# IKEv2 Client-to-Site Connection Configuration in GFI KerioControl





# Overview

Internet Key Exchange version 2 (IKEv2) is a tunneling protocol, based on IPsec. It is responsible for setting up a Security Association (SA) for secure communication between VPN clients and VPN servers within IPSec. IKEv2 supports all major platforms, including Windows, macOS, Android, iOS, Linux, and routers. The protocol is also compatible with smart devices like Smart TVs and some streaming devices.

The VPN protocol is widely implemented in mobile devices mainly due to its fast speed, stability, and high reliability when switching between networks. In this guide, we will cover how you can connect your iOS or Android device to the GFI KerioControl firewall over an IKEv2 VPN connection.

# iOS devices Using Preshared key

In this section, we will cover how you can connect to the GFI KerioControl firewall over an IKEv2 connection using a preshared key from an iOS device.

## Server-side configuration

Configure the VPN interface as below:

General			
Enable IPsec VPN Serv	er		
Enable Kerio VPN Serve	r		
Assign IP addresses to VP	I clients using the following netw	vork:	
VPN Network:	172.27.156.0		
Mask:	255.255.255.0		
10	Date I Hante		
IPSEC VPN KERIO VPN	DNS WINS		1.5
Certificate: 🕕	server9	▼ Edit	)
IKE version:	IKEv1/IKEv2	~	
IKEv2 preshared key ident	ty: kerio		
Use certificate for clien	ts		
Vse preshared key:	*******		
Enable MS-CHAP v2 au	thentication		

**Note:** You can set your preferred value for "preshared key" and "IKEv2 preshared key identity".



## iOS device configuration

- Description: <choose any>
- Server: GFI KerioControl domain/IP address
- Remote ID: GFI KerioControl domain/IP address
- Local ID: IKEv2 preshared key identity from GFI KerioControl VPN server configuration
- User Authentication: Set to "username"
- Username: GFI KerioControl user having permission to use VPN connections
- Password: GFI KerioControl user's password

### iOS devices Using a certificate

In this section, we will cover how you can connect your iOS device to the GFI KerioControl firewall over an IKEv2 connection using a certificate.

## Server-side configuration

Configure the VPN interface as below:

General		
Enable IPsec VPN Ser	ver	
Enable Kerio VPN Ser	ver	
Assign IP addresses to V	PN clients using the following netv	vork:
VPN Network:	172.27.156.0	(dentropie)
Mask:	255,255,255,0	
	233,233,233,0	
	~ <u> </u>	
IPsec VPN Kerio VPN	DNS WINS	
Certificate: 1	server9	✓ Edit
IKE version:	IKEv1/IKEv2	×
IKEv2 preshared key ider	itity: kerio	
Use certificate for clie	nts	
Use preshared key:	*******	
Enable MS-CHAP v2 a	uthentication	



#### iOS device configuration

- Description: <choose any>
- Server: Domain name of the GFI KerioControl certificate
- Remote ID: Domain name of the GFI KerioControl certificate
- Local ID: GFI KerioControl user having permission to use VPN connections
- User Authentication: Set to "username"
- Username: GFI KerioControl user having permission to use VPN connections
- Password: GFI KerioControl user's password

#### Android devices Using certificate

In this section, we will cover how you can connect your Android device to the GFI KerioControl firewall over an IKEv2 connection using a certificate.

#### Server-side configuration

General		
Enable IPsec VPN Server		
Enable Kerio VPN Server		
Assign IP addresses to VPN clie	ents using the following network:	
VPN Network:	172.27.156.0	
Mask:	255.255.255.0	
IPsec VPN Kerio VPN DP	NS WINS	_
Certificate: 🕕	server9 🗸 Edit	2
IKE version:	IKEv1/IKEv2	
IKEv2 preshared key identity:	kerio	
Use certificate for clients		
Vise preshared key:	******	
Enable MS-CHAP v2 authen	tication	



#### **Client-side configuration**

- Description: <choose any>
- Type: IKEv2/IPSEC MSCHAPv2
- Server address: Domain name of the GFI KerioControl certificate
- IPSec identifier: GFI KerioControl user having permission to use VPN connections
- IPSec CA certificate: In case of self-signed certificates issued by GFI KerioControl, it should be set to the imported 'Local Authority' GFI KerioControl's certificate
- IPSec server certificate: received from the server
- Username: GFI KerioControl user having permission to use VPN connections
- Password: GFI KerioControl user's password

Note: If you're using a LetsEncrypt-issued certificate and face any issues, please add this certificate into trusted CA roots on the Android device.

