

Kerio Control Virtual Appliance for Hyper-V

Quick Setup Guide

This document 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. 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 Virtual Appliance for Hyper-V

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 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.

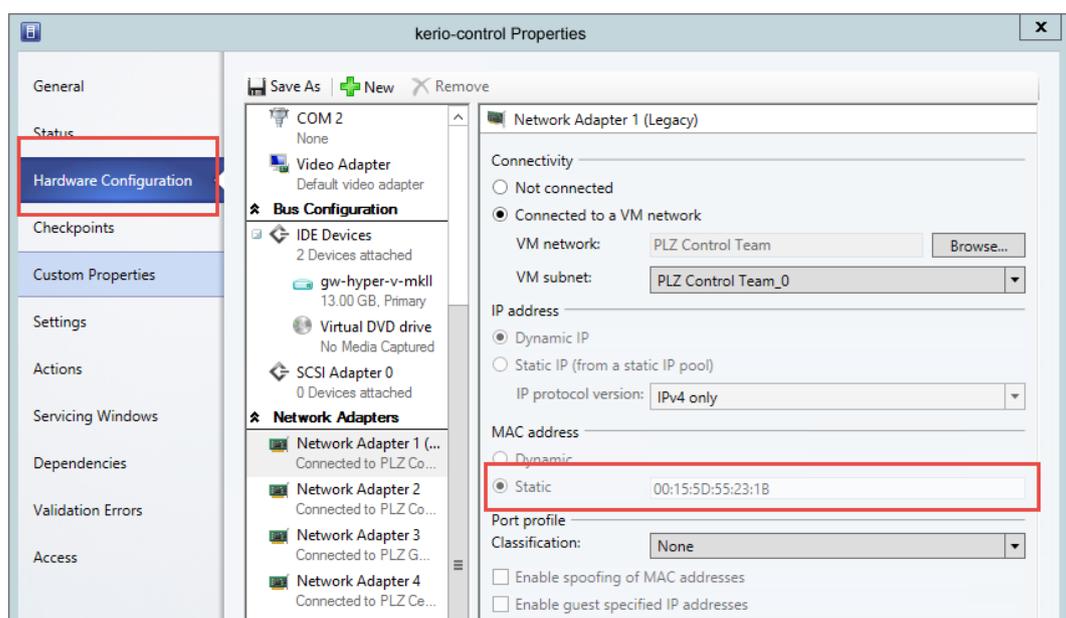
To change the automatic pre-configuration, go to Kerio Control Administration to section **Interfaces**. For more information, read [Configuring network interfaces](#).

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.



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.



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 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.