Server Setup Guide for IKEv2 Connection

GSS Version 21.03.0 | Date: July 14, 2021

IKEv2 Overview

The GoSilent Server (GSS) supports the use of two IKE protocols. IKEv1 with pre-shared keys (PSK's) and IKEv2 with certificates. Only one IKE protocol can be configured and used on a given server. Changing the IKE protocol requires a server restart. A GSS server is configured to use the IKEv1 protocol with PSKs by default. There are a number of steps to follow when converting a GSS server to use the IKEv2 protocol with certificates, including a server restart. Those steps are described in the remainder of this document.

Table of Contents

Changing System Settings

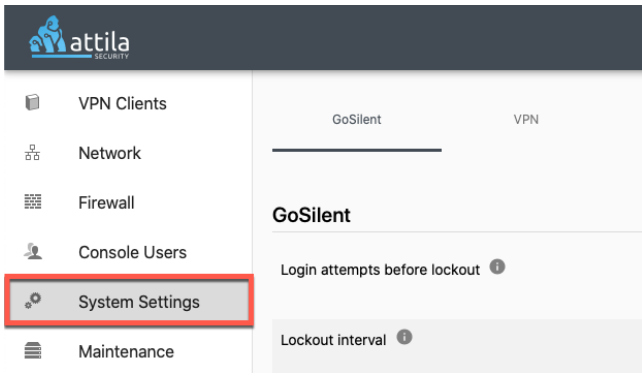
1. Log into the "Server Admin Console"

- Log into the "**Server Admin Console**" your administrator or IT professional has provided.

Please note if you do not have this login to contact our customer support team at https://attilasec.zendesk.com who will be glad to assist you.

2. Select "System Settings"

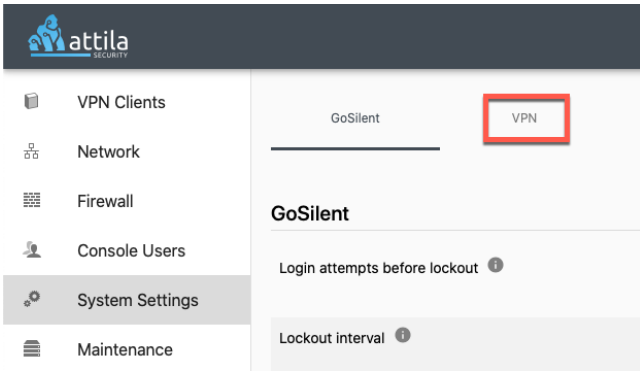
- The "**System Settings**" can be found on the left menu below Console Users and above Maintenance. If your menu is collapsed simply select the icon showing two gears.



3. Select "VPN"

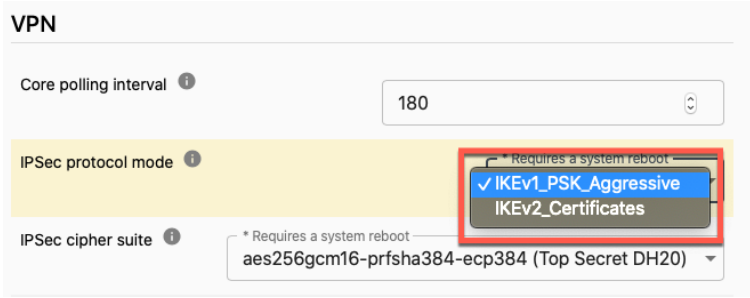
- Select "**VPN**" or "**VPN Server**" depending on your server version. This can be located in the middle of the page on the right-hand side of GoSilent.

Please note some settings if updated and saved will require a server restart for the changes to be applied.



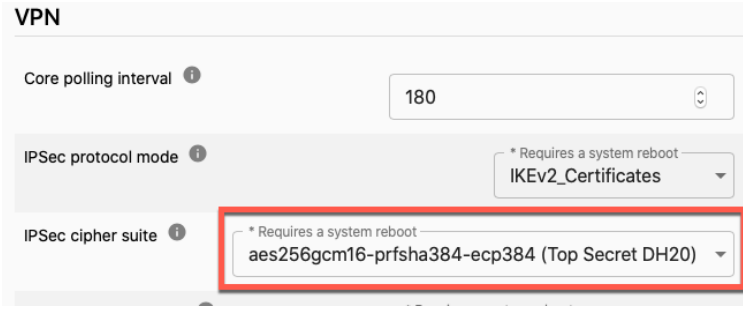
4. Change “IPSec protocol mode”

- On the right-hand side of “**IPSec protocol mode**” select the drop-down menu from the “**IKEv1_PSK_Aggresive**” and change it to “**IKEv2_Certificates** “.



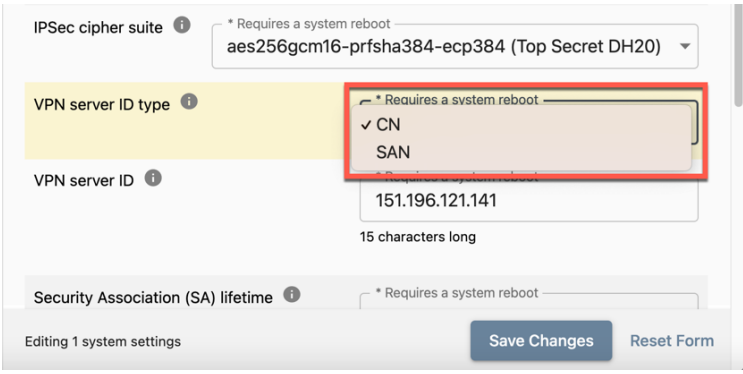
5. [OPTIONAL] Change or verify “IPSec cipher suite”

- The default for “**IPSec cipher suite**” is “**Top Secret DH20**” however we do have a total of 12 IPsec cipher suites to choose from. Feel free to either change this setting or leave it as the defaulted “**Top Secret DH20**”.



6. [OPTIONAL] Change “VPN server ID type”

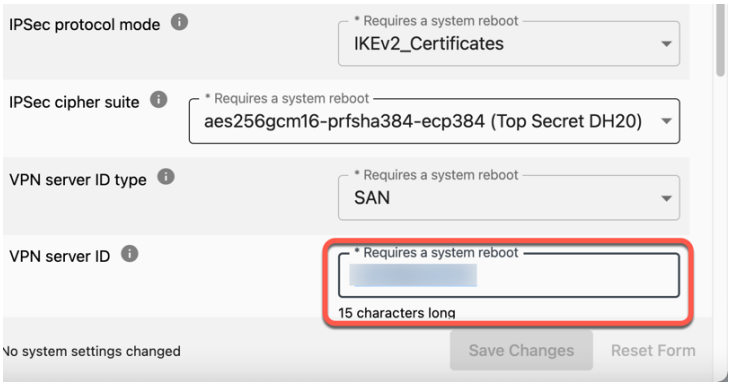
- You can now select if you would like to update your “**VPN server ID type**”. Here you have the options of either “**CN**” (Common Name) or “**SAN**” (Subject Alternative Name).



7. Input “VPN Server ID”

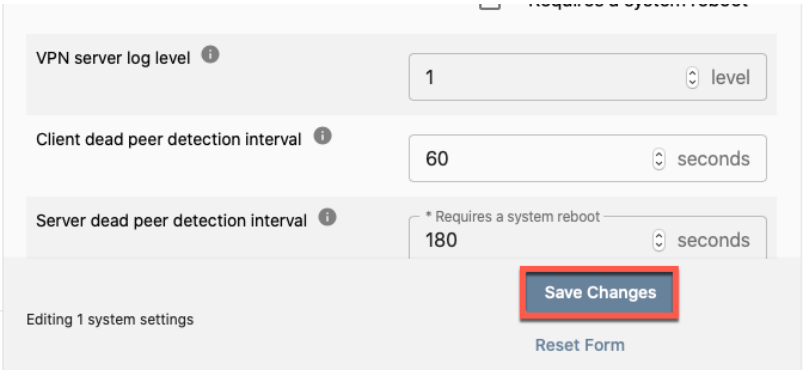
- The “**VPN Server ID**” is right below VPN Server ID type. Update the text from “**tcp**” to the host name of your server.

Please note: The “VPN Server ID (or CN)” should match the Common Name (CN) in Step 15 of your CSR



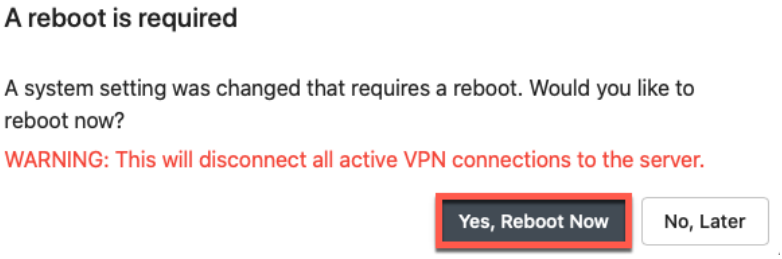
8. Select “Save Changes”

- After making all the above necessary changes you can now select “**Save Changes**” which is located near the bottom of the page and may require you to scroll down depending on our MAC/PCs resolution.



9. Select “Yes, Reboot Now”

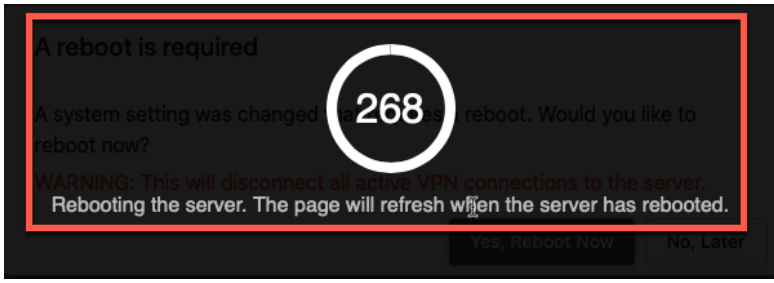
- Select **“Yes, Reboot Now”** when the pop up appears. Please note this will disconnect any active VPN connections your company may have while it’s rebooting.



10. Wait for Server to fully reboot

- The **"Rebooting Server Countdown"** will begin.

Please note the page will automatically refresh once this process is complete and the server has fully rebooted. This process can take up to 2 minutes to complete.



Adding Server Certificates

Items Needed

Before starting this process, you must identify a Certificate Authority (CA) that can be used to sign Certificate Signing Request (CSR). This CA may be a trusted third-party CA or may be an internal CA that is hosted on-premise by your company.

Please note: There are currently two ways to upload server certificates.

- Method 1: Create a CSR within the GoSilent interface and then have your Certificate Authority sign it with their own CA and upload a CA Chain. If your using Method 1 then please continue to step 11.

- Method 2: Upload a Full PEM Bundle that is created by your Certificate Authority which contains a private key, signed certificate, and a CA Chain in one file. If you are using Method 2 you may continue to step 13 and then skip to step 28.

Certificate Requirements

CN without SAN

Gosilent servers **prior to the 21.03** release must use this method.
Gosilent servers **21.03 and later** release may use this method though it is optional

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

- The **Subject** field must contain **only** a Common Name (CN) attribute, which is set to the **VPN server ID** value that matches the one on your **VPN Server ID within the system settings**.
  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 example:
  X509v3 Basic Constraints: critical
  CA: False

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

  Here is example:
  X509v3 Extended Key Usage:
  TLS Web Server Authentication

CN with SAN

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

If you are creating a GoSilent server IKEv2 certificate with SAN, following 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 **IP address** or **DNS Name** that matches the one on within the system settings within the VPN tab

- The certificate **must** be an **end-entity/leaf** certificate, it **cannot** be 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 **server authentication**

  Here is an example:
  X509v3 Extended Key Usage:
  TLS Web Server Authentication

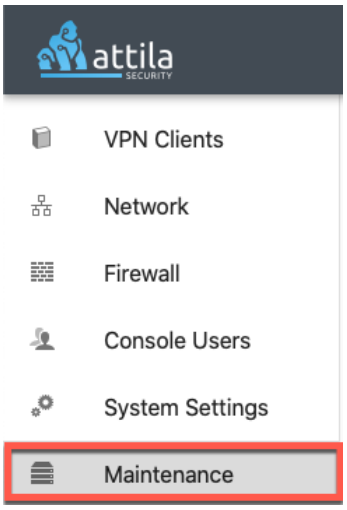
Create CSR and Import Signed Certificate

11. Log into the "Server Admin Console"

- Log into the "**Server Admin Console**" your administrator or IT professional has provided.

Please note if you do not have this login to contact our customer support team at https://attilasec.zendesk.com who will be glad to assist you.

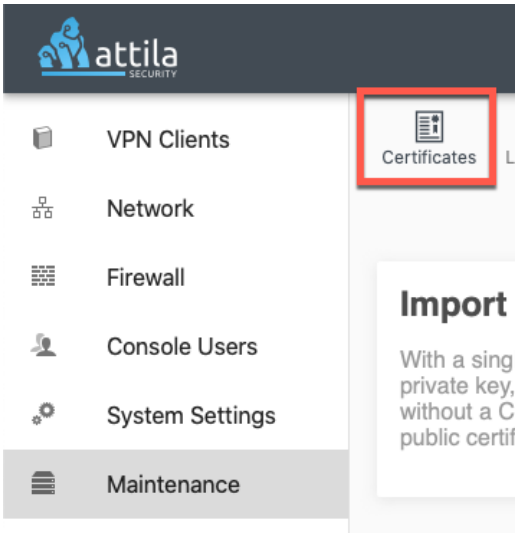
12. Select "Maintenance"



- The "**Maintenance**" page can be found on the left-hand menu below system settings. If your menu is collapsed simply select the icon showing 3 server icons.

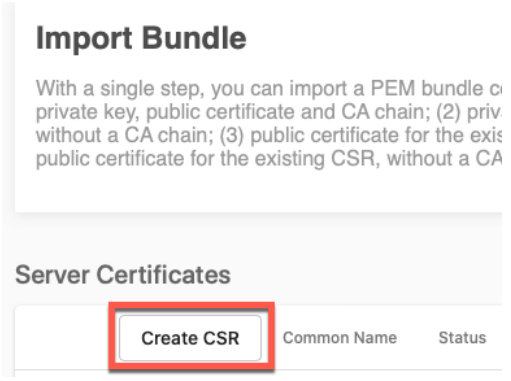
13. Select “Certificates”

- Select the “**Certificates**” tab near the top of the page above Import Bundle.



14. Select “Create CSR”

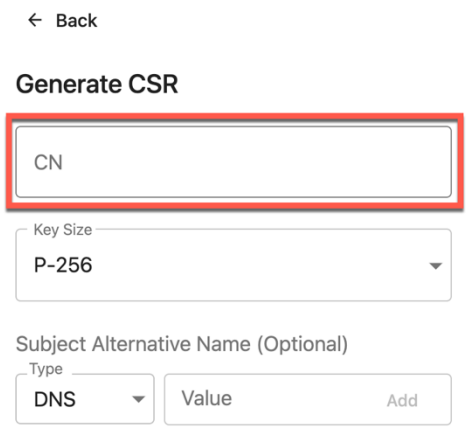
- Select “**Create CSR**” near the top of the page right below Server Certificates. This will display a pop-up drawer on the right-hand side of the screen containing a few fields.



15. Input Common Name “CN”

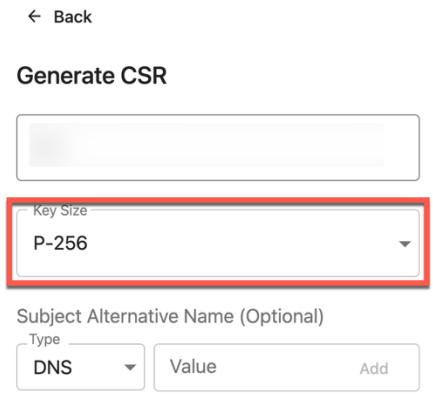
Please note: The “VPN server ID (or CN) from Step 7 must match what is entered into the Common Name (CN) field

- For the “**CN**” or Common Name field, please type in the same “VPN server ID (or CN)” you entered earlier in step 7684.



16. Select “Key Size”

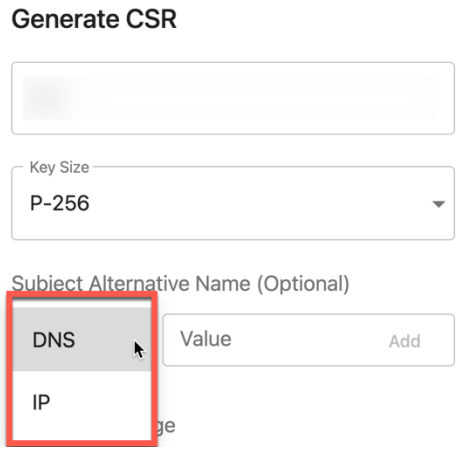
- Select the “**Key Size**” on the right-hand menu. Select either P-256 or P-384 depending on the bit length of the key you prefer.



17. [OPTIONAL]: Select Subject Alternative Name (SAN) Type

- As an additional option you can also input a Subject Alternative Name or (SAN). Select either “**DNS**” or “**IP**” on the drop-down menu.

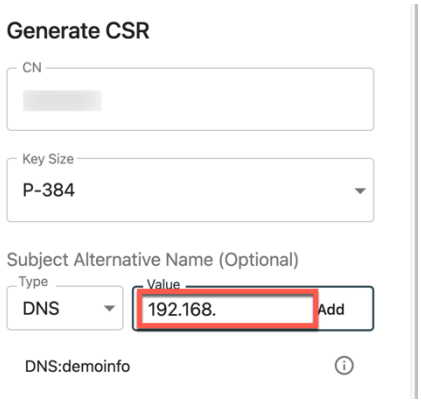
  Import Note: This is optional and if you do not have any additional SANs feel free to skip this step



18. [OPTIONAL]: Input “Subject Alternative Name” (SAN)

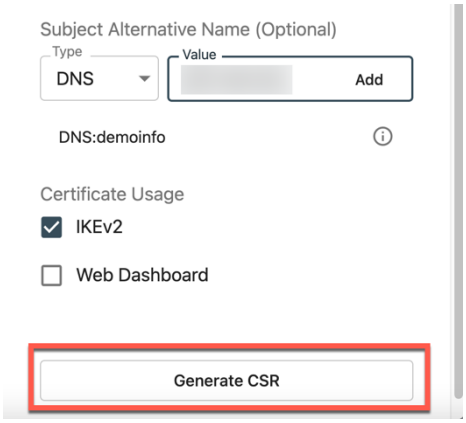
- You can now type in the “**DNS**” or “**IP**” address you would like to use for the “**Subject Alternative Name**” (SAN). After typing in select “Add” on the right-hand side of the SAN value information.

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



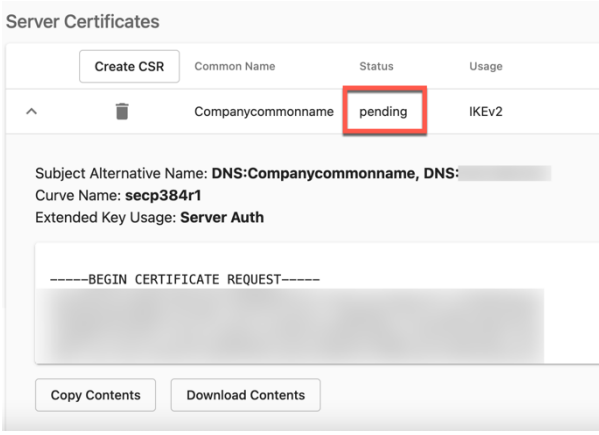
19. Select “Generate CSR”

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



20. Verify “CSR Upload”

- You should now see the “**Unsigned Certificate**” under the Server Certificates area with the common name that you had typed in earlier steps along with the optional SAN with a status of “**pending**”

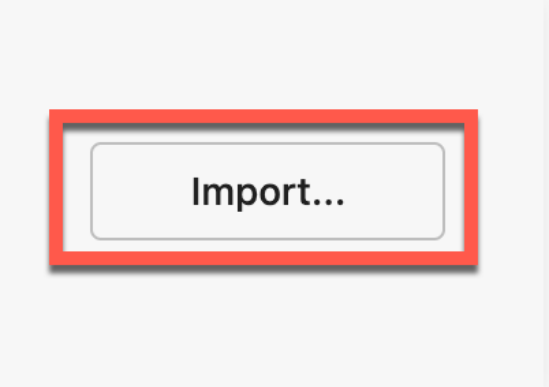


21. Submit “Unsigned CSR” to trusted CA

- 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 trusted CA to be signed.

22. Select “Import”

- Once you have received a “**Signed Certificate**” from your trusted CA, please save the file to your PC/MAC. Select “**Import…**” near the top right right-hand corner of the page on the right-hand side of “Import Bundle”.

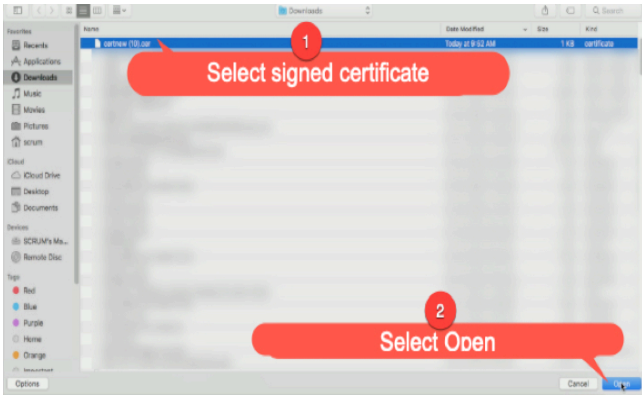


23. Select “Upload Files”

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

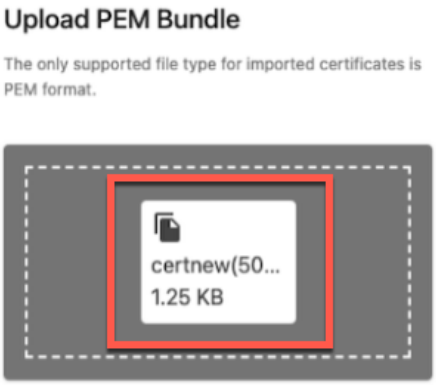
24. Select Signed Certificate and Open

- 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.



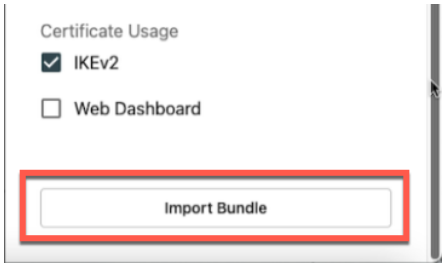
25. Verify Selected File

- You should now be able to the see the "**Signed Certificate**" file under the Upload Certificate area on the right-hand menu. You can verify it is the correct file you uploaded by the name.



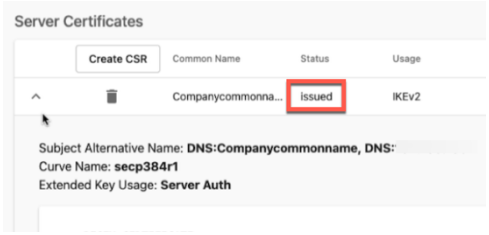
26. Select "Import Bundle"

- 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 if the certificate was successfully uploaded.



27. Verify Signed Certificate is "issued"

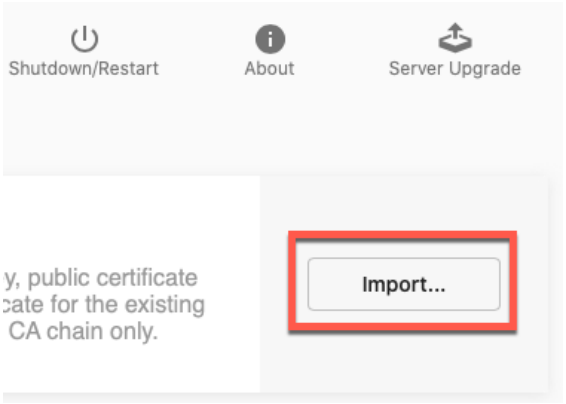
- Once you have uploaded your signed certificate you should now see "**issued**" in the middle of the page under the status area indicating that the signed certificate has been issued correctly.



Import Signed CA Chain or Full PEM Bundle

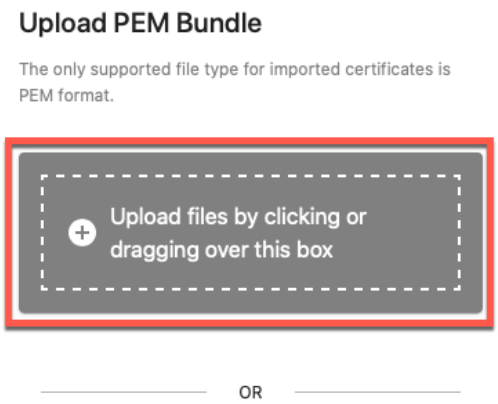
28. Select "Import"

- Select "**Import…**" near the top right-hand corner of the page on the right-hand side of "Import Bundle" to begin the process of importing a "**Signed CA Chain**" or "**Full PEM Bundle**".



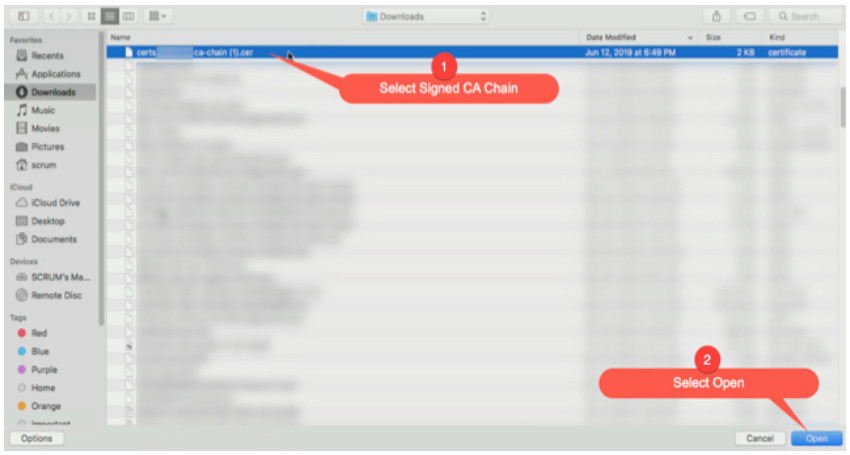
29. Select "Upload Files"

- 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**".



30. Select the "Signed CA Chain"

- Find and select the "**Signed CA Chain**" or "**Full PEM bundle**" 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.

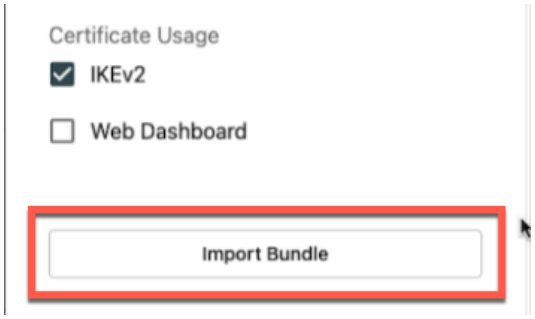


31. Verify Selected File

- You should now be able to see the "**Signed CA Chain**" or "**Full PEM Bundle**" file under the "Upload PEM Bundle" area on the right-hand menu. You can verify it is the correct file you uploaded by the name.

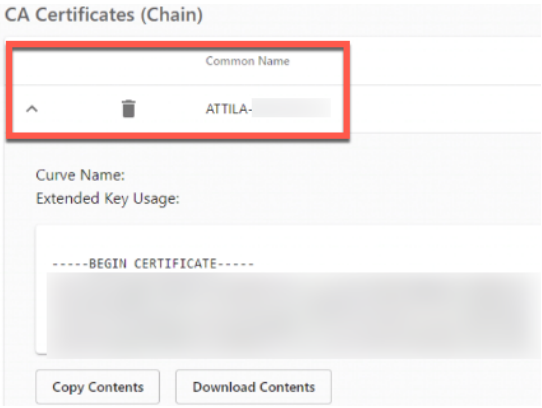
32. Select "Import Bundle"

- 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 if the file was successfully uploaded.



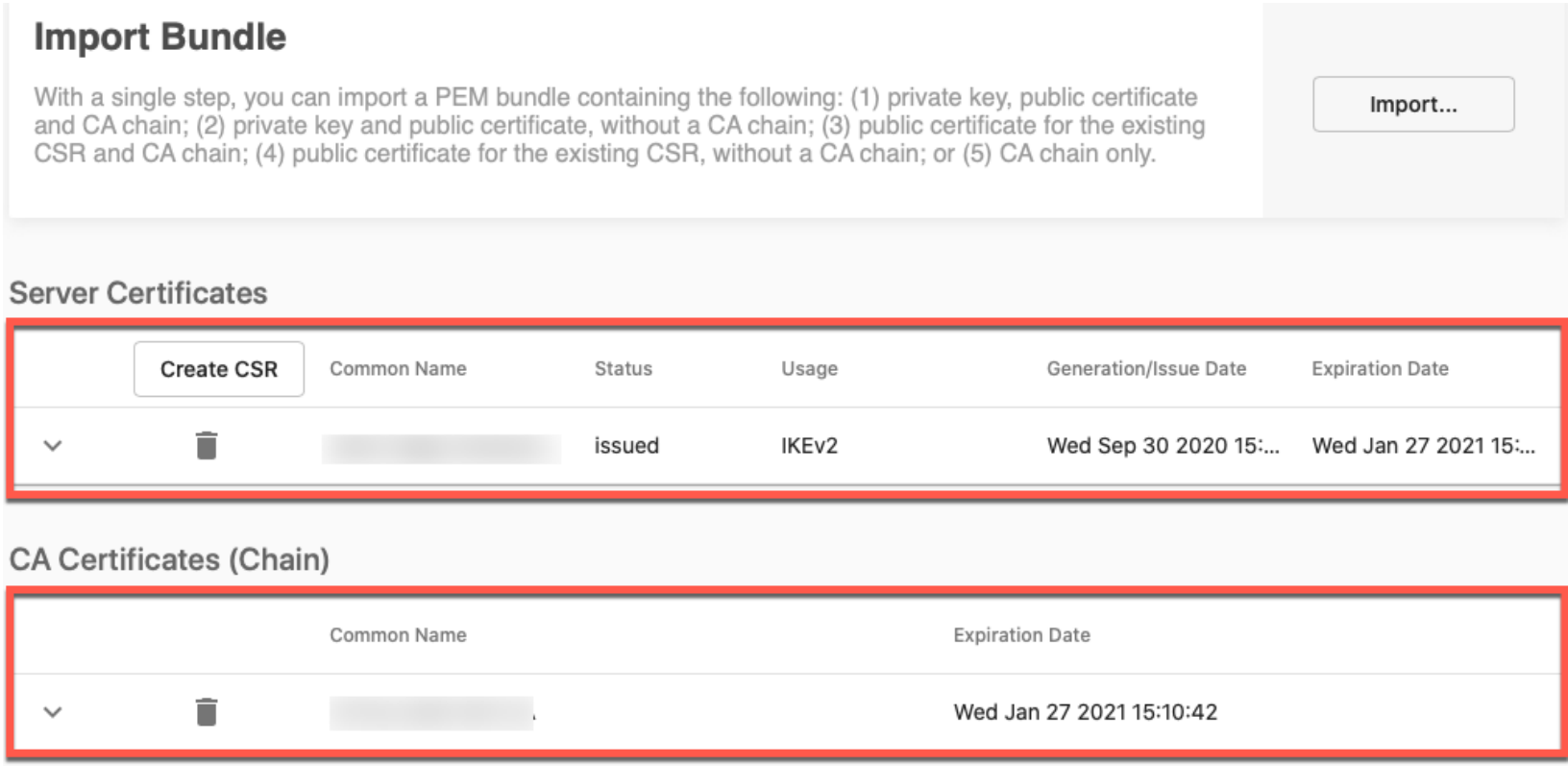
33. Verify "Upload"

- Once uploaded the CA Chain should appear in the CA Certificates (Chain) area



34. Verify Issued Server Certificate and CA Chain

- After uploading the "**CA Chain**" or "**Full PEM Bundle**" 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 "**Server Certificate**" with status of "**Issued**" with the correct "**Common Name**" and a "**CA Certificate**" and "**Expiration Date**"



You have now completed the GoSilent Server IKEv2 Setup Guide

Contact Us

If you should have any further questions, concerns, or feedback regarding this guide or anything else, please feel free to reach out to our Attila Security Support team at any time.

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