

GUIDE

GeoIP User Guide



GFI Software™

Overview

GeoIP identifies a user's location based on their IP address. It reveals where someone is connecting from. When you browse the web, GeoIP checks your IP against a database, mapping you to a spot on the globe like a country or city.

Benefit of for Using GeoIPs

- 1 Blocking all incoming traffic from a specific country
- 2 Blocking traffic from countries known for high levels of cyber threats
- 3 Restricting access to sensitive resources based on geographical location
- 4 Regulatory compliance that mandates traffic control from specific countries.

Usage of GeoIP in Kerio Control

1 GeoIP Filtering:

Kerio Control allows you to enable a GeoIP filter for incoming traffic. This filter helps you effectively stop malicious traffic and potential threats. To block all incoming connections from a specific country:

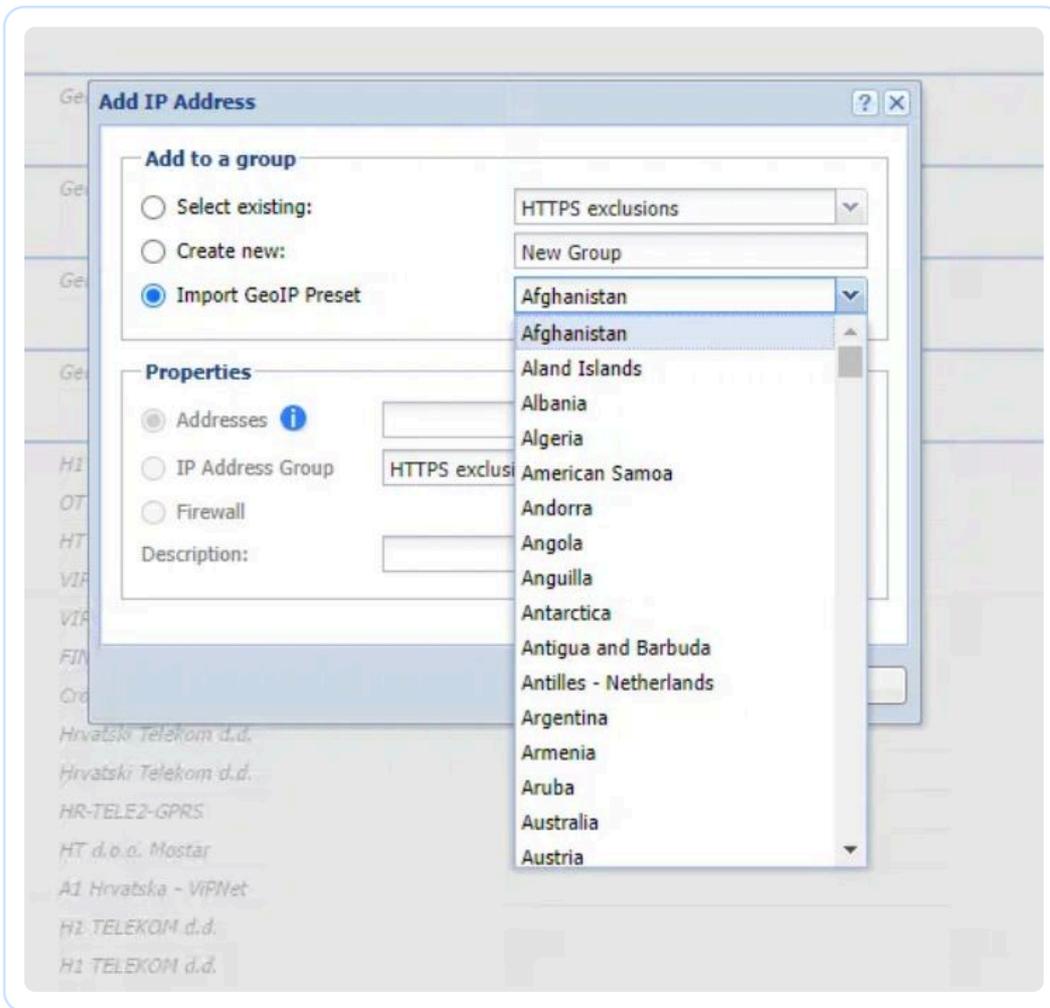
- a. In the administration interface, go to **SecuritySettings > GeoIPFilter**.
- b. Verify that the **Blockincoming traffic from the following countries** option is enabled.
- c. Click **Add**.
- d. In the **Select Items** dialog box, select the countries you want to block.
- e. Click **OK**.
- f. Click **Apply**.
- g. From now on, Kerio Control blocks **ALL** traffic connections from the selected countries. Outgoing connections are allowed.

2 Rule Creation:

Network administrators can create firewall rules that incorporate GeoIP data.

- a. Create a GeoIP within IP Address groups
- b. Select the GeoIP Checkbox

c.



d. Use the GeoIP Group in FW rules.

3 GeoIP use in GFI AppManager:

Administrators can use the GFI AppManager to create GeoIP within IP Address Groups that can be used for firewall rules.

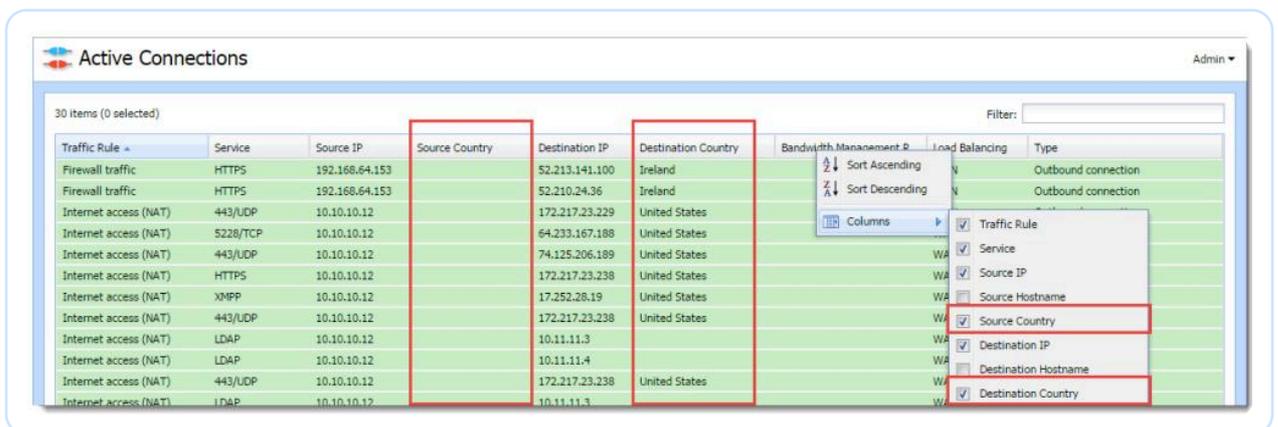
- a. Go to your GFI AppManager and your GFI KerioConnect.
- b. Navigate to the to Create IP Address Group



4 Traffic Monitoring (Firewall Rules):

GeoIP data can be used to monitor and log traffic patterns based on geographic origin. 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:

- a. In the administration interface, go to **SecuritySettings > GeoIPFilter**.
- b. Select **Blocking incoming** traffic from the following countries.
- c. Click **Apply**.
- d. In the administration interface, go to **Status > Active Connections**.
- e. Right-click the table header.
- f. In the context menu, scroll down to **Columns** and select **Source Country** and **Destination Country**.



Monitor Firewall Rule Usage

Traffic Rule Menu

Each time a firewall rule is used, there will be a timestamp indicating when it was used. Administrators can view this information in the Traffic Rule menu to track when specific rules are triggered.

- **Enable Debug Logging:** To monitor detailed usage of firewall rules, enable the Debug log:
 - Go to **Logs > Debug** in the administration interface.
 - Right-click the log window and select **Messages**.
 - In the **Logging Messages** dialog box, select **Packets dropped** for some reason to view blocked traffic and rule usage.

- **Status > Active Connections:** In the Active Connections section, administrators can see which connections are being managed by specific firewall rules. This provides real-time insights into how rules are applied to traffic.

5 **Logging blocked incoming connections from specified countries:**

To verify which packets are dropped by Kerio Control, use the Debug log

- a. In the administration interface, go to **Logs > Debug**.
- b. Right-click to the log window.
- c. In the context menu, click **Messages**.
- d. In the **Logging Messages** dialog box, select **Packets dropped for some reason**.
- d. Click **OK**.

Below is a list of features and the GFI KerioControl version they are available in:

- 1 **GeoIP Filtering:** Version 9.2 and later
- 2 **Rule Creation:** Version 9.4.5p1 and later
- 3 **GeoIP use in GFI AppManager:** Version 9.4.5 and later
- 4 **Traffic Monitoring:** Version 9.2 and later
- 5 **Logging blocked incoming connections from specified countries:** Version 9.2 and later



[Contact us](#) today to learn how GFI KerioControl can help you meet your security and compliance requirements