GUIDE

OpenVPN Integration in GFI KerioControl

GFI Software™

GFI KerioControl 9.5.0 introduces native support for OpenVPN, providing a secure, flexible, and widely compatible VPN solution directly from the GFI KerioControl interface. This integration allows organizations to offer safe remote access to internal networks, leveraging the robust OpenVPN protocol across multiple operating systems. The feature simplifies setup, enhances security, and streamlines management for administrators and end users alike.

Benefits

Enhanced Security

OpenVPN uses SSL/TLS for encryption and authentication, protecting data transmitted between remote users and the internal network.

Broad Compatibility

Users can connect from Windows, macOS, Linux, iOS, and Android devices using standard OpenVPN clients.

Simple Deployment

Configuration files can be exported from Kerio Control and easily imported into client devices, minimizing setup time and user errors.

Key Features

Built-In OpenVPN Server

No need for separate VPN hardware or software.

Customizable Settings

Administrators can select ports, IP ranges, and traffic rules for VPN access.

Certificate-Based Authentication

Uses SSL certificates for secure user verification.

Easy Monitoring

Real-time overview of connected VPN clients from the GFI KerioControl dashboard.

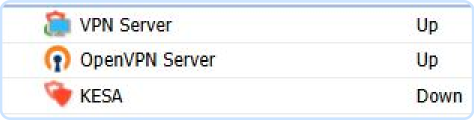
Prerequisite

GFI KerioControl requires its WAN interface to be accessible from the Internet to ensure proper connectivity and functionality.

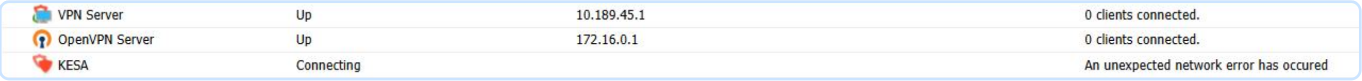
How to Configure OpenVPN

1 Enable OpenVPN

- Go to **Configuration** > **Interfaces** in the GFI KerioControl admin interface.
- Double-click **VPN Server** and check **Enable OpenVPN Server.**



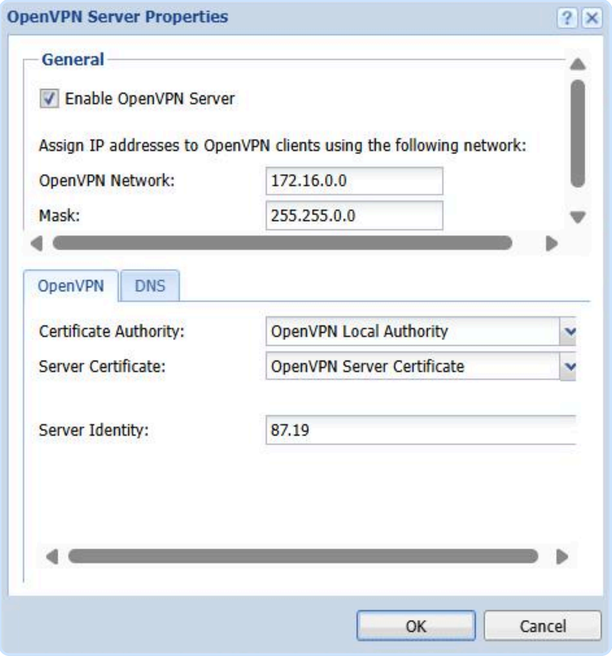
VPN Server	Up
OpenVPN Server	Up
KESA	Down



VPN Server	Up	10.189.45.1	0 clients connected.
OpenVPN Server	Up	172.16.0.1	0 clients connected.
KESA	Connecting		An unexpected network error has occured

2 Configure OpenVPN Settings

- Select a valid SSL certificate.
- Set the VPN subnet (e.g., 10.10.10.0/24) and port (default: 1194).
- Set the public IP address or hostname that allows GFI KerioControl to be accessed from the Internet as the "Server Identity."



OpenVPN Server Properties

General

☑ Enable OpenVPN Server

Assign IP addresses to OpenVPN clients using the following network:

OpenVPN Network: 172.16.0.0

Mask: 255.255.0.0

Certificate Authority: OpenVPN Local Authority

Server Certificate: OpenVPN Server Certificate

Server Identity: 87.19

3 Adjust Traffic Rules

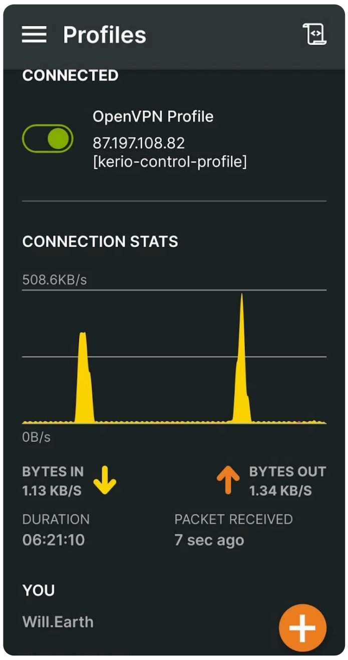
- Make sure VPN traffic is allowed by reviewing **Configuration** > **Traffic Rules.**
- Create or modify rules to permit VPN connections to internal resources.

4 Export and Distribute Client Configurations

- Export the OpenVPN configuration file from GFI KerioControl.
- Provide it to users for import into their OpenVPN client application.

5 Client Connection

- Users install the OpenVPN client for their OS.
- Import the configuration and connect.



Profiles

CONNECTED

OpenVPN Profile
87.197.108.82
[kerio-control-profile]

CONNECTION STATS

508.6KB/s

0B/s

BYTES IN 1.13 KB/S

BYTES OUT 1.34 KB/S

DURATION 06:21:10

PACKET RECEIVED 7 sec ago

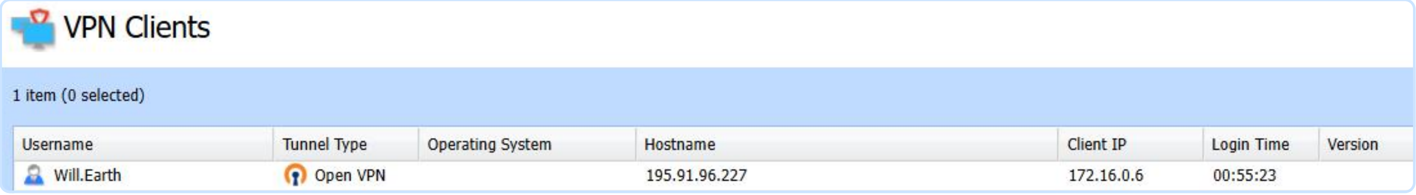
YOU

Will.Earth

Additional Notes

- Make sure users have VPN access rights in Users and Groups.
- Confirm the firewall allows connections on the OpenVPN port.
- Monitor and manage active VPN sessions in Status > VPN Clients.

Important: If 2FA is enabled globally for the VPN, OpenVPN will connect but may not work properly. The app won't prompt for the 2FA token automatically, so users need to manually open a web browser and enter the 2FA URL to complete the login.



VPN Clients

1 item (0 selected)

Username	Tunnel Type	Operating System	Hostname	Client IP	Login Time	Version
Will.Earth	Open VPN		195.91.96.227	172.16.0.6	00:55:23	