

Configure Postman

- [Prerequisites](#)
- [Importing collection](#)
- [Additional configurations](#)
 - [Configure baseUrl on collection global variables](#)
 - [Configure auth certificates inside Postman \(optional\)](#)
 - [Configure Client SSL certificates when pointing to SaaS environment \(optional\)](#)

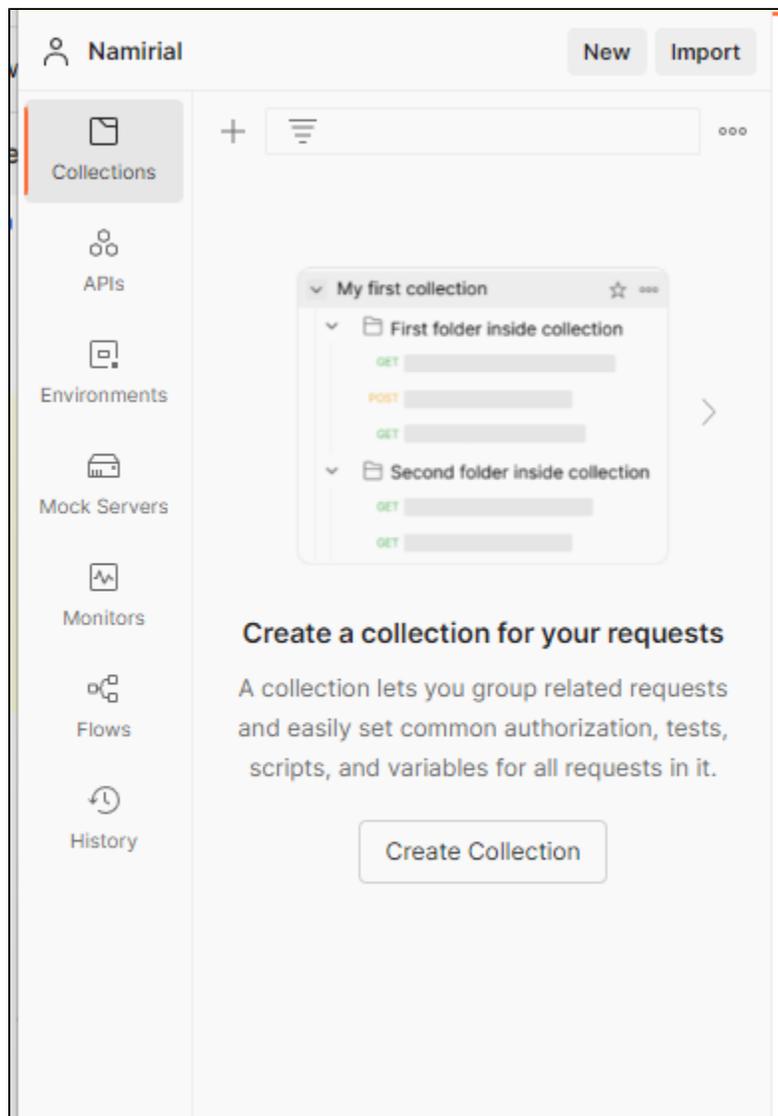
Prerequisites

1. SWS Postman collection: [collection download](#)
2. SWS Postman collection example files: [download example files](#)
3. Postman (<https://www.postman.com/downloads/>)

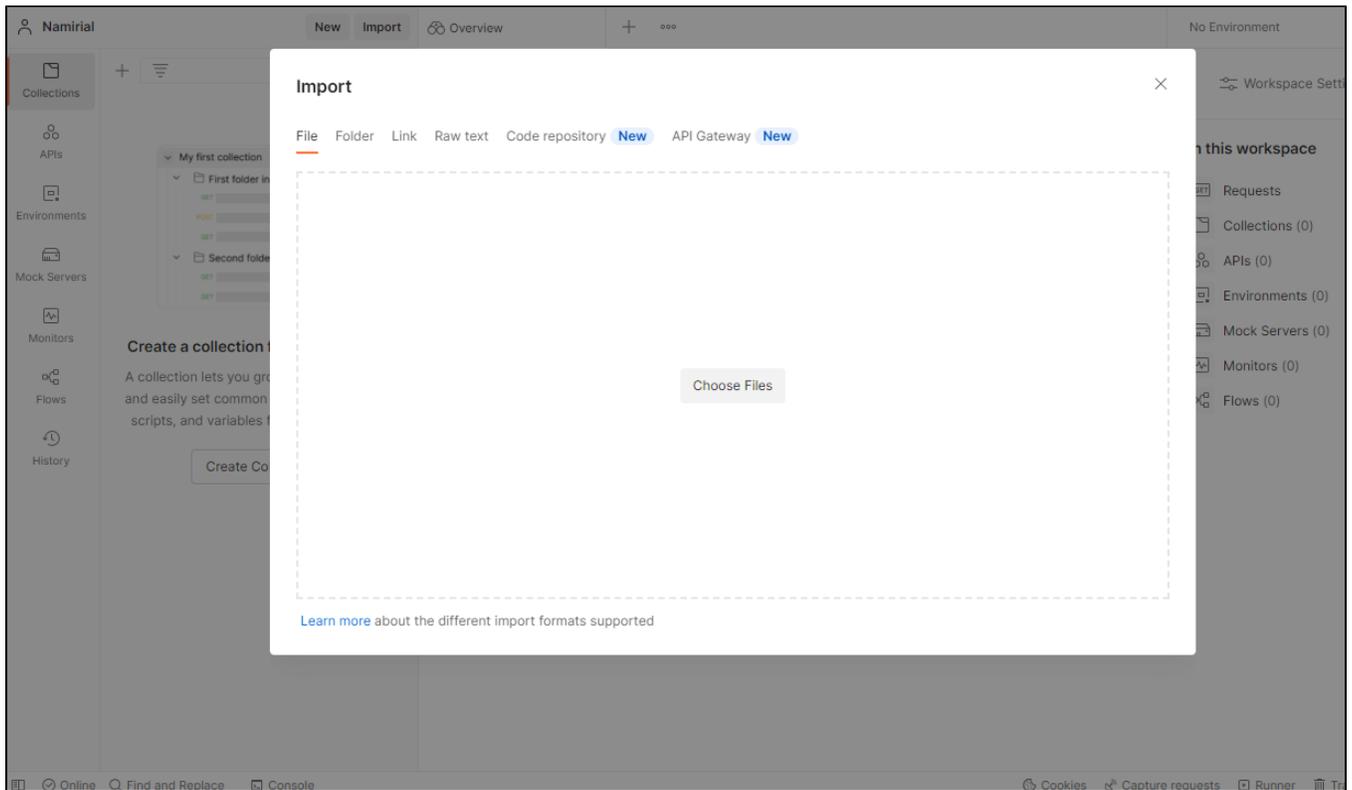
Importing collection

Once collection is downloaded then import the collection inside your Postman app.

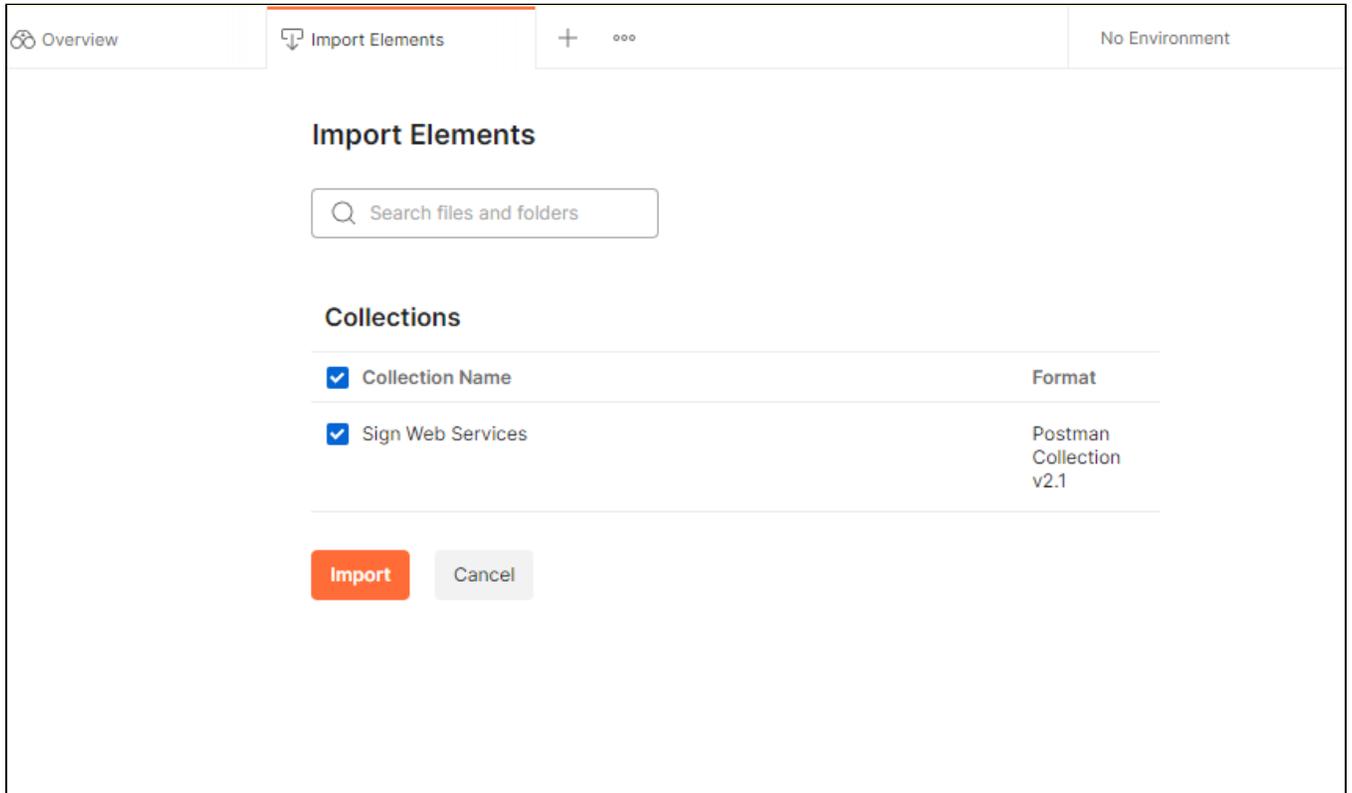
Go to "Collections"



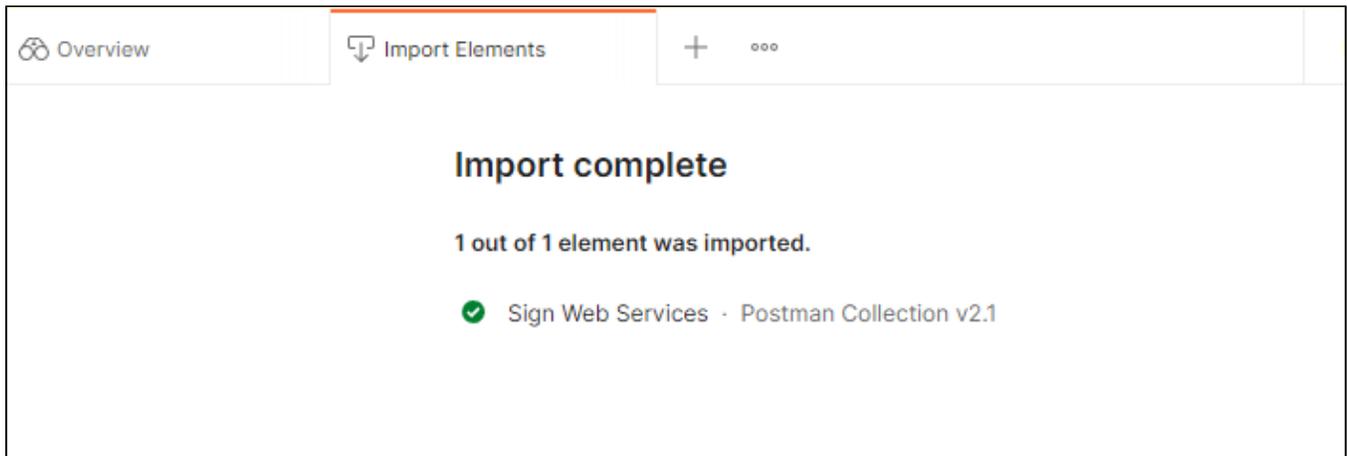
"Import" "File" "choose the collection previously downloaded"



After choosing the file from your download directory you must see something like this:



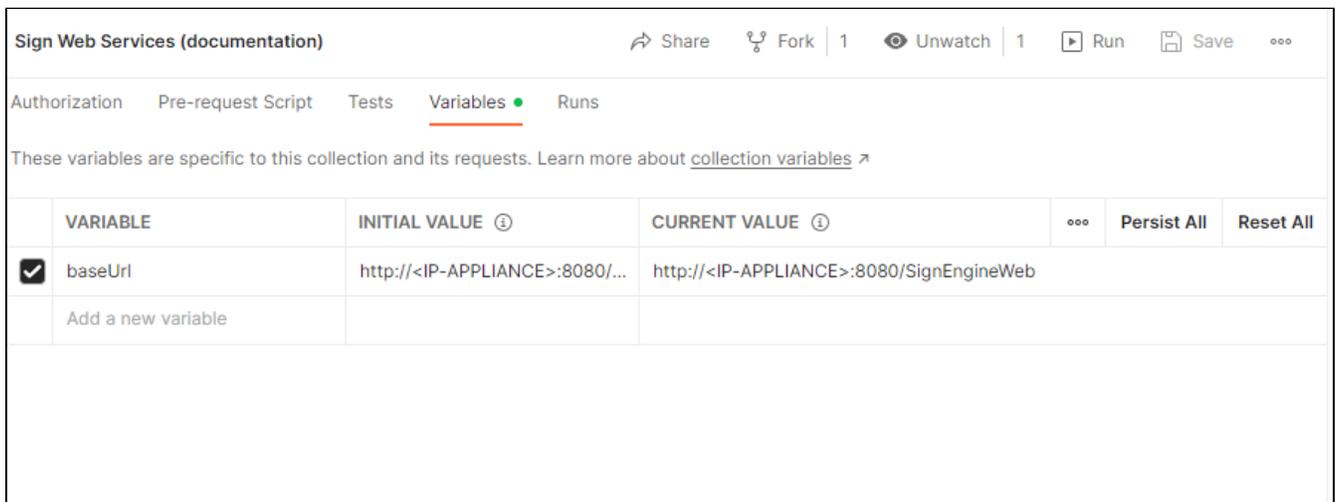
Choose "Import" , if everything was successful a new collection must be created inside your workspace and message like this appears inside the screen:



Additional configurations

Configure baseUrl on collection global variables

All the requests inside the collection are parametrized using the variable `{{baseUrl}}` inside request urls so change it to point to your domain



NOTE: if you are testing the TEST SWS SaasS the "baseUrl" is:

```
https://sws-companynamesaas.test.namirialtsp.com/SignEngineWeb
```

While the p12/jks can be downloaded at this [link](#)

Check files inside your workspace

Before sending the first requests check that files inside body requests are correctly configured with your environment if not try to reload files from your file system, because when importing SWS collection all file location link has to be reconfigured.

Sign Web Services

- rest
 - enquiry
 - service
 - sign
 - POST Close previously created session, see openS...
 - POST Get remaining seconds available for current s...
 - POST Open a new session and return back a sessio...
 - POST Send OTP via SMS, used by remote signature...
 - POST Sign generic file using CAAdES format
 - POST Sign files using PKCS1 format
 - POST Sign PDF file using PAdES format
 - POST Sign XML files using XAdES format
 - PUT /rest/admin/remove-certificate-from-cache
 - GET /rest/ready
 - POST Get TSR from a given input file
 - PUT Change password for the given user

POST `{{baseUrl}}/rest/sign/signPades` Send

Params Auth Headers (11) **Body** Pre-req. Tests Settings Cookies

form-data

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	credentials	{"idOtp": "-58457700", "otp": "culpa cupidat...			
<input checked="" type="checkbox"/>	padesPreferences	{"fileNameInTSD": "veniam ad cupidat...			
<input checked="" type="checkbox"/>	buffer	Select Files			
	Key	Value	Description		

Response



Configure auth certificates inside Postman (optional)

Goto "File" "Settings" Certificates

SETTINGS

General Themes Shortcuts Data Add-ons **Certificates** Proxy Update About

CA Certificates OFF

The file should consist of one or more trusted certificates in PEM format.

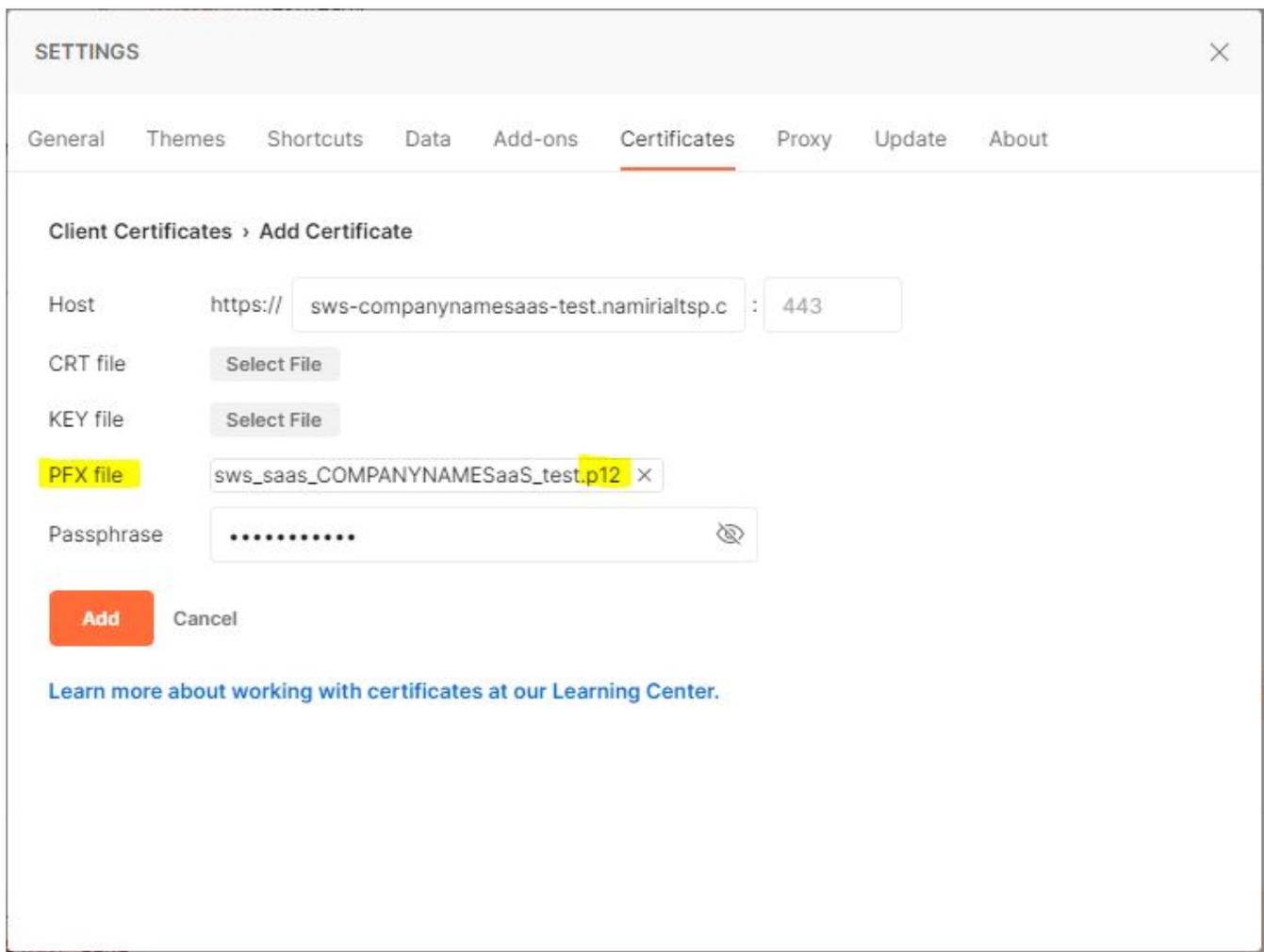
PEM file Select File

Client Certificates Add Certificate

Add and manage SSL certificates on a per domain basis.

[Learn more about working with certificates at our Learning Center](#)

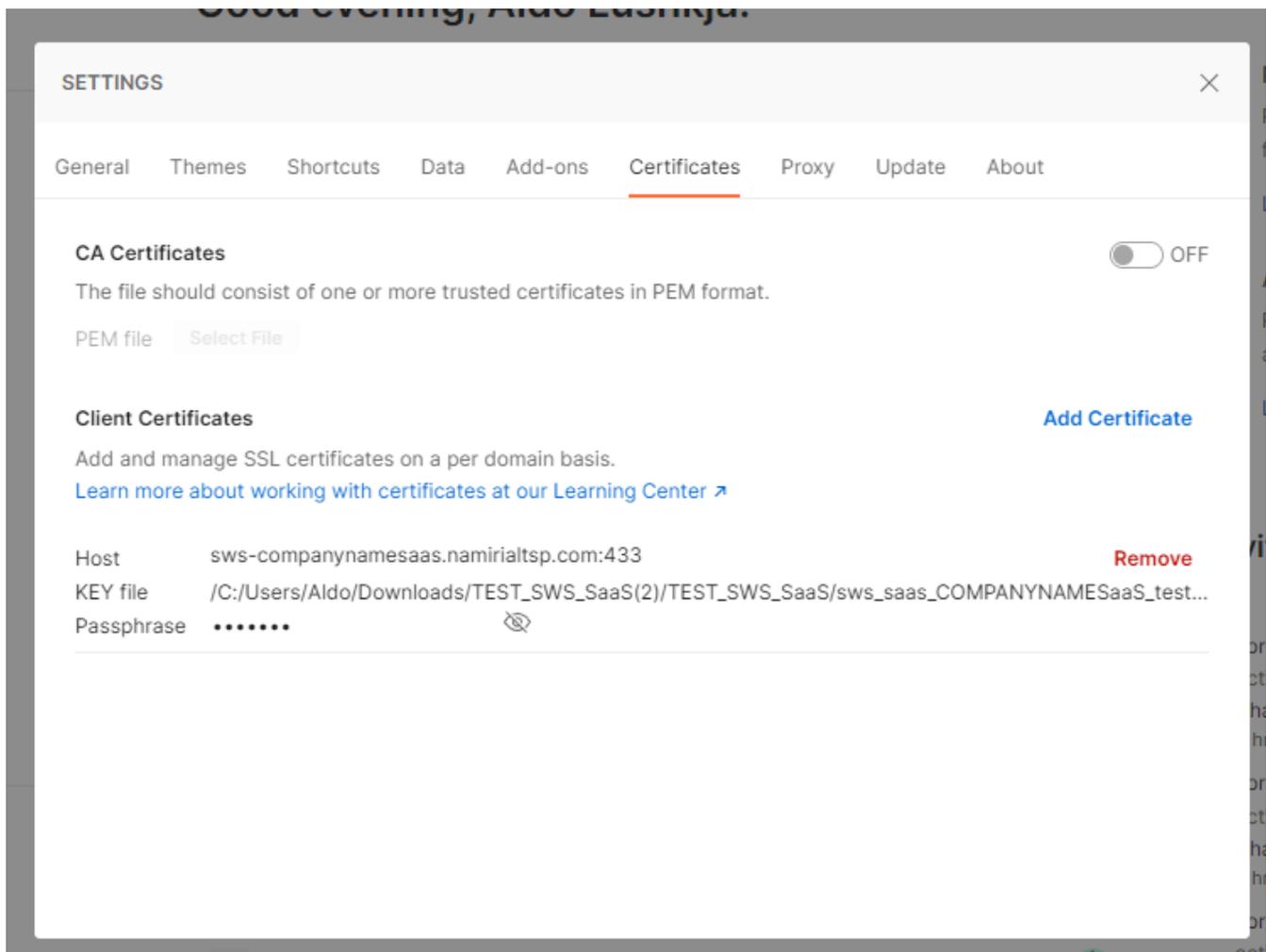
Choose "Client Certificates" "Add Certificate"



Configure your endpoint address and your PFX file with your passphrase than click "Add"

NOTE: pay attention that postman does not support JKS format.

Once completed you should see something like this:



Configure Client SSL certificates when pointing to SaaS environment (optional)

When you have a SWS SaaS based solution, then you must configure client ssl certificate against your production fqdn (sws-<your_company_name>saas.namirialtsp.com). See also: [ConfigureauthcertificatesinsidePostman\(optional\)](#)