

# Kerio Control VMware Virtual Appliance

## Quick Setup Guide

This document provides detailed description on installation and basic configuration of the Kerio Control VMware Virtual Appliance, version 8. All additional modifications and updates reserved. For detailed information on Kerio Control, refer to [Kerio Knowledge Base](#) and related documents.

© 2017 Kerio Technologies s.r.o. All rights reserved.

### Kerio Control VMware Virtual Appliance

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

#### System requirements

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

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

#### Licensing Policy

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 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://download.kerio.com/dwn/control/  
kerio-control-appliance-1.2.3-4567-linux.ovf
```

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

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**. For more information, read [Configuring network 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.



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 startup on VMware. All configuration parameters any other data will be removed and the initial configuration wizard is started again (see section [3](#)). Restoration of default configuration is useful especially if the firewall does not work correctly and you cannot easily fix the configuration.