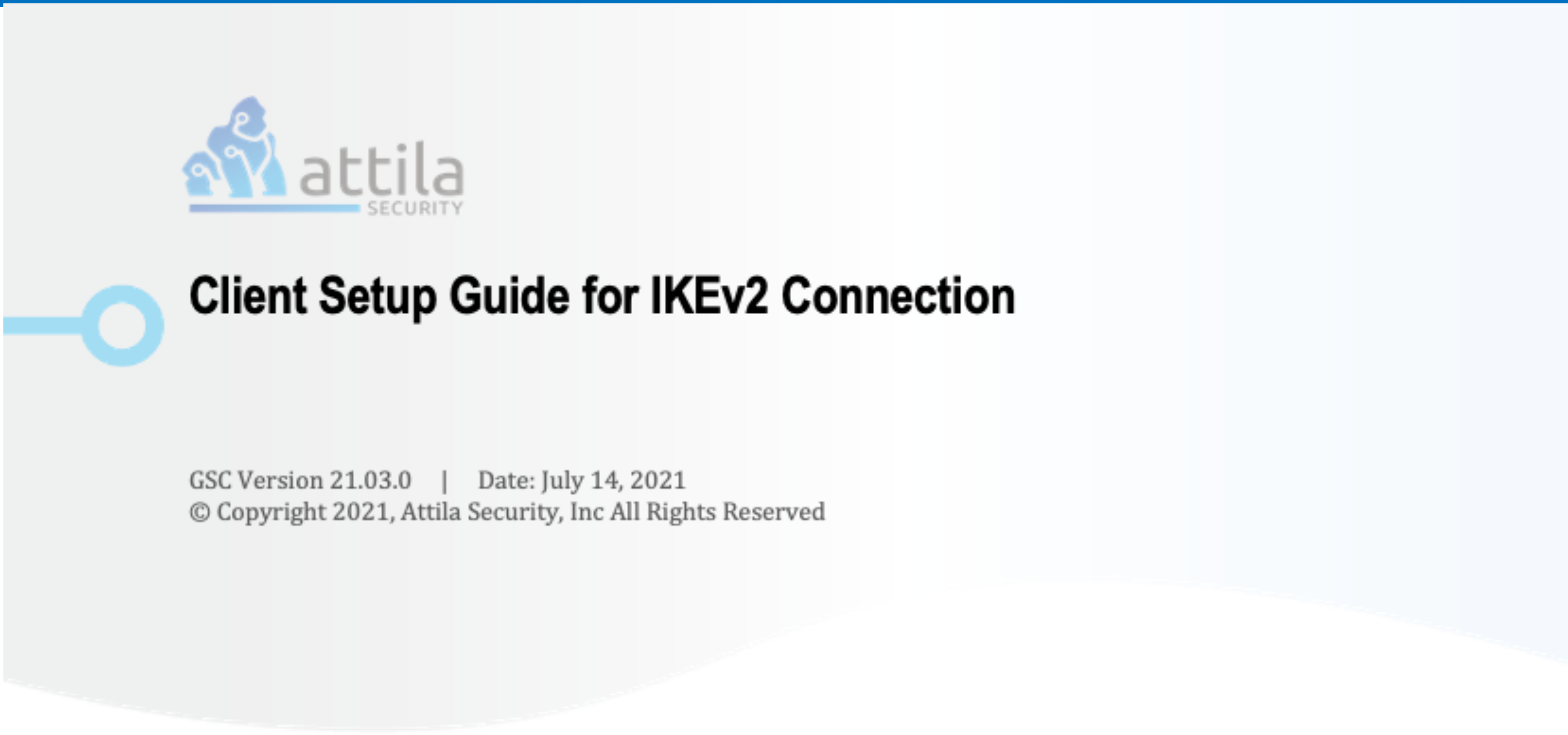
CLIENT SETUP GUIDE FOR IKEV2 CONNECTION



Client Setup Guide for IKEv2 Connection

GSC Version 21.03.0 | Date: July 14, 2021

Background:

The GoSilent Server supports the use of two IKE protocols. IKEv1 with pre-shared keys (PSK's) and IKEv2 with certificates. In order to set your GoSilent client up with IKEv2 your server must first be setup with IKEv2. There are a number of steps to follow when setting up the IKEv2 protocol for a GoSilent client connection. Those steps are described in the remainder of this document.

CLIENT SETUP GUIDE FOR IKEV2 CONNECTION

Table of Contents

Certificate Requirements

CN without SAN

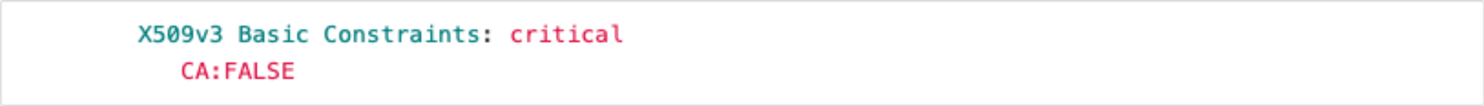
GoSilent clients **prior to the 21.03** release must use this method.
GoSilent clients **21.03 and later** release may use this method.

If you are creating a GoSilent client IKEv2 certificate without SAN, follow these requirements:

- The **Subject** field must contain **only** a Common Name (CN) attribute, which is set to **Client ID** value that matches the one on the GoSilent Server.
  Other **Subject** field attributes such as O, OU, C, etc. are **not** allowed

- The certificate **must** be an **end-entity/leaf** certificate, it **cannot** be a CA certificate.
  This is specified when generating the certificate by setting a **basic constraint** to **CA:FALSE**

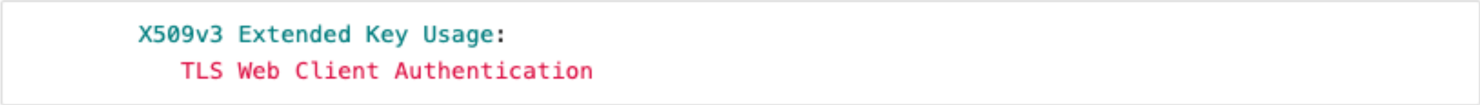
  Here is an example:



```
X509v3 Basic Constraints: critical
   CA:FALSE
```

- The **Extended Key Usage** must be set to **client authentication**

  Here is an example:



```
X509v3 Extended Key Usage:
   TLS Web Client Authentication
```

Certificate Requirements

CN with SAN

This method is supported only for GoSilent client releases **21.03 and later.**

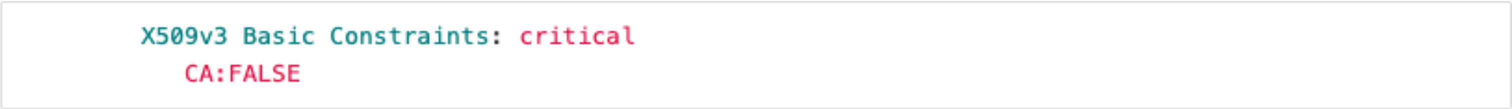
If you are creating a GoSilent client IKEv2 certificate with SAN, follow these requirements:

- The **Subject** field may contain any attributes defined in X.509 specification, such as CN, O, OU, C, etc.

- The **SAN** field must contain the value of **Client ID** that matches the one on the GoSilent server.

- The certificate **must** be an **end-entity/leaf** certificate, it **cannot** be a CA certificate
  This is specified when generating the certificate by setting a **basic constraint** to **CA:FALSE**

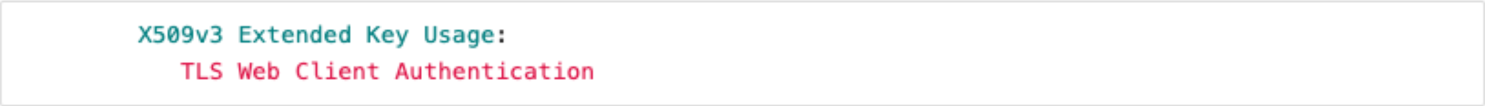
  Here is an example:



```
        X509v3 Basic Constraints: critical
           CA:FALSE
```

- The **Extended Key Usage** must be set to **client authentication**

Here is an example:

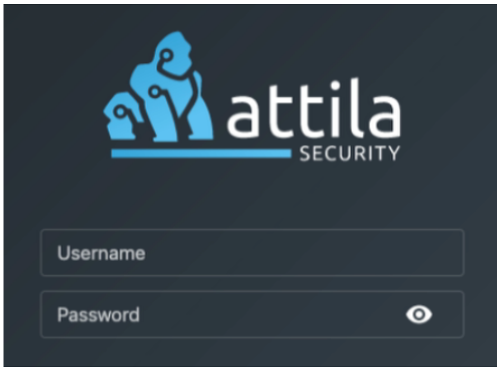


```
        X509v3 Extended Key Usage:
           TLS Web Client Authentication
```

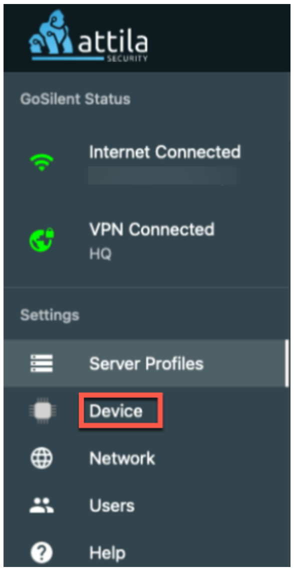
Client Certificates: Navigation

1 Log into the "GoSilent Console"

*Log into the "**GoSilent Cube Console**" by navigating to "https://setup.gosilent". Please note if you do not have this login information to contact our customer support team at "https://attilasec.zendesk.com" who will be glad to assist you*



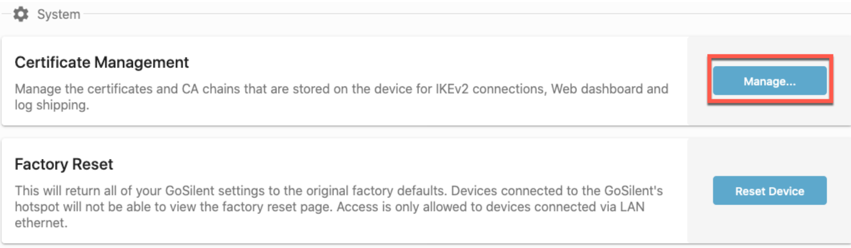
2 Select "Device"



*Select the "**Device**" page which can be found on the left menu below Servers Profiles. If your menu is collapsed simply select the icon displaying a circuit*

3 Select "Manage"

*On the right hand-side of Certificate Management, select "**Manage…**". Depending on your MAC/PC's resolution, this may require you to scroll down*



Certificate Management

Manage the certificates and CA chains that are stored on the device for IKEv2 connections, Web dashboard and log shipping.

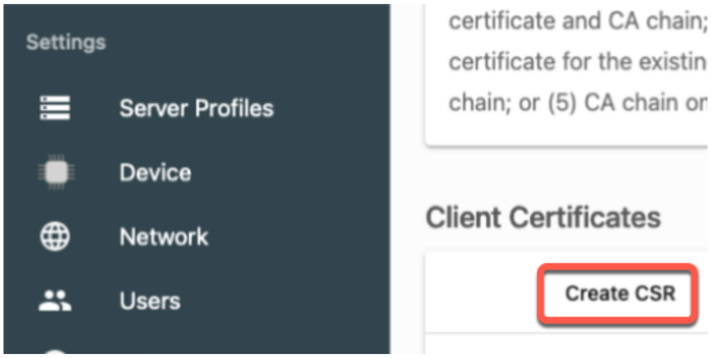
Factory Reset

This will return all of your GoSilent settings to the original factory defaults. Devices connected to the GoSilent's hotspot will not be able to view the factory reset page. Access is only allowed to devices connected via LAN ethernet.

Client Certificates: Common Name / Key Size

4 Select "Create CSR"

*Select **"Create CSR"** which is located directly below Client Certificates. Once this has been selected a menu will appear on the right-hand side*

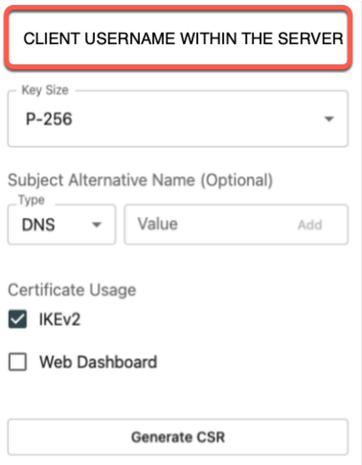


certificate and CA chain;
certificate for the existin
chain; or (5) CA chain or

5 Input the "Common Name" (CN)

*On the right-hand menu, enter the "**Common Name**" in the "**CN**" field.*

Important Note: The Common Name "CN" must match exactly with the "Client Username" within your Virtual Server otherwise the VPN connection will fail due to invalid credentials



CLIENT USERNAME WITHIN THE SERVER

Key Size: P-256

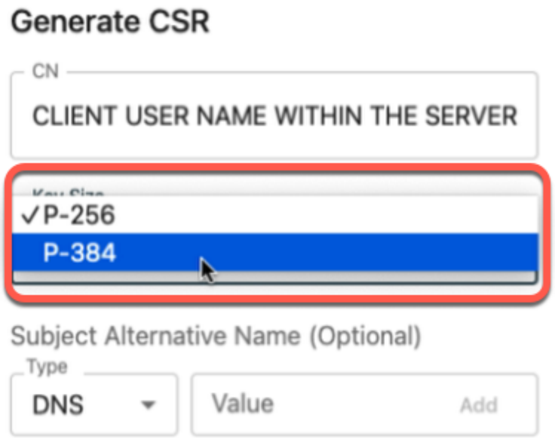
Type: DNS

☑ IKEv2

☐ Web Dashboard

6 Select "Key Size"

*Select **"Key Size"** on the right-hand menu. Select either P-256 or P-384 depending on your encryption bit size preference*



CN: CLIENT USER NAME WITHIN THE SERVER

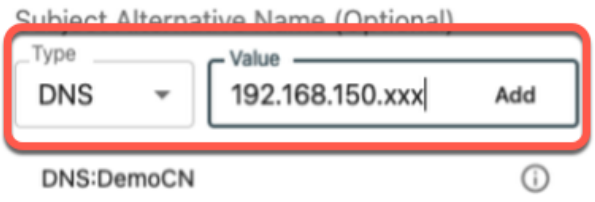
Type: DNS

Client Certificates: SAN / Generating CSR

7 Input "Subject Alternative Name"

*[OPTIONAL]: As an additional option you can also input a Subject Alternative Name or (SAN). The SAN can add an additional "**DNS**" or "**IP**" address.*

Important Note: This is optional and if you do not have any additional SANs feel free to skip this step

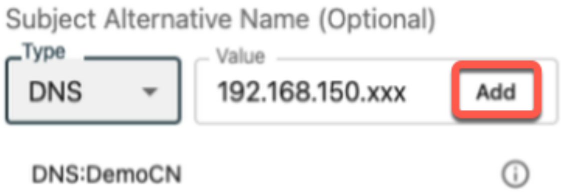

Subject Alternative Name (Optional)
Type: DNS
Value: 192.168.150.xxx

DNS:DemoCN

8 Select "Add"

*[OPTIONAL]: Once you have added your additional DNS or IP select "**Add**" on the right-hand side of the SAN value information.*

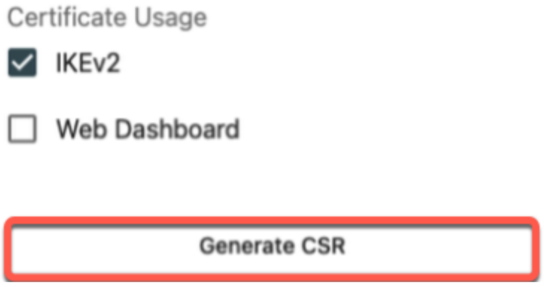
Important Note: This is optional and if you do not have any additional SANs feel free to skip this step


Subject Alternative Name (Optional)
Type: DNS
Value: 192.168.150.xxx

DNS:DemoCN

9 Select "Generate CSR"

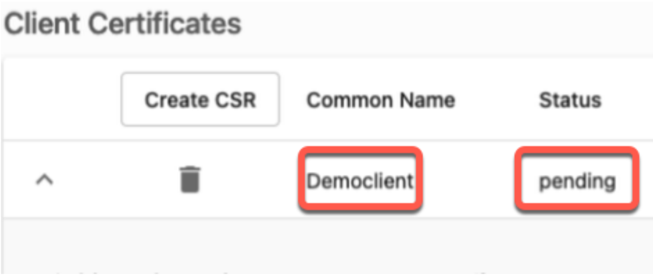
*Select **"Generate CSR"** on the right-hand menu near the bottom of the page. Once this has been selected, your **"Unsigned CSR"** should display, and a success message should appear on the bottom right-hand corner*


Certificate Usage
☑ IKEv2
□ Web Dashboard

Client Certificates: Submitting Unsigned CSR

10 Verify "CSR Upload"

*You should now see the "**Unsigned Certificate**" under the Client Certificates area with the common name that you had typed in earlier steps with a status of "**pending**"*

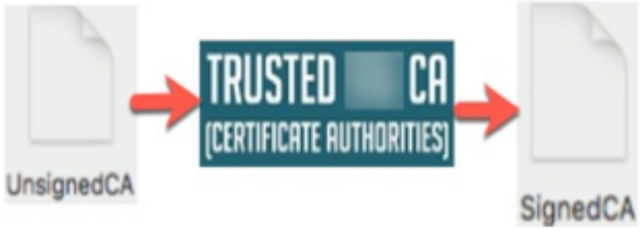


Client Certificates

Create CSR	Common Name	Status
	Democlient	pending

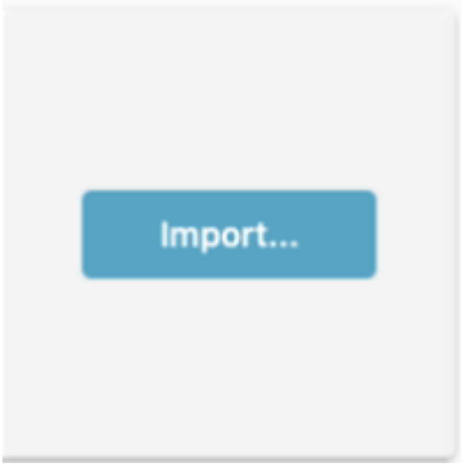
11 Submit "Unsigned CSR" to trusted CA

*At this point you can now select either "**Copy Contents**" and put this information into a text editor or select "**Download Contents**" and send the downloaded file to your personal or companies trusted CA provider to be signed.*



12 Select "Import"

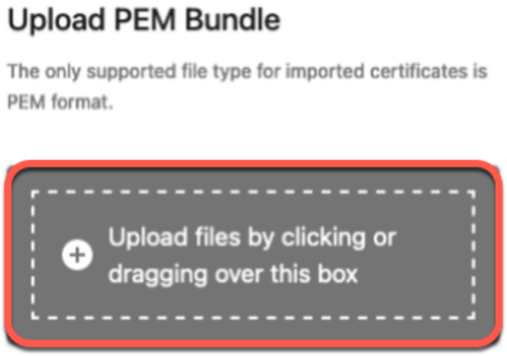
*Once you have received a "**Signed Certificate**" from your trusted CA, please save the file to your PC/MAC. You may now select the "**Import…**" icon near the top right corner of the page to the right of Import bundle*



Client Certificates: Submitting Signed CSR

13 Select “Upload File”

*After selecting the upload icon, a menu should appear on the right-hand side. Select **“Upload files by clicking or dragging over this box”***



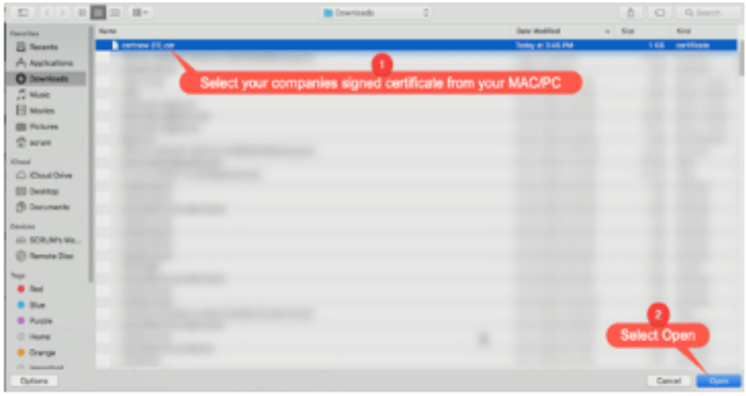
Upload PEM Bundle

The only supported file type for imported certificates is PEM format.

Upload files by clicking or dragging over this box

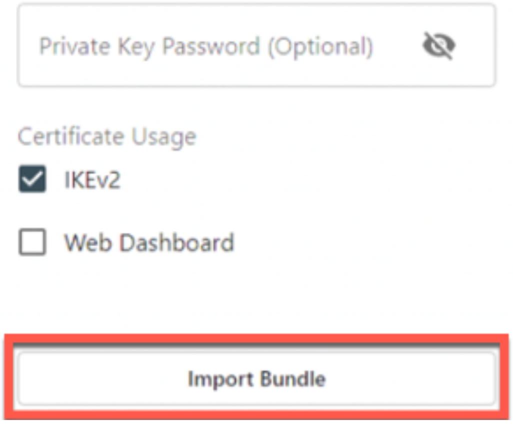
14 Select “Signed Certificate” and “Open”

*Find and select the **“Signed Certificate”** you have received from your Trusted CA provider from the file explorer menu. Then select **“Open”** on the bottom right-hand corner of the file explore menu*



15 Select “Import Bundle”

*Select **“Import Bundle”** on the bottom right-hand corner of the menu. You may have to scroll down depending on your Mac/PCs resolution. You should now receive a success message on the bottom right hand corner*



Private Key Password (Optional)

Certificate Usage

☑ IKEv2

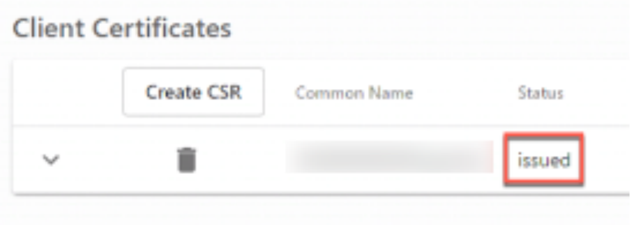
☐ Web Dashboard

Import Bundle

Client Certificates: Verifying Upload

16 Verify Signed Certificate is "Issued"

*After selecting Import… you should now see that the certificate displays "**Issued**" under the status area*



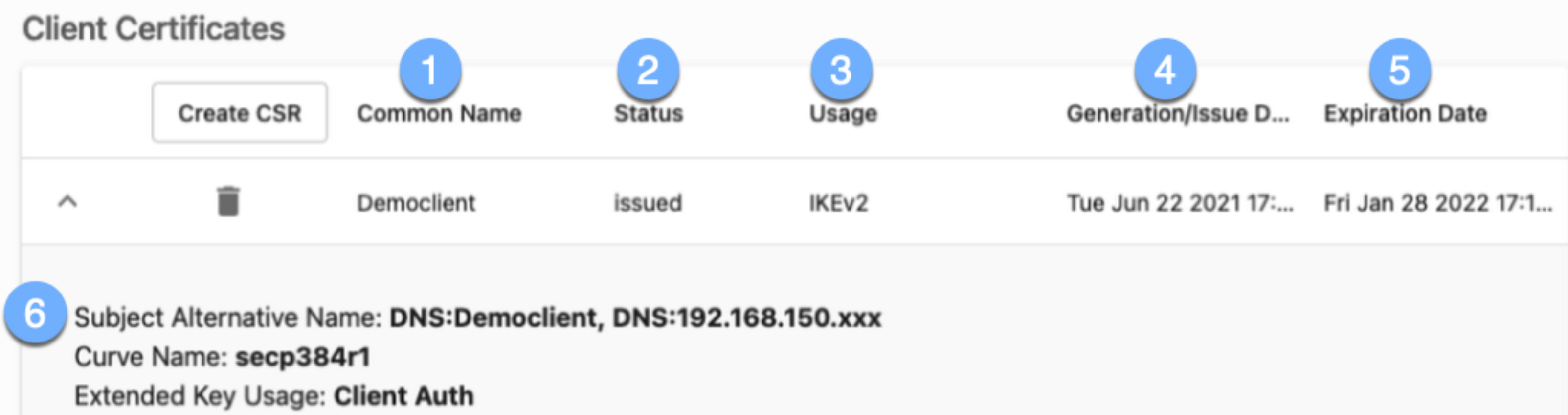
Client Certificates

Create CSR	Common Name	Status
	[redacted]	issued

17 Verify all uploaded info

Once the client has been issued verify the certificate displays all the correct information

1.) **Common Name:** This should match the exact username you have on your GoSilent Server
2.) **Status:** This should now display "Issued"
3.) **Usage:** This should either display IKEv2 or Web Dashboard depending on your selection
4.) **Generation/Issue Date:** This should display the date and time the certificate was generated
5.) **Expiration Date:** This will display the date that the certificate is set to expire
6.) **Subject Alternative Name (with all SANs entered):** This should display any SANs you have entered



Client Certificates

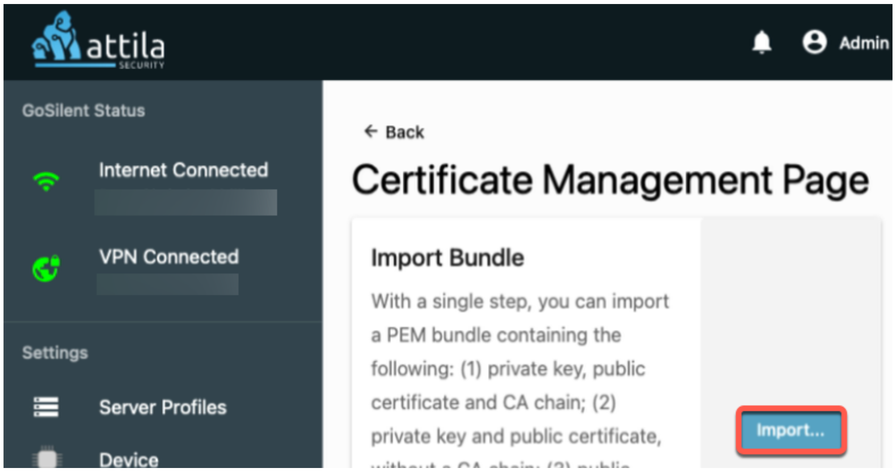
Create CSR	1 Common Name	2 Status	3 Usage	4 Generation/Issue D...	5 Expiration Date
	Democlient	issued	IKEv2	Tue Jun 22 2021 17:...	Fri Jan 28 2022 17:1...

6 Subject Alternative Name: **DNS:Democlient, DNS:192.168.150.xxx**
Curve Name: **secp384r1**
Extended Key Usage: **Client Auth**

CA Certificates: Uploading Signed CA Chain

18 Select “Import”

Select ***“Import…”*** *near the top right-hand corner of the page on the right-hand side of “Import Bundle”*



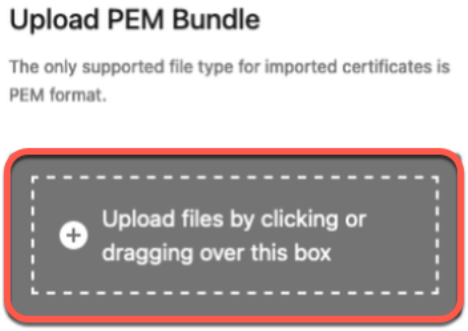
Certificate Management Page

Import Bundle

With a single step, you can import a PEM bundle containing the following: (1) private key, public certificate and CA chain; (2) private key and public certificate, without a CA chain; (3) public

19 Select “Upload files”

After selecting Import… a menu should appear on the right-hand side of the screen. Select ***“Upload files by clicking or dragging over this box”***

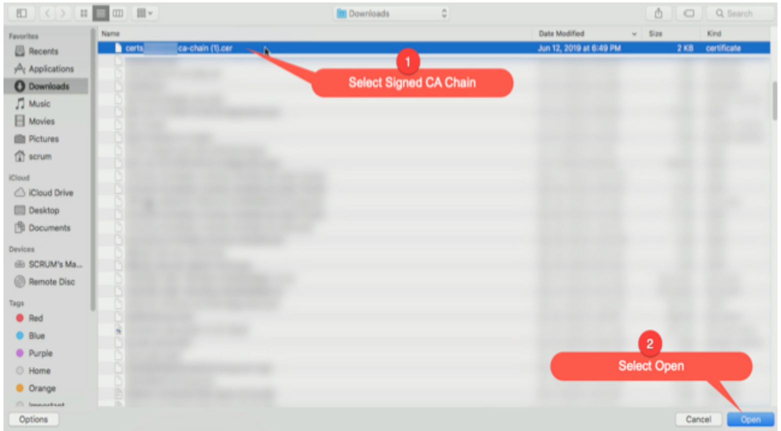


Upload PEM Bundle

The only supported file type for imported certificates is PEM format.

20 Select the “Signed CA Chain”

Find and select the ***“Signed CA Certificate Chain”*** *you have received from your Trusted CA provider from the file explorer menu. Then select* ***“Open”*** *on the bottom right-hand corner of the file explorer menu. Select* ***“Import Bundle”*** *on the bottom right-hand corner of the menu*



Name	Date Modified	Size	Kind
certs[redacted]ca-chain (1).cer	Jun 12, 2019 at 6:49 PM	2 KB	certificate

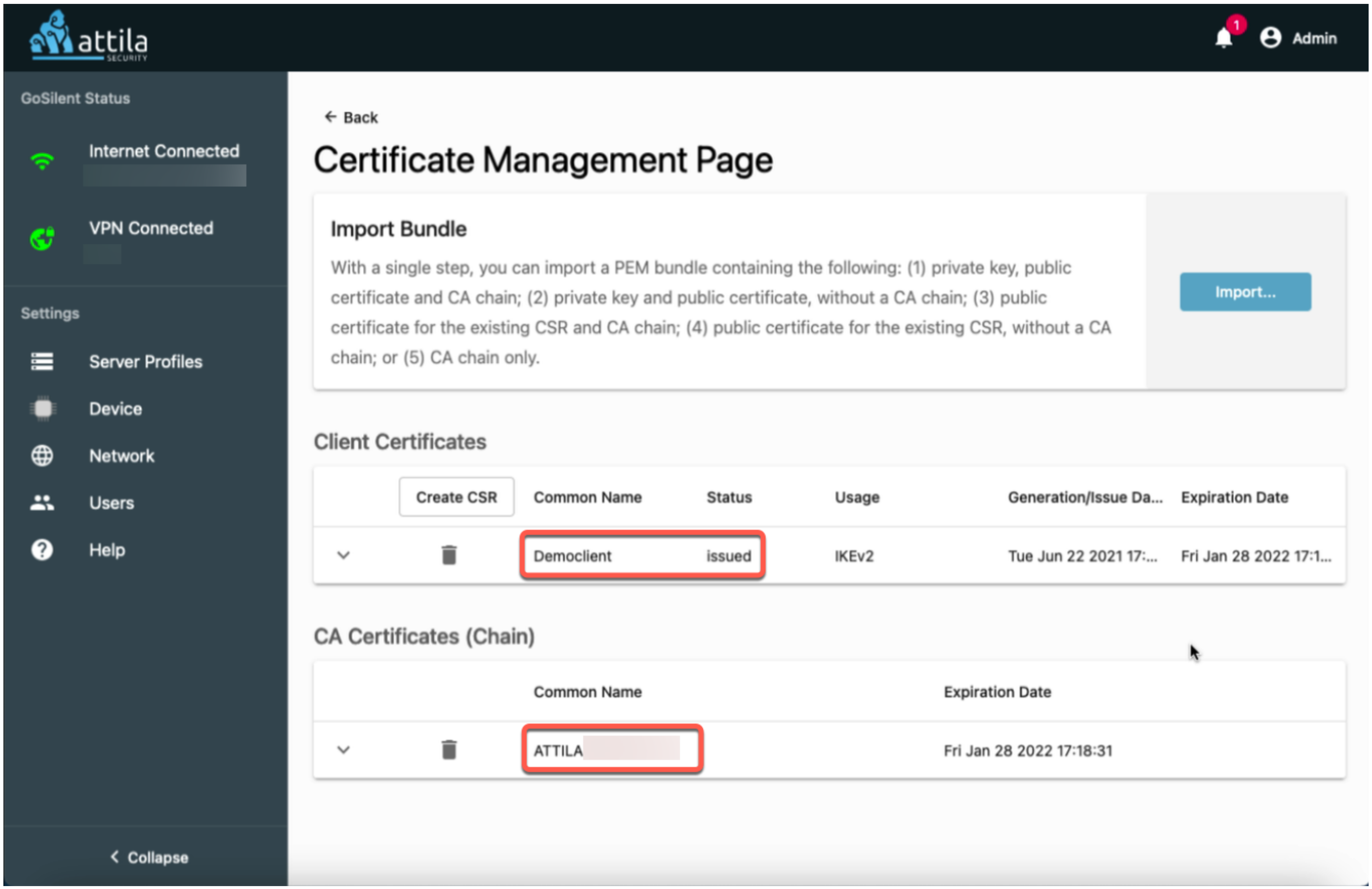
Certificates: Verifying Certificates

21 Verify CA Chain Upload

*After uploading the **"CA Chain"** you should now see the CA chain information below the CA Certificate (Chain) area with the **"Common Name"** and **"Expiration date"**. It's at this point you have now completed the IKEv2 server process. If everything was uploaded correctly you should see*

1.) *"**Server Certificate**" with a status of "**issued**" with the correct "**Common Name**"*

2.) *"**CA Certificate (Chain)**" with the correct "**CA Certificate**" info*



Internet Connected
[redacted]

VPN Connected
[redacted]

Certificate Management Page

Import Bundle

With a single step, you can import a PEM bundle containing the following: (1) private key, public certificate and CA chain; (2) private key and public certificate, without a CA chain; (3) public certificate for the existing CSR and CA chain; (4) public certificate for the existing CSR, without a CA chain; or (5) CA chain only.

Client Certificates

	Create CSR	Common Name	Status	Usage	Generation/Issue Da...	Expiration Date
⌄	🗑	Democlient	issued	IKEv2	Tue Jun 22 2021 17:...	Fri Jan 28 2022 17:1...

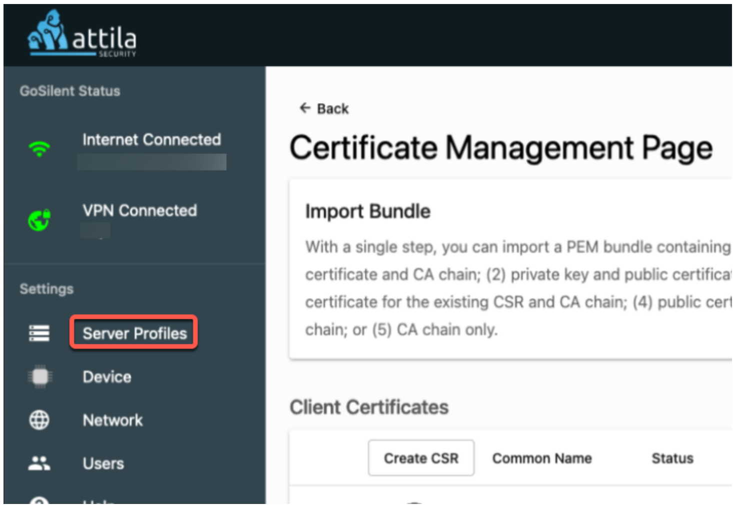
CA Certificates (Chain)

		Common Name	Expiration Date
⌄	🗑	ATTILA [redacted]	Fri Jan 28 2022 17:18:31

VPN Server Profile: Navigation / Protocol

22 Select "Server Profiles" tab

*Select the **"Server Profiles"** page which can be found on the left menu below the GoSilent Status. If your menu is collapsed simply select the 3 server's icon*


attila SECURITY

GoSilent Status

Internet Connected
[redacted]

VPN Connected
[redacted]

Settings

Server Profiles

Device

Network

Users

← Back

Certificate Management Page

Import Bundle

With a single step, you can import a PEM bundle containing
certificate and CA chain; (2) private key and public certifica
certificate for the existing CSR and CA chain; (4) public cert
chain; or (5) CA chain only.

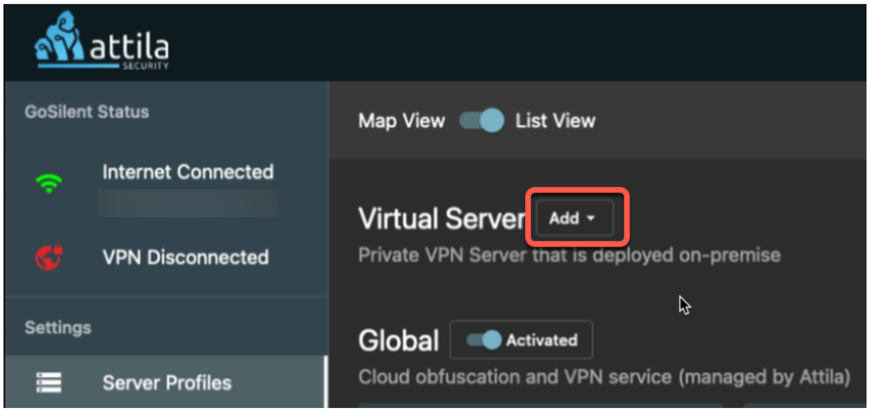
Client Certificates

Create CSR | Common Name | Status

23 Select "Add" on Virtual Server

*Select **"Add"** on the right-hand side of "**Virtual Server**".*

*Then select "**+ New Virtual Server**" on the drop-down menu*


attila SECURITY

GoSilent Status

Internet Connected
[redacted]

VPN Disconnected

Settings

Server Profiles

Map View | List View

Virtual Server | Add ▾

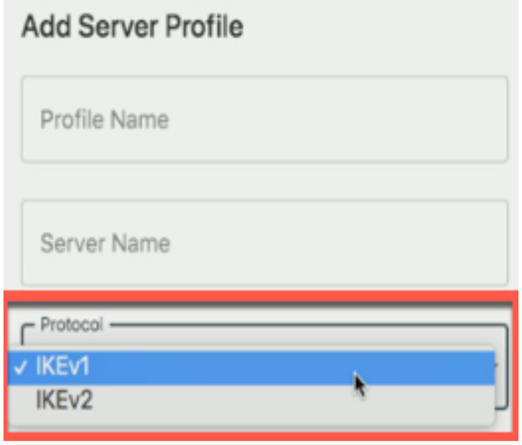
Private VPN Server that is deployed on-premise

Global | Activated

Cloud obfuscation and VPN service (managed by Attila)

24 Change "Protocol" to IKEv2

*On the right-hand menu select the drop-down menu for the "**Protocol**" field select **"IKEv1"** and change it to **"IKEv2"***


Add Server Profile

Profile Name

Server Name

Protocol

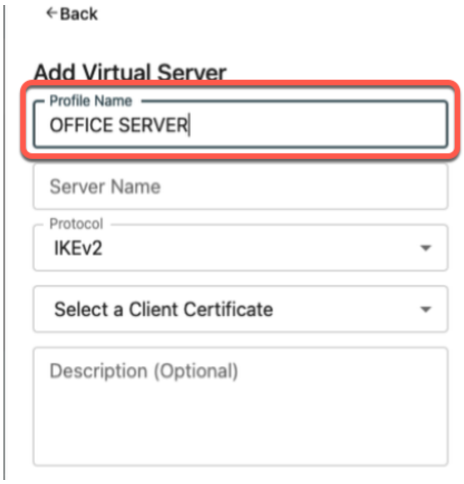
✓ IKEv1

IKEv2

VPN Server Profile: Profile Name / Server Name

25 Input “Profile Name”

*Within the **“Profile Name”** field, enter a name that you will remember. For example (Office Server) or (Home Office Server). This is the name that will display for your server profile going forward.*

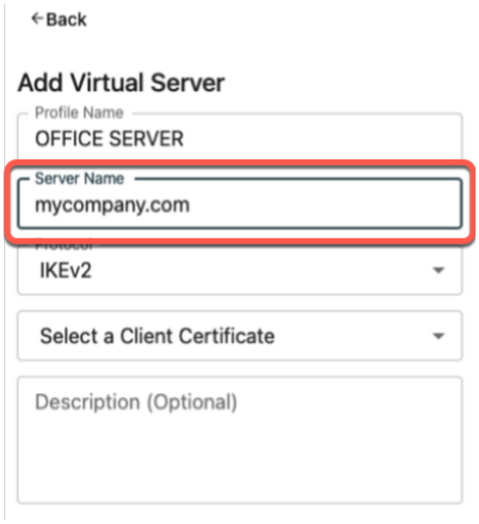


Profile Name: OFFICE SERVER

Protocol: IKEv2

26 Input “Server Name”

*Select the **“Server Name”** field below Profile Name. Type in the “Server Name” that should match the “VPN server ID (or CN)” in the server’s VPN settings. So, if the “VPN server ID (or CN)” contains a domain name (e.g. mycompany.com), then the “Server Name” should be identical. Alternativity, if the “VPN server ID (or CN)” contains an IP address, then the “Server Name” should be identical.*



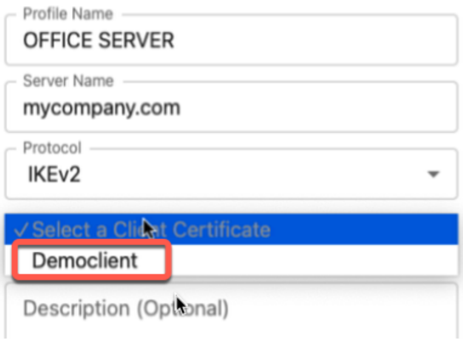
Profile Name: OFFICE SERVER

Server Name: mycompany.com

IKEv2

27 Select “Client Certificate”

*Select “**Select a Client Certificate**”and find the common name (CN) you uploaded earlier from the drop-down menu. This should automatically appear in the list.*



Profile Name: OFFICE SERVER

Server Name: mycompany.com

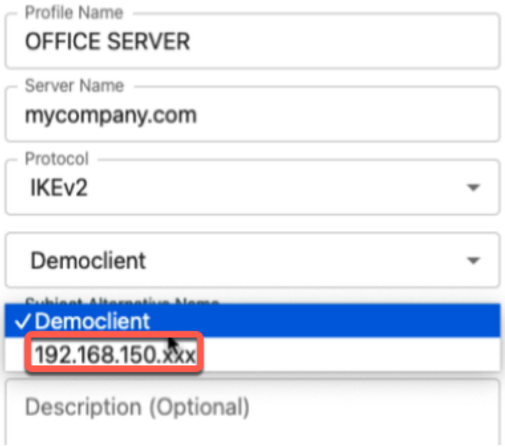
Protocol: IKEv2

VPN Server Profile: SAN / Adding Virtual Server

28 Select "Subject Alternative Name"

*[OPTIONAL]: Below the Client Certificate field, you will see **"Subject Alternative Name"** here you can select the additional SAN you created earlier.*

Important Note: This is optional and if you do not have any additional SANs feel free to skip this step



Profile Name: OFFICE SERVER

Server Name: mycompany.com

Protocol: IKEv2

Democlient

✓ Democlient

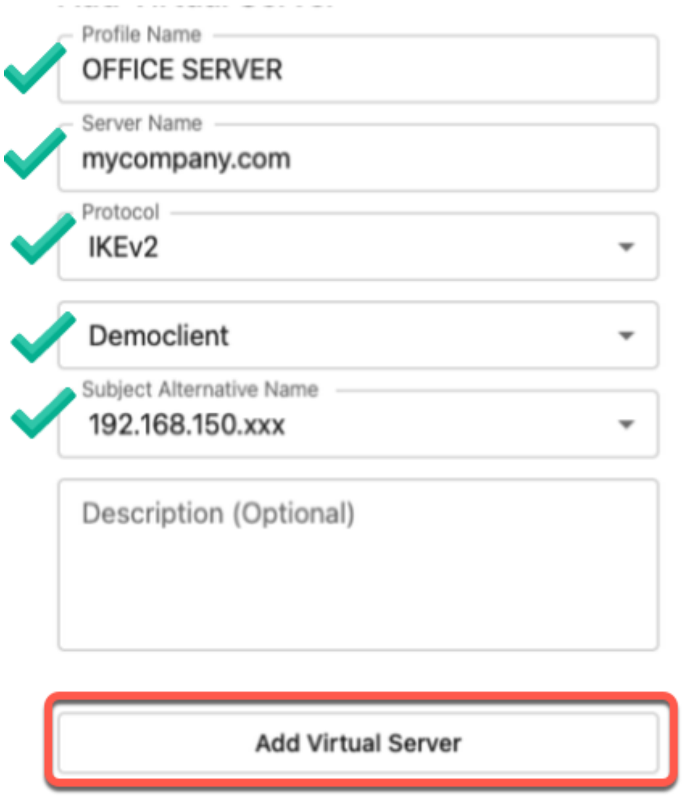
192.168.150.xxx

29 Select "Add Virtual Server"

*Verify you have all the following information and select "**Add Virtual Server**"*

1. *Profile Name*
2. *Server Name*
3. *Protocol*
4. *Client Certificate*
5. *[OPTIONAL] Subject Alternative Name (SAN)*

Special Note: You may have to scroll down depending on your MAC/PCs screen resolution to view "Add Virtual Server"



✓ Profile Name: OFFICE SERVER

✓ Server Name: mycompany.com

✓ Protocol: IKEv2

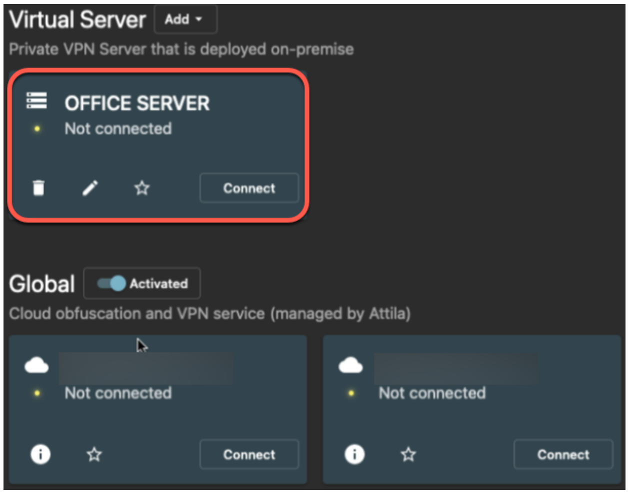
✓ Democlient

✓ Subject Alternative Name: 192.168.150.xxx

VPN Server Profile: Verifying Upload / Connecting

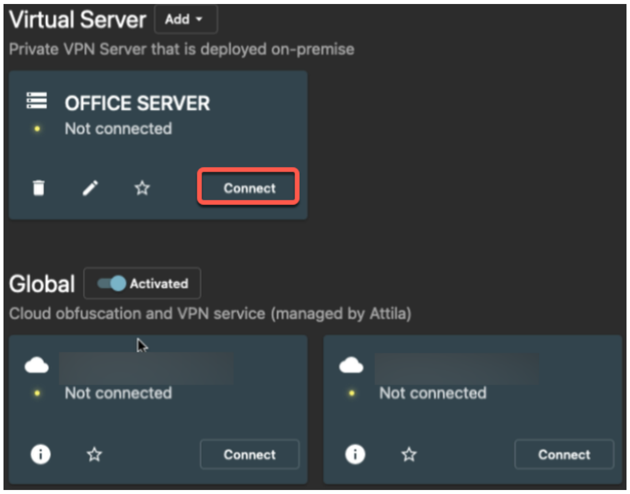
30 Verify Server Upload

*Once you have entered your office server information it should appear under the "**Virtual Server**" list area*


Virtual Server
Private VPN Server that is deployed on-premise
OFFICE SERVER
Not connected
Global Activated
Cloud obfuscation and VPN service (managed by Attila)
Not connected
Not connected

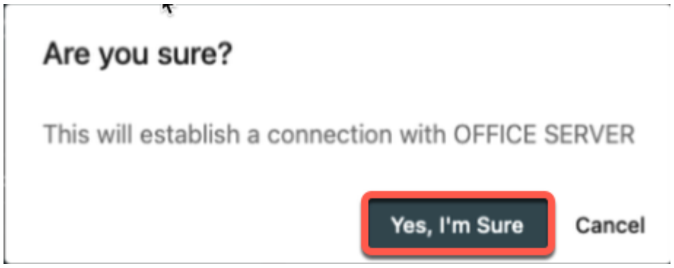
31 Select "Connect"

*Select the "**Connect**" on the server that was created. This can be located below the server name on the right-hand side of the star icon*


Virtual Server
Private VPN Server that is deployed on-premise
OFFICE SERVER
Not connected
Global Activated
Cloud obfuscation and VPN service (managed by Attila)
Not connected
Not connected

32 Select "Yes, I'm Sure"

*Once you have selected Connect you should then receive a pop-up asking if you are sure you want to disconnect from your currently connected server and connect with your newly created server. Select "**Yes, I'm Sure**"*


Are you sure?

This will establish a connection with OFFICE SERVER

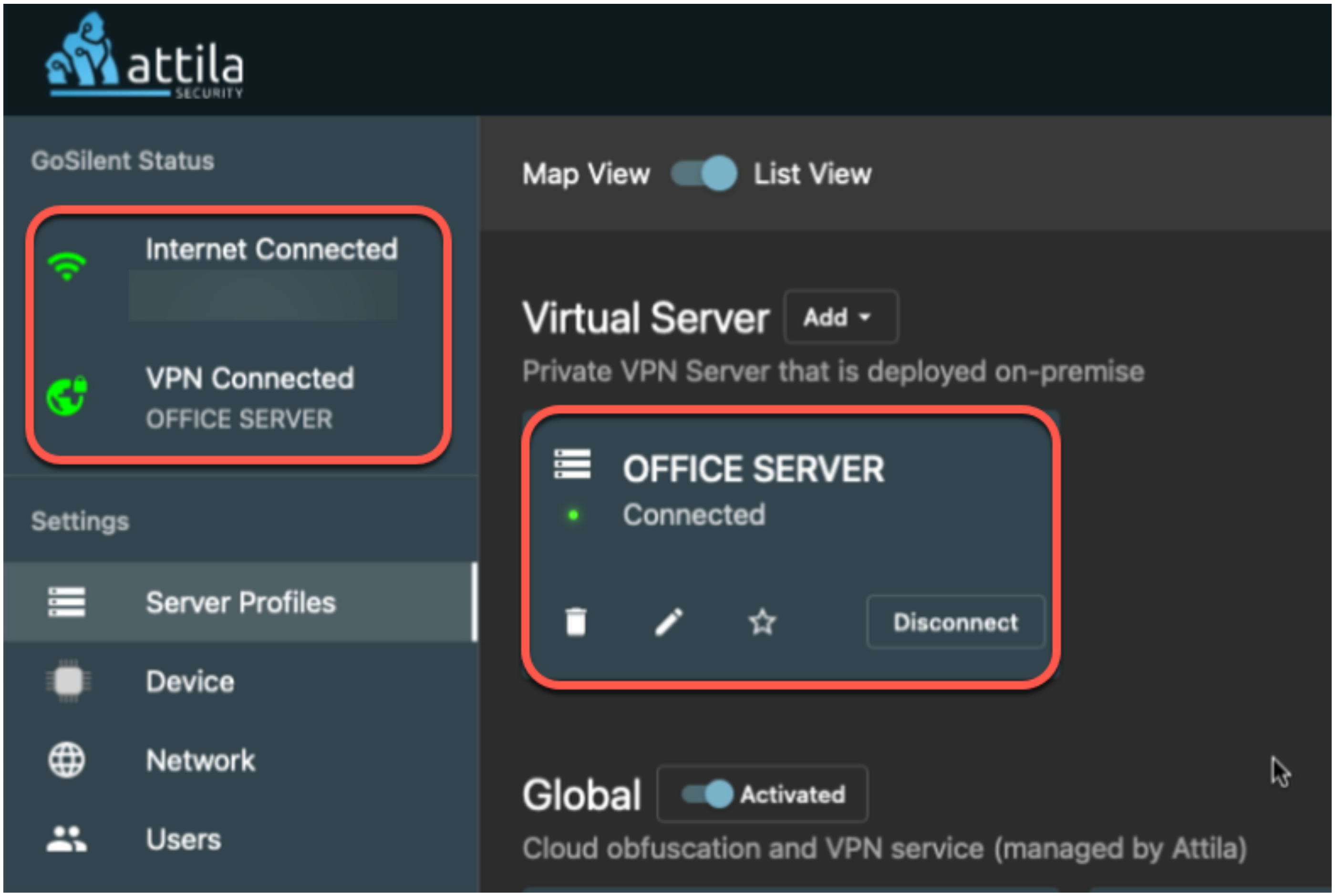
Important Note: New connections to a server can take 30 to 90 seconds to fully connect.

VPN Server Profile: Verifying Server Connection

33 Verify Server Connection

*Once connected correctly you should see the Office Server information on the left-hand side under **"VPN Connected"** and the status of **"Connected"** in green on the server itself. This indicates that you are now fully connected to your office server via an IKEv2 connection. This process is now complete. If you are having any problems connecting, please feel free to contact our customer support team at https://attilasec.zendesk.com who will be glad to assist you.*

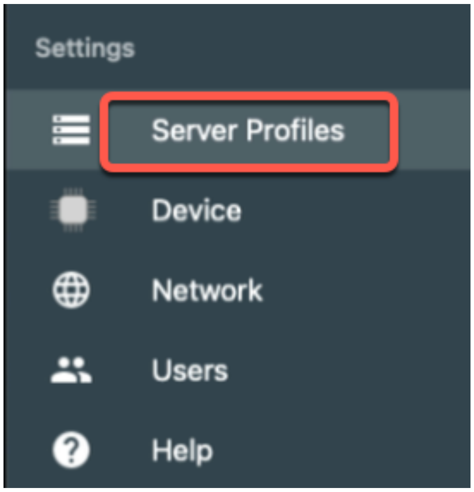
Import Note: If you would like for your GoSilent cube to automatically try to connect to this in the future, please continue to go through the "Setting Default Server Profile" instructions below. This is a process we recommend following so you will not have to manually connect anytime you power on or restart your GoSilent cube.



Setting Default Server Profile: Navigation

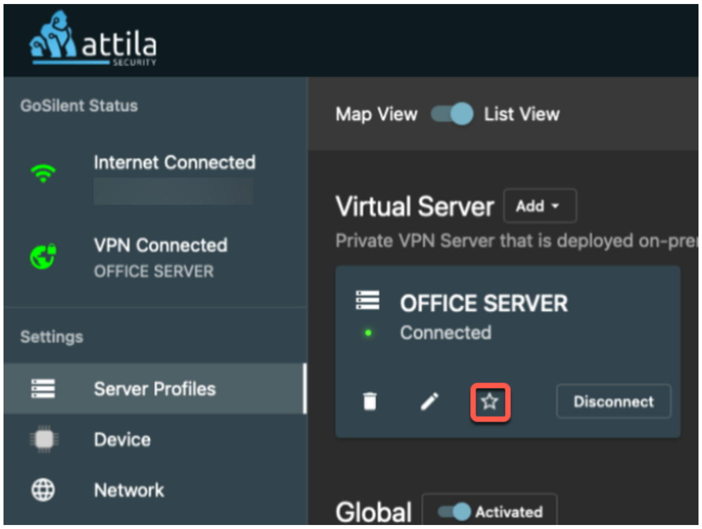
34 Select “Server Profiles”

*Select the “**Server Profiles**” page which can be found on the left menu below GoSilent status. If your menu is collapsed simply select the icon displaying 3 server icons*



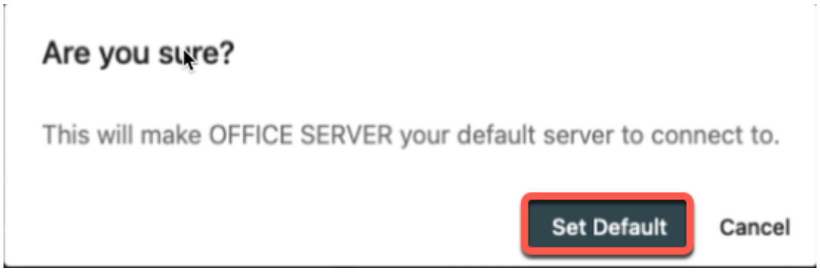
35 Select “Star Icon”

*Select the “**Star**” icon on the left-hand side of the disconnect button under the desired server profile*



36 Select “Set Default”

*Once you have selected the star icon, you should then receive a pop-up asking if you are sure you want to set the server as default. Select “**Set Default**”*



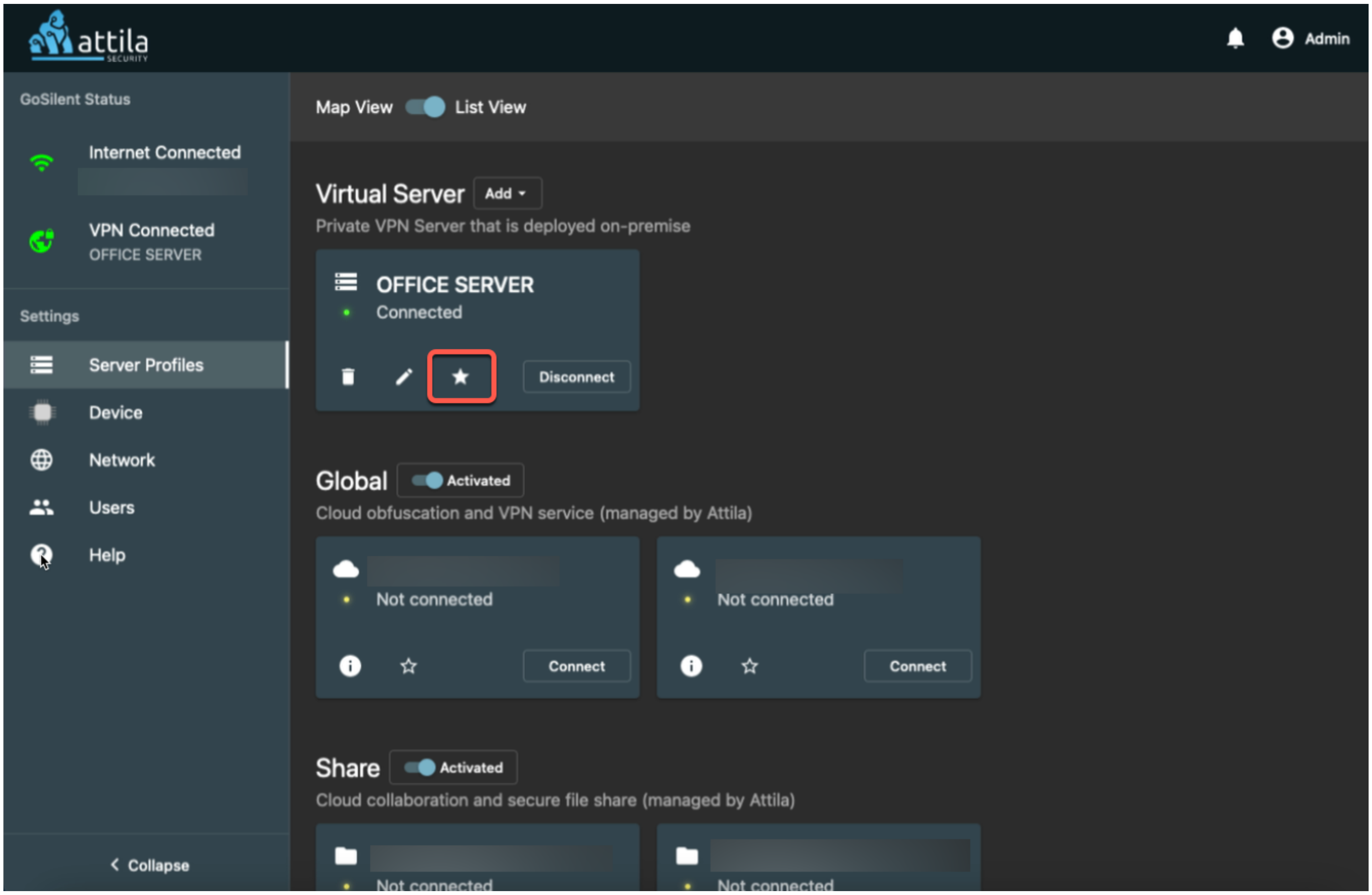
Are you sure?

This will make OFFICE SERVER your default server to connect to.

Setting Default Server Profile: Verifying Default

37 Verify Default Setting

The star icon (Default) will now display in a solid grey/white color. This indicates this is now your default server and anytime you power on or establish a new internet connect your GoSilent cube will try connecting to the default server automatically. The GoSilent cube must be able to automatically connect to a known Wi-Fi network or an ethernet network



Support: Questions / Problems

Congratulations on completing the setup using an IKEv2 connection. If you should have any problems, questions, or concerns please feel free to contact our customer support team at https://attilasec.zendesk.com who will be glad to assist you and we thank you for your business with Attila Security!

Contact Us

Support Email:

Support@attilaSec.Zendesk.com

Submit Issue:
Https://attilasec.zendesk.com/hc/en-us/requests/new

Company Address:
10960 Grandchester Way, Suite 530, Columbia MD 21044