# Native iOS IPsec VPN Client

https://campus.barracuda.com/doc/73718947/

If you are not using CudaLaunch, you can also manually configure the native IPsec client on iOS devices. This setup must be completed on every device that connects to the client-to-site VPN and is valid only for IPsec IKEv1 VPN configurations. Changes to the VPN configuration must be replicated manually on every connected device.

Manually configuring and managing IPsec VPN connections on mobile devices is not recommended. Due to the large number of device types, operating system variants, and the frequency of system updates, manually configured IPsec VPN connections often do not work. Instead of manually configuring IPsec VPN connections on mobile devices, we strongly recommend using CudaLaunch to automatically manage the VPN connection and to keep the client configuration up-to-date.

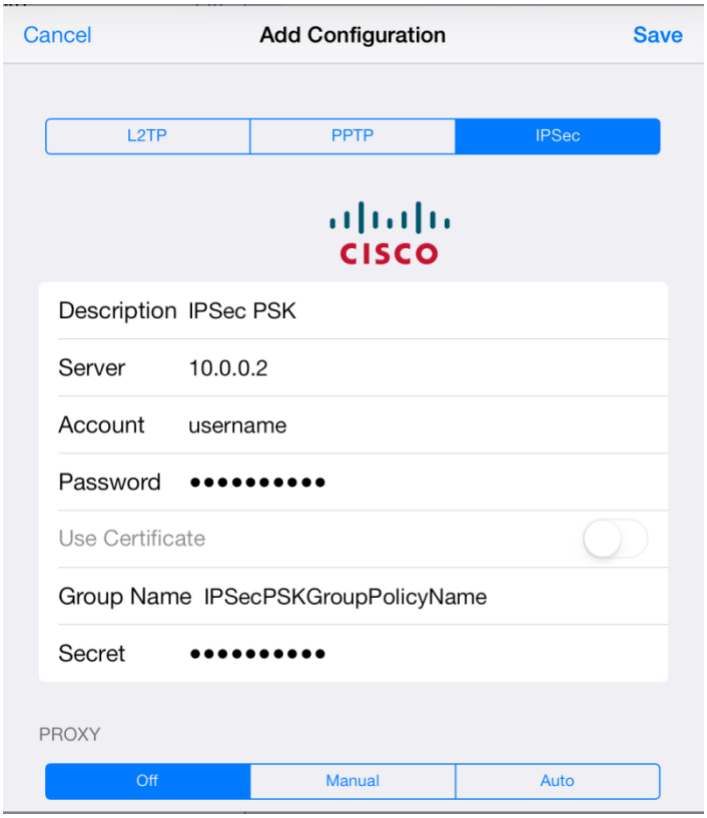
For more information, see CudaLaunch.

## Before You Begin

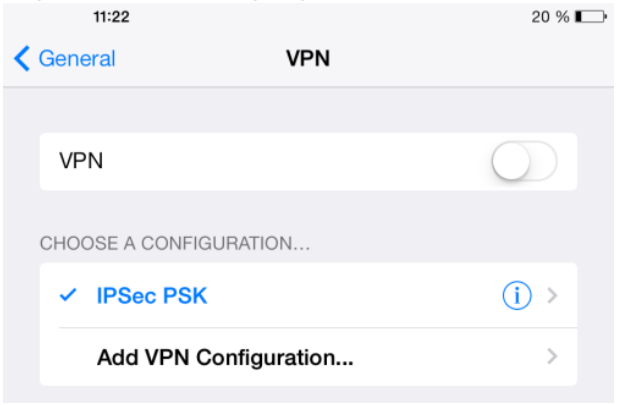
- Verify that the device is using iOS 6.0 or above.
- Configure the client-to-site IPsec IKEv1 VPN with PSK or client certificate authentication. For more information, see Client-to-Site VPN.

## Configure the Native iOS VPN Client for Client-to-Site IPsec VPNs with PSK

1. On the Apple iOS device, tap **Settings > General > VPN > Add VPN Configuration**.
2. On the **Add VPN configuration** screen, tap the **IPSec** tab.
3. Configure the following settings:
   - **Server** – The IP address or FQDN that the VPN service is listening on (e.g., `10.0.0.2`).
   - **Account** and **Password** – Enter the username and password.
   - **Secret** – Enter the PSK.
   - **Group Name** – Enter the VPN Group Policy name configured on the firewall. This string is also used as part of the IP group identifier on the **VPN > Client-to-Site** page.




4. Tap **Save** in the top right corner. The VPN configuration then appears on the **VPN** screen.




After configuring the Apple device, you can connect to the IPsec VPN. Tap **Settings** and then turn on **VPN**. After a few seconds, the VPN icon appears in the status bar to indicate that the connection is successful.

## Configure the Native iOS VPN Client for Client-to-Site IPsec VPNs with Certificate Authentication

#### Step 1. Verify that the Certificate meets Apple's Requirements

For the iOS devices to be able to connect to a client-to-site IPsec VPN with certificate-based

authentication, verify that the root, server, and client certificates are created according to Apple's specifications. Do not use identical **Subject Alternative Names** settings. **Subject Alternative Names** must not contain the management IP address of the firewall.

| X.509 Certificate Type | Installation Device | File Type | Chain of Trust | X.509 Extensions and Values |
|---|---|---|---|---|
| root certificate | firewall + iOS device | PEM | trust anchor | • Mandatory option for key usage**:** **Certificate sign**; **CRL sign**. |
| server certificate | firewall | PKCS12 | end instance | • **Key Usage** – Include the **Digital Signature** flag. • **Subject Alternative Name** – DNS: tag with the FQDN that resolves to the IP that the VPN service listens on, or create a wildcard certificate. For example: `DNS:vpn.yourdomain.com` or `DNS:*` |
| client certificate | Apple iOS device | PKCS12 | end instance | • **Key Usage** – Include the **Digital Signature** flag. |

#### Step 2. Configure the iOS Device

You must import the root and the client certificate on the Apple iOS device. You can import the certificate via email or by downloading it from a web server. If you are using a Mobile Device Management (MDM) server, you can also push the certificates to your devices.

To configure an Apple iOS device for IPsec VPN connections with the Barracuda CloudGen Firewall:

1. On the iOS device, tap **Settings > General > VPN > Add VPN Configuration**.
2. On the **Add VPN configuration** screen, tap the **IPsec** tab.
3. Configure the following settings:
   - **Server** – The Subject Alternative Name used in your certificates.
   - **Account** and **Password** – The XAUTH username and password.
   - **Use Certificate** – Enable it.
   - **Certificate** – The X.509 client certificate.

Establishing VPN through NAT can be problematic. If you experience connection losses, increase the UDP timeout on the NAT'd device. For example, the iPhone sends keepalive packets every 60 seconds, so you can enter any value over 60 seconds. Unfortunately, many cell phone providers use NAT to connect mobile devices to the Internet. Contact your cell phone provider support for help.

## Figures

1. IOS-PSK_01.png
2. IOS-PSK_02.png