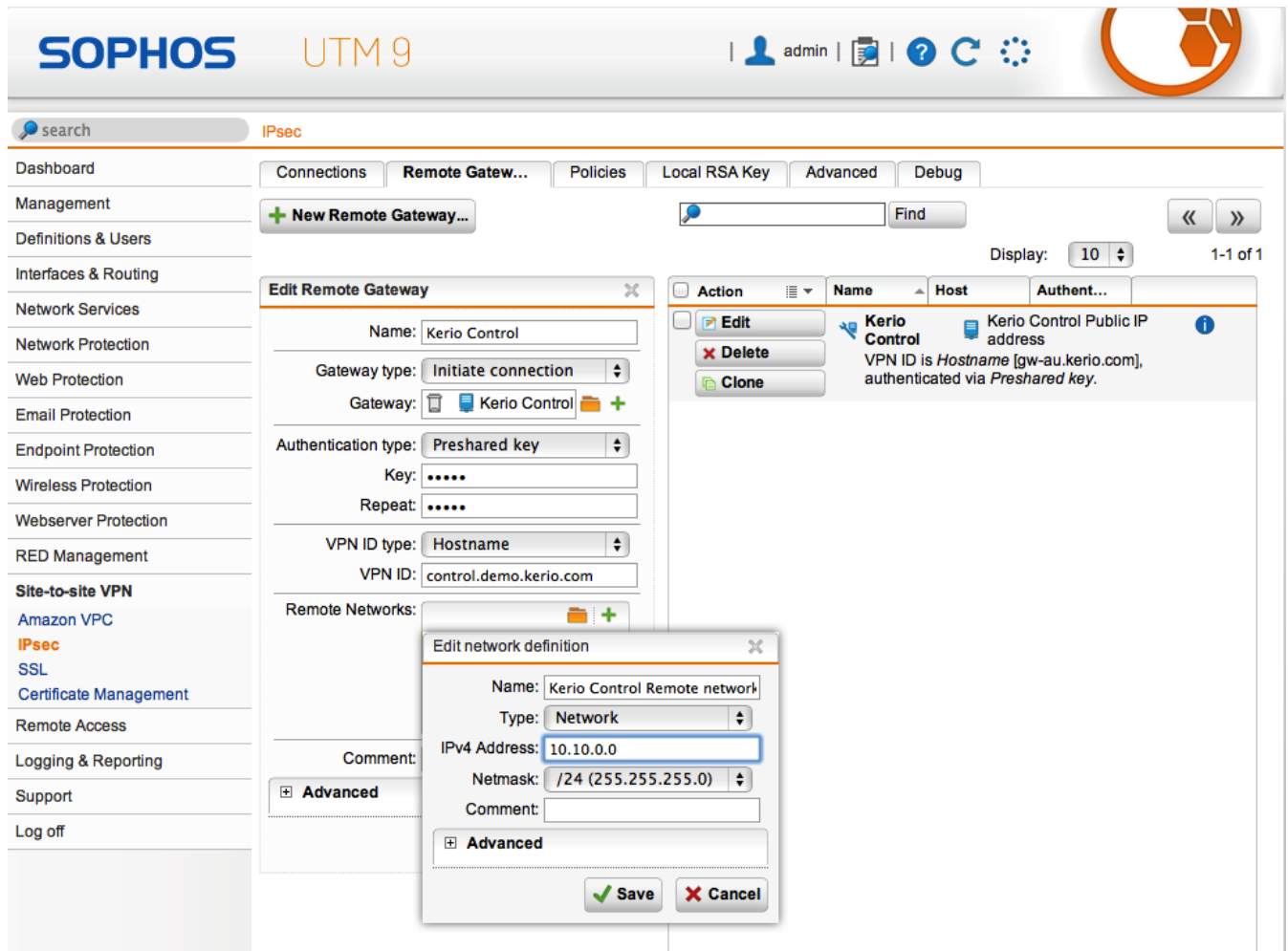
To configure Astaro:

1. From the Astaro administration, go to **Site-to-site VPN > IPsec**.
2. In the Remote Gateway section, create a **New Remote Gateway**. Assign a name.
3. For the Gateway type, choose **Initiate connection**, and add the remote host of the Kerio Control gateway.
4. For the authentication type, choose **Preshared key**, and input the same value inputted into the Kerio Control tunnel properties.

- For the **VPN ID** type, choose **Hostname**, and input the value which Kerio Control provided under the **Local ID** field of its VPN tunnel properties.
- In the **Remote Networks** dialog, add the IP subnets that are located behind the Kerio Control firewall.

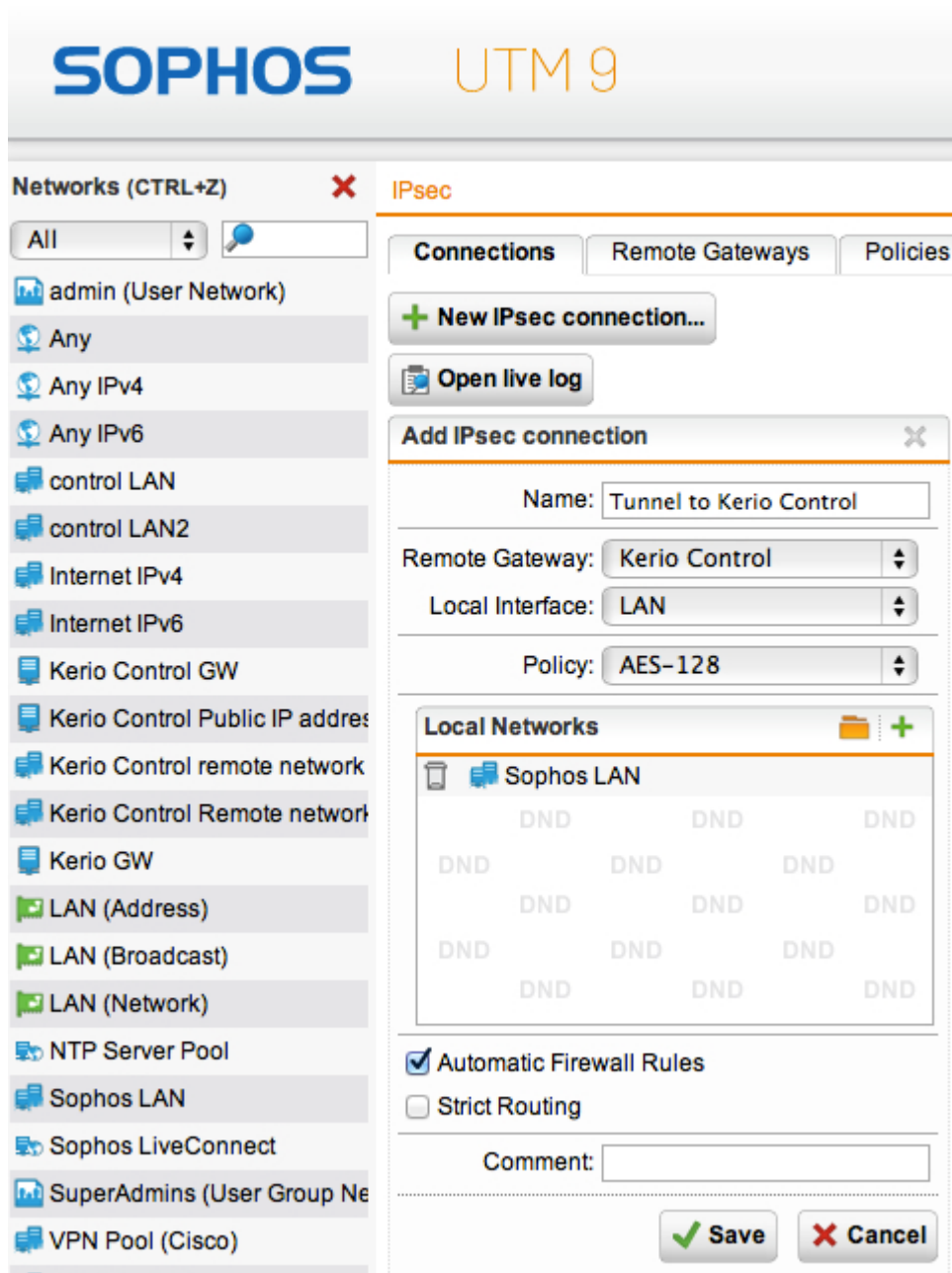
IMPORTANT

The **Remote Networks** defined in each tunnel should not overlap in scope. Otherwise, it may disrupt routing over the tunnel.



Screenshot 41: Editing network definition

- In the Connections section, create a **New IPsec connection...**



Screenshot 42: Configuring IPsec connection

8. Enter the following information:

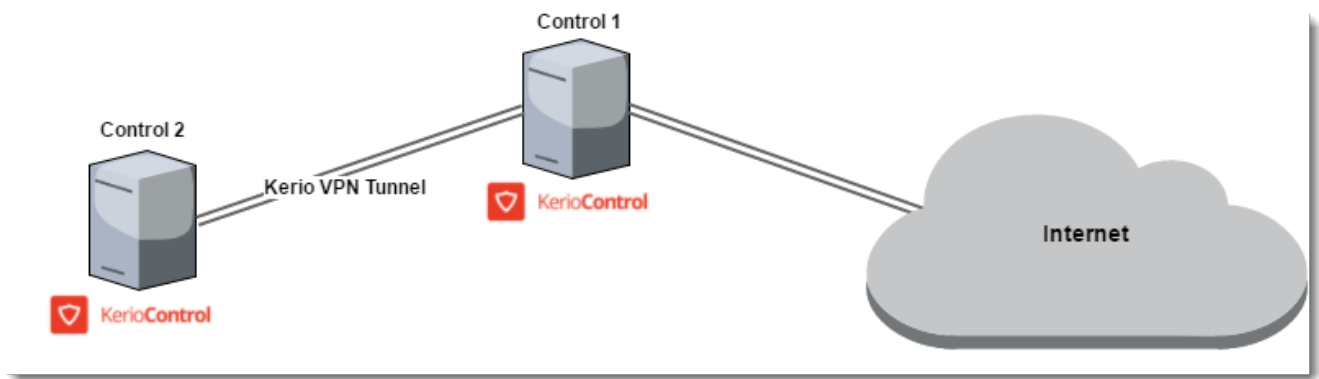
Field	Description
Name	Fill the Assign a name to the tunnel.
Remote Gateway	Assign the Remote Gateway which was created in the previous step.
Local Interface	Assign the local interface you want to access from the remote network via the tunnel.
Policy	Assign the policy AES-128 .

3.9.3 Routing all traffic through Kerio VPN Tunnel

This article describes how to route all traffic from one Kerio Control through the Kerio VPN tunnel to another Kerio Control.

This scenario is useful if you want to gather user statistics for all users in a single Kerio Control.

The steps below use the scenario illustrated in the following diagram:



Screenshot 43: Connecting Kerio installations using VPN tunnel

Licensing

You need a license for each user going through the Kerio Server. On the example illustrated in the screenshot above, the **Control 1** server needs licenses for all **Control 1** and **Control 2** users, while the **Control 2**, you need a license for each **Control 2** user.

Configuring the Kerio VPN tunnel

Follow these steps to configure the Kerio VPN tunnel:

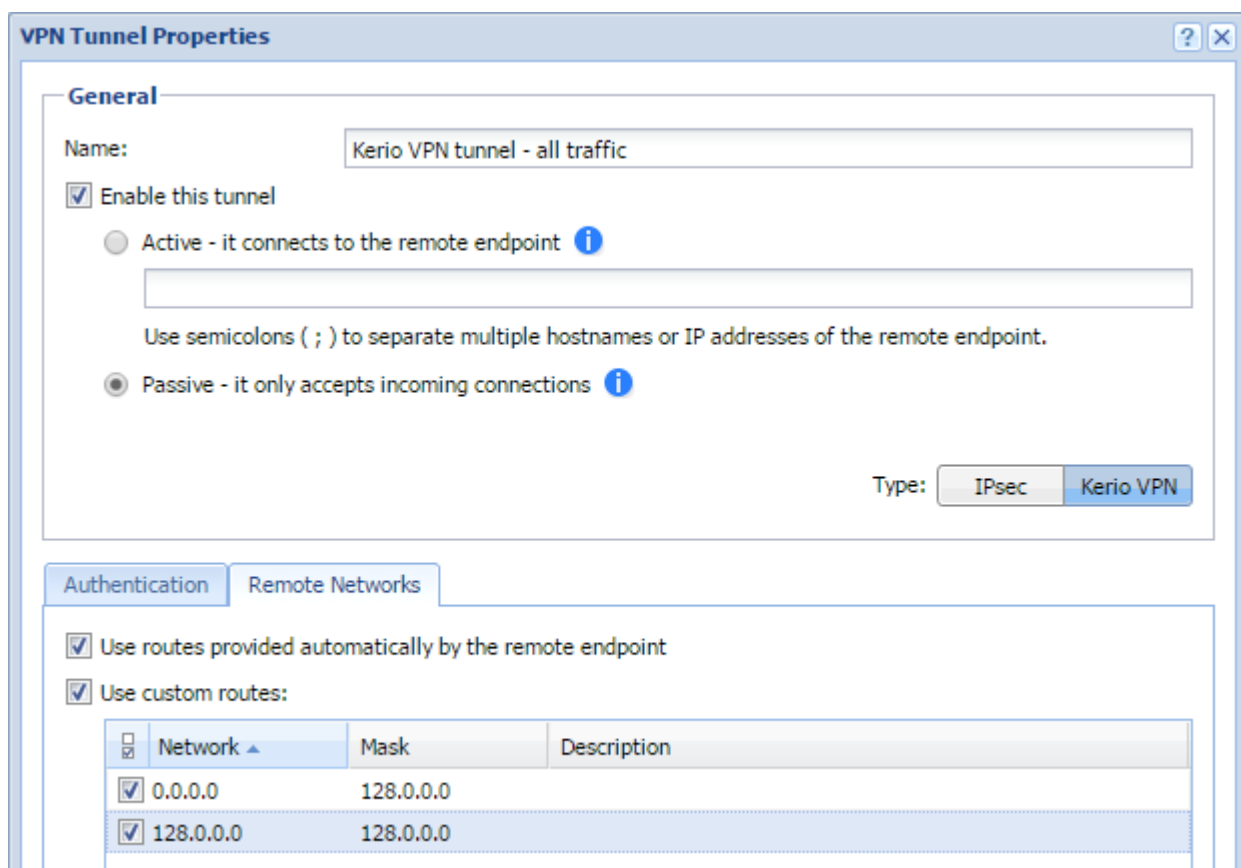
Step 1: Add a Kerio VPN tunnel

See [Configuring Kerio VPN tunnel](#) if you do not already have one set up.

Step 2: Configure remote endpoint routing

After establishing a Kerio VPN tunnel, you need to set up routes in the **Control 2** server:

1. In the **Control 2** administration interface, go to **Interfaces**.
2. Double-click the tunnel.
3. In **VPN Tunnel Properties**, click the **Remote Networks** tab.
4. Add two routes — `128.0.0.0/1` and `0.0.0.0/1` — for routing all traffic through the tunnel.



Screenshot 44: VPN tunnel properties

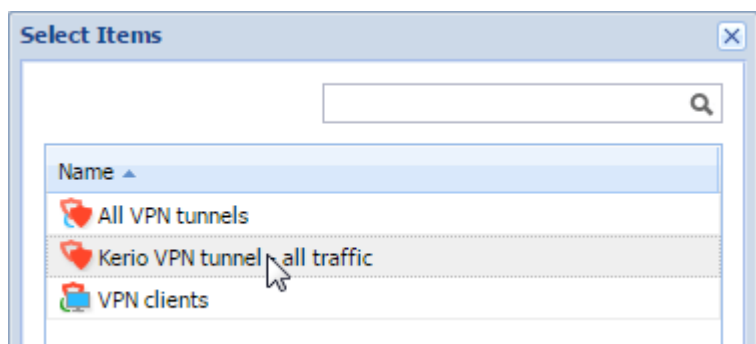
5. Click OK.

6. Click **Apply**.

Step 3: Create traffic rules

In the **Control 1** VPN endpoint, add a traffic rule to allow users from the VPN tunnel to access the Internet:

1. In the **Control 1** administration interface, go to **Traffic Rules**.
2. In the **Internet access (NAT)** rule, double-click the **Source** column.
3. In the **Traffic Rule - Source** dialog box, click **VPN**.
4. In the **Select Item** dialog box, double-click the Kerio VPN tunnel you want to use to route all traffic to another Kerio Control.



Screenshot 45: Selecting Kerio VPN tunnel all traffic

5. Click **OK**
6. Click **Apply**.

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

Screenshot 46: Kerio VPN tunnel showing in the dashboard

From now on, users from the **Control 2** server can access the Internet.

Step 4: Configure DNS forwarding

If users from the **Control 2** server cannot reach the Internet, verify that **Control 2** uses the same server as **Control 1**:

1. In the **Control 2** administration interface, go to the **DNS** section.
2. Select **Enable custom DNS forwarding**.
3. Click **Edit**.
4. In the **Custom DNS Forwarding** dialog box, click **Add**.
5. In the **Custom DNS Forwarding** dialog box, select **Match DNS query name** and type * (asterisk).
6. Select **Forward the query** and type the IP address of the **Control 1** DNS server.

Custom DNS Forwarding

DNS query type

☒ Match DNS query name
☐ Match IP address from reverse DNS query
 DNS name:
 Wildcard characters (*, ?) are allowed.

Forwarding

☐ Do not forward
☒ Forward the query
 DNS server(s):
 Use semicolons (;) to separate individual entries.

OK

Cancel

Screenshot 47: Configuring custom DNS forwarding

7. Click **OK** twice.
8. Click **Apply**.

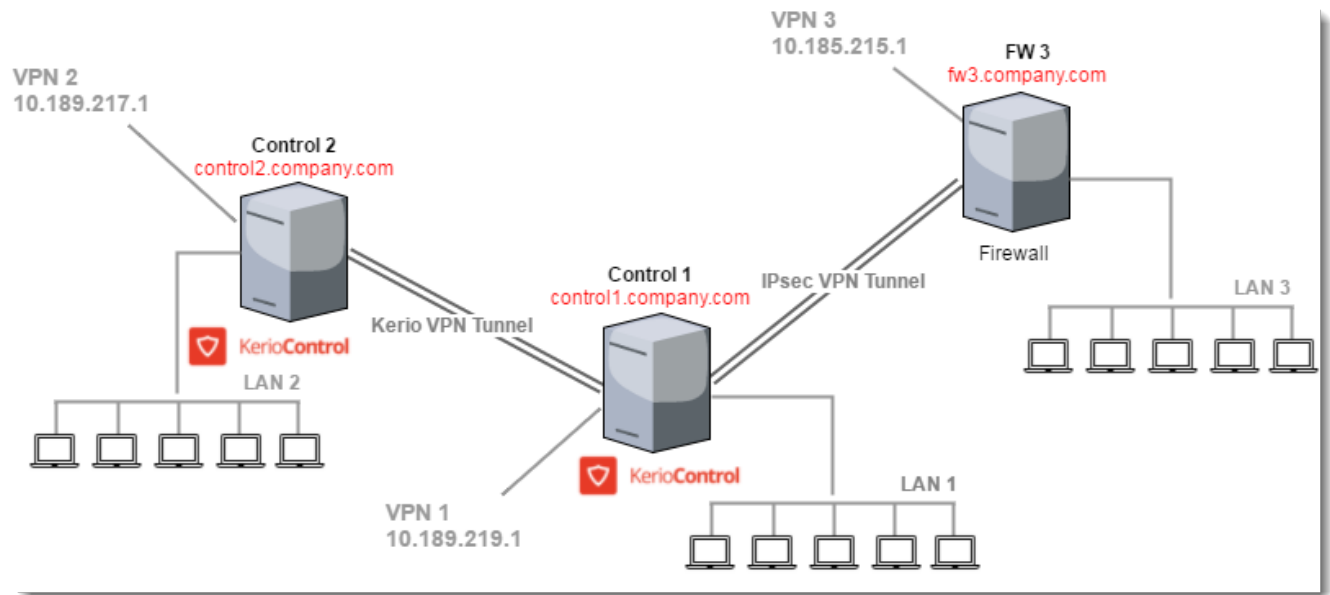
For more information, refer to [DNS forwarding service in Kerio Control](#) (page 323).

3.9.4 Connecting multiple offices via Kerio VPN and IPsec VPN tunnels

In Kerio Control, you can create both Kerio VPN and IPsec VPN tunnels. The article describes, how to configure routes between those two tunnels so that each host sees all other hosts in all subnets in the network.

The Kerio VPN tunnel includes a routing daemon. So, by default, all subnets are visible behind the remote endpoint of the Kerio VPN tunnel. For the IPsec tunnel, you must add all routes manually.

The steps below use the scenario illustrated in the following diagram:



Screenshot 48: Subnets linked by VPN tunnels

Diagram nodes:

- » The **Control 1** server is connected with the **FW 3** server via IPsec tunnel.
- » The **Control 1** server is connected with the **Control 2** server via Kerio VPN Tunnel.
- » The **Control 1** server includes **LAN 1** and **VPN 1** networks.
- » The **Control 2** server includes **LAN 2** and **VPN 2** networks.
- » The **FW 3** server includes **LAN 3** and **VPN 3** networks.

Configuring the Kerio VPN tunnel

For the initial tunnel configuration between **Control 1** and **Control 2**, see [Configuring Kerio VPN Tunnel](#).

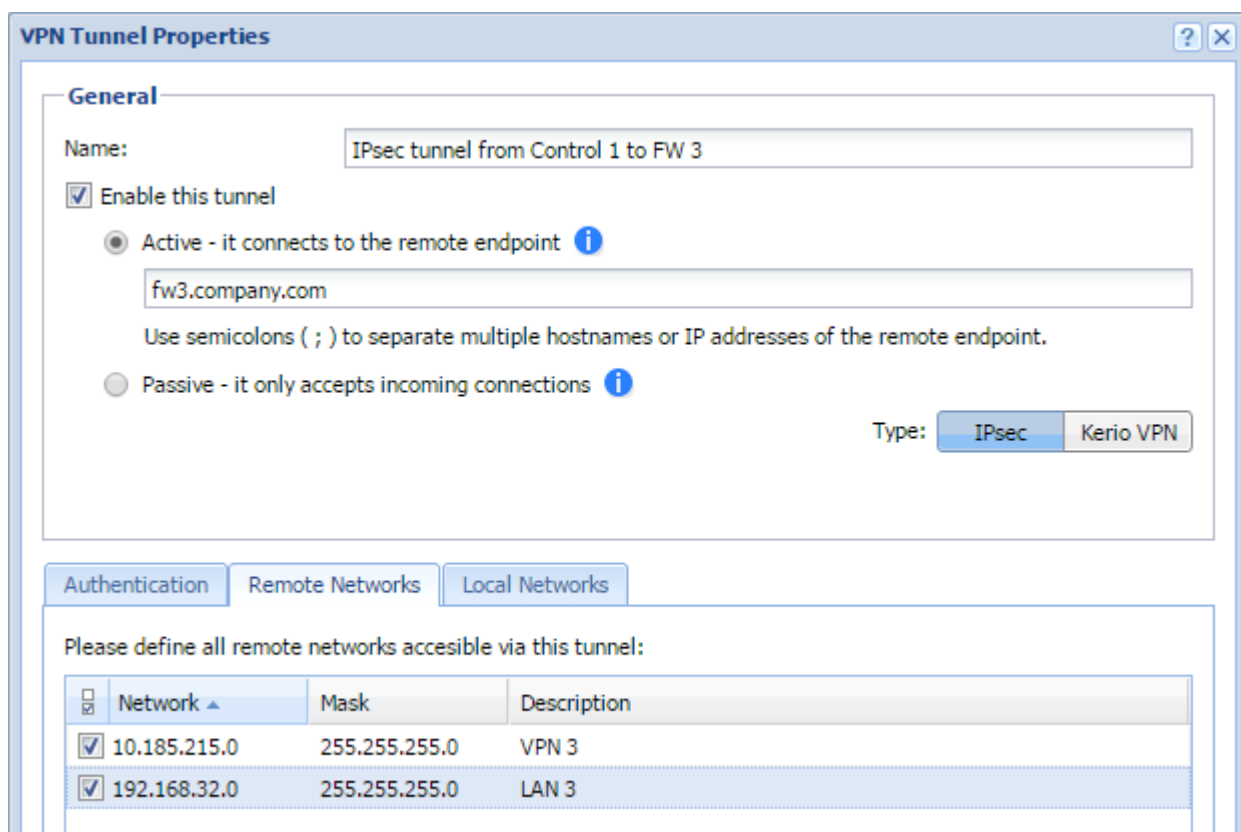
Kerio VPN automatically shares all routes, including the Kerio Control VPN.

Be sure to verify that the tunnel works. For example, send a ping command from a computer connected to **LAN 1** to a computer connected to **LAN 2**, and vice versa.

Also verify that users with VPN clients can ping all computers from **LAN 1** and **LAN 2**.

Configuring the IPsec VPN tunnel

For the initial configuration of the IPsec VPN tunnel, see [Configuring IPsec VPN tunnel](#). When adding remote networks to the **Control 1** server, add **LAN 3** and **VPN 3**.



Screenshot 49: Enabling IPsec VPN tunnel

NOTE

You must also add all **Control 1** routes to the **FW 3** settings.

Verify that the tunnel works. For example, send a ping command from a computer connected to **LAN 1** to a computer connected to **LAN 3**, and vice versa.

Check also that users with VPN clients can ping all computers from **LAN 1** and **LAN 3**.

Configuring Kerio VPN + IPsec VPN interoperability

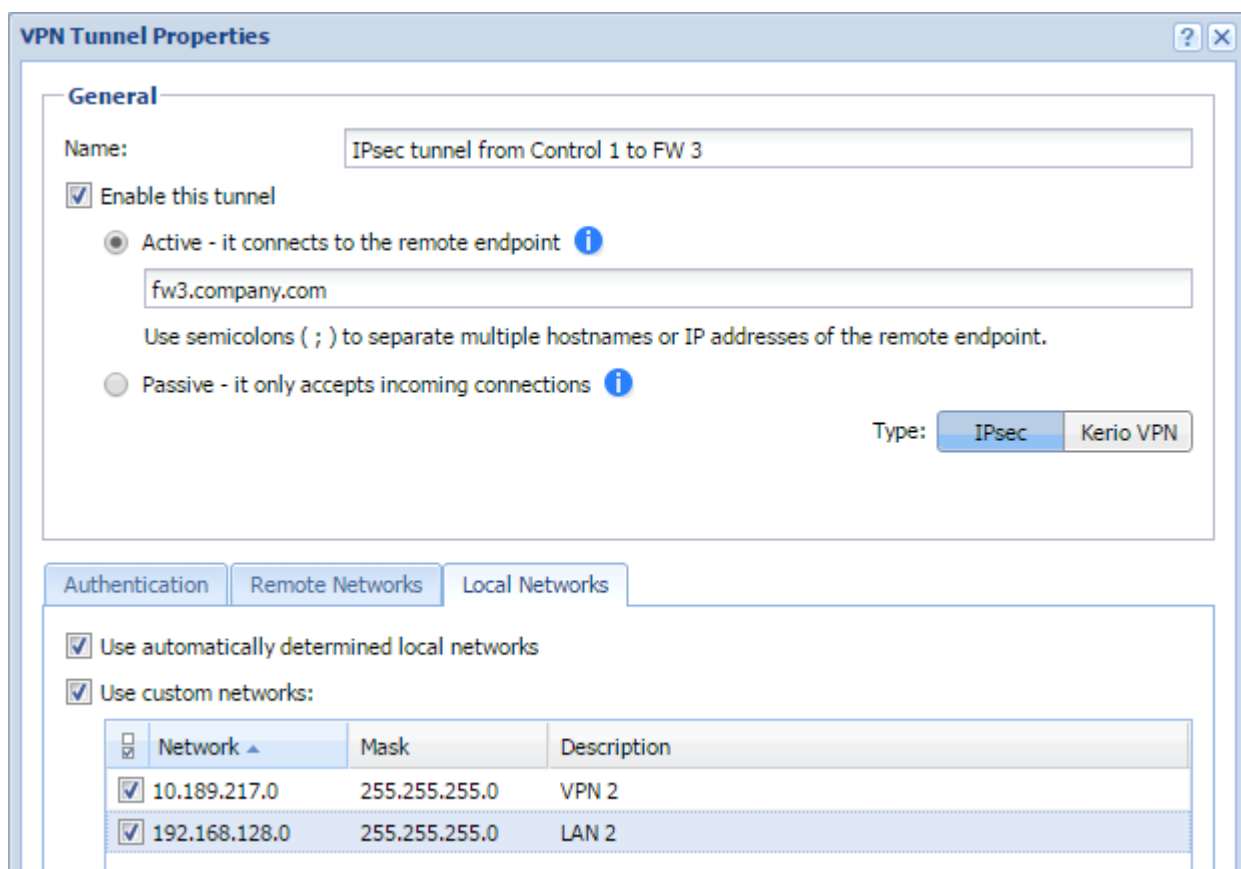
Both tunnels work separately at this point. The next step is to ensure that all users can communicate with each other using both tunnels:

- » To ensure that the IPsec tunnel knows about **LAN 2** and **VPN 2**, add **LAN 2** and **VPN 2** to the local networks of the **Control 1** server.
- » To ensure that **LAN 3** and **VPN 3** communicate with **LAN 2** and **VPN 2**, configure the remote networks of the **Control 2** server.
- » To ensure that **VPN 1** communicates with **LAN 3** and **VPN 3**, add custom routes in the Kerio VPN server settings.
- » On the **FW 3** server, add **LAN 1**, **LAN 2**, **VPN 1** and **VPN 2** to remote networks.

Configuring local networks on Control 1

The **FW 3** server does not see local networks on the **Control 2** server. You must add **LAN 2** and **VPN 2** to the local networks on **Control 1**:

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



VPN Tunnel Properties

General

Name: IPsec tunnel from Control 1 to FW 3

☒ Enable this tunnel

☒ Active - it connects to the remote endpoint **i**

fw3.company.com

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

☐ Passive - it only accepts incoming connections **i**

Type: IPsec Kerio VPN

Authentication Remote Networks Local Networks

☒ Use automatically determined local networks

☒ Use custom networks:

<input type="checkbox"/>	Network ▲	Mask	Description
<input checked="" type="checkbox"/>	10.189.217.0	255.255.255.0	VPN 2
<input checked="" type="checkbox"/>	192.168.128.0	255.255.255.0	LAN 2

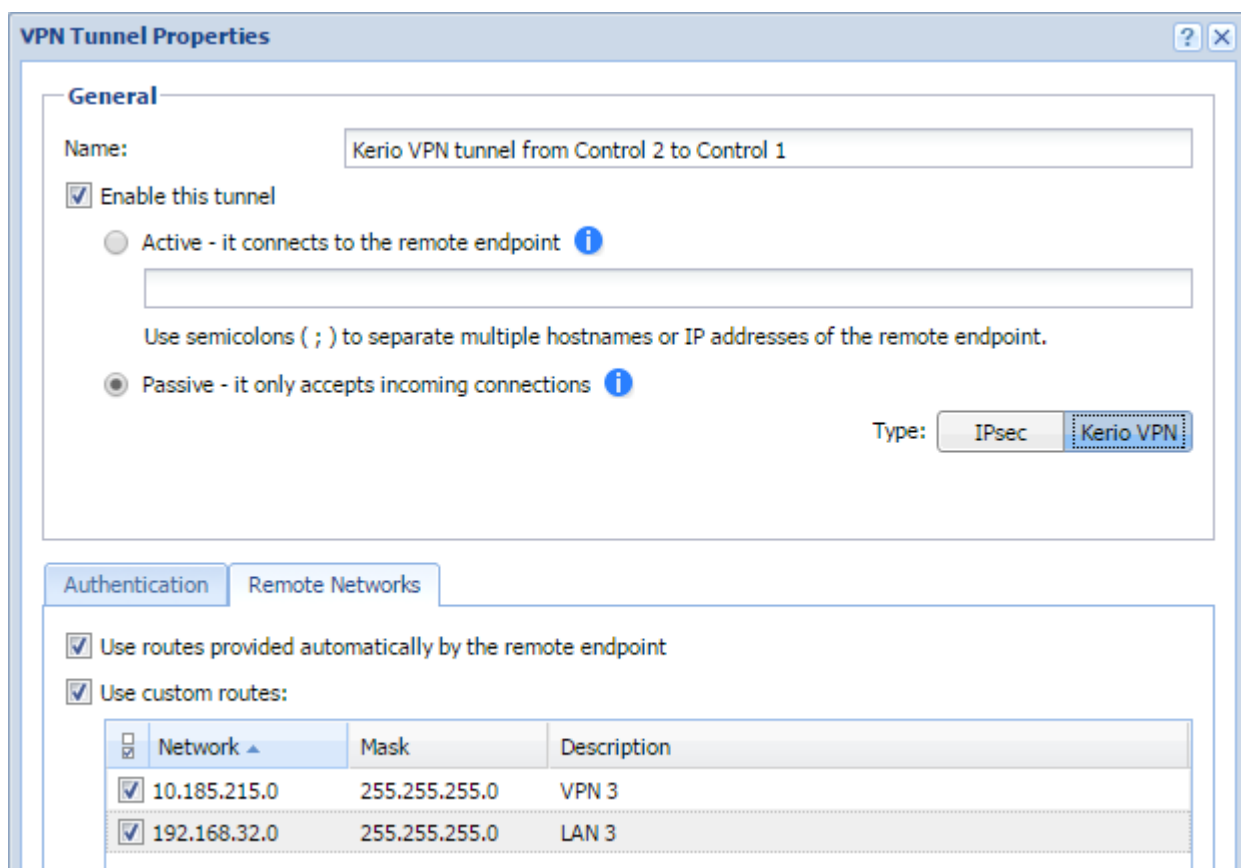
Screenshot 50: VPN tunnel properties

3. On the **Local Networks** tab, select **Use automatically determined local networks**.
4. Select **Use custom networks**.
5. Click **Add**.
6. In the **Add Route** dialog box, define all networks from the remote endpoint of Kerio VPN tunnel, and their masks and descriptions. In our example, the networks are **LAN 2** and **VPN 2**.
7. Click **OK** twice.

Configuring networks for FW 3

The **Control 2** server does not see local networks on the **FW 3** server. You must add all FW 3 routes to the remote networks on **Control 2**.

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



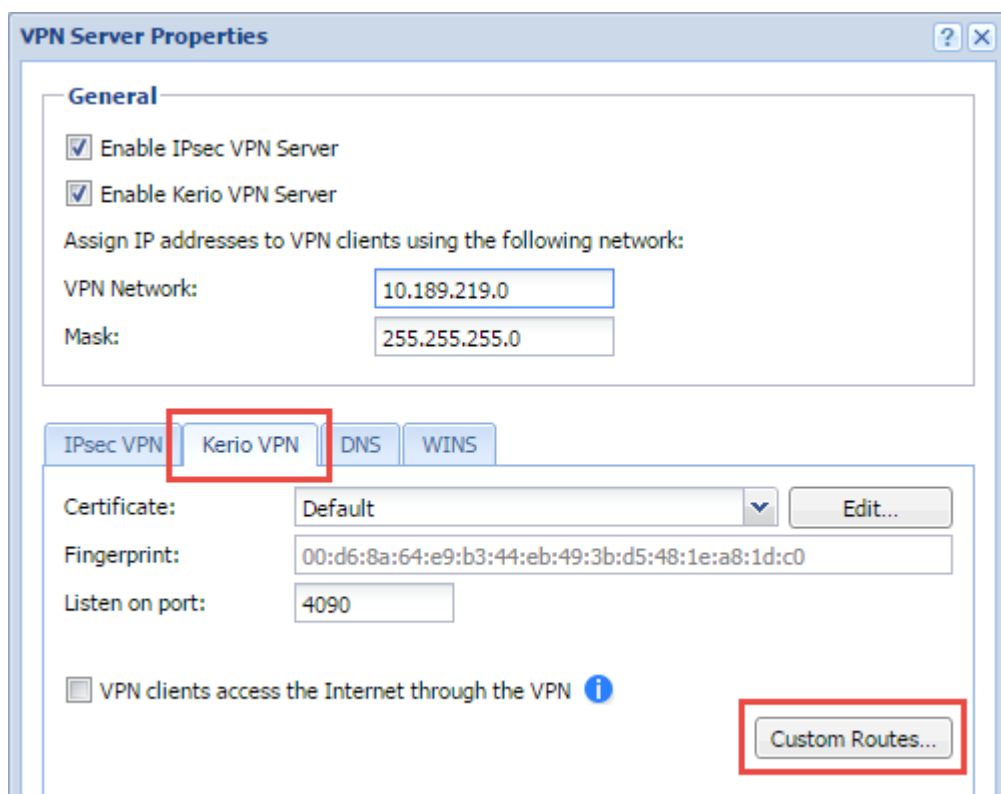
Screenshot 51: Remote Networks configuration

- On the **Remote Networks** tab, select **Use custom networks**
- Click **Add**.
- In the **Add Route** dialog box, define networks on the IPsec tunnel endpoint and their masks and descriptions. In our example, in the networks are **LAN 3** and **VPN 3**.
- Click **OK** twice.

Configuring local routes in Kerio VPN Server

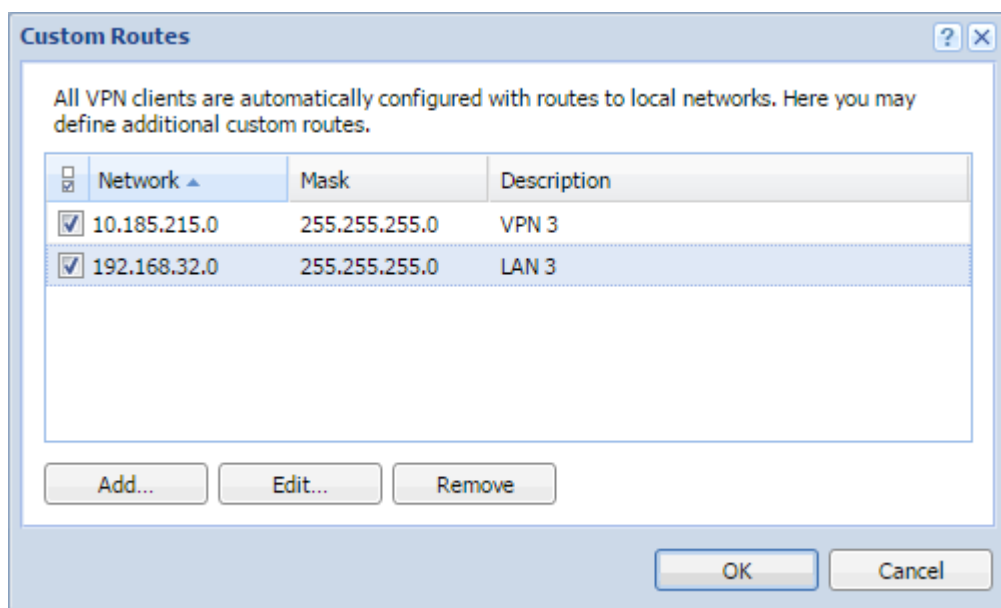
To make **VPN 3** and **LAN 3** visible to users connected through **VPN 1**, you must add **VPN 3** and **LAN 3** to the local routes of the Kerio VPN Server.

- In the **Control 1** administration interface, go to **Interfaces**.
- Double-click **VPN Server**.
- In the **VPN Server Properties** dialog box, click the **Kerio VPN** tab.
- Click **Custom Routes**



Screenshot 52: VPN Server properties

5. In the **Custom Routes** dialog box, add **LAN 3** and **VPN 3**.



Screenshot 53: Adding custom routes

6. Click **OK** twice.

From now on, all users connected through **VPN 1** see all users connected to **VPN 3**.

At this point, the setup is finished. To verify that all computers and VPN subnets in the network can communicate, send multiple ping commands from one network to another.

3.9.5 Assigning static IP addresses for Kerio Control VPN Clients

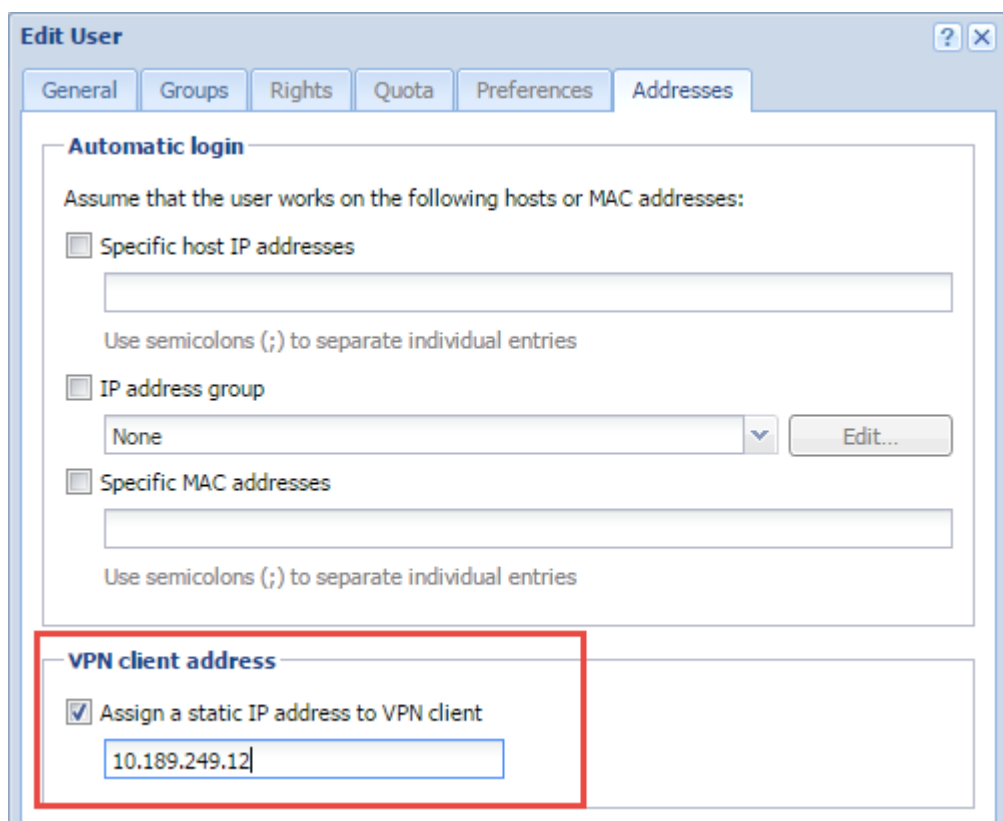
If Kerio Control user needs to access services hosted on the Kerio Control VPN Client, you can assign a static IP address to Kerio Control VPN Client.

NOTES

- » Do not set the same IP address to multiple users, Kerio Control assigns 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.
- » A user with an assigned static Kerio Control VPN Client address can connect to just one device at a time.

To assign static IP address to VPN clients:

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.



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

Screenshot 54: Configuring VPN client address

4. Select **Assign a static IP address to VPN client**.
5. Type the static IP address.
6. Click **OK**

For more information, refer to [Configuring Kerio VPN Server](#) (page 146).

3.9.6 Kerio Control VPN Client for administrators

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.

NOTE

Kerio Control 9.2.8 does not work with previous versions of Kerio Control VPN Client.

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.

NOTE

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. For more information, refer to [Assigning static IP addresses for Kerio Control VPN Clients](#) (page 181).

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 more information go to http://go.gfi.com/?pageid=control_help#cshid=1303
3. (Optional) Consider using 2-step verification. For more information, refer to [Configuring 2-step verification](#) (page 212).

NOTE

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.

3.9.7 Using Logs to troubleshoot VPN Client issues

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`
- » OSX: `/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: `C:\Users\username\AppData\Roaming\Kerio\vpnclient\logs`
- » OSX: `/Users/username/.kerio/vpnclient/logs`

SSL Certificate issues

Check the troubleshooting sections of this manual to find solutions for issues with SSL certificates. For more information, refer to [Troubleshooting SSL certificates](#) (page 354).

4 Settings

This topic contains information about:

4.1 Interfaces	184
4.2 Security	212
4.3 IPv6	228
4.4 Traffic rules	235
4.5 Content filtering	251
4.6 Bandwidth optimization	284
4.7 Proxy server	294
4.8 Server configuration	302
4.9 SSL certificates	343

4.1 Interfaces

This section helps you configure network and virtual interfaces in Kerio Control.

4.1.1 Configuring network interfaces	184
4.1.2 Configuring the guest network	187
4.1.3 Configuring PPPoE connections	190
4.1.4 Configuring PPTP tunnel	191
4.1.5 Configuring TCP/IP settings in Kerio Control interfaces	192
4.1.6 Configuring L2TP tunnel	194
4.1.7 Configuring multiple WAN IPs with PPPoE	196
4.1.8 Configuring VLANs	199
4.1.9 Changing MAC addresses of network interfaces	200
4.1.10 Changing the MTU of network interfaces	201
4.1.11 Changing the speed and duplex settings of Ethernet interfaces	202
4.1.12 Using alert messages	204
4.1.13 Sending log message alerts	208
4.1.14 Using IP Tools	210

4.1.1 Configuring network interfaces

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. For more information, refer to [Configuring the guest network](#) (page 187).
- » **Other Interfaces** — interfaces which do not belong to any of the groups listed above (i.e. dial-like links).

NOTE

If you want to configure WiFi in your Kerio Control NG100W or NG300W, see [Managing WiFi in Kerio Control NG100W and NG300W](#).

Adding new interfaces

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. For more information, refer to [Configuration Assistant](#) (page 10).

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

You can configure interfaces directly in the **Interfaces** section. For more information, refer to [Configuring TCP/IP settings in Kerio Control interfaces](#) (page 192).

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 — For more information, refer to [Configuring PPTP tunnel](#) (page 191).
- » PPPoE — For more information, refer to [Configuring PPPoE connections](#) (page 190).
- » L2TP — For more information, refer to [Configuring L2TP tunnel](#) (page 194).
- » VPN — see [Configuring Kerio VPN tunnel](#) and [Configuring IPsec VPN tunnel](#)

Configuring Ethernet ports

Hardware appliance Edition

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

- » Standalone interface
- » Switch for LAN
- » Not assigned — the port is inactive.

NOTE

It is also possible to use a virtual network (VLAN). For more information, refer to [Configuring VLANs](#) (page 199).

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 is used as a standalone Ethernet interface.
 - **Switch for LAN** — port is a part of the switch which, in Kerio Control, behaves as one Ethernet interface.
 - **Not assigned** — the port is 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 hardware appliance edition.

Related articles

[Managing WiFi in Kerio Control NG100W and NG300W.](#)

[Configuring WiFi guest networks in Kerio Control NG100W and NG300W.](#)

[Wireless bridging on Kerio Control NG100W and NG300W.](#)

[Configuring TCP/IP settings in Kerio Control interfaces](#)

[Configuring VLANs](#)

[Configuring IPv6 networking in Kerio Control](#)

[Configuring Kerio VPN tunnel](#)

[Configuring IPsec VPN tunnel](#)

[Configuring L2TP tunnel](#)

[Configuring PPTP tunnel](#)

[Configuring PPPoE connections](#)

[Changing the MTU of network interfaces](#)

[Changing MAC addresses of network interfaces](#)

[Changing the speed and duplex of Ethernet interfaces](#)

4.1.2 Configuring the guest network

NOTE

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. For more information, refer to [Customizing the welcome page](#) (page 189).
- » 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. For more information, refer to [Setting shared password for guest users](#) (page 189).
- » Kerio Control redirects guest network users to the welcome page after 2 hours of inactivity.

IMPORTANT

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. For more information, refer to [Configuring network interfaces](#) (page 184).

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.

The screenshot shows the 'Interfaces' configuration page in Kerio Control. At the top, there's a section for 'Internet connectivity' with a dropdown menu set to 'A Single Internet Link' and a 'Manage Ports...' button. Below this is a table of interfaces organized into groups. The 'Guest Interfaces' group is highlighted with a red oval and contains one entry: 'Port 8 - Guest Interface' with status 'Up', IPv4 address '192.168.94.2', and port '8'. At the bottom of the page, there are buttons for 'Add', 'Edit...', 'Dial', 'More Actions', 'Apply', and 'Reset'. The 'Add' button is highlighted with a red circle.

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.

For more information, refer to [DHCP server in Kerio Control](#) (page 319).

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.

NOTE

You can format the message in HTML. For more information, refer to [Creating HTML content in your Welcome page](#) (page 189).

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. For more information, refer to [Customizing the welcome page](#) (page 189).

Traffic rules for the guest network

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

Traffic Rules							
<div> <div>Search:</div> <div> <div>Test Rules</div> <div>Restore View</div> </div> </div>							
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

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. For more information, refer to [Services in Kerio Control](#) (page 337).

IMPORTANT

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

4.1.3 Configuring PPPoE connections

Kerio Control supports PPPoE (Point-to-point protocol over Ethernet). Some Internet providers use PPPoE to create tunnels for connecting you to the Internet.

Configure a PPPoE interface if your provider requires this protocol. You can:

- » Establish a single Internet link by configuring a [PPPoE mode in the Internet interface](#).
- » Create another interface to the Internet by adding a [PPPoE tunnel](#).

Prerequisites

You need the following information from your provider:

- » Username
- » Password

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.

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. Click **OK**
7. Click **Apply**.

The new connection is displayed as **Up** in the **Interfaces** section. The Internet connection is established.

Configuring PPPoE tunnel

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.

NOTE

If you set the interface to **Any**, Kerio Control automatically selects the appropriate interface which is 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 demands manual dialing. The link can be hung up automatically after defined period of idleness.

The new tunnel is displayed as **Up** in the **Interfaces** section. The Internet connection is established.

4.1.4 Configuring PPTP tunnel

Kerio Control supports PPTP (Point-to-Point Tunneling Protocol). Some Internet providers use PPTP to create tunnels for connecting you to the Internet.

Configure a PPTP interface if your provider requires this protocol.

Prerequisites

You need the following information from your provider:

- » PPTP server hostname
- » Username and password for PPTP server access

Configuring PPTP tunnel

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.

The new tunnel is displayed as **Up** in the **Interfaces** section. The Internet connection is established.

4.1.5 Configuring TCP/IP settings in Kerio Control interfaces

This article describes how to configure IP addresses, gateways and DNS servers in Kerio Control.

Configuring IPv4 settings

Each Kerio Control interface in the **Internet**, **Trusted/Local**, and **Other** Interfaces groups can be set up in either of two modes:

- » **Automatic** mode is used if Kerio Control detects a DHCP server on the interface and receives an IP address from DHCP.
- » **Manual** (static) mode is used if Kerio Control cannot detect a DHCP server on the interface. This is typically all interfaces in the **Trusted/Local Interfaces** and **Other Interfaces** groups. If Kerio Control does not detect a DHCP server on the interface, it runs its own DHCP server through all **Trusted/Local Interfaces** and **Other Interfaces** configured to **10.10.X.Y**, where **X** is the index of the LAN interface (starting with 10) and **Y** is 1 for the Control interface and 11-254 for DHCP assigned hosts. However, the interface properties stay in **Manual** mode, because the configuration is static and IP addresses do not change.

Ethernet Interface Properties

General

Name: WAN

Interface Group: Internet Interfaces

☒ Enable this interface

Mode: Native PPPoE

IPv4 IPv6 VLAN

☒ Enable

Configuration: Automatic

IP address: 192.168.64.198

Mask: 255.255.255.0

Gateway: 192.168.64.1 ☒ Autodetect

DNS server: 10.11.11.3;10.11.11.4;192.168.1 ☒ Autodetect

Advanced...

OK Cancel

Ethernet Interface Properties

General

Name: LAN

Interface Group: Trusted/Local Interfaces

☒ Enable this interface

Mode: Native PPPoE

IPv4 IPv6 VLAN

☒ Enable

Configuration: Manual

IP address: 10.10.10.2

Mask: 255.255.255.0

Gateway:

DNS server:

Define Additional IP Addresses...

Advanced...

OK Cancel

WARNING

Do not type the default gateway to local network interfaces (**Trusted/Local Interfaces**, **Other Interfaces** and **Guest Interfaces** groups).

To configure the interface properties manually:

1. In the Kerio Control administration interface, go to **Interfaces**.
2. Double-click the interface.
3. In the **Interface Properties** dialog box, select the **Native** mode. The **Native** term means settings for persistent connection. If you need to set up a DSL connection through and use PPPoE, see [Configuring PPPoE connections](#).
4. Click the **IPv4** tab.
5. In the **Configuration** drop-down list, select **Manual**.
6. Type the **IP address**, **Mask**, **Gateway**, and **DNS server** information manually.
7. Click **OK**.
8. Click **Apply**.

When you configure TCP/IP values, the routing table is updated automatically. For more information, refer to [Configuring a routing table in Kerio Control](#) (page 303).

Configuring gateways and DNS servers in the Automatic mode

Although an interface is in the **Automatic** mode, you can configure the gateway and DNS servers manually:

1. In the administration interface, go to **Interfaces**.
2. Double-click the interface.
3. In the **Interface Properties** dialog box, click the **IPv4** tab.
4. In the **Configuration** drop-down list, select **Automatic**.
5. In the **Gateway** field, deselect **Autodetect**.
6. Type the gateway.
7. In the **DNS server** field, deselect **Autodetect**.
8. Type the DNS servers separated by semi-colon.
9. Click **OK**.
10. Click **Apply**.

Verify that the interface is **Up** and you can access the Internet through the interface.

Configuring IPv6 settings

IPv6 settings are completely independent of IPv4 settings.

IPv6 settings for network interfaces have three possible modes:

- » **Automatic** — Kerio Control supports SLAAC.
- » **Manual**
- » **Link-Local only** — In this mode, the interface supports only the Link-Local addresses and sees only devices in the subnet.

By default, IPv6 is disabled on all interfaces. For more information, refer to [Configuring IPv6 networking in Kerio Control](#) (page 228).

Related articles

[Configuring network interfaces](#)

[Configuring VLANs](#)

[Configuring IPv6 networking in Kerio Control](#)

[Configuring Kerio VPN tunnel](#)

[Configuring IPsec VPN tunnel](#)

[Configuring L2TP tunnel](#)

[Configuring PPTP tunnel](#)

[Configuring PPPoE connections](#)

[Changing the MTU of network interfaces](#)

[Changing MAC addresses of network interfaces](#)

[Changing the speed and duplex of Ethernet interfaces](#)

4.1.6 Configuring L2TP tunnel

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. For more information, refer to [Configuring IPsec VPN Server](#) (page 154). 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.
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.

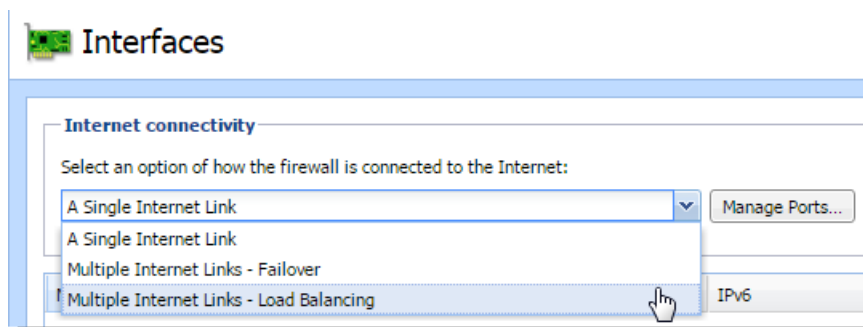
When the **Status** is **Up** in the **Interfaces** section, the L2TP tunnel is active.

Go to **Dial** log for more details about L2TP communications and dialing the line. For more information, refer to [Using the Dial log](#) (page 132).

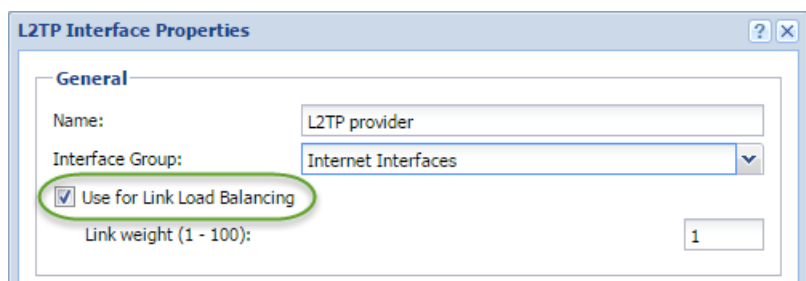
Configuring L2TP tunnel with public IP address

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

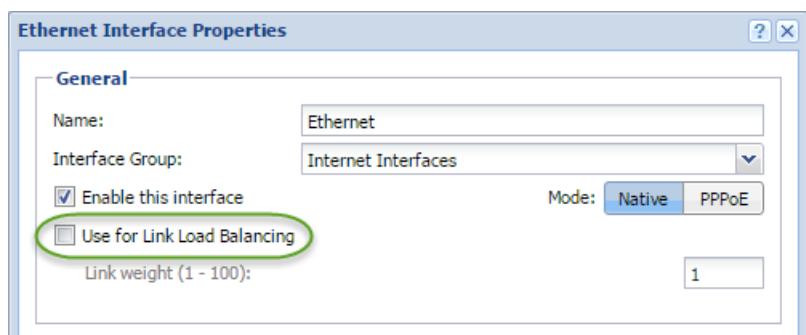
1. In the administration interface, go to **Interfaces**.
2. Change **Internet connectivity** to **Multiple Internet Links - Load Balancing**.



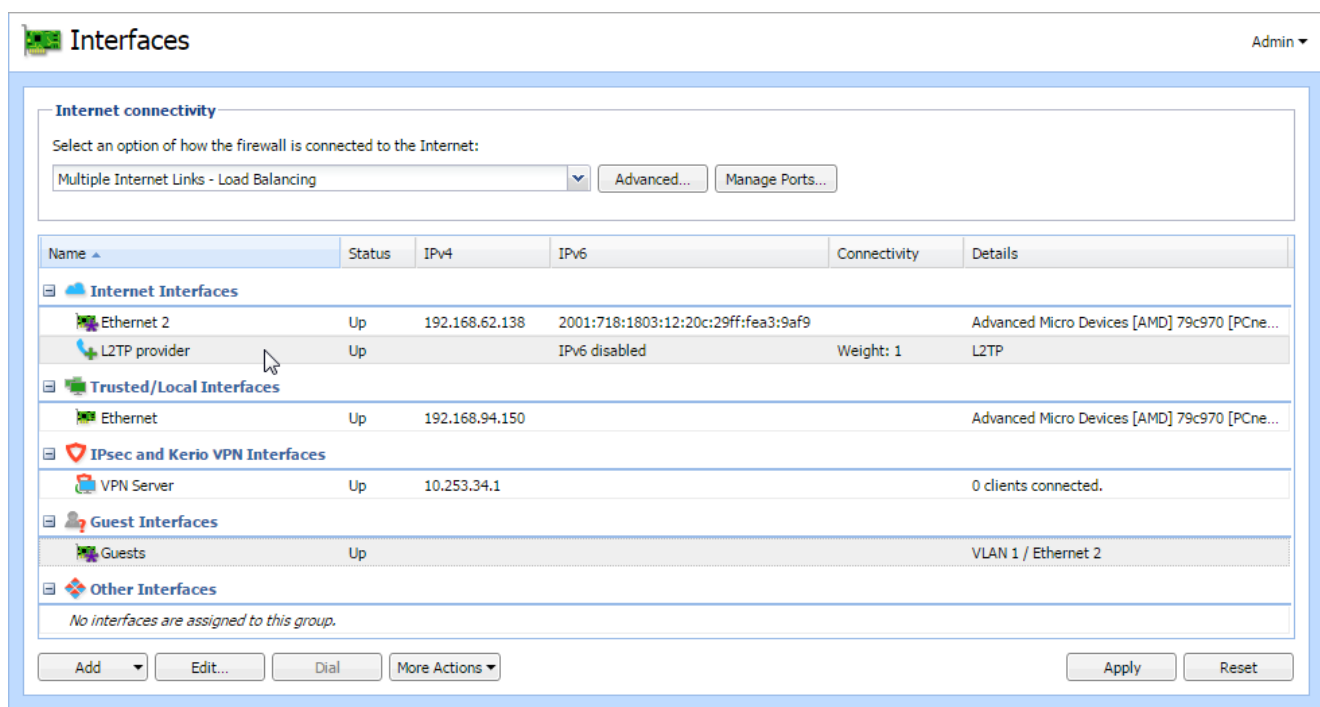
3. Add L2TP tunnel (see above).
4. In **Interface Group**, select **Internet Interfaces**.
5. Enable **Use for Link Load Balancing** in the **L2TP Interface Properties** dialog.



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



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 communication and dialing the line. For more information, refer to [Using the Dial log](#) (page 132).

4.1.7 Configuring multiple WAN IPs with PPPoE

Some Internet Service Providers will route multiple static IP addresses over a PPPoE connection. This article covers the necessary configuration within the appliance edition of Kerio Control.

Details

PPPoE is a type of tunneled, or encapsulated link, which is established over top of a physical network interface. In relation to Kerio Control, this means that IP Addresses assigned to the physical interface can be routed through the PPPoE link. Since the gateway is assigned by the PPPoE link, no default gateway should be defined on the physical Interface to which the PPPoE link is bound.

Configuration

From the web administration, go to **Interfaces** and edit the Interface which is connected to the modem. Define one of the static IP addresses and subnet mask assigned by your ISP. Do not provide a gateway. DNS values are optional, as in most cases they will be assigned by the PPPoE link. Click **Define Additional IP Addresses...** button to add the additional IP addresses assigned by your ISP. Apply the changes.

Ethernet Interface Properties ? X

General

Name: WAN

Interface Group: Internet Interfaces

☒ Enable this interface Mode: Native PPPoE

IPv4 IPv6 VLAN

☒ Enable

Configuration: Manual

IP address: 198.51.100.1

Mask: 255.255.255.248

Gateway:

DNS server: 8.8.8.8

Define Additional IP Addresses...

Advanced...

OK Cancel

Additional IP Addresses ? X

IP Address	Mask
198.51.100.1	255.255.255.248
198.51.100.2	255.255.255.248
198.51.100.3	255.255.255.248
198.51.100.4	255.255.255.248

Add... Edit... Remove

OK Cancel

Back in the **Interfaces** section, click **Add > PPPoE**. Configure the Username and Password for your PPPoE account, and define any connection intervals if necessary.

PPPoE Interface Properties

General

Name:

Interface Group:

Dialing Settings

Interface:

Username:

Password:

☒ Keep connected in the following time interval:

☐ Keep disconnected in the following time interval:

☐ Hangup if idle for minutes.

After the PPPoE interface is added, the connection will be dialed and the gateway and DNS values will be assigned to the PPPoE interface.

Name ▲	Status	IPv4
Internet Interfaces		
WAN	Up	198.51.100.1
PPPoE	Up	198.51.100.5

4.1.8 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.
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.

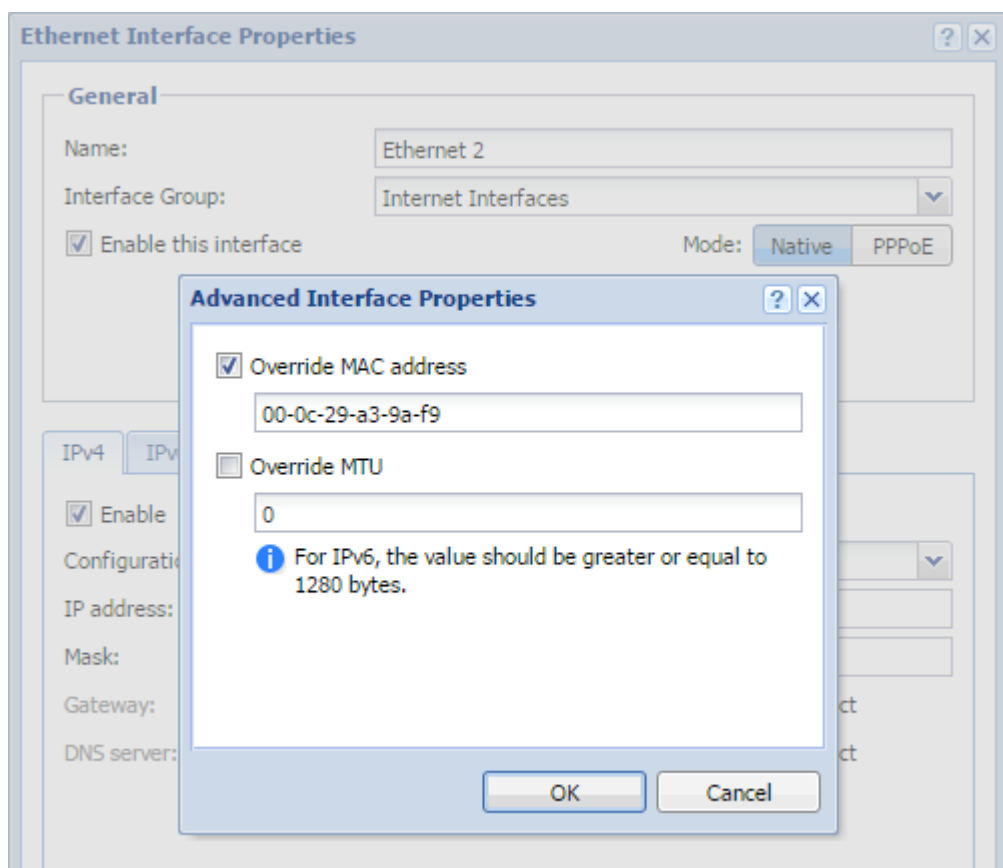
4.1.9 Changing MAC addresses of network interfaces

A MAC address identifies devices in a network. Some routers or Internet service providers permit only specific MAC addresses for specific devices. When you need to use a device or network adapter with a different 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.

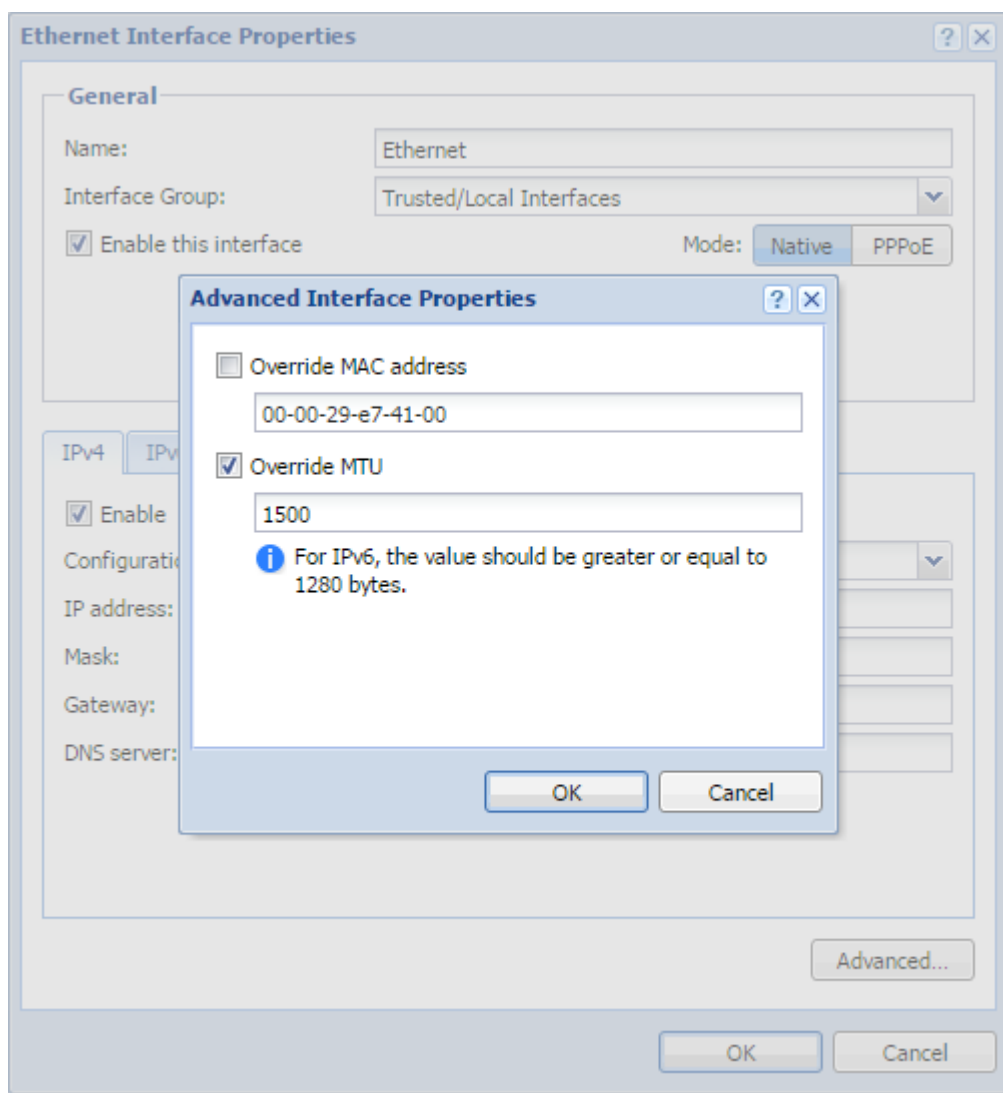
The interface now uses the newly configured MAC address.

4.1.10 Changing the MTU of network interfaces

The MTU (maximum transmission unit) is the maximum size of an IP packet that can be transmitted without fragmentation. If your network device requires a specific MTU (as, for example, some types of modems do), you can define the MTU in the Kerio Control interface.

Changing the MTU

1. In the administration interface, go to **Interfaces**.
2. Double-click the interface.
3. In the **Interface Properties** dialog box, click **Advanced**.



4. In the **Advanced Interface Properties** dialog box, select **Override MTU** and type the value in bytes. For ADSL, the MTU value is 1492 or less. See documentation for your ADSL modem.

5. Click **OK** twice.

The interface now uses the newly configured MTU.

4.1.11 Changing the speed and duplex settings of Ethernet interfaces

Typically, the port speed and duplex mode of Ethernet interfaces is negotiated and set automatically between hardware devices.

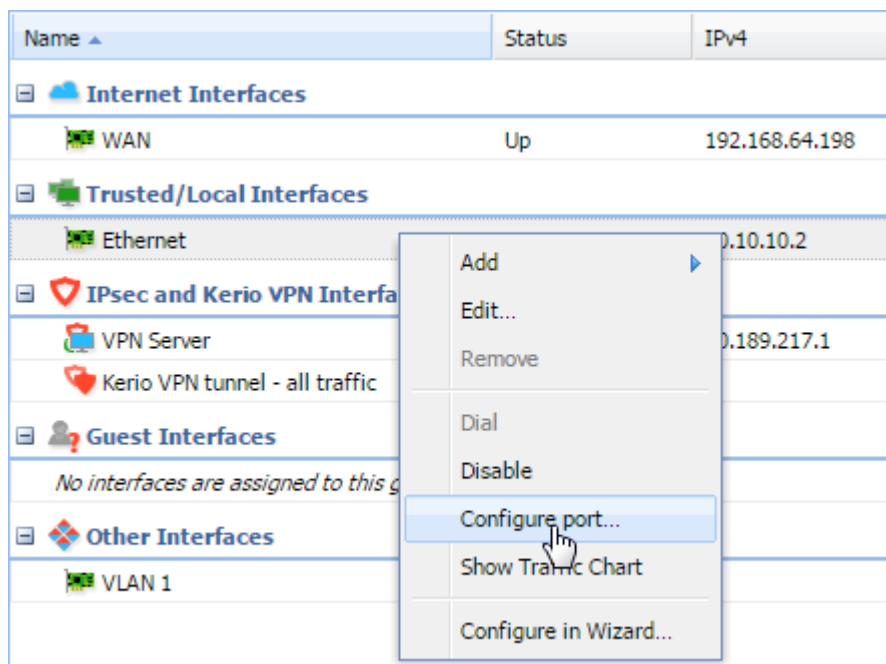
Some (usually older) hardware devices do not auto-detect speed and duplex mode, but instead use a hard-set speed and duplex mode. In this case, when Kerio Control attempts to auto detect the speed of connected devices, it fails. This results in packet loss and poor line speed.

To optimize the Internet connection, find the correct speed and duplex mode for the device and configure the same values in Kerio Control.

Changing speed and duplex mode

Setting speed and duplex mode must be done separately for each interface:

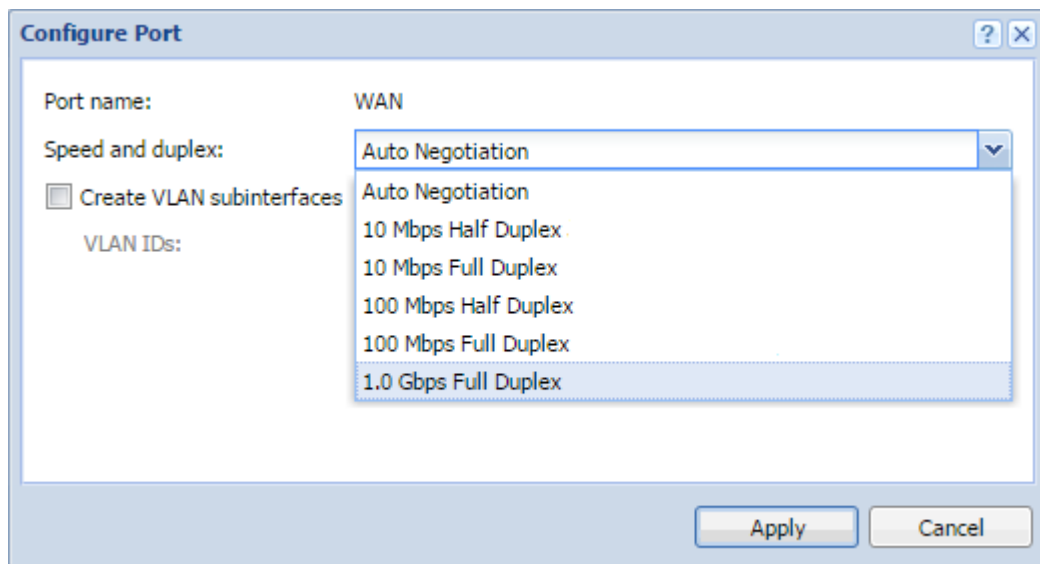
1. In the Kerio Control administration interface, go to **Interfaces**.
2. Right-click the interface.
3. In the context menu, select **Configure port**.



4. In the **Configure Port** dialog box, select the speed and duplex mode.

NOTE

Kerio Control Software Appliance only: some values may not be supported.



5. Click **OK**.
6. Click **Apply**.

The speed of the Internet connection and duplex mode is the same as on the other hardware device.

4.1.12 Using alert messages

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

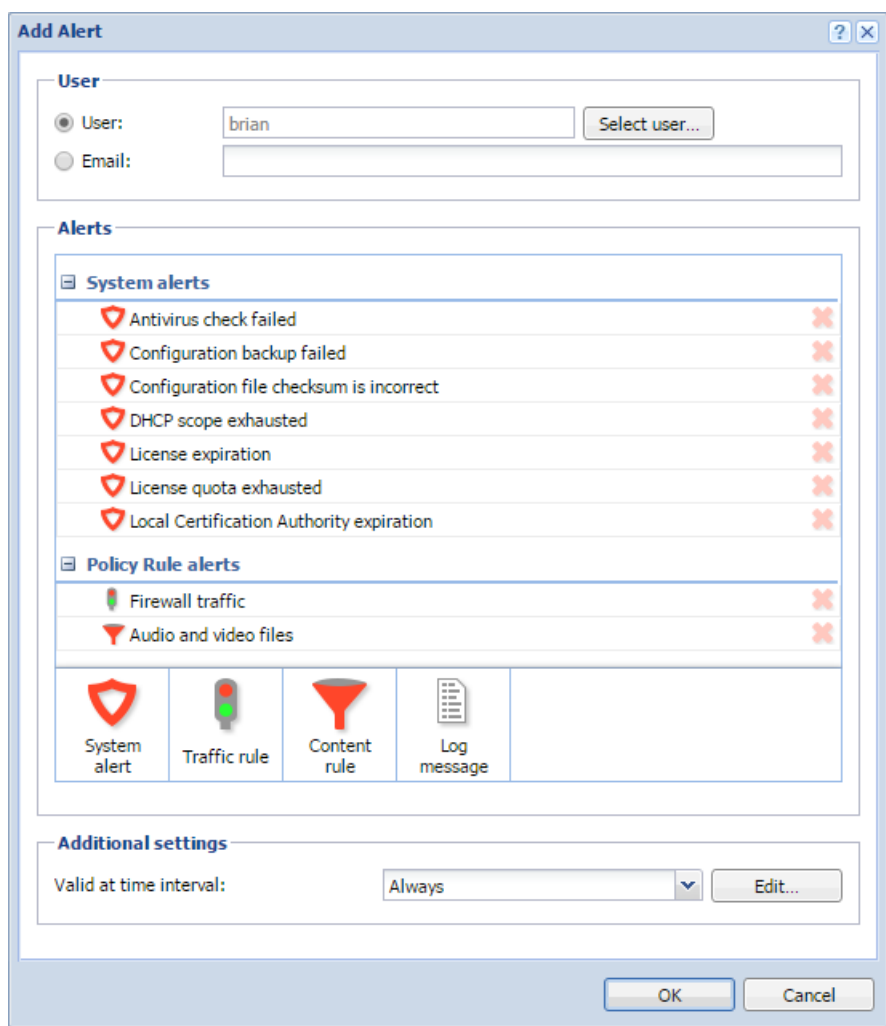
- » Default alert language
- » Recipients
- » Alert types
- » Timing

NOTE

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. For more information, refer to [System alerts](#) (page 206).
 - 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. For more information, refer to [Sending log message alerts](#) (page 207).

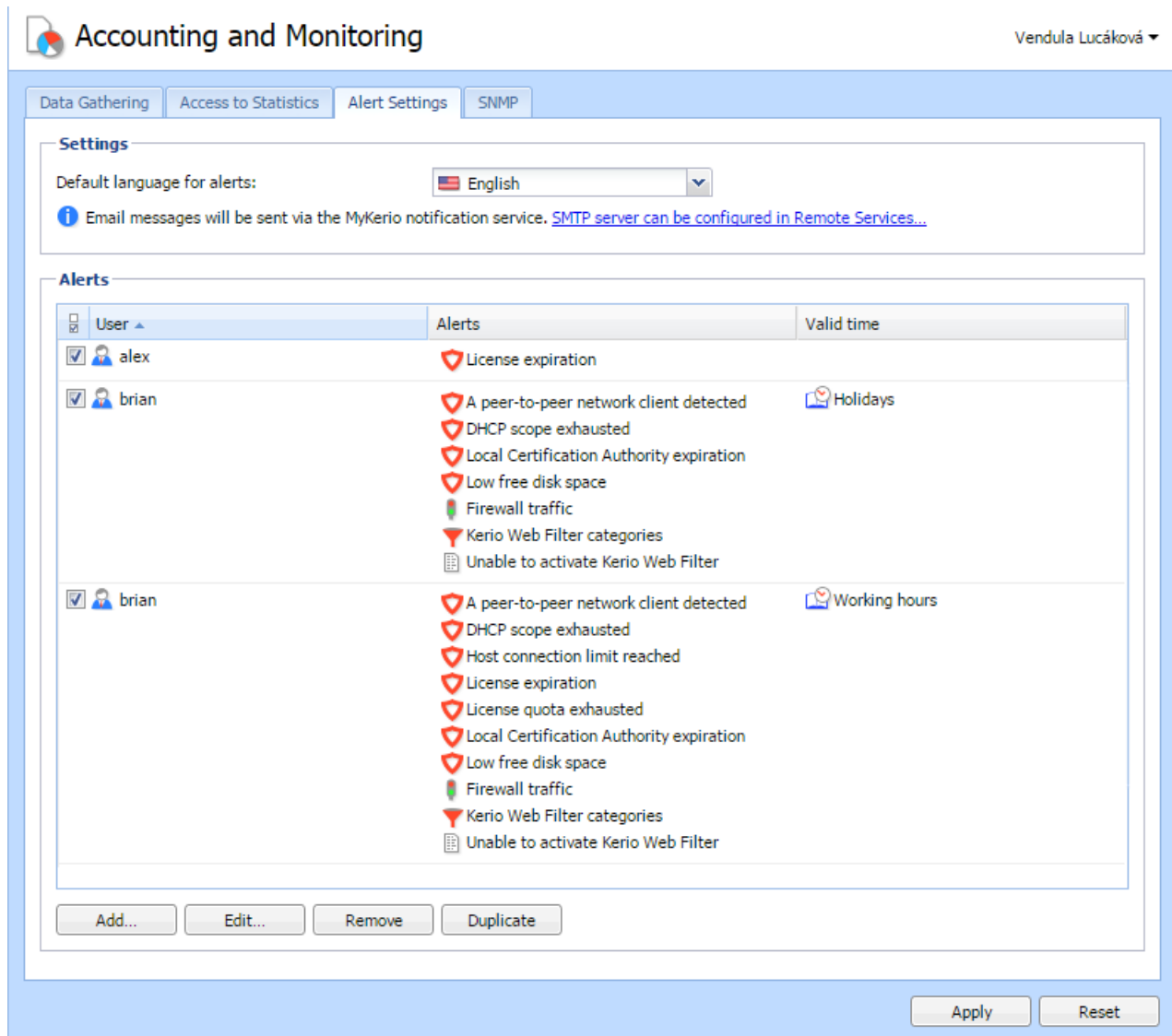


7. Configure the alert and click **OK** and the **Add Alert** dialog displays the list of active alerts, grouped by type. You can add more particular alerts for a selected recipient.

8. When you have finished adding alerts, select a time interval in which Kerio Control sends the alerts. For more information, refer to [Creating time ranges in Kerio Control](#) (page 338).

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.



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 information, refer to [DHCP server in Kerio Control](#) (page 319).
- » **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 Kerio 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, refer to [Filtering HTTPS connections](#) (page 275).
- » **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.

NOTE

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.

NOTE

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 more information, refer to [Sending log message alerts](#) (page 208).

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

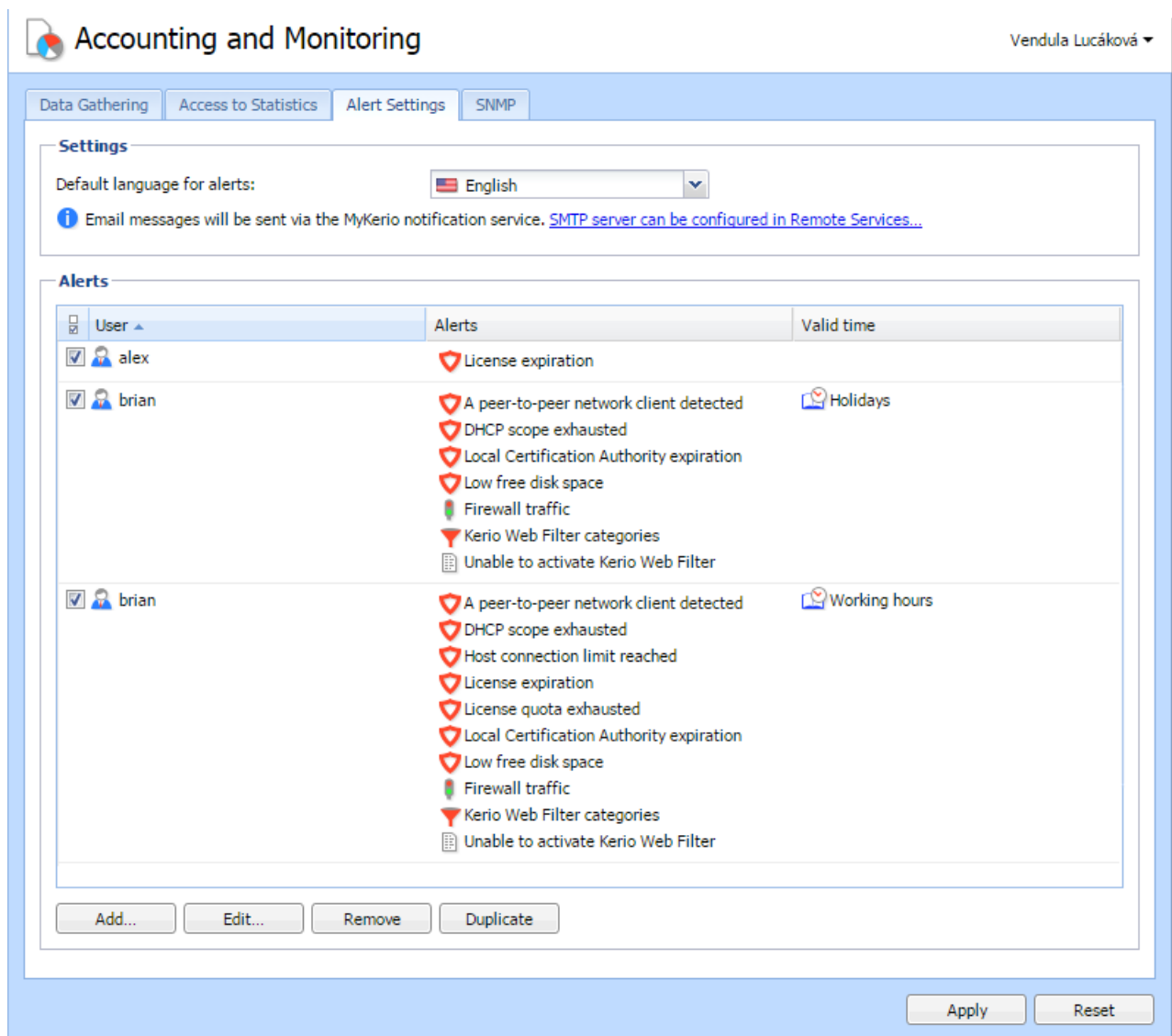
All system alert messages are recorded in the **Alert** log.

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.

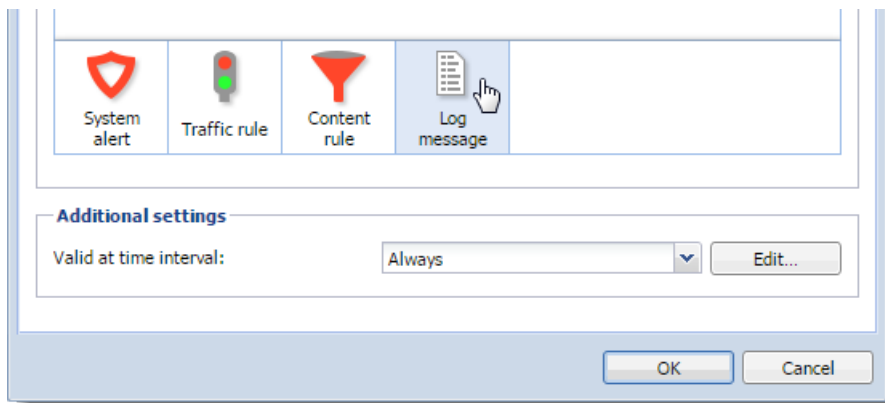
4.1.13 Sending log message alerts

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



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**.

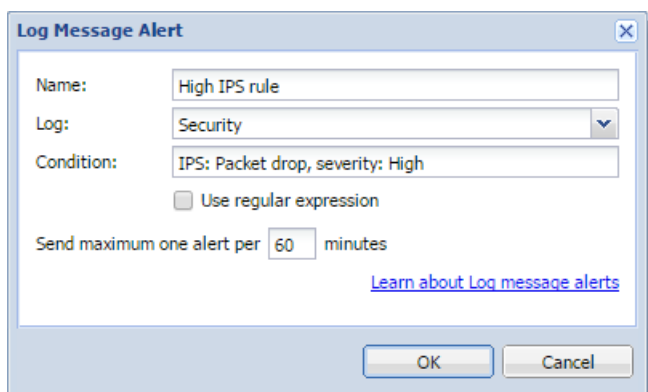


3. In the **Log Message Alert** dialog box, type a name for the alert. The name appears in the subject line of the email message the alert sends.
4. From the **Log** menu, select the log type.
5. In the **Condition** field, type the text string you want Kerio Control to search for. Kerio Control compares 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**

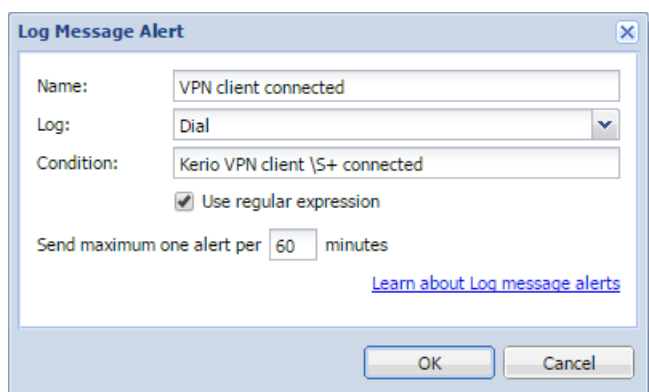
Kerio Control sends the alert whenever the condition matches a text string in the log.

Examples of log alerts

High severity IPS events



VPN client connected (regular expressions)



Log Message Alert

Name: VPN client connected

Log: Dial

Condition: Kerio VPN client \S+ connected

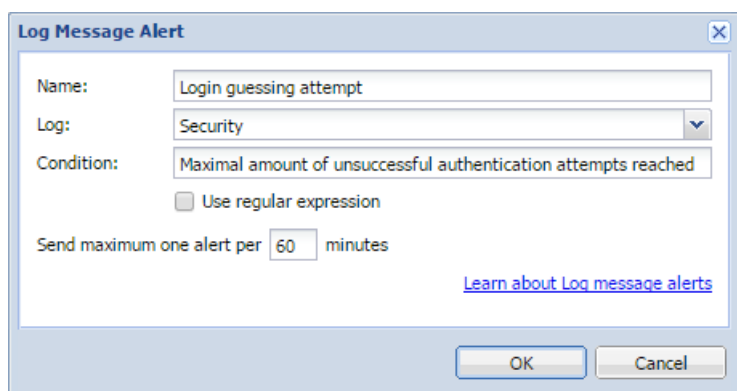
☒ Use regular expression

Send maximum one alert per 60 minutes

[Learn about Log message alerts](#)

OK Cancel

Login guessing attempt



Log Message Alert

Name: Login guessing attempt

Log: Security

Condition: Maximal amount of unsuccessful authentication attempts reached

☐ Use regular expression

Send maximum one alert per 60 minutes

[Learn about Log message alerts](#)

OK Cancel

4.1.14 Using IP Tools

Kerio Control includes several tools 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 IP Tools, input a value and parameters into the appropriate fields. Choose the 'start' button and refer to the Command output window.

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.

NOTE

Some hosts may filter ping requests, in which case ping cannot accurately test connectivity to that host.

Parameters for Ping

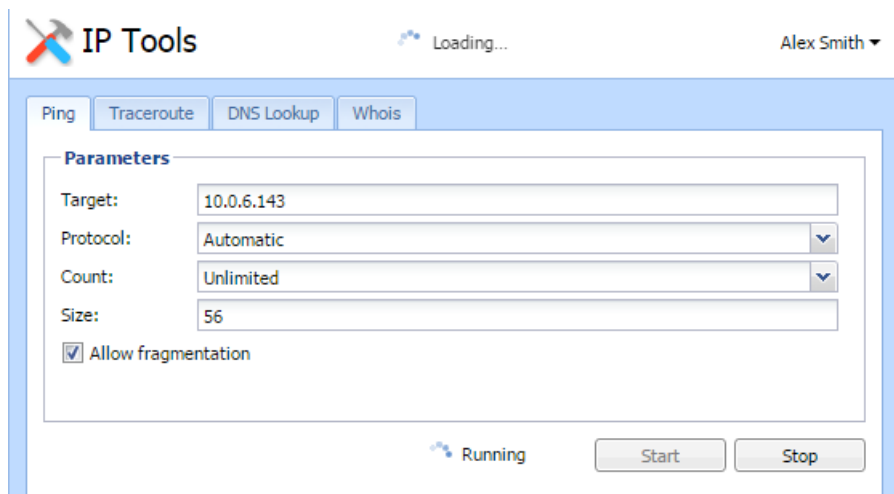
Target — IP address or hostname of the remote host

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 fragmented 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 the response time is very slow, you can use traceroute to determine where the problem may be introduced.

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

The Domain Name System (DNS) translates easily memorized names into IP addresses. A DNS lookup is the process of querying 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 (e.g. www.kerio.com)

Tool — specifies the used tool and 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 (e.g. 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 of 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 may perform a 'whois' lookup against the offending host.

Input an IP address or hostname into the 'Host' field to perform a whois query.

4.2 Security

This section helps you secure your network with Kerio Control.

4.2.1 Configuring 2-step verification	212
4.2.2 Blocking all incoming connections from specified countries in Kerio Control	215
4.2.3 Configuring connection limits	217
4.2.4 Configuring intrusion prevention system	221
4.2.5 Filtering MAC addresses	222
4.2.6 Protecting users against password guessing attacks	223
4.2.7 Protocol inspection in Kerio Control	224
4.2.8 Encrypting User Data	227

4.2.1 Configuring 2-step verification

NOTE

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.

NOTE

It is possible to enable the option to force hostname for clients connected via the Kerio VPN for 2-factor authentication. For more information, refer to [Configuring Hostname Settings](#)

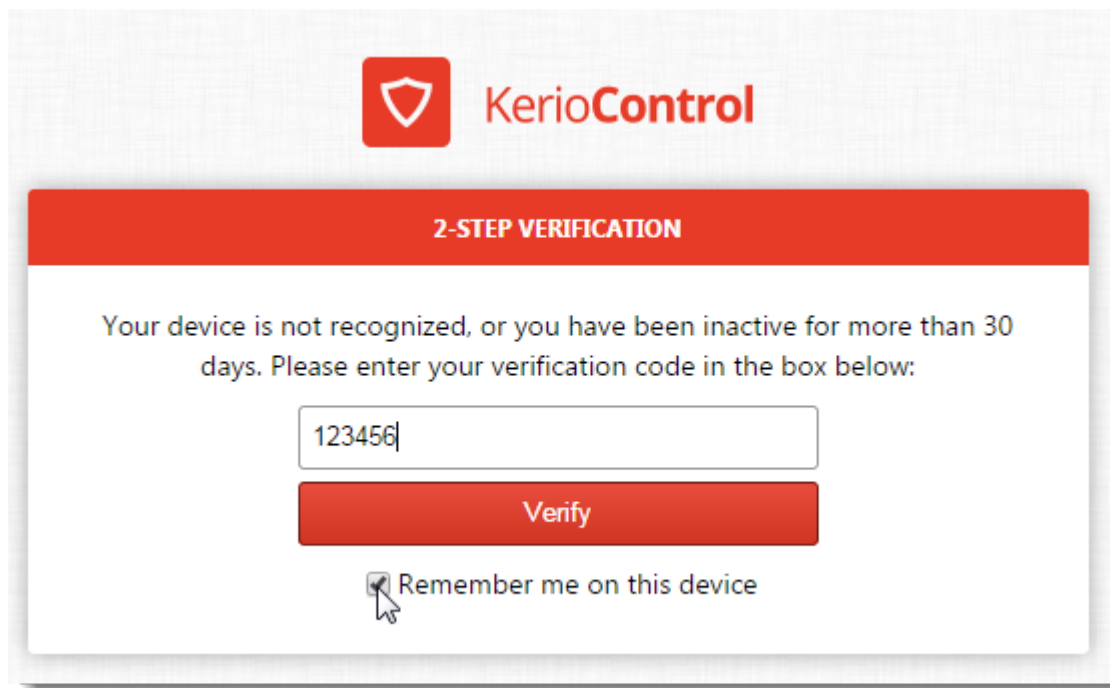
This type of verification protects access to Kerio Control and your LAN from the Internet with two independent steps. Users must use their credentials to authenticate and also type a special time-limited code generated by an authentication application on their phones or computers that supports RFC 6238, 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://mattrubin.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.



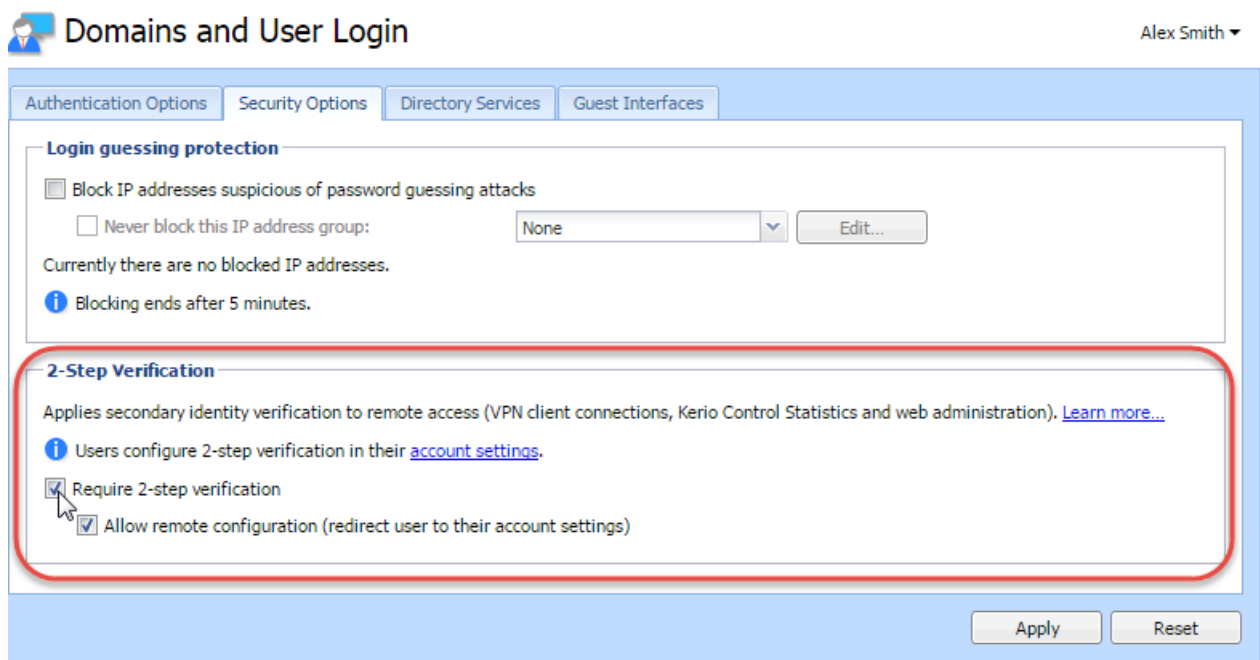
Configuring the 2-step verification in Kerio Control Administration

Users can set up their 2-step verification in Kerio Control Statistics themselves. For more information go to http://go.gfi.com/?pageid=control_help#cshid=1698

As an 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**.

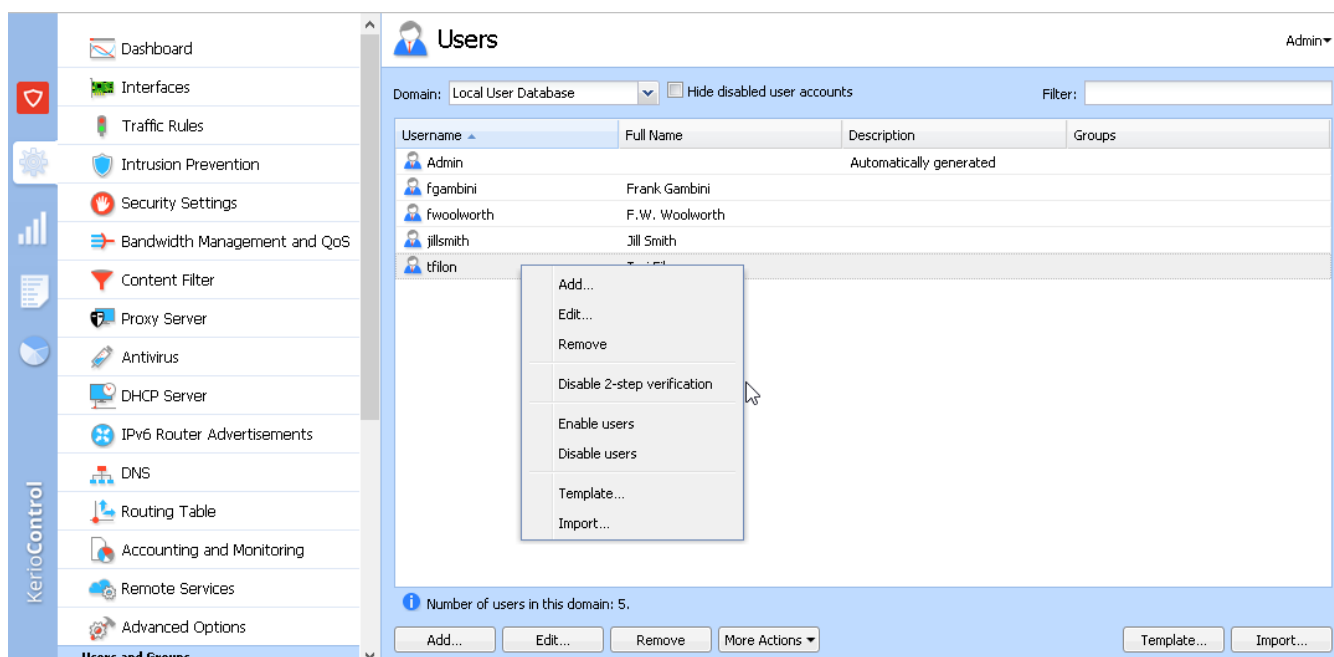
Kerio Control now starts to require the 2-step verification. Users must pair their mobile devices with their Kerio Control account. They authenticate to the Kerio Control network with their credentials and a verification code.

Disabling the 2-step verification for a particular user

If a user loses the mobile device associated with 2-step verification, you must disable the 2-step verification for that user account. Otherwise, the user cannot access the Kerio Control network from the Internet. There are two ways to disable 2-step verification on a user account:

Using the context menu in Users administration to disable 2-step verification

1. In 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 **Disable 2-step verification**.



Screenshot 55: The context menu displayed in the Users administration panel.

Using the More Actions button in Users administration to disable 2-step verification

1. In Kerio Control Administration, go to **Users and Groups > Users**.
2. Click the user account you want to disable 2-step verification for
3. Click **More Actions > Disable 2-step verification**

The user can now enable 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 go to http://go.gfi.com/?pageid=control_help#cshid=1698

4.2.2 Blocking all incoming connections from specified countries in Kerio Control

NOTE

New in Kerio Control 9.2!

Kerio Control allows you to enable a GeoIP filter for incoming traffic. This filter helps you effectively stop malicious traffic and potential threats.

The GeoIP filter matches each IP address to its source country and displays the result in the **Active Connections** section. You can see any suspicious connections there and block all traffic from a given country.

Displaying countries in Active Connections

To display the countries associated with IP addresses in **Active Connections**, enable the GeoIP filter and display the **Source Country** and **Destination Country** columns in **Active Connections**:

1. In the administration interface, go to **Security Settings > GeoIP Filter**.
2. Select **Block incoming traffic from the following countries**.

3. Click **Apply**.
 4. In the administration interface, go to **Status > Active Connections**.
 5. Right-click the table header.
 6. In the context menu, scroll down to **Columns** and select **Source Country** and **Destination Country**.
- From now on, the source and destination country appear for all active connections with a nonlocal IP address.

Active Connections

30 items (0 selected)

Traffic Rule	Service	Source IP	Source Country	Destination IP	Destination Country	Bandwidth Management R	Load Balancing	Type
Firewall traffic	HTTPS	192.168.64.153		52.213.141.100	Ireland			Outbound connection
Firewall traffic	HTTPS	192.168.64.153		52.210.24.36	Ireland			Outbound connection
Internet access (NAT)	443/UDP	10.10.10.12		172.217.23.229	United States			
Internet access (NAT)	5228/TCP	10.10.10.12		64.233.167.188	United States			
Internet access (NAT)	443/UDP	10.10.10.12		74.125.206.189	United States			
Internet access (NAT)	HTTPS	10.10.10.12		172.217.23.238	United States			
Internet access (NAT)	XMPP	10.10.10.12		17.252.28.19	United States			
Internet access (NAT)	443/UDP	10.10.10.12		172.217.23.238	United States			
Internet access (NAT)	LDAP	10.10.10.12		10.11.11.3				
Internet access (NAT)	LDAP	10.10.10.12		10.11.11.4				
Internet access (NAT)	443/UDP	10.10.10.12		172.217.23.238	United States			
Internet access (NAT)	LDAP	10.10.10.12		10.11.11.3				

Adding new countries to the filter

To block all incoming connections from a specific country:

1. In the administration interface, go to **Security Settings > GeoIP Filter**.
2. Verify that the **Block incoming traffic from the following countries** option is enabled.
3. Click **Add**.
4. In the **Select Items** dialog box, select the countries you want to block.
5. Click **OK**.
6. Click **Apply**.

From now on, Kerio Control blocks all incoming connections from the selected countries. Outgoing connections are allowed.

Logging blocked incoming connections from specified countries

To verify which packets are dropped by Kerio Control, use the Debug log:

1. In the administration interface, go to **Logs > Debug**.
2. Right-click to the log window.
3. In the context menu, click **Messages**.
4. In the **Logging Messages** dialog box, select **Packets dropped for some reason**.
5. Click **OK**.

After finishing debugging process, unselect the **Packets dropped for some reason**. Displaying too much information slows Kerio Control's performance. For more information, refer to [Using the Debug log](#) (page 130).

4.2.3 Configuring connection limits

Host connection limits in Kerio Control 9.0 and later

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. For more information, refer to [Monitoring active hosts](#) (page 110). 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

The screenshot shows the 'Security Settings' window with the 'Connection Limits' tab selected. The interface includes a top navigation bar with tabs for 'MAC Filter', 'IPv6', 'Zero-configuration Networking', 'Connection Limits', and 'Miscellaneous'. The 'Connection Limits' section contains several 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: HTTPS exclusions (dropdown menu) [Edit...]
- ☐ Limit maximum concurrent connections from 1 source IP address: 0
- ☐ Limit new connections per minute from 1 source IP address: 0

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

NOTE

Kerio Control can send system alerts to your email address if a host reaches a connection limit. For more information, refer to [Using alert messages](#) (page 204).

Changing default values

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

NOTE

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.

☒ Use different settings for any connection from/to this IP addresses:

☐ Limit maximum concurrent connections from 1 source IP address

☐ Limit new connections per minute from 1 source IP address

Skype users Edit...

0

0

Setting different limits for specific IP address groups

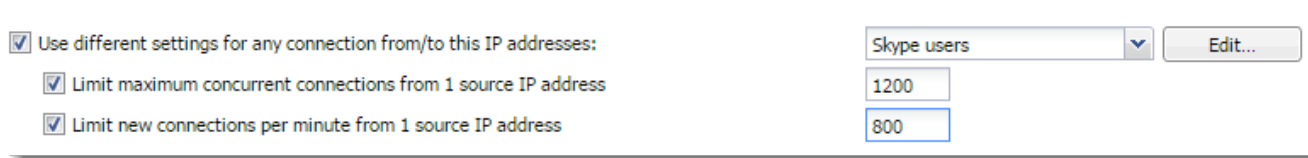
To set different limits for any connection from/to a specific IP address group:

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.



The screenshot shows a settings window with the following elements:

- A checked checkbox labeled "Use different settings for any connection from/to this IP addresses:".
- A dropdown menu currently showing "Skype users" with a downward arrow.
- An "Edit..." button to the right of the dropdown.
- A checked checkbox labeled "Limit maximum concurrent connections from 1 source IP address" with a text input field containing "1200".
- A checked checkbox labeled "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

Kerio Control counts the number of connections for each active host and its peers in the Kerio Control network.

Note that 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.

NOTE

Kerio Control can send system alerts to your email address if a host reaches a connection limit. For more information, refer to [Using alert messages](#) (page 204).

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.

NOTE

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: 100

For all peers: 1000

☐ New connections per minute: 600

☒ Apply different limits for: Web servers Edit...

For a single peer: 50

For all peers: 1000

☐ New connections per minute: 600

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.
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.

4.2.4 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.

Note that:

- » 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. For more information, refer to [Configuring traffic rules](#) (page 236).

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).
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.

NOTE

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

IMPORTANT

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

4.2.5 Filtering MAC addresses

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.

NOTE

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 (a0deb f33ce12)
6. Double check that listed addresses are correct.
7. Click **Apply**.

Your filter is fully configured and active.

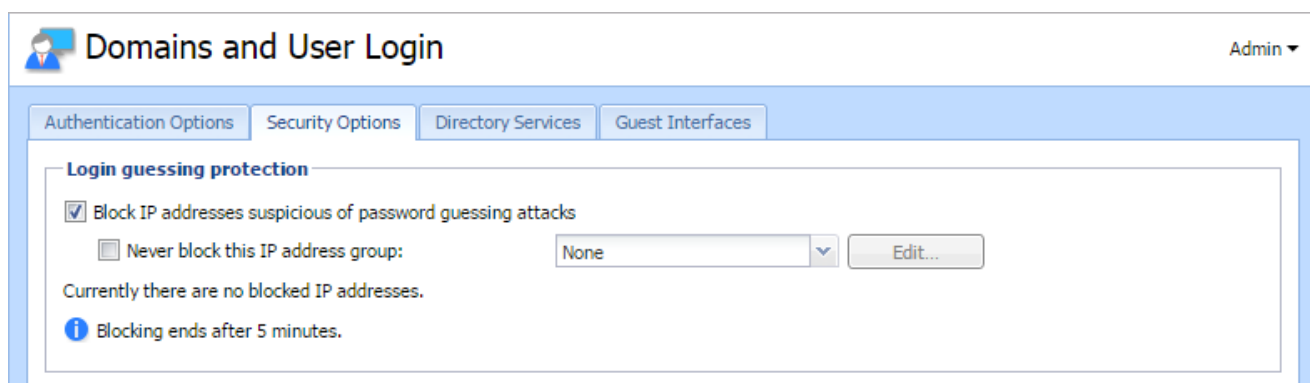
4.2.6 Protecting users against password guessing attacks

Protecting against password guessing attacks

Kerio Control can block IP addresses suspicious of password guessing attacks.

If an attacker tries to log in unsuccessfully 10 times (through various services), Kerio Control blocks the IP address.

1. Go to section **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. For more information, refer to [Configuring IP address groups](#) (page 332).
4. Click **Apply**.



When Kerio Control blocks an account, user cannot log in. Kerio Control unlocks the blocked IP addresses after 5 minutes.

4.2.7 Protocol inspection in Kerio Control

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 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:

Description:

Protocol:

Protocol inspector:

Source port

Condition:

Destination port

Condition:

Port number:

From now on, Kerio Control applies the FTP protocol on the non-standard port 2101.

Disabling a protocol inspector

IMPORTANT

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:

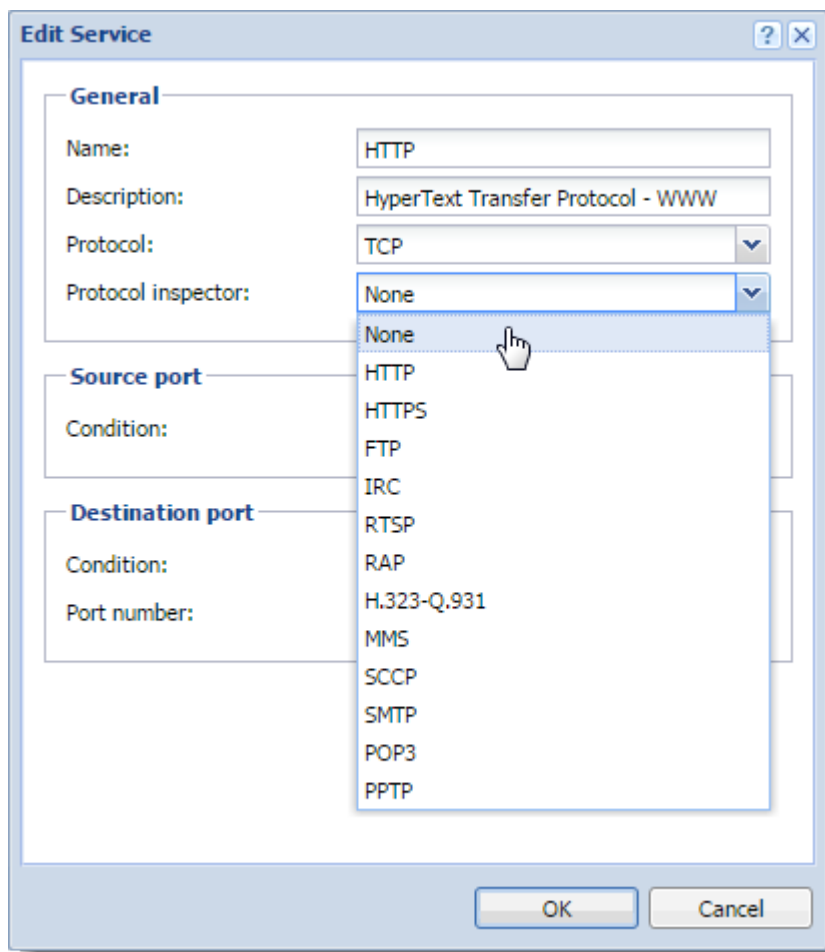
- » In the **Services** section, to disable protocol inspection for all traffic
- » In the **Traffic Rules** section, to disable protocol inspection for traffic meeting the condition of the rule

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.



Screenshot 56: Disabling a protocol inspector

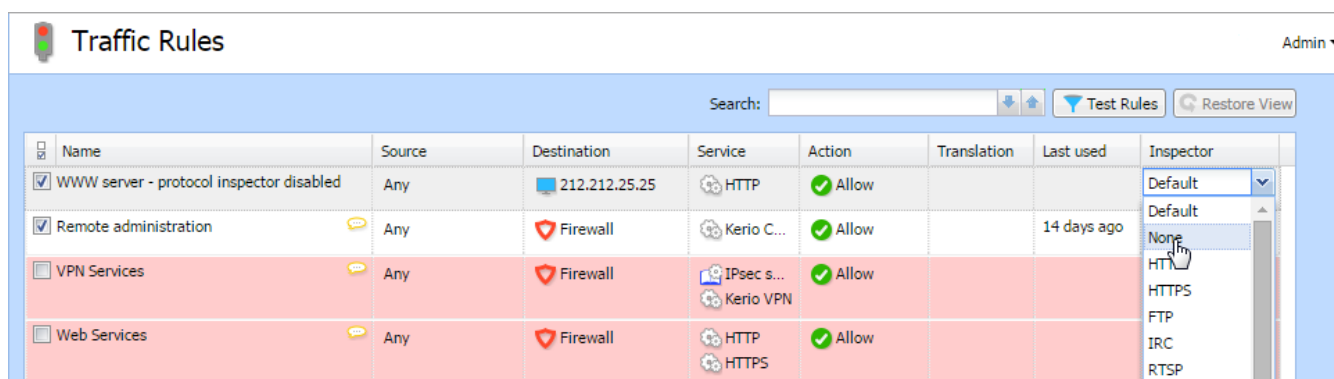
Now try to access the HTTP server from the Internet. If it is accessible, you have your answer. Enable the HTTP protocol inspector for the service and disable it in the particular traffic rule, as described below.

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.



Screenshot 57: Disable a protocol inspector

4.2.8 Encrypting User Data

You can enable encryption to ensure that Kerio Control encrypts logs, configuration, statistics, and reporting data before writing it to the disk.

IMPORTANT

Encryption is bound to a specific storage device, so if you plan to change the hardware you must first disable encryption. Also, encryption results in more resources being utilized so performance maybe impacted.

Enabling Encryption

1. In the Kerio Control administration interface, go to **Configuration > Advanced Options**.
2. Go to the **Data Encryption** tab.

Data Encryption

Enable Encryption to ensure that Kerio Control will encrypt all data prior writing it to the disk. [Learn more...](#)

☐ Disabled. Data encryption is disabled.

Password:

Confirm password:

Screenshot 58: The data encryption tab

3. Key-in the **Password** and re-enter to confirm the same.

IMPORTANT

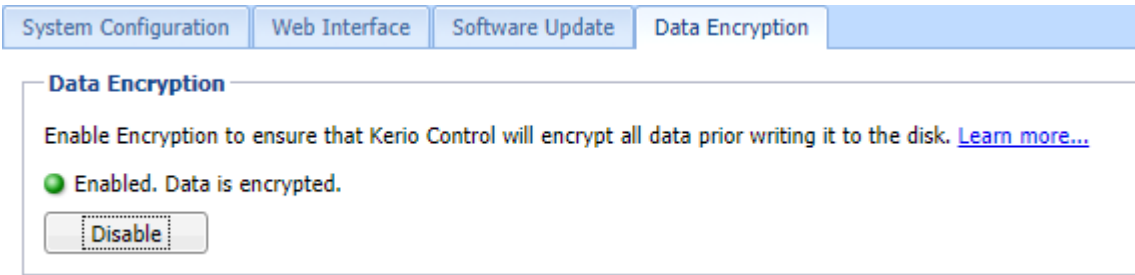
Once encryption is enabled, the password cannot be changed. Remember this password, as you would require it to decrypt data.

4. Click **Encrypt** and confirm the action.

Disabling Encryption

To decrypt data and disable encryption:

1. In the Kerio Control administration interface, go to **Configuration > Advanced Options**.
2. Go to the **Data Encryption** tab.



Screenshot 59: The data encryption tab

3. Click **Decrypt**.
4. Key-in the **Password** set while encrypting and confirm the action.

4.3 IPv6

This section helps you configure IPv6 in your Kerio Control network.

4.3.1 Configuring IPv6 networking in Kerio Control	228
4.3.2 Support for IPv6 protocol	230
4.3.3 Configuring traffic rules for IPv6 network	231

4.3.1 Configuring IPv6 networking in Kerio Control

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](#).

WARNING

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

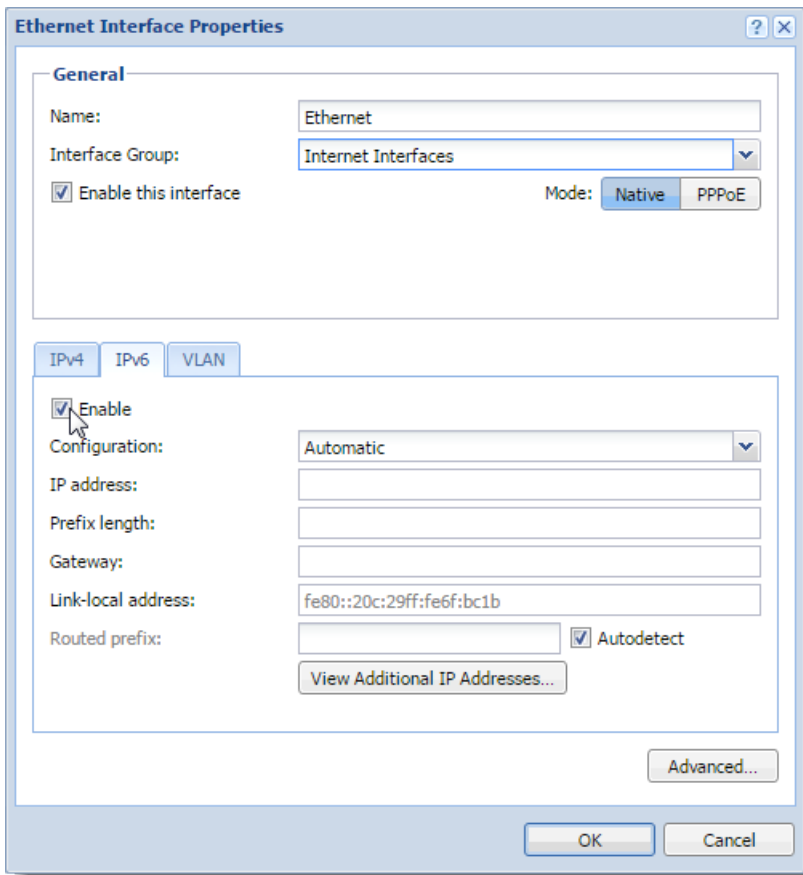
Obtaining an IPv6 prefix from your ISP

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 Interfaces**.
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**.

4.3.2 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.

WARNING

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.

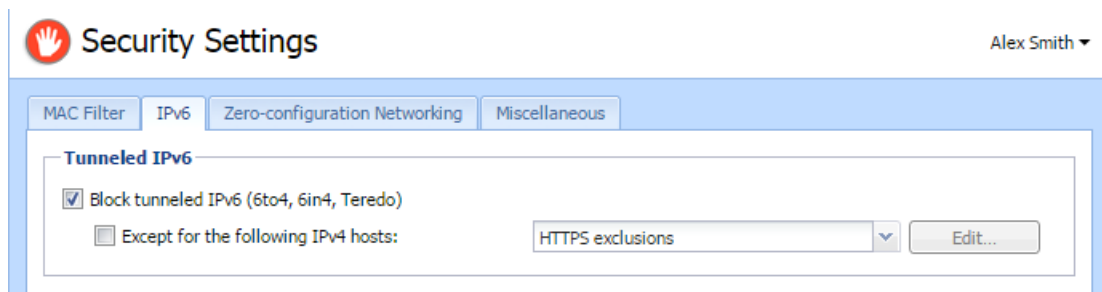
For security reasons, any incoming native and tunneled IPv6 traffic is disabled by default.

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 [For more information, refer to Configuring traffic rules for IPv6 network](#) (page 231).
3. Click **Apply**.

Blocking IPv6 tunneling



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**.

4.3.3 Configuring traffic rules for IPv6 network

Traffic rules for IPv6 overview

Kerio Control supports IPv6 traffic rules.

If you are looking for a general article about traffic rules, go to the [Configuring traffic rules](#) article.

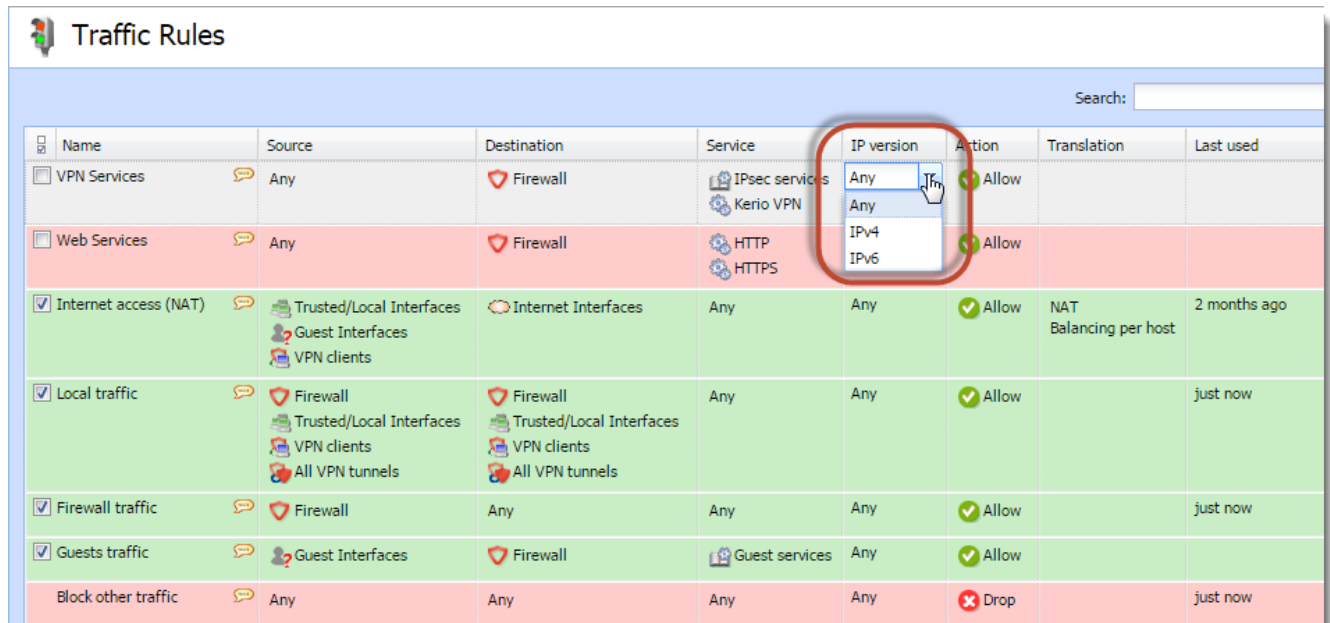
NOTE

During the upgrade to Kerio Control 8.4.0, your IPv6 prefixes allowed on the **Security Settings > IPv6** tab are transformed to **Traffic Rules**.

IPv6 in traffic rules

When you configure traffic rules in the **Traffic rules** section, you can include IPv6 into traffic rules:

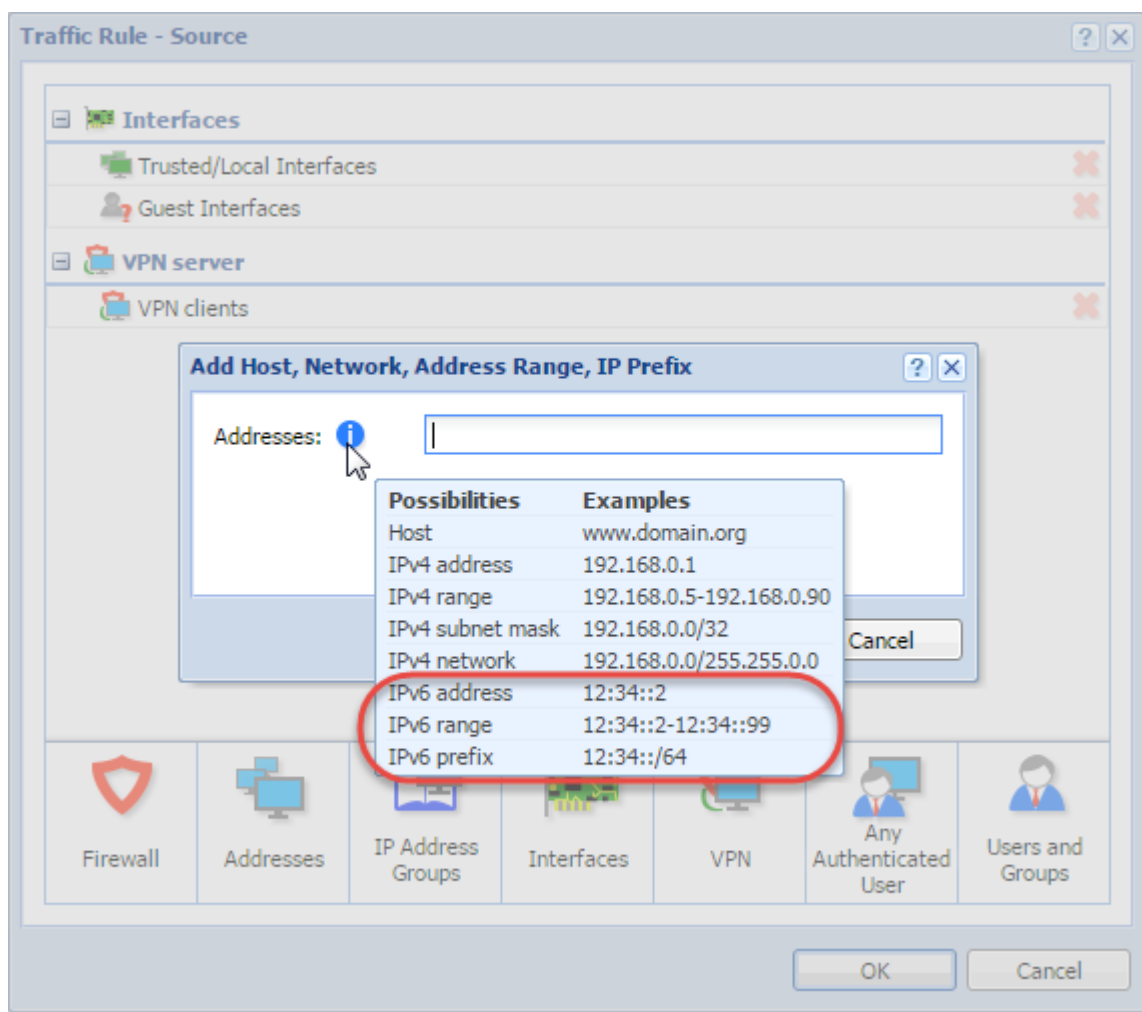
- » You can decide if the rule is valid for IPv4, IPv6 or both types of the IP protocol in the **IP version** column.



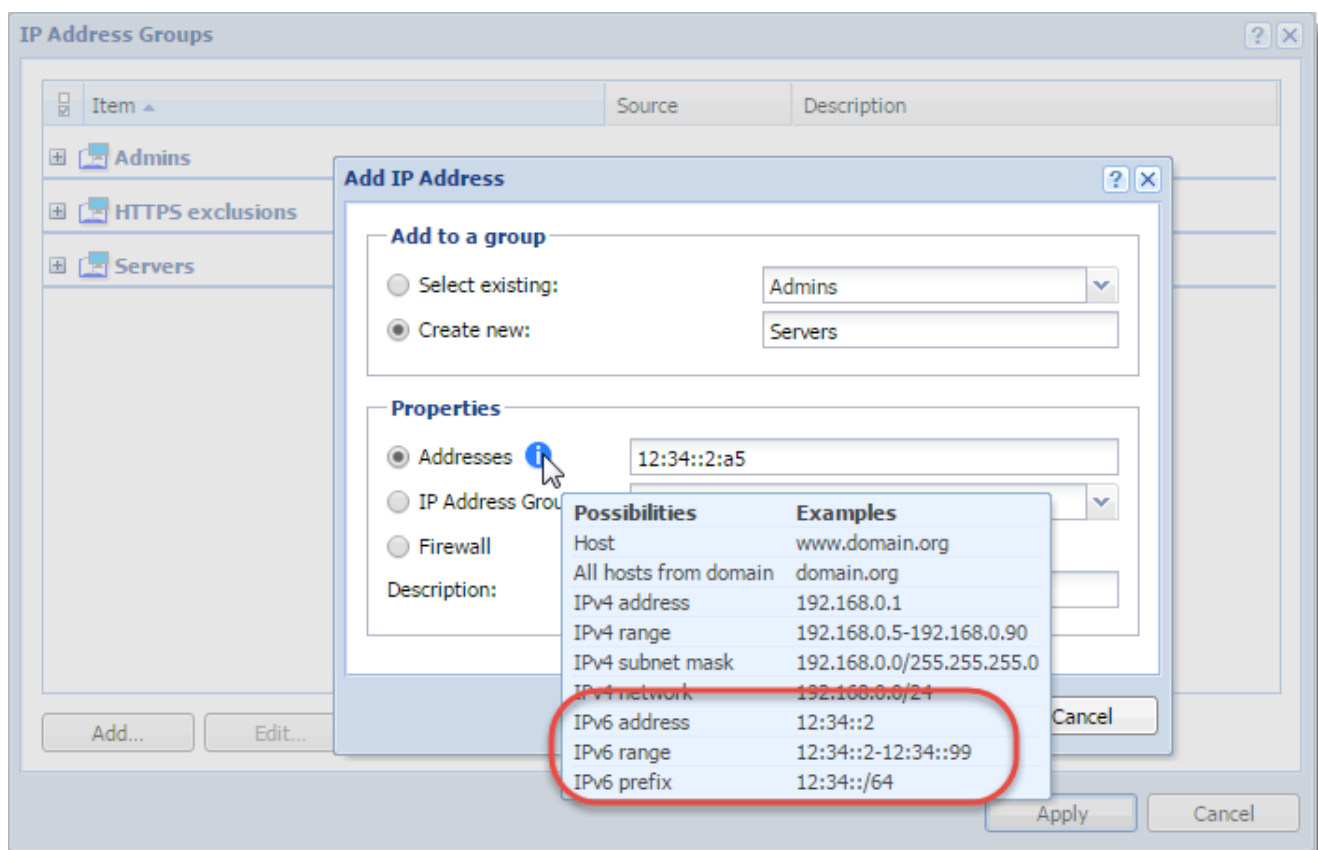
Name	Source	Destination	Service	IP version	Action	Translation	Last used
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow		
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	2 months ago
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

Screenshot 60: Traffic Rules > the IP version column

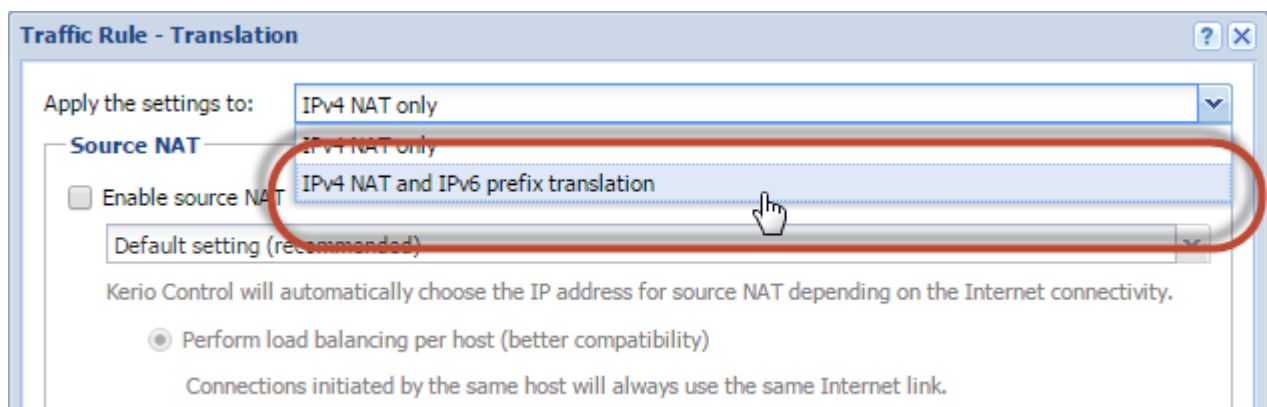
- » You can set an IPv6 address, a range or a prefix in the **Source** and **Destination** columns for each traffic rule.



» You can set an IPv6 address, a range or a prefix for an IP address group in the **Source** and **Destination** columns for each traffic rule.



» In **Translation**, you can apply the settings to IPv6 prefix translation.

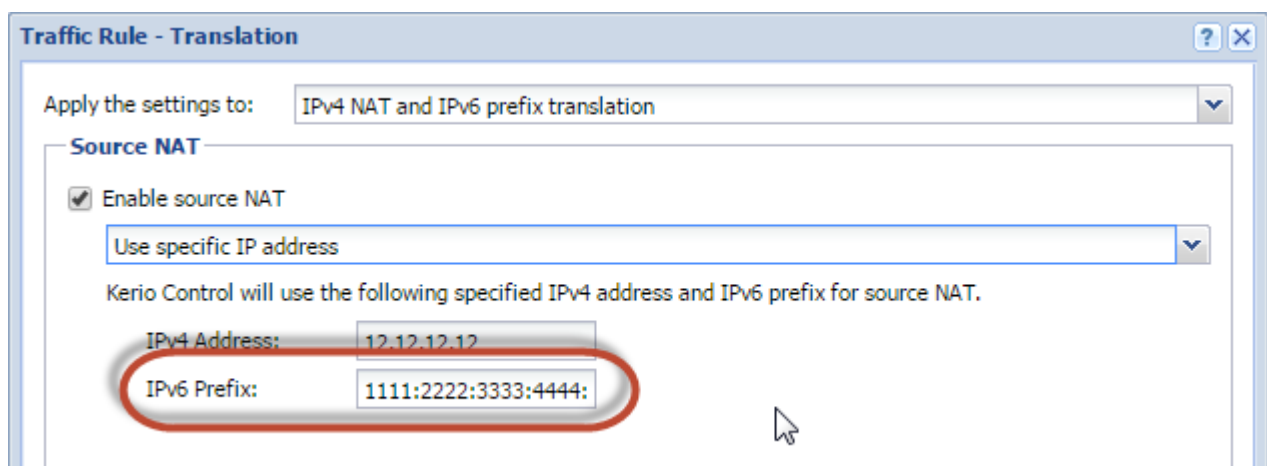


Screenshot 61: The Translation dialog box

NOTE

Do not forget that IPv4 NAT is also applied. When you want to set source or destination NAT, you must type also IPv4 address.

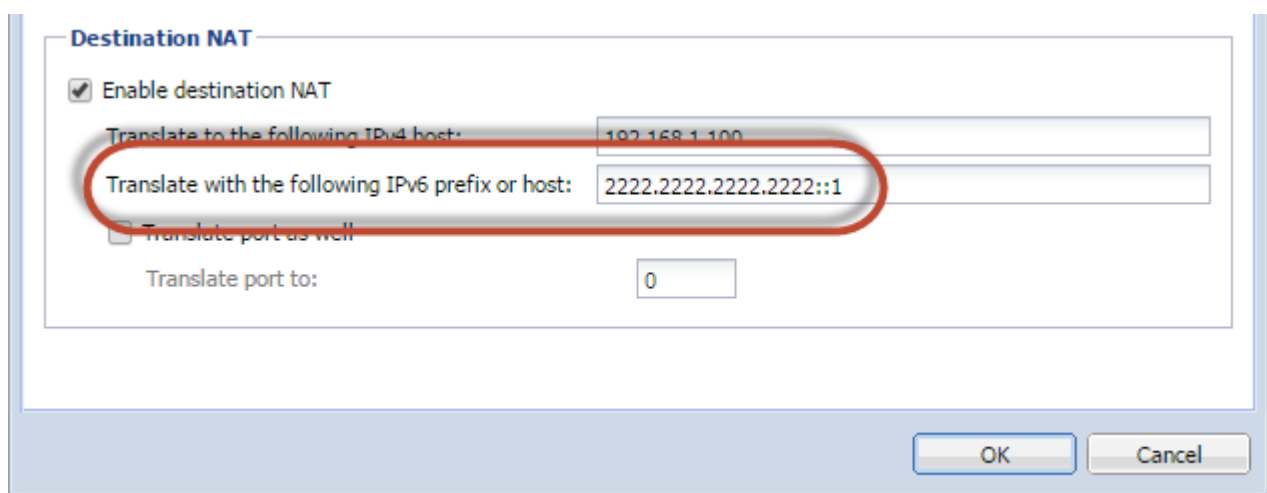
- To enable source NAT in an IPv6 rule, select **Use specific IP address**, and type IPv6 prefix.



Screenshot 62: The Translation dialog — Enable source NAT

When you enable source NAT and use **Default settings** or **Use specific outgoing interface**, you must type IPv6 prefix to the used interface:

- i. Go to **Interfaces**.
 - ii. Double-click the interface to which the communication should be translated.
 - iii. In the dialog for interface configuration, select IPv6 tab.
 - iv. Click **Enable** and configure it.
 - v. Save the settings.
- To enable destination NAT in an IPv6 rule, select **Translate with the following IPv6 prefix or host**, and type IPv6 prefix.



Screenshot 63: The Translation dialog — Enable destination NAT

4.4 Traffic rules

This topic provides information about creating and configuring traffic rules and their order.

4.4.1 Configuring traffic rules	236
---------------------------------------	-----

4.4.2 Configuring IP address translation	241
4.4.3 Configuring Demilitarized Zone (DMZ)	244
4.4.4 Configuring traffic rules - exclusions	245
4.4.5 Configuring traffic rules - multihoming	245
4.4.6 Limiting Internet access with traffic rules	247
4.4.7 Troubleshooting traffic rules	248

4.4.1 Configuring traffic rules

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.

NOTE

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**).

The screenshot shows the 'Traffic Rules' window in Kerio Control. The interface includes a search bar at the top, a table of rules, and a context menu on the left. Annotations with red arrows point to various features:

- Find the rule quickly:** Points to the search bar.
- Verify whether the rules are configured properly:** Points to the 'Test Rules' button.
- Red color highlights inbound rules:** Points to the first two rules (IPsec services and HTTP/HTTPS).
- Green color highlights outbound rules:** Points to the 'Internet access (NAT)' rule.
- The rule order is important!:** Points to the up/down arrow buttons on the right side of the table.
- Checkbox enables/disables the rule:** Points to the checkbox in the first column of the table.
- A default rule denying all traffic:** Points to the 'Block other traffic' rule at the bottom.

Name	Source	Destination	Service	IP version	Action	Translation	Last used
Check All	Any	Firewall	IPsec services	Any	Allow		
Uncheck All	Any	Firewall	Kerio VPN	Any	Allow		
Check Selected	Any	Firewall	HTTP	Any	Allow		
Uncheck Selected	Any	Firewall	HTTPS	Any	Allow		
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	2 months ago
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

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

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**.

Add New Rule

Rule type

Source

Destination

Services

Name:

Rule type

☒ **Generic** - allow or deny a particular traffic.

Action:

☐ **Port mapping** - make a service in LAN accessible from the Internet.

Host:

Service:

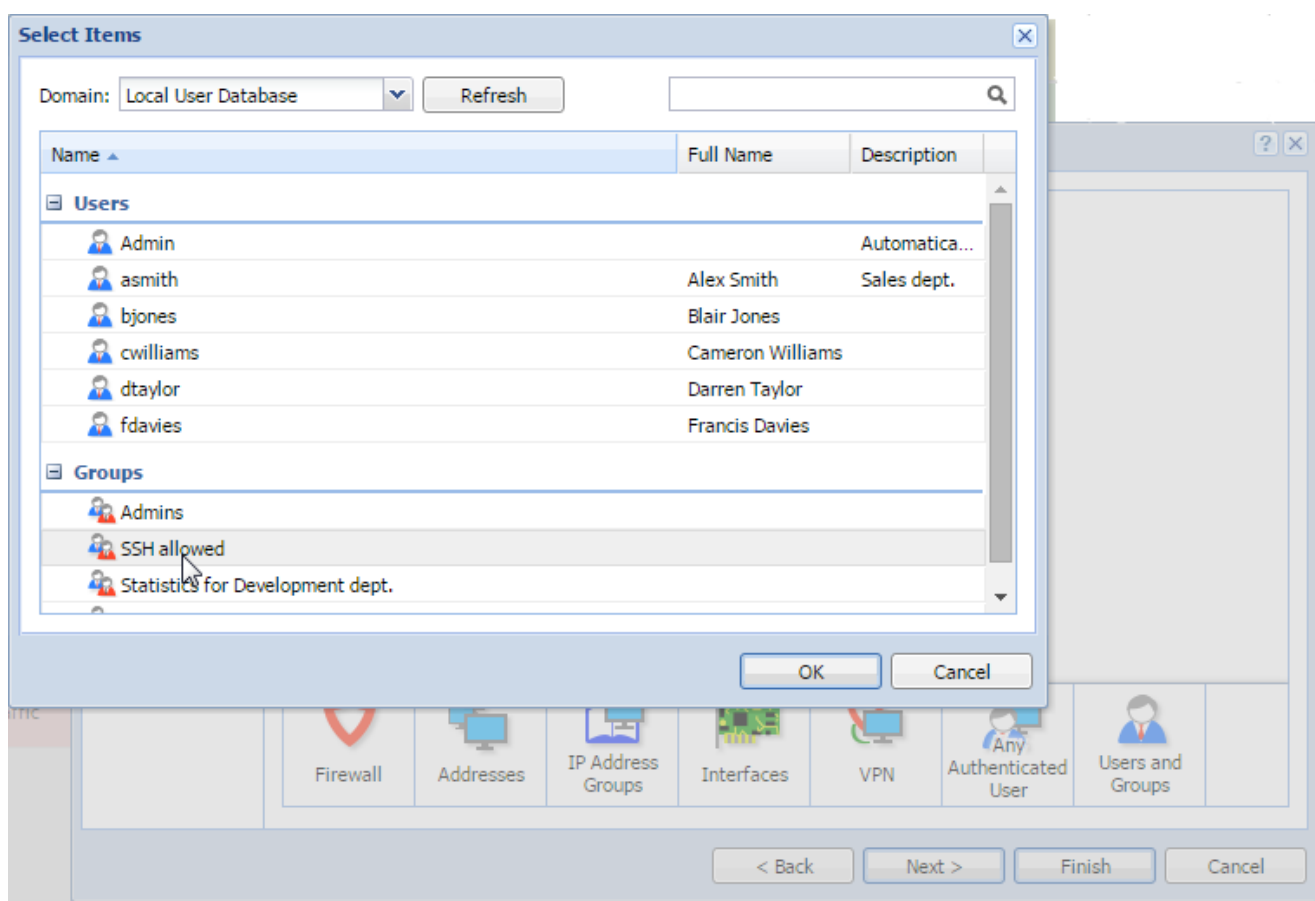
☐ **Policy routing** - use a specific outgoing interface or a public IP address for a particular traffic.

☒ Interface:

☐ IP Address:

< Back Next > Finish Cancel

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



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.

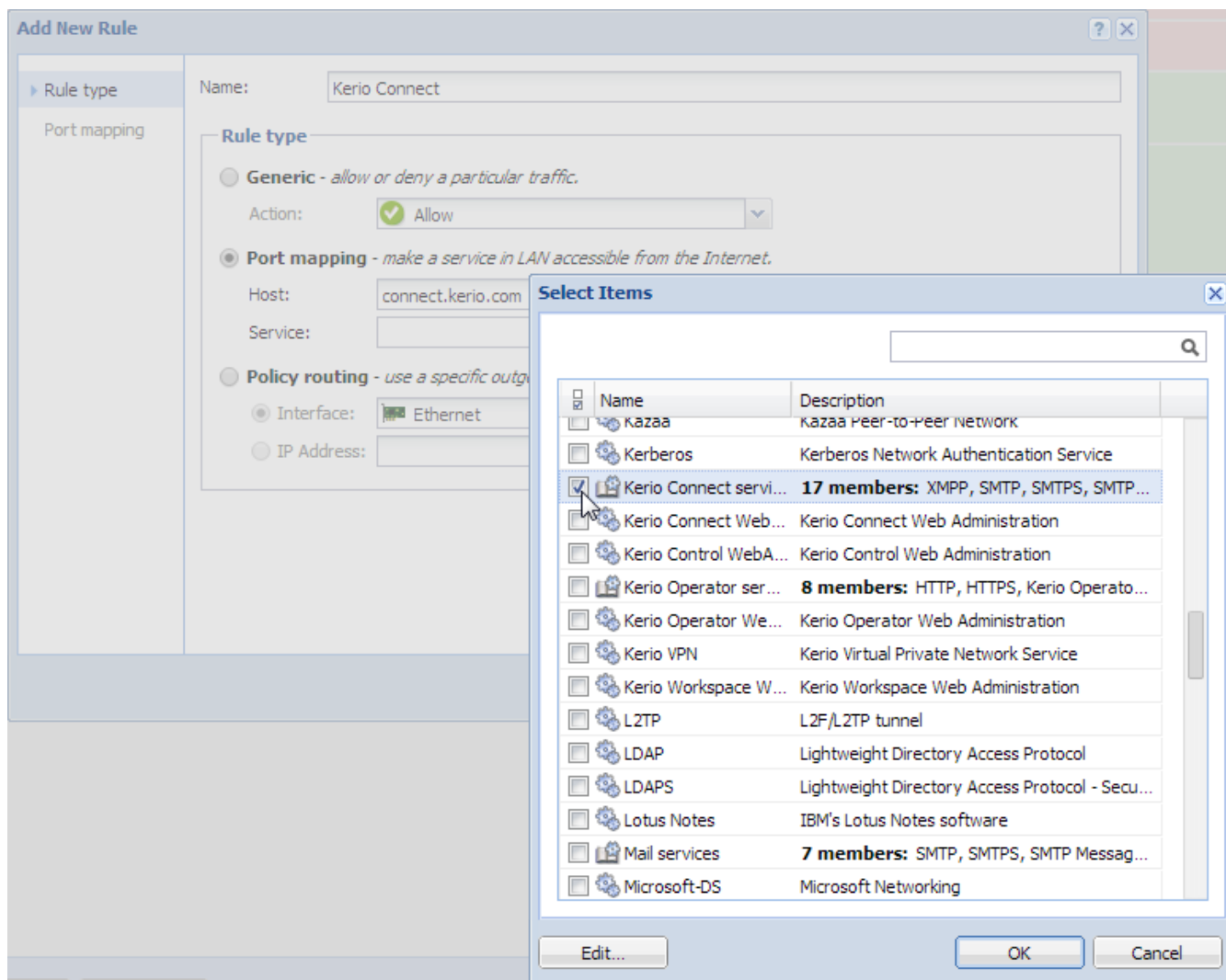
<input checked="" type="checkbox"/> Allow SSH to a group	SSH allowed	Internet Interfaces	SSH	Any	Allow		
Block other traffic	Any	Any	Any	Any	Drop		just now

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.



8. Click **Finish**.
9. Move the rule to the top of the table of traffic rules.

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):

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.

<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 asmith	Internet Interfaces	Any	Any	Allow	NAT Balancing per host

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.

IMPORTANT

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:

Test Rules

Restore View

<input type="checkbox"/>	Name	Source	Destination	Service	IP version	Action	Translation
<input checked="" type="checkbox"/>	WWW without authentica...	<div><div></div>Trusted/Local Interfac...</div>	<div><div></div>Internet Interfaces</div>	<div><div></div>HTTP</div>	Any	<div><div></div>Allow</div>	NAT Balancing per host
<input checked="" type="checkbox"/>	Internet access (NAT)	<div><div><div></div>Trusted/Local Interfac...</div><div><div></div>Guest Interfaces</div><div><div></div>VPN clients</div><div><div></div>asmith</div></div>	<div><div></div>Internet Interfaces</div>	Any	Any	<div><div></div>Allow</div>	NAT Balancing per host

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



Content Filter

Admin






Content Rules

Forbidden Words

Kerio Control Web Filter

HTTPS Filtering

Advanced Settings

<input type="checkbox"/>	Name	Detected content	Source	Action
<input checked="" type="checkbox"/>	Allow access to selected users	Any	 asmith  bjones	 Allow
<input checked="" type="checkbox"/>	Deny access to all other users	 *	Any	 Deny

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 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.

NOTE

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)

For more information, refer to [Configuring Demilitarized Zone \(DMZ\)](#) (page 244).

Policy routing

For more information, refer to [Configuring policy routing](#) (page 289).

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 information, refer to [Protocol inspection in Kerio Control](#) (page 224).

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.

IMPORTANT

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**.

4.4.2 Configuring IP address translation

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:

Source NAT Type	Description
Default setting (recommended)	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> » 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. 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. <div> HINT For maximal efficiency of the connection's capacity, go to the Configuring policy routing article. </div>
Use specific outgoing interface	<p>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.</p> <p>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.</p>
Use specific IP address	<p>An IP address for NAT will be used as the source IP address for all packets sent from the LAN to the Internet.</p> <ul style="list-style-type: none"> » 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.

NOTE

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:

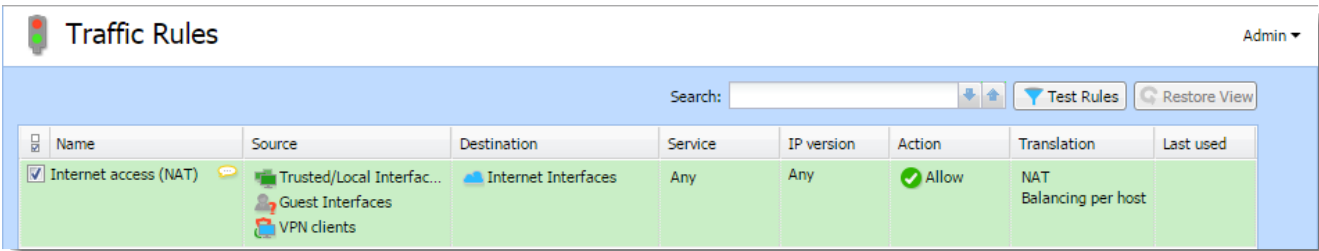
- 1. Check **Enable destination NAT**.
- 2. In field **Translate to the following host**, type a host address or DNS name. IP address that will substitute the packet's destination address. This address also represents the address/name of the host on which the service is actually running.
- 3. If you 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.

NOTE

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

For more information, refer to [Configuring traffic rules](#) (page 236).

A default NAT rule description



Screenshot 64: A typical traffic rule for NAT (Internet connection sharing)

Settings	Description
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. For more information, refer to Configuring a routing table in Kerio Control (page 303).
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. <div>WARNING Destination NAT should not be configured for outgoing rules, except under very unique circumstances.</div>

Settings	Description
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.

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

Screenshot 65: Rule for traffic between the firewall and hosts in the Internet

4.4.3 Configuring 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).

Traffic Rules								Admin ▾
<div>Search: <input type="text"/></div> <div> </div>								
<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		

Screenshot 66: 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](#).

4.4.4 Configuring traffic rules - exclusions

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

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

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

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

Screenshot 67: Exception — SSH is available only for selected user group(s)

4.4.5 Configuring traffic rules - multihoming

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:

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"/>	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.

6. Save all the dialogs.

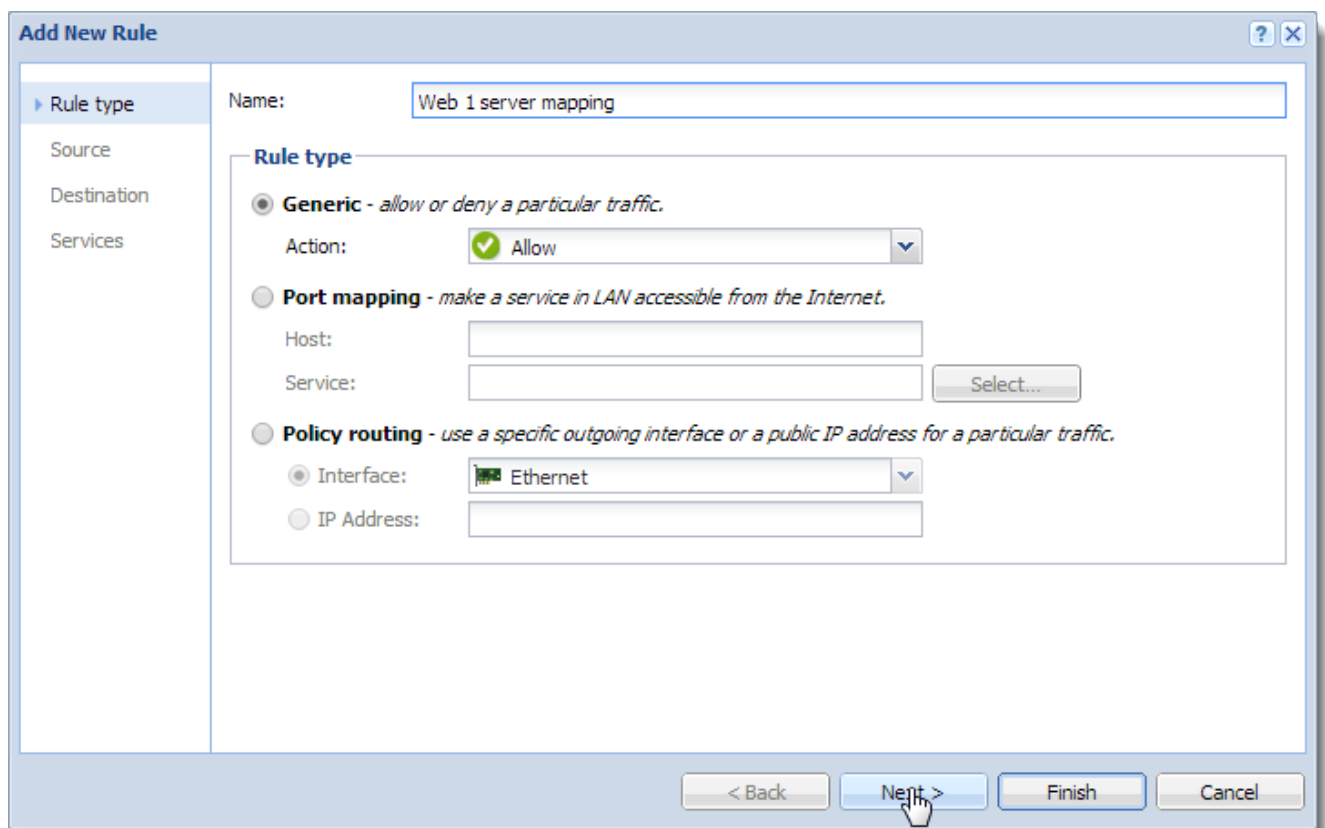
7. Click **Apply**.

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, and below it, 'Source', 'Destination', and 'Services' are listed. The main area has a 'Name' field with the text 'Web 1 server mapping'. Below this, the 'Rule type' section has three radio buttons: 'Generic' (selected), 'Port mapping', and 'Policy routing'. Under 'Generic', the 'Action' is set to 'Allow'. Under 'Port mapping', there are fields for 'Host' and 'Service', and a 'Select...' button. Under 'Policy routing', there are radio buttons for 'Interface' (selected, set to 'Ethernet') and 'IP Address' (empty). 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.

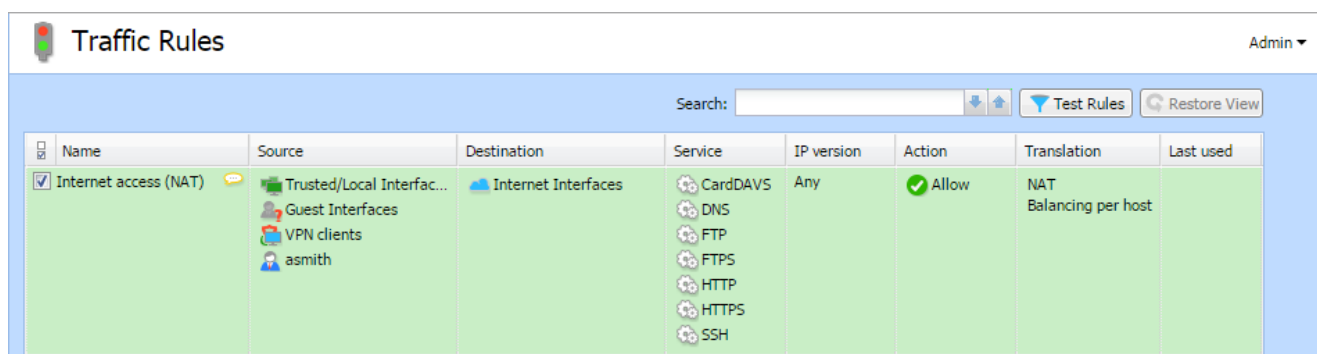
4.4.6 Limiting Internet access with traffic rules

Access to Internet services from the local network can be limited in several ways. In the following examples, the limitation rules use IP translation. For more information, refer to [Configuring IP address translation](#) (page 241).

NOTE

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.

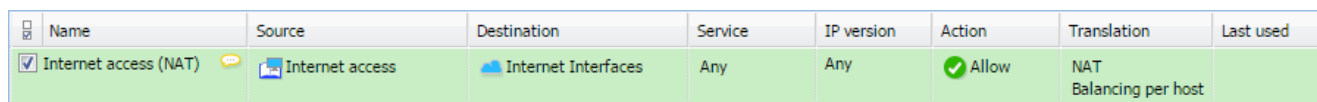


The screenshot shows the 'Traffic Rules' configuration window. A search bar is at the top right. Below it is a table with columns: Name, Source, Destination, Service, IP version, Action, Translation, and Last used. The first rule, 'Internet access (NAT)', is selected. Its Source is 'Trusted/Local Interfaces' (with sub-items: Guest Interfaces, VPN clients, asmith). Its Destination is 'Internet Interfaces'. Its Service list includes CardDAV, DNS, FTP, FTPS, HTTP, HTTPS, and SSH. Its Action is 'Allow' (checked). Its Translation is 'NAT Balancing per host'.

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	

Screenshot 68: 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**.



The screenshot shows the 'Traffic Rules' configuration window. The table has the same columns as Screenshot 68. The rule 'Internet access (NAT)' is selected. Its Source is 'Internet access'. Its Destination is 'Internet Interfaces'. Its Service is 'Any'. Its IP version is 'Any'. Its Action is 'Allow' (checked). Its Translation is 'NAT Balancing per host'.

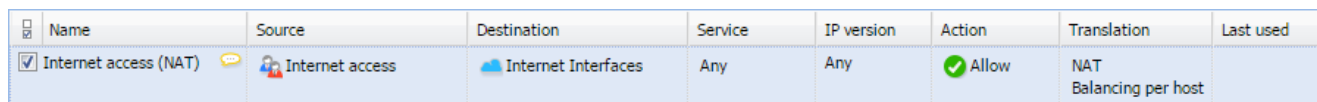
Name	Source	Destination	Service	IP version	Action	Translation	Last used
Internet access (NAT)	Internet access	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	

Screenshot 69: Only selected IP address group(s) is/are allowed to connect to the Internet

NOTE

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.








The screenshot shows the 'Traffic Rules' configuration window. The table has the same columns as Screenshot 68. The rule 'Internet access (NAT)' is selected. Its Source is 'Internet access' (with a user icon). Its Destination is 'Internet Interfaces'. Its Service is 'Any'. Its IP version is 'Any'. Its Action is 'Allow' (checked). Its Translation is 'NAT Balancing per host'.

Name	Source	Destination	Service	IP version	Action	Translation	Last used
Internet access (NAT)	Internet access	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	

Screenshot 70: Only selected user group(s) is/are allowed to connect to the Internet

4. 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	

Screenshot 71: Only authenticated users are allowed to connect to the Internet

NOTE

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

4.4.7 Troubleshooting traffic rules

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 **DNS Lookup** tool in Kerio Control:

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

IP Tools Admin ▾

Ping Traceroute **DNS Lookup** Whois

Parameters

Name:

Tool: ☒ nslookup ☐ dig

Server: ▾

Type: ▾

Start Stop

Command output

```
Server:      10.11.11.3
Address:     10.11.11.3#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
```

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:

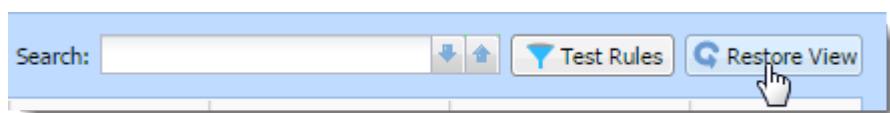
1. In the administration interface, go to **Logs > Debug**.
2. Right-click the **Debug** window.
3. In the context menu, click **Messages**.
4. In the **Filtering** section, select **Packets dropped for some reason**.
5. In the **Debug** log, find the dropped packets using the IP address of the server.

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:

Log Text	Description
[22/Dec/2015 15:32:40]	Date and time of the dropped packet



Now, you can again see all traffic rules.

4.5 Content filtering

This section provides information about creating and configuring content rules and their order.

4.5.1 Configuring the Content Filter	251
4.5.2 Application awareness in Kerio Control	258
4.5.3 Configuring FTP policy	267
4.5.4 Configuring HTTP policy	268
4.5.5 Filtering web content by word occurrence	272
4.5.6 Blocking inappropriate or explicit content in search results	273
4.5.7 Filtering HTTPS connections	275
4.5.8 HTTPS filtering specifics	279
4.5.9 Using Kerio Control Web Filter	279
4.5.10 Slow Internet connection with activated Kerio WebFilter	281
4.5.11 Eliminating Peer-to-Peer traffic	282

4.5.1 Configuring the Content Filter

NOTE

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). 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.

NOTE

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

Configuring content rules

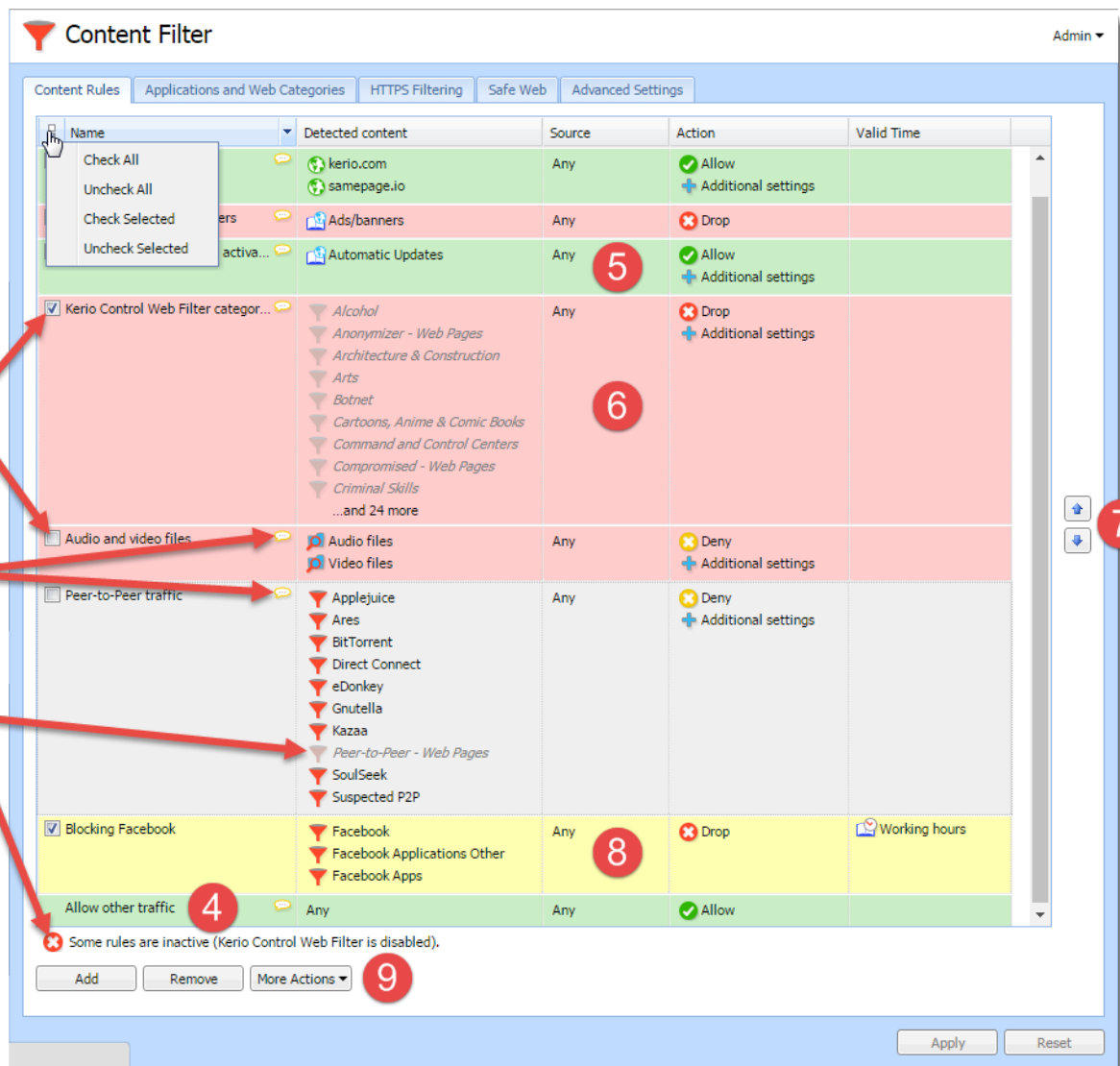
The **Content Rules** table includes several predefined rules.

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 rule order is important. Use the arrows to adjust the order of rules. For details, see [Ordering rules](#) (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

NOTE

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:

Action	Description
Allow	<p>Traffic allowed. With the allow rule you can create the following types of rules:</p> <ul style="list-style-type: none"> » 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.
Deny	<p>User will be redirected to the firewall page with information that access is denied. You can:</p> <ul style="list-style-type: none"> » redirect a user to another page <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <p>WARNING</p> <p>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.</p> </div> <ul style="list-style-type: none"> » 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.
Drop	Access is denied and the user will see the page as unavailable.

Rule order

Kerio Control goes through rules from top to down and stop with the first match. Therefore, order the rules from specific to general. The most general rule, **Allow other traffic**, is created by default and it is placed at the bottom.

You can change the order with:

- » Arrows placed on the right side of the window
- » Drag&Drop and move rule or more rules with mouse

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.

<input type="checkbox"/>	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	

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.

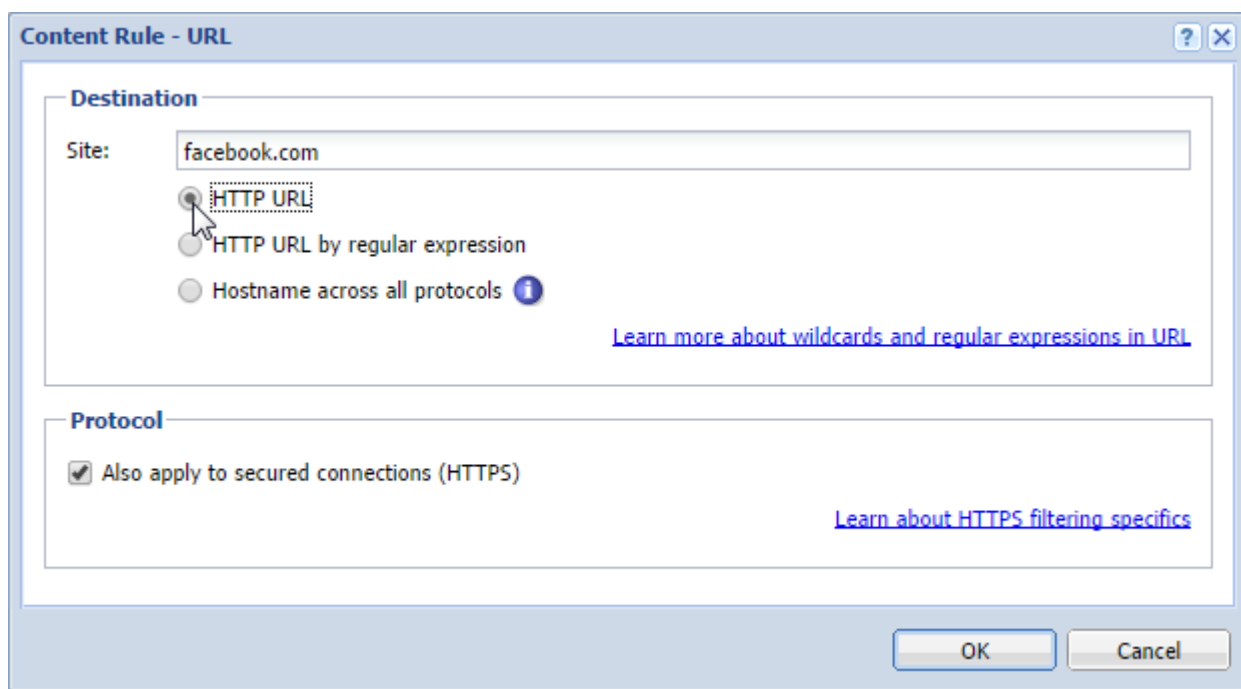
Blocking Facebook

NOTE

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:

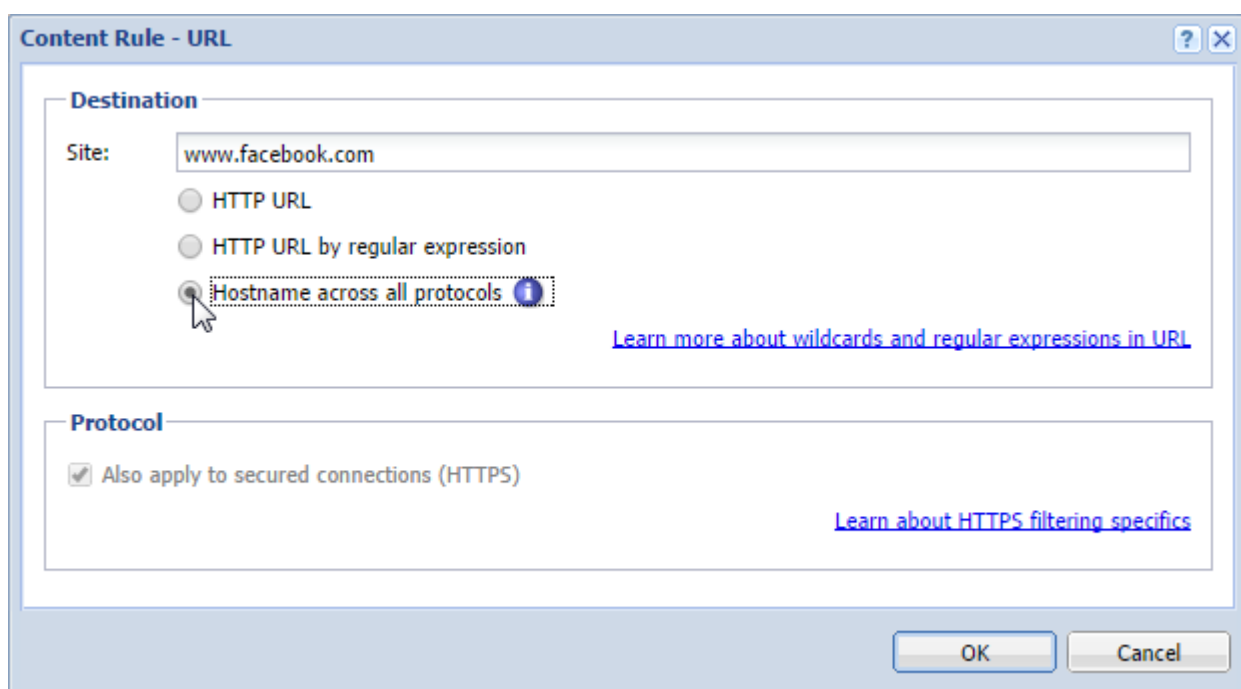
1. On the **Content Rules** tab, click **Add**.
2. Type a name of the new rule.
3. Double-click **Detected Content**.
4. In the **Content Rule - Detected Content** dialog, click **Add > URL and Hostname**.
5. Type `facebook.com` into the **Site** field.
6. Check option **Also apply to secured connections (HTTPS)**. This option has exceptions written in the [HTTPS filtering specifics](#) article.



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.

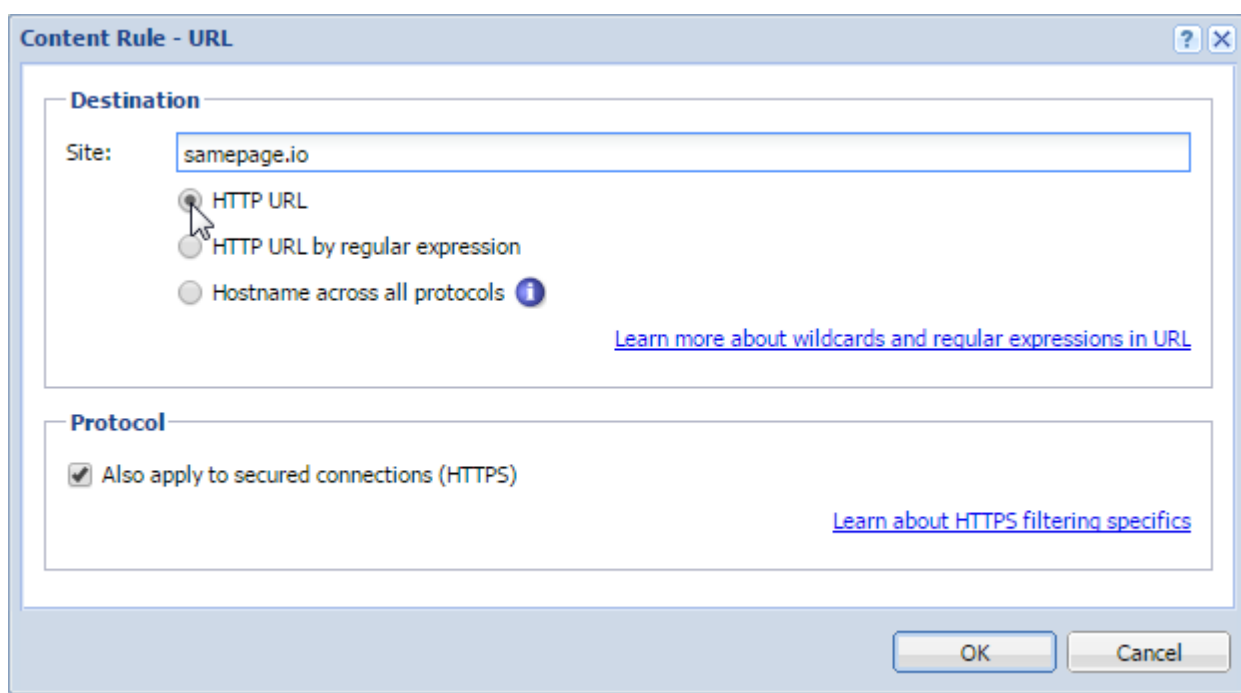
Allowing all content from Samepage.io

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**.

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.

4.5.2 Application awareness in Kerio Control

NOTE

Watch the [Application visibility and control](#) video.

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](#).

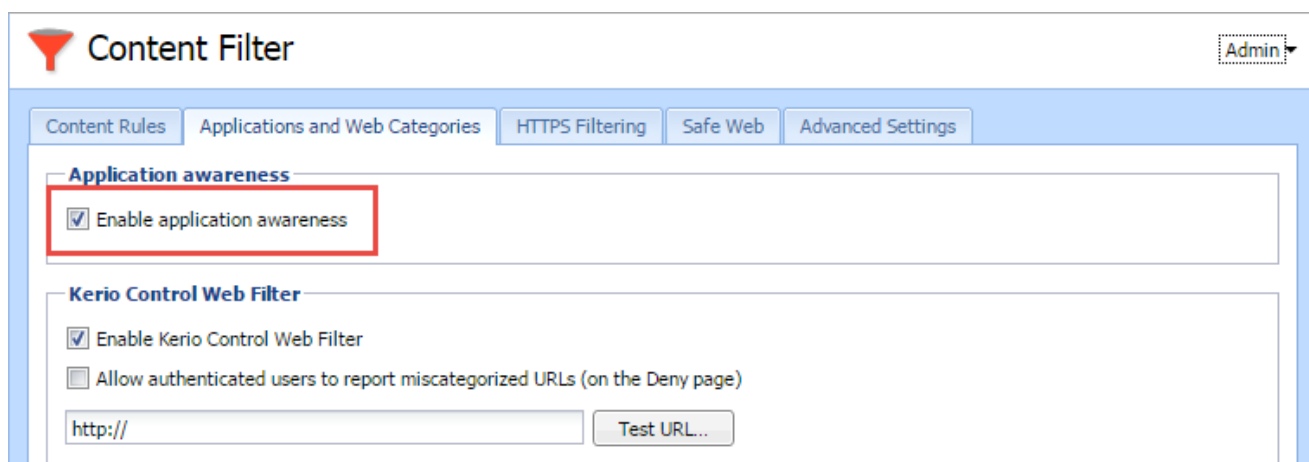
The new application awareness means that the behavior of content filtering and bandwidth management in Kerio Control changes. Rules may become more strict and can be applied to more applications or connections that they match.

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**.

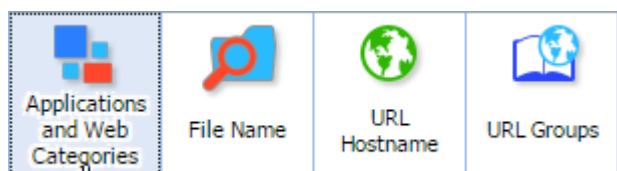


Setting content rules

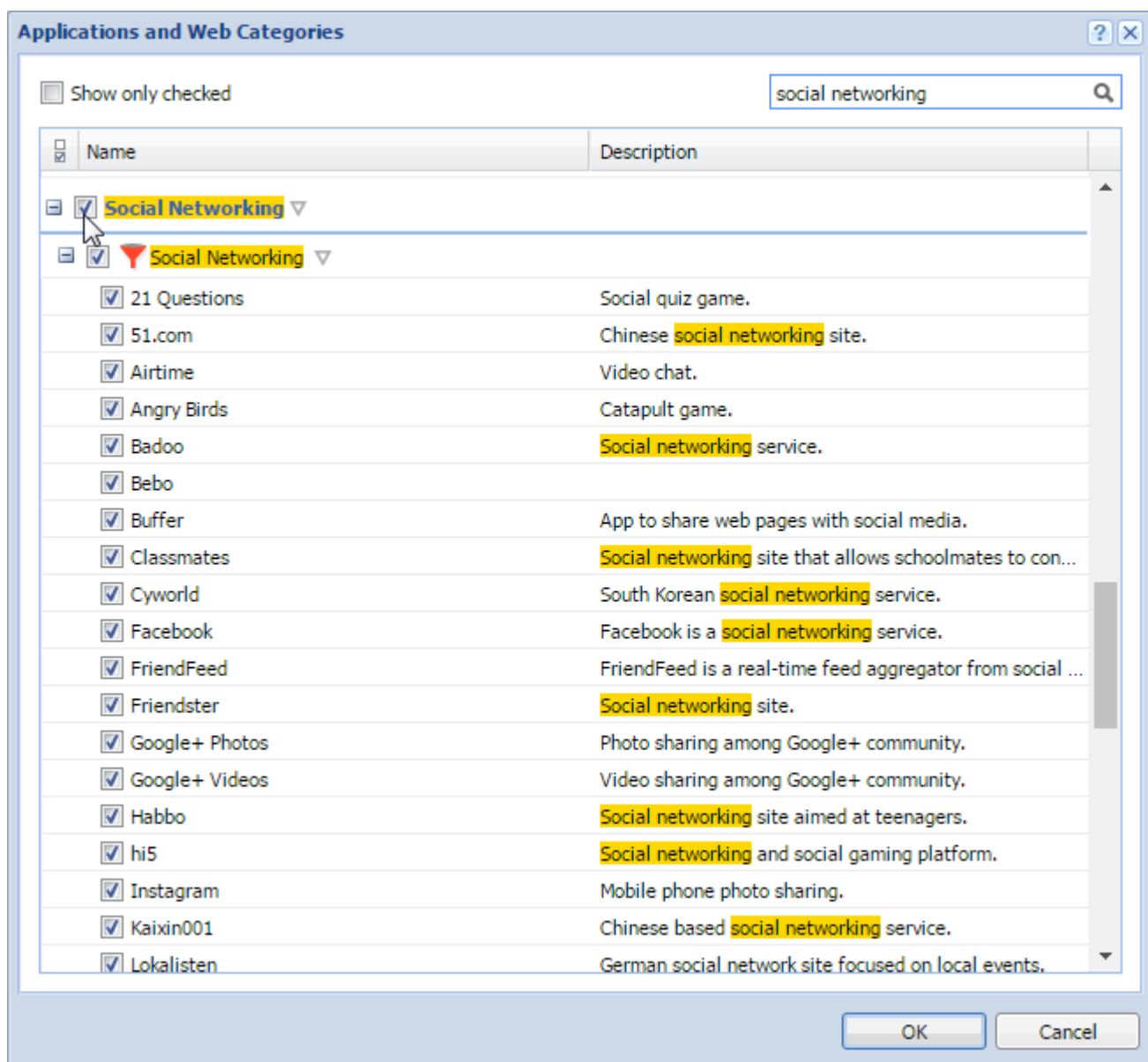
Example: Social networks

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**.



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**.

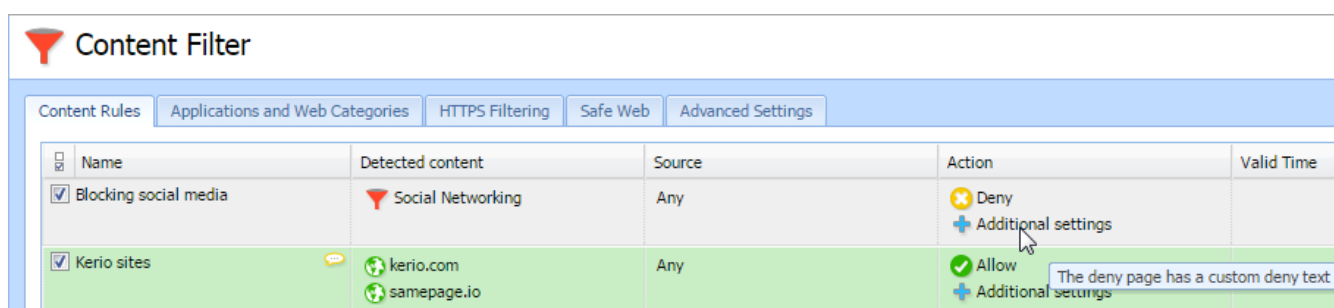


11. Type a deny text that appears to users in their browsers when the rule is matched.

12. Click **OK**

13. Click **Apply**.

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



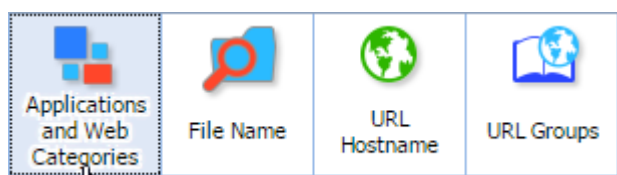
Example: YouTube, Twitter and Skype

If you don't want to be as strict as in the [Example: Social networks](#) rule, forbid access only:

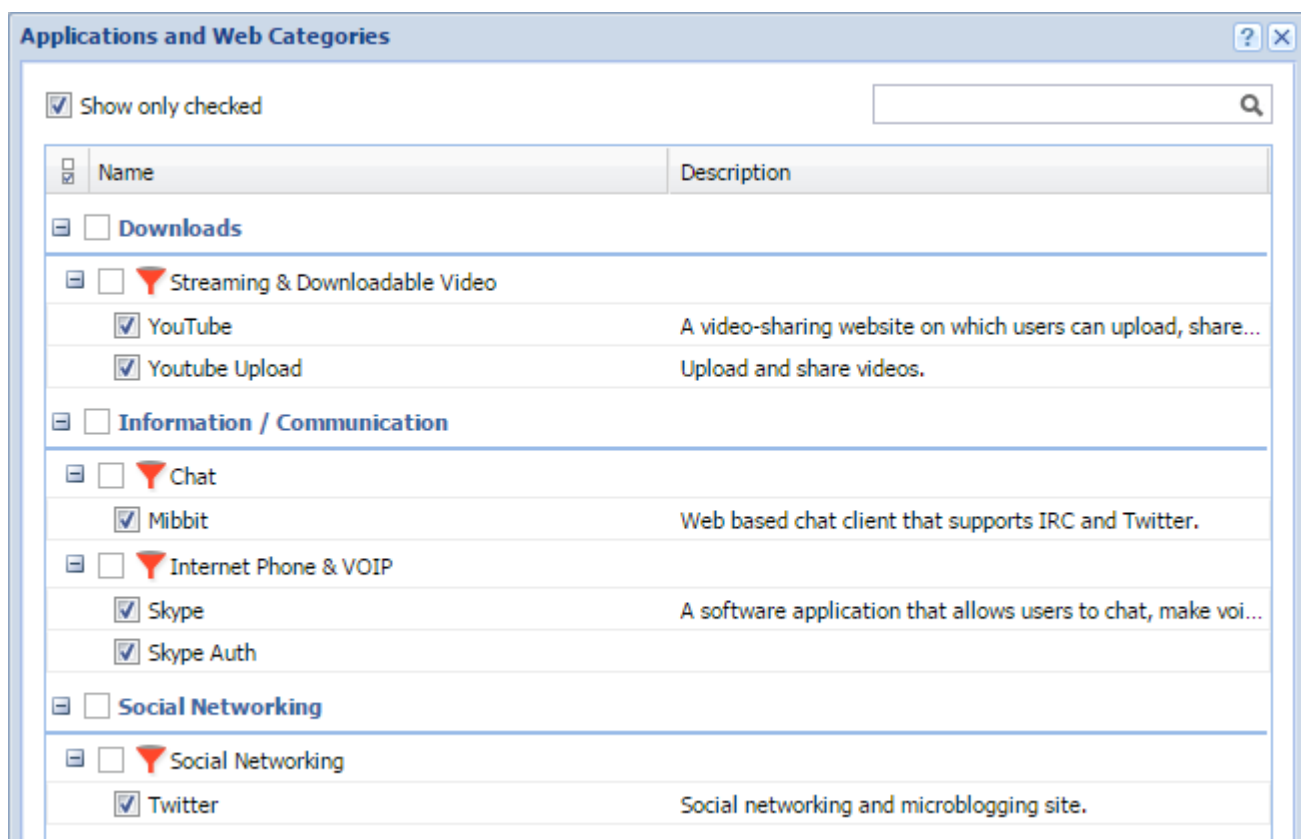
- » To a group of users
- » To YouTube, Twitter, and Skype
- » During working hours

To configure such rule:

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, for example, YouTube, Twitter and Skype.
4. Double-click the **Detected content** column.
5. In the **Content Rule - Detected Content** dialog box, click **Applications and Web Categories**.



6. In the **Applications and Web Categories** dialog box, find and select all items which include YouTube, Twitter, and Skype.



7. Click OK twice.

8. Double-click the **Source** column.

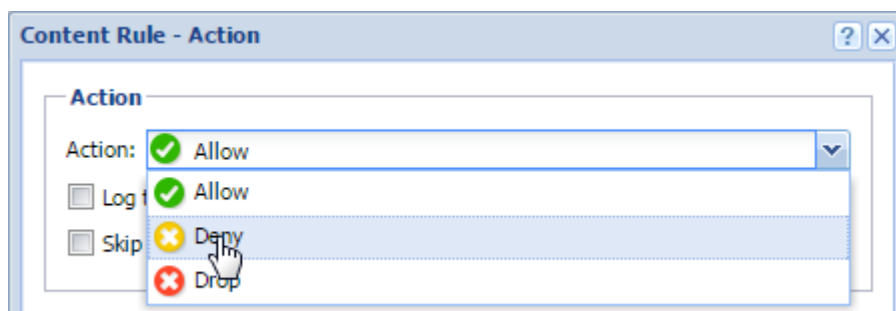
9. In the **Content Rule - Source** dialog box, select **Users and Groups**.

10. In the **Select Items** dialog box, select a group you want to restrict from using YouTube, Twitter, and Skype. For details, see [Creating user groups in Kerio Control](#).

11. Click **OK** twice.

12. Double-click the **Action** column.

13. In the **Content Rule - Action** dialog box, select **Deny**.



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

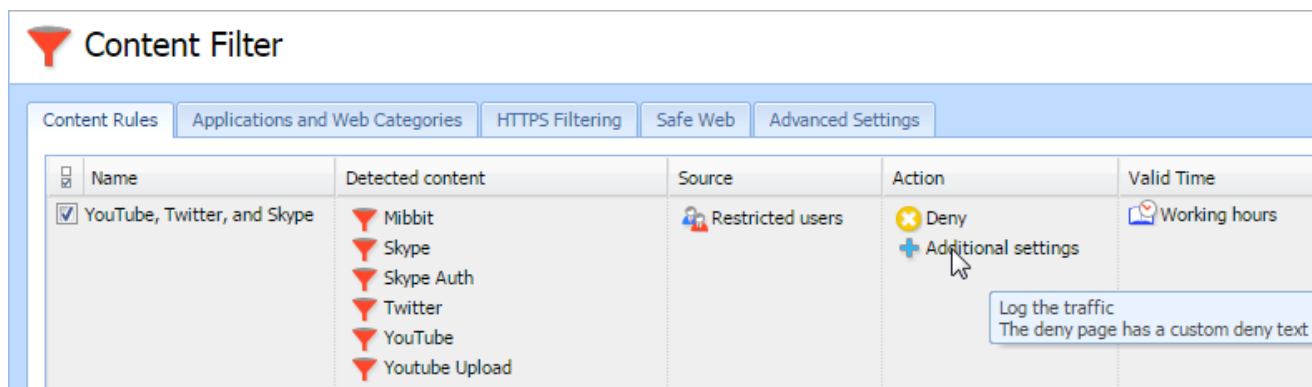
15. Click **OK**

16. Double-click the **Valid Time** column.

17. In the drop down list, select a time range. For details, see [Creating time ranges in Kerio Control](#).

18. Click **Apply**.

From now on, Kerio Control refuses all attempts to use YouTube, Twitter and Skype during working hours.

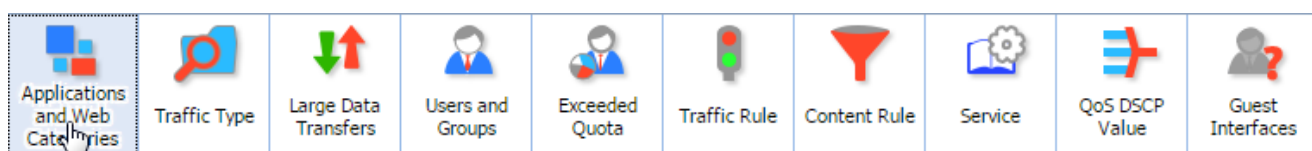


Setting bandwidth rules

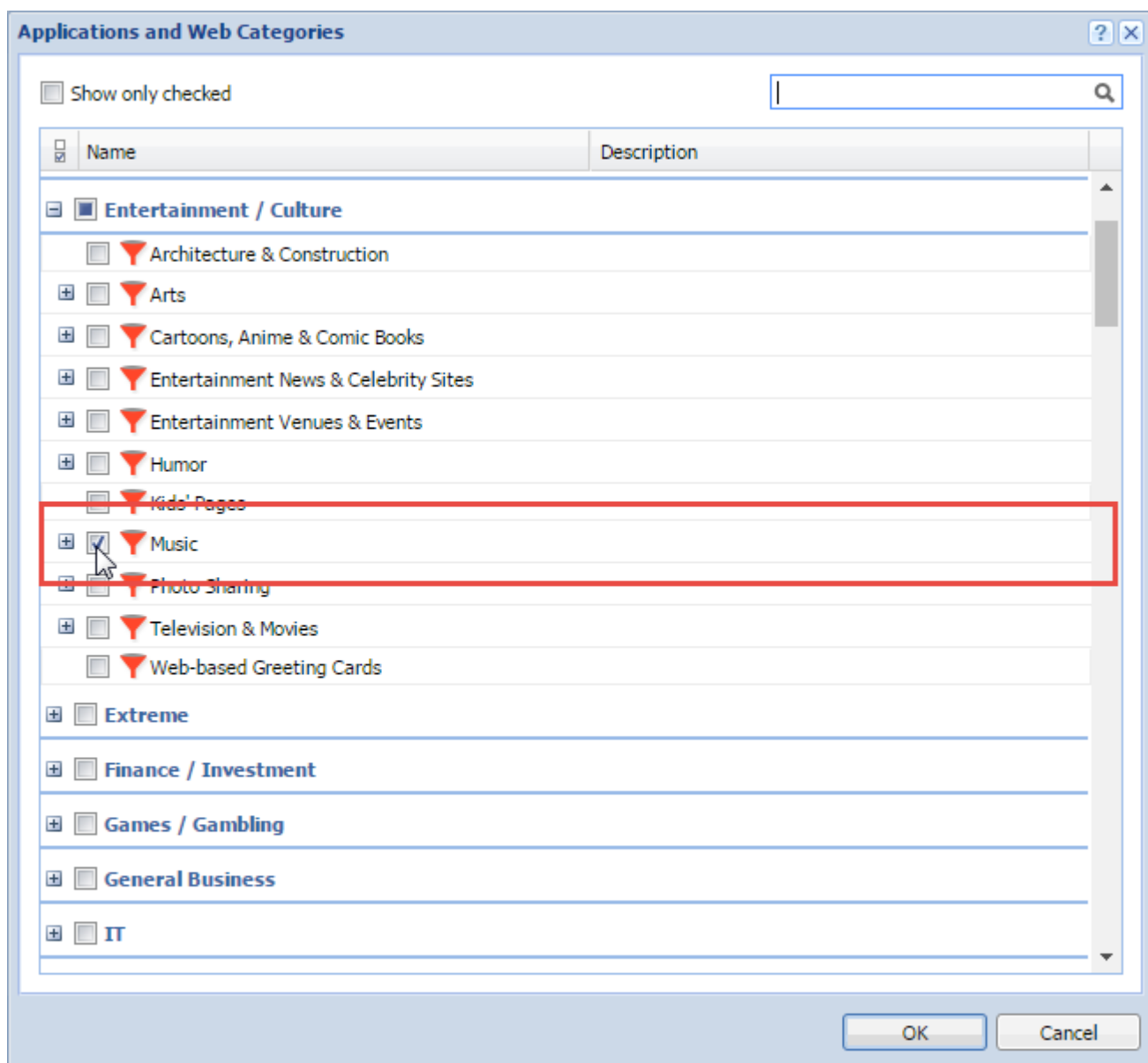
Example: Limiting music access

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**.



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							
<input type="checkbox"/>	Name	Traffic	Download	Upload	Interface	Valid Time	<input type="checkbox"/> 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**.

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

Active Connections					
1180 items (0 selected)					
Traffic Rule ▲	Service	Source	Destination	Info	
Internet access (NAT)	40030/UDP	192.168.44.138	111.221.77.161		
Internet access (NAT)	40022/UDP	192.168.44.138	157.55.235.166		
Internet access (NAT)	47562/UDP	192.168.44.138	147.228.127.78		
Internet access (NAT)	40018/UDP	192.168.64.129	65.55.223.22		
Internet access (NAT)	HTTPS	192.168.64.146	216.58.209.162	DoubleClick	
Internet access (NAT)	XMPP	192.168.44.147	74.125.133.125	Jabber	
Internet access (NAT)	HTTPS	192.168.44.137	191.232.139.128		
Internet access (NAT)	HTTPS	192.168.12.90	178.237.19.121	ICQ	
Internet access (NAT)	40004/TCP	192.168.12.90	157.55.235.170	TeamSound	
Internet access (NAT)	HTTPS	192.168.12.90	191.232.139.13		

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

NOTE

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

If you have existing rules based on the following web categories, you need a Kerio Control Web Filter license.

- » 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

4.5.3 Configuring FTP policy

FTP policy overview

Available in Kerio Control 8.1 and older. FTP policy is included in [the new content filter](#).

Kerio Control provides a wide range of filters for FTP protocol. You can block access to undesirable servers, block certain types of files with this tool.

Here are the main purposes of FTP content filtering:

- » access to certain FTP servers is denied
- » limitations based on or filenames
- » transfer of files is limited to one direction only (i.e. download only)
- » certain FTP commands are blocked

Conditions for FTP filtering

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

1. Traffic must be controlled by a FTP protocol inspector. The FTP protocol inspector is activated automatically unless its use is denied by traffic rules.
2. Secured FTP traffic (FTPS) cannot be filtered.
3. FTP rules are applied also when the Kerio Control's proxy server is used. However, FTP protocol cannot be filtered if the parent proxy server is used. In such a case, FTP rules are not applied.

Enabling FTP rules

1. In the administration interface, go to **FTP Policy**.
2. Enable predefined rules:
 - **Forbid resume due to antivirus scanning** — blocks download resumption after interruption. This rule can increase effectivity of the antivirus control (each file will be checked as a whole). However, if larger files are transferred, it can be counterproductive — repeating of the whole transfer would burden Internet connection redundantly.
 - **Forbid upload** — blocks uploading files to FTP servers. This is one of the methods that can be used to avoid leak of fragile information from the local network.
 - Two rules that block audio and video files downloads — these files are usually large and their download burdens Internet connection.
3. Click **Apply**.

Creating a FTP rule

The usage will be better understood through the following example that describes a rule allowing selected user John Smith to send files without antivirus scanning from server `example.com`:

1. In the administration interface, go to **FTP Policy**.
2. Click **Add** and type a name of the rule.
3. Double-click **Action** and select **Allow**.
4. In the **Properties** column, select **Skip antivirus scanning**.
5. Double-click **Server**, select the **server** option and type `example.com`.
6. Double-click **Users** and select user John Smith.
7. Click **Apply**.

4.5.4 Configuring HTTP policy

IMPORTANT

Available in Kerio Control 8.1 and older. The new Content Filter is described in article [Configuring the Content Filter](#).

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

Here are the main purposes of HTTP content filtering:

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

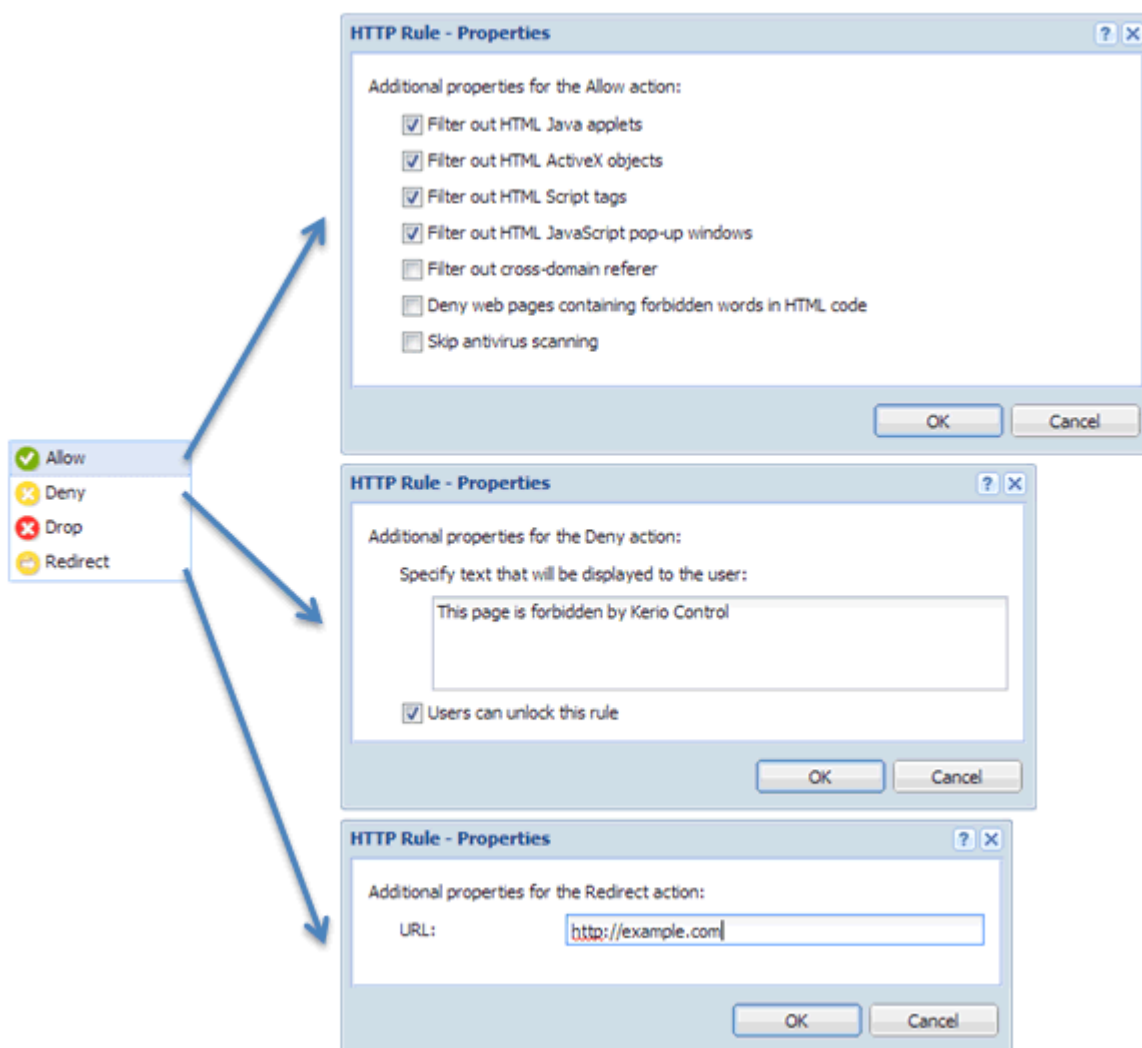
Conditions for HTTP filtering

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

1. Traffic must be controlled by the HTTP protocol inspector. The HTTP protocol inspector is activated automatically unless its use is denied by traffic rules.
2. Kerio Control performs URL based filtering for encrypted traffic (HTTPS protocol). Learn more in the special article [HTTPS filtering specifics](#).

Adding HTTP rules

1. In the administration interface, go to **HTTP Policy**.
2. On tab **URL Rules**, click **Add**.
3. Type a name of the new rule.
4. Double-click **Action** and select:
 - **Allow** — traffic allowed, user does not even notice anything happening. In the **Properties**, you can add additional actions.
 - **Deny** — user will be redirected to the firewall page with information that access is denied. In the **Properties**, you can add information about forbidden pages and you can check **Users can unlock this rule**. All unlocked pages are logged in the Security log.
 - **Drop** — access is denied and the user will see the page as unavailable.
 - **Redirect** — user will be automatically redirected to the specified URL.



5. Double-click **URL** and set:

- **Site** — any URL starting with the specified string. It is possible to use wildcards * (asterisk) and ? (question mark). **Example:** Blocking rule for *.kerio.com blocks access to `http://www.kerio.com/`, `http://mail.kerio.com/` and `http://kerio.com/`, yet not to `http://www.mykerio.com/` or `http://mykerio.com/`.
- **URL from the group** — you can select from existing groups or you can go to **Definitions > URL Groups** and add a new one (see section [URL Groups](#)).
- **URL rated by Kerio Control Web Filter rating system** — all pages sorted in the selected categories by the Kerio Control Web Filter module.
- **Any URL where server is specified by an IP address** — this can be used only for unsecured traffic (HTTP).
- **Also apply to secured connections (HTTPS)** — Kerio Control will apply the domain part of the defined URL to this rule for secure websites.

6. Double-click **Users** and decide to whom the rule will apply.

7. Double-click **MIME Type** and select one option. MIME type of downloaded files. It is possible to use wildcard * (asterisk) for any MIME type.

8. Double-click **Valid Time** and select a time range. You can create a new time range in **Definitions > Time Ranges**.

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

10. Click **Apply**.

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

NOTE

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

Applying rules also for local servers

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

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

URL Groups

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

The default Kerio Control installation already includes predefined URL groups:

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

NOTE

These URL groups are used in predefined URL rules.

Defining a new URL group

1. In the administration interface, go to **Definitions > URL Groups**
2. Click **Add**.
3. Type a name for the group.
4. In **Type**, select **URL**. URL can be specified as follows:

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

Examples:

`www.example.com/index.html` — a particular page

`www.*` — all URL addresses starting with `www.`

`*sex*` — all URL addresses containing the `sex` string

sex?? .cz — all URL addresses containing such strings as sexxx .cz, sex99 .cz, etc.

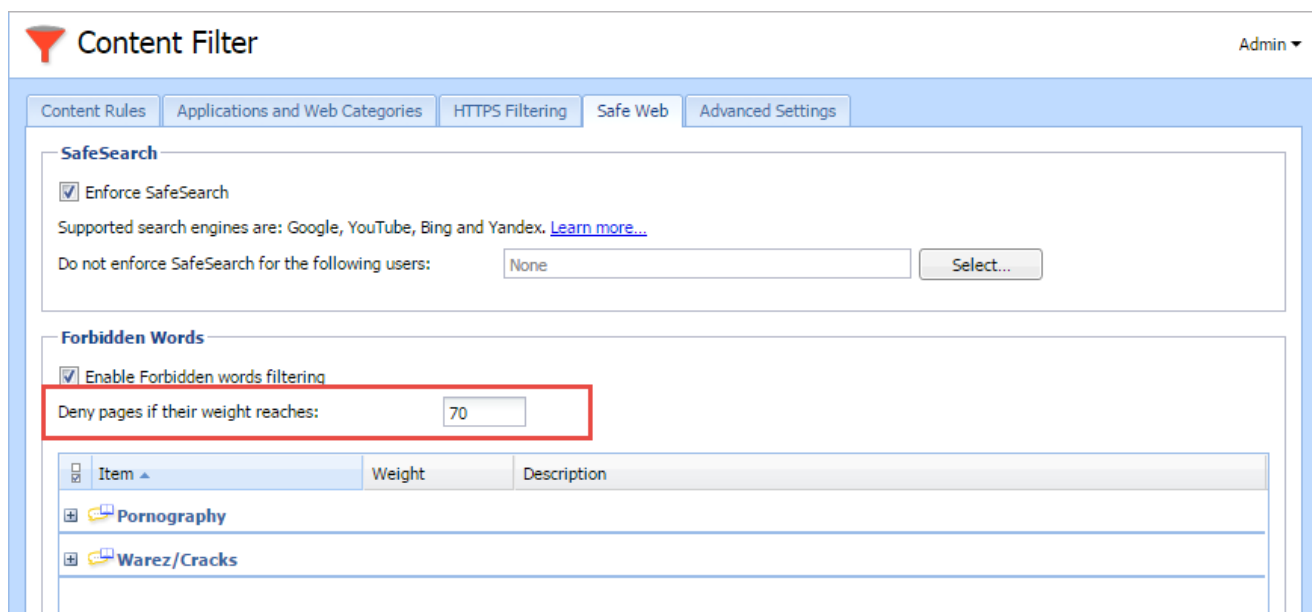
5. Save the settings.

You can use the URL group in URL rules.

4.5.5 Filtering web content by word occurrence

Kerio Control filters web pages that include undesirable words.

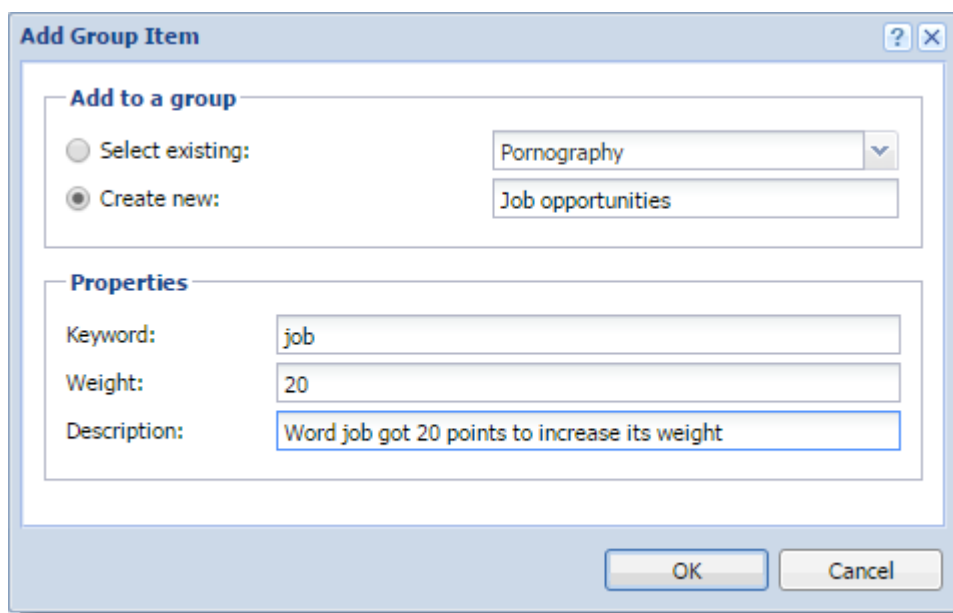
Filtering mechanism: Forbidden words get a weight (a whole positive integer). If a web page includes more forbidden words, weights are summed (weight of each word is counted only once). If the total weight exceeds the defined limit (see screenshot below), the page is blocked.



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



6. Click **OK**

7. On the **Safe Web** tab, click **Apply**.

4.5.6 Blocking inappropriate or explicit content in search results

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:

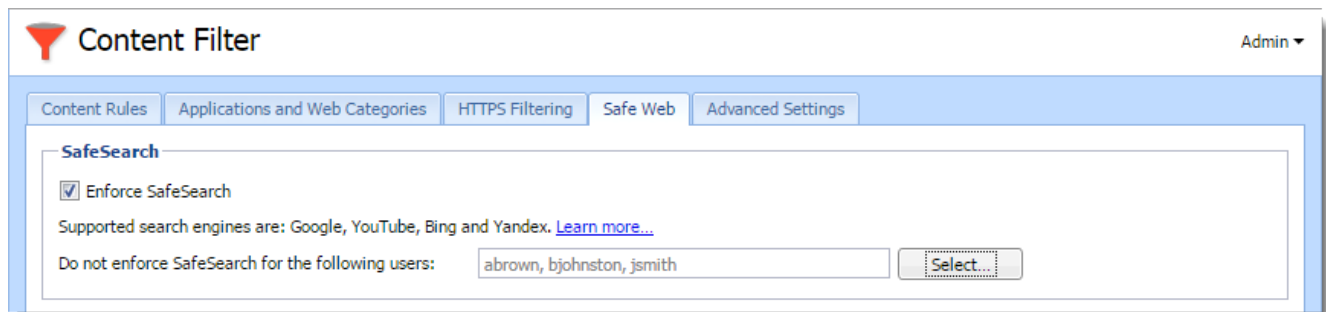
1. In the administration interface, go to **Content Filter > Safe Web**.
2. Click **Enforce SafeSearch**.

3. Click **Apply**.

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

NOTE

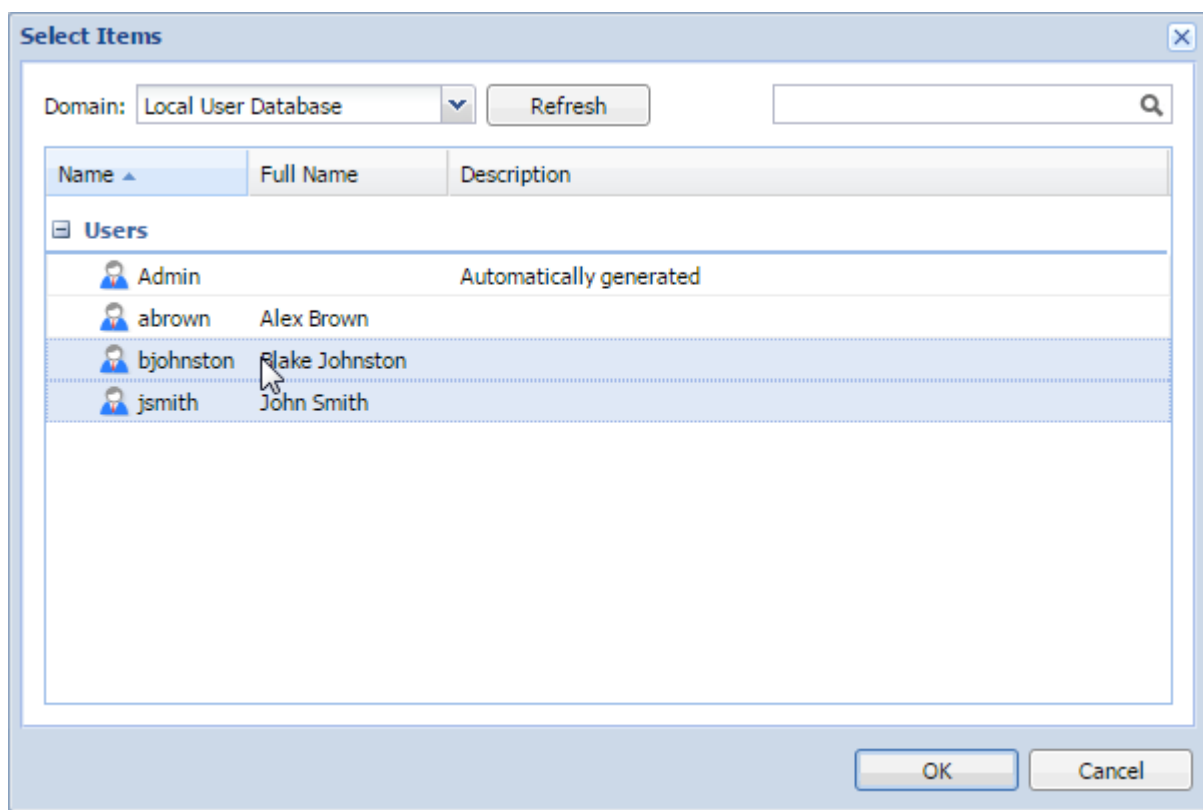
Because of DNS limitations, SafeSearch does not block content cached in browsers and user computers before enabling SafeSearch. You can flush caches in your browser and computer or wait for rewriting the caches. It may take up to 24 hours.



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.

4.5.7 Filtering HTTPS connections

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](#).

NOTE

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.

WARNING

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.

The screenshot shows the 'Content Filter' administration interface. The 'HTTPS Filtering' tab is selected. Under 'HTTPS decryption', both 'Decrypt and filter HTTPS traffic' and 'Show Legal Notice to users' are checked. Below this, there are links for 'Learn more about HTTPS filtering' and 'how to install certificate on client OS or via Active Directory®'. Under 'HTTPS Filtering Exceptions', the 'Exclude specified traffic from decryption' radio button is selected. There are two input fields: 'Traffic to/from IP addresses which belong to:' with a dropdown menu showing 'HTTPS exclusions' and an 'Edit...' button, and 'Traffic from the following users:' with a text box containing 'abrown, bjohnston' and a 'Select...' button. At the bottom right, there are 'Apply' and 'Reset' buttons.

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:

- » IP addresses
- » users

Excluding traffic to/from IP addresses

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.

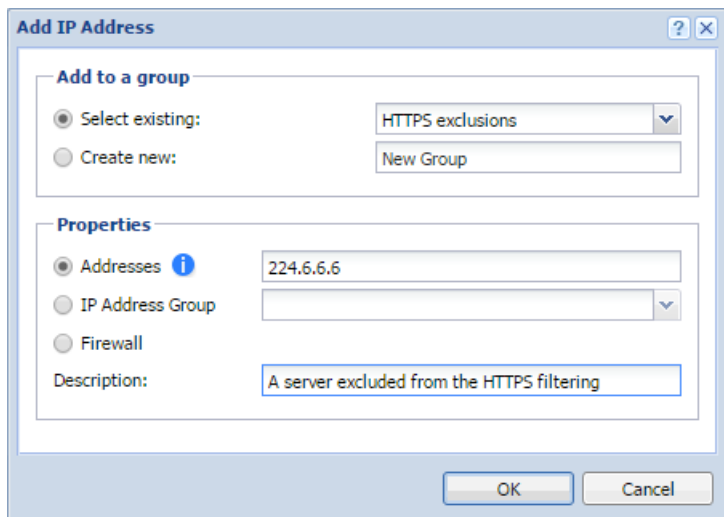
To set exceptions for an web application, you must know its IP address, domain name, or hostname:

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.

WARNING

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.



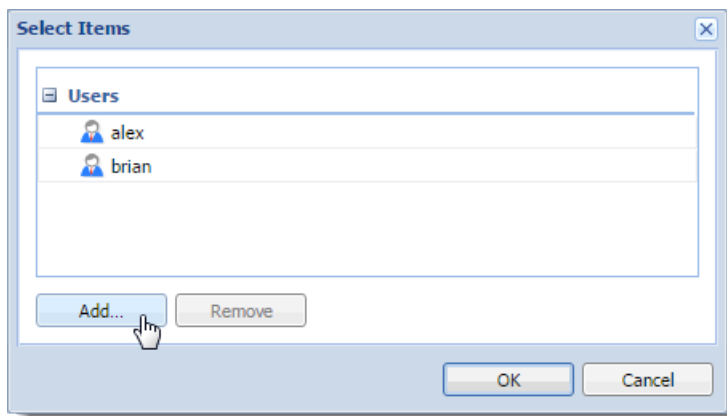
NOTE

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.
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.

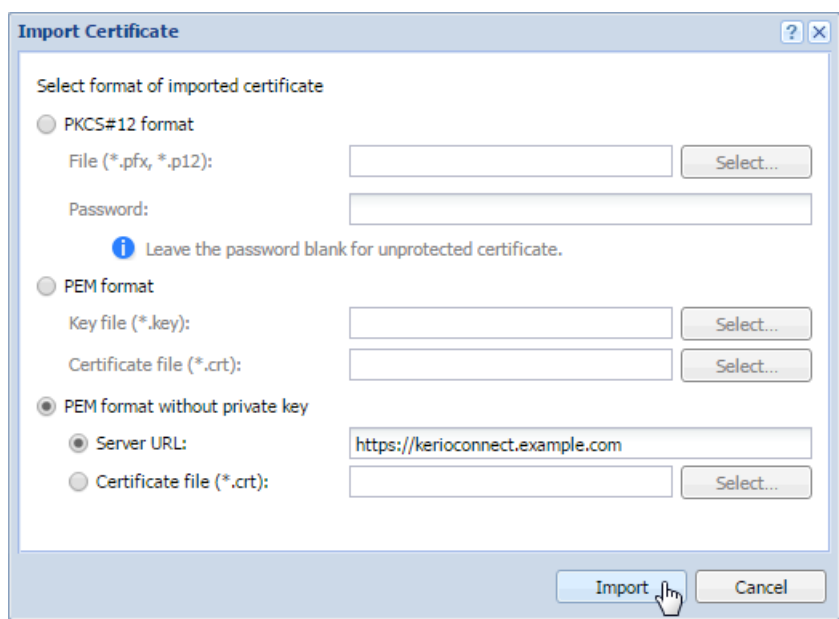
Importing a certificate for an untrusted web applications into Kerio Control

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**.



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

4.5.8 HTTPS filtering specifics

Kerio Control 8.4.0 and higher includes a full HTTPS filter. Read more in the [Filtering HTTPS connections](#) article. However, if you do not want to use the full HTTPS filter, be aware of the following facts:

- » HTTPS filtering of URLs is limited only to the domain name. The resource identifier part of the request (e.g. /path/index) is not considered as part of the condition of a rule unless non-transparent proxy server is used.
- » It is not possible to filter individual objects at HTTPS servers.
- » For technical reasons, it is not possible to apply HTTPS blocking to clients using Internet Explorer on Windows XP.

4.5.9 Using Kerio Control Web Filter

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.

NOTE

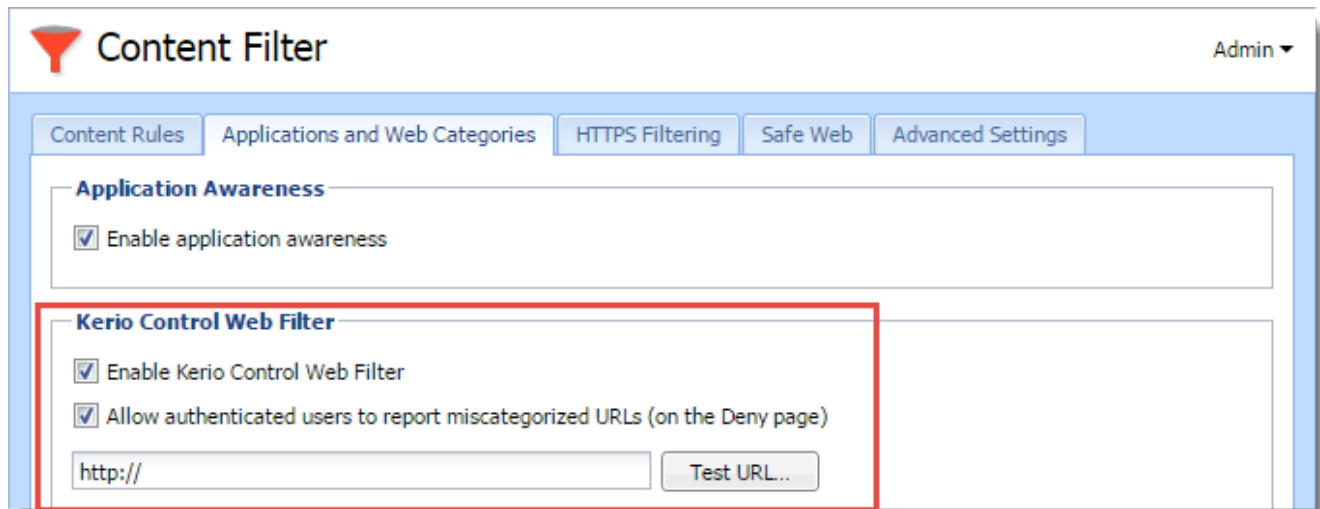
Kerio Control Web Filter requires a special license. Unless Kerio Control includes this module, it behaves as a trial version only (this means that it is automatically disabled after 30 days from the Kerio Control installation and options in the **Applications and Web Categories** tab will not be available).

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 **Applications and Web Categories**.
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 **Applications and Web Categories**.
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. `*.kerio.*`). An asterisk stands for any number of characters (even zero), a `*.kerio.*` 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](#).

4.5.10 Slow Internet connection with activated Kerio WebFilter

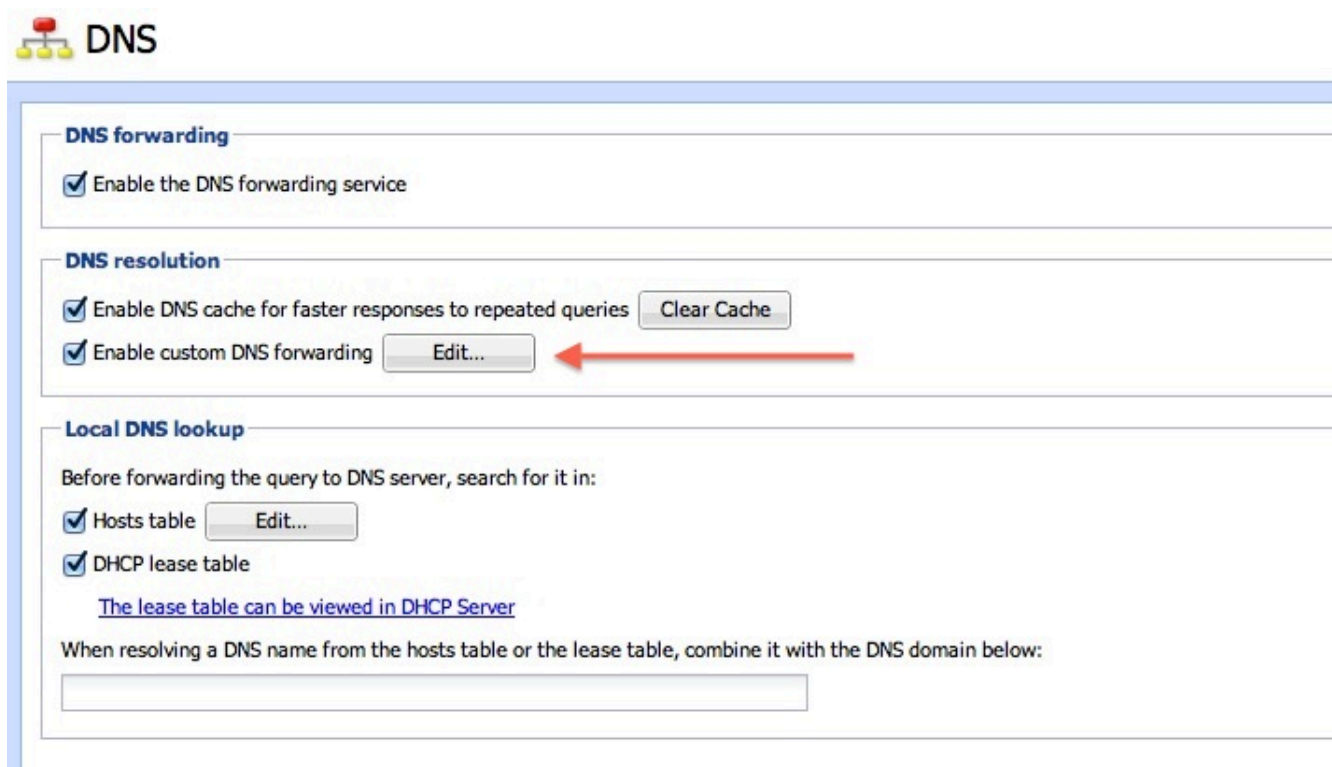
You experience slow internet connections with Kerio WebFilter activated. Some pages load very slowly and some pages do not load at all.

Details

The cause of this issue is how some ISPs handle requests to their DNS. As the Kerio WebFilter makes a lot of requests to the database of zvelo.com to categorize pages, some ISPs have a maximum of fast requests to their DNS servers in a given time period. The Deutsche Telekom for example.

To avoid the requests to zvelo.com slowing down your internet connection, you need to configure a custom DNS forward in the DNS section of Kerio Control.

1. Login to the Web Admin of your Kerio Control and navigate to the "DNS" section
2. Tick the box "Enable custom DNS forwarding" and click "Edit.."



3. For the "DNS name" enter the following URL: *zvelo.com and for "DNS server(s)" enter the Google DNS: 8.8.8.8

Custom DNS Forwarding

DNS query type

☒ Match DNS query name

☐ Match IP address from reverse DNS query

DNS name:

Wildcard characters (*, ?) are allowed.

Forwarding

☐ Do not forward

☒ Forward the query

DNS server(s):

Use semicolons (;) to separate individual entries.

OK Cancel

4. Click OK and then "Apply" to save your changes to your configuration.

5. Reboot the Kerio Control

Your internet connection should be fast and responsive again.

4.5.11 Eliminating Peer-to-Peer traffic

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.

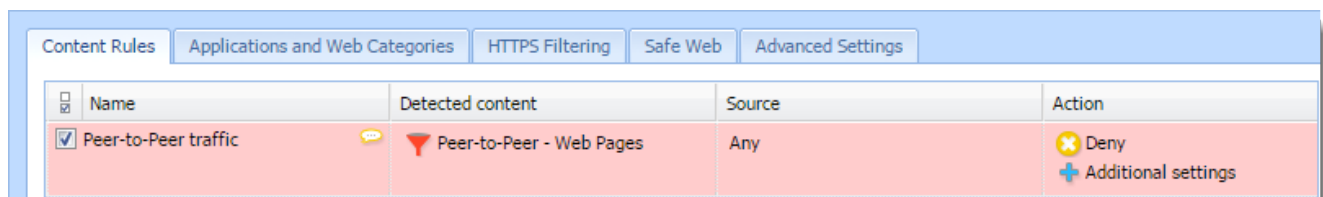
Configuring/Adding the P2P traffic rule




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.
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.



Content Rules				
Applications and Web Categories				
HTTPS Filtering				
Safe Web				
Advanced Settings				
<input type="checkbox"/>	Name	Detected content	Source	Action
<input checked="" type="checkbox"/>	Peer-to-Peer traffic	 Peer-to-Peer - Web Pages	Any	 Deny  Additional settings

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

NOTE

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.

IMPORTANT

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).

4.6 Bandwidth optimization

This section provides information about creating and configuring bandwidth rules and their order.

4.6.1 Configuring bandwidth management	284
4.6.2 Configuring policy routing	289
4.6.3 Setting limit per host	292
4.6.4 Detecting large data transfers	293
4.6.5 Bandwidth management - setting the speed of the link	294

4.6.1 Configuring bandwidth management

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

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.

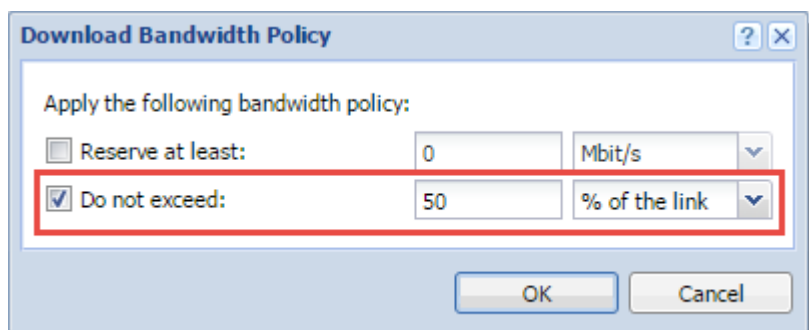
Example: For an ADSL line with a declared 8192/512 Kbit/s, set the download speed to 6250 Kbit/s and the upload speed to 400 Kbit/s.

Configuring bandwidth management rules

Limiting bandwidth for Alex Smith

Suppose you want to restrict user Alex 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 (Alex Smith).
4. Double-click **Traffic**.
5. In the **Traffic** dialog box, click **Users and Groups**, select users or groups, and click save.
6. Double-click **Download**, check **Do not exceed**, and set the limit as shown here:



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.

NOTE

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

Alex Smith can use max. 50% of the link in all interfaces during the work hours. Downloading is slower now for Alex.

Bandwidth Management and QoS							Admin ▾
The Bandwidth Management allows you to fine-tune your Internet bandwidth utilization. You can reserve as well as limit bandwidth for selected traffic.							
Bandwidth Management rules							
Name	Traffic	Download	Upload	Interface	Valid Time	Chart	
<input checked="" type="checkbox"/> VPN	VPN	Reserve: 32 KB/s	Reserve: 32 KB/s	All			
<input checked="" type="checkbox"/> Remote Access	Remote Access	Reserve: 20% of the li...	Reserve: 20% ...	All			
<input type="checkbox"/> SIP VoIP	SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All			<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Alex Smith's rule	asmith	Limit: 50% of the link	No limit	All	Working hours		<input checked="" type="checkbox"/>
Other traffic	Any	No limit	No limit	All			

NOTE

You can create a similar rule for the whole user group. Kerio Control applies the limit to all users added to the rule together. It doesn't matter if you add users to the rule separately or in user groups.

Reserving bandwidth for sales and support departments

Suppose you want to reserve 20 Mbit/s for sales and support departments in all interfaces because they need to communicate with customers with a company online portal:

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 (Sales and Support reservation).
4. Double-click **Traffic**.
5. In the **Traffic** dialog box, click **Users and Groups**.
6. In the **Select Items** dialog box, select user groups for sales and support people.
7. Click OK twice.
8. In the **Bandwidth Management rules** tab, double-click **Download** in the **Sales and Support reservation** row.
9. In the **Download Bandwidth Policy** dialog box, select **Reserve at least** and set 20 Mbit/s.

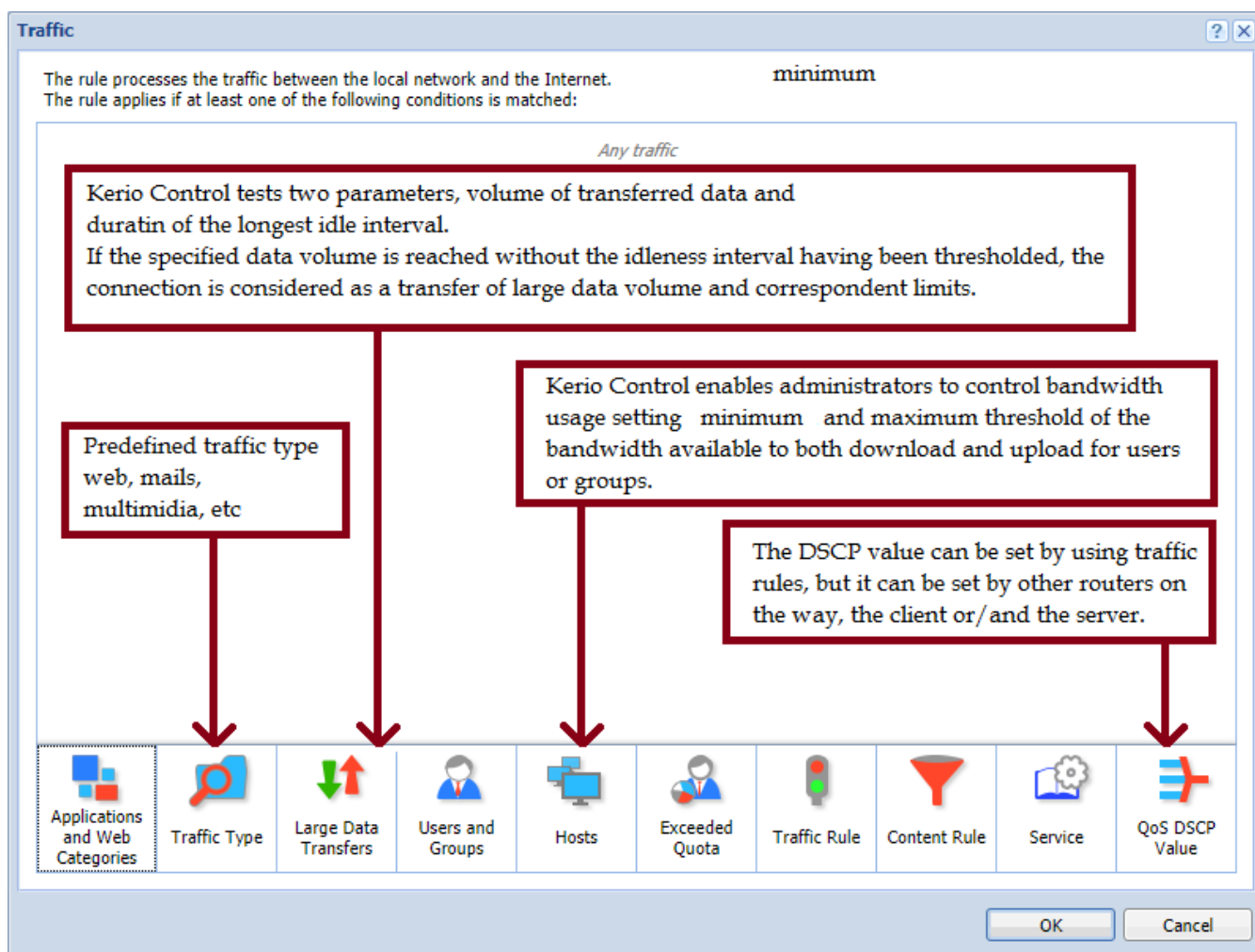
10. Click OK.
11. In the **Bandwidth Management rules** tab, double-click **Upload** in the **Sales and Support reservation** row.
12. In the **Upload Bandwidth Policy** dialog box, select **Reserve at least** and set 20 Mbit/s.
13. Click **OK**

From now on, all users from the support and sales department have reserved 20 Mbit/s for communication with their customers. Kerio Control applies the limit to all users added to the rule together. It doesn't matter if you add users to the rule separately or in user groups.

Traffic types used in bandwidth management

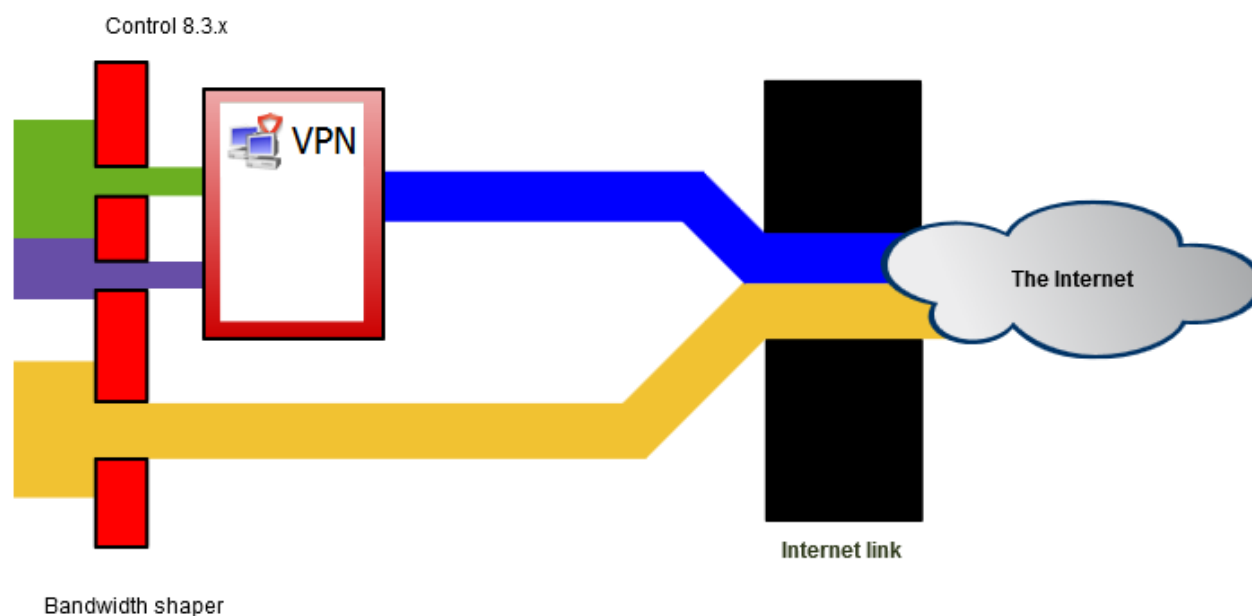
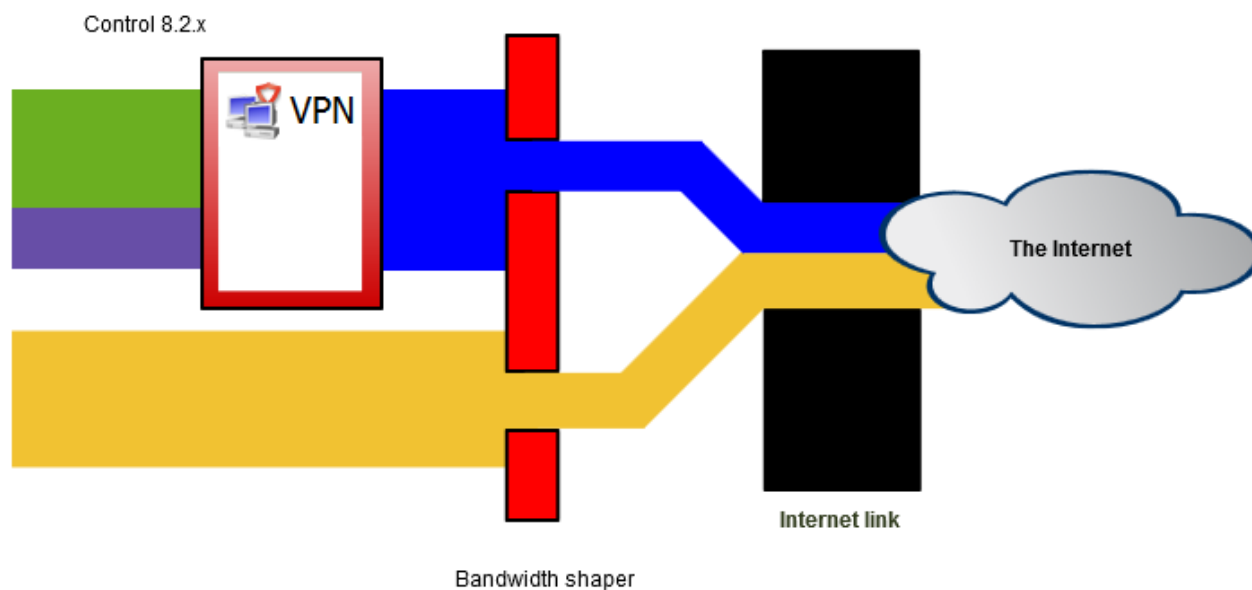
You can apply limit or reserves on bandwidth to different types of traffic. You can select them in the **Traffic** column:

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 **User Groups** section includes bandwidth usage control setting a minimum and maximum threshold of the bandwidth available to both download and upload for host, networks and address ranges.
5. The **Hosts** section includes
6. The **Exceeded Quota** is connected with user quota settings. For more information, refer to [Managing user quotas in Kerio Control](#) (page 81).
7. 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.



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.



NOTE

In a new installation, the option **Use rules for VPN tunnels before encrypting** 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.

4.6.2 Configuring policy routing

When 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).

NOTE

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 mail server 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	Allow	NAT (Internet 4Mbit)	
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	

The setting of NAT in the rule for email services is shown in the figure below. Allow use of a backup link in case the preferred link fails. Otherwise, email services will be unavailable when the connection fails.

Traffic Rule - Translation

Apply the settings to:

Source NAT

☒ Enable source NAT

Kerio Control will use IPv4 address and IPv6 prefix of the following specified interface for source NAT.

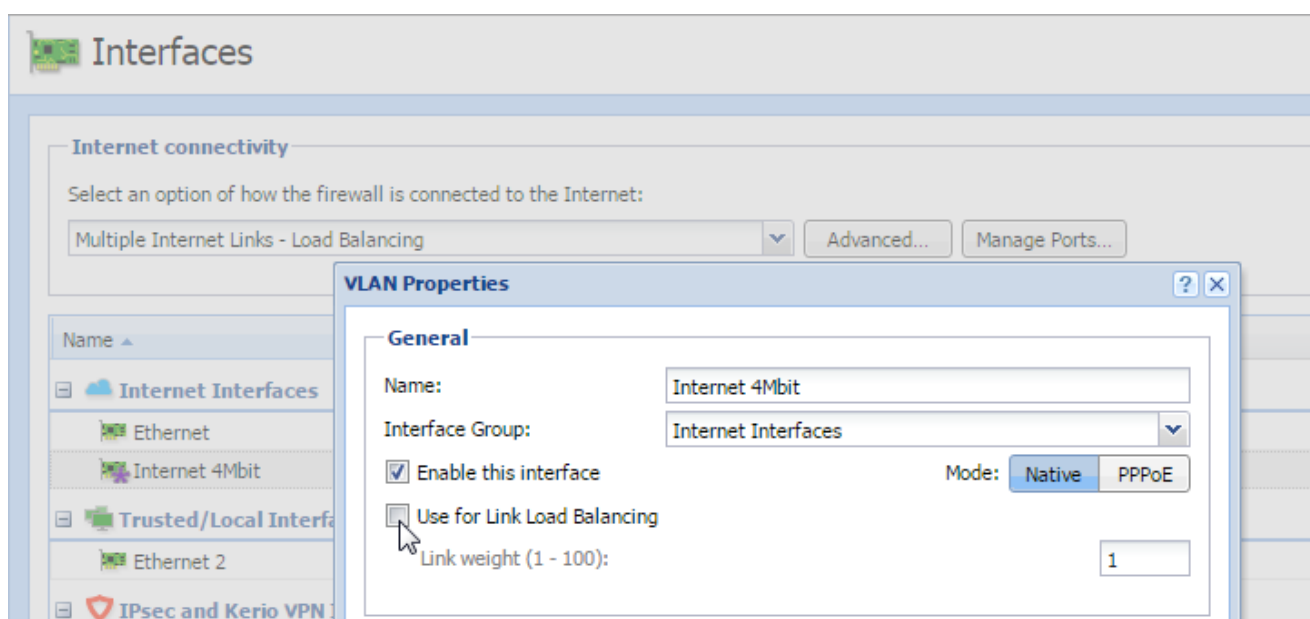
Interface:

☒ Allow using of a different interface if this one becomes unavailable

NOTE

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 the 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.



Configuring an optimization of network traffic load balancing

Kerio Control provides two options of network traffic load balancing:

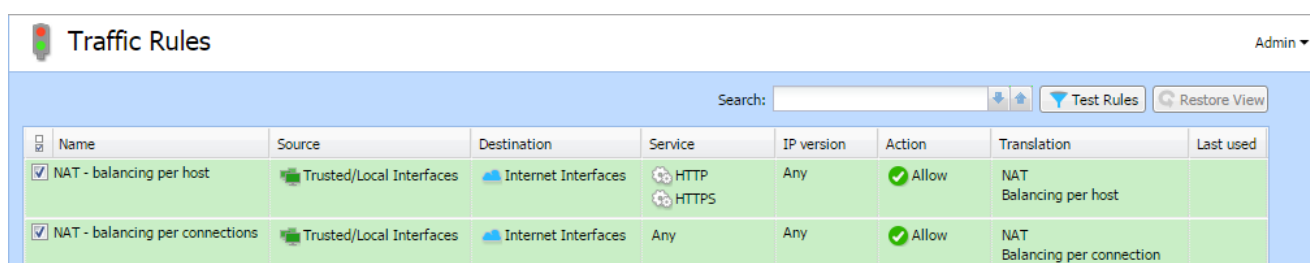
- » per host (clients)
- » per connection

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 a 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.

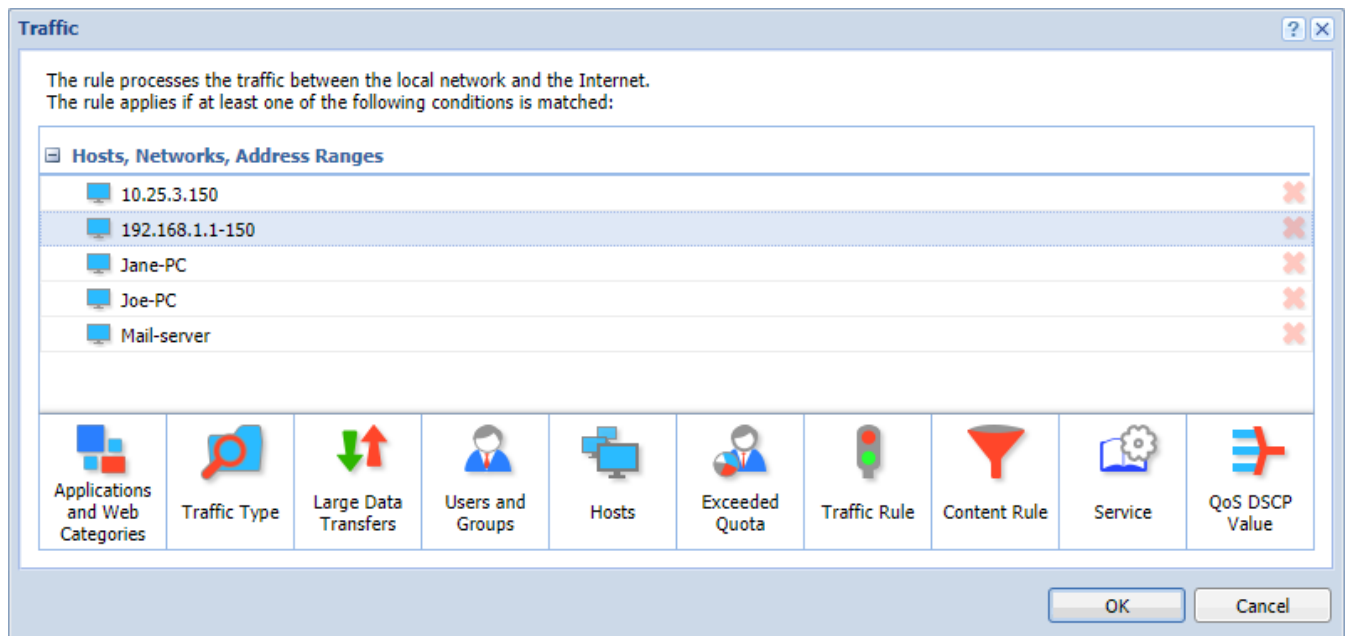


Screenshot 73: Policy routing — load balancing optimization

4.6.3 Setting limit per host

Kerio Control enables administrators to control bandwidth usage setting a minimum and a maximum threshold of the bandwidth available to both download and upload for host, network and IP ranges.

Kerio Control includes bandwidth management, which regulates network traffic to ensure the reliability of essentials services to hosts that need it most, avoiding congestion and slow network speed. For more information, refer to [Configuring bandwidth management](#) (page 284).



To create a policy to set limit per host

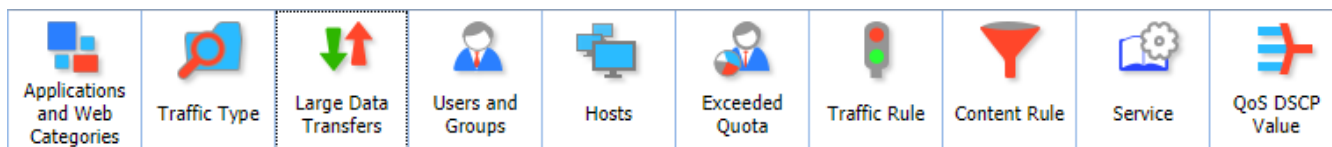
1. In the administration interface, go to **Bandwidth Management and QoS**.
2. To create a new rule, click **Add**.
3. Type a name for the rule.
4. Double-click **Traffic**.
5. In the **Traffic** dialog box, click **Hosts** in the menu in the bottom.
6. Type IP address, IP ranges or hostname of the machines, and click **Ok**
7. Double-click **Download**, set a minimum and a maximum limit using the **Reserve at least** and **Do not exceed** options respectively.
8. Double-click **Upload**, set a minimum and a maximum limit using the **Reserve at least** and **Do not exceed** options respectively.
9. (Optional) Double-click **Interface** to select interfaces. By default, **All** interfaces are selected.
10. (Optional) Double-click **Valid Time** to set a time when the policy is applied. If no values are entered, the policy applies at all time.
11. Click **Apply**.

4.6.4 Detecting large data transfers

Downloading large files can congest your network. You can detect large data transfers with Kerio Control's bandwidth management.

Configuring Kerio Control

When configuring the bandwidth management rules, set the traffic type to **Large data transfer**.



Detecting large data transfers

Kerio Control tests:

- » The volume of the transferred data
- » The duration of the longest idle interval

If Kerio Control detects at least **1000 KB** of data (**200 KB** for Kerio Control 8.6.2 and older) without an interruption of at least **5 seconds**, then the transfer is considered as a large data transfer.

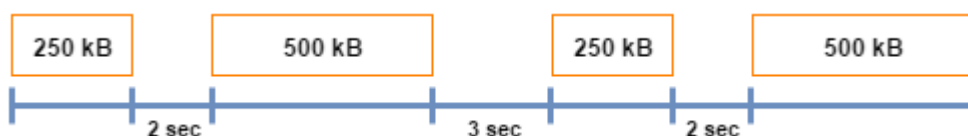
See the following examples for details.

Examples of large data detection

Example 1

After transferring the third data load, Kerio Control detects the transmission as a large data transfer.

The connection has transferred 1000 KB of data with the longest idle interval of three seconds.



Example 2

Kerio Control does not detect the transmission as a large data transfer.

The connections have transferred 750 KB of data followed by a five-second interval.



Example 3

After transferring the third data load, Kerio Control detects the transmission as a large data transfer.

The first data load is followed by a six-second idle interval > Kerio Control does not detect the transmission as a large data transfer and sets the data counter to zero.

When the second and third data load is transferred (1000 KB), the longest idle interval is three seconds > Kerio Control detects a large data transfer.



4.6.5 Bandwidth management - setting the speed of the link

Typically, problems with bandwidth management are caused by the Internet link speed being set incorrectly. To provide the necessary bandwidth for mission-critical applications, Kerio Control enables you to reserve bandwidth for those applications and then automatically limits lower priority traffic to the remaining available bandwidth. However, the bandwidth management feature decreases the link's capacity somewhat. For that reason, Kerio Control needs to know the real bandwidth of the link.

Real link bandwidth

The real bandwidth is the maximum speed of the link's data transmission. Because control information is transmitted in addition to data, the real bandwidth is around 20 percent lower than the speed stated by the ISP.

Technology	Speed stated by ISP	Real speed
SDSL	2 Mbit/s	1592 Kbit/s
ADSL	Download: 8 Mbit/s, Upload: 512 Kbit/s	Download: 6250 Kbit/s, Upload: 400 Kbit/s
Optical fiber	20 Mbit/s	15.8 Mbit/s
Ethernet	100 Mbit/s	79 Mbit/s

How to find out the link's speed

To find out the speed of your link, use an open tool, such as www.speedtest.net.

4.7 Proxy server

This section helps you to configure Kerio Control's proxy server and reverse proxy.

4.7.1 Configuring proxy server	294
4.7.2 Configuring the reverse proxy	297

4.7.1 Configuring proxy server

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).

NOTE

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

WARNING

If you use a non-transparent proxy server, the filtering of HTTPS connections does not work.

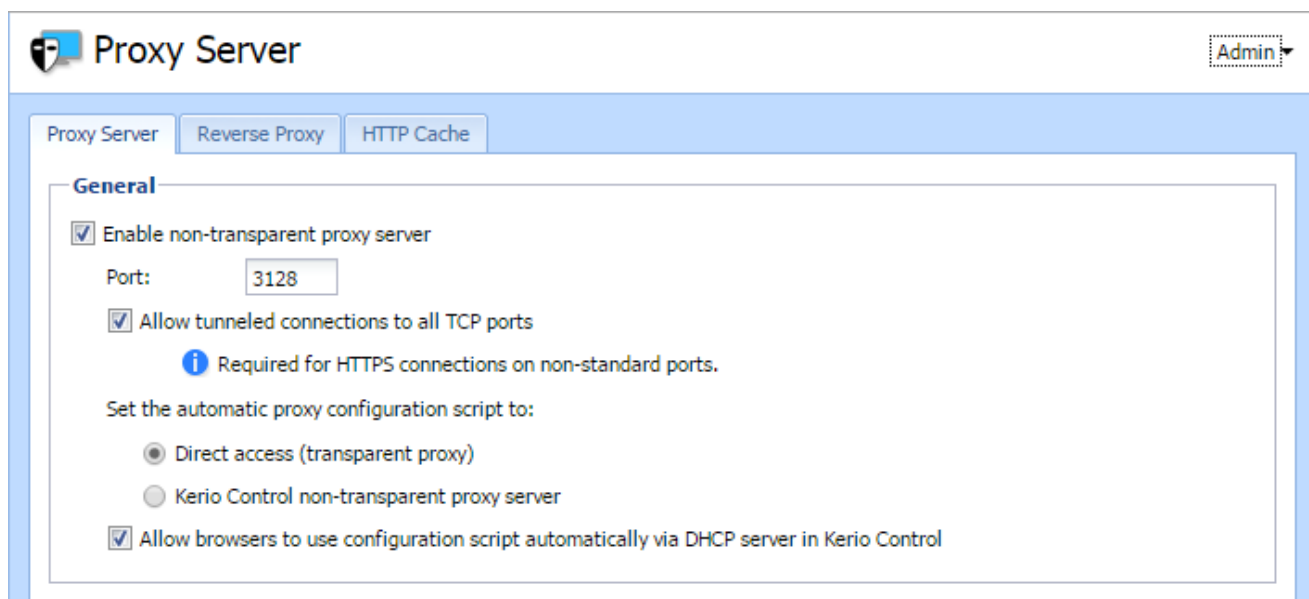
Configuring the proxy server

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**.

NOTE

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:

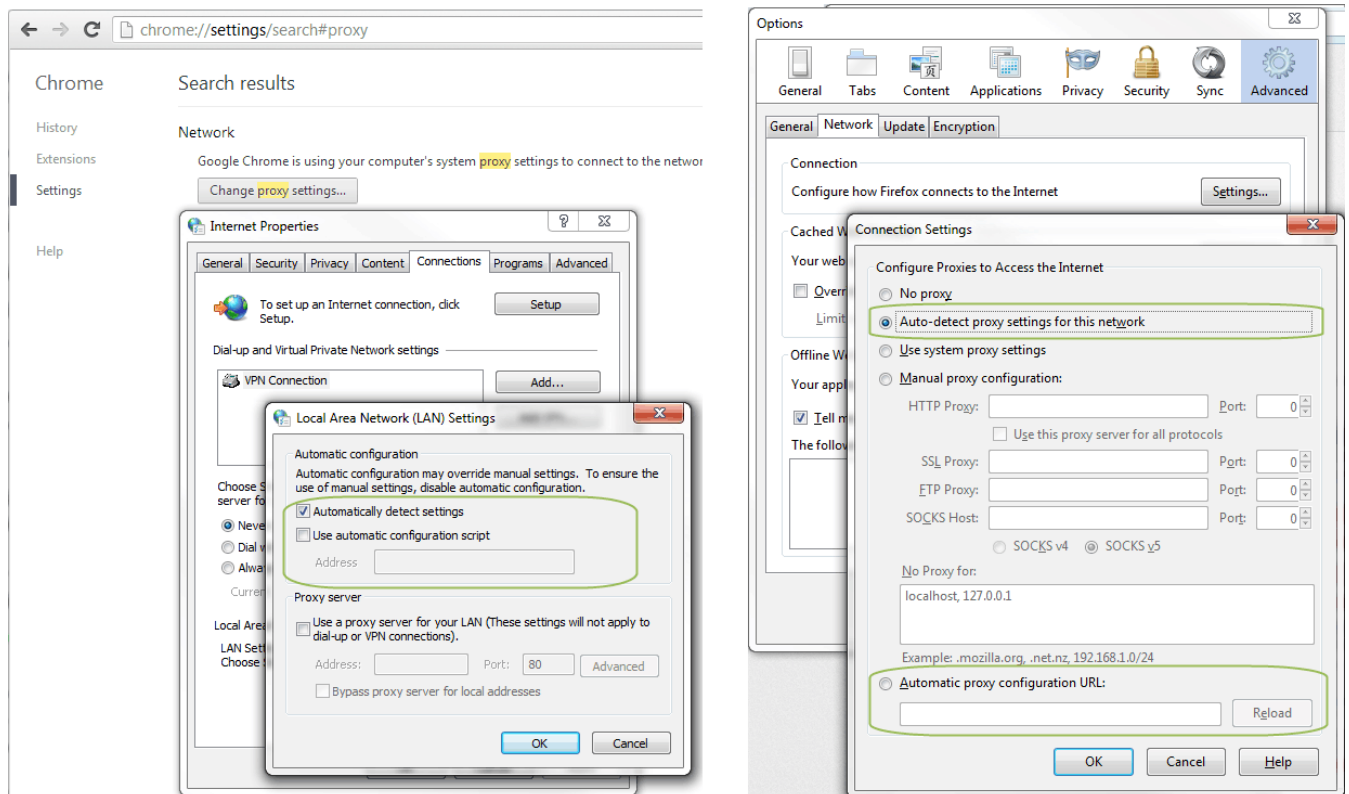
- » Configure browsers manually: type the IP address or DNS name of the proxy server and port (3128 is the default port for Kerio Control) in the proxy server settings in the browser
- » In the Kerio Control administration in the **Proxy Server** section, switch the mode for automatic proxy configuration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

NOTE

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



Forwarding to parent proxy server

You can use a parent proxy server for non-transparent proxy traffic, update checks, Kerio Antivirus 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.

NOTE

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:

4.7.2 Configuring the reverse proxy

Why use the reverse proxy server in Kerio Control

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.

NOTE

Content filter rules are not applied to the reverse proxy traffic in Kerio Control.

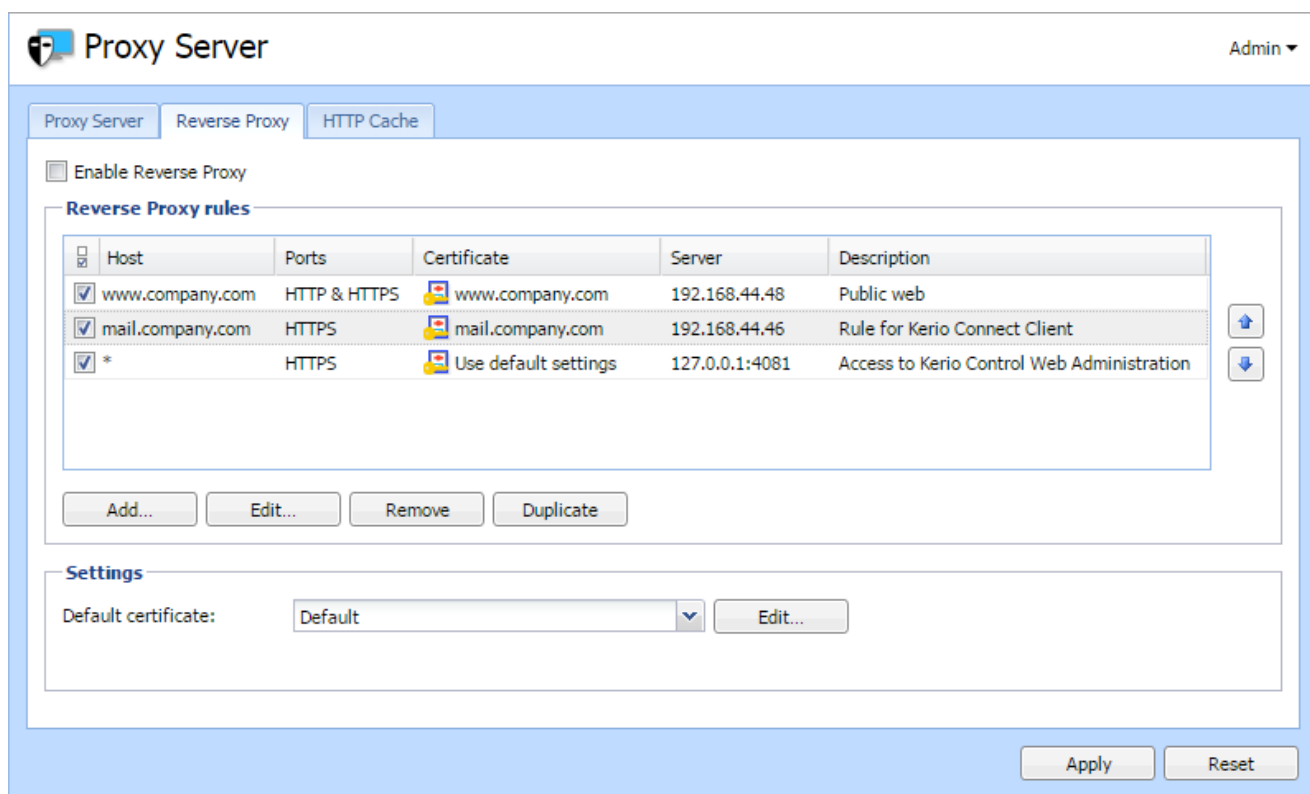
Configuring the reverse proxy

IMPORTANT

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.

IMPORTANT

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.

NOTE

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.

IMPORTANT

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**.

Reverse Proxy Rule

Public server name

Host:

Protocol: ☐ HTTP ☒ HTTPS

Internal server

Server: ☐ Use secured connection

Antivirus: ☒ Perform antivirus scanning

Description:

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

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.

Traffic Rules								Admin ▾
Search: <input type="text"/>								Test Rules Restore View
<input type="checkbox"/>	Name	Source	Destination	Service	IP version	Action	Translation	Last used
<input type="checkbox"/>	VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow		
<input checked="" type="checkbox"/>	Web Services	Any	Firewall	HTTP HTTPS	Any	Allow		
<input checked="" type="checkbox"/>	Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	
<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
<input checked="" type="checkbox"/>	Firewall traffic	Firewall	Any	Any	Any	Allow		just now
<input checked="" type="checkbox"/>	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.

NOTE

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

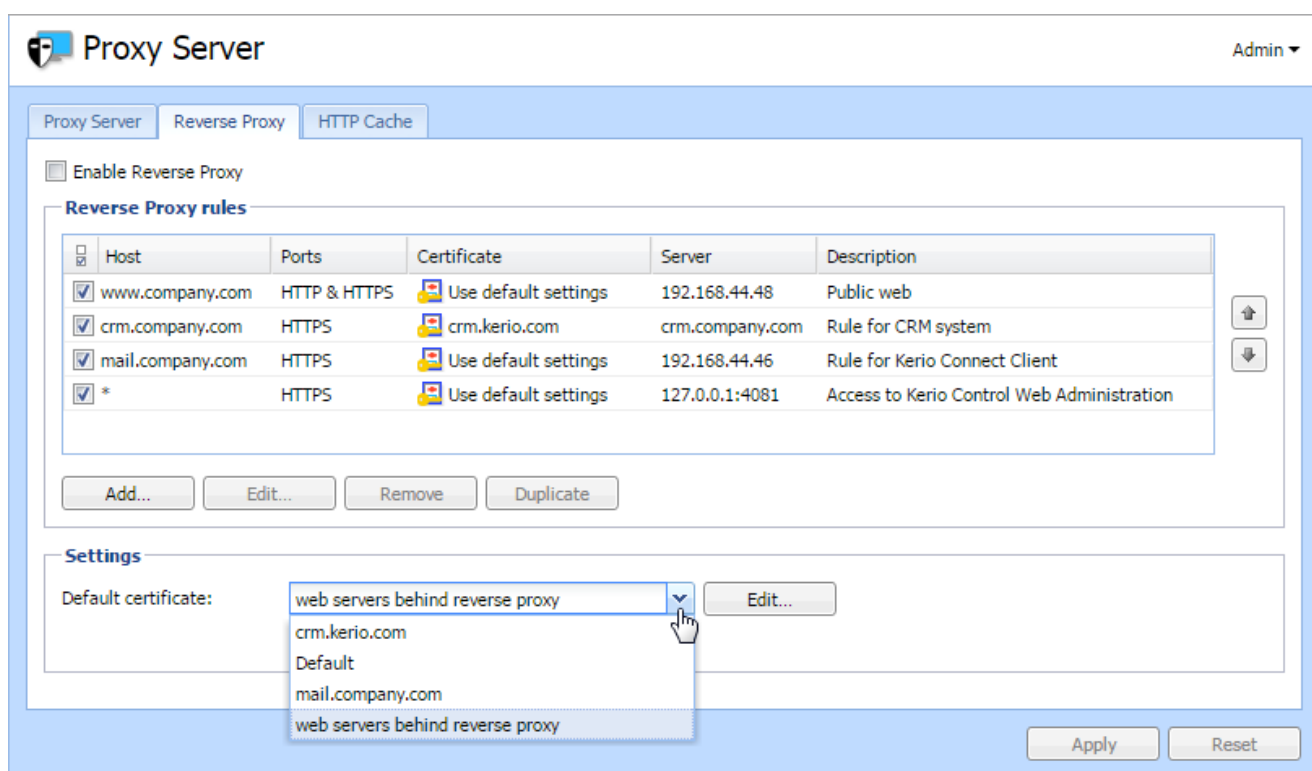
NOTE

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 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 information, refer to [Configuring HTTP cache](#) (page 306).

4.8 Server configuration

This topic contains information about:

4.8.1 Configuring a routing table in Kerio Control	303
4.8.2 Configuring HTTP cache	306
4.8.3 Configuring Service Discovery forwarding in the Kerio Control network	307
4.8.4 Configuring the Kerio Control web interface	308
4.8.5 Configuring system settings date, time, time zone and server name	309
4.8.6 Customizing logo on Kerio Control login page, denial pages and user alerts	312
4.8.7 Customizing the language used in Kerio Control interfaces	312
4.8.8 Configuring statistics and reports	313
4.8.9 Configuring the SMTP server	318
4.8.10 DHCP server in Kerio Control	319

4.8.11 DNS forwarding service in Kerio Control	323
4.8.12 Modifying parameters in Kerio Control configuration	325
4.8.13 Optimizing performance with large segment offload	326
4.8.14 Using RADIUS server in Kerio Control	327
4.8.15 Configuring IP address groups	332
4.8.16 Configuring URL groups	335
4.8.17 Services in Kerio Control	337
4.8.18 Creating time ranges in Kerio Control	338
4.8.19 Configuring Universal Plug-and-Play (UPnP)	340
4.8.20 Using Remote Desktop IP Virtualization	341
4.8.21 Wildcards and regular expressions in URL	342
4.8.22 Dynamic DNS for public IP address of the firewall	342


4.8.1 Configuring a routing table in Kerio Control

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.

NOTE

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

<input type="checkbox"/>	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

Route types

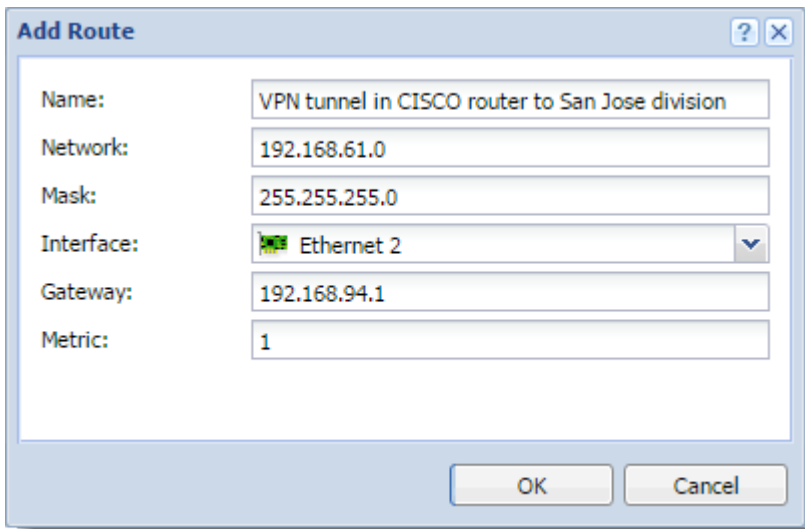
The following route types are available:

- » 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

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 'Add Route' dialog box contains the following fields and values:

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

Buttons: OK, Cancel

4.8.2 Configuring HTTP cache

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.

NOTE

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. For more information, refer to [Configuring proxy server](#) (page 294). Also you can use it for Kerio Control reverse proxy. For more information, refer to [Configuring the reverse proxy](#) (page 297). 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.
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.

4.8.3 Configuring Service Discovery forwarding in the Kerio Control network

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

NOTE

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

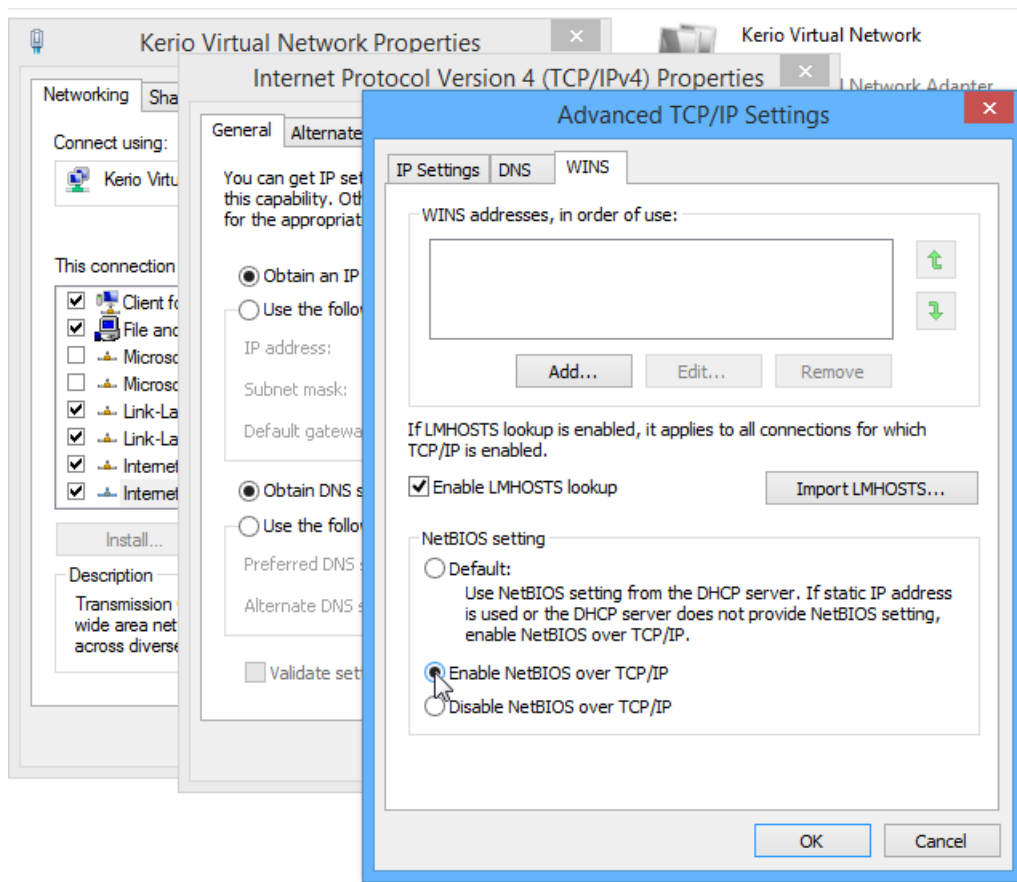
If you have trouble with service discovery forwarding, verify that the firewall is set properly on the client computers.

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.



4.8.4 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**.

IMPORTANT

Unchecking of this option is a security risk.

3. Click **Apply**.

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. For more information, refer to [Configuring SSL certificates in Kerio Control](#) (page 343).

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**.

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

The Kerio Control administration console allows the 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 a correct setting of date, time and time zone on the firewall. Kerio Control allows manual settings or synchronization with an NTP server (recommended).

Date and time settings

Current date and time:

☒ **Keep synchronized with NTP server**

NTP server name:

Use semicolons (;) to separate individual entries.

To configure date and time:

1. In the administration interface, go to **Advanced Options > System Configuration > Date and time settings**.
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

Kerio Control enables easy management of times zones to avoid synchronization problems in various settings.

Time zone settings

Server time zone: ▼

To change your time zone:

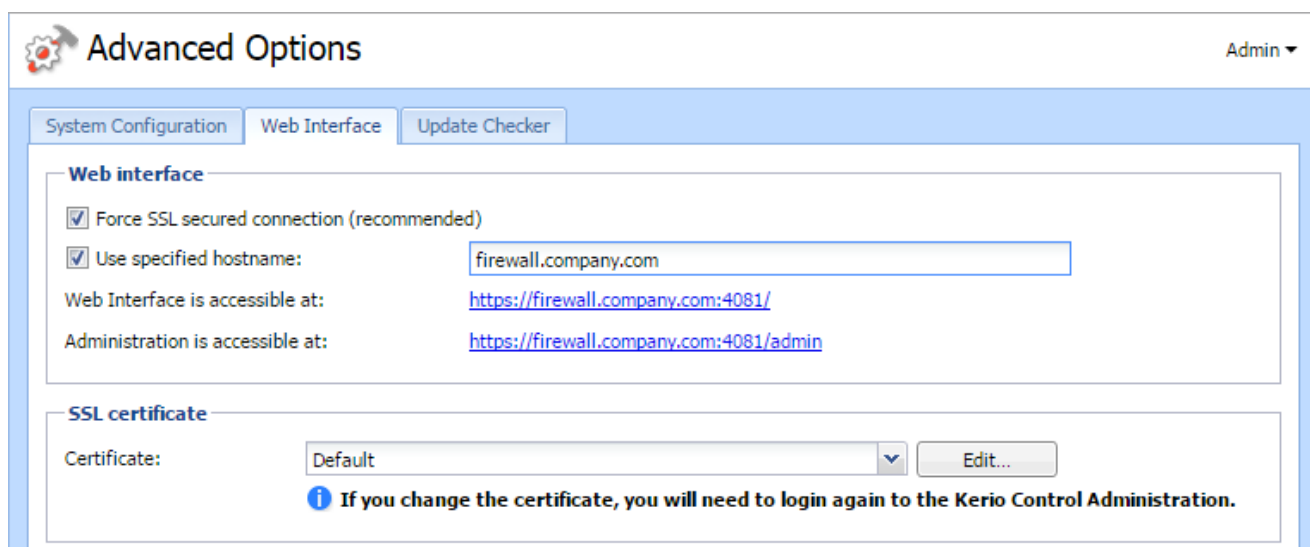
1. In the administration interface, go to **Advanced Options > System Configuration > Time zone settings**.
2. Select a time zone from the **Server time zone** list.
3. Click **Apply**.

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`.

If Kerio Control is not a member of a domain, the hostname will be only `control`. In this case, a problem could occur when using an 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`).



Advanced Options Admin ▾

System Configuration Web Interface Update Checker

Web interface

☒ Force SSL secured connection (recommended)

☒ Use specified hostname:

Web Interface is accessible at: <https://firewall.company.com:4081/>

Administration is accessible at: <https://firewall.company.com:4081/admin>

SSL certificate

Certificate:

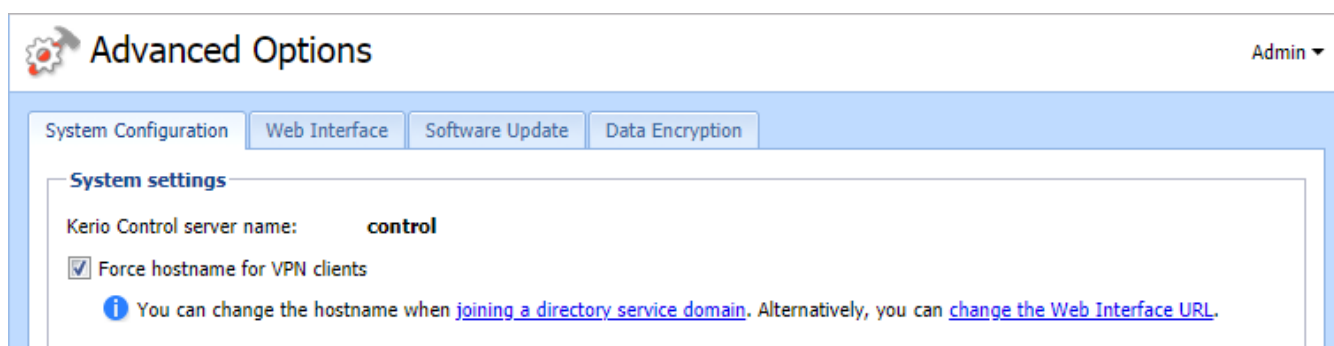
i If you change the certificate, you will need to login again to the Kerio Control Administration.

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**.

Configuring Hostname Settings

Kerio Control offers administrators the option to force hostname for clients connected via the Kerio VPN for 2-step authentication. If this option is selected VPN Clients are redirected to an URL constructed from the hostname to verify the 2-step authentication.



Advanced Options Admin ▾

System Configuration Web Interface Software Update Data Encryption

System settings

Kerio Control server name: **control**

☒ Force hostname for VPN clients

i You can change the hostname when [joining a directory service domain](#). Alternatively, you can [change the Web Interface URL](#).

To force hostname for VPN clients:

1. In the administration interface, go to **Advanced Options > System Configuration > System settings**.
2. Check **Force hostname for VPN clients**.
3. Click **Apply**.

NOTE

You can change the hostname when joining a [directory service domain](#). Alternatively, you can change the [Web Interface URL](#).

4.8.6 Customizing logo on Kerio Control login page, denial pages and user alerts

Kerio Control allows you to customize a logo, page title and favicon on:

- » the login page that allows your users to access to the Internet
- » denial pages
- » user alerts

Login pages for access to Kerio Control administration and Kerio Control Statistics and Reports are not influenced.

Changing a logo

You can change the logo, follow these steps:

1. In the administration interface, go to **Advanced Options**.
2. On the **Web Interface** tab, check the **Use custom logo on login page, denial pages and user alerts** option.
3. To change the title of the page, type the new title to the **Page title** field.
4. To change the logo, click the **Change** button (The recommended size is 300 x 60px.).
5. To change the favicon, click the **Change** button next the favicon preview. Favicon is the icon in the tab header of the login page.

The Kerio Control login page has now the new logo.

4.8.7 Customizing the language used in Kerio Control interfaces

You can set a preferred language for each user in Kerio Control. Kerio Control uses that language for:

- » Kerio Control Administration
- » Kerio Control Statistics
- » All alerts and emails sent by Kerio Control

NOTE

Language settings also affect the format of dates and numbers.

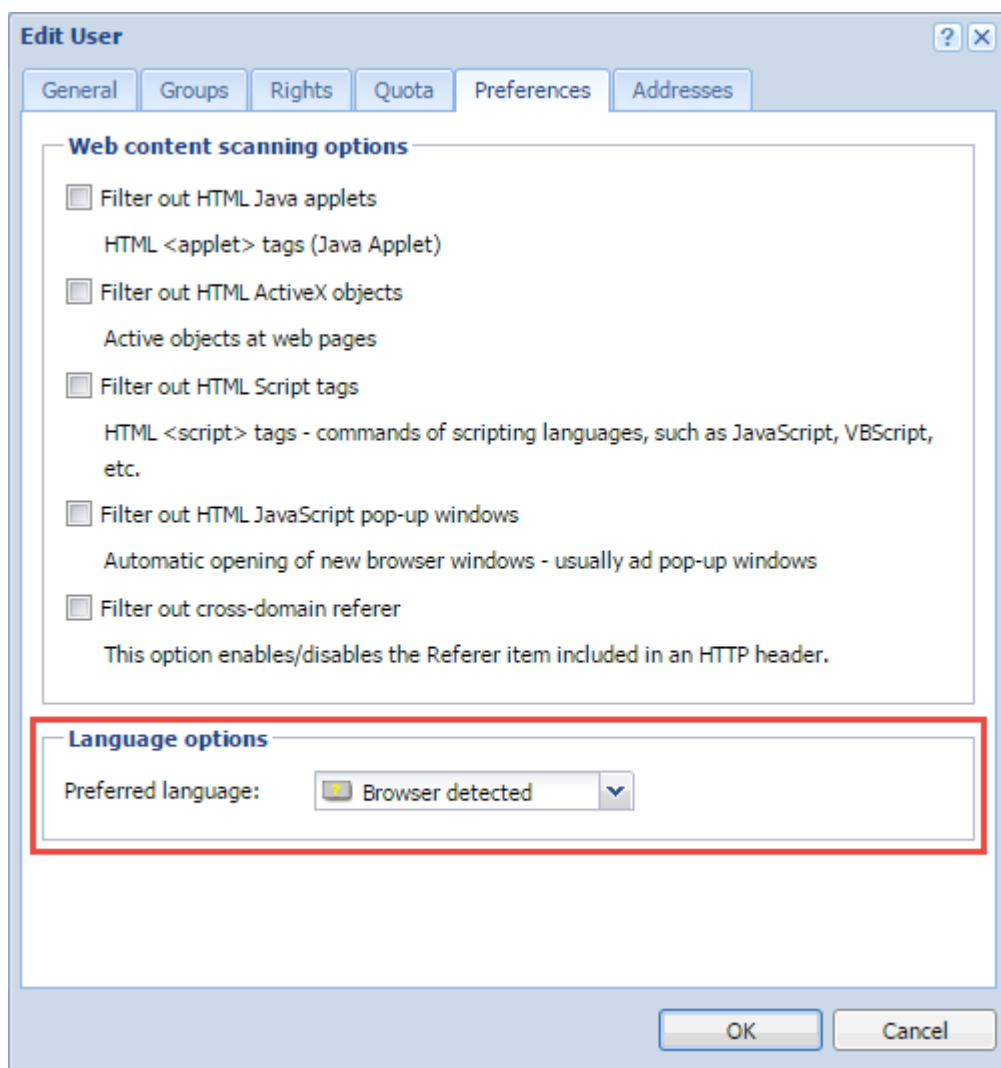
By default, Kerio Control copies the user's browser settings. If that language is not suitable, you can customize it.

Users can also customize the language themselves in the Kerio Control Statistics interface. For more information go to http://go.gfi.com/?pageid=control_help#cshid=1792

Customizing the language for users

1. In the administration interface, go to the **Users** section.
2. Double-click a user's name, or click **Template** to change the language for all users in the domain.
3. In the **Edit User** or **Edit User Template** dialog box, go to **Preferences**.
4. In the **Preferred language** drop-down list, select a language.
5. Click **OK**

This language is now used in Kerio Control Administration, Kerio Control Statistics, and all alert emails.



4.8.8 Configuring statistics and reports

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

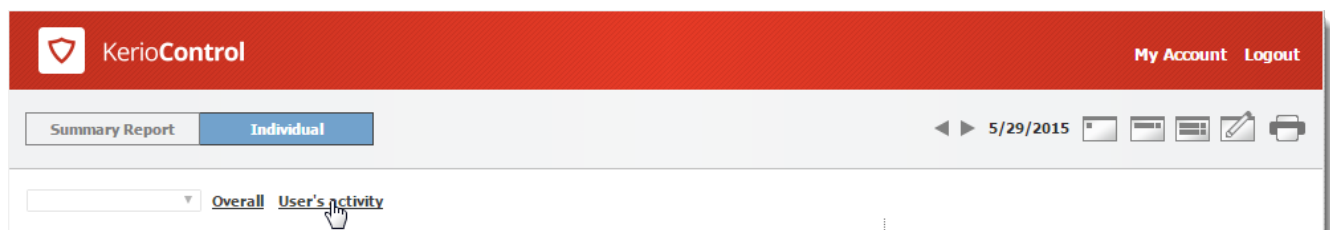
- » The firewall requires user authentication. You can set user authentication in **Domains and User Login > Authentication Options**.

» 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).



WARNING

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.
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.

Accounting and Monitoring Admin ▾

Data Gathering | Access to Statistics | Alert Settings | SNMP

☒ Gather internet usage statistics

Statistics

☒ Gather user's activity records

Delete statistics older than: month(s)

Gather group statistics for these groups:

Accounting periods for statistics and quota

First day of week: ▾

First day of month:

Accounting exceptions

Account traffic only in the given time interval: ▾

Exclude website statistics for URLs which belong to: ▾

Exclude traffic to/from IP addresses which belong to: ▾

Exclude the following users from statistics:

Screenshot 74: 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 go to http://go.gfi.com/?pageid=control_help#cshid=1782

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.

NOTE

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**.

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.

NOTE

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.

Access Rights and 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

4.8.9 Configuring the SMTP server

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**.

4.8.10 DHCP server in Kerio Control

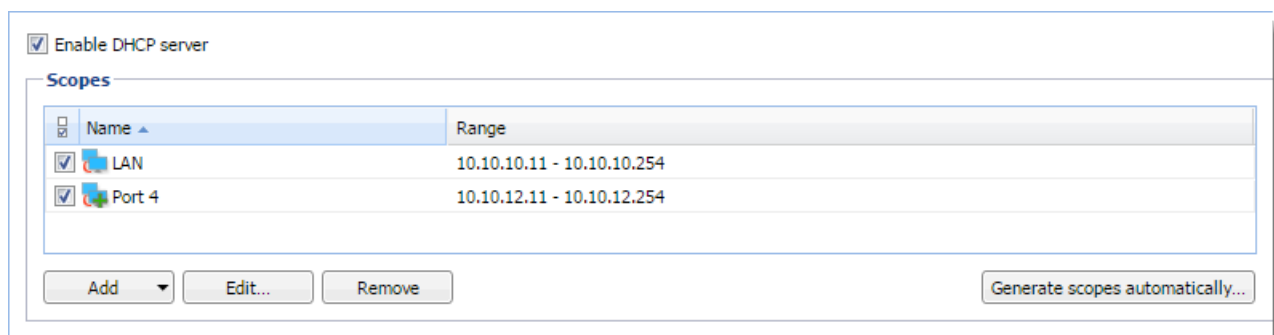
Kerio Control includes a DHCP server. The DHCP server assigns clients IP addresses within a predefined scope for a certain period (lease time). If an IP address is to be kept, the client must request an extension on the period of time before the lease expires. If the client has not required an extension 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.



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.

NOTE

Kerio Control does not ping an IP address before assigning it via DHCP. Ensure that there are no static addresses assigned to any network devices which are also configured in the DHCP range.

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.

NOTE

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**.

NOTE

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.

NOTE

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.

NOTE

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. For more information, refer to [Defining individual scopes](#) (page 321).
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.

NOTE

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.

Scope: LAN 1		Filter: <input type="text"/>			
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	

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.

IMPORTANT

If you use Kerio Control MAC Filter, check the **Also permit MAC addresses used in DHCP reservations or automatic user login** option. For more information, refer to [Filtering MAC addresses](#) (page 222).

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**.

4.8.11 DNS forwarding service in Kerio Control

Kerio Control includes a DNS server. We recommend to configure the DNS server with the DHCP server in Kerio Control together. For more information, refer to [DHCP server in Kerio Control](#) (page 319). Configuration and administration is simple and responses to repeated DNS queries are fast.

NOTE

In case of Active Directory environments, Kerio Control forwards DNS queries to the internal Domain Name Server if Kerio Control is joined to the domain. For more information, refer to [Connecting Kerio Control to directory service](#) (page 89).

IMPORTANT

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. Select **Enable the DNS forwarding service**. If the DNS forwarding service is disabled, the DNS module is used only as a Kerio Control's DNS resolver.
3. Select **Enable DNS cache for faster responses to repeat queries**. Responses to repeated queries are much faster with this option enabled (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 `j.smith-pc`). The DNS module can complete the query with the local domain. For more information, refer to [Hosts table](#) (page 323).
 - A host can send the DNS query in the `j.smith-pc.example.com` format. If the DNS module knows the local domain `example.com`, the name is divided into host: `j.smith-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:

A single record with separate individual names:

```
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.

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

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

NOTE

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.

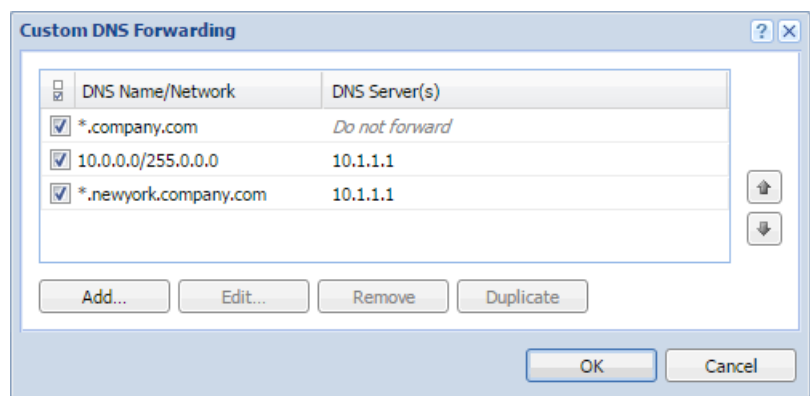
4. In the **Custom DNS Forwarding** dialog, you can create these types of rules:

- **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.



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.

4.8.12 Modifying parameters in Kerio Control configuration

In special situations, you may need to change the Kerio Control configuration directly. This is necessary, for example, when you need to adjust a setting that is not available in the web administration.

IMPORTANT

Do not make changes directly to the configuration unless a Kerio support representative provides you with specific instructions.

Accessing the operating system

To update the configuration directly, you must login to the operating system shell environment. You can access the shell either directly from the console, or remotely using a secure shell tunnel (SSH).

Accessing the shell via local console

1. In the Kerio Control console, press **Alt + F2**.
2. As the login name, type **root**.
3. Type a local administrator password.
4. To close the session, type **exit**. Press **Alt + F1** to return to the initial screen.

Accessing the shell via remote login (SSH)

To remotely access the secure shell, you need a client program, such as Putty. If you are using Linux or Mac, you can open a secure shell tunnel using the terminal.

NOTE

In the default traffic rules configuration, Kerio Control allows remote login only from the Trusted / Local network.

1. Enable remote login in the web administration. Hold the **Shift** key and go to **Status > System Health**.
2. Select the button **Enable SSH**.
3. In your secure shell program, open a new connection to the Kerio Control server address.
4. As the login name, type **root**.
5. Type a local administrator password.

Modifying the configuration

To update configuration, type:

```
/opt/kerio/winroute/tinydbclient "update table set variable=value"
```

To apply the new configuration, type:

```
/etc/boxinit.d/60winroute restart
```

Examples

Disabling the 3-way TCP handshake security feature:

```
~ # /opt/kerio/winroute/tinydbclient "update Firewall set  
Require3WayHandshake=0"  
~ # /etc/boxinit.d/60winroute restart
```

Requiring TLS version 1.1 and higher:

```
~ # /opt/kerio/winroute/tinydbclient "update ssl set forcetlsver_  
1=1"  
~ # /etc/boxinit.d/60winroute restart
```

4.8.13 Optimizing performance with large segment offload

NOTE

New in Kerio Control 9.2.1!

Kerio Control includes large segment offload (LSO), also referred to as generic segmentation offload. LSO allows the network interface controller to process the segmentation of data transfers and significantly improves performance. However, these improvements are noticeable only during large data transfers, such as file downloads, or video streams.

LSO is supported on all Kerio Control NG hardware devices. Kerio Control virtual and software appliances support LSO only if your hardware supports it as well.

Configuring large segment offload

Verifying LSO support on Internet network adapters

LSO works only if you use network adapters that support LSO.

To verify that your network adapters support LSO, connect to Kerio Control via SSH and use the command `ethtool`:

1. Connect to Kerio Control [via SSH](#).
2. Type `ethtool -k xxxx | grep generic-segmentation`, where `xxxx` represents your Internet interface, for example `eth0` (the default value in Kerio Control).

If your Internet network adapter supports LSO, the result is

```
generic segmentation-offload: on
```

Disabling LSO in Kerio Control

In Kerio Control LSO is enabled by default. To disable LSO, connect to Kerio Control via SSH and update the `tinydbclient` configuration file:

1. Connect to Kerio Control [via SSH](#).
2. Type `/opt/kerio/winroute/tinydbclient "update Misc set PktOffloading=0"`
3. To apply the new configuration, restart Kerio Control with

```
/etc/boxinit.d/60winroute restart
```

After the restart, Kerio Control disables LSO.

4.8.14 Using RADIUS server in Kerio Control

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.

IMPORTANT

There is a known issue with Windows 7 clients: Windows 7 does not accept untrustworthy certificates. If you Windows 7 clients cannot connect through RADIUS, read the [Configuring Windows 7 clients](#) section. For more information, refer to [Configuring Windows 7 clients](#) (page 328).

Configuring Kerio Control

1. In the administration interface, go to **Domains and User Login**.
2. Select the **Server Certificate**. If you have one, use the certificate signed by a certification authority, because devices connecting to Wi-Fi access point may have problems reading self-signed certificates.
3. In **Wi-Fi Authentication**, select **Enable external access point authentication**.
4. Type the RADIUS password - 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.

IMPORTANT

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)

Server certificate: Default ▾ Edit...

☒ Enable external access point authentication

RADIUS password:

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. For more information, refer to [Configuring Kerio Control](#) (page 327).

Configuring Windows 7 clients

Windows 7 does not provide an interface for accepting untrusted certificates.

The recommendation is that you use the certificate signed by a certification authority, because devices connecting to Wi-Fi access point may have problems reading self-signed certificates. If that is not possible follow this procedure in case that your users with Windows 7 cannot connect through RADIUS:

Windows 7 clients are connected to your network

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.

NOTE

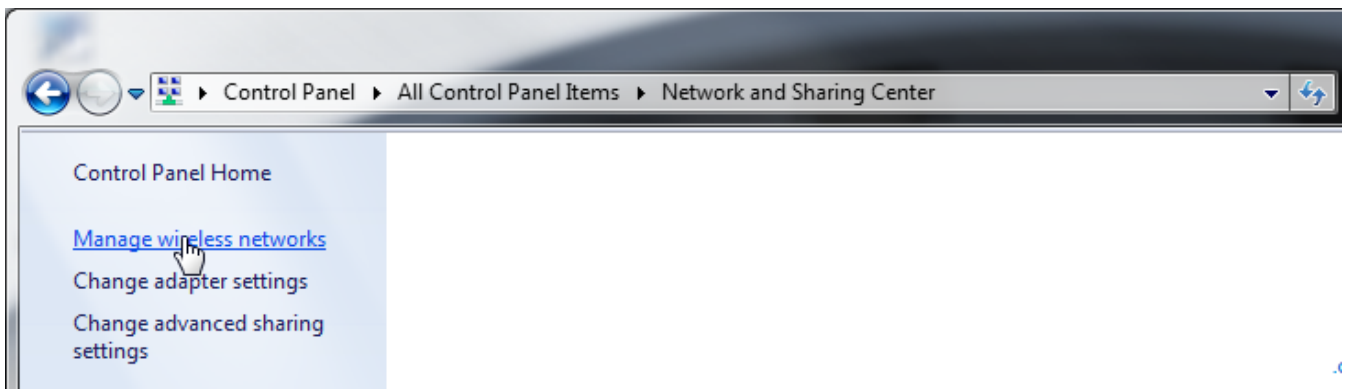
Although Windows 7 knows the SSL certificate, the warning **The connection attempt cannot be completed** appears to the users during the first connection attempt. Users must click **Connect** in this window.

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:

Step 1: Create a network profile

1. In **Windows 7**, click the **Start** menu.
2. Go to **Control Panel > Network and Internet > Network and Sharing Center > Manage wireless networks**.



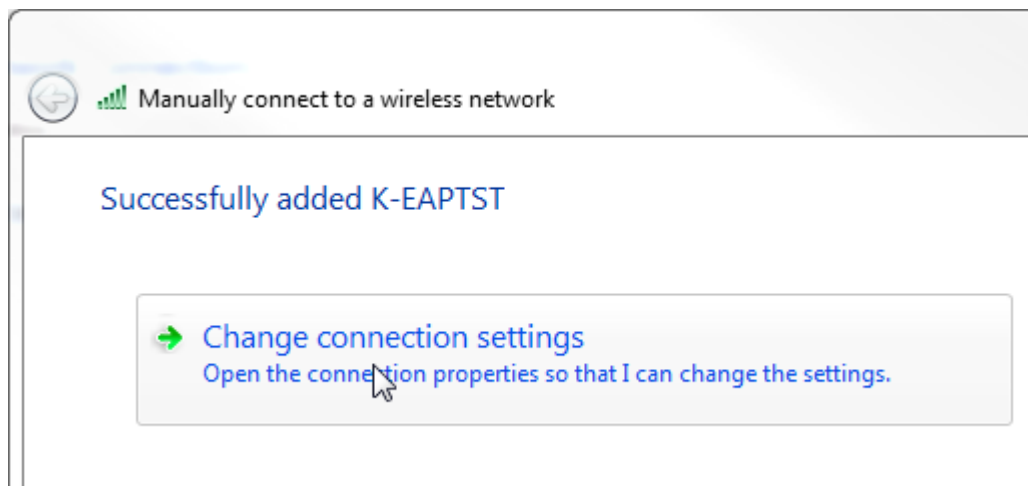
Screenshot 75: Managing wireless networks

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.

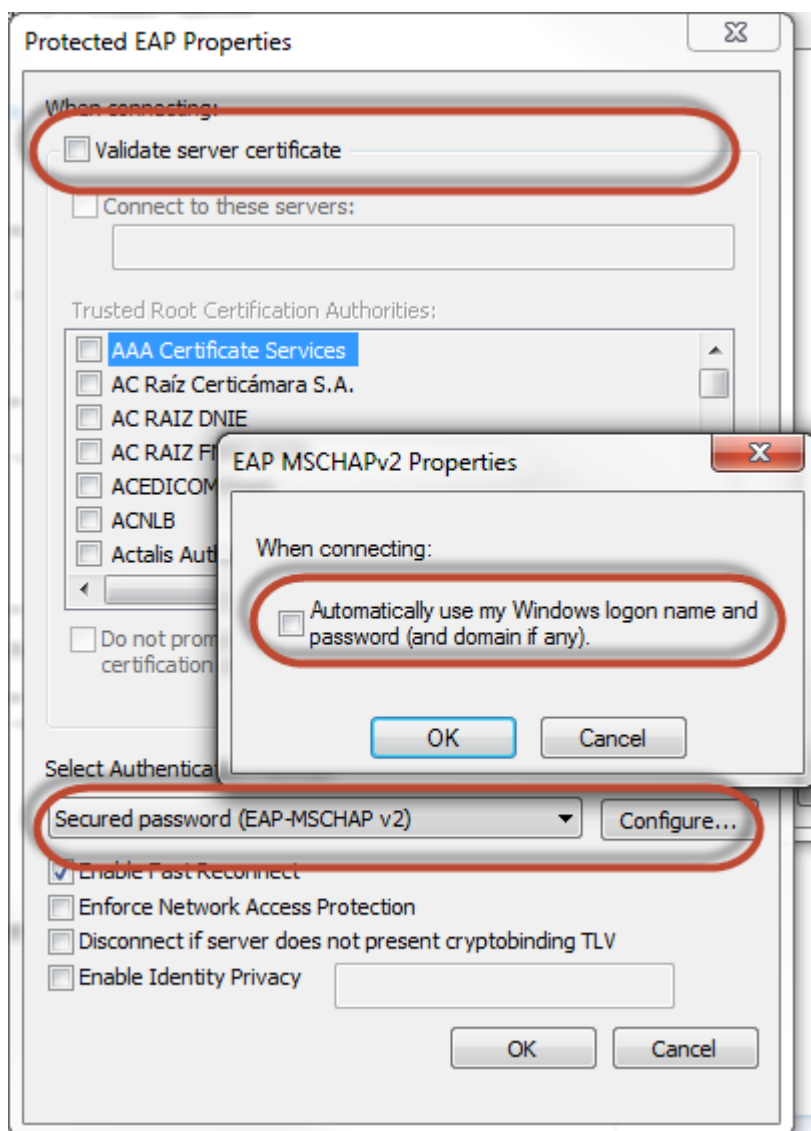
Step 2: Uncheck validation of a server certificate

1. Click **Change connection settings**.



Screenshot 76: Changing 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** and the **EAP-MSCHAP v2 Properties** opens.
6. Unselect **Automatically use my Windows logon name and password**.

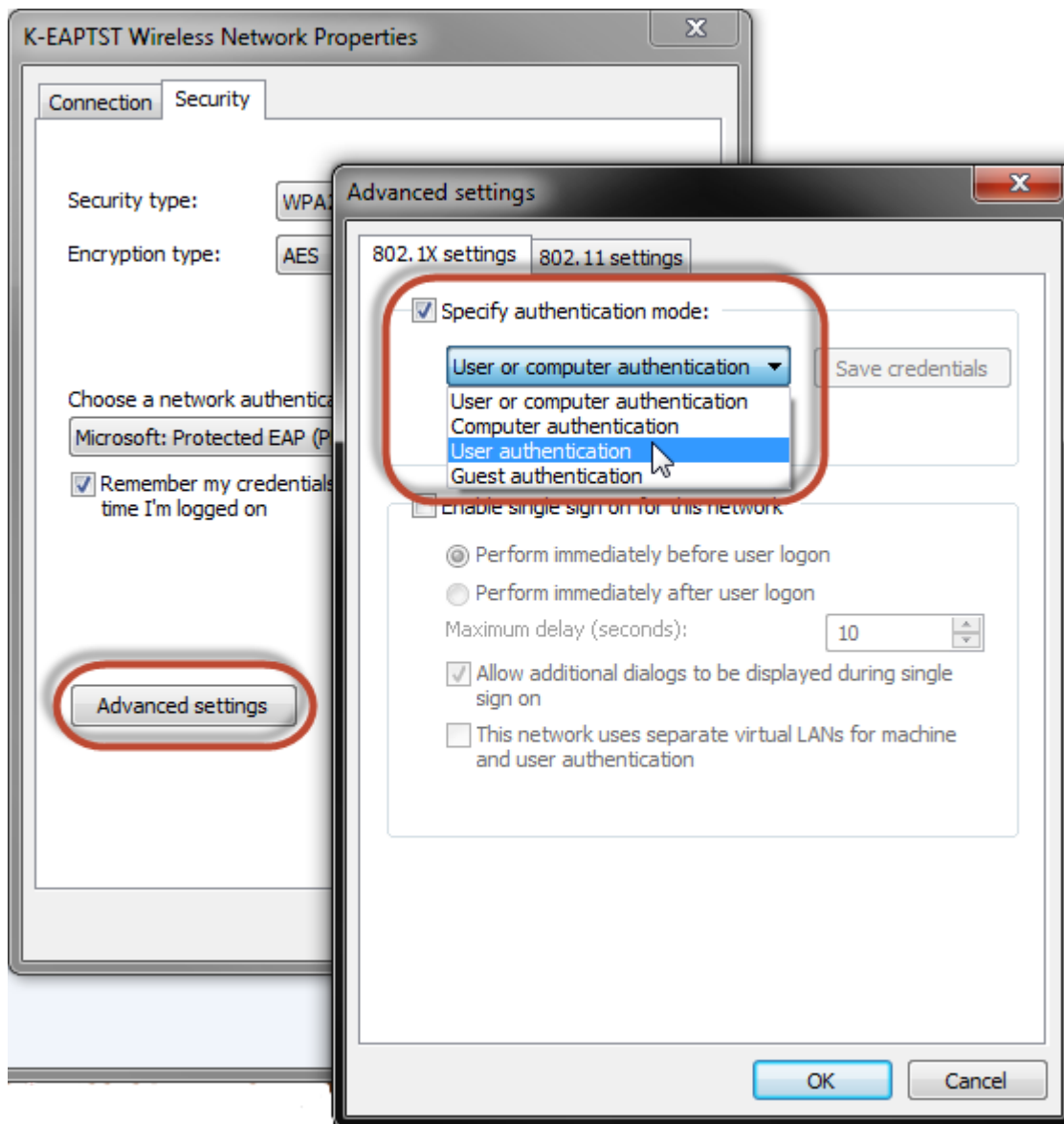


Screenshot 77: Changing authentication method for wireless connection

7. Click **OK**

Step 3: 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**.



Screenshot 78: Configuring advanced settings

5. Click **OK**

4.8.15 Configuring 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.

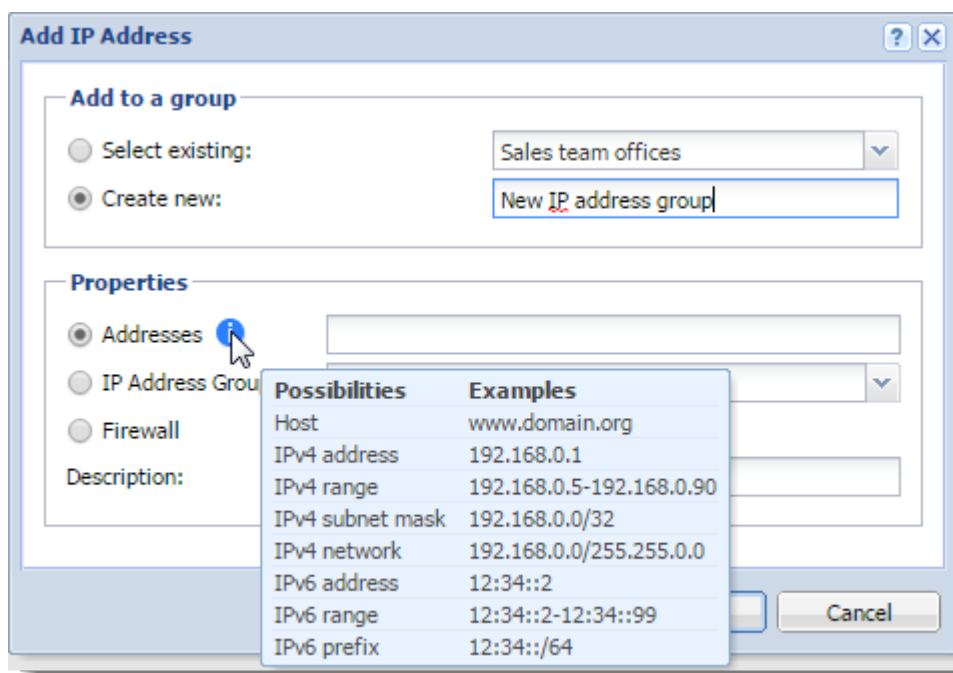
IP Address Groups			Admin ▾
Filter: <input type="text"/>			
Item ▴	Source	Description	
Admins			
<input checked="" type="checkbox"/> 192.168.48.48	MyKerio	Sydney	
<input checked="" type="checkbox"/> 192.168.48.49	MyKerio	Alex	
HTTPS exclusions			
<input checked="" type="checkbox"/> dropbox.com	Local	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	

NOTE

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**.
3. In the **Add IP Address** dialog box, select **Create new** and type a name of the IP address group.
4. Select:
 - **Addresses** is 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).



IMPORTANT

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** is a group of IP addresses. Groups can be cascaded.
- **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**.
3. In the **Add IP Address** dialog box, select **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.
5. Click **OK**

NOTE

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.
For more information, refer to [Moving items from one IP address group to another](#) (page 334).

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:

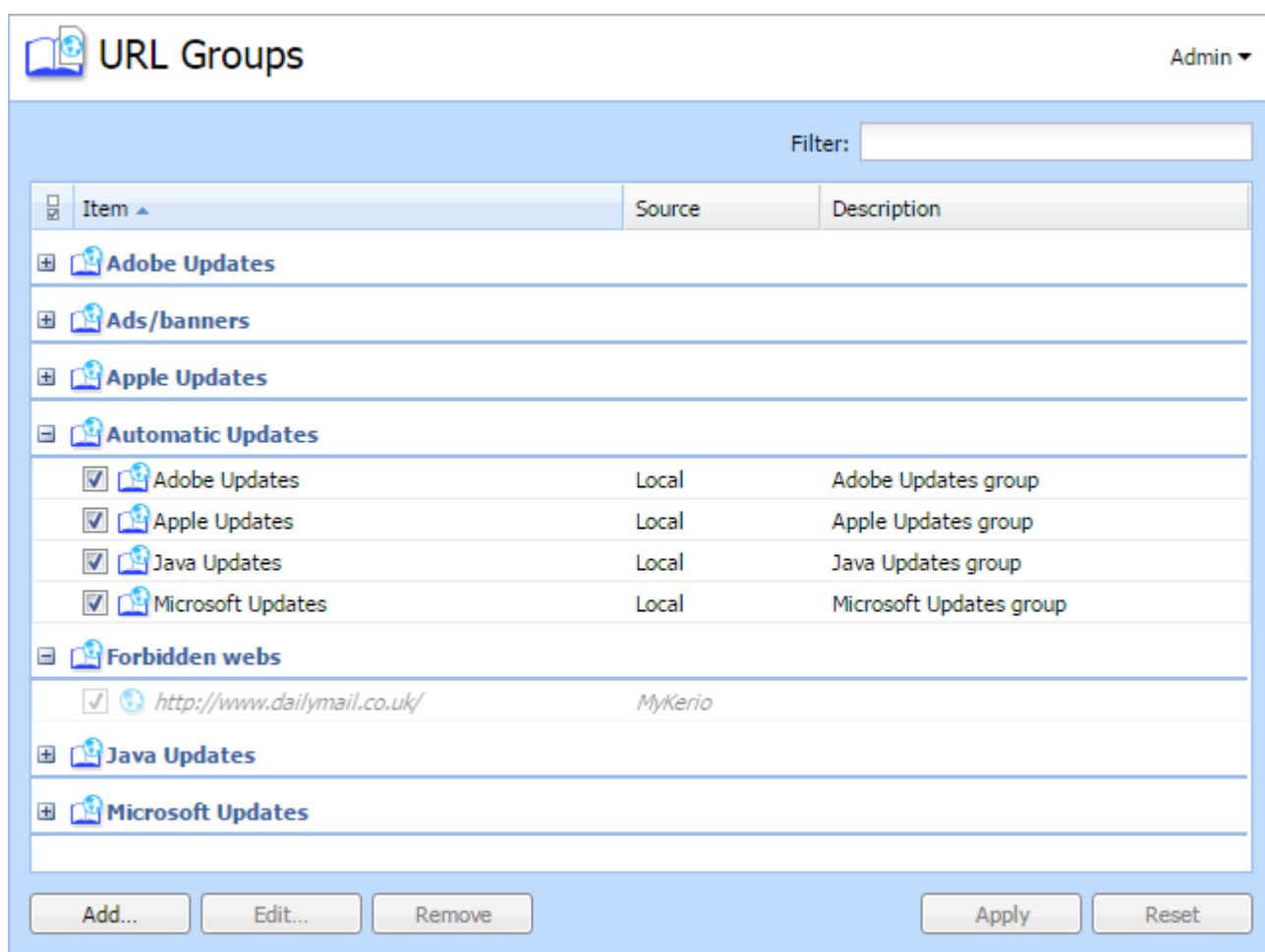
1. In the administration interface, go to **Definitions > IP Address Groups**.
2. Right-click the item.
3. In the context menu, click **Edit**.
4. In the **Edit IP Address** dialog box, select **Move to existing** and specify the desired IP address group from the selection menu.
5. Click OK.

4.8.16 Configuring 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.



NOTE

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 more information, refer to [Wildcards and regular expressions in URL](#) (page 342).
5. Save the settings.

4.8.17 Services in Kerio Control

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. For more information, refer to [Protocol inspection in Kerio Control](#) (page 224).

Using services

Example: You want to perform protocol inspector 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.

NOTE

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 – 65 535)
 - **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)

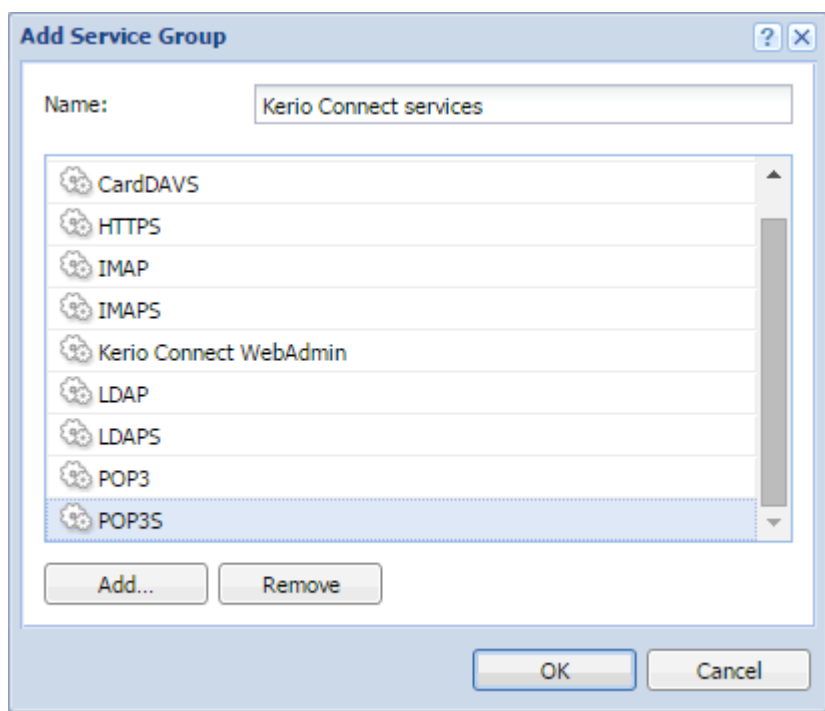
8. Save the settings.

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

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. For more information, refer to [Configuring traffic rules](#) (page 236).

A good example for creating group of services is Kerio Connect — mail server from Kerio Technologies.




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.

4.8.18 Creating time ranges in Kerio Control

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.



Time Ranges

Admin ▾

Filter:

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

NOTE

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

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.

4.8.19 Configuring Universal Plug-and-Play (UPnP)

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.

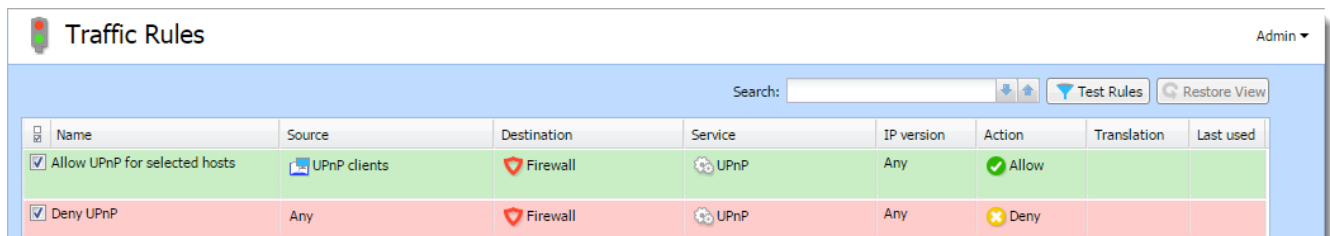
Configuring the UPnP support

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**.

Example

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.



Name	Source	Destination	Service	IP version	Action	Translation	Last used
Allow UPnP for selected hosts	UPnP clients	Firewall	UPnP	Any	Allow		
Deny UPnP	Any	Firewall	UPnP	Any	Deny		

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

4.8.20 Using Remote Desktop IP Virtualization

Windows 2008 R2 and newer

On Windows Server 2008 R2 and newer, Terminal Server is changed to the Remote Desktop Session server that supports Remote Desktop IP Virtualization and no longer needs the usage of proxy servers.

Remote Desktop IP Virtualization works in two modes:

- » **Per-Session mode** assigns an IP address per user session.
- » **Per-program mode** assigns an IP address for specified applications.

For more details and information about configuring Remote Desktop IP Virtualization, see [the official Microsoft blog](#).

Windows 2008 and older

On Windows Server 2008 and older, Terminal Server works only with a single IP address that is shared among all users of Terminal Server. This may cause problems, because Kerio Control cannot distinguish the users in the environment of Terminal Server.

Use a proxy server and force the authentication with each request, but this authentication is not compatible with the NTLM protocol, full HTTPS filtering and other protocols.

4.8.21 Wildcards and regular expressions in URL

Wildcards

Kerio Control allows using wildcards when you [create a content rule](#) based on a URL or a URL group:

1. Select the **HTTP URL** option.
2. In the **Site** field, write the URL. Use substrings with special characters — * and ?. An asterisk (*) stands for any number of characters, a question mark (?) represents one character.
3. Click **OK**

Examples:

- » `www.example.com/index.html` — a particular page
- » `www.*` — all URL addresses starting with `www.`
- » `*exploit*` — all URL addresses containing the `exploit` string
- » `*warez??.cz*` — all URL addresses containing such strings as `warezzz.cz`, `warez99.cz`, etc.

Do not select the **HTTP URL by regular expression** option, if you want to use only wildcards.

Regular expressions

Kerio Control allows you to use regular expressions when you create a content rule based on a URL or a URL group:

1. Select the **HTTP URL by regular expression** option.
2. In the **Site** field, write the regular expression. Kerio Control uses Perl Regular Expression Syntax. For complete specification, go to <http://www.boost.org>.
3. Click **OK**

Example:

Type `facebook\.com.*` in the **Site** field if you want to create a content rule for all URL addresses that contain `facebook.com`.

4.8.22 Dynamic DNS for public IP address of the firewall

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. For 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: [ChangelP](#), [DynDNS](#), or [No-IP](#).
2. In the administration interface, go to **Remote Services > Dynamic DNS**.
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. 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**.

4.9 SSL certificates

This section helps you to generate, maintain and use SSL certificates in Kerio Control.

4.9.1 Configuring SSL certificates in Kerio Control	343
4.9.2 Exporting and importing Kerio Control local authority as root certificate	346
4.9.3 Changing SSL certificates in Kerio Control	347
4.9.4 Deploying Kerio Control certificate via Microsoft Active Directory	347

4.9.1 Configuring SSL certificates in Kerio Control

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.
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**.

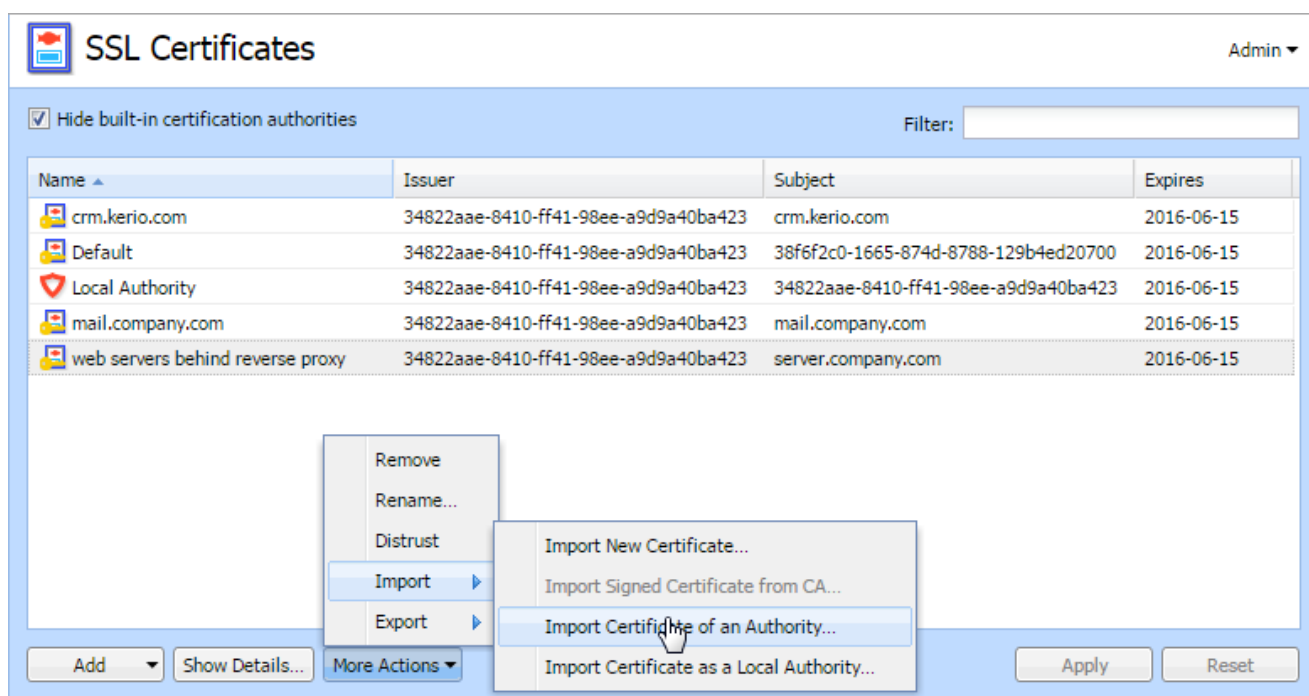
The certificate replaces the certificate request. You can use this certificate. Using the certificate means that you have to select it in the specific settings (for example SSL certificate for VPN server you have to select in **Interfaces > VPN Server**).

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.

NOTE

If you have multiple intermediate certificates, add them all in the same way.

Changing SSL certificates

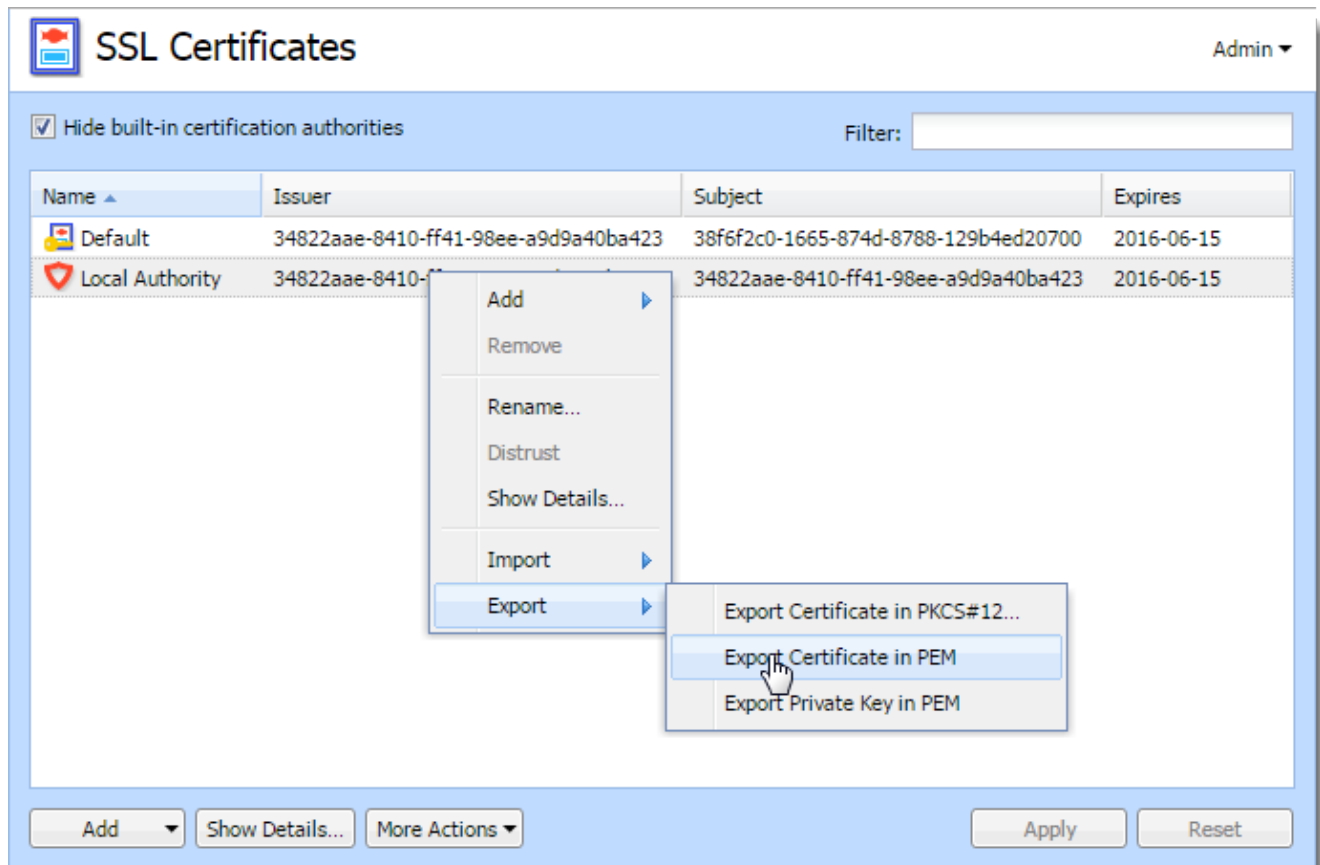
If your certificate is expiring and you need to import a new one, you must also select the certificate in all Kerio Control services where the expiring certificate is used. For more information, refer to [Changing SSL certificates in Kerio Control](#) (page 347).

4.9.2 Exporting and importing Kerio Control local authority as root certificate

Exporting a certificate from Kerio Control

You must export a certificate of the Kerio Control local authority in PEM format to install it to users' browsers.

1. In the administration interface, go to **Definitions > SSL Certificates**.
2. Right-click the **Local Authority** row.
3. Click **Export > Export Certificate in PEM**.
4. Save the certificate.



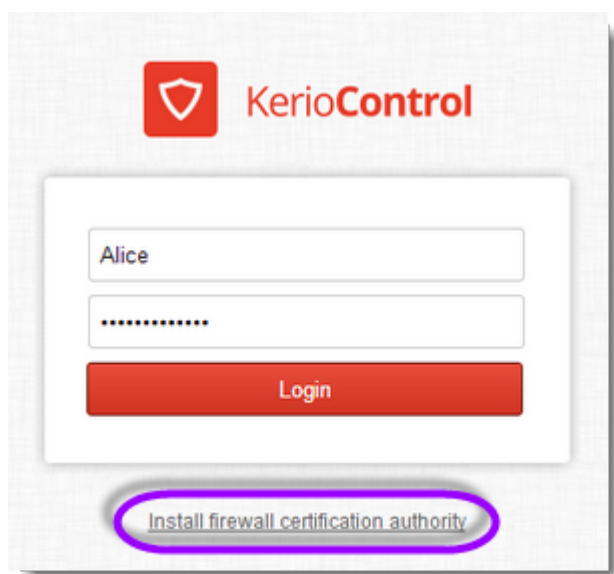
Screenshot 79: Exporting a certificate

Importing the Kerio Control certificate as a root certificate authority

You must import the Kerio Control certificate as a root certification authority into browsers on users' computers. Otherwise users have to confirm a security exception with each access to a HTTPS page which is annoying.

If you use Microsoft Active Directory, you can deploy the Kerio Control certificate into Microsoft Internet Explorer. For more information, refer to [Deploying Kerio Control certificate via Microsoft Active Directory](#) (page 347).

If you use a Kerio Control internal user database or Apple Open Directory, your users must install the Kerio Control certificate into their browsers themselves. In all the major browsers, a link to instructions for doing so appears on the Kerio Control client login screen, as shown below.



Screenshot 80: Exporting a certificate

4.9.3 Changing SSL certificates in Kerio Control

If your certificate is expiring and you need to import a new one, you must also select the certificate in all Kerio Control services where the expiring certificate is used.

Changing active certificates

1. In the administration interface, go to **Definitions > SSL Certificates**.
2. Create a new certificate. For more information, refer to [Configuring SSL certificates in Kerio Control](#) (page 343).
3. Verify, that the certificate is included in the **SSL Certificates** section.
4. Select the certificate in all places where the expiring certificate is used (see the table below).

Services which need a valid SSL certificate	Section in Kerio Control Administration
Kerio VPN Server	Interfaces
Kerio IPsec Server	Interfaces
Kerio VPN Tunnel	Interfaces
IPsec VPN Tunnel	Interfaces
Wi-Fi Authentication (RADIUS server)	Domains and User Login > Authentication Options
Reverse Proxy server	Proxy Server > Reverse Proxy
SSL certificate for a reverse proxy rule. The certificate hostname must be the full DNS server name.	Proxy Server > Reverse Proxy > Reverse Proxy Rule
Kerio Control Administration and Kerio Control Statistics	Advanced Options > Web Interface

4.9.4 Deploying Kerio Control certificate via Microsoft Active Directory

If you use HTTPS filtering in Kerio Control and administer your users through Microsoft Active Directory, you can deploy a Kerio Control certificate to users' computers via Active Directory. The whole process has two steps:

- » Exporting a certificate from Kerio Control. For more information, refer to [Exporting and importing Kerio Control local authority as root certificate](#) (page 346).
- » Deploying root certificate via Active Directory

Deploying root certificate via Active Directory

1. Log into your Active Directory server as administrator and open the **Group Policy Management Console**.
2. Find an existing **GPO** or create a new one. The GPO must be associated with the domain, or organizational unit of the computers you want to affect.
3. Right-click the GPO and select **Edit**. The **Group Policy Management Editor** opens, and displays the current contents of the policy object.
4. Go to **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
5. Right-click **Trusted Root Certification Authorities** and select the **Import** option.
6. Follow the **Certificate Import Wizard** to find and import the certificate.

To verify that the certificate is deployed to the workstations:

1. Choose a workstation joined to the domain and restart it, or execute the command `gpupdate /force`
2. Open **Internet Explorer > Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities**
3. Verify that your certificate is present.

For detailed information, see [Distribute Certificates to Client Computers Using Group Policy](#).

5 Troubleshooting

This topic helps you fix problems you might encounter when using Kerio Control.

5.1 How do I generate a network trace (packet dump) for Kerio technical support?	349
5.2 Common issues	350
5.3 Wifi issues	355
5.4 USB tools	356
5.5 Vulnerabilities	369

5.1 How do I generate a network trace (packet dump) for Kerio technical support?

5.1.1 Discussion

A network trace, also called a packet dump, sometimes must be generated to analyze packet traffic between systems to troubleshoot difficult application or networking problems. A network trace may be requested by Kerio Technical Support for analysis by upper level technicians and developers. This article describes the steps to be taken to generate a network trace on the major platforms. Select the platform below where the packet trace will be initiated.

5.1.2 Windows and MacOSX

Wireshark is the recommended application for generating network traces on Windows and Mac OSX platforms. From a machine involved in the transmission of data, download Wireshark from [here](#) and install it (including the WinPcap application, if applicable). Follow these steps to create the trace:

1. From within Wireshark, click **Capture Options**.
2. In the **Interface:** field, select the network card that connects to the remote system involved in the network transmission.
3. In the **Capture filter:** field, type "host" followed by the IP address of the remote system: `host xxx.xxx.xxx.xxx` where xxx.xxx.xxx.xxx is the IP address of the remote machine
4. Click on the Browse button next to the **File:** field and select Desktop in the "Save in folder" field.
5. Type a file name, such as problem.cap, in the **Name:** field and click **OK**
6. Click the **Start** button, or from the **Capture** menu, select **Start**.
7. Perform the network connection that displays the problem.
8. When the network operation is complete, click on the **Stop** button or, from the **Capture** menu, select **Stop**.
9. Reply to the ticket sent by Kerio technical support, attaching the generated `problem.cap` file.

5.1.3 Linux

tcpdump is the recommended application for generating network traces and is already installed on most Linux platforms. Here are the basic steps for creating a trace using the tcpdump command line application:

1. Open a Terminal session and log in as the "root" user and, to start the network trace, type:

```
tcpdump -s 0 -w /problem.cap -f host xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the IP address of the remote machine, such as 192.168.200.201

2. Perform the network connection that displays the problem.

3. When the network operation is complete, type ctrl-c on the Terminal to stop tcpdump.

4. Reply to the ticket sent by Kerio technical support, attaching the generated problem.cap file.

After you have sent the problem.cap file to Kerio technical support, the file will be analyzed and you will be contacted regarding the results of the analysis.

5.2 Common issues

This section helps you resolve possible known issues.

5.2.1 Authenticating iPhone 5 (iOS6) device to WiFi fails	350
5.2.2 Dshield Identified Top Attackers blocks access from LAN	351
5.2.3 I have a page that is miscategorized by Kerio Web Filter	351
5.2.4 Redirecting users to the authentication page does not work, the page cannot be displayed.	352
5.2.5 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded)	352
5.2.6 Browser extensions or add-ons may interfere with Kerio products	352
5.2.7 User is prompted for credentials	353
5.2.8 Troubleshooting SSL certificates	354

5.2.1 Authenticating iPhone 5 (iOS6) device to WiFi fails

When the iPhone 5 device tries to authenticate via WiFi, a blank screen appears and the WiFi authentication fails. Kerio Control is configured to require user authentication for internet access.

Details

While the device is connecting to WiFi, it checks internet connectivity by accessing an apple.com page. Because Kerio Control requires users to be authenticated, access to this page is forbidden and the iPhone fails to connect to the internet (a blank white screen is displayed during the internet connectivity test). After that, the WiFi connection is disconnected automatically.

To resolve the problem, add an HTTP exception rule in Kerio Control that allows traffic to **http://*apple.com*** without authentication.

- » Navigate to **Configuration > HTTP policy > URL rule**
- » Add a new rule
- » Set Action to Allow, URL to **http://*apple.com***, User to Any, Do not require authentication

<input checked="" type="checkbox"/> iOS6 devices	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> *apple.com*	<input type="checkbox"/> Don't authenticate
--	---	--------------------------------------	---

- » Be sure you do not have any other restricting rule(s) for the same URL above. If so, move this rule to the top of the list.
- » You are able to authenticate to wifi with your iOS6 device.

NOTE

This behavior is a current feature of iPhone 5 (iOS 6) based devices and it may be changed by Apple in the future.

5.2.2 Dshield Identified Top Attackers blocks access from LAN

The IDS/IPS security update (version 2.413) released on the 1st of October 2013 can cause the 'Dshield Identified Top Attackers' to block LAN traffic from 192.168.0.0 / 24. As we have identified the problem, we have now released an update of the IDS/IPS rules immediately (version 2.414). The IDS/IPS rules will then be updated automatically within the default update interval. You may need to reboot your Kerio control system to solve this problem.

Details - for all Kerio Control versions

- » If it is possible to access the administration interface from a different source IP address (eg. via VPN client, remotely from the internet, from a another network IP address range) - click the **Update Now** button to update rules manually.
- » If it is not possible to access the Kerio Control Administration - restart the server and the Kerio Control should invoke the update automatically within 10 minutes after the restart.

5.2.3 I have a page that is miscategorized by Kerio Web Filter

What do I do?

- » Because each web page is individually filtered in the new Kerio Web Filter, the first step must be to check and where necessary change the category. Use the following URL to do so: test a site
- » When prompted, please enter the FULL Page URL, and also the CAPTCHA text below the URL edit box.
- » A list of the currently assigned categories is displayed for review.
- » If the list of currently assigned categories does not match what you think should be selected, use the link "Incorrect or missing categories? Suggest new ones." to suggest a new list.
- » Any suggestions you make will be a completely new list of categories. If you only want to add a category, you must also include the category in addition to suggested categories.
- » If you want to remove a category from the list, simply suggest a list without the category you want to remove.

What happens after I have submitted my response

- » As soon as your suggestions are submitted, it goes to the very top of the priority list of URLs and generally a trained web analyst will review the URL and the suggestions within a few minutes of submission. If the web analyst agrees with your suggestion, the changes will be made available immediately. However, the Kerio Web Filter uses DNS queries as a transport protocol, so the overall process may take up to a day to update all DNS cache records across the Internet. Please be patient if the category is not updated immediately.
- » Within 24 hours, a web analyst supervisor will double check the judgment of the web analyst to be sure the submitted URL is correctly categorized.
- » If the category is not updated within a day, it may mean that our web analysts believe the URL is properly categorized. Please see the category listings for a high level overview of how the categories are defined. Alternately, it

could indicate a temporary communications problem. Resubmitting once after 24 hours without a change is encouraged if you suspect the report wasn't received.

What should I do if there is still a problem?

» If the problem persists or you find any other issues related to categorization process or to Kerio Web Filter, contact our technical support department for further assistance.

5.2.4 Redirecting users to the authentication page does not work, the page cannot be displayed.

Redirecting users to the authentication page does not work, the page cannot be displayed.

Details

If Kerio Control is configured to **Always require users to be authenticated when accessing web pages**, then it is possible for Kerio Control to redirect users to a name (for example, `https://fw.control.local:4081`), rather than an IP address (for example, `https://10.0.0.1:4081`).

This setting is specified in **Configuration > Advanced options > Web Interface > Use specified hostname**. Type in a name that resolves to the IP address of the Kerio Control machine.

If the client machines in the local network use the IP address of the Kerio Control machine as their DNS server, you will need to have DNS Forwarding properly configured. The DNS servers used must be able to resolve the Kerio Control DNS name into a proper IP address.

One quick method of doing this is Simple DNS Resolution. In the DNS Forwarder section, enable the "'hosts' file" option. Press the "Edit File" button. Add an entry for the server at the very bottom of the file. The format is "IP address", a single space, and then "hostname". Do not include quotes.

For more details on setting up DNS Forwarding and Simple DNS Resolution, see [DNS forwarding service in Kerio Control](#)

5.2.5 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded)

When importing users from Active Directory, the import fails and returns the following error:

```
(8503:4) Active Directory/LDAP error: Unable to search in  
dc=example,dc=domain,dc=com (Size limit exceeded)
```

By default, Active Directory does not respond to LDAP based queries which return more than 1000 results. If you have more than 1000 users configured in Active Directory, it is necessary to increase the maximum page size (MaxPageSize) using the Ntdsutil.exe tool.

5.2.6 Browser extensions or add-ons may interfere with Kerio products

When you have trouble working with an administration or client interface of Kerio products, you can try to disable or uninstall all your browser's extensions/add-ons.

Here are some tips on how to do it in the most common browsers:

- » **Google Chrome** — [Disable your extensions](#) or run the browser in the [incognito mode](#).
- » **Mozilla Firefox** — [Disable your add-ons](#) or run the browser in [Save Mode](#).
- » **Safari** — [Turn all extension off](#).
- » **Internet Explorer** — [Disable your add-ons](#) or run the browser in **No Add-ons** mode.

5.2.7 User is prompted for credentials

Issue encountered

User is prompted for credentials. Client enters the details, but after a few seconds, a new pop-up appears. Authentication is set to use NTLM.

Causes

There could be different causes for this issue:

- » Time settings are out of sync.
- » Kerio Control server name does not have a valid DNS name.
- » Old credentials are stored in Windows Password Manager.

Possible Solutions

You can try one or more of the solutions below. The order is not important.

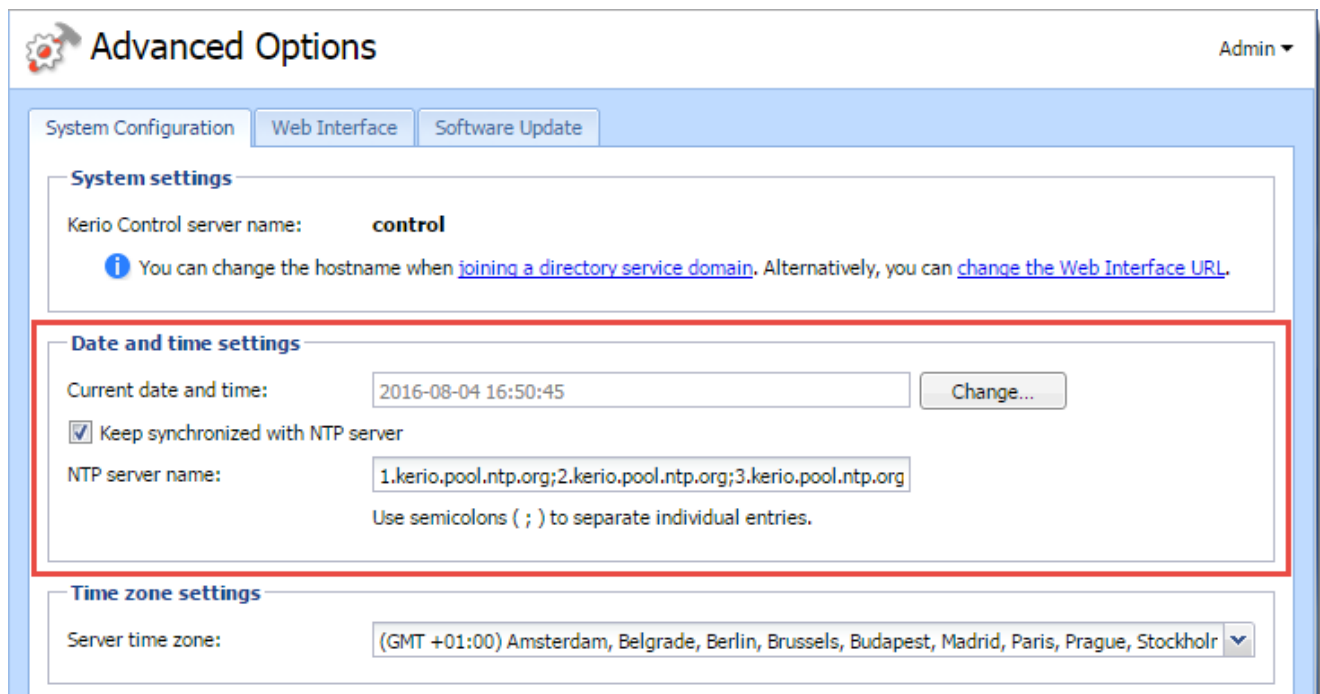
Synchronize time settings

Verify that the time on Domain Controller, Kerio Control, and client hosts are the same.

To have the same time on all computers in your network, use an NTP server.

To configure date and time settings in Kerio Control:

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



The screenshot shows the 'Advanced Options' window in Kerio Control. The 'System Configuration' tab is selected. The 'Date and time settings' section is highlighted with a red border. It contains the following fields and options:

- System settings:** Kerio Control server name: **control**. A note states: "You can change the hostname when [joining a directory service domain](#). Alternatively, you can [change the Web Interface URL](#)."
- Date and time settings:**
 - Current date and time:
 - ☒ Keep synchronized with NTP server
 - NTP server name:
Use semicolons (;) to separate individual entries.
- Time zone settings:** Server time zone:

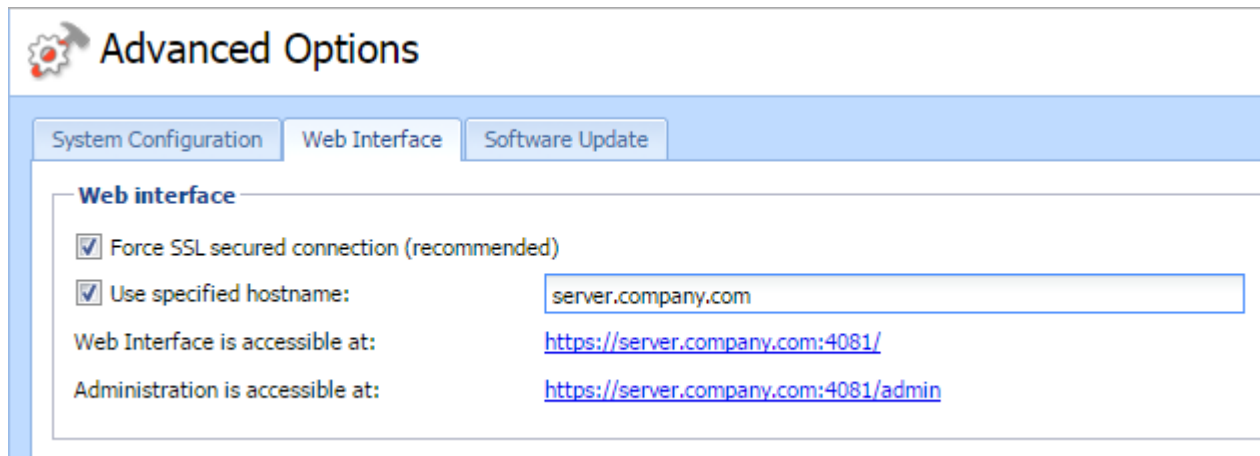
Screenshot 81: Kerio Control date and time settings

2. Under the **System Configuration**, find Current date and time and click **Change...** do adjust settings.
3. If using an NTP Server check **Keep synchronized with NTP Server** and enter the hostname of the servers under **NTP server name**:

Validate DNS name

Verify that the Kerio Control server name is correct:

1. Go to **Advanced Options > Web Interface**.



Screenshot 82: Web interface configuration

2. Select **Use specified hostname**.
3. Type a valid DNS name of the Kerio Control server.

Remove locally stored password in Windows Password Manager

The Kerio Control log-in dialog box is displayed only if NTLM authentication fails.

NTLM authentication may fail if invalid credentials are saved in Windows Password Manager.

To remove all Kerio Control usernames and passwords from Windows Password Manager:

1. Click **Start > Control Panel > User Accounts > Credential Manager**.
2. Select the **Windows Credentials**.
3. Locate the set of credentials that have *Kerio* in the name.
4. Click **Remove from Vault**.

Further troubleshooting steps

Kerio Control records information about failed authentication in the **Error** log. For more information, refer to [Using the Error log](#) (page 133).

5.2.8 Troubleshooting SSL certificates

Issue Encountered

Kerio Control displays a warning when it detects any certificate-related problems with VPN Clients.

Possible causes

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.
- » The name referred to the certificate does not match the server name. It means that 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 at an intrusion attempt (a false DNS record with an invalid IP address has been used).

NOTE

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

Possible Solutions

If you consider the Kerio Control server trustworthy, confirm the warning. Kerio Control VPN Client saves the certificate.

Generate a new certificate using Kerio Control. For more information, refer to [Configuring SSL certificates in Kerio Control](#) (page 343).

Export a certificate of the Kerio Control local authority in PEM format to install it to users' browsers. For more information, refer to [Exporting and importing Kerio Control local authority as root certificate](#) (page 346).

5.3 Wifi issues

This section helps you resolve possible known issues related to Wifi connections.

5.3.1 WiFi connection is slow	355
5.3.2 Wireless devices cannot connect to WiFi	356

5.3.1 WiFi connection is slow

Issue encountered

WiFi connection is slow.

Cause

Another WiFi access point interferes with your device.

Solutions

Change the band and channel used by Kerio Control device.

1. In the administration interface, go to **Interfaces and WiFi**.
2. Click the **WiFi** button.

- 3. In the **Band** drop down list switch to another band (a, b, g, or n).
- 4. In the **Channel** drop-down list, select a different channel.

Change the location of the device.

Keep your Kerio hardware device away from devices that can interfere with the Kerio Control WiFi module, such as microwave ovens, baby monitors, wireless phones, and wireless peripheral devices.

NOTE

Users from Germany, Netherlands, and Bulgaria should use channels less than 140 for optimal power performance. For further information refer to <https://www.gfi.com/support/products/Using-Wifi-channels-above-140-in-Kerio-Control-NG100W-and-NG300W>.

5.3.2 Wireless devices cannot connect to WiFi

Issue encountered

Wireless devices cannot connect to WiFi.

Causes

- » Devices do not support 5 GHz.
- » Devices do not support the WPA2 authentication.

Solutions

Change the WiFi band

- 1. In the administration interface, go to **Interfaces and WiFi**.
- 2. Click the **WiFi** button.
- 3. In the **Band** drop-down list switch to another band (802.11b, g, or n 2.4 GHz).

Change the authentication to WPA

- 1. In the administration interface, go to **Interfaces and WiFi**.
- 2. Click the **WiFi** button.
- 3. Open **WiFi Settings**.
- 4. In the **Security** drop-down menu, select **WPA Enterprise**.

5.4 USB tools

This topic provides information about password recovery, factory reset, and diagnosing Kerio Control hardware appliances via an USB flash drive.

5.4.1 Recovering your Kerio Control Box NG series password using a USB flash drive	357
5.4.2 Recovering your Kerio Control password using a USB flash drive	357

5.4.3 Restoring the Kerio Control Box NG series default configuration using a USB flash drive	358
5.4.4 Restoring the Kerio Control default configuration using a USB flash drive	362
5.4.5 Updating Kerio Control Box NG series using a USB flash drive	365
5.4.6 Updating Kerio Control using a USB flash drive	365
5.4.7 Diagnostic tool for Kerio Control Box	367
5.4.8 Diagnostic tool for Kerio Control Box NG series	368

5.4.1 Recovering your Kerio Control Box NG series password using a USB flash drive

You can recover your password for the administration interface with a USB flash drive.

The password recovery tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

IMPORTANT

There are two types of USB flash drives on the market. Kerio Control NG 500 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control NG 500, but can be reconfigured to work. For more information, refer to [Restoring the Kerio Control Box NG series default configuration using a USB flash drive](#) (page 358).

Creating and using a password recovery tool

To recover a lost administration password:

1. Insert the flash drive into a USB port on your computer.
2. Make sure that only one partition with the **FAT16** or **FAT32 (VFAT)** file system is created on the flash drive. The USB disk must **not** be formatted by the NTFS, ext2, ext3, or ext4 file systems.
3. Download and save the file [kerio-control-password-reset](#) to the flash drive.
4. Switch off Kerio Control.
5. Plug the USB flash drive into a USB port of your Kerio Control box.
6. Switch on Kerio Control.
7. When the Kerio Control Engine starts up, open the Kerio Control administration interface in a browser. Then the activation wizard opens.
8. In the activation wizard, create a new password for the admin account.

5.4.2 Recovering your Kerio Control password using a USB flash drive

Kerio Technologies provide a tool for password recovery. The tool is designed to run from a USB flash drive.

IMPORTANT

We recommend to use this method to update Kerio Control Box and Kerio Control Software Appliance. In this article, Kerio Control refers to both Kerio Control Box or Kerio Control Software Appliance.

NOTE

This article describes Kerio Control Box 1000/3000 series. For Kerio Control NG series, read [Recovering your Kerio Control Box NG series password using a USB flash drive](#). The password recovery tool is designed for a single use. Once you perform the operation, the content cannot be reused even if you restart with the flash drive still in the USB port.

Creating and using a password recovery tool

To recover a lost administration password:

1. Insert a USB flash drive into a USB port on your computer.
2. Make sure that only one partition with file system FAT16 or FAT32 (VFAT) is created on the flash drive. The USB drive must not be formatted by file system NTFS or ext2, ext3, or ext4.
3. Save the file [kerio-control-password-reset](#) to the flash drive.
4. Switch off Kerio Control.
5. Plug the USB flash drive into the USB port of your Kerio Control Box or the computer where Kerio Control Software Appliance is installed.
6. Switch on Kerio Control. When the password is reset, the box beeps once.
7. Wait for the Kerio Control Engine to start up (three beeps).
8. In your web browser, open the Kerio Control administration interface. Then the activation wizard opens.
9. The wizard asks for a new administration password.
10. Create a new password for the admin account.

If the steps above do not work, try another flash drive. Different Kerio Control Box models require different USB drive formats:

- » Kerio Control Box 1110, 3110, 3120, and 3130 require a USB flash drive formatted like a floppy disk (not partitioned).
- » Kerio Control Box 1120 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control Box, but can be reconfigured to work. See [Formatting a USB flash drive with MBR](#).

Related articles

[Diagnostic tools for Kerio Control Box](#)

[Restoring Kerio Control default configuration using a USB flash drive](#)

[Updating Kerio Control using a USB flash drive](#)

5.4.3 Restoring the Kerio Control Box NG series default configuration using a USB flash drive

Kerio Technologies provides a set of tools for solutions for situations in which it is not possible to connect to Kerio Control on a network and administer it through the Kerio Control Administration web interface.

These tools are designed to run from a USB flash drive.

You need a flash drive with the capacity of at least 1 GB to run the tools. For restoring the default configuration, 256 MB suffice.

We recommend to use this method to update Kerio Control Box and Kerio Control Software Appliance. In this article, Kerio Control refers to Kerio Control Box or Kerio Control Software Appliance.

If you have any issues after using the tools, for example, if Kerio Control fails to work even after you perform a complete system recovery, please contact [our technical support](#).

Restoring the default configuration

Recovering to factory settings includes removal of all configuration data including activation and the statistics database.

This USB tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

WARNING

There are two types of USB flash drives on the market. Kerio Control NG 500 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control NG 500, but can be reconfigured to work. See [Formatting a USB flash drive with MBR](#).

1. Insert the flash drive into a USB port on your computer (256 MB and more).
2. Make sure that only one partition with the **FAT16** or **FAT32 (VFAT)** file system is created on the flash drive. The USB disk must **not** be formatted by the NTFS, ext2, ext3, or ext4 file systems.
3. Download and save the [kerio-control-factory-reset](#) file to the flash drive.
4. Switch off Kerio Control.
5. Plug the USB flash drive into a USB port of your Kerio Control box.
6. Switch on the Kerio Control box for resetting the configuration.
7. Kerio Control restarts automatically.
8. For additional instructions, continue with the [Installing Kerio Control](#) article.

Running a complete system recovery

During the complete system recovery, all configuration data, including activation and the statistics database, is completely rewritten. This means that you must reactivate and reconfigure the device afterwards.

WARNING

Before doing a complete system recovery, [restore the default configuration](#) and then retest the connection to Kerio Control.

Preparing a flash drive for a complete system recovery

For a complete system recovery, you must save the installation disk image directly to the physical device.

Microsoft Windows

1. Insert the flash drive into a USB port on your computer (1 GB and more).

NOTE

All data on the flash drive is completely overwritten.

2. Download and unpack [Image Writer](#) (it does not require installation).
3. Download the [kerio-control-rescue](#) file.
4. In Image Writer, find the file, select your flash drive and click **Write**.
5. Eject the flash drive securely and remove it from your computer.

Linux

1. Insert the flash drive into a USB port on your computer (1 GB and more).

NOTE

All data on the flash drive will be completely overwritten.

2. Download the [kerio-control-rescue](#) file.
3. Run the terminal (console) in the super-user mode (for example, using the `su` or `sudo -s` command depending on your Linux distribution).
4. Use the command `fdisk -l` to detect the USB flash drive name (for example, `/dev/sdx`).
5. Save the [kerio-control-rescue](#) file to the flash drive using the following command: `dd if=rescue.img of=/dev/sdx bs=1M` and replace `rescue.img` with the real file name and `/dev/sdx` with the actual device name. You must type the physical device (for example, `/dev/sdx`), not a partition (for example, `/dev/sdx1`).
6. Use the `sync` command to ensure all disk operations finish.
7. Eject the USB drive safely and remove it from the USB port.

Mac OS X

1. Insert the flash drive into a USB port on your computer (1 GB and more).

NOTE

All data on the flash drive will be completely overwritten.

2. Download the [kerio-control-rescue](#) file.
3. Run the terminal: **Applications > Utilities > Terminal**.
4. Use the `sudo diskutil list` command to detect the USB flash drive name (for example, `/dev/diskX`).

NOTE

The drive name is case sensitive.

5. Use the `sudo diskutil unmountDisk /dev/diskX` command to unmount the flash drive.
6. Save the [kerio-control-rescue](#) file to the USB flash drive using the following command: `sudo dd if=rescue.img of=/dev/disk1 bs=1m` and replace `rescue.img` with the real file name and `/dev/diskX` with the actual device name.
7. Eject the flash drive securely and remove it from your computer.

Kerio Control Box system recovery

1. Switch off Kerio Control.
2. Plug the USB flash drive into a USB port of your Kerio Control Box.
3. Switch on Kerio Control. Wait for applying the [kerio-control-rescue](#) script.
4. Kerio Control turns off after the recovery finishes.
5. Switch on Kerio Control.
6. For additional instructions, continue with the [Installing Kerio Control](#) article.

Recovering the USB flash drive for further use

The recovery file creates partitions on the USB flash drive. To reuse the USB drive for other purposes, you need to remove all disk partitions, create new partitions, and reformat the disk for your file system.

Microsoft Window

1. Click **Start** and in the **Search** field type `cmd.exe` to open the **Command Prompt** window.
2. In the command line, type `diskpart`. You may need to confirm that you have administration rights.
3. Type `list disk` to display the list of drives and look up the number of the physical USB drive.
4. Type `select disk X` (replace X with the number of the corresponding disk).
5. Type `clean` to remove all partitions.
6. Create a new disk partition by typing the following commands in the order listed:

```
create partition primary
select partition 1
format fs=fat32 label="USB Flash" quick
exit
```

Linux

Use the graphical tool GParted or the command `fdisk`.

Mac OS X

Use the system tool Disk Utility: **Application > Utilities > Disk Utility**.

Formatting a USB flash drive with MBR

1. Click **Start** and in the **Search** field type `cmd.exe` to open the **Command Prompt** window.
2. In the command line, type `diskpart`. You may need to confirm that you have administration rights.
3. Type `list disk` to display the list of drives and look up the number of the physical USB drive.
4. Type `select disk X` (replace X with the number of the corresponding disk).
5. Type `clean` to remove all partitions.
6. Create a new disk partition by typing the following commands in the order listed:

```
create partition primary
select partition 1
```

```
format fs=fat32 label="USB Flash" quick  
exit
```

Related articles

[Recovering your Kerio Control Box NG series password using a USB flash drive](#)

[Updating Kerio Control Box NG series using a USB flash drive](#)

5.4.4 Restoring the Kerio Control default configuration using a USB flash drive

Kerio Technologies provides a set of tools for solutions for situations in which it is not possible to connect to Kerio Control on a network and administer it through the Kerio Control Administration web interface.

These tools are designed to run from a USB flash drive.

You need a flash drive with the capacity of at least 1 GB to run the tools. For restoring the default configuration, 256 MB suffice.

We recommend using these tools for Kerio Control Box and Kerio Control Software Appliance. In this article, Kerio Control refers to Kerio Control Box or Kerio Control Software Appliance.

NOTE

This article describes Kerio Control Box 1000/3000 series. For more information, refer to [Restoring the Kerio Control Box NG series default configuration using a USB flash drive](#) (page 358).

Should any issues arise (for example, if Kerio Control fails to work even after you perform a complete system recovery) contact [our technical support](#).

Restoring the default configuration

The factory settings of Kerio Control can be recovered with the file [kerio-control-factory-reset](#).

Factory settings recovery includes removal of all configuration data including activation and the statistics database.

This USB tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

1. Insert a USB flash drive to your computer (256 MB or larger) into a USB port on your computer.
2. Make sure that only one partition with file system FAT16 or FAT32 (VFAT) is created on the flash drive. The USB drive must not be formatted by file system NTFS or ext2, ext3, or ext4.
3. Save the [kerio-control-factory-reset](#) file to the flash drive.
4. Switch off Kerio Control.
5. Plug the USB flash drive into one of the USB ports of your Kerio Control.
6. Switch on Kerio Control. Once Kerio Control boots, the box beeps once. Once the configuration is reset, the box beeps once.
7. Kerio Control re-boots automatically and beeps once. Once Kerio Control is up, the box beeps three times.
8. Install Kerio Control. For more information, refer to [Installing Kerio Control](#) (page 22).

If the steps above do not work, try another flash drive. Different Kerio Control Box models require different USB drive formats:

- » Kerio Control Box 1110, 3110, 3120, and 3130 require a USB flash drive formatted like a floppy disk (not partitioned).
- » Kerio Control Box 1120 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control Box, but can be reconfigured to work. For more information, refer to [Formatting a USB flash drive with MBR](#) (page 364).

Running a complete system recovery

Kerio Control can be completely recovered with the [kerio-control-rescue](#) file. In the system recovery, all configuration data, including activation and the statistics database, is completely rewritten. This means the device have to be reactivated and reconfigured for further use.

IMPORTANT

Before doing a complete system recovery, we recommend that you should first [restore the factory settings](#) and then retest the connection to Kerio Control.

Preparing a flash drive for system recovery

For complete system recovery, Kerio Control first needs to introduce the operating system from a USB drive. The [kerio-control-rescue](#) file is an image of an installation disk and must be saved directly on the physical device. Follow the instructions for your client system below.

NOTE

During the installation of the rescue tool, the box beeps several times:

When Kerio Control boots, the box beeps twice.

When Kerio Control Engine starts up, the box beeps three times.

Operating System	Description
Microsoft Windows	<ol style="list-style-type: none"> 1. Insert the USB flash drive (at least 1 GB capacity) into a USB port on your computer. <div> IMPORTANT All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere. </div> <ol style="list-style-type: none"> 2. Download and unpack Image Writer (it does not require installation). 3. Download the kerio-control-rescue file. 4. In Image Writer, find the file, select your flash drive and click Write. 5. Eject the flash drive securely and remove it from your computer.
Linux	<ol style="list-style-type: none"> 1. Insert the flash drive into a USB port on your computer. <div> IMPORTANT All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere. </div> <ol style="list-style-type: none"> 2. Download the kerio-control-rescue file. 3. Run the terminal (console) in the super-user mode (e.g., using the <code>su</code> or <code>sudo -s</code> command — depending on your Linux distribution). 4. Use the command <code>fdisk -l</code> to detect the USB flash drive name (e.g., <code>/dev/sdx</code>). 5. Save the kerio-control-rescue file to the flash drive using this command: <code>dd if=rescue.img of=/dev/sdx bs=1M</code>. Replace <code>rescue.img</code> with the real file name and <code>/dev/sdx</code> with the actual device name. You must enter the physical device (e.g. <code>/dev/sdx</code>), not a partition (e.g. <code>/dev/sdx1</code>). 6. Use the <code>sync</code> command to ensure all disk operations finish. 7. Eject the USB drive safely and remove it from the USB port.

Operating System	Description
Mac OS X	<ol style="list-style-type: none"> 1. Insert the flash drive into a USB port on your computer. <div> IMPORTANT All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere. </div> <ol style="list-style-type: none"> 2. Download the kerio-control-rescue file. 3. Run the terminal: Applications > Utilities > Terminal. 4. Use the command <code>sudo diskutil list</code> to detect the USB flash drive name (e.g., <code>/dev/diskX</code> or <code>/dev/DiskY</code>). Note that this is case sensitive. 5. Use the command <code>sudo diskutil unmountDisk /dev/diskX</code> to unmount the flash drive. 6. Save the kerio-control-rescue file to the USB flash drive using this command: <code>sudo dd if=rescue.img of=/dev/disk1 bs=1m</code>. Replace <code>rescue.img</code> with the real file name and <code>/dev/diskX</code> with the actual device name. 7. Eject the flash drive securely and remove it from your computer.

Kerio Control device system recovery

1. Switch off Kerio Control.
2. Plug the USB flash drive into one of the USB ports of your Kerio Control.
3. Switch on Kerio Control. Wait for applying the [kerio-control-rescue](#) script.
4. Kerio Control turns off after the factory reset finishes. Turn off Kerio Control Box 3110 and 3120 manually after some time (15 min) of inactivity.
5. Switch on Kerio Control.
6. Install Kerio Control. For more information, refer to [Installing Kerio Control](#) (page 22).

Recovering the USB flash drive for further use

The recovery file creates partitions on the USB flash drive. To reuse the USB drive for other purposes, you need to remove all disk partitions, create one or more new partitions, and reformat the disk for your file system.

Operating System	Description
Microsoft Windows	<ol style="list-style-type: none"> 1. Click Start and in the Search field enter <code>cmd.exe</code> to open the Command Prompt window. 2. On the command line, enter <code>diskpart</code>. You may need to confirm that you have administration rights. 3. Enter the command <code>list disk</code> to display the list of drives and look up the number of the physical USB drive. 4. Enter the command <code>select disk X</code> (replace X with the number of the corresponding disk). 5. Use the command <code>clean</code> to remove all partitions. 6. Create a new disk partition by entering these commands in the order listed: <pre>create partition primary select partition 1 format fs=fat32 label="USB Flash" quick exit</pre>
Linux	Use the graphical tool GParted or the command <code>fdisk</code> .
Mac OS X	Use the system tool Disk Utility: Application > Utilities > Disk Utility .

Formatting a USB flash drive with MBR

1. Click **Start** and in the **Search** field enter `cmd.exe` to open the **Command Prompt** window.
2. On the command line, enter `diskpart`. You may need to confirm that you have administration rights.

3. Enter the command `list disk` to display the list of drives and look up the number of the physical USB drive.
4. Enter the command `select disk X` (replace X with the number of the corresponding disk).
5. Use the command `clean` to remove all partitions.
6. Create a new disk partition by entering these commands in the order listed:

```
create partition primary
select partition 1
format fs=fat32 label="USB Flash" quick
exit
```

5.4.5 Updating Kerio Control Box NG series using a USB flash drive

You can upgrade the system in your Kerio Control NG box with a USB flash drive.

The update tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

All data and settings remain preserved after the upgrade.

WARNING

There are two types of USB flash drives on the market. Kerio Control NG 500 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control NG 500, but can be reconfigured to work. See [Formatting a USB flash drive with MBR](#).

Upgrading Kerio Control

1. Insert the flash drive into a USB port on your computer.
2. Make sure that only one partition with the **FAT16** or **FAT32 (VFAT)** file system is created on the flash drive. The USB disk must **not** be formatted by the NTFS, ext2, ext3, or ext4 file systems.
3. Download and save the [kerio-control-usbupgrade](#) file to the flash drive.
4. Switch off the Kerio Control box.
5. Plug the USB flash drive into a USB port of your Kerio Control box.
6. Switch on the Kerio Control box. Then the upgrade starts.
7. When the upgrade is complete, the Kerio Control box reboots to the new version.
8. Remove the flash drive from the Kerio Control box.

Kerio Control is upgraded to the desired version.

Related articles

[Recovering your Kerio Control Box NG series password using a USB flash drive](#)

[Restoring the Kerio Control Box NG series default configuration using a USB flash drive](#)

5.4.6 Updating Kerio Control using a USB flash drive

Kerio Technologies provides a system update tool that uses a USB flash drive.

WARNING

We recommend using these tools for Kerio Control Box and Kerio Control Software Appliance. In this article, Kerio Control refers to Kerio Control Box or Kerio Control Software Appliance.

NOTE

This article describes Kerio Control Box 1000/3000 series. For Kerio Control NG series, read [Updating Kerio Control Box NG series using a USB flash drive](#).

The Update tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

Updating Kerio Control

To upgrade Kerio Control:

1. Download the file [kerio-control-usbupgrade](#).
2. Insert the flash drive to your computer into a USB port on your computer.
3. Make sure that only one partition with file system FAT16 or FAT32 (VFAT) is created on the flash drive. The USB disk must not be formatted by file system NTFS, ext2, ext3, or ext4.
4. Save the file [kerio-control-usbupgrade](#) to the flash drive.
5. Switch off Kerio Control.
6. Plug the USB flash drive into one of the USB ports of your Kerio Control.
 - When upgrade process begins, the box beeps once.
 - When upgrade process ends, the box beeps once.
7. Switch on Kerio Control.
 - When Kerio Control boots, the box beeps twice.
 - When Kerio Control Engine starts up, the box beeps three times.

Kerio Control is up to date, and all settings and data are saved.

If the steps above do not work, try another flash drive. Different Kerio Control Box models require different USB drive formats:

- » Kerio Control Box 1110, 3110, 3120, and 3130 require a USB flash drive formatted like a floppy disk (not partitioned).
- » Kerio Control Box 1120 requires a flash drive formatted with a master boot record (MBR). USB drives with floppy-type formatting cannot connect to Kerio Control Box, but can be reconfigured to work. See [Formatting a USB flash drive with MBR](#).

Related articles

[Recovering your Kerio Control password using a USB flash drive](#)

[Diagnostic tools for Kerio Control Box](#)

[Restoring Kerio Control default configuration using USB flash drive](#)

5.4.7 Diagnostic tool for Kerio Control Box

Kerio Technologies provides a tool for diagnosing hardware problems with the Kerio Control Box. This tool collects crucial information for the Kerio Technologies technical support. It is designed to be run from a USB flash drive.

The diagnostic tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

Creating the diagnostic flash drive

The diagnostic tool file, [kerio-control-usbdia](#), is an image of an installation disk and must be saved directly on the physical device. Follow the instructions for your client system below.

Microsoft Windows	<ol style="list-style-type: none">1. Insert the flash drive to your computer into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.2. Download and unpack Image Writer (it does not require installation).3. Download the kerio-control-usbdia file.4. In Image Writer, find the file, select your flash drive and click Write.5. Eject the flash drive securely and remove it from your computer.
Linux	<ol style="list-style-type: none">1. Insert the flash drive into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.2. Download the kerio-control-usbdia file.3. Run the terminal (console).4. Use the command <code>sudo fdisk -l</code> to detect the USB flash drive name (e.g., <code>/dev/sdx</code>).5. Save the kerio-control-usbdia file on the flash drive using this command: <code>sudo dd if=usbdia.img of=/dev/sdx bs=1M</code> where you replace <code>usbdia.img</code> with the real file name and <code>/dev/sdx</code> with the actual device name. You must enter the physical device (e.g., <code>/dev/sdx</code>), not the partition (e.g., <code>/dev/sdx1</code>).6. Use the command <code>sudo sync</code> to ensure that all disk operations finish.7. Eject the flash drive securely and remove it from your computer.
Mac OS X	<ol style="list-style-type: none">1. Insert the flash drive into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.2. Download the kerio-control-usbdia file.3. Run the terminal: Applications > Utilities > Terminal.4. Use the command <code>sudo diskutil list</code> to detect the USB flash drive name (e.g., <code>/dev/diskX</code> or <code>/dev/DiskY</code>). Note that this is case sensitive.5. Use the command <code>sudo diskutil unmountDisk /dev/diskX</code> to eject the flash drive.6. Save the kerio-control-usbdia file on the USB flash drive using this command: <code>sudo dd if=usbdia.img of=/dev/disk1 bs=1m</code> where you replace string <code>usbdia.img</code> with the real file name and <code>/dev/diskX</code> with the real device.7. Eject the flash drive securely and remove it from your computer.

Using the diagnostic flash drive

1. Switch off Kerio Control Box.
2. Plug the USB flash drive into one of the USB ports of your **Kerio Control Box**.
3. Switch on Kerio Control Box.
4. After approximately 2 minutes Kerio Control Box beeps three times. This means that the operating system has been introduced and the diagnostic test has started. If the device does not beep within the following 10 minutes, the test has failed. In that case switch off the device, eject the USB flash drive and send the diagnostic information to Kerio Technologies technical support.
5. The test starts with 10 beeps and runs for about 60 minutes — a 40-minute memory test and a diagnostic test. If you want to skip the memory test, press any key during the ten-beep interval. Once the test is finished, Kerio Control Box

starts beeping every 30 seconds.

6. Switch off Kerio Control Box and eject the USB flash drive.

Test results processing

Reinsert the flash drive into the USB port.

Find the partition called **KerioDiag** on the flash drive. It contains the file with test results.

Send this file to Kerio Technologies technical support, and optionally describe the problem of your Kerio Control Box.

Recovering USB flash drive for further use

To reuse your flash drive, you will need to reformat it to remove the partitions. For more information, refer to [Recovering the USB flash drive for further use](#) (page 364).

Related articles

[Recovering your Kerio Control password using a USB flash drive](#)

[Restoring Kerio Control default configuration using a USB flash drive](#)

[Updating Kerio Control using a USB flash drive](#)

5.4.8 Diagnostic tool for Kerio Control Box NG series

Kerio Technologies provides a tool for diagnosing hardware problems with the Kerio Control Box NG series. This tool collects crucial information for the Kerio Technologies technical support. It is designed to be run from a USB flash drive.

You need a USB flash drive with a capacity of at least 256 MB.

The diagnostic tool is designed for a single use. An operation does not repeat if you restart with the flash drive still in the USB port. Once you perform the operation unplug the flash drive.

Creating the diagnostic flash drive

The diagnostic tool file, [kerio-control-usbdiag](#), is an image of an installation disk and must be saved directly on the physical device. Follow the instructions for your client system below.

Microsoft Windows	<ol style="list-style-type: none">1. Insert the flash drive to your computer (256 MB or larger) into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.2. Download and unpack Image Writer (it does not require installation).3. Download the kerio-control-usbdiag file.4. In Image Writer, find the file, select your flash drive and click Write.5. Eject the flash drive securely and remove it from your computer.
Linux	<ol style="list-style-type: none">1. Insert the flash drive into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.2. Download the kerio-control-usbdiag file.3. Run the terminal (console).4. Use the command <code>sudo fdisk -l</code> to detect the USB flash drive name (e.g., <code>/dev/sdx</code>).5. Save the kerio-control-usbdiag file on the flash drive using this command: <code>sudo dd if=usbdiag.img of=/dev/sdx bs=1M</code> and replace <code>usbdiag.img</code> with the real file name and <code>/dev/sdx</code> with the actual device name. You must enter the physical device (e.g., <code>/dev/sdx</code>), not the partition (e.g., <code>/dev/sdx1</code>).6. Use the command <code>sudo sync</code> to ensure that all disk operations finish.7. Eject the flash drive securely and remove it from your computer.

- Mac OS X
1. Insert the flash drive into a USB port on your computer. All data on the flash drive will be completely overwritten, so be sure to save any files you need elsewhere.
 2. Download the [kerio-control-usbdiag](#) file.
 3. Run the terminal: **Applications > Utilities > Terminal**.
 4. Use the command `sudo diskutil list` to detect the USB flash drive name (e.g., `/dev/diskX` or `/dev/DiskY`). Note that this is case sensitive.
 5. Use the command `sudo diskutil unmountDisk /dev/diskX` to eject the flash drive.
 6. Save the [kerio-control-usbdiag](#) file on the USB flash drive using this command: `sudo dd if=usbdiag.img of=/dev/disk1 bs=1m` and replace string `usbdiag.img` with the real file name and `/dev/diskX` with the real device.
 7. Eject the flash drive securely and remove it from your computer.

Using the diagnostic flash drive

1. Switch off Kerio Control Box.
2. Plug the USB flash drive into one of the USB ports of your **Kerio Control Box**.
3. Switch on Kerio Control Box. It may take some time (approximately 2 minutes).
4. The diagnostic test should run for about 60 minutes.
5. Switch off Kerio Control Box and eject the USB flash drive.

Test results processing

Reinsert the flash drive into the USB port.

Find the partition called **KerioDiag** on the flash drive. It contains the file with test results.

Send this file to Kerio Technologies technical support, and optionally describe the problem of your Kerio Control Box.

Recovering USB flash drive for further use

To reuse your flash drive, you will need to reformat it to remove the partitions. For more information, refer to [Recovering the USB flash drive for further use](#) (page 364).

Related articles

[Recovering your Kerio Control password using a USB flash drive](#)

[Restoring Kerio Control default configuration using a USB flash drive](#)

[Updating Kerio Control using a USB flash drive](#)

5.5 Vulnerabilities

Vulnerability	Description
Bash vulnerability CVE-2014-6271, CVE-2014-7169 (ShellShock)	The shellshock vulnerability (aka CVE-2014-6271 and CVE-2014-7169) is a security bug affecting Unix-like operating systems through the Bash shell. For information on its impact on Kerio products, read Bash vulnerability CVE-2014-6271, CVE-2014-7169 (ShellShock) article.
Linux Glibc vulnerability CVE-2015-7547	A vulnerability in the Linux glibc system library has been found. An attacker can gain root access to the server and execute a code. For more details on its impact on Kerio products, read Linux Glibc vulnerability CVE-2015-7547 article.

Vulnerability	Description
Linux vulnerability CVE-2015-0235 (GHOST)	<p>There is a vulnerability in Linux glibc system library. An attacker can exploit this vulnerability and gain root access to your server and execute a code.</p> <p>For more details on its impact on Kerio products, read Linux vulnerability CVE-2015-0235 (GHOST) article.</p>
OpenSSL vulnerability CVE-2014-0160 (Heartbleed)	<p>The National Institute of Standards and Technology (NIST) has published a vulnerability to OpenSSL 1.0.1. Details regarding the vulnerability are available from the NIST website. Kerio Control 8.2.0 up to 8.2.2 used the affected version of the OpenSSL library. However, a fix is available for Kerio Control as of version 8.2.2 patch 2. You can download this release from the Kerio Website.</p> <p>For additional information and security precautions, read OpenSSL vulnerability CVE-2014-0160 article.</p>
SSL 3.0 vulnerability CVE-2014-3566 and POODLE	<p>This vulnerability is a flaw in the protocol design. An attacker that controls the network between the client and the server can interfere with any attempted handshake offering TLS 1.0 or later and force both client and server to use SSL 3.0 protocol instead. They can then use other attack techniques (eg. BEAST attack) to decipher transmitted data.</p> <p>For information on its impact on Kerio products, read SSL 3.0 vulnerability CVE-2014-3566 (POODLE) article.</p>

6 Glossary

2

2-step verification

Security authentication which includes two steps, which includes password and a special time-limited code.

A

active connection

Any connection between different subnets and the Internet which goes through Kerio Control is an active connection.

Active Directory

A directory service for Windows domain networks.

active host

All hosts and users in the Kerio Control network using Kerio Control for communication with the Internet.

ADSL line

Asymmetric digital subscriber line - A technology for transmitting digital information at a high bandwidth on existing phone lines.

Apple Open Directory

A directory service for Apple based networks.

Application awareness

A part of next generation firewall which allows you to identify and filter traffic according to particular applications.

ASCII

American Standard Code for Information Interchange - A character encoding standard.

B

bridge

A network unit which connects separated subnets.

C

Cacti

Monitoring tool based on SNMP.

D

DHCP

Dynamic Host Configuration Protocol - A protocol that automatically gives IP addresses and additional configuration to hosts in a network.

DMZ

Demilitarized zone - A security method that separates internal LAN networks from external networks.

DNS

Domain Name System - A database enables the translation of hostnames to IP addresses and provides other domain related information.

Domain Controller

A server ensures authentication process in Microsoft Active Directory.

DoS

Denial of Service - An attack that can overload the server and makes it unavailable to users.

DSL

Digital Subscriber Line - A high-speed Internet service over ordinary phone lines using broadband modem technology.

duplex mode

A point-to-point system composed of two connected parties or devices that can communicate with one another in both directions.

E

email alert

Kerio Control can send automatic email messages (alerts) about important events that happen in the Kerio Control environment.

F

FTP

File Transfer Protocol - Protocol for transferring computer files from a server.

G

gateway

Network element that connects networks and shows packets where to go.

GeoIP

The GeoIP filter blocks IP addresses from defined geographical areas (countries).

GPO

Group Policy Object - A collection of settings that define what a system will look like and how it will behave for a defined group of users.

H**hardware appliance**

Kerio Control installed and delivered with standardized and tested hardware box.

HTTP

Hypertext Transfer Protocol - protocol for exchange of hypertext documents in HTML.

HTTPS

Hypertext Transfer Protocol - version of HTTP secured by SSL.

I**IDS/IPS**

An intrusion detection and prevention system that detects malicious activities in the network.

IMAP

Internet Message Access Protocol - One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.

intrusion prevention system

A technology that protects against network and application-level attacks, securing organizations against intrusion attempts, malware, trojans etc.

IP address

An identifier assigned to devices connected to a TCP/IP network.

IPsec

Internet Protocol security - A network protocol used to encrypt and secure data sent over a network.

IPv4

Version 4 of the Internet Protocol.

IPv6

Version 6 of the Internet Protocol.

IPv6 prefix

IPv6 prefix is a part of IPv6 address dedicated for routing in IPv6 networks.

ISP

Internet Service Provider - the organization which can provide Internet service.

K

Kerio Antivirus

An integrated antivirus engine powered by Bitdefender.

L

L2TP

Layer 2 Tunneling Protocol - A tunneling protocol used with IPsec.

LAN

Local area network - A network that connects computers and other devices in a small area.

LAN switch

A network unit which connects separated subnets.

large segment offload (LSO)

A technique for increasing egress throughput of high-bandwidth network connections by reducing CPU overhead.

LDAP

Lightweight Directory Access Protocol - A protocol that enables users to access centrally managed contacts.

load balancing

Algorithm distributes network or application traffic across multiple internet links.

M

MAC address

Media Access Control Address - A unique identifier that specifies a device in a network.

MTU

Maximum Transmission Unit - The largest size packet specified in octets that can be sent in a packet or frame based network such as the Internet.

multihoming

Term for the internet interface which uses multiple public IP addresses.

N

NAT

Network address translation - A method that remaps IP addresses by changing network address information.

non-transparent proxy

A non-transparent is used so that the web browser and other client applications know that a proxy is being used, and so can act accordingly.

NTLM

NT LAN Manager - Security protocols that provide authentication for Windows networks.

P

P2P

Peer-to-Peer networks are worldwide distributed systems where each node can be used both as a client and a server.

packet dump

A network trace or intercepting a data packet that is crossing or moving over a specific computer network.

Peer-to-Peer

A distributed application architecture that partitions tasks or workloads between peers.

policy routing

Policy routing allows you to force certain types of traffic out a particular interface.

POP3

Post Office Protocol 3 - A protocol used by local email clients to retrieve emails from mailboxes over a TCP/IP connection.

PPPoE

A type of tunneled link, which is established over top of a physical network interface.

PPTP

Point-to-Point Tunneling Protocol - A set of communication rules that allows to extend corporate network through private tunnels over public Internet.

protocol inspector

The inspector filters the communication or adapt the firewall's behavior according to the protocol type.

Q

QoS

Quality of service - Network's ability to obtain maximum bandwidth and manage other network performance elements like latency, error rate and uptime.

R

RADIUS

Remote Authentication Dial-In User Service - A protocol that offers authentication, authorization, and accounting of users in a network.

Remote Desktop IP Virtualization

Assigning IP addresses to remote desktop connections on a per session or per program basis.

root certificate

A certificate issued by a trusted certificate authority (CA). In the SSL, anyone can generate a signing key and sign a new certificate.

root certificate authority

A trusted entity that issues electronic documents that verify a digital entity's identity on the Internet.

S**SafeSearch**

Blocks inappropriate or explicit content in search results.

Service Discovery protocols

Protocols that allow remote users across VPN tunnels or other networks to locate and reach devices.

SIP

Session Initiation Protocol - Communication protocol used for voice and video calls in Internet telephony or private IP telephone systems.

SNMP

Simple Network Management Protocol - A protocol to manage network.

Software Appliance

A special operating system designed to run on a computer.

split tunneling

A method of routing traffic between their ISP and a VPN.

SSH

Secure Shell - A cryptographic network protocol that enables you to connect securely over an unsecured network.

SSL

Secure Sockets Layer - A protocol that ensures integral and secure communication between networks.

SSL certificate

SSL certificates are used to authenticate an identity on a server.

T**TCP**

Transmission Control Protocol - ensures packet transmission.

TCP/IP

Transmission Control Protocol/Internet Protocol - Communication protocols that connect computer hosts to the Internet.

TLS

Transport Layer Security - A follower of the SSL protocol and ensures secure communication between networks.

transparent proxy

A server which redirects requests and responses between computers in the Internet and those in local network.

U

UDP

User Datagram Protocol - ensures packet transmission.

V

Virtual Appliance

Pre-configured Kerio Control virtual machine image for VMware or Hyper-V.

VoIP

Voice over Internet protocol - A digital telephone system that uses the internet as the transmission medium, rather than the PSTN.

VPN

Virtual private network - A network that enables users connect securely to a private network over the Internet.

VPN server

Kerio Control includes a VPN server which provides users to connect to the Kerio Control network from the Internet securely.

VPN tunnel

Kerio Control includes a VPN tunnel which allows to distributed offices to interconnect their offices securely.

W

WAN

Wide area network - A network that connects computers and other devices in a large area.

7 Legal Notices

7.1 Trademarks and registered trademarks

- » Microsoft®, Windows®, Hyper-V®, 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.
- » Bitdefender® is registered trademark of BitDefender IPR Management Ltd.

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

7.2 Open source software

Kerio Control contains the following open-source software:

7.2.1 bindlib

Copyright © 1983, 1993 The Regents of the University of California. All rights reserved.

Portions Copyright © 1993 by Digital Equipment Corporation.

7.2.2 Clearsilver

Clearsilver is a fast, powerful, and language-neutral HTML template system.

Copyright © 2001 Brandon Long and Neotonic Software Corporation. All rights reserved.

This product includes software developed by the Neotonic Software Corporation. (<http://www.neotonic.com/>)

7.2.3 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/>

7.2.4 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.

7.2.5 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/>

7.2.6 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/>

7.2.7 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/>

7.2.8 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/>

7.2.9 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/>

7.2.10 libcurl

Copyright © 1996-2008, Daniel Stenberg.

7.2.11 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/>

7.2.12 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.

7.2.13 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.

7.2.14 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

7.2.15 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.

7.2.16 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.

7.2.17 Operating system

Kerio Control in editions Appliance and Box are based on various open source software. 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/>

7.2.18 PHP

Copyright © 1999-2006 The PHP Group. All rights reserved.

This product includes PHP software, freely available from <http://www.php.net/software/>

7.2.19 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/>

7.2.20 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/>

7.2.21 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/>

7.2.22 ScoopyNG

The VMware detection tool.

This product includes software written by Tobias Klein.

Copyright © 2008, Tobias Klein. All Rights Reserved.

7.2.23 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/>

7.2.24 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.

7.2.25 zlib

Copyright © Jean-Loup Gailly and Mark Adler.