SSL CERTIFICATE ON CHECK POINT

Raghu
Diamond Services

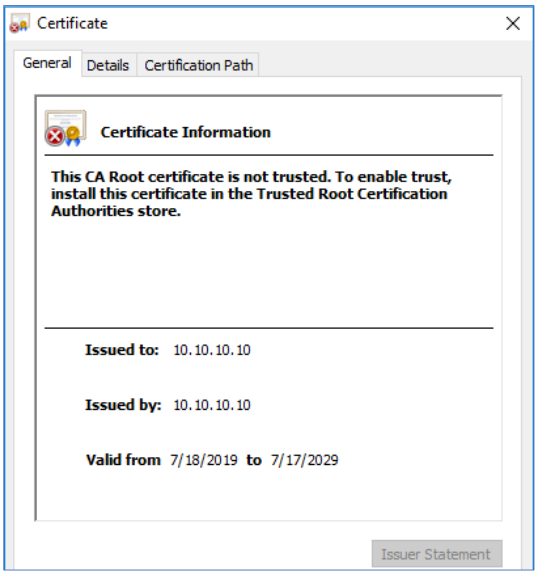
Contents

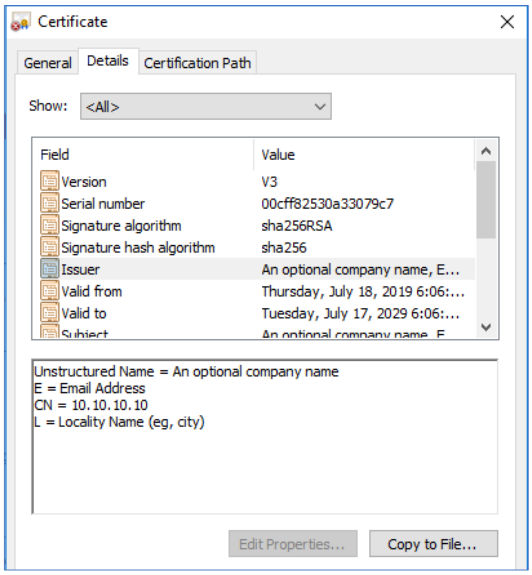
Overview

1. When we install a Check Point Operating System (say Gaia) and boot the device for the first time, by default a Private Key, CSR (using the default parameters) & a Self-Signed Certificate will be created.

```
Fulcrum switch not installed
Creating initial configuration database...

Generating a 2048 bit RSA private key
.....................+++
.....................................................................................................+++
writing new private key to '/web/conf/server.key'
-----
1085 bindings were imported
Update Interfaces in Database:  interfaces in loop:
Mgmt
```

While Generating the CSR, it took the default parameters and the CN field as the interface IP-address defined during the OS installation of this VM (192.168.1.1 on CP Devices).

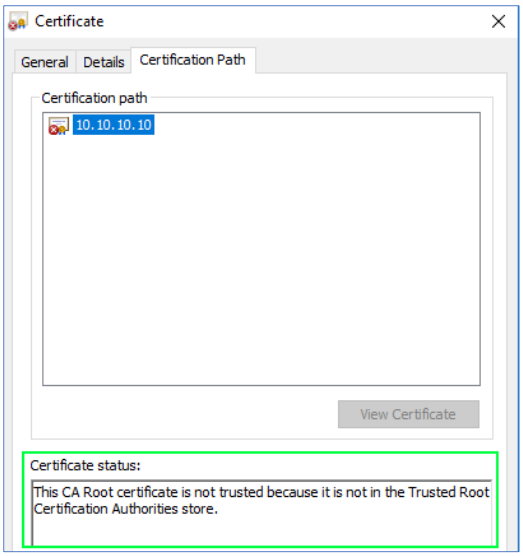




The Private Key & Self-Signed Certificate will be stored in **`/web/conf`** directory of that device.

```
[Expert@RK-FW-BNG:0]# cd /web/conf/
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# ls -lh
total 88K
drwxr-xr-x 2 admin root 4.0K Jul 11 18:22 extra
-rw-r--r-- 1 admin root  20K Jul 24 17:58 httpd2.conf
-rw-r--r-- 1 admin root  18K Jul 11 17:30 httpd2.conf.backup
-rw-r--r-- 1 admin root  433 Jul 24 19:57 httpd2_mp.conf
-rwsr-xr-x 1 admin root  22K Jul 11 17:30 login
lrwxrwxrwx 1 admin root   46 Jul 11 17:30 mime.types -> /web/cpshared/web/Apache/2.2.0/conf/mime.types
-rw-r----- 1 admin root 8.2K Jul 24 19:48 server.crt
-rw-r----- 1 admin root 1.7K Jul 24 19:48 server.key
[Expert@RK-FW-BNG:0]#
```

2. As it's a Self-Signed Certificate (not from a Trusted CA), browsers will throw a HTTPS Certificate Warning while accessing the device (Gaia Portal / SSL VPN portal / RA VPN Client).



3. In Check Point below features will use the SSL Certificates of the device for their functionality:

- Gaia Portal
- IPSec VPN (Certificate Based Tunnel)
- Remote Access VPN
- SSL VPN

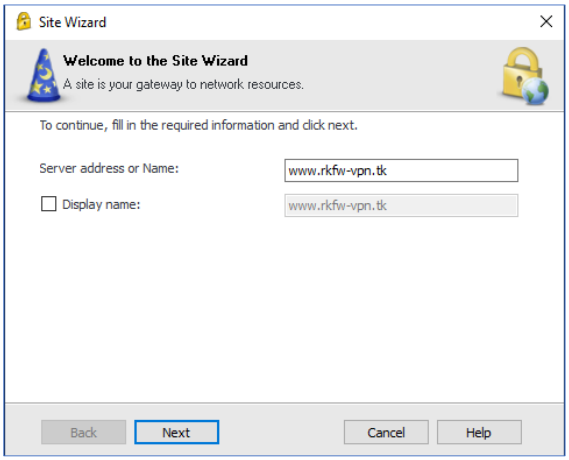
4. There will be a requirement for any organization to replace the Self-Signed Certificate with a Trusted CA SSL Certificate to give the confidence to users accessing these features.

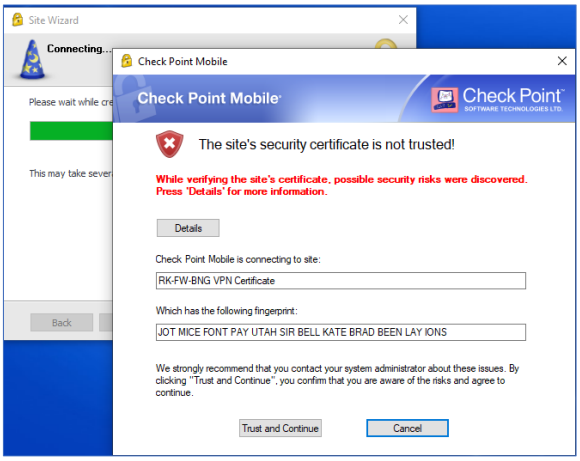
5. The Trusted CA SSL Certificate installation needs the following to be taken care:

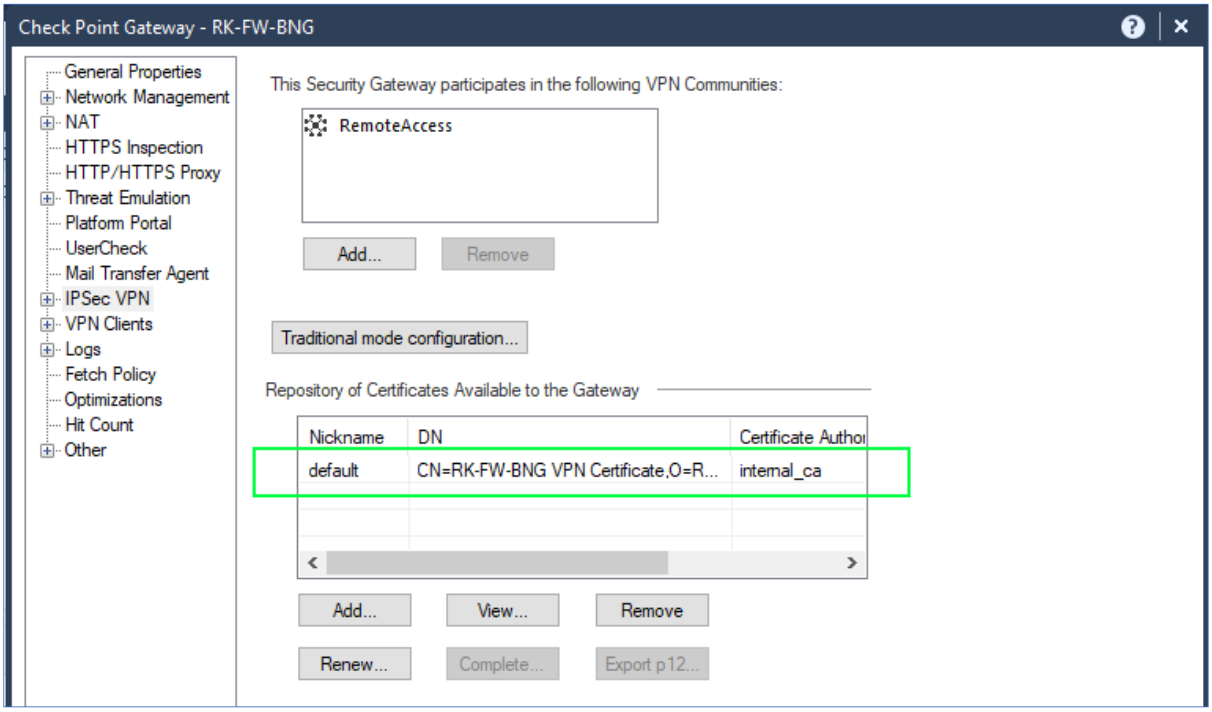
- CSR Generation on the Check Point device.
- Purchase an SSL Certificate from the Trusted CA.
- Request for an SSL Certificate for the generated CSR.
- Download & Install the Trusted SSL CA on the Check Point device.

SSL Certificate for IPSec & Remote Access VPN Feature

1. Our VPN Gateway's public IP-address (**49.206.27.13**) is associated with the domain name ***www.rkfw-vpn.tk*** . If we attempt to access the VPN Gateway using RA VPN client then users get Certificate Warning because of the **Self-Signed Certificate** associated with the VPN feature of this Gateway issued by the Management Server's **Internal CA**.



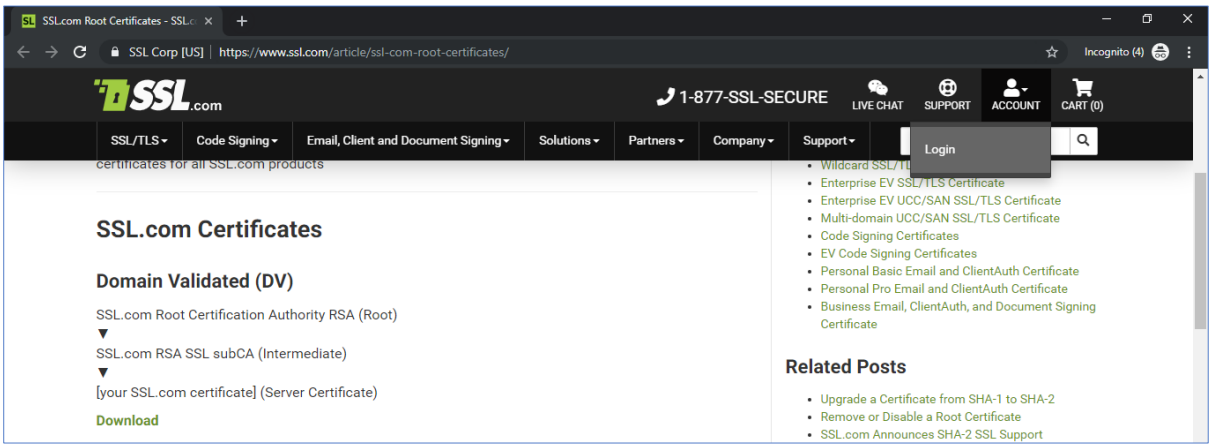




2. For VPN feature, installing a trusted 3rd party SSL Certificate involves different approach,

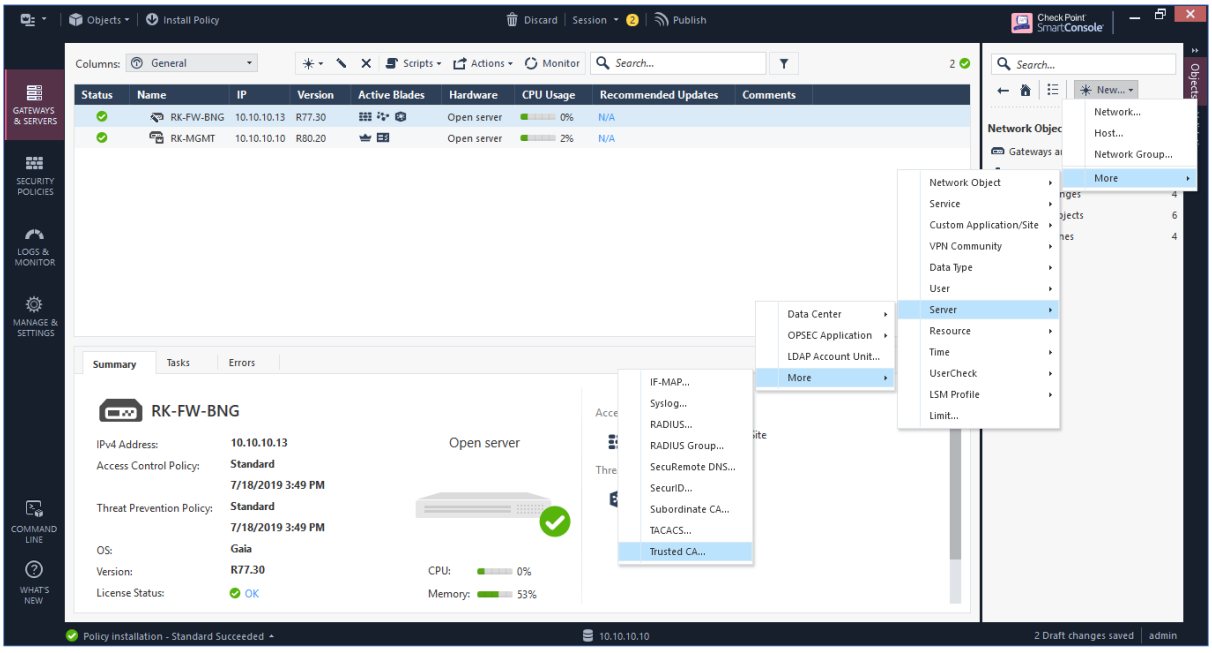
- Creating a Trusted 3rd Party Root CA on Check Point
- Creating a Trusted 3rd Party Intermediate CA on Check Point
- Generating a CSR from for the VPN Gateway.
- Request for an SSL Certificate using the generated CSR from Trusted 3rd Party CA.
- Install the SSL Certificate on the VPN Gateway.

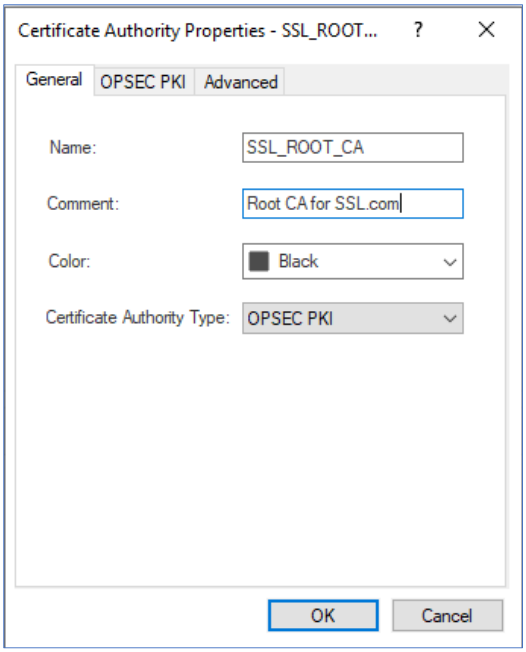
3. For any Trusted 3rd Party CA that you are planning to buy the license from, will provide its Root CA & Intermediate CA Certificate to download online. In this scenario we are considering ***SSL.com CA*** & its Root & Intermediate CA can be downloaded below,

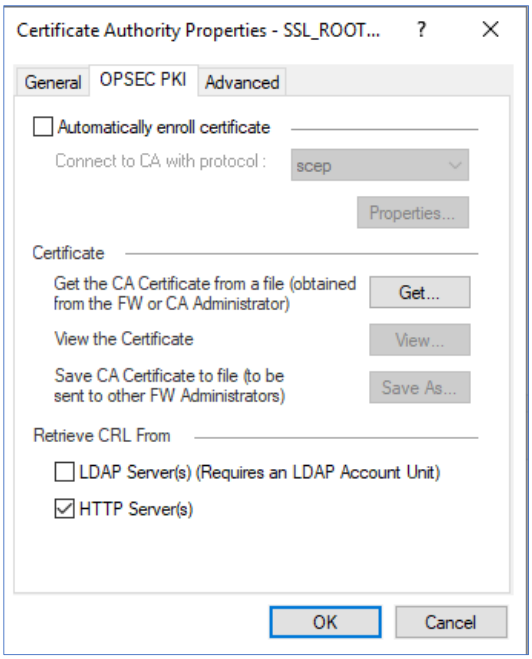


4. Let's get started with defining the Trusted CA's on our Check Point setup.

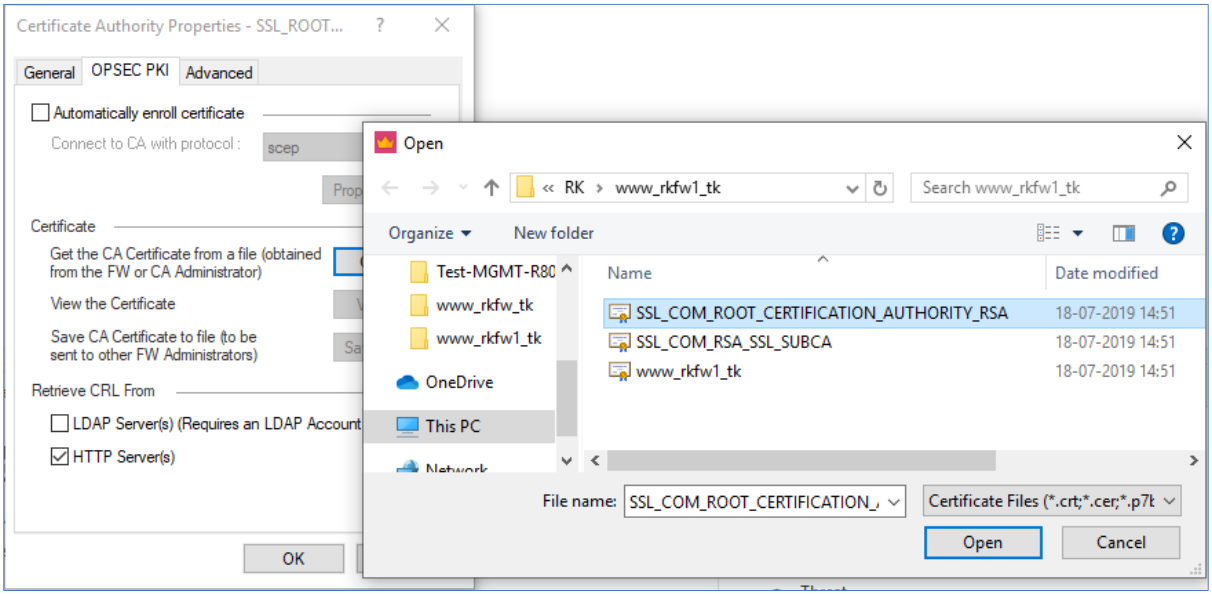
- Create the Trusted Root CA for ***SSL.com***,



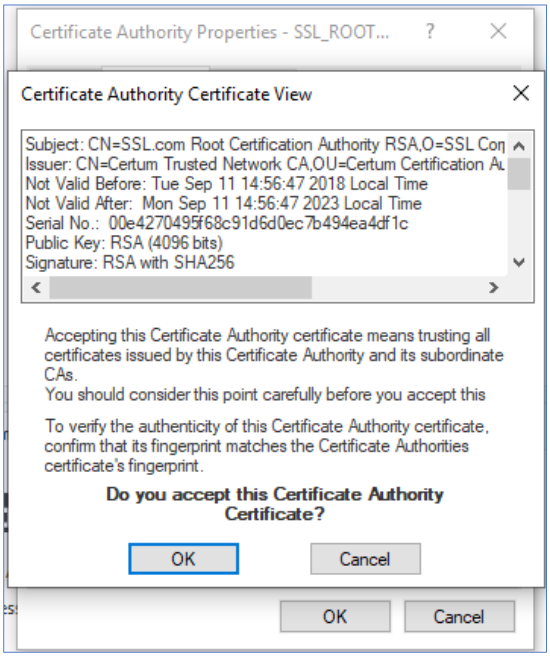




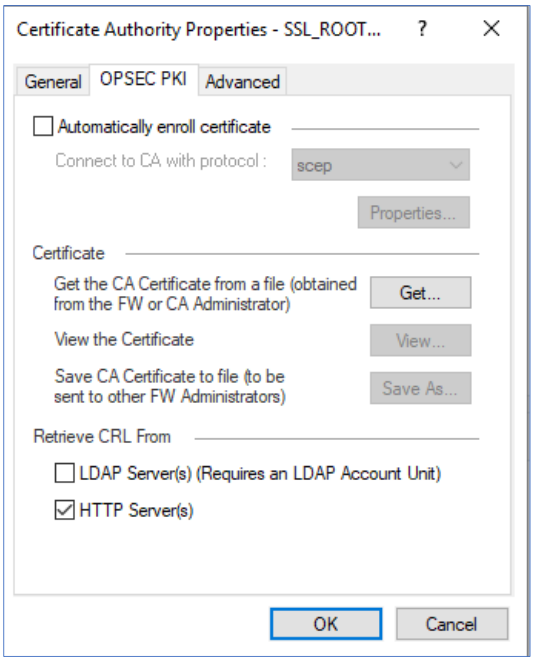
- Select the **OPSEC PKI** tab & inside the "**Certificate**" section, click on **Get** to insert the Root CA certificate & Browse the Root CA Certificate for ***SSL.com*** (a ***.crt*** or ***.cer*** file)***,***



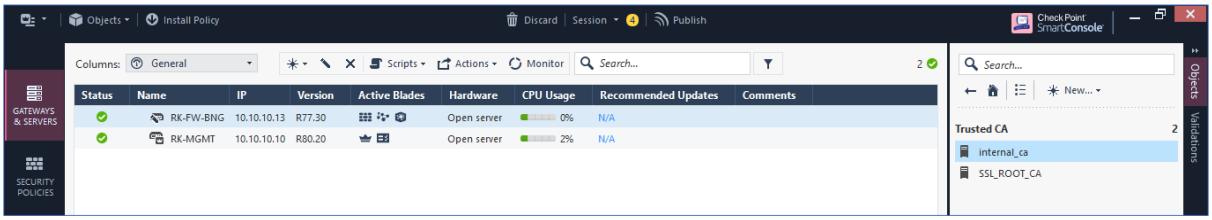
- You will be able to see the content of this Root CA certificate, Click **OK** to accept the Root CA Certificate.



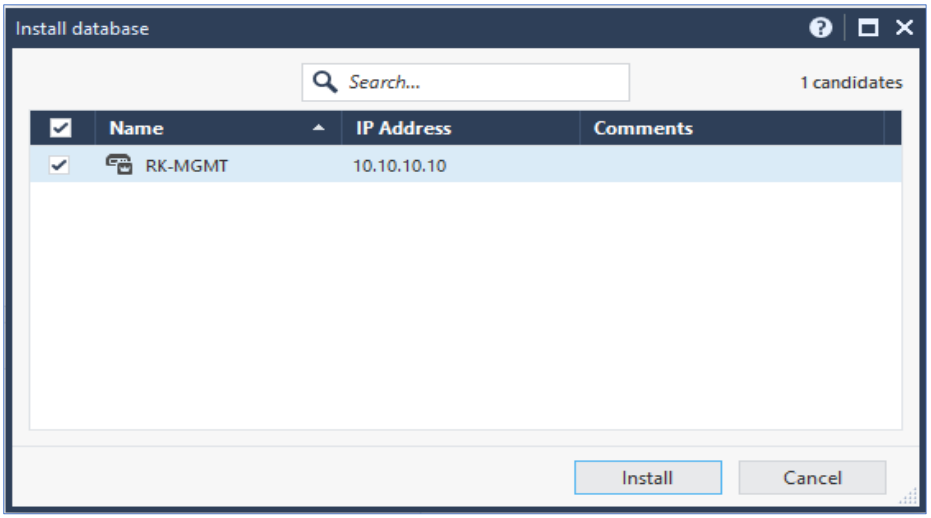
- In the "**Retrieve CRL from" section, make sure that only "HTTP Server(s)"** is selected. Click **OK** to save this object.



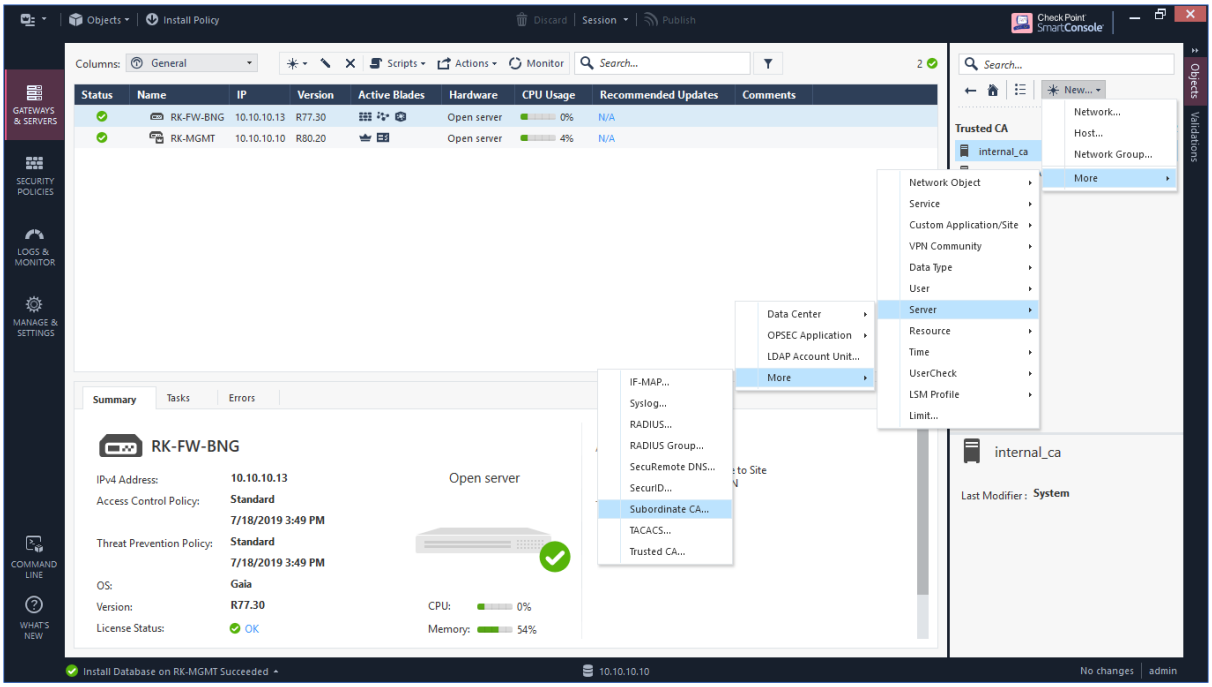
- Under **Trusted CA** section, along with Management Server's ***internal_ca*** you can see ***SSL.com Root CA.***



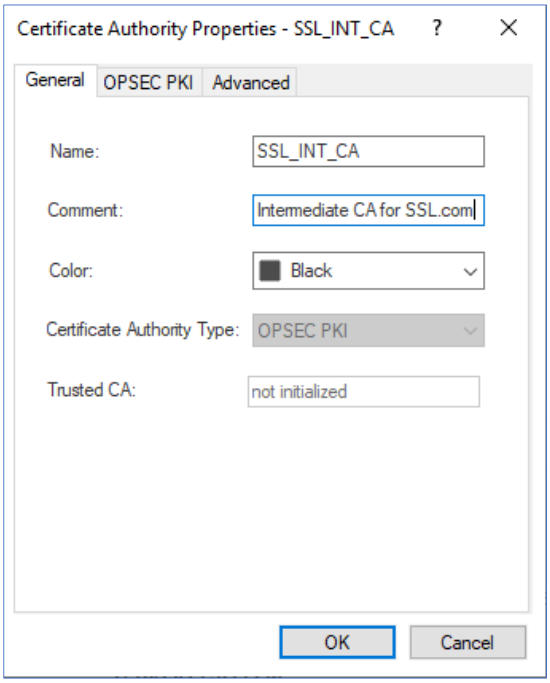
- Install the Database on the Management Server (with publishing the changes).

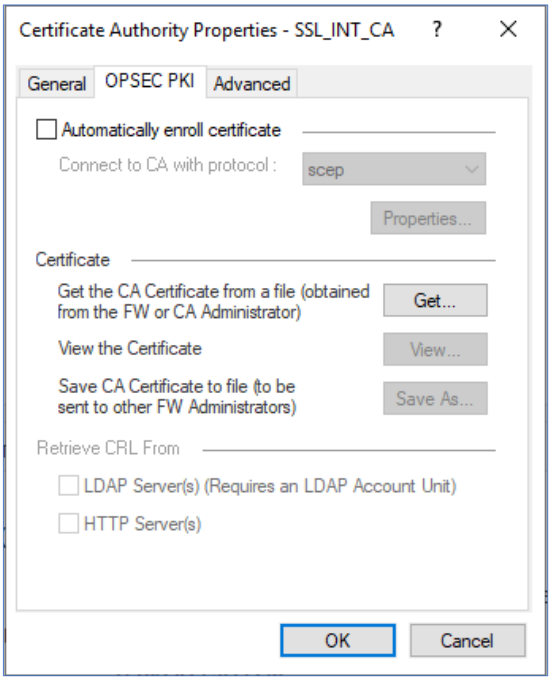


5. Now, define the **SSL.com Intermediate CA (Subordinate CA)** using the Intermediate CA Certificate that we downloaded before.

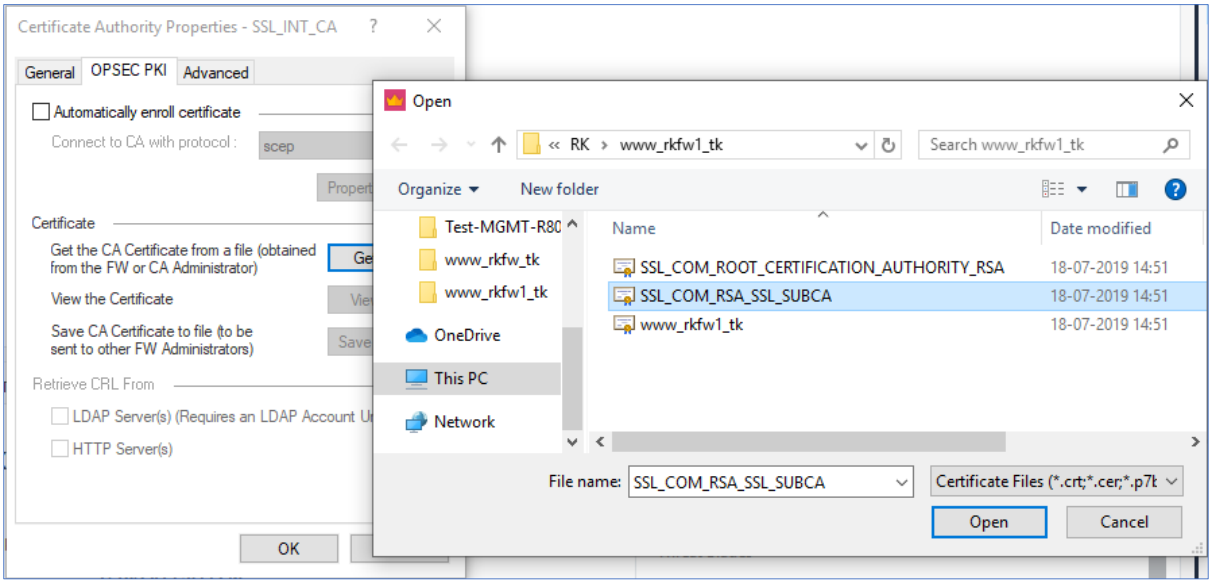


- Provide a name for the Intermediate CA and don't worry about the **Trusted CA** section showing as "***not initialized***".

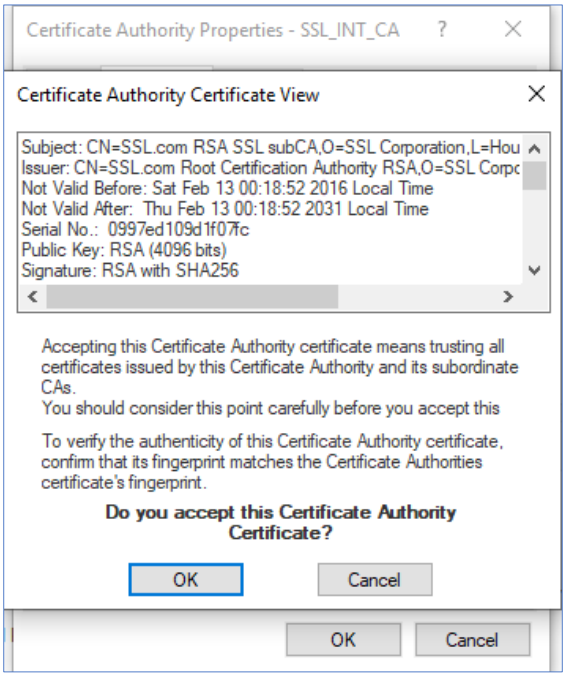




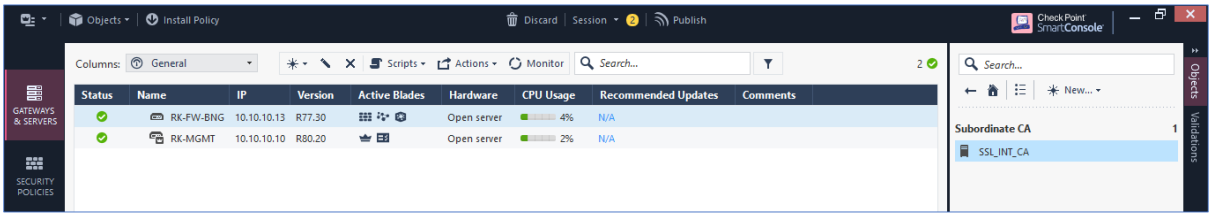
- Select the **OPSEC PKI** tab, inside the "**Certificate**" section, click ***Get*** to insert the Intermediate CA certificate & Browse the Intermediate CA Certificate for ***SSL.com*** (a ***.crt*** or ***.cer*** file)***,***



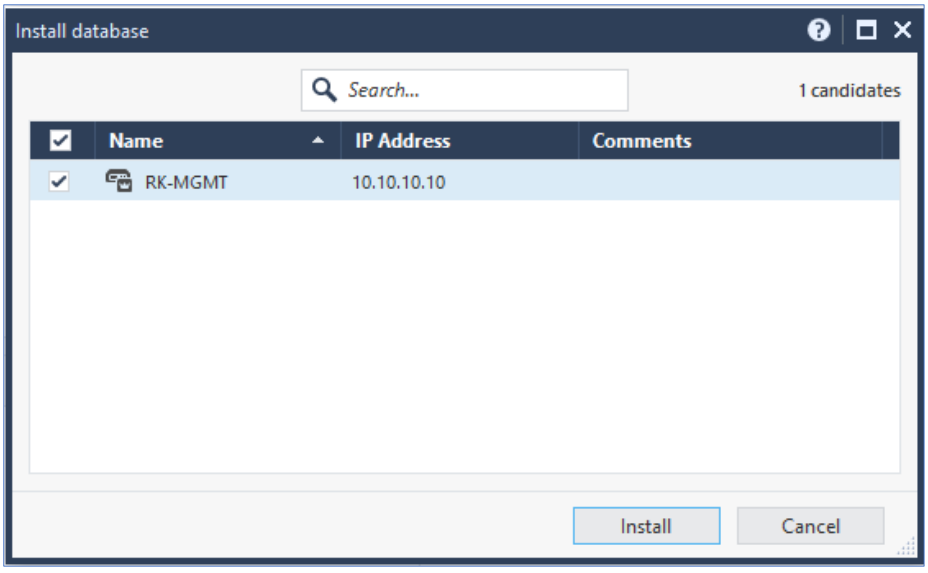
- You will be able to see the content of this Intermediate CA certificate, Click **OK** to accept the Intermediate CA Certificate.



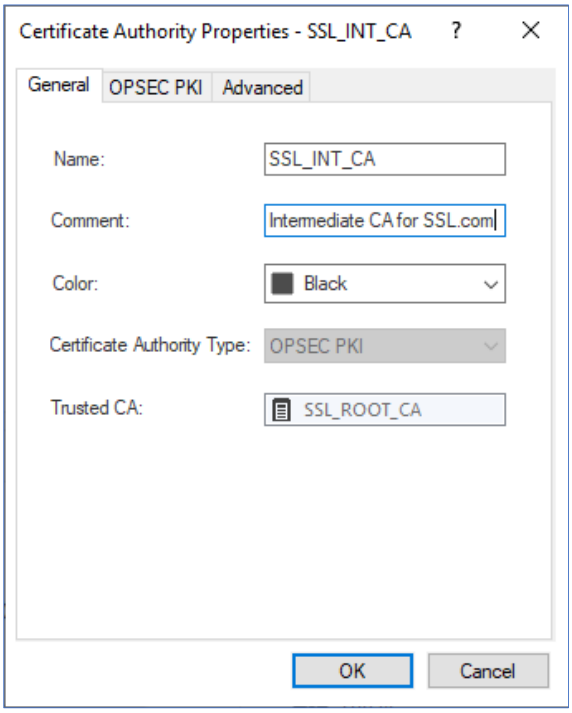
- We can see the Intermediate CA object in the **Subordinate CA** section.



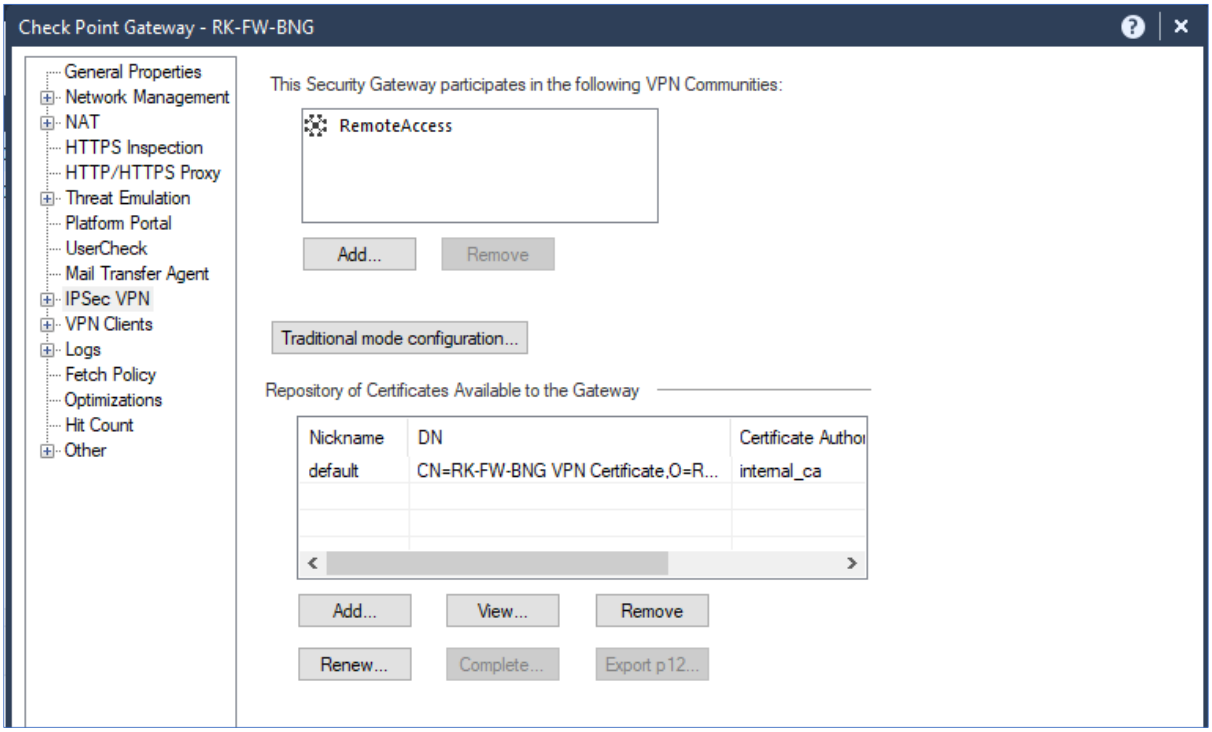
- Install the Database on the Management Server (with publishing the changes).



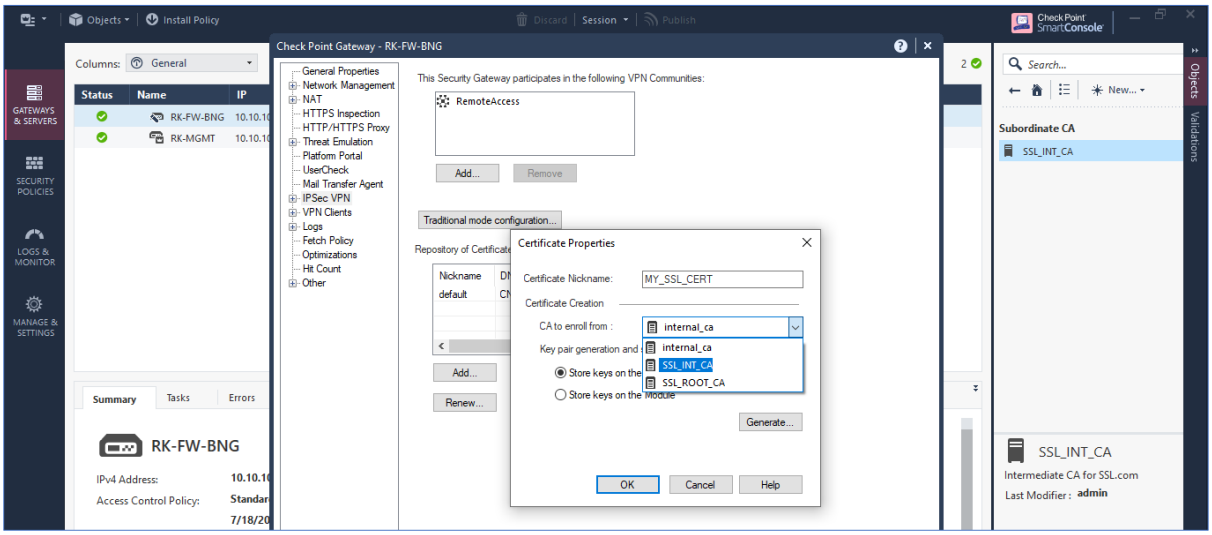
- Open the Intermediate CA object and we can see our Root CA Object ***SSL_ROOT_CA*** under **Trusted CA** section.

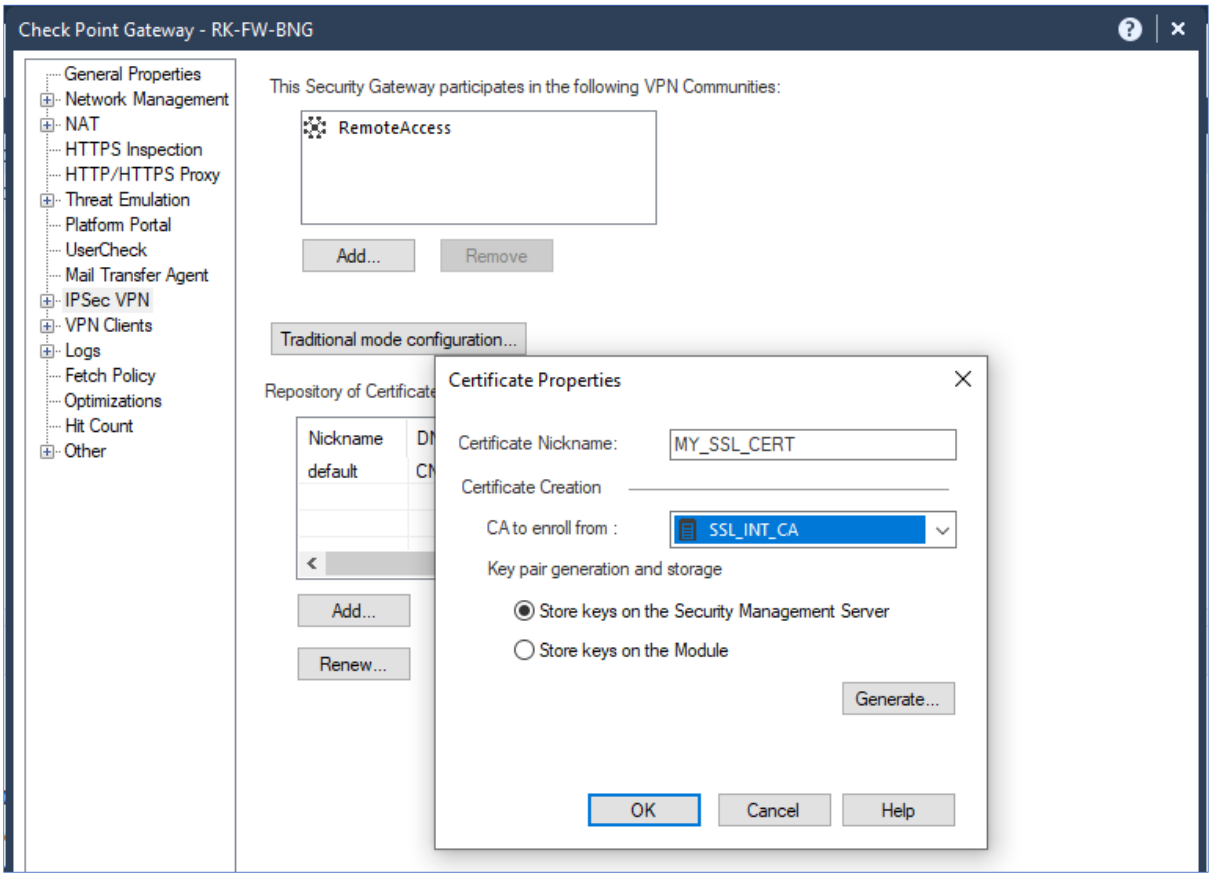


7. Open the VPN Gateway object and go to the IPSec VPN section.

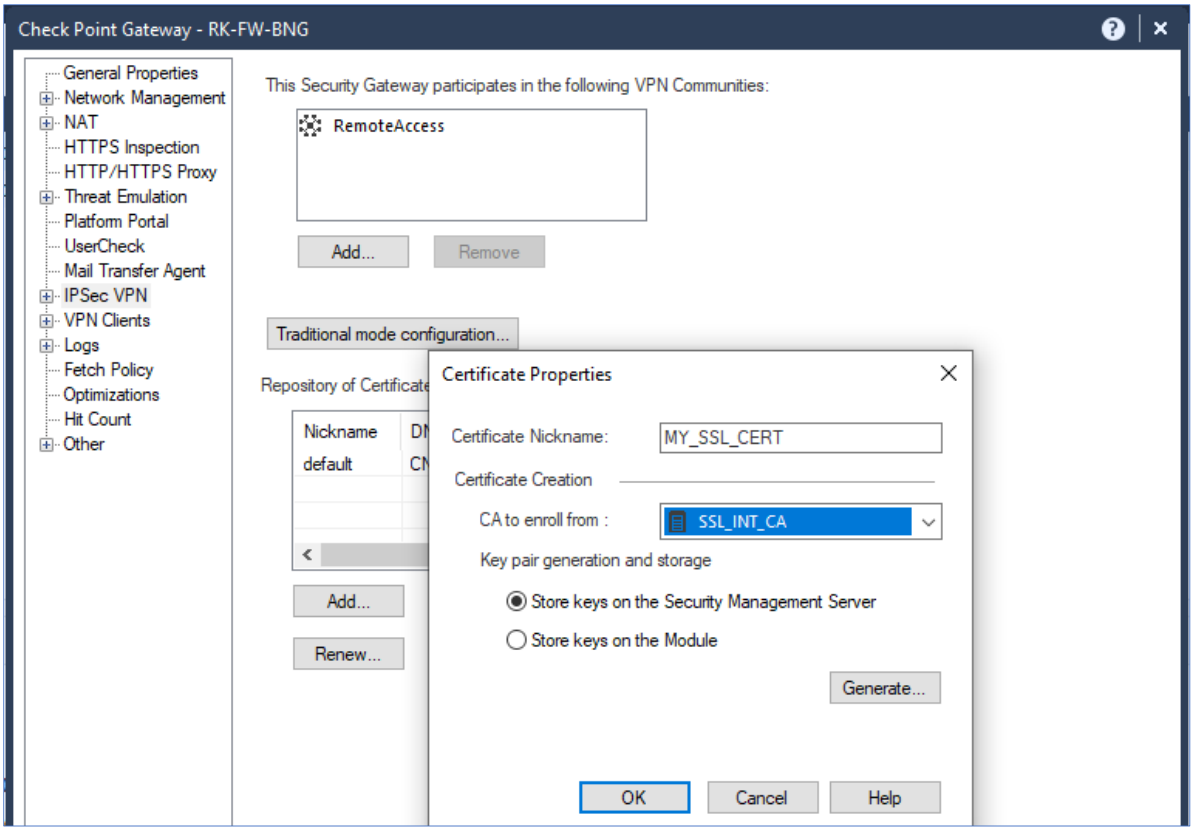


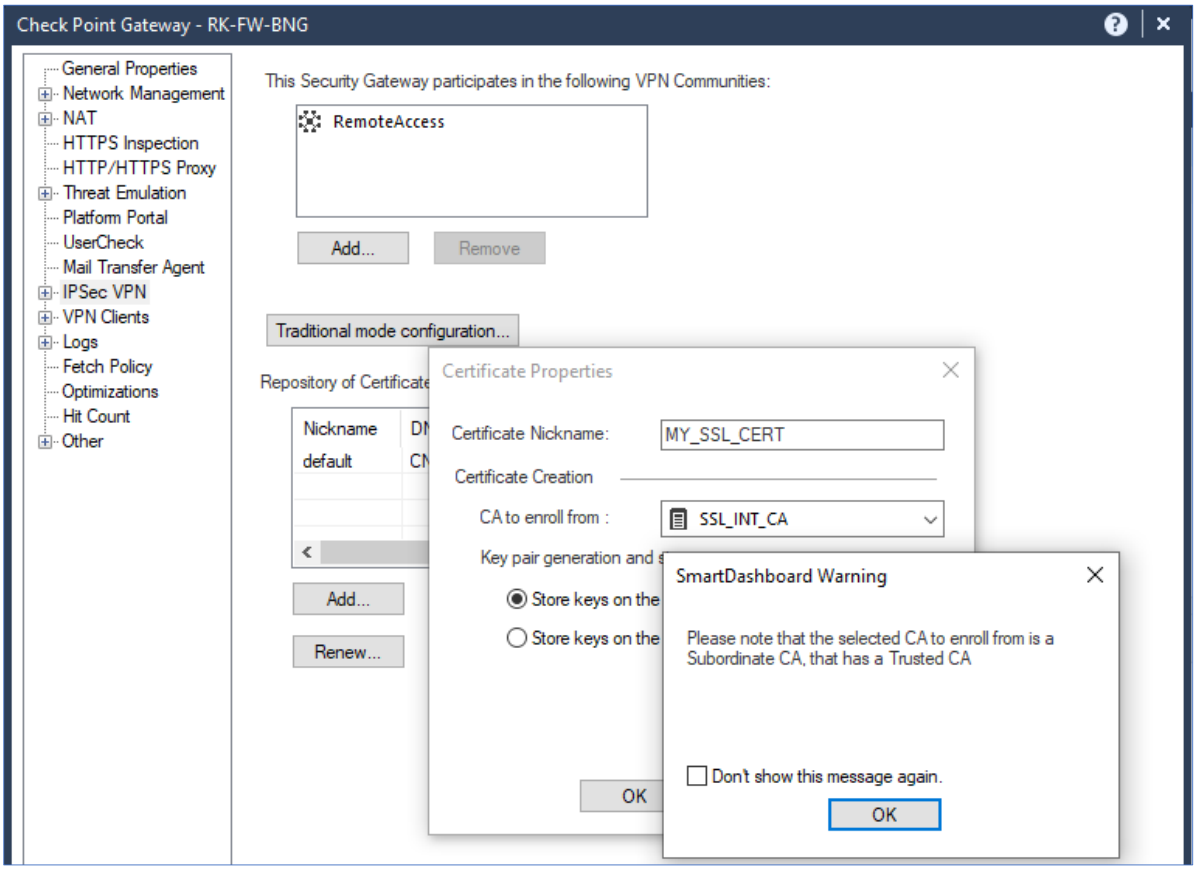
8. Click on ***Add*** and define our Trusted SSL Certificate Properties to generate the **CSR** out of it. Select Intermediate CA object (***SSL_INT_CA***) under **CA to enroll from** section.

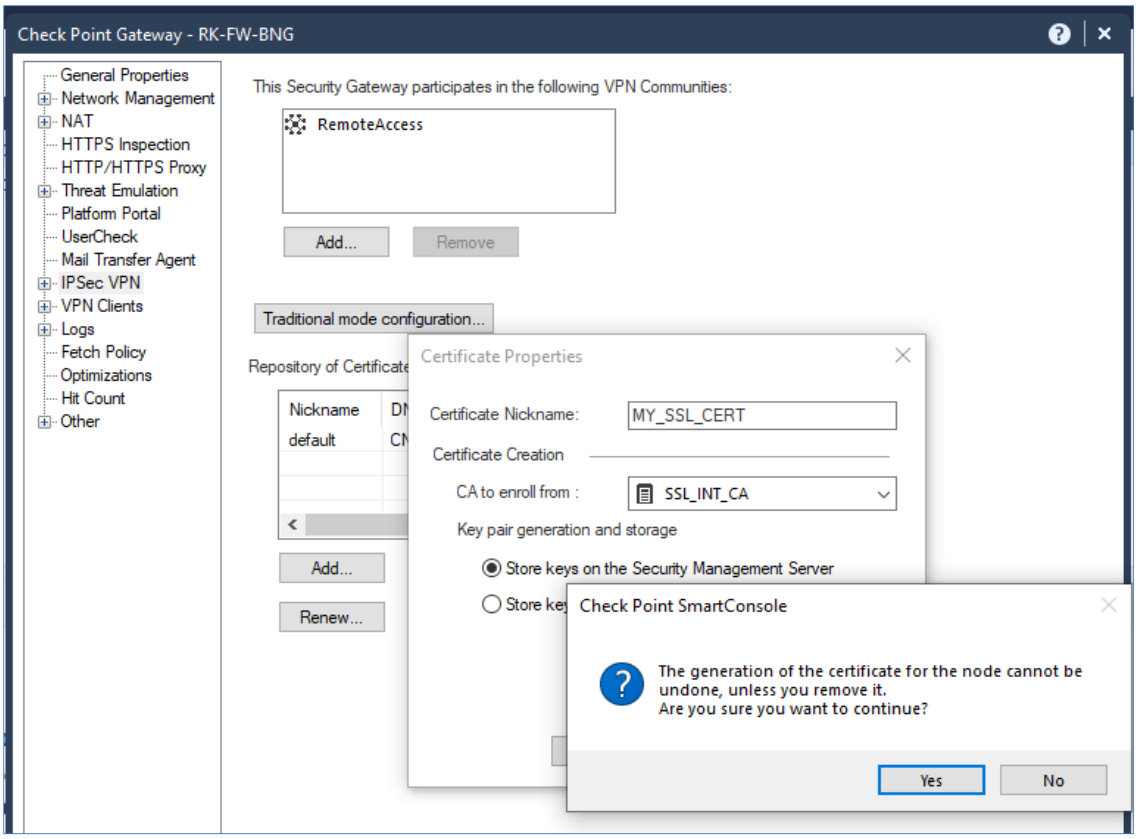


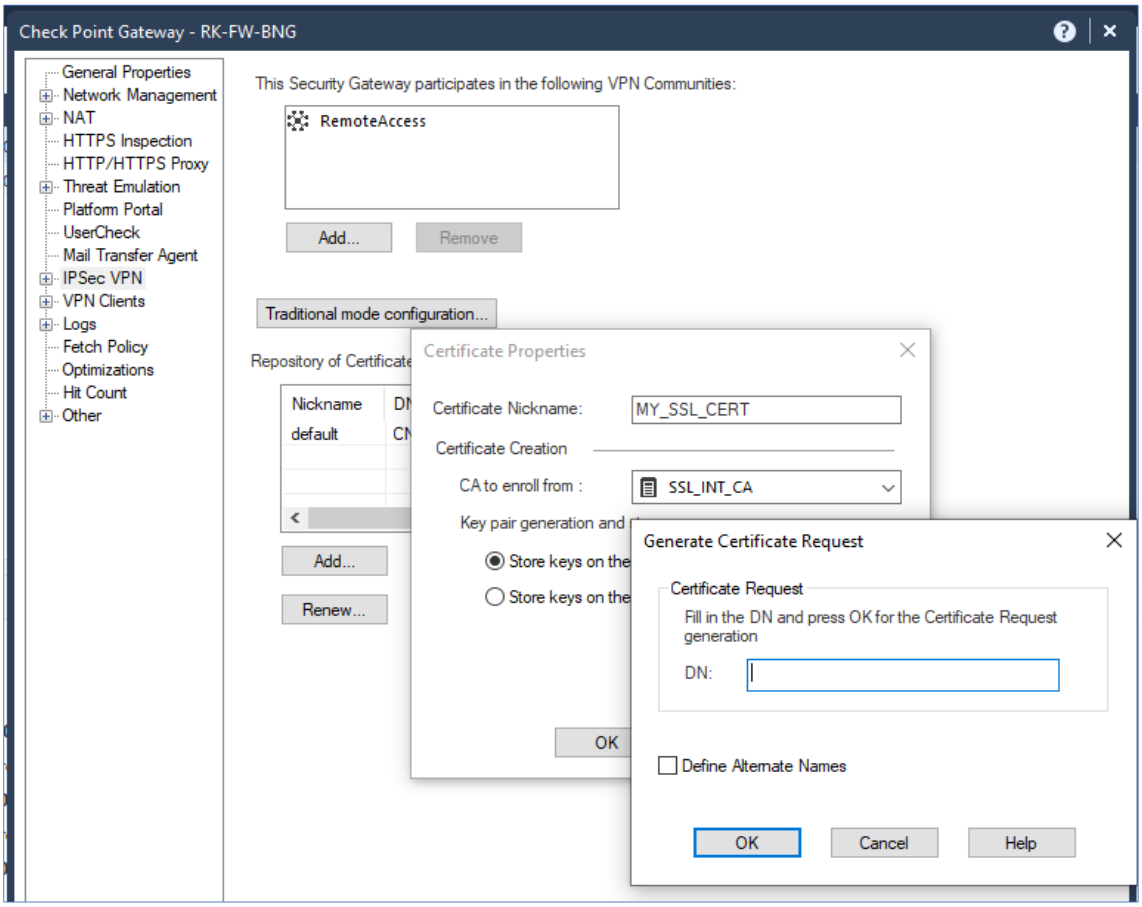


9. Click on **Generate** to generate the CSR






Check Point Gateway - RK-FW-BNG
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Threat Emulation
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other
This Security Gateway participates in the following VPN Communities:
RemoteAccess
Add...
Remove
Traditional mode configuration...
Repository of Certificate
Nickname
default
Add...
Renew...
Certificate Properties
Certificate Nickname:
MY_SSL_CERT
Certificate Creation
CA to enroll from :
SSL_INT_CA
Key pair generation and storage
Store keys on the Security Management Server
Store key
Check Point SmartConsole
The generation of the certificate for the node cannot be undone, unless you remove it.
Are you sure you want to continue?
Yes
No

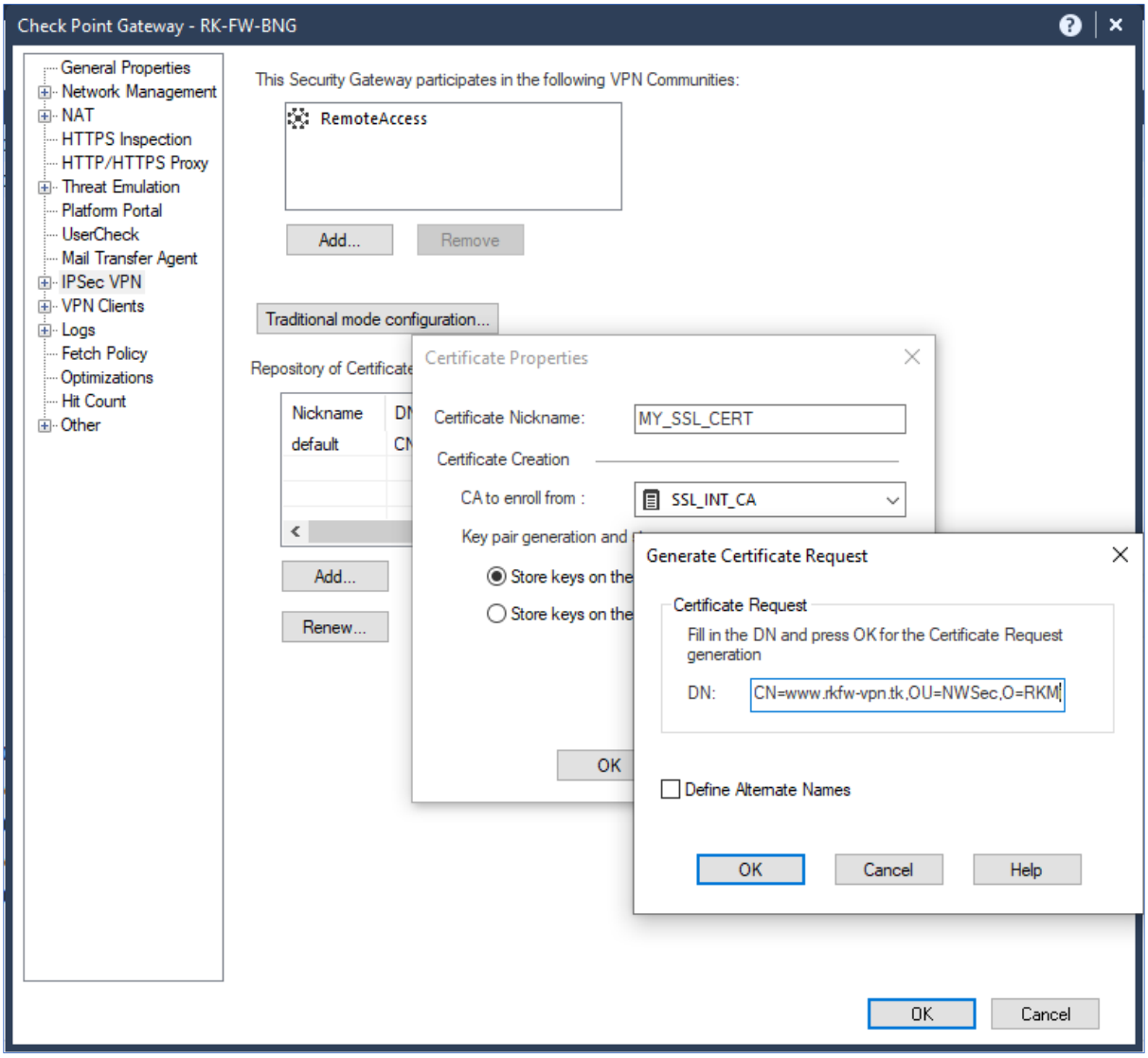

Check Point Gateway - RK-FW-BNG
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Threat Emulation
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other
This Security Gateway participates in the following VPN Communities:
RemoteAccess
Add...
Remove
Traditional mode configuration...
Repository of Certificate
Nickname
default
Add...
Renew...
Certificate Properties
Certificate Nickname:
MY_SSL_CERT
Certificate Creation
CA to enroll from :
SSL_INT_CA
Key pair generation and
Store keys on the
Store keys on the
OK
Generate Certificate Request
Certificate Request
Fill in the DN and press OK for the Certificate Request generation
DN:
Define Alternate Names
OK
Cancel
Help

10. Define the **DN (Distinguished Name)** as follows,

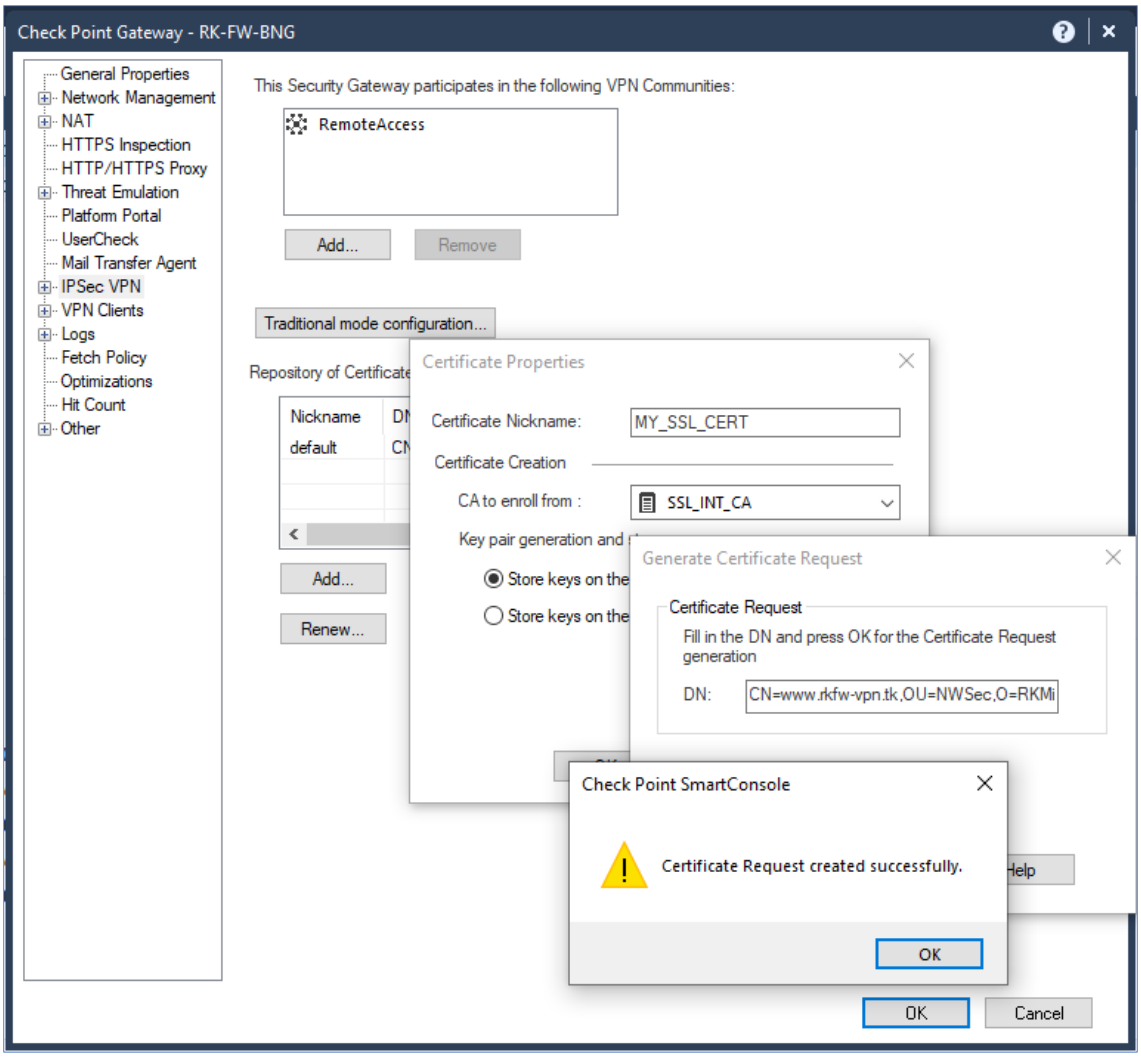
`CN=`***`DomainName`***`,OU=`***`Department`***`,O=`***`Organization`***`,L=`***`Locality`***`,ST=`***`State`***`,C=`***`Country`***

In our case let's define a Domain Name for our VPN Gateway as ***rkfw-vpn.tk,***

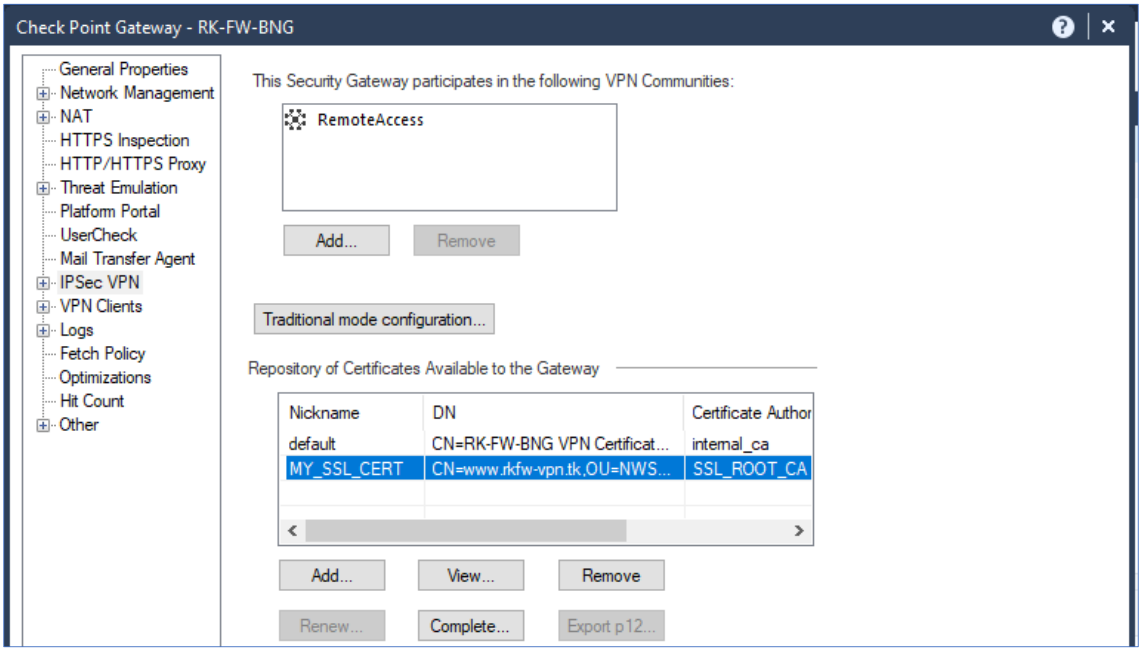
`CN=`***`www.rkfw-vpn.tk`***`,OU=`***`NWSec`***`,O=`***`RKMillets`***`,L=`***`Bengaluru`***`,ST=`***`Karnataka`***`,C=`***`IN`***



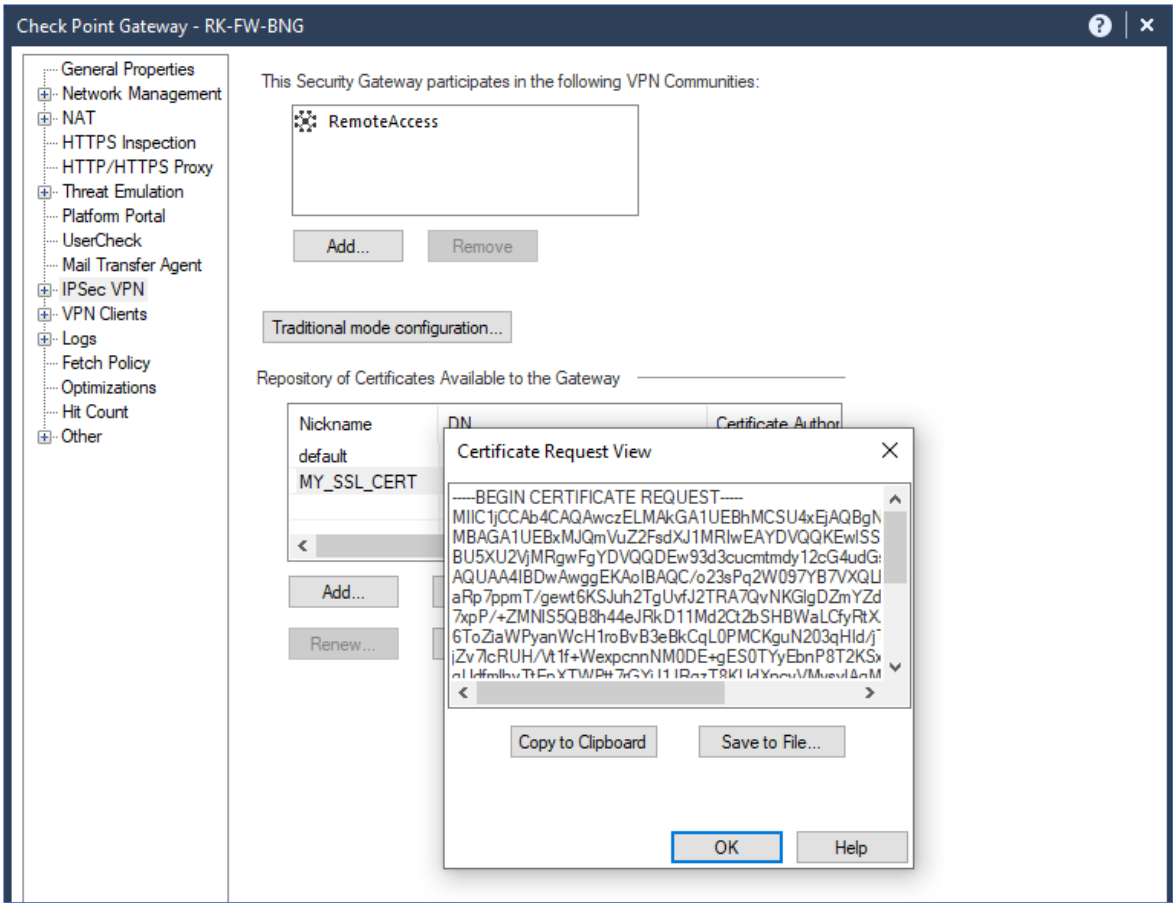
Click **OK** and a CSR is created after this.



11. Under Certificate Repository we can see our Trusted 3rd Party CA entry.

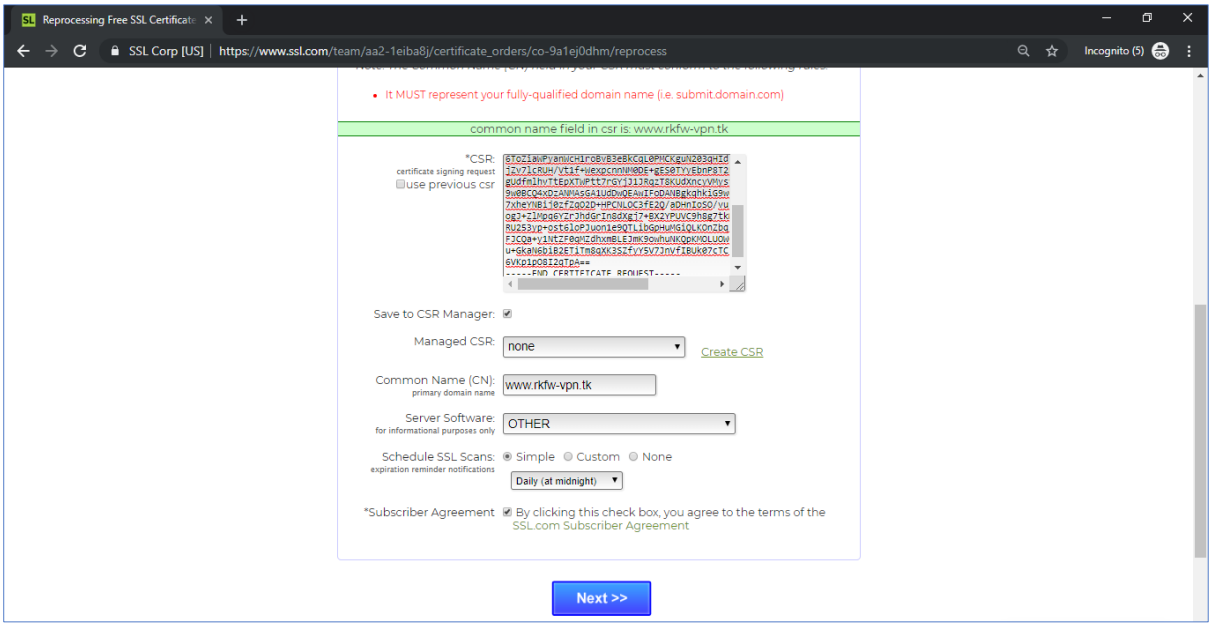


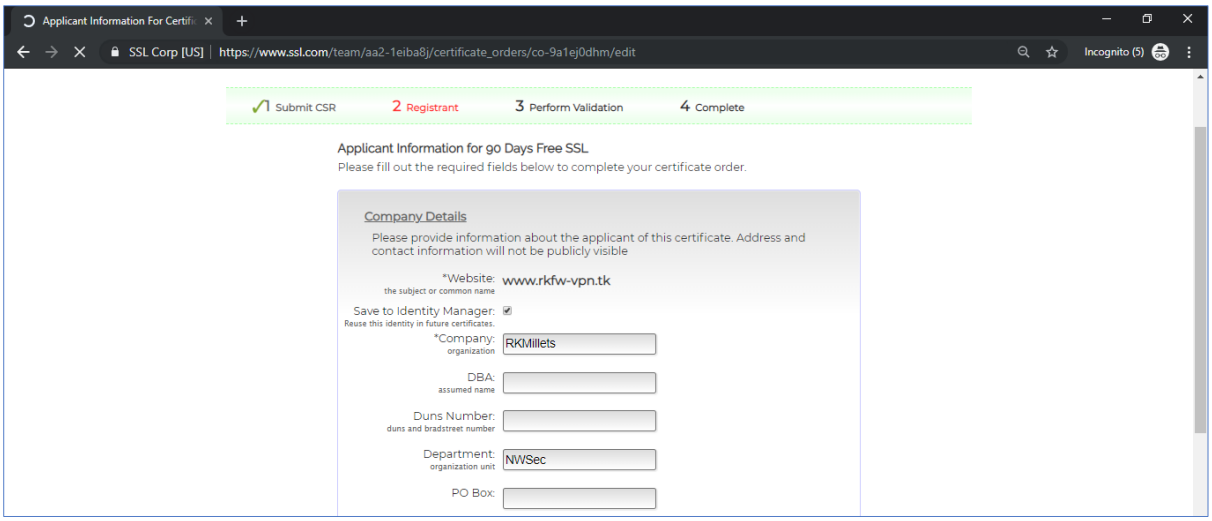
12. Click on **View** and copy the CSR content from it.

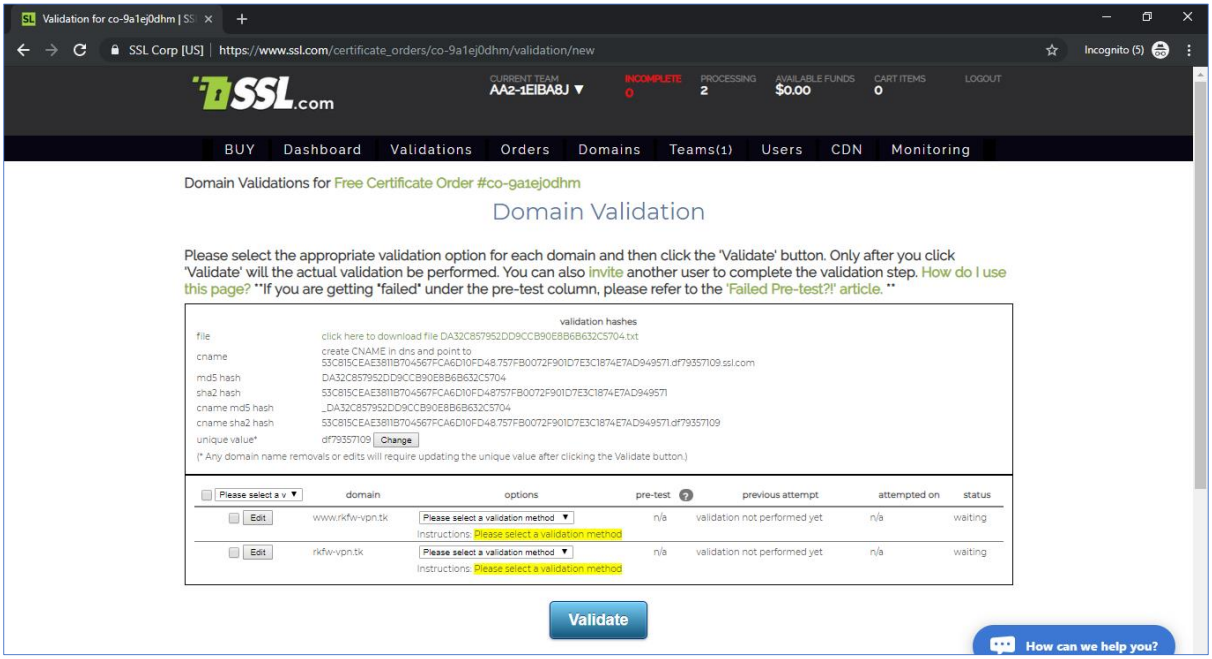


13. Purchase an SSL Certificate and provide this CSR to get an SSL Certificate for our VPN Gateway.

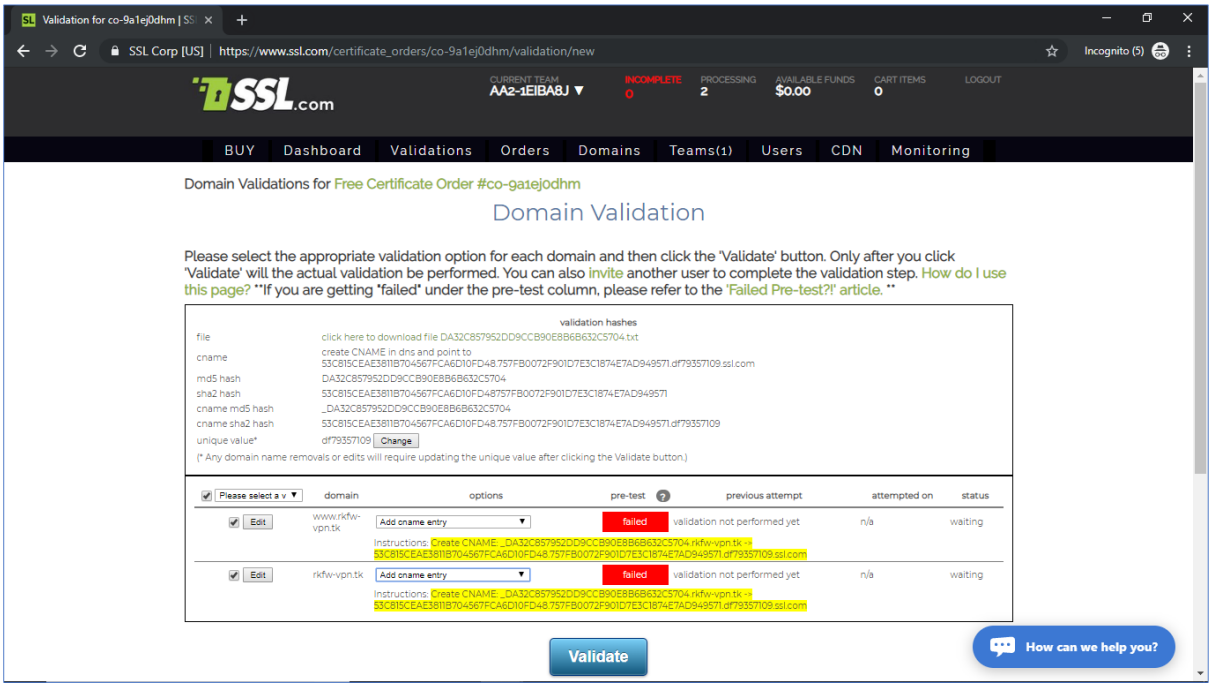
- Start the SSL Certificate wizard and paste the CSR content that we have copied previously.




Applicant Information For Certifi
SSL Corp [US] | https://www.ssl.com/team/aa2-1eiba8j/certificate_orders/co-9a1ej0dhm/edit
Incognito (5)
Submit CSR
2 Registrant
3 Perform Validation
4 Complete
Applicant Information for 90 Days Free SSL
Please fill out the required fields below to complete your certificate order.
Company Details
Please provide information about the applicant of this certificate. Address and contact information will not be publicly visible
*Website: www.rkfw-vpn.tk
the subject or common name
Save to Identity Manager:
Reuse this identity in future certificates.
*Company: RKMillets
organization
DBA:
assumed name
Duns Number:
duns and bradstreet number
Department: NWSec
organization unit
PO Box:


Validation for co-9a1ej0dhm | SS
SSL Corp [US] | https://www.ssl.com/certificate_orders/co-9a1ej0dhm/validation/new
Incognito (5)
CURRENT TEAM AA2-1EIBA8J
INCOMPLETE 0
PROCESSING 2
AVAILABLE FUNDS $0.00
CART ITEMS 0
LOGOUT
BUY
Dashboard
Validations
Orders
Domains
Teams(1)
Users
CDN
Monitoring
Domain Validations for Free Certificate Order #co-9a1ej0dhm
Domain Validation
Please select the appropriate validation option for each domain and then click the 'Validate' button. Only after you click 'Validate' will the actual validation be performed. You can also invite another user to complete the validation step. How do I use this page? **If you are getting "failed" under the pre-test column, please refer to the 'Failed Pre-test?!' article. **
validation hashes
file
click here to download file DA32C857952DD9CCB90E8B6B632C5704.txt
cname
create CNAME in dns and point to 53C815CEAE38111B704567FCA6D10FD48757FB0072F901D7E3C1874E7AD949571.df79357109.ssl.com
md5 hash
DA32C857952DD9CCB90E8B6B632C5704
sha2 hash
53C815CEAE38111B704567FCA6D10FD48757FB0072F901D7E3C1874E7AD949571
cname md5 hash
_DA32C857952DD9CCB90E8B6B632C5704
cname sha2 hash
53C815CEAE38111B704567FCA6D10FD48757FB0072F901D7E3C1874E7AD949571.df79357109
unique value*
df79357109 Change
(* Any domain name removals or edits will require updating the unique value after clicking the Validate button.)
Please select a v
domain
options
pre-test
previous attempt
attempted on
status
Edit
www.rkfw-vpn.tk
Please select a validation method
Instructions: Please select a validation method
n/a
validation not performed yet
n/a
waiting
Edit
rkfw-vpn.tk
Please select a validation method
Instructions: Please select a validation method
n/a
validation not performed yet
n/a
waiting
Validate
How can we help you?

- We will do the domain validation for ***rkfw-vpn.tk*** domain using the DNS CNAME record method.

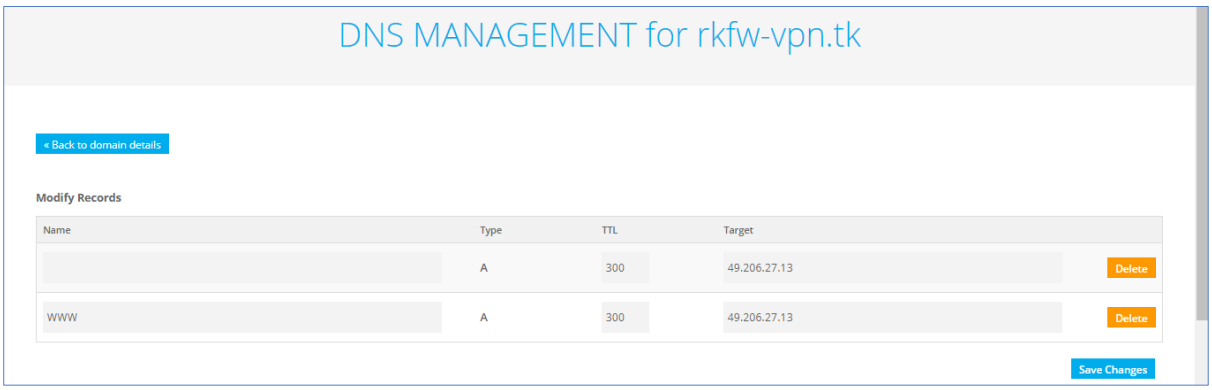


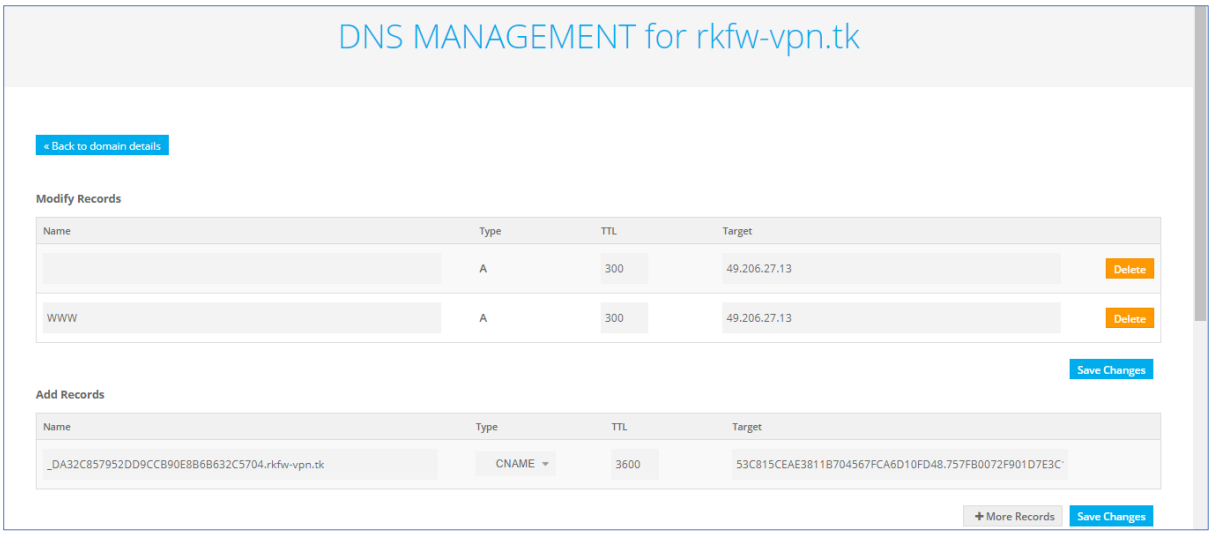
- Define a CNAME record on our DNS Server pointing to the ***SSL.COM*** domain. Meaning point the CNAME

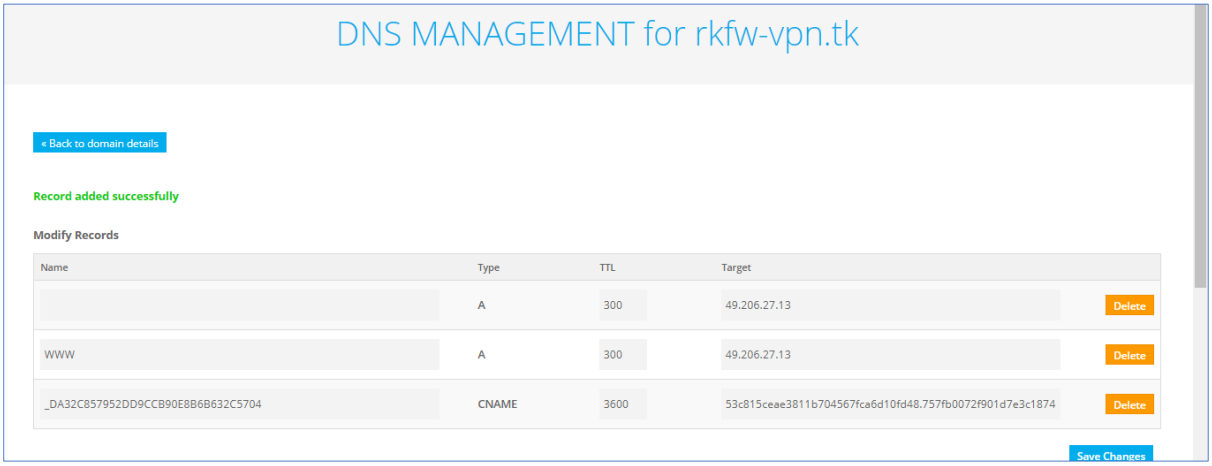
  `_DA32C857952DD9CCB90E8B6B632C5704.rkfw-vpn.tk`

  to

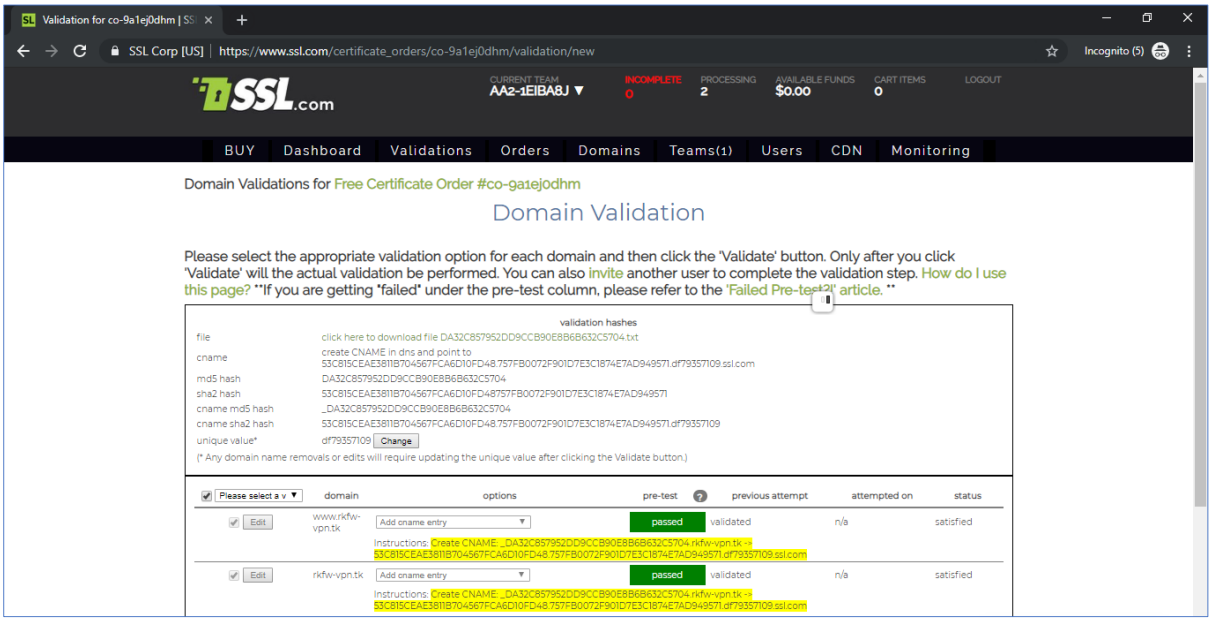
  `53C815CEAE3811B704567FCA6D10FD48.757FB0072F901D7E3C1874E7AD949571.df79357109.ssl.com`

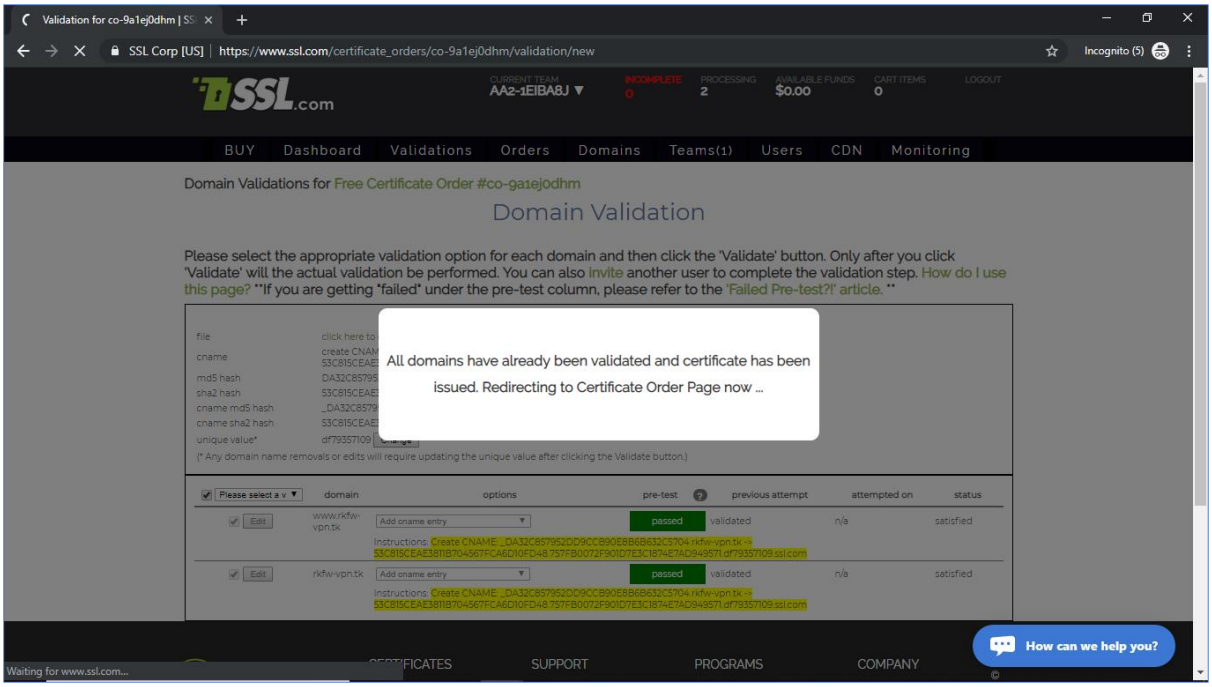


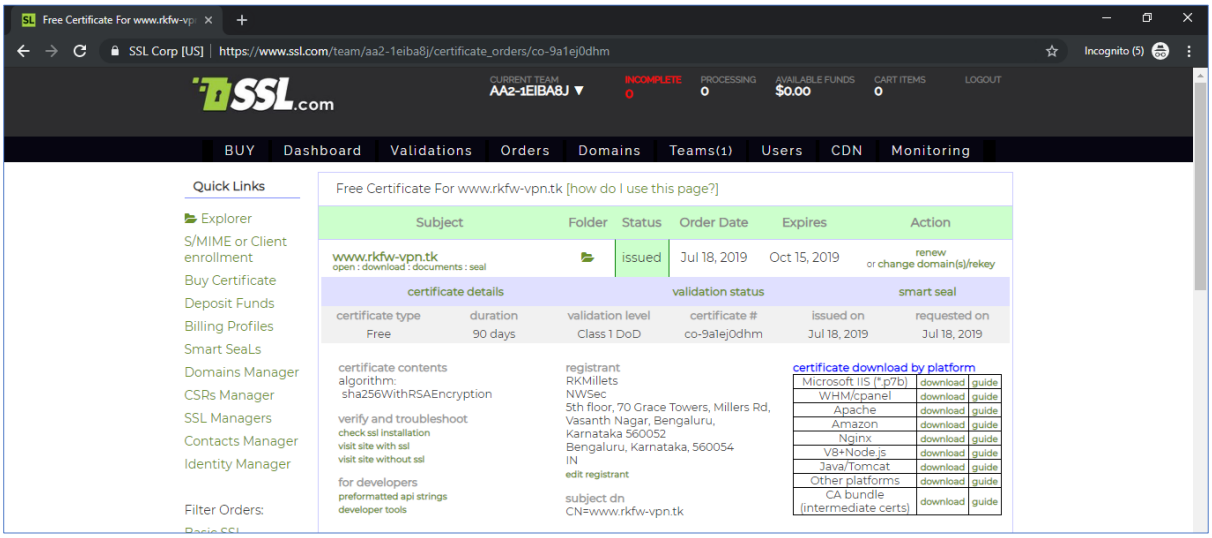




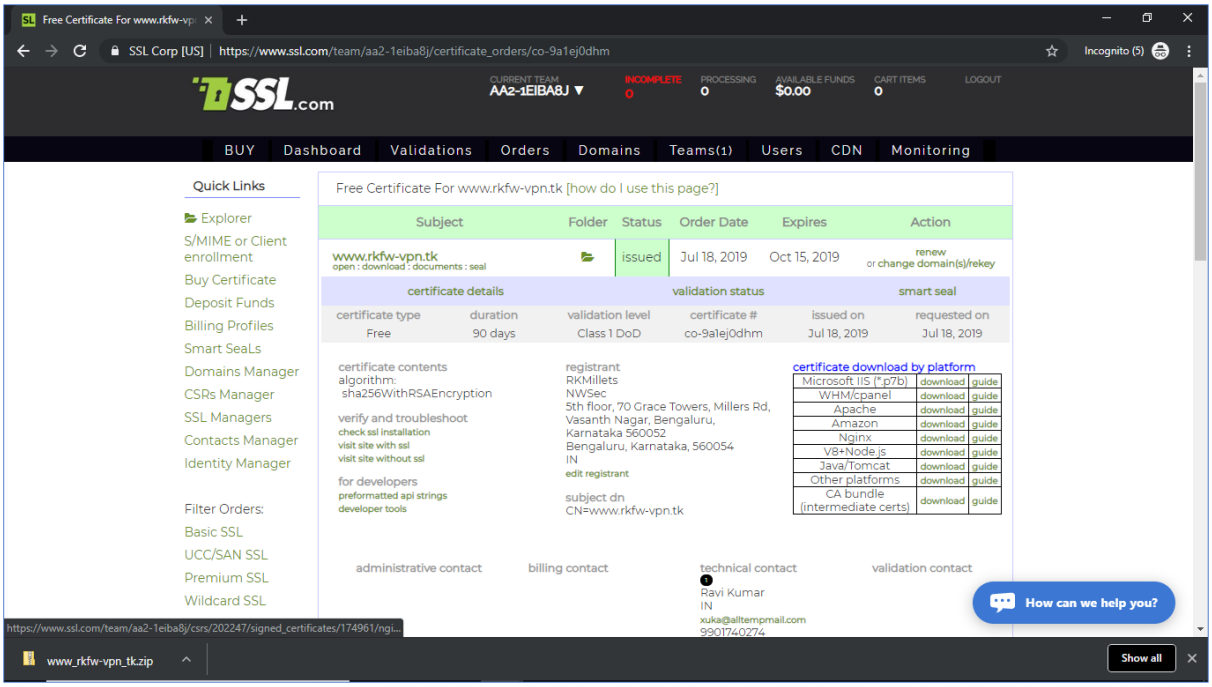
- Once we add a CNAME record, the domain validation of the SSL.com will pass.

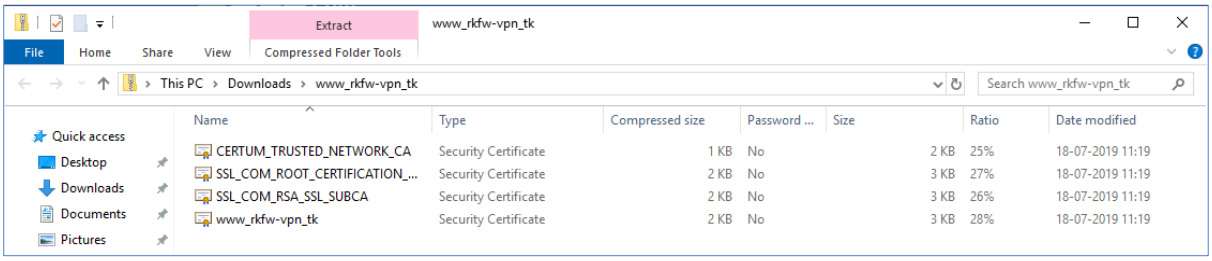



Validation for co-9a1ej0dhm | SS
SSL Corp [US] | https://www.ssl.com/certificate_orders/co-9a1ej0dhm/validation/new
Incognito (5)
CURRENT TEAM AA2-1EIBA8J
INCOMPLETE 0
PROCESSING 2
AVAILABLE FUNDS $0.00
CART ITEMS 0
LOGOUT
BUY Dashboard Validations Orders Domains Teams(1) Users CDN Monitoring
Domain Validations for Free Certificate Order #co-ga1ej0dhm
Domain Validation
Please select the appropriate validation option for each domain and then click the 'Validate' button. Only after you click 'Validate' will the actual validation be performed. You can also invite another user to complete the validation step. How do I use this page? **If you are getting "failed" under the pre-test column, please refer to the 'Failed Pre-test?!' article. **
All domains have already been validated and certificate has been issued. Redirecting to Certificate Order Page now ...
file
cname
md5 hash
sha2 hash
cname md5 hash
cname sha2 hash
unique value*
(* Any domain name removals or edits will require updating the unique value after clicking the Validate button.)
Please select a v
domain
options
pre-test
previous attempt
attempted on
status
Edit
www.rkfw-vpn.tk
rkfw-vpn.tk
Add cname entry
passed
validated
n/a
satisfied
Instructions: Create CNAME: _DA32C857952DD9CCB90E8B6B632C5704.rkfw-vpn.tk -> 53C815CEAE3811B704567FCA6D10FD48.757FB0072F901D7E3C1874E7AD949571.df79357109.ssl.com
How can we help you?
CERTIFICATES
SUPPORT
PROGRAMS
COMPANY
Waiting for www.ssl.com...

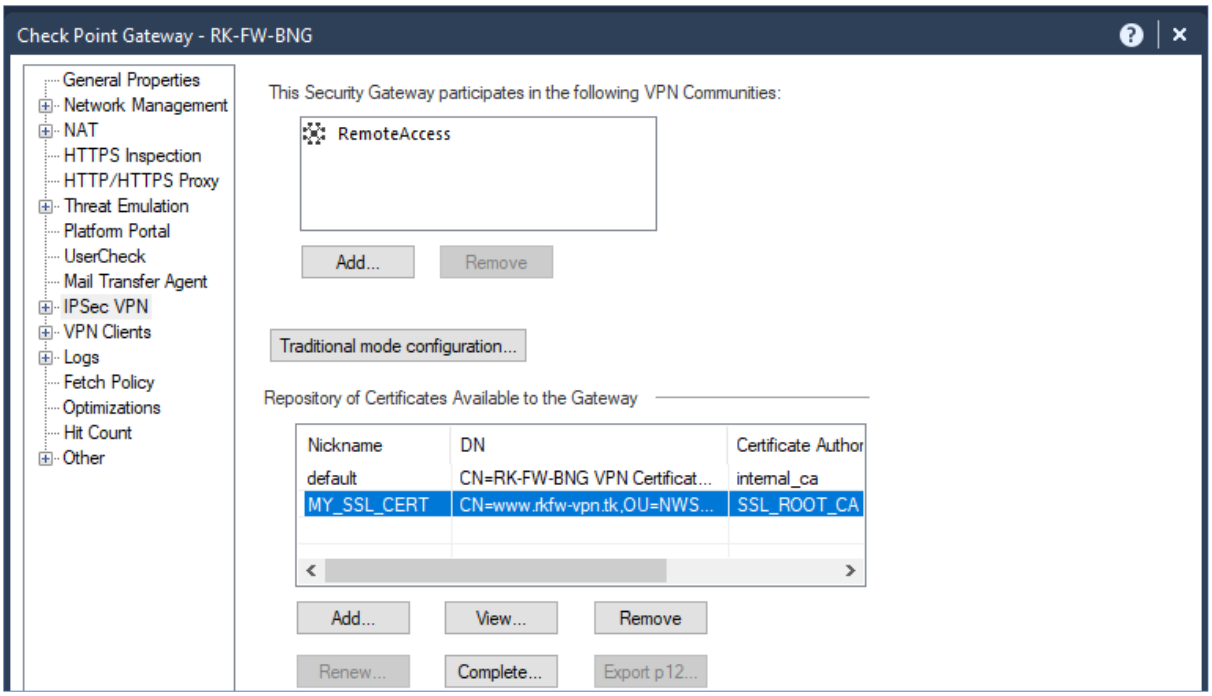

Free Certificate For www.rkfw-vp
SSL Corp [US] | https://www.ssl.com/team/aa2-1eiba8j/certificate_orders/co-9a1ej0dhm
Incognito (5)
CURRENT TEAM AA2-1EIBA8J
INCOMPLETE 0
PROCESSING 0
AVAILABLE FUNDS $0.00
CART ITEMS 0
LOGOUT
BUY Dashboard Validations Orders Domains Teams(1) Users CDN Monitoring
Quick Links
Explorer
S/MIME or Client enrollment
Buy Certificate
Deposit Funds
Billing Profiles
Smart SeaLs
Domains Manager
CSRs Manager
SSL Managers
Contacts Manager
Identity Manager
Filter Orders:
Free Certificate For www.rkfw-vpn.tk [how do I use this page?]
Subject
Folder
Status
Order Date
Expires
Action
www.rkfw-vpn.tk
open : download : documents : seal
issued
Jul 18, 2019
Oct 15, 2019
renew
or change domain(s)/rekey
certificate details
validation status
smart seal
certificate type
duration
validation level
certificate #
issued on
requested on
Free
90 days
Class 1 DoD
co-9a1ej0dhm
Jul 18, 2019
Jul 18, 2019
certificate contents
algorithm:
sha256WithRSAEncryption
verify and troubleshoot
check ssl installation
visit site with ssl
visit site without ssl
for developers
preformatted api strings
developer tools
registrant
RKMillets
NWSec
5th floor, 70 Grace Towers, Millers Rd,
Vasanth Nagar, Bengaluru,
Karnataka 560052
Bengaluru, Karnataka, 560054
IN
edit registrant
subject dn
CN=www.rkfw-vpn.tk
certificate download by platform
Microsoft IIS (*.p7b) download guide
WHM/cpanel download guide
Apache download guide
Amazon download guide
Nginx download guide
V8+Node.js download guide
Java/Tomcat download guide
Other platforms download guide
CA bundle (intermediate certs) download guide

14. Now, Download the SSL Certificate for our VPN Gateway domain.

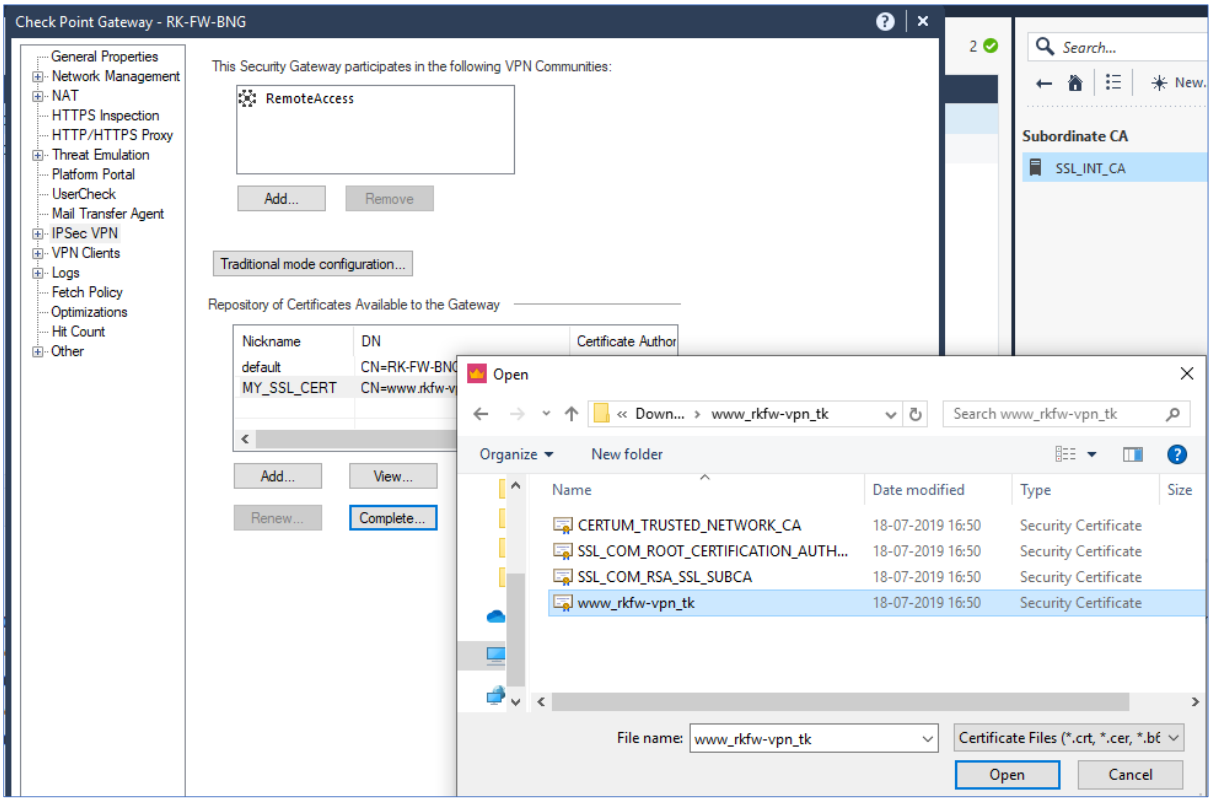




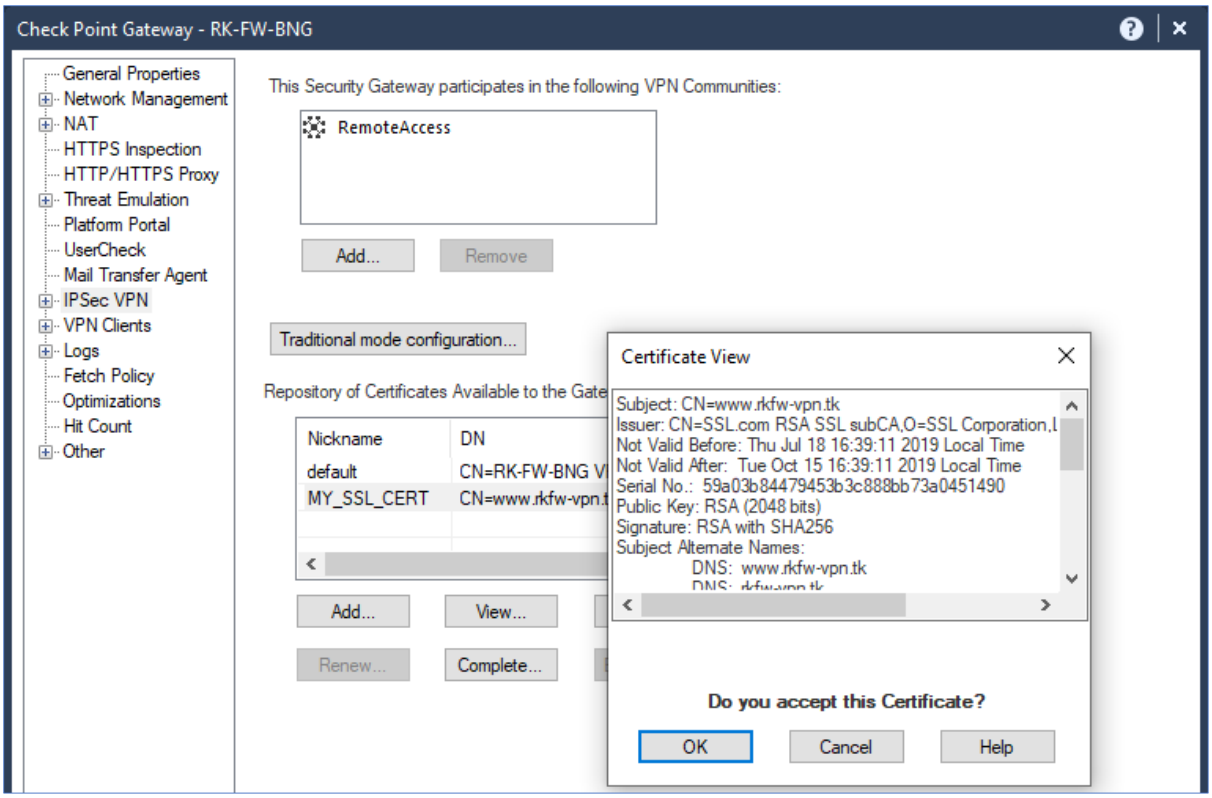
15. Go back to the VPN Gateway Object and IPSec VPN section. Select the Trusted 3rd Party CA that we have added.



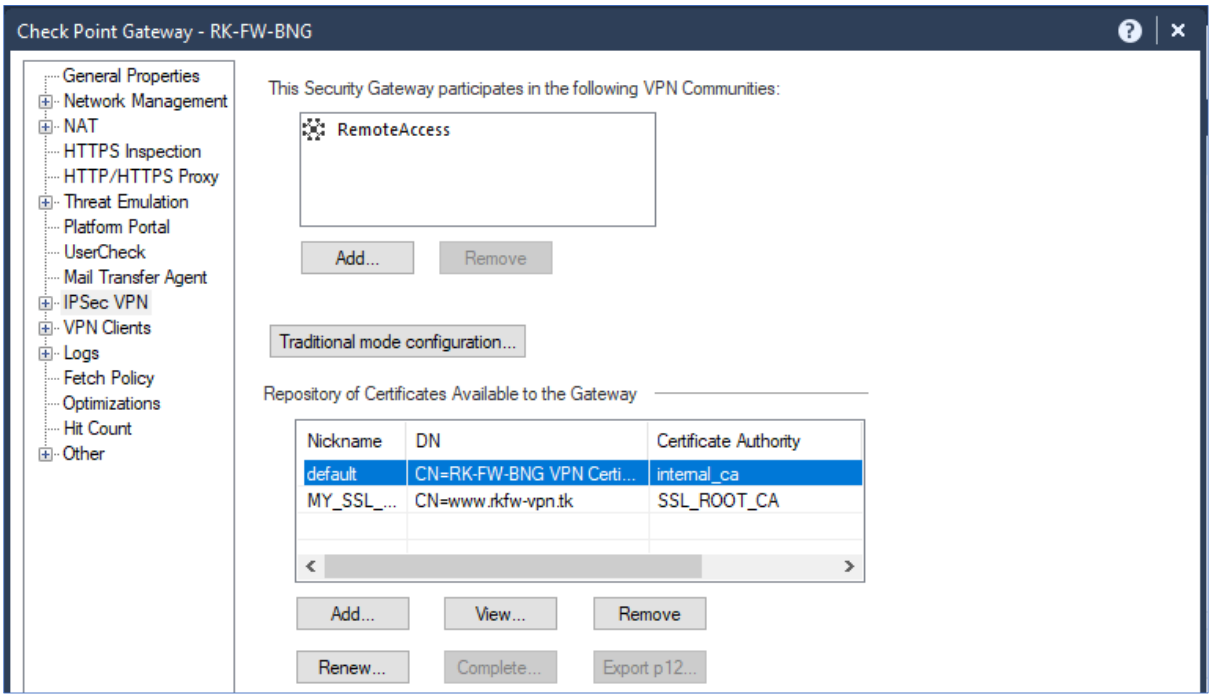
16. Click on **Complete,** and upload the domain certificate (***www.rkfw-vpn.tk***) that we downloaded from the ***SSL.com CA.***

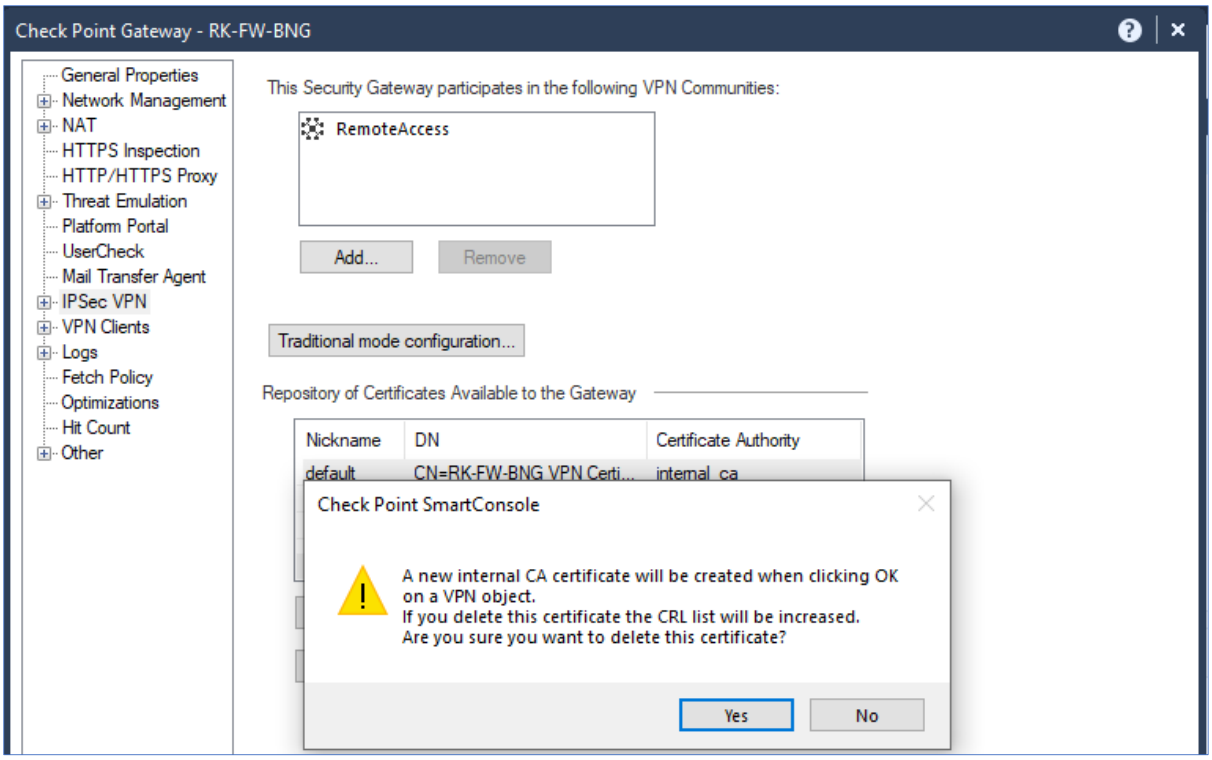


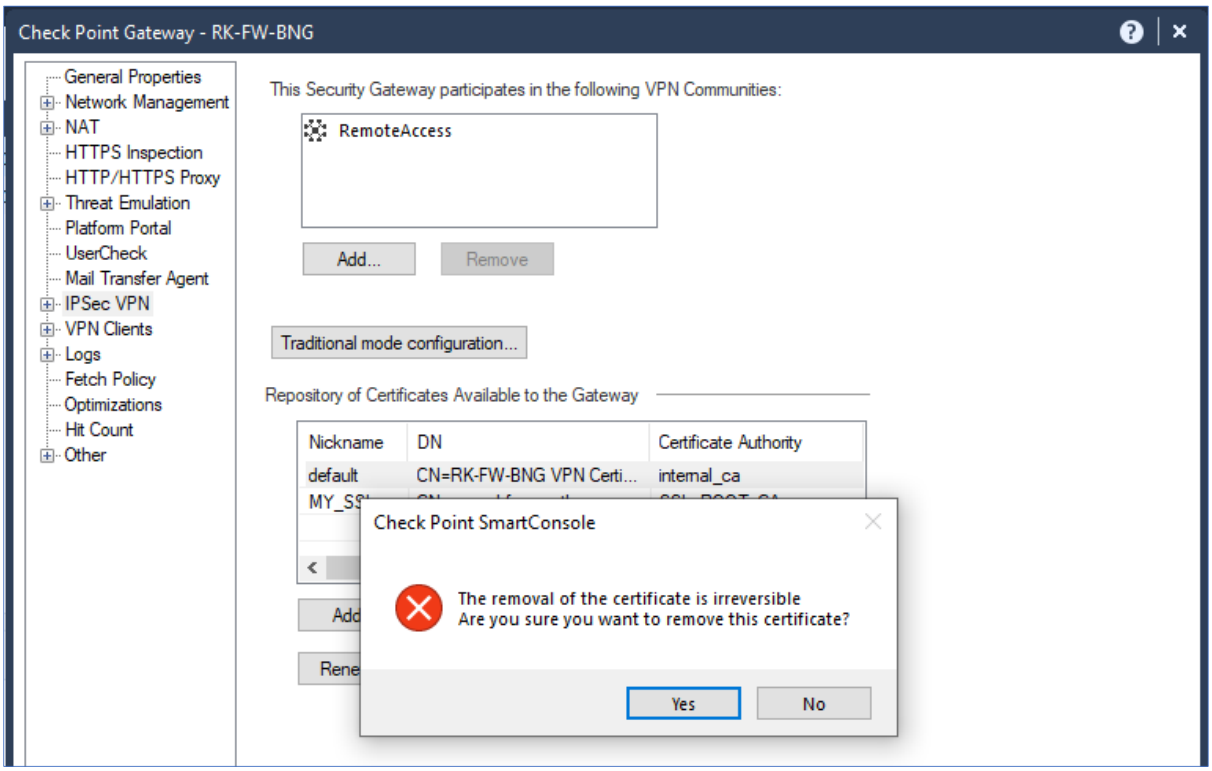
Accept the trusted domain certificate for our VPN Gateway.

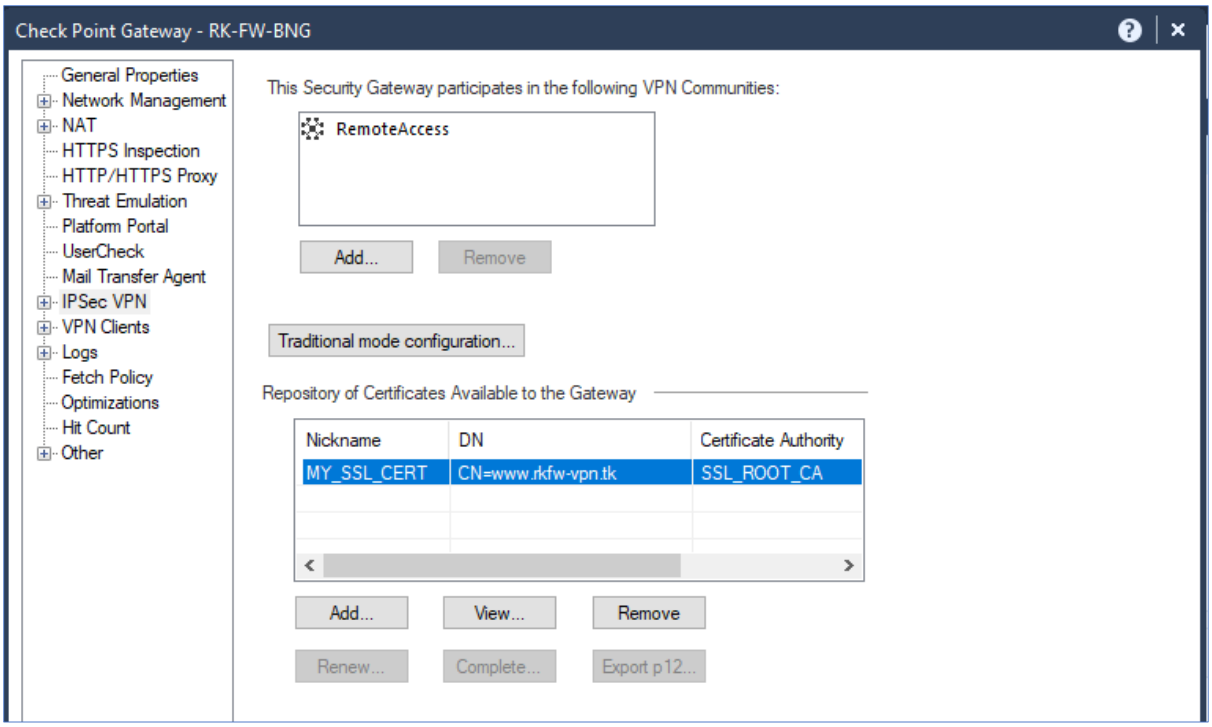


17. We can delete the ***Default Self-Signed VPN Certificate*** to make use of our Trusted CA SSL Certificate. For any future Certificate based S2S VPN communication, this certificate will be used which can be trusted by the ***Peer End VPN Gateway***.

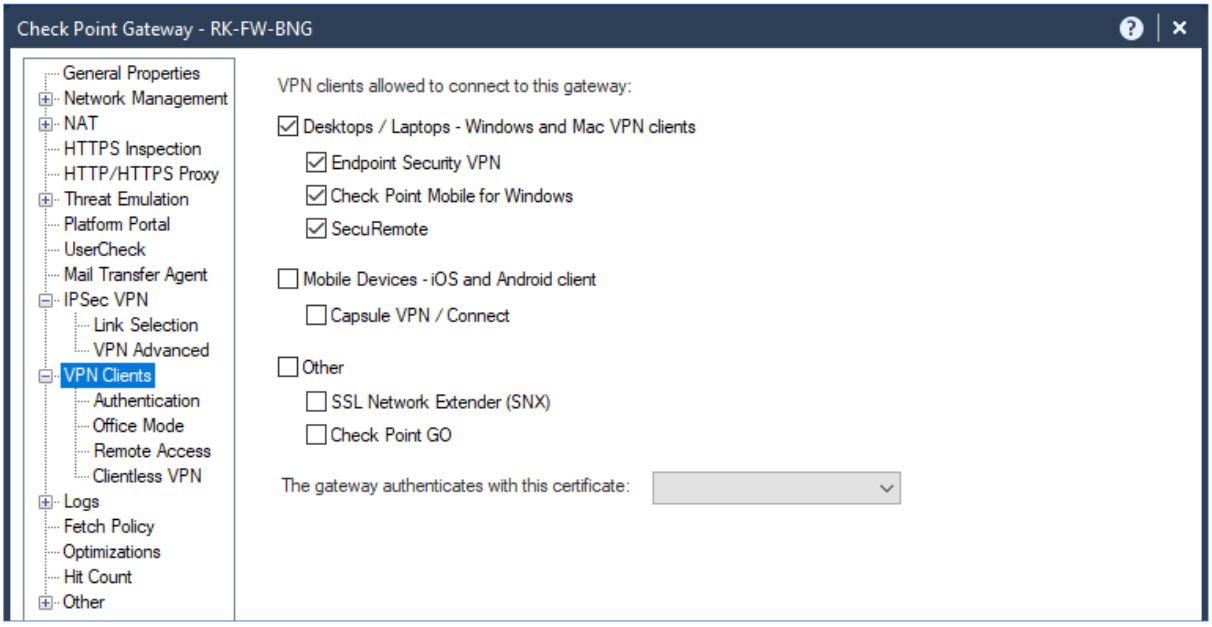


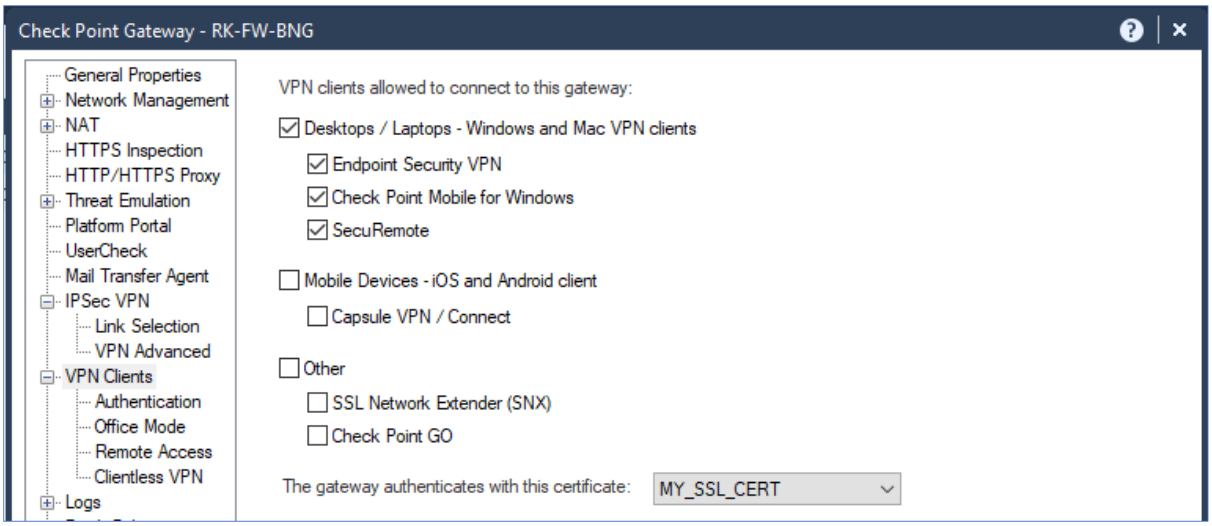

Check Point Gateway - RK-FW-BNG
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Threat Emulation
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other
This Security Gateway participates in the following VPN Communities:
RemoteAccess
Add...
Remove
Traditional mode configuration...
Repository of Certificates Available to the Gateway
Nickname
DN
Certificate Authority
default
CN=RK-FW-BNG VPN Certi...
internal_ca
Check Point SmartConsole
A new internal CA certificate will be created when clicking OK on a VPN object.
If you delete this certificate the CRL list will be increased.
Are you sure you want to delete this certificate?
Yes
No


Check Point Gateway - RK-FW-BNG
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Threat Emulation
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other
This Security Gateway participates in the following VPN Communities:
RemoteAccess
Add...
Remove
Traditional mode configuration...
Repository of Certificates Available to the Gateway
Nickname
DN
Certificate Authority
default
CN=RK-FW-BNG VPN Certi...
internal_ca
Check Point SmartConsole
The removal of the certificate is irreversible
Are you sure you want to remove this certificate?
Yes
No

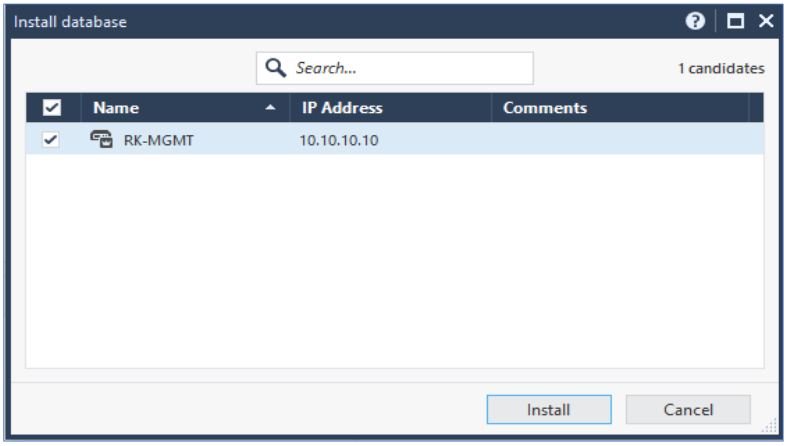


18. Under **VPN Clients** section, Select our certificate.

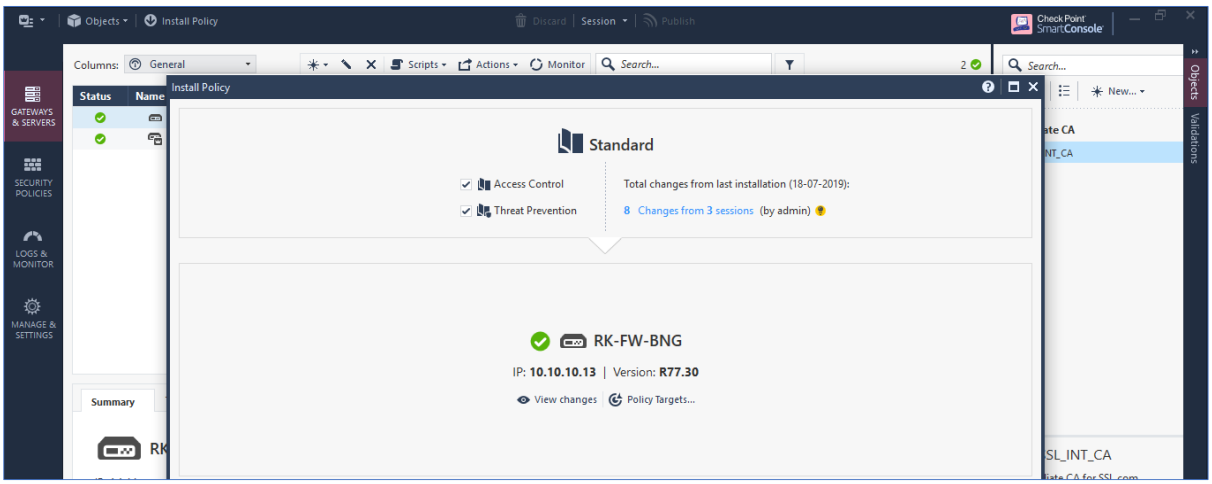




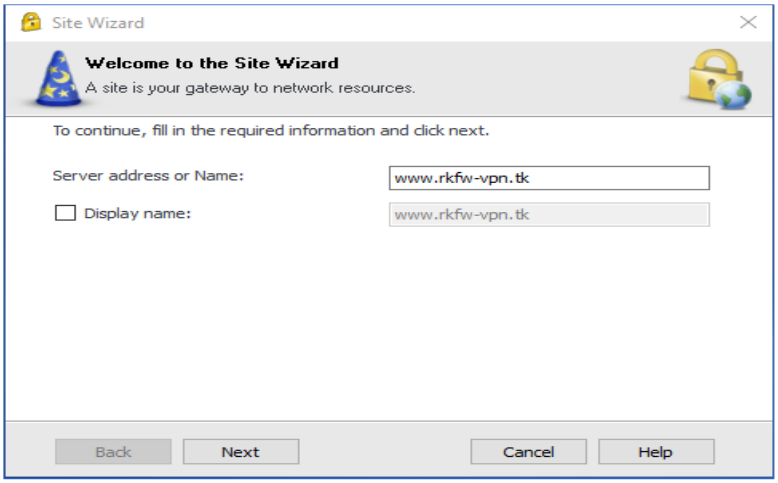
19. Install the database on the Management Server.

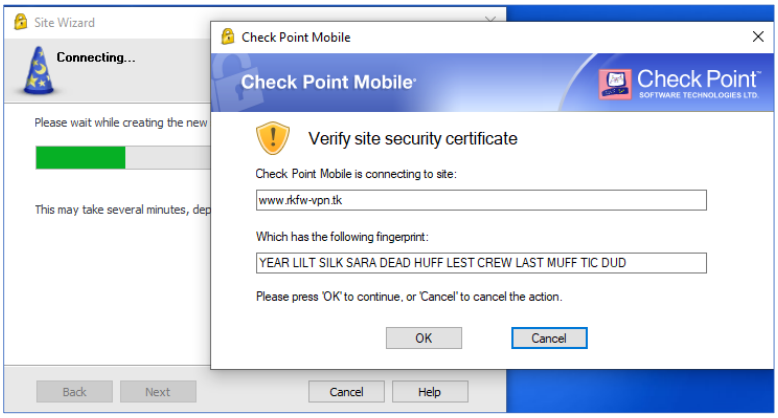


20. Install the Policy on our VPN Gateway.



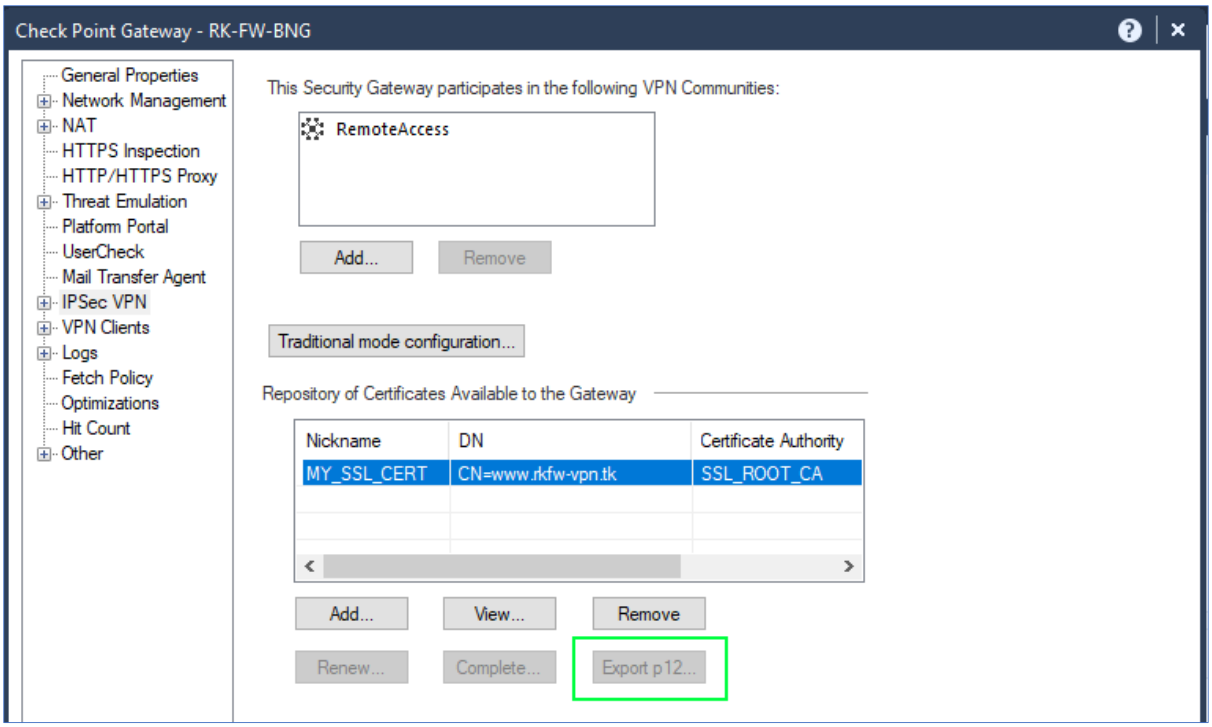
21. Now, access the VPN Gateway using the RA VPN Client,





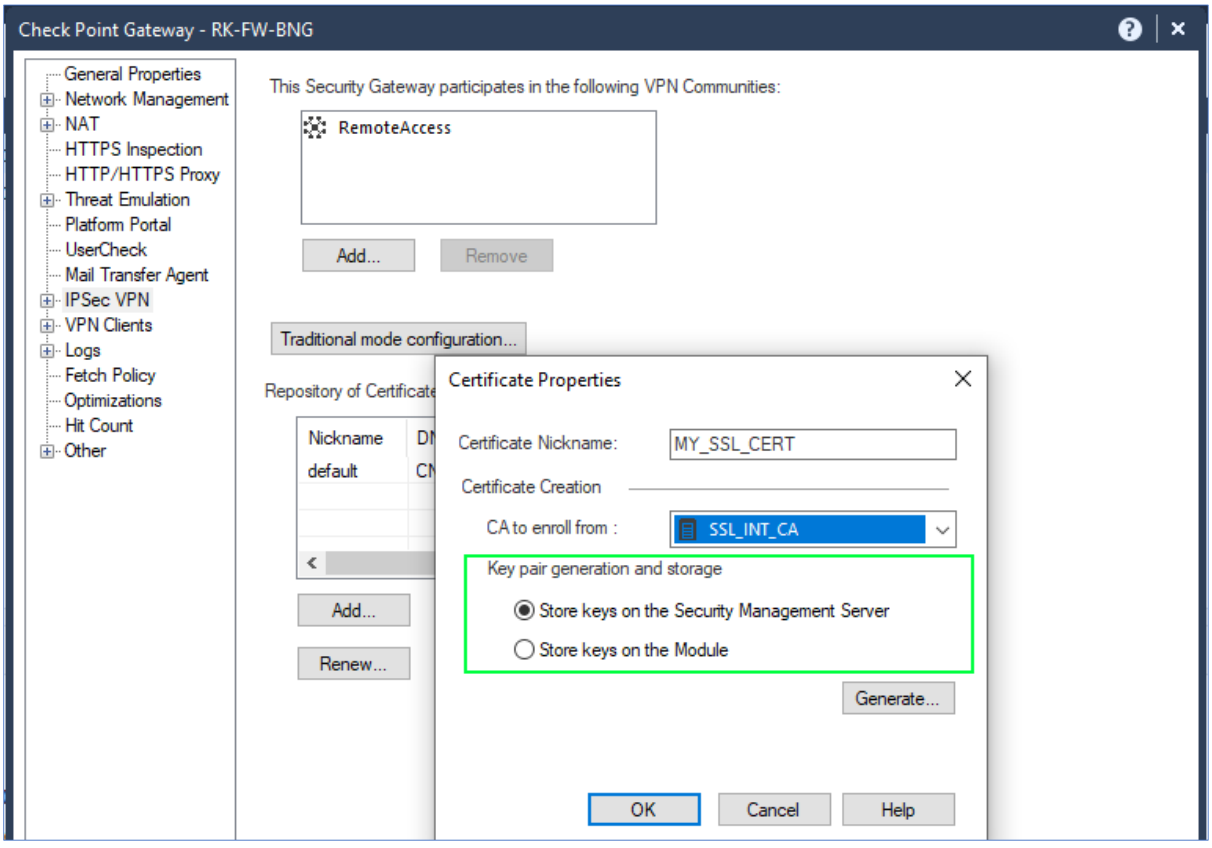
Unlike the previous attempt, we won't get Certificate Warning because of the mapping of our Trusted 3rd Party CA SSL Certificate which our Operating System or Browser trusts.

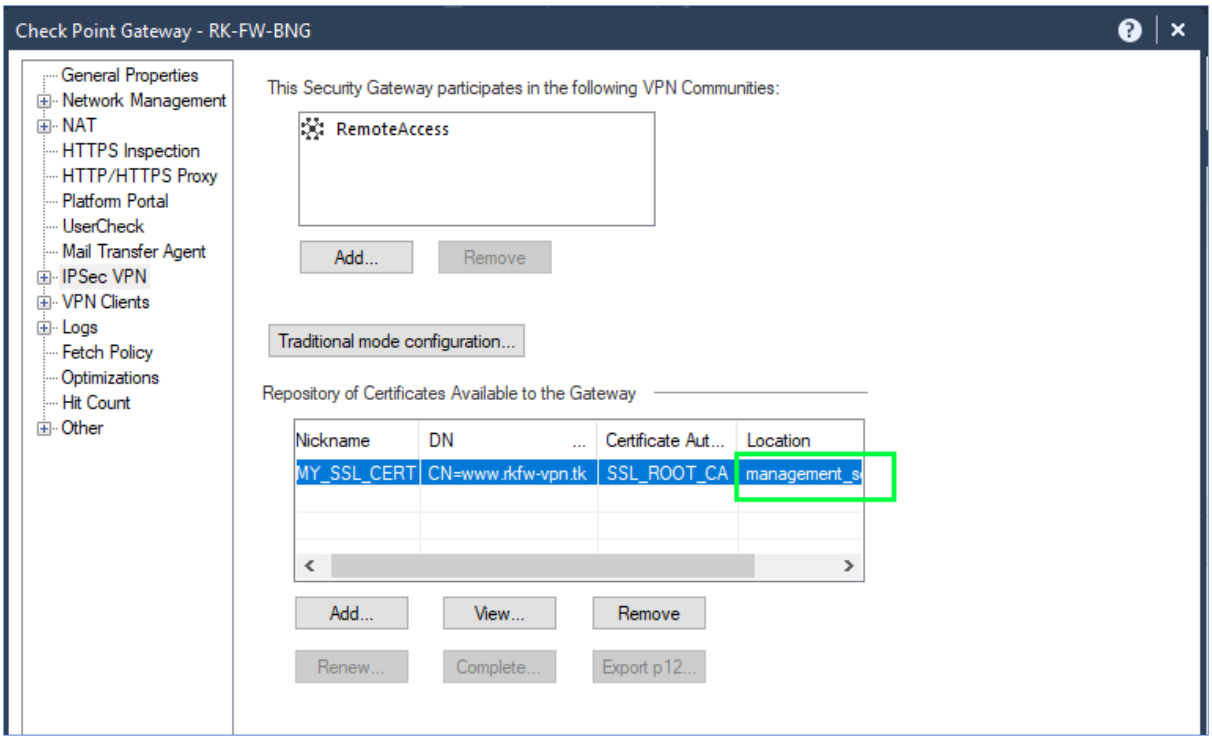
22. You can use this trusted 3rd party SSL Certificate which is mapped to our domain (www.rkfw-vpn.tk) for other Check Point features like SSL VPN, Gaia Portal. But on the SmartConsole the option to export this certificate is greyed-out (reason unknown) under IPSec VPN section of VPN Gateway.



23. We have an alternative for this concern – ***export_p12*** command.

- If you remember while generating the CSR using our trusted CA's, we chose an option to store our keys on the Management Server & our trusted CA certificate too resides on the Management Server.



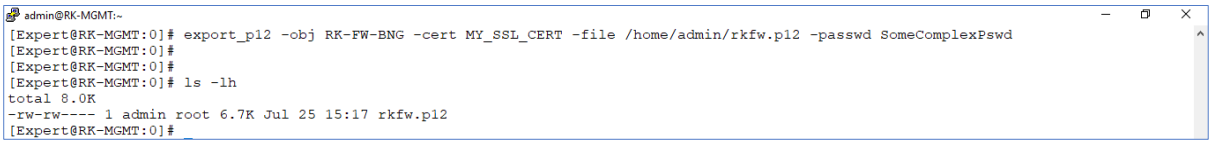


- So, take the SSH to Management Server which is managing the VPN Gateway and run the ***export_p12*** command, whose Syntax goes like this:

```
# export_p12 -obj <Name_of_GW_Object> -cert <NickName_of_CA_Repository> -
file <Name_of_Output_P12_File.p12> -passwd
<Password_to_Open_Output_P12_File>
```

In our case it is:

```
# export_p12 -obj RK-FW-BNG -cert MY_SSL_CERT -file /home/admin/rkfw.p12 -
passwd SomeComplexPswd
```

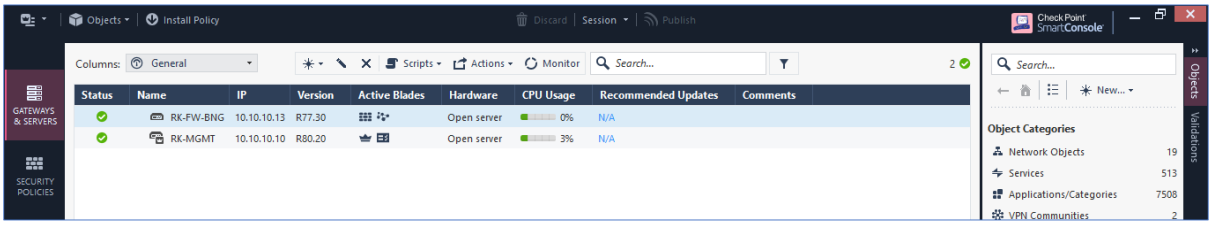


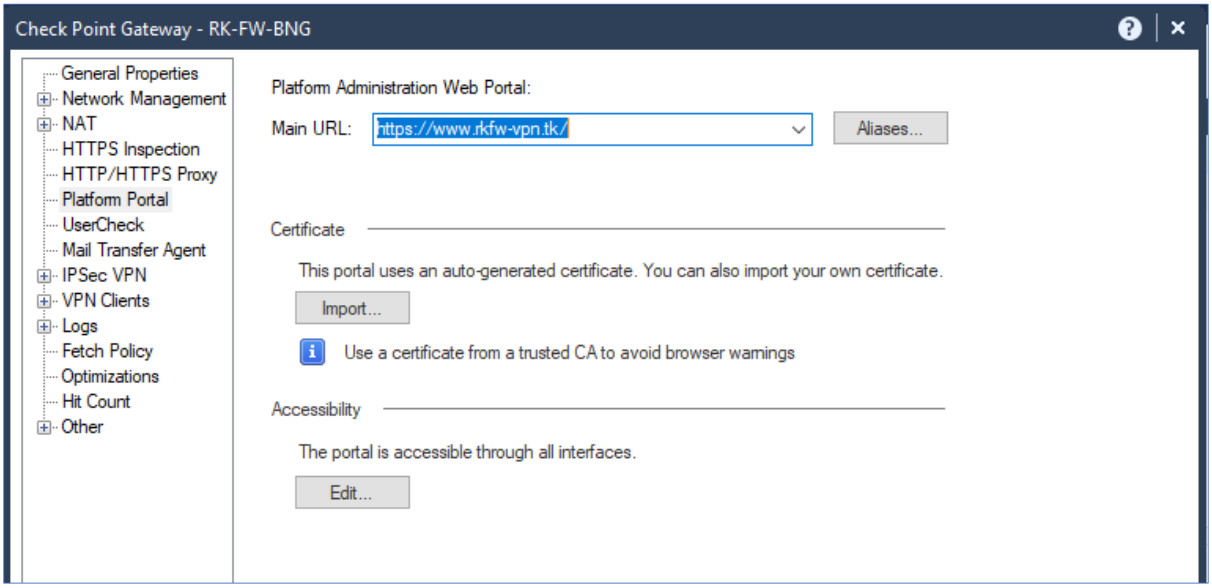
- Copy the output ***.p12*** certificate file and use it on the other Check Point features.

SSL Certificate for Gaia Portal

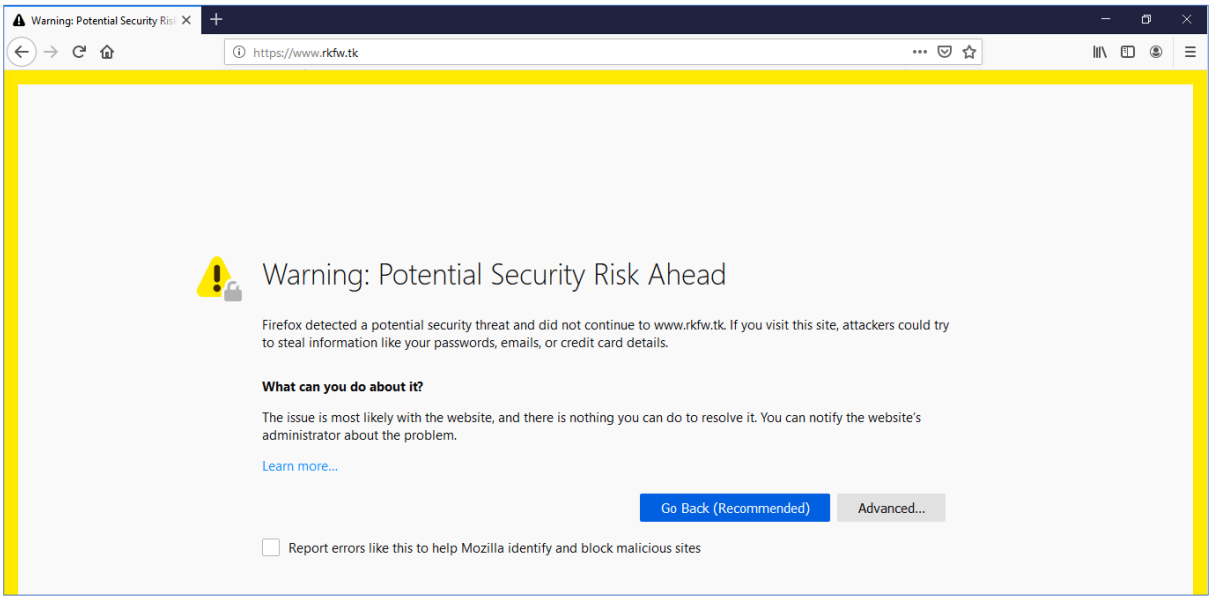
Note: If you have the trusted 3rd party CA SSL Certificate for VPN feature then go to step 16.

1. Our Gateway is defined with a domain name ***www.rkfw.tk*.**





2. While accessing the Gaia Portal we get a Browser warning on the device **Self-Signed SSL Certificate**, which is stored in the ***/web/conf*** directory of this device.



```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# ls -lh /web/conf/
total 88K
drwxr-xr-x 2 admin root 4.0K Jul 11 18:22 extra
-rw-r--r-- 1 admin root  20K Jul 24 17:58 httpd2.conf
-rw-r--r-- 1 admin root  18K Jul 11 17:30 httpd2.conf.backup
-rw-r--r-- 1 admin root  433 Jul 24 19:11 httpd2_mp.conf
-rwsr-xr-x 1 admin root  22K Jul 11 17:30 login
lrwxrwxrwx 1 admin root   46 Jul 11 17:30 mime.types -> /web/cpshared/web/Apache/2.2.0/conf/mime.types
-rw-r----- 1 admin root 8.2K Jul 11 15:11 server.crt
-rw-r----- 1 admin root 1.7K Jul 11 15:04 server.key
[Expert@RK-FW-BNG:0]#
```

3. If we want to avoid such warnings then map an SSL Certificate to our Gateway's Gaia Portal. Getting an SSL Certificate for the Gateway involves the same steps as like a Web Server.

4. In Check Point we have a port of **OPENSSL** tool which we call it **CPOPENSSL**.

5. Generate the CSR & a Private Key using **CPOPENSSL** tool in any directory (say ***/home/admin***).

 # cpopenssl req -new -newkey rsa:2048 -nodes -out *<A_CSR_File>* -keyout *<A_Private_Key>* -config $CPDIR/conf/openssl.cnf

<u>In our case:</u>

 # cpopenssl req -new -newkey rsa:2048 -nodes -out *rkfw.csr* -keyout *rkfw.key* -config $CPDIR/conf/openssl.cnf

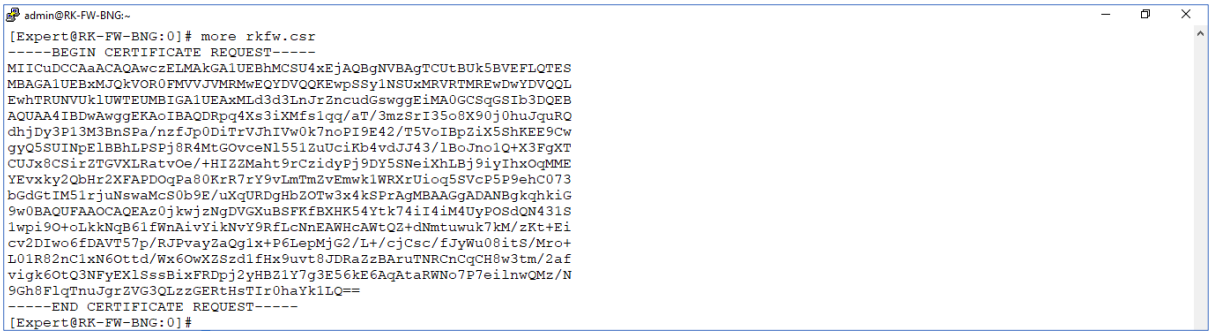
Provide the CSR details such as the CN or Domain Name, in our case let's consider ***www.rkfw.tk***

```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# cpopenssl req -new -newkey rsa:2048 -nodes -out rkfw.csr -keyout rkfw.key -config $CPDIR/conf/openssl.cnf
Generating a 2048 bit RSA private key
.....................................................................+++
.............................+++
writing new private key to 'rkfw.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:KARNATAKA
Locality Name (eg, city) []:BENGALURU
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RK-MILLETS
Organizational Unit Name (eg, section) []:SECURITY
Common Name (eg, your name or your server's hostname) []:www.rkfw.tk
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[Expert@RK-FW-BNG:0]#
```

6. Output of the above CPOPENSSL Command will be a CSR file & Private Key file.

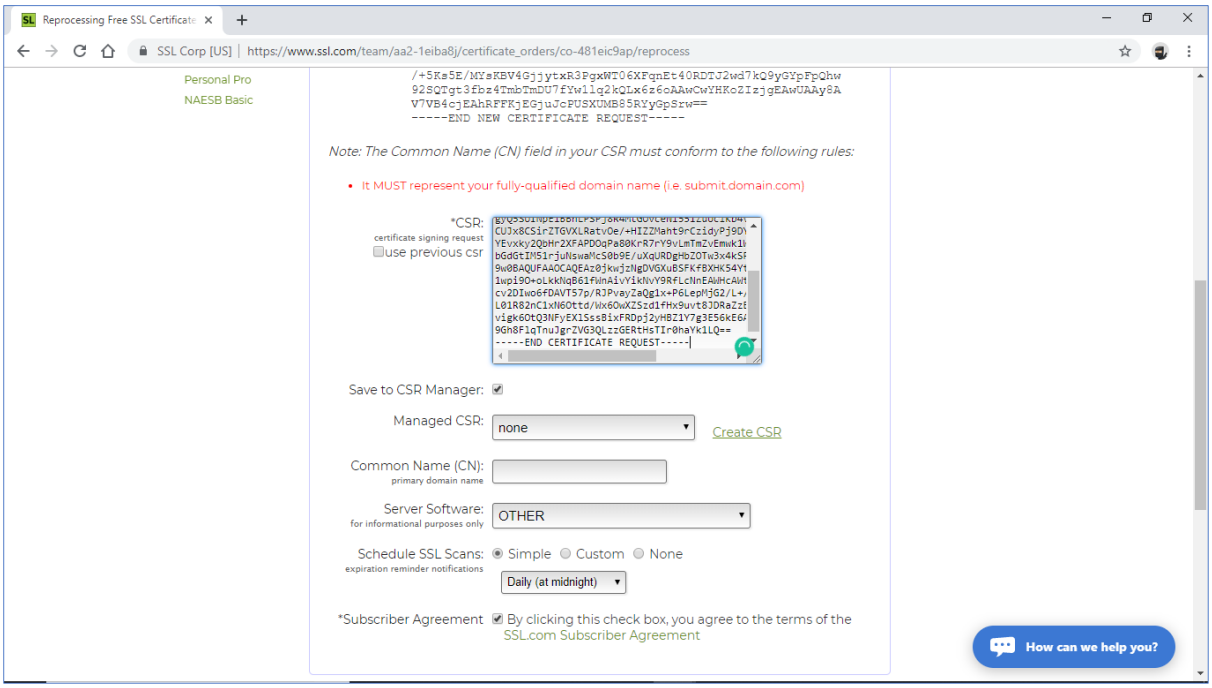
```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# ls -lh
total 8.0K
-rw-rw---- 1 admin root 1021 Jul 24 19:14 rkfw.csr
-rw-rw---- 1 admin root 1.7K Jul 24 19:14 rkfw.key
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# pwd
/home/admin
[Expert@RK-FW-BNG:0]#
```

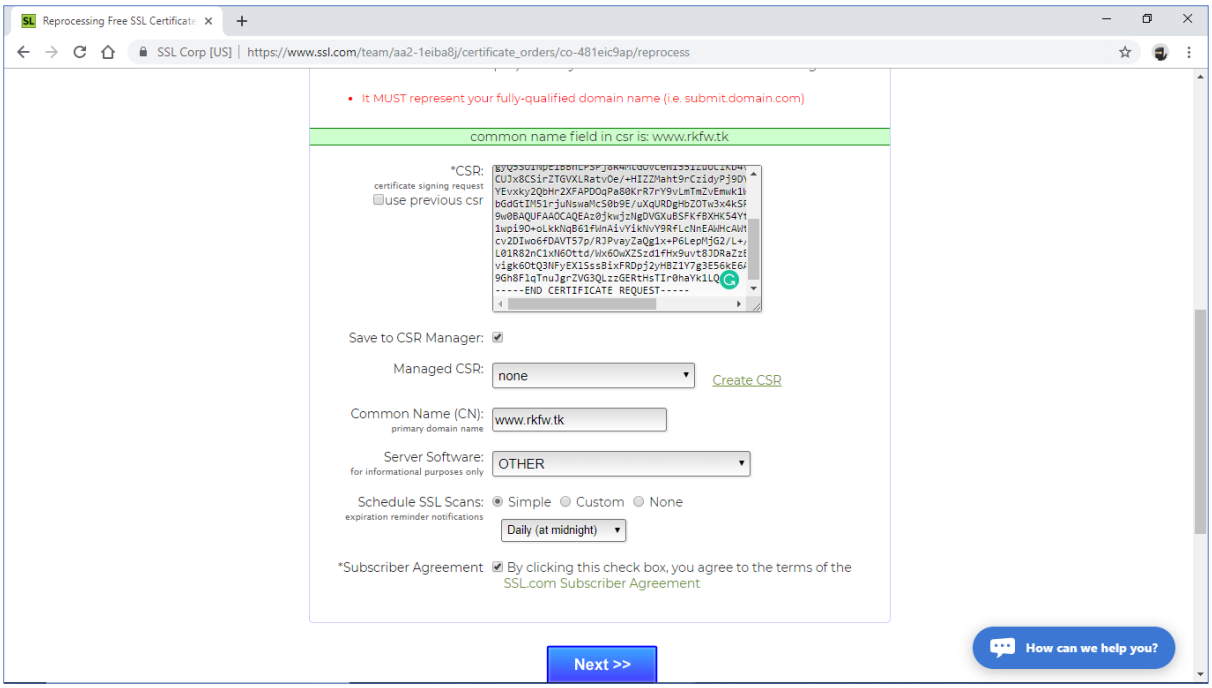
7. Copy the CSR file (***rkfw.csr***) content.

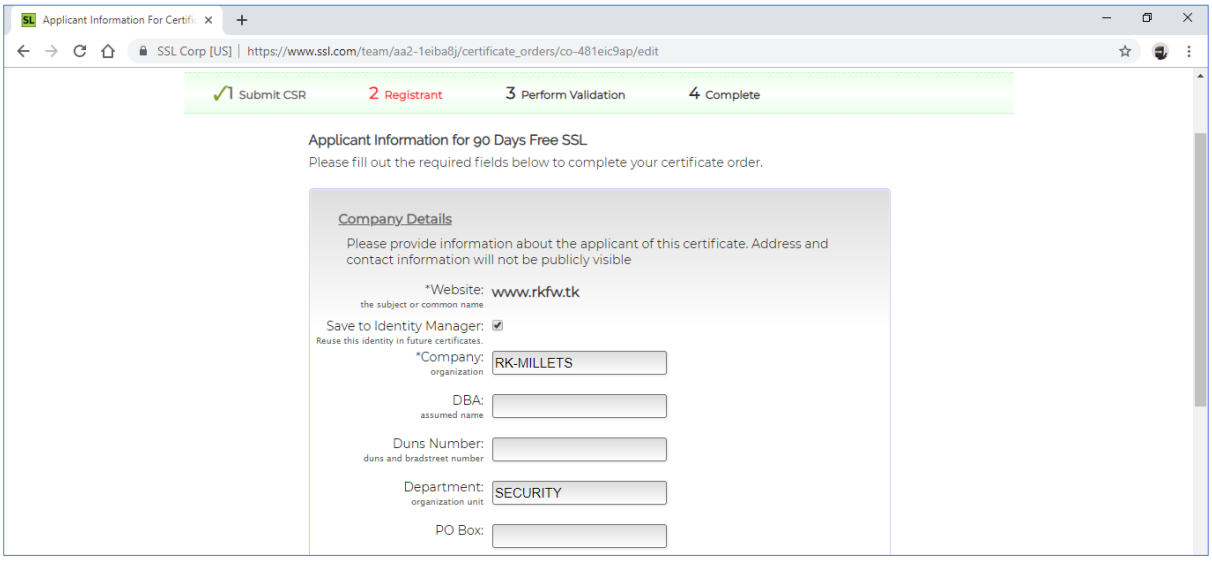


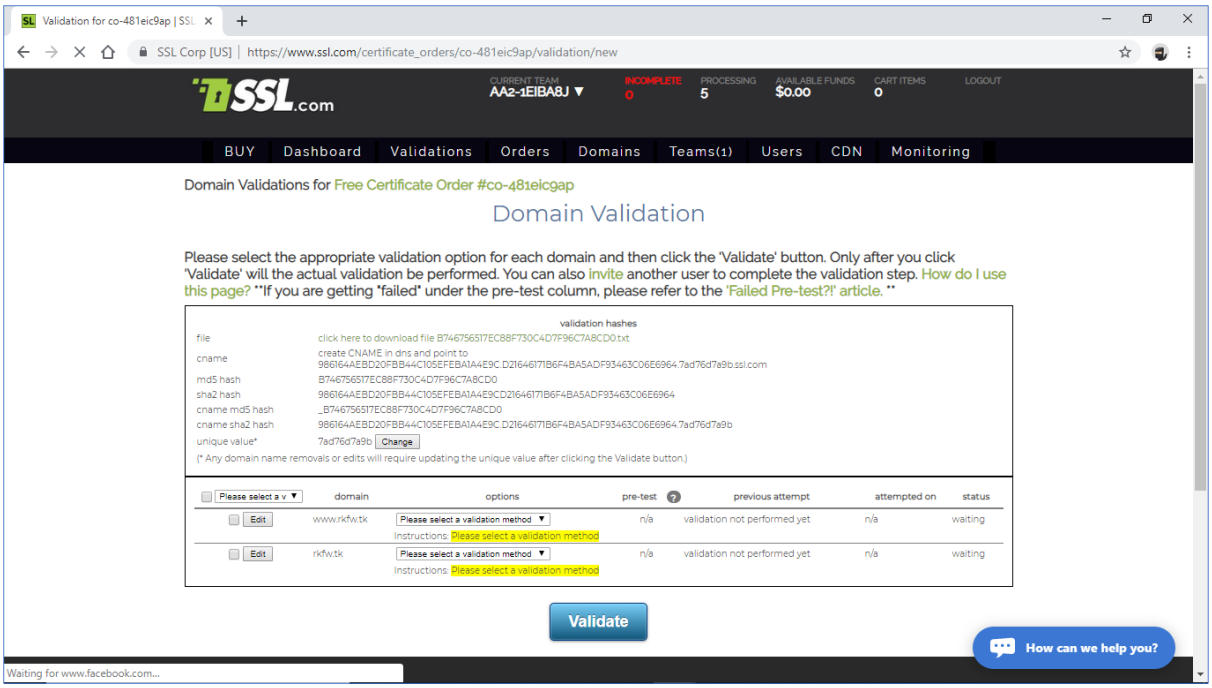
8. Purchase an SSL Certificate and provide this CSR to get an SSL Certificate for our Gateway.

- Start the SSL Certificate wizard and paste the CSR content that we have copied previously.




Reprocessing Free SSL Certificate
SSL Corp [US] | https://www.ssl.com/team/aa2-1eiba8j/certificate_orders/co-481eic9ap/reprocess
It MUST represent your fully-qualified domain name (i.e. submit.domain.com)
common name field in csr is: www.rkfw.tk
*CSR:
certificate signing request
use previous csr
-----END CERTIFICATE REQUEST-----
Save to CSR Manager:
Managed CSR:
none
Create CSR
Common Name (CN):
primary domain name
www.rkfw.tk
Server Software:
for informational purposes only
OTHER
Schedule SSL Scans:
expiration reminder notifications
Simple
Custom
None
Daily (at midnight)
*Subscriber Agreement
By clicking this check box, you agree to the terms of the SSL.com Subscriber Agreement
Next >>
How can we help you?


Applicant Information For Certifi
SSL Corp [US] | https://www.ssl.com/team/aa2-1eiba8j/certificate_orders/co-481eic9ap/edit
Submit CSR
2 Registrant
3 Perform Validation
4 Complete
Applicant Information for 90 Days Free SSL
Please fill out the required fields below to complete your certificate order.
Company Details
Please provide information about the applicant of this certificate. Address and contact information will not be publicly visible
*Website:
the subject or common name
www.rkfw.tk
Save to Identity Manager:
Reuse this identity in future certificates.
*Company:
organization
RK-MILLETS
DBA:
assumed name
Duns Number:
duns and bradstreet number
Department:
organization unit
SECURITY
PO Box:



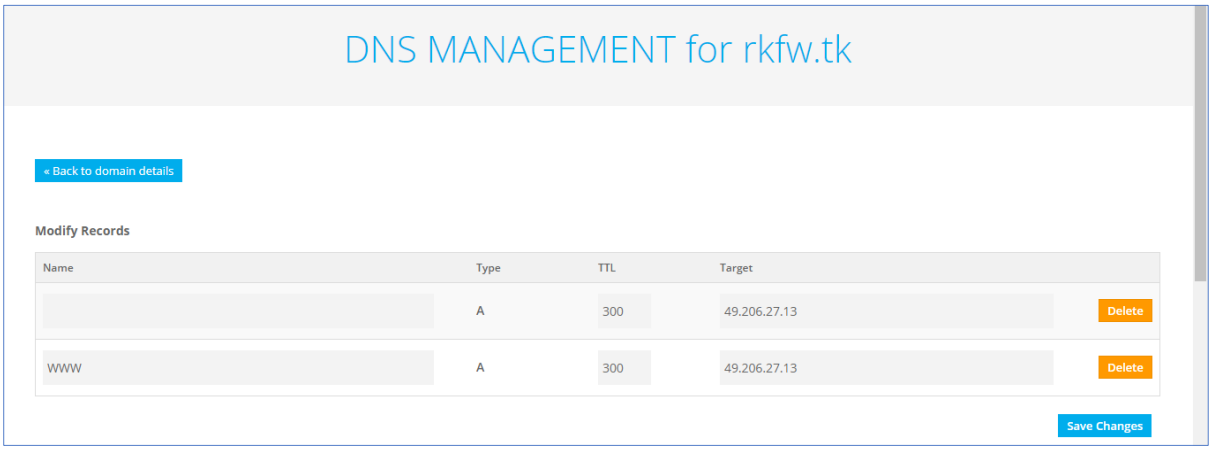
- We will do the domain validation for www.rkfw.tk domain using the DNS CNAME record method.

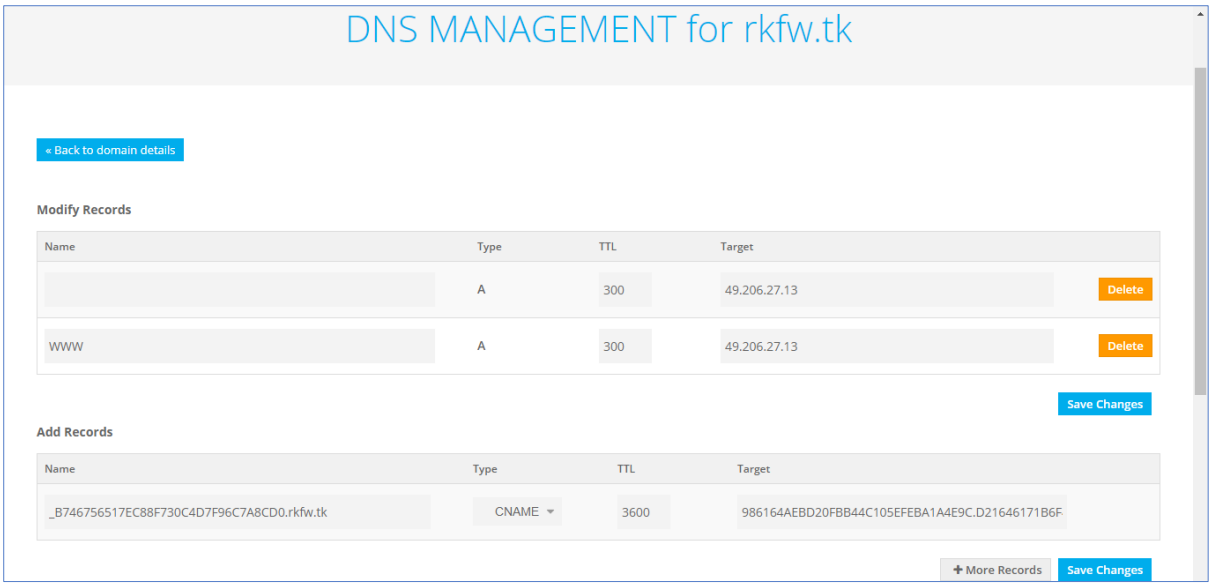
- Define a CNAME record on our DNS Server pointing to the SSL.COM domain. Meaning point the CNAME

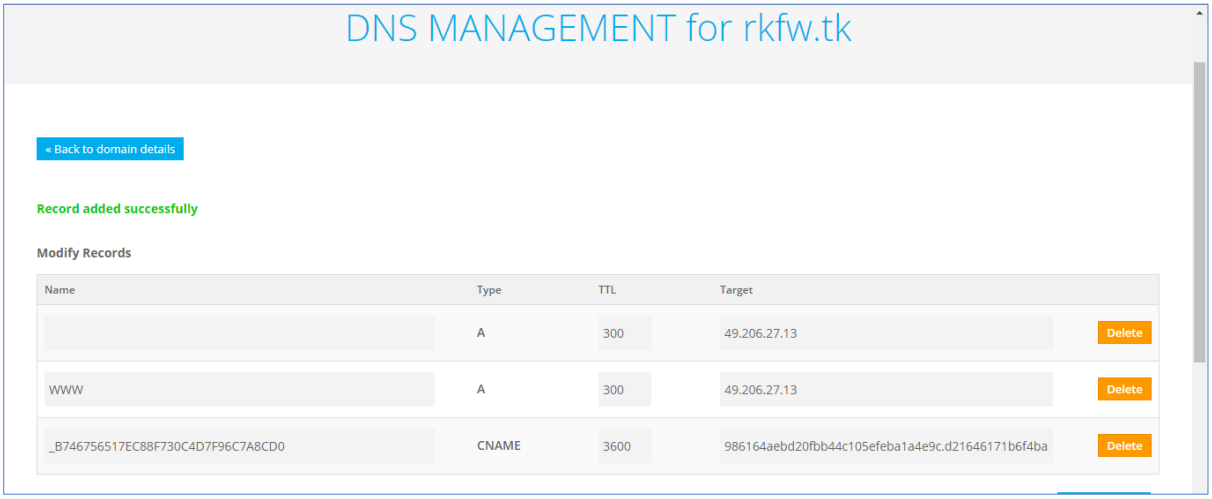
  `_B746756517EC88F730C4D7F96C7A8CD0.rkfw.tk`

  to

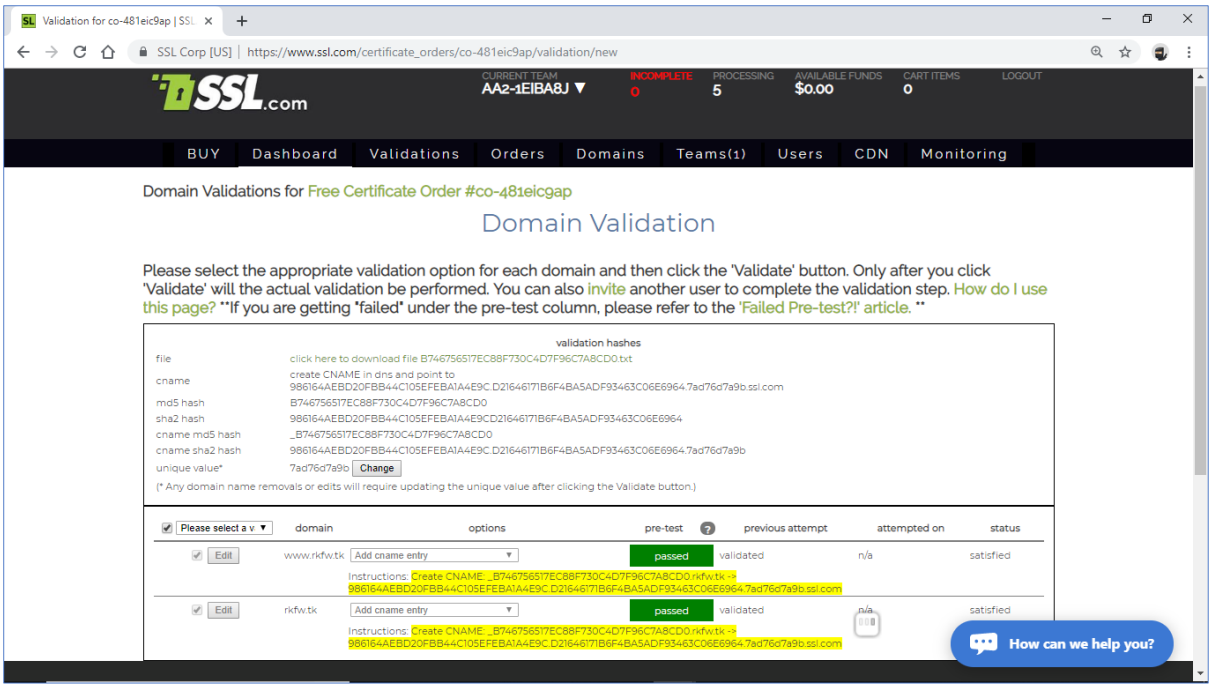
  `986164AEBD20FBB44C105EFEBA1A4E9C.D21646171B6F4BA5ADF93463C06E6964.7ad76d7a9b.ssl.com`

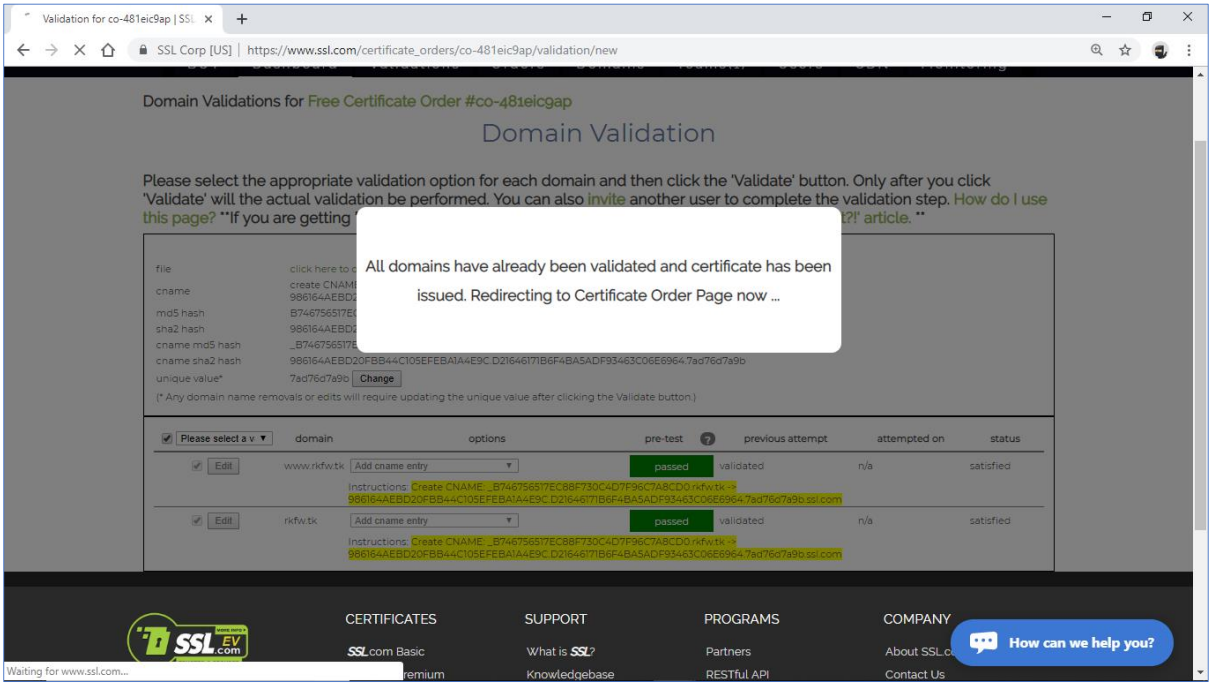


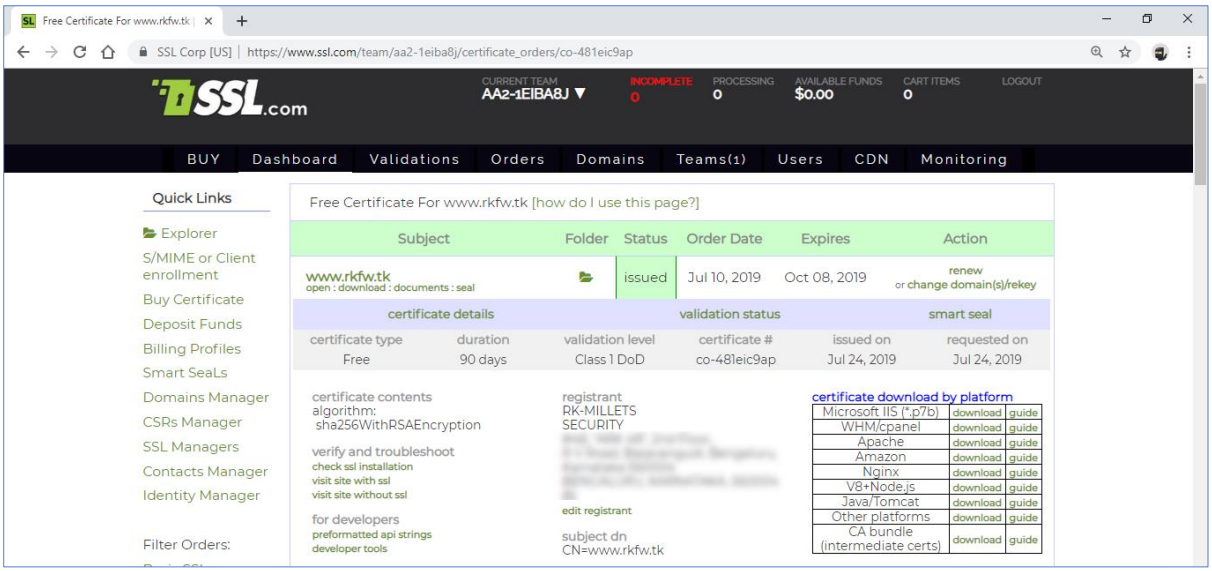




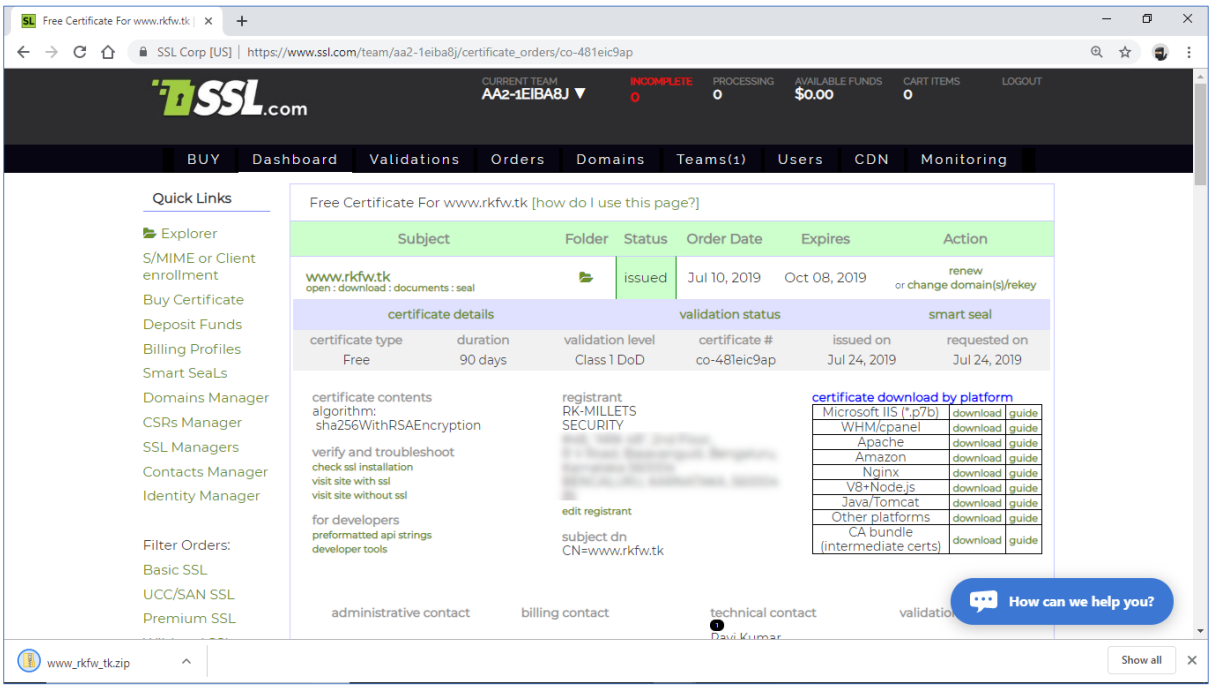
- Once we add a CNAME record, the domain validation of the SSL.com will pass.


Validation for co-481eic9ap | SSL
SSL Corp [US] | https://www.ssl.com/certificate_orders/co-481eic9ap/validation/new
CURRENT TEAM
AA2-1EIBA8J
INCOMPLETE
0
PROCESSING
5
AVAILABLE FUNDS
$0.00
CART ITEMS
0
LOGOUT
BUY
Dashboard
Validations
Orders
Domains
Teams(1)
Users
CDN
Monitoring
Domain Validations for Free Certificate Order #co-481eicgap
Domain Validation
Please select the appropriate validation option for each domain and then click the 'Validate' button. Only after you click 'Validate' will the actual validation be performed. You can also invite another user to complete the validation step. How do I use this page? **If you are getting "failed" under the pre-test column, please refer to the 'Failed Pre-test?!' article. **
validation hashes
file
click here to download file B746756517EC88F730C4D7F96C7A8CD0.txt
cname
create CNAME in dns and point to 986164AEBD20FBB44C105EFEBA1A4E9C.D21646171B6F4BA5ADF93463C06E6964.7ad76d7a9b.ssl.com
md5 hash
B746756517EC88F730C4D7F96C7A8CD0
sha2 hash
986164AEBD20FBB44C105EFEBA1A4E9CD21646171B6F4BA5ADF93463C06E6964
cname md5 hash
_B746756517EC88F730C4D7F96C7A8CD0
cname sha2 hash
986164AEBD20FBB44C105EFEBA1A4E9C.D21646171B6F4BA5ADF93463C06E6964.7ad76d7a9b
unique value*
7ad76d7a9b
Change
(* Any domain name removals or edits will require updating the unique value after clicking the Validate button.)
Please select a v
domain
options
pre-test
previous attempt
attempted on
status
Edit
www.rkfw.tk
Add cname entry
passed
validated
n/a
satisfied
Instructions: Create CNAME: _B746756517EC88F730C4D7F96C7A8CD0.rkfw.tk -> 986164AEBD20FBB44C105EFEBA1A4E9C.D21646171B6F4BA5ADF93463C06E6964.7ad76d7a9b.ssl.com
Edit
rkfw.tk
Add cname entry
passed
validated
n/a
satisfied
Instructions: Create CNAME: _B746756517EC88F730C4D7F96C7A8CD0.rkfw.tk -> 986164AEBD20FBB44C105EFEBA1A4E9C.D21646171B6F4BA5ADF93463C06E6964.7ad76d7a9b.ssl.com
How can we help you?

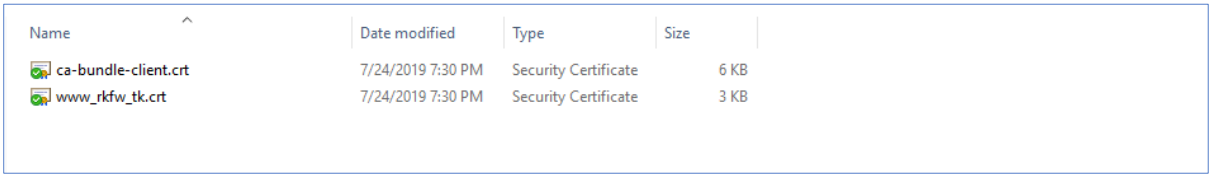

Validation for co-481eic9ap | SSL
SSL Corp [US] | https://www.ssl.com/certificate_orders/co-481eic9ap/validation/new
Domain Validations for Free Certificate Order #co-481eicgap
Domain Validation
Please select the appropriate validation option for each domain and then click the 'Validate' button. Only after you click 'Validate' will the actual validation be performed. You can also invite another user to complete the validation step. How do I use this page? **If you are getting
All domains have already been validated and certificate has been issued. Redirecting to Certificate Order Page now ...
Change
(* Any domain name removals or edits will require updating the unique value after clicking the Validate button.)
Please select a v
domain
options
pre-test
previous attempt
attempted on
status
Edit
www.rkfw.tk
Add cname entry
passed
validated
n/a
satisfied
Edit
rkfw.tk
Add cname entry
passed
validated
n/a
satisfied
CERTIFICATES
SSL.com Basic
SUPPORT
What is SSL?
Knowledgebase
PROGRAMS
Partners
RESTful API
COMPANY
About SSL.c
Contact Us
How can we help you?
Waiting for www.ssl.com...



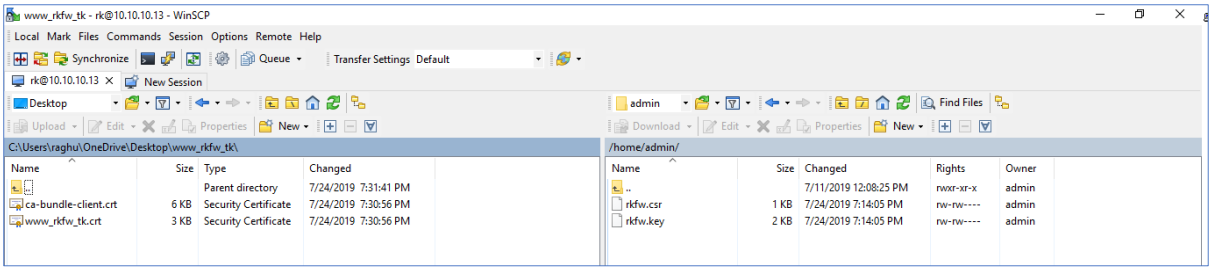
9. Now, Download the SSL Certificate for our Gateway domain. Choose Apache as Server type.

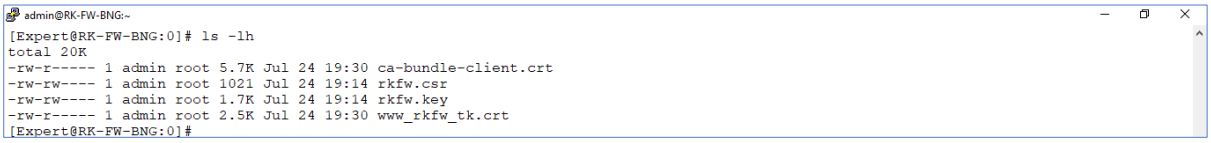


The downloaded zip file has the domain certificate (***www_rkfw_tk.crt***) & a bundled certificate (***ca-bundled-client.crt***) of our SSL.COM Root & Intermediate certificate.



10. Copy these two files on to our Gateway where we generated the CSR (***/home/admin***).

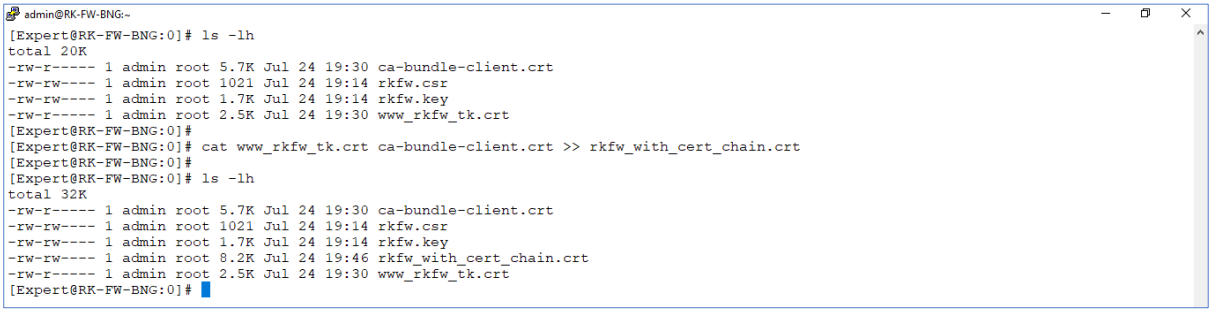




11. Merge the content of domain certificate & the bundled CA Certificate in such way that it resembles:

```
-----BEGIN CERTIFICATE-----

(Your Primary SSL certificate: www_rkfw_tk.crt)

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

(Your Intermediate certificate: SSL-COM-RSA-SSL-SUBCA.crt)

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

(Your Root certificate: SSL-COM-ROOT-CERTIFICATION-AUTHORITY-RSA.crt)

-----END CERTIFICATE-----
```

So, combine the two certificate files that we have downloaded from SSL.COM and create a single certificate file (***rkfw_with_cert_chain.crt***) which will have the above format.



12. Rename the trusted SSL Certificate file (***rkfw_with_cert_chain.crt***) and the Private Key file (***rkfw.key***) as ***server.crt*** and ***server.key*** respectively.

```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# ls -lh
total 32K
-rw-r----- 1 admin root 5.7K Jul 24 19:30 ca-bundle-client.crt
-rw-rw---- 1 admin root 1021 Jul 24 19:14 rkfw.csr
-rw-rw---- 1 admin root 1.7K Jul 24 19:14 rkfw.key
-rw-rw---- 1 admin root 8.2K Jul 24 19:46 rkfw_with_cert_chain.crt
-rw-r----- 1 admin root 2.5K Jul 24 19:30 www_rkfw_tk.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# mv rkfw_with_cert_chain.crt server.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# mv rkfw.key server.key
[Expert@RK-FW-BNG:0]# _
```

13. Replace our Gateway's default Self-Signed Certificate & the Private Key stored in ***/web/conf*** directory with our trusted SSL Certificate & the Private Key stored in ***/home/admin*** directory.

Note: Backup the original ***server.crt*** & ***server.key*** file stored in ***/web/conf*** before doing the changes.

```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# ls -lh
total 32K
-rw-r----- 1 admin root 5.7K Jul 24 19:30 ca-bundle-client.crt
-rw-rw---- 1 admin root 1021 Jul 24 19:14 rkfw.csr
-rw-rw---- 1 admin root 8.2K Jul 24 19:46 server.crt
-rw-rw---- 1 admin root 1.7K Jul 24 19:14 server.key
-rw-r----- 1 admin root 2.5K Jul 24 19:30 www_rkfw_tk.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# cp server.crt /web/conf/server.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# cp server.key /web/conf/server.key
[Expert@RK-FW-BNG:0]#
```

14. From the ***/home/admin*** directory, generate a ***.p12*** certificate file (supported file type on our SmartConsole) by making use of our trusted SSL Certificate & it's Private Key. Run the below command to create a ***.p12*** file:

 # cpopenssl pkcs12 -export -out *<Output_p12_File>* -in *<Certificate_File>* -inkey *<Certificate's_Private_Key>*

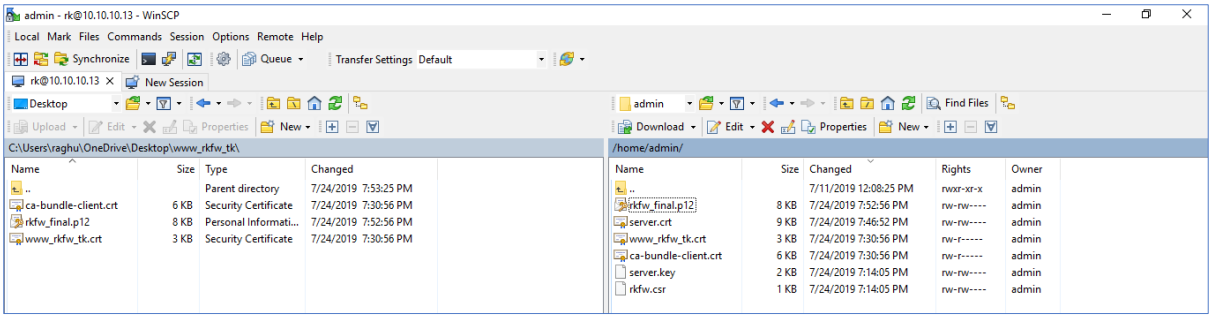
In our case it is:

 # cpopenssl pkcs12 -export -out *rkfw_final.p12* -in *server.crt* -inkey *server.key*

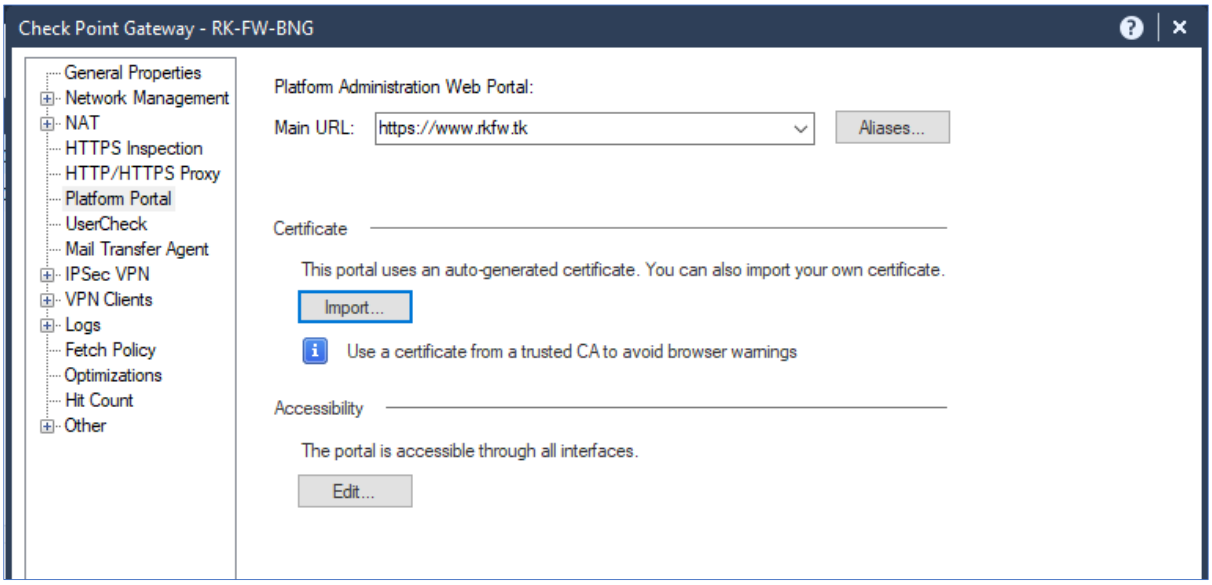
Provide the ***.p12*** **export password** while generating the file.

```
admin@RK-FW-BNG:~
[Expert@RK-FW-BNG:0]# ls -lh
total 32K
-rw-r----- 1 admin root 5.7K Jul 24 19:30 ca-bundle-client.crt
-rw-rw---- 1 admin root 1021 Jul 24 19:14 rkfw.csr
-rw-rw---- 1 admin root 8.2K Jul 24 19:46 server.crt
-rw-rw---- 1 admin root 1.7K Jul 24 19:14 server.key
-rw-r----- 1 admin root 2.5K Jul 24 19:30 www_rkfw_tk.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# cpopenssl pkcs12 -export -out rkfw_final.p12 -in server.crt -inkey server.key
Enter Export Password:
Verifying - Enter Export Password:
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# ls -lh
total 40K
-rw-r----- 1 admin root 5.7K Jul 24 19:30 ca-bundle-client.crt
-rw-rw---- 1 admin root 1021 Jul 24 19:14 rkfw.csr
-rw-rw---- 1 admin root 7.6K Jul 24 19:52 rkfw_final.p12
-rw-rw---- 1 admin root 8.2K Jul 24 19:46 server.crt
-rw-rw---- 1 admin root 1.7K Jul 24 19:14 server.key
-rw-r----- 1 admin root 2.5K Jul 24 19:30 www_rkfw_tk.crt
[Expert@RK-FW-BNG:0]#
```

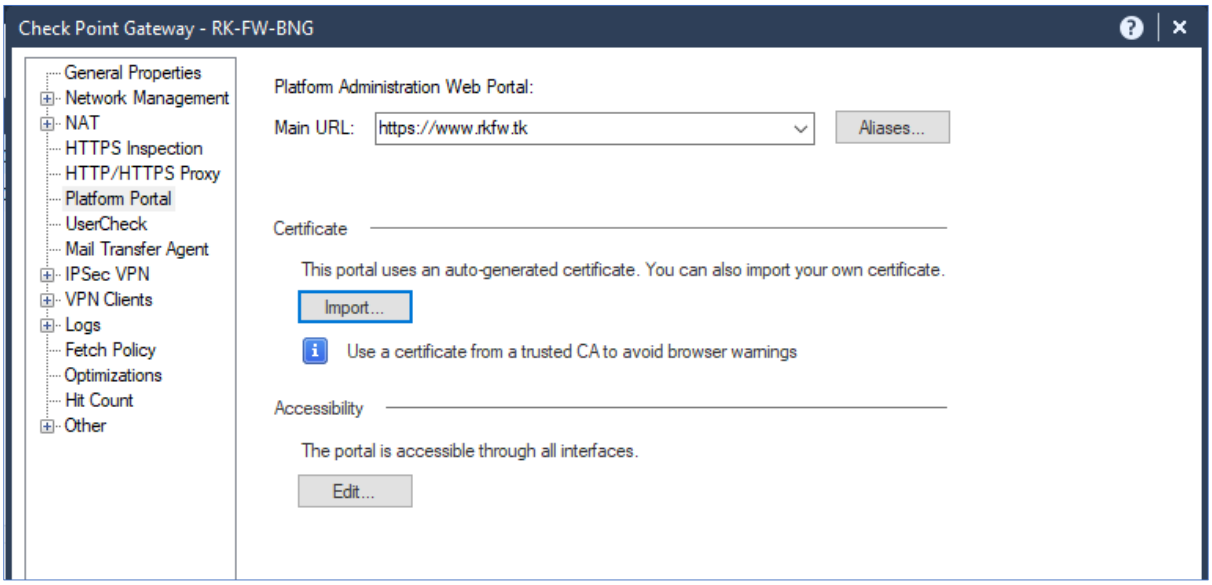
15. Copy this ***.p12*** file which we will be using on our SmartConsole.

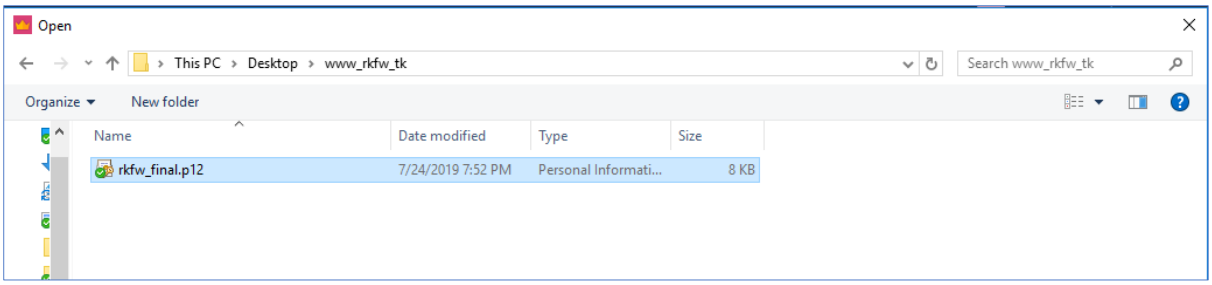


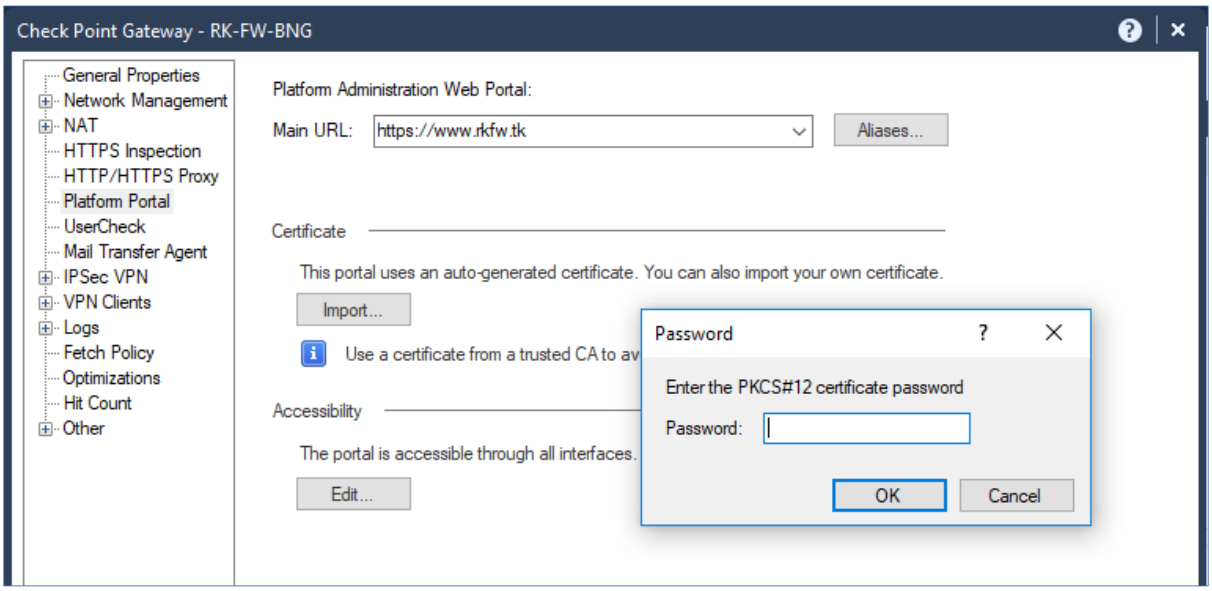
16. Open the Gateway Object and go to Platform Portal section.



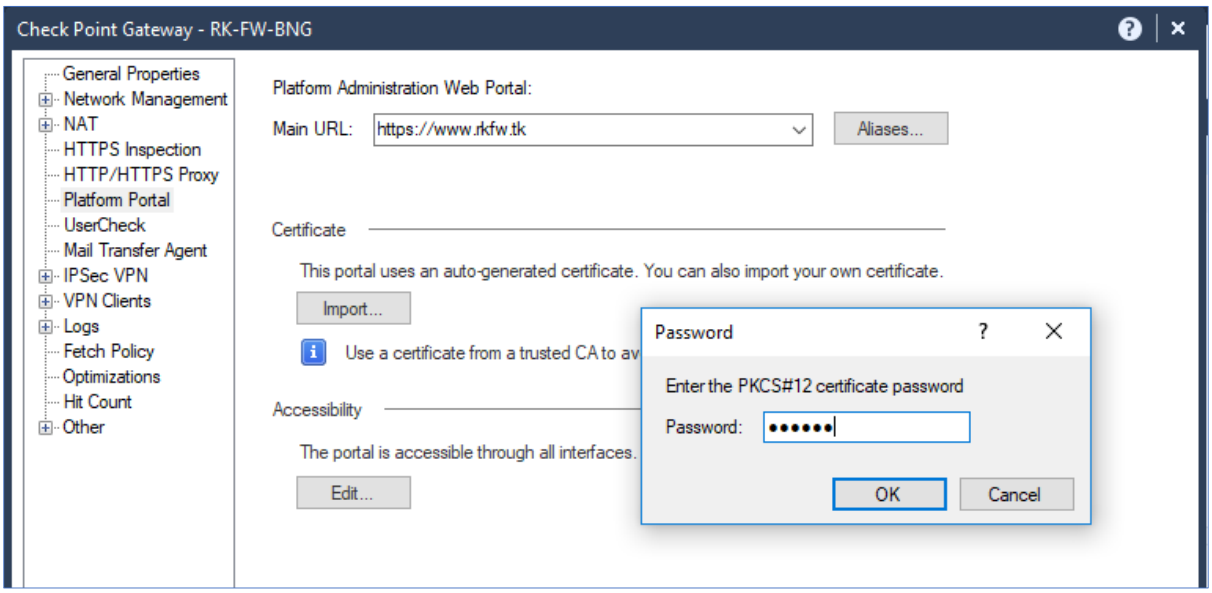
17. Click on **Import** and map the ***.p12*** file that we have copied from the device.



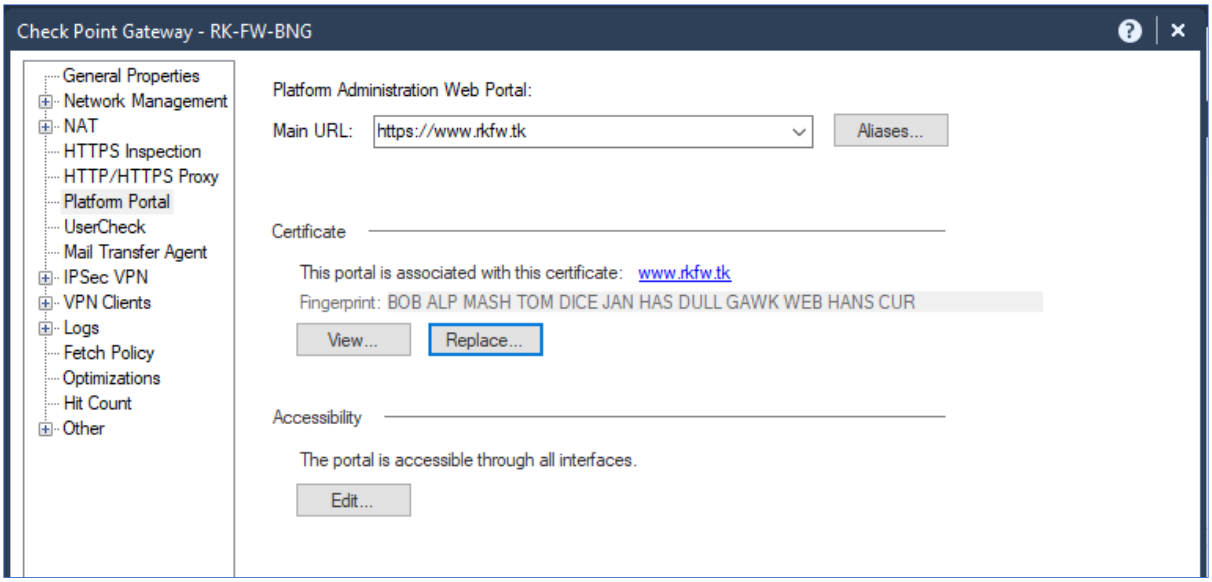




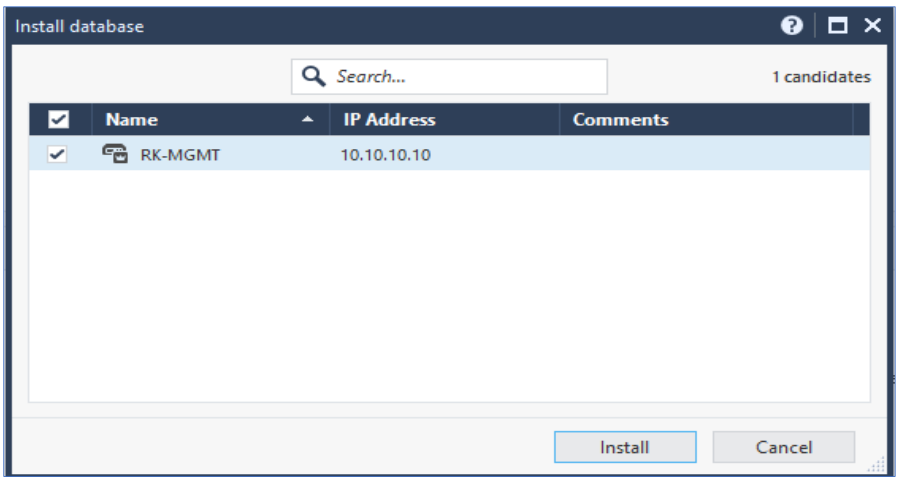
Enter the export password that we set while generating the ***.p12*** file.



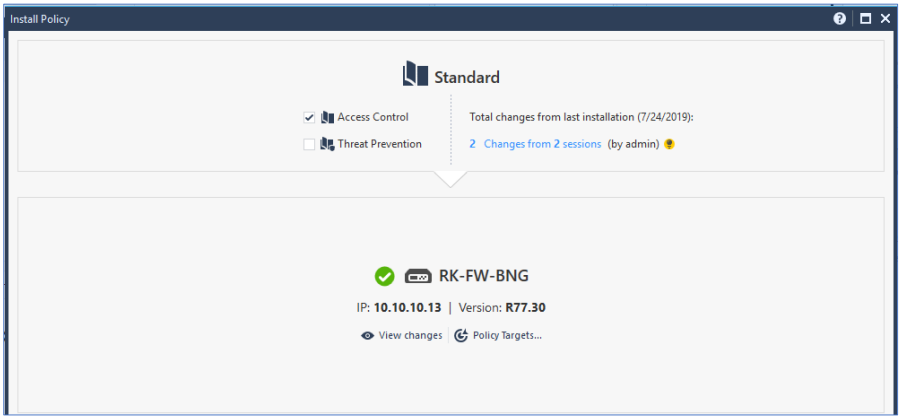
18. The SSL Certificate that we have imported is valid and mapped to our domain (www.rkfw.tk) ,



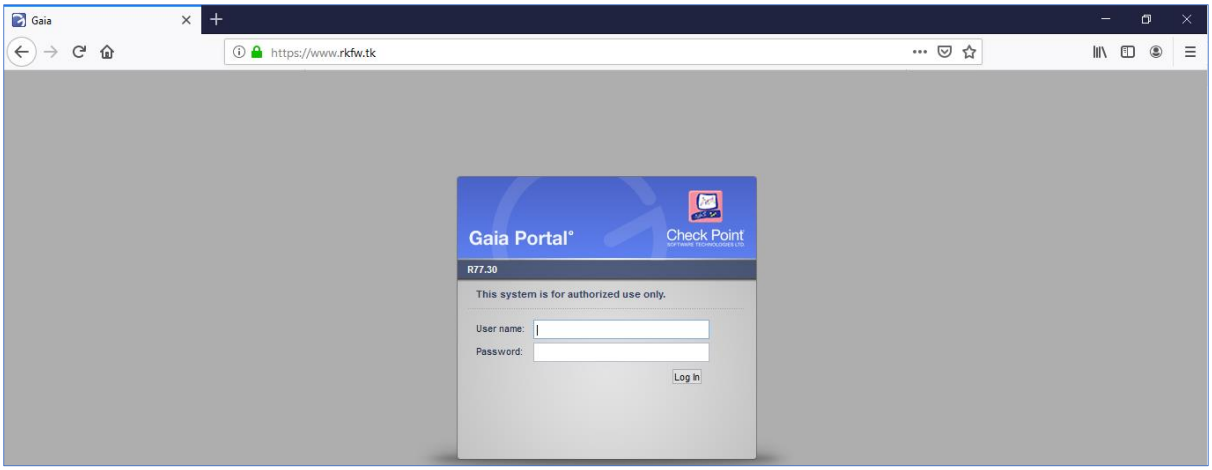
19. Click on **OK** and Save the configuration by **Publishing** the changes. Install the **Database** on the Management Server.

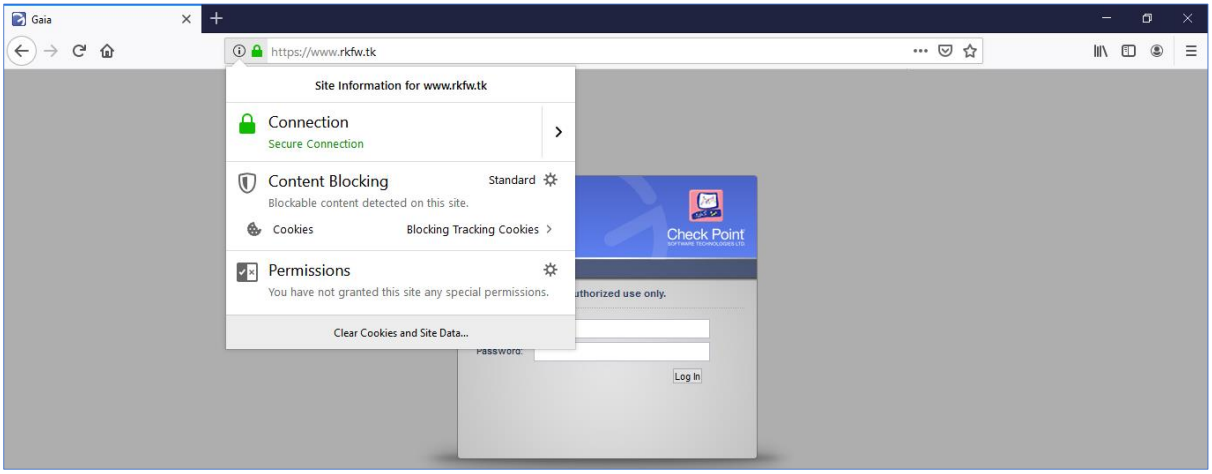


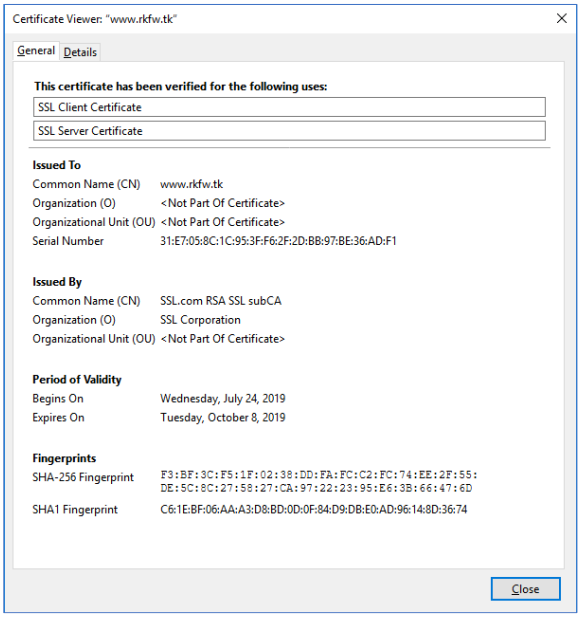
20. Install the Policy on the Gateway Object.

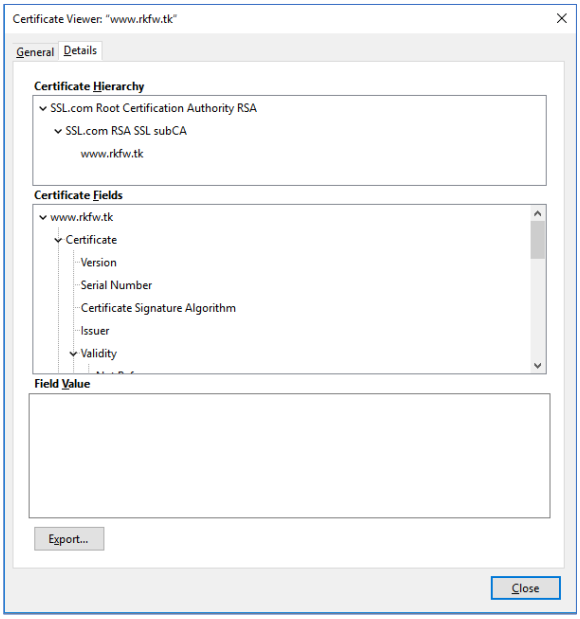


21. Now, try to access the Gateway's Gaia Portal using the domain name www.rkfw.tk ,

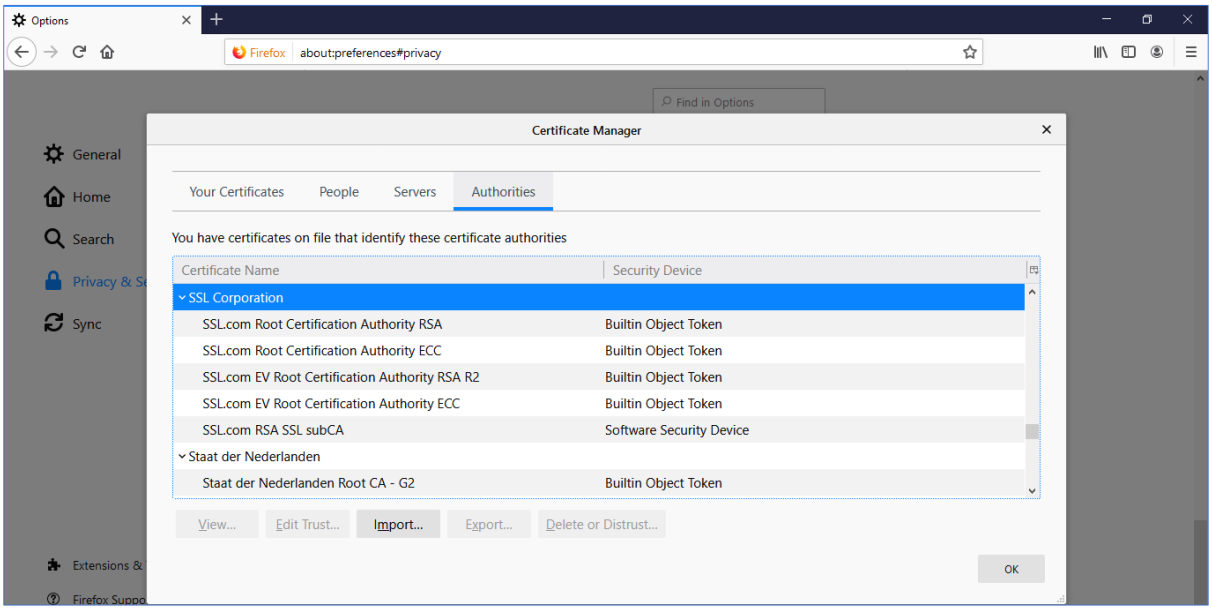






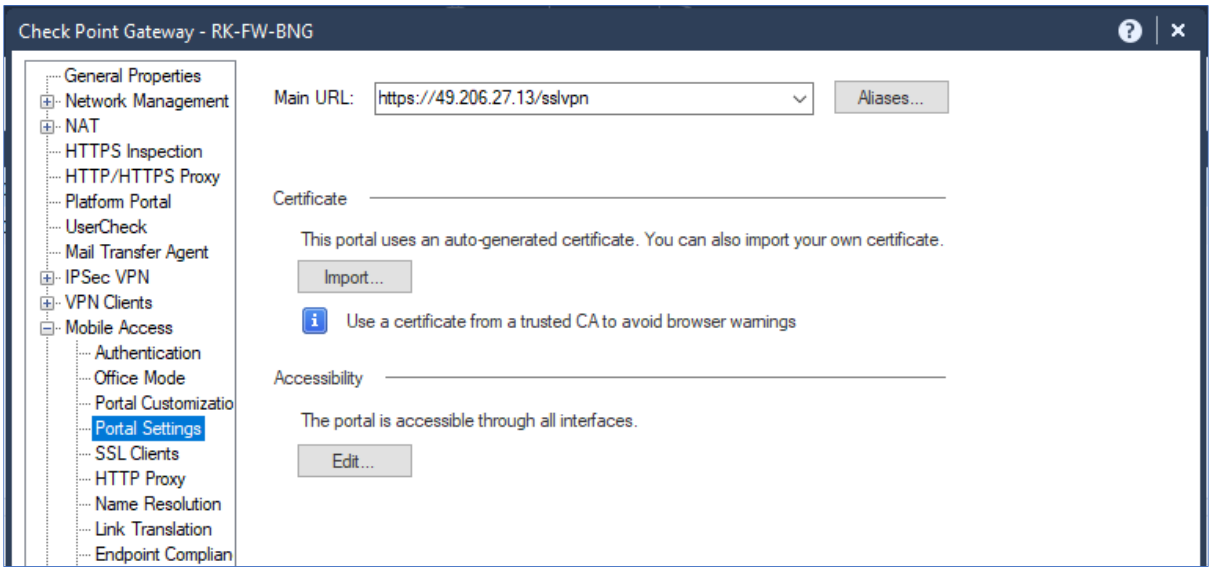


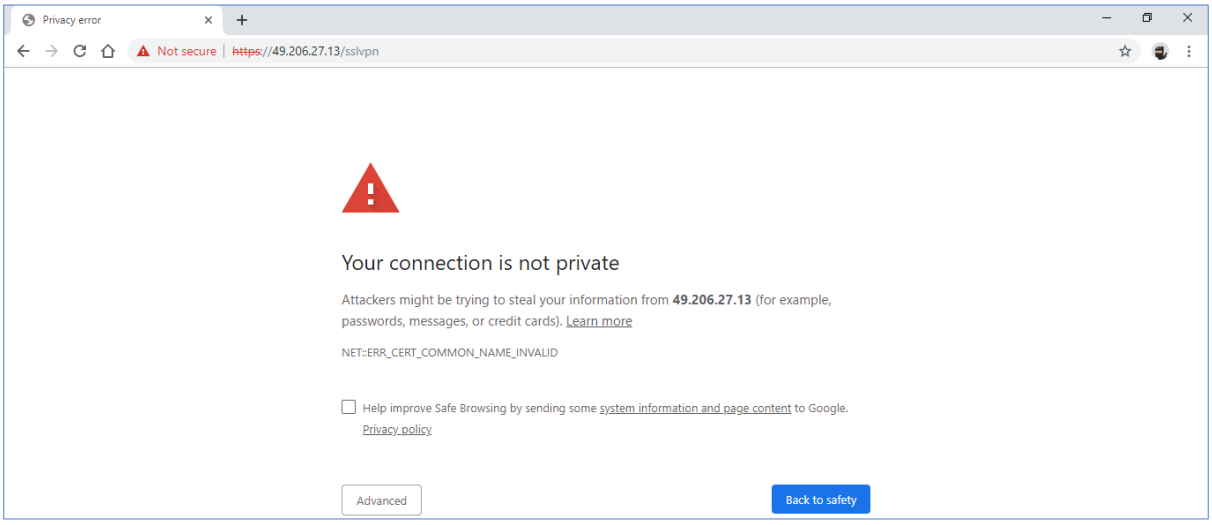
We are no more getting the SSL Certificate warning on the browser, as it is issued by a **Trusted CA - SSL.COM** which our Operating System or Browser trust upon.

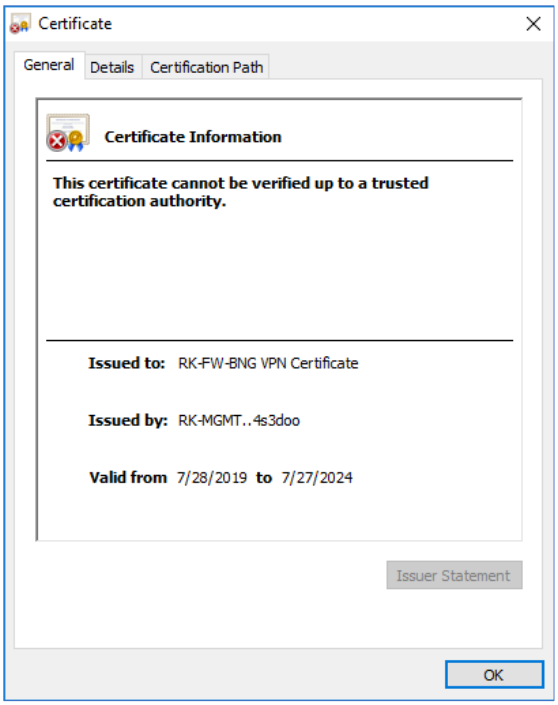


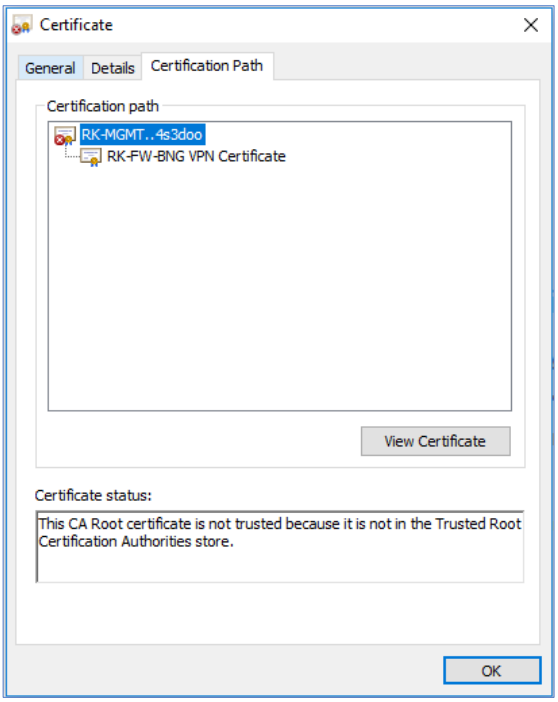
SSL Certificate for Mobile Access / SSL VPN

1. Mobile Access VPN portal will also use the Self-Signed Certificate issued by the Management Server's ***Internal CA*** by default, which gives a Certificate Warning on any browser.

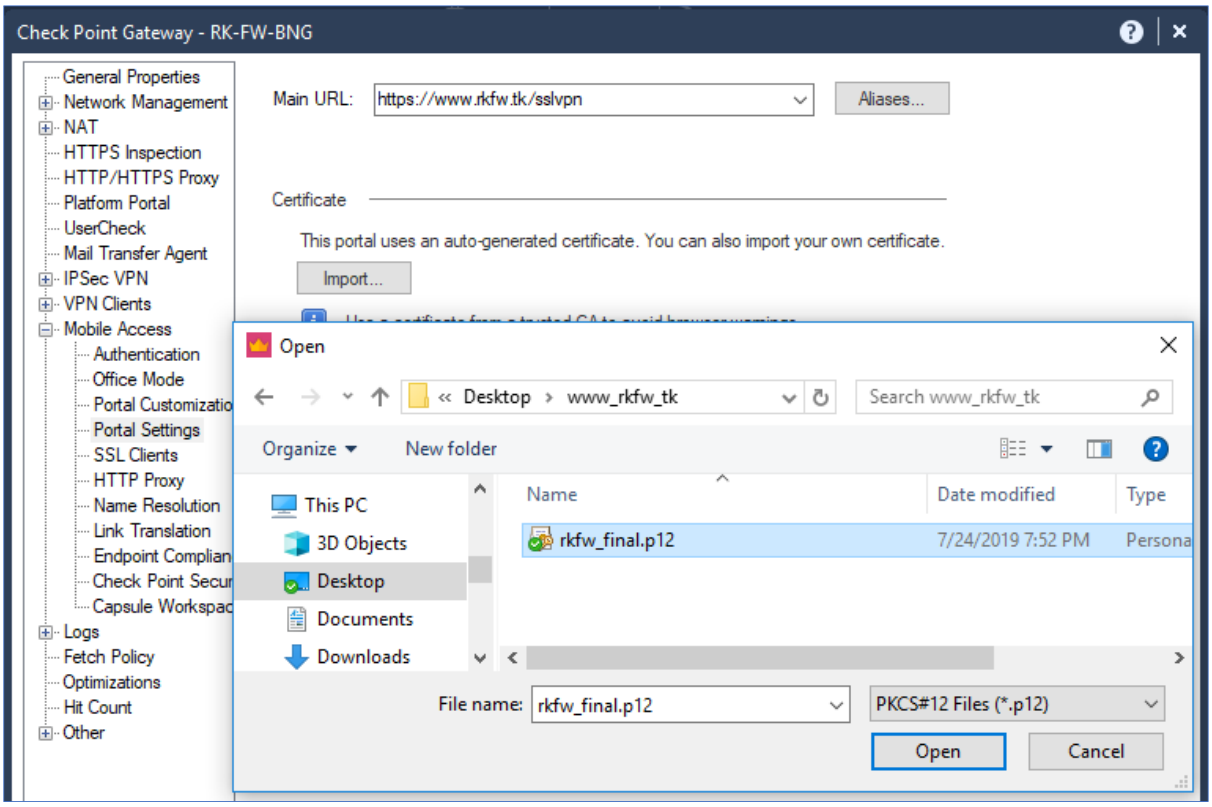


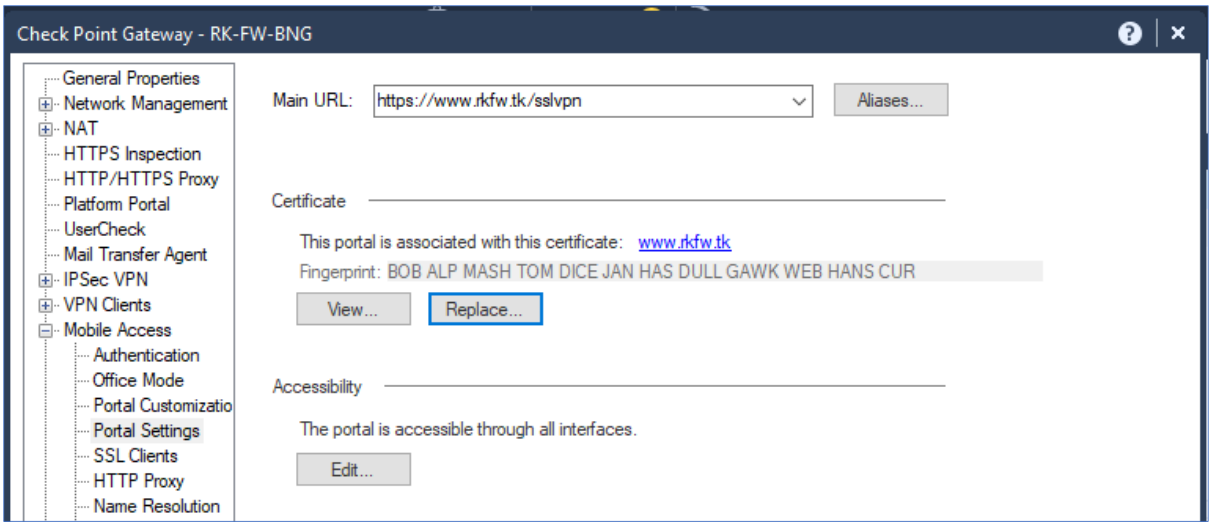




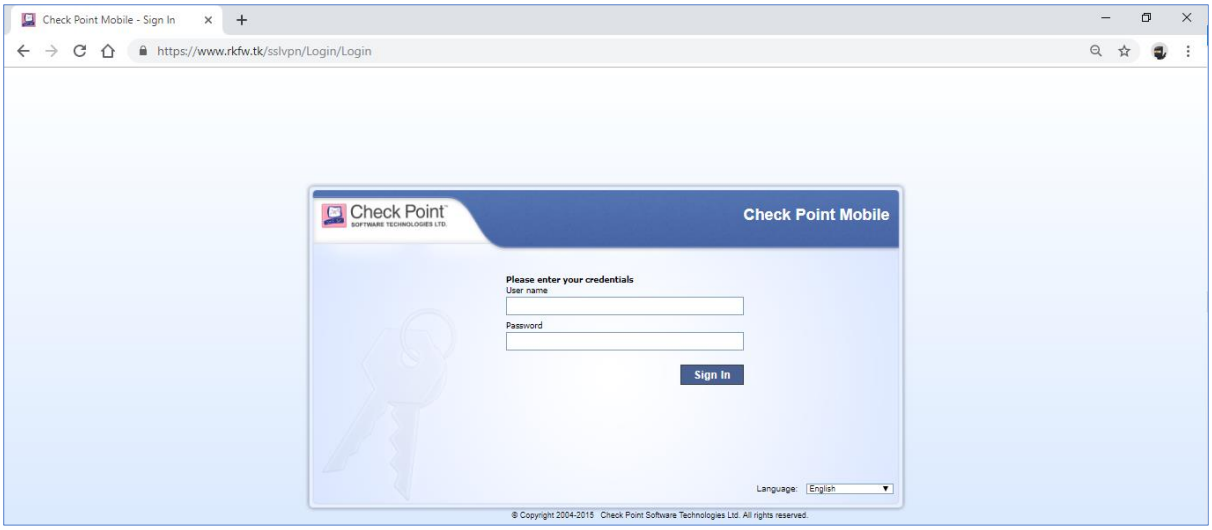


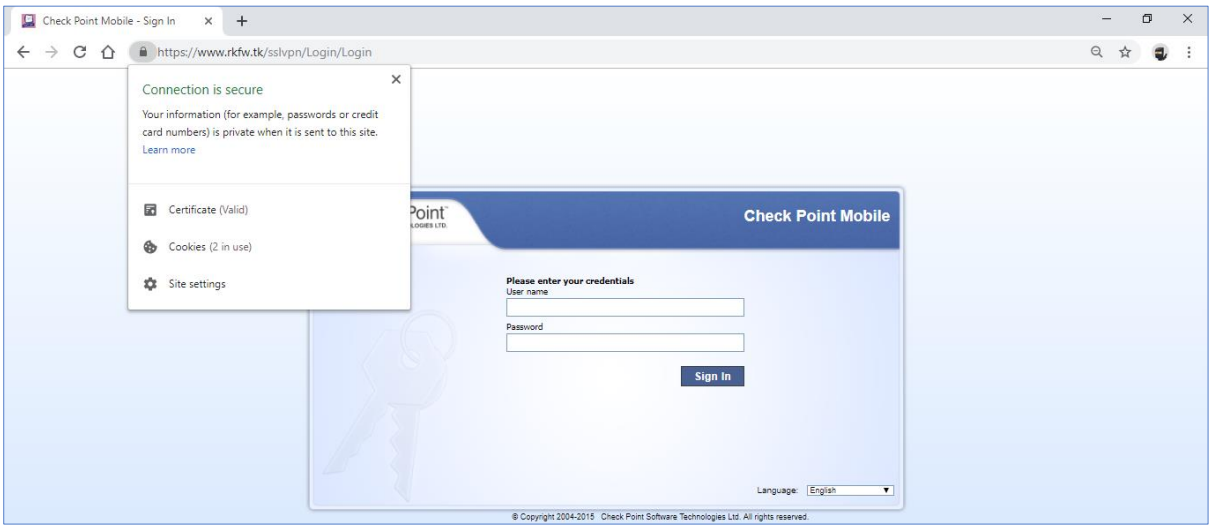
2. We can use the Trusted 3rd Party CA Certificate that we have generated earlier on Mobile Access VPN Feature by importing the certificate in ***.p12*** format.

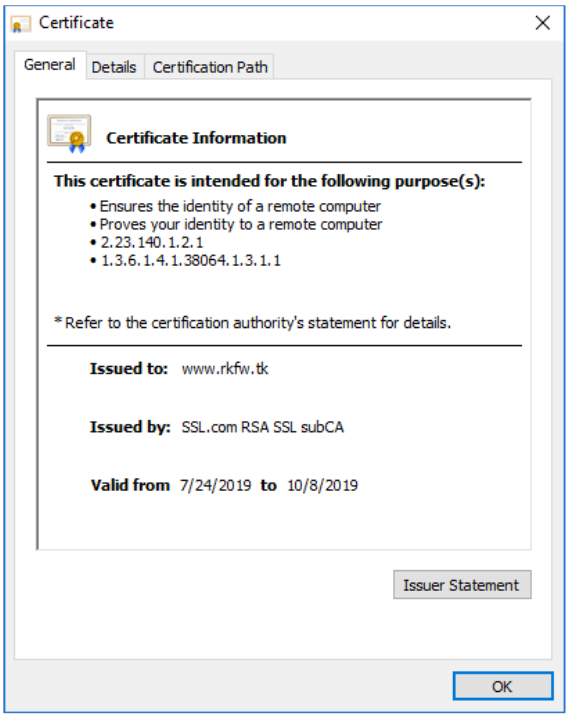


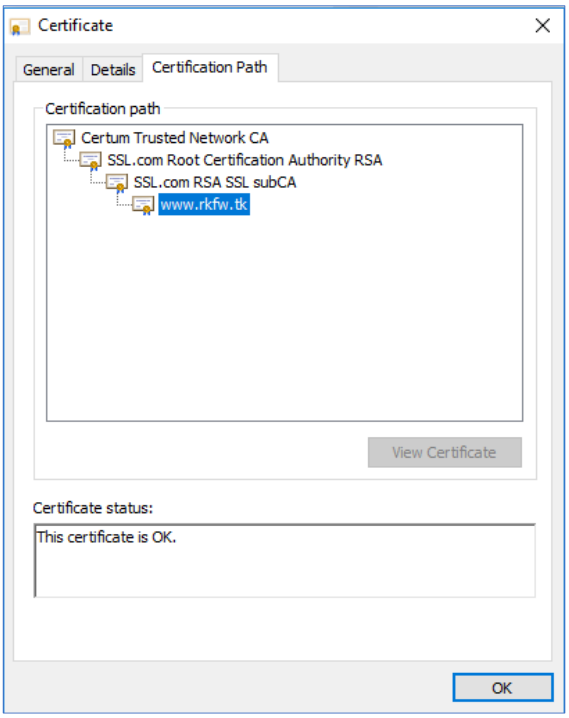


3. Install the Database on the Management Server & Install the Policy on the Gateway. You will be able to access the Mobile Access Portal without any Certificate Warning.



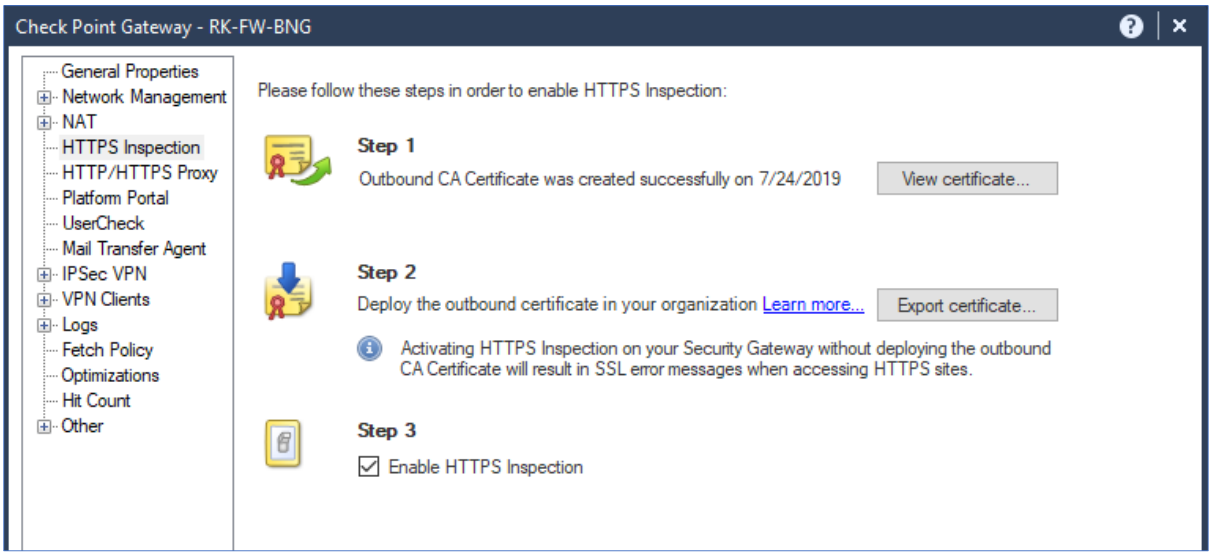



Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• 2.23.140.1.2.1
• 1.3.6.1.4.1.38064.1.3.1.1
* Refer to the certification authority's statement for details.
Issued to: www.rkfw.tk
Issued by: SSL.com RSA SSL subCA
Valid from 7/24/2019 to 10/8/2019
Issuer Statement
OK

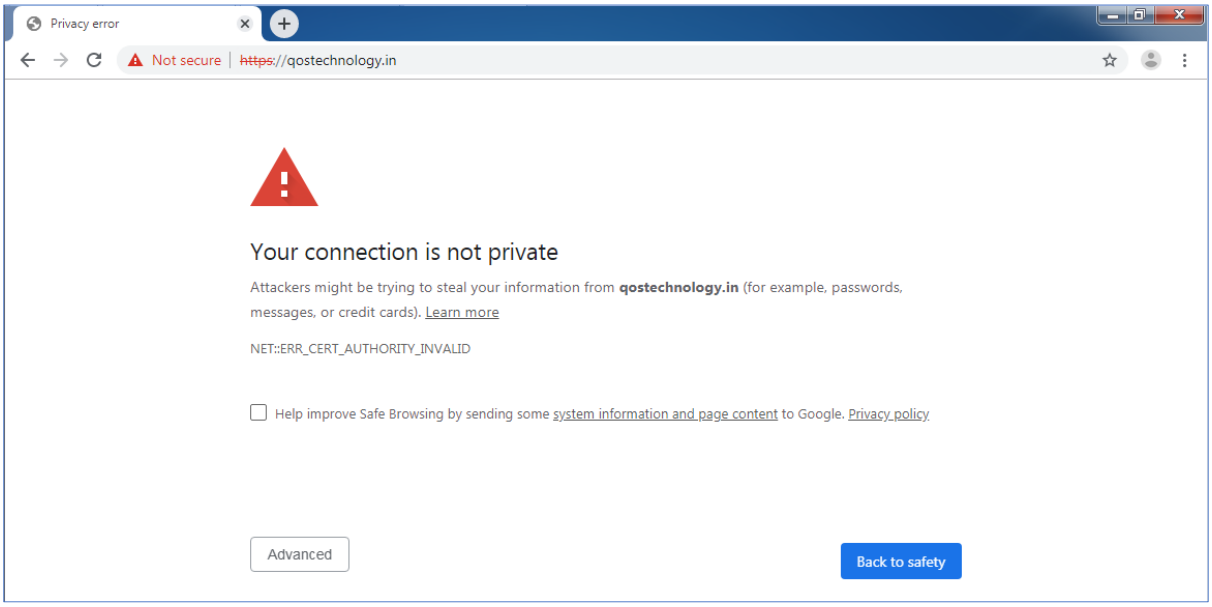

Certificate
General
Details
Certification Path
Certification path
Certum Trusted Network CA
SSL.com Root Certification Authority RSA
SSL.com RSA SSL subCA
www.rkfw.tk
View Certificate
Certificate status:
This certificate is OK.
OK

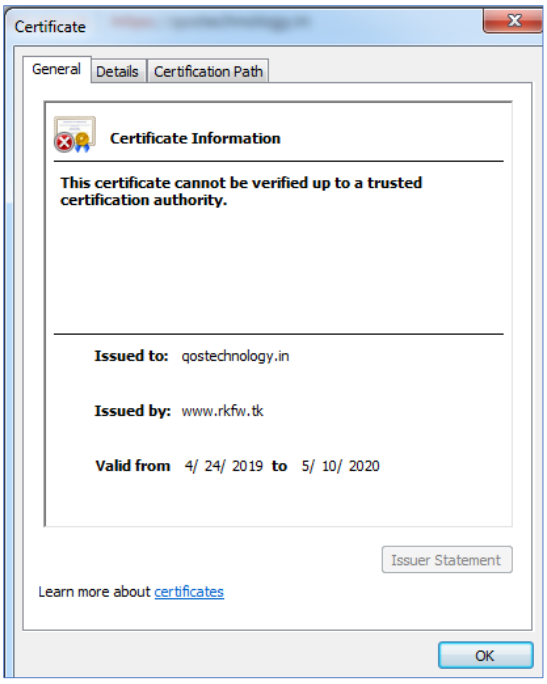
SSL Certificate for HTTPS Inspection Feature (Outbound Traffic)

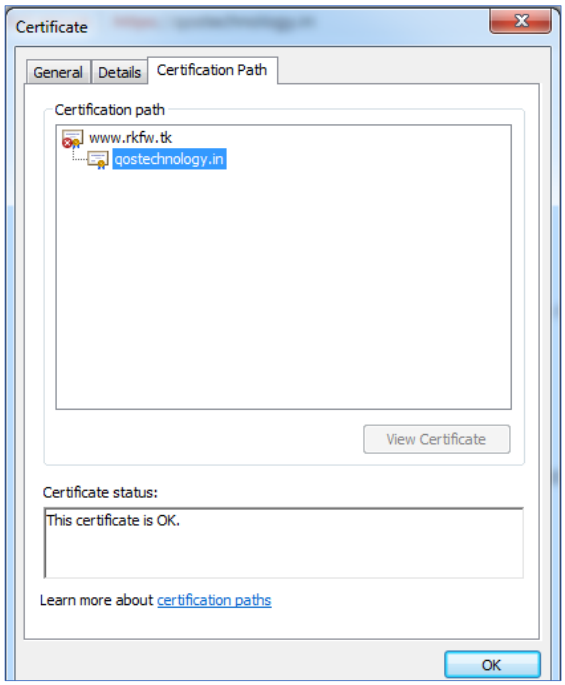
1. Our Gateway is enabled with HTTPS Inspection feature to inspect the web traffic using the Self-Signed Certificate that we created while enabling this feature.



2. We get a Certificate Warning on each user to whom HTTPS inspection rule being enforced.



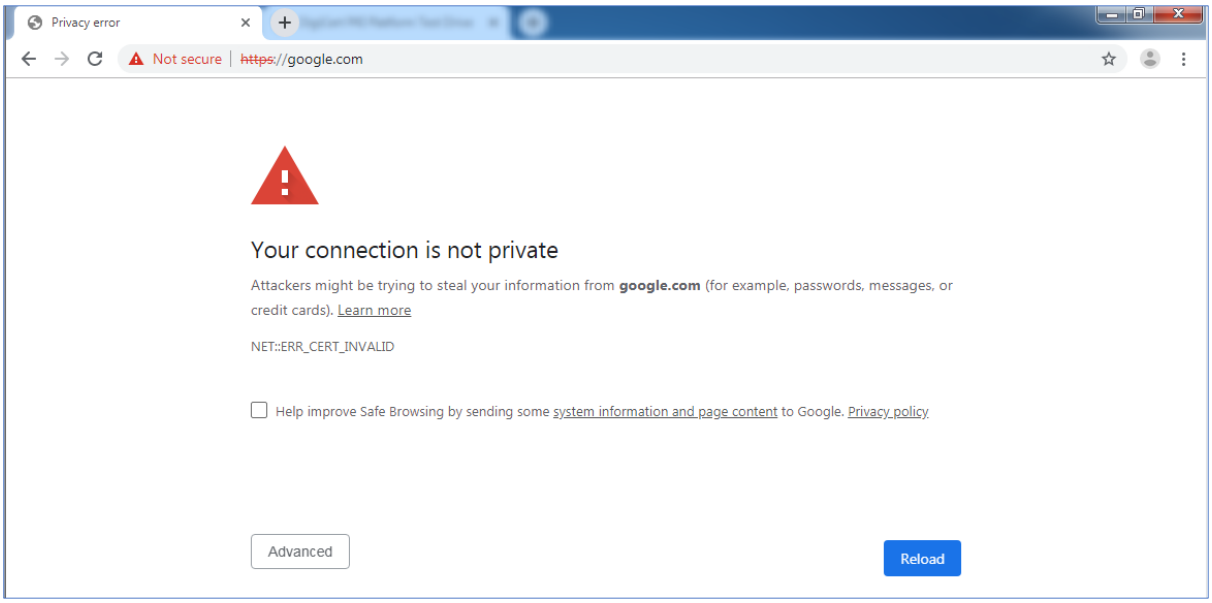


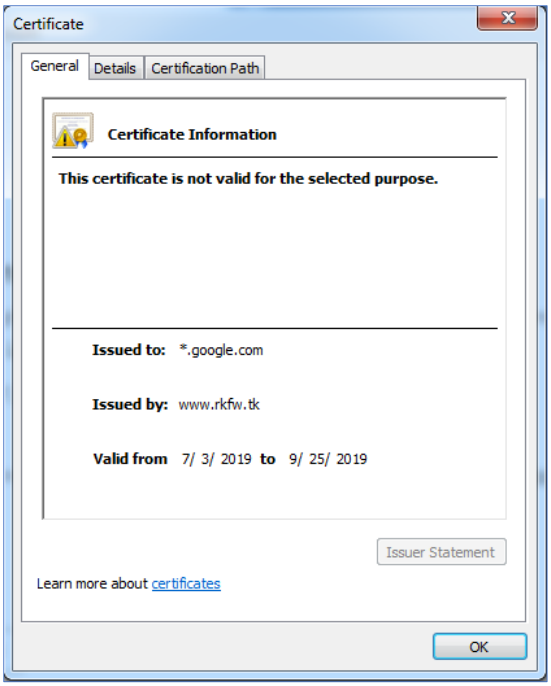


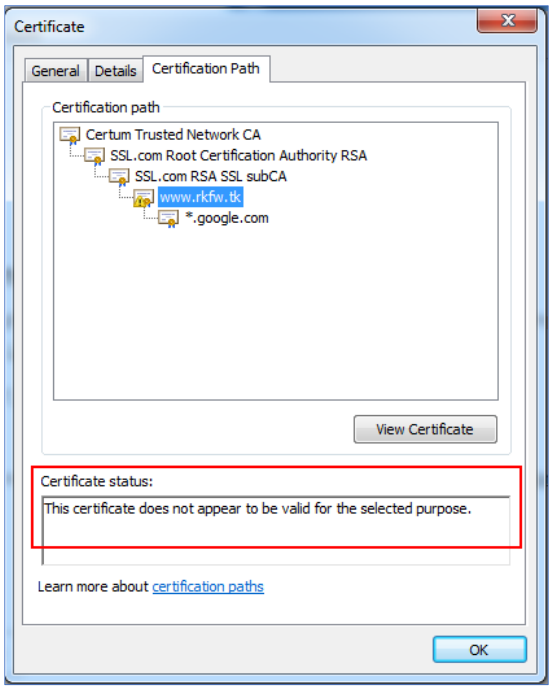
3. Clearly the Self-Signed Certificate that we have created is not there either in the OS Trusted Certificate Store or Browsers Certificate Store.

4. You won't able to resolve the above issue using a Domain Certificate associated with the Gateway, reason being the Domain Certificate are not designed to issue a certificate to some other domains. In other words, Domain Certificates can't act as an Intermediate Certificate Authority to issue Certificates to other Domains.

You will get the below error is you do so:







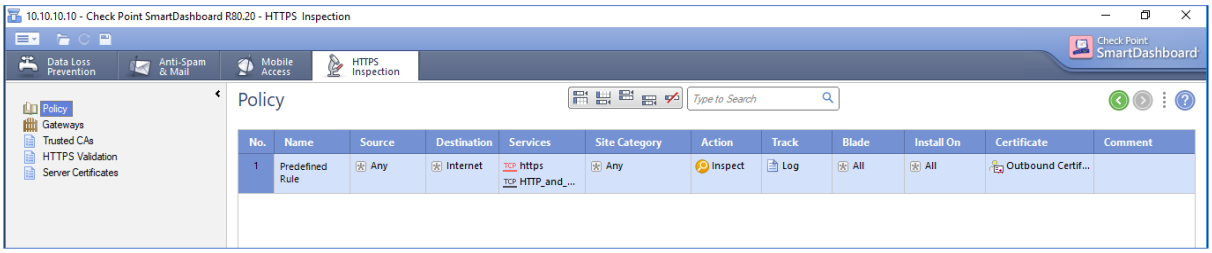
5. So the Certificate that we use in HTTPS Inspection (Outbound Traffic) needs to be either a Root Certificate or Intermediate CA!. But No CA will provide the access to their Root or Intermediate Certificates & Private Key to anyone.

6. In order to avoid our original concern related to HTTPS Inspection, we have two options:

- Distribute the Self-Signed Certificate generated on the Gateway to all the User Machines Trusted Root CA repository either **Manually** or using **Microsoft GPO** – An easy Approach.
- Establish a **Private PKI infrastructure** for your organization and import a Certificate on to the Check Point Gateway.

SSL Certificate for HTTPS Inspection Feature (Inbound Server Traffic)

1. HTTPS Inspection rule that we have defined in the previous case was to inspect only the traffic originated from the internal users (outbound) using the Self-Signed Certificate.



2. If there is a need to inspect the traffic from Internet destined to an Internal Server, then you have to define an Inbound HTTPS Inspection Rule.

3. As we are aware if there is a Man in the Middle for any HTTPS Traffic, the end user will be notified with the Certificate Warning.

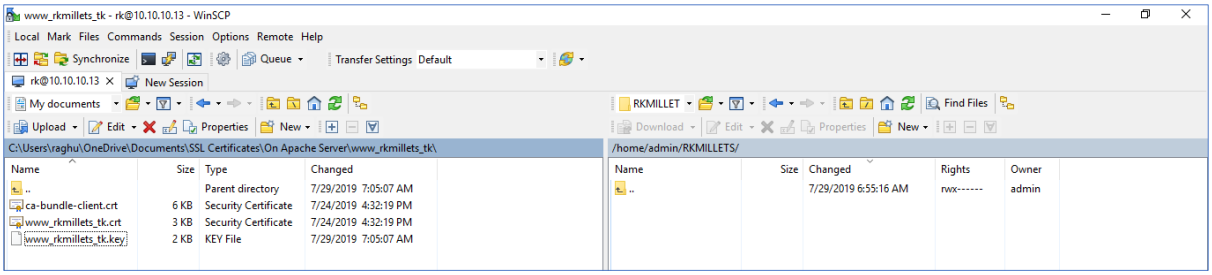
4. So, you need to import the Domain Certificate of the Server on the Gateway so that the Gateway can give a healthy feel to the internet user who's accessing the Server even though there is an interception of the HTTPS traffic destined to the Server.

5. Let's consider our RKMILLETS website www.rkmillet.tk , if we want to inspect this traffic then we need to:

- Import the Server's Domain Certificate on the Check Point Gateway.
- Create an Inbound HTTPS Inspection Rule.

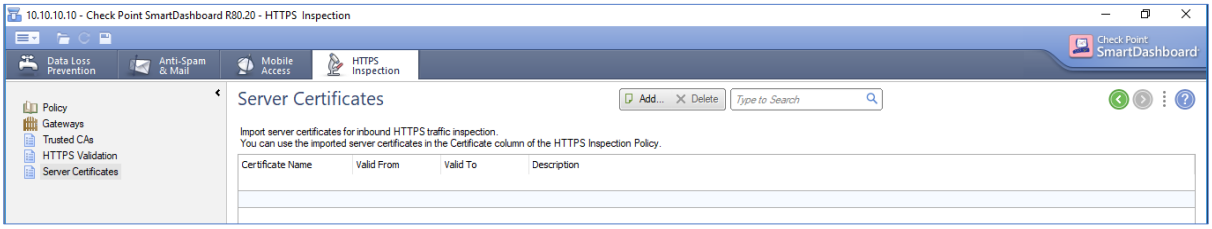
6. Import the RKMILLETS Server's domain certificate (***.p12 extension***) under **Server Certificate** section of the HTTPS Inspection,

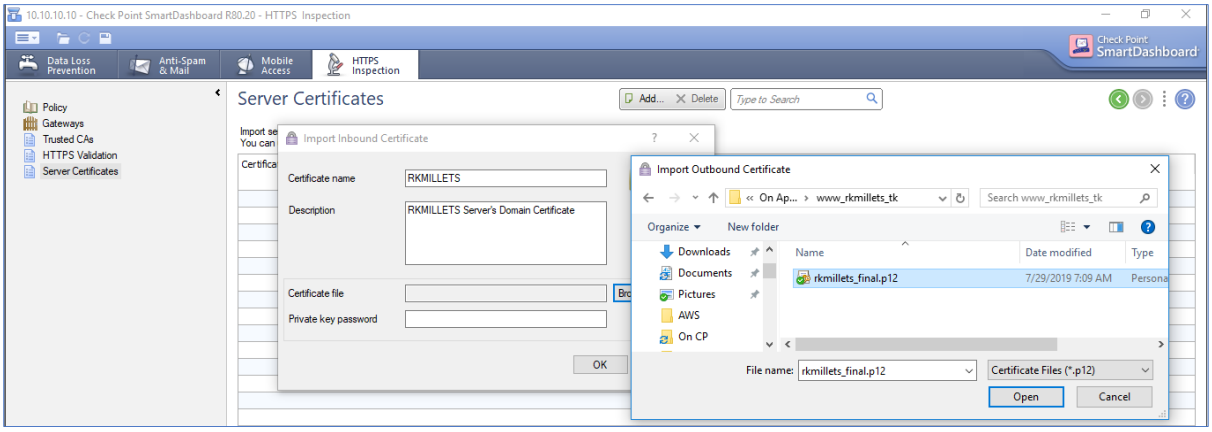
- On any Linux machine copy the RKMILLETS Server's Domain Certificate & it's Private Key and then generate the ***.p12*** certificate.

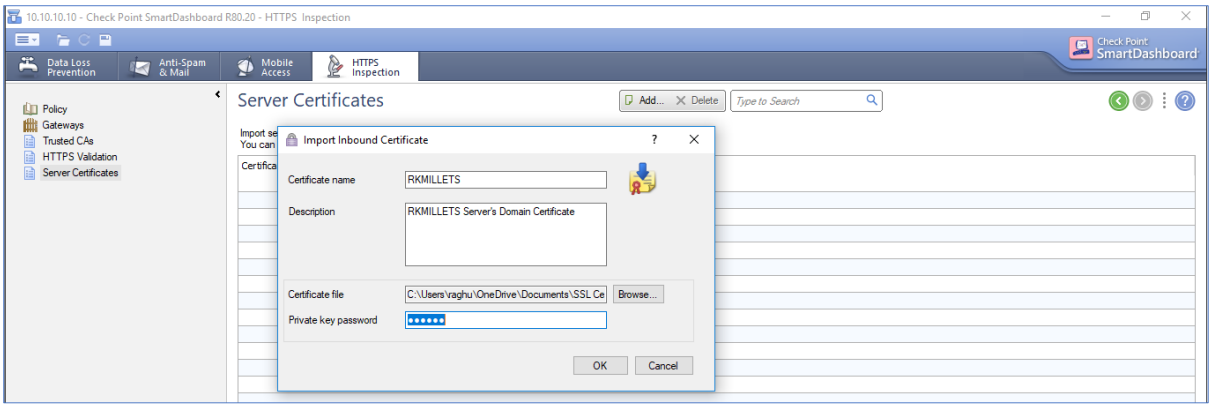


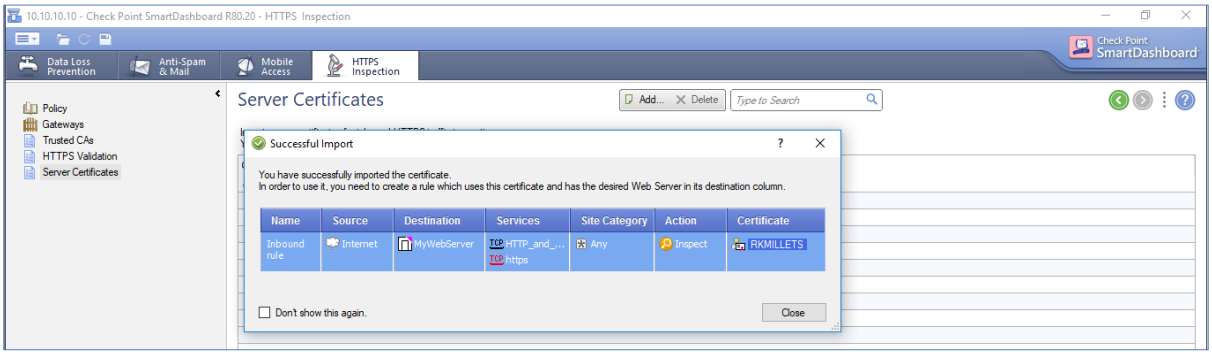
```
admin@RK-FW-BNG:~/RKMILLETS
[Expert@RK-FW-BNG:0]# cd RKMILLETS/
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# ls -lh
total 16K
-rw-r----- 1 admin root 5.7K Jul 24 16:32 ca-bundle-client.crt
-rw-r----- 1 admin root 2.6K Jul 24 16:32 www_rkmillets_tk.crt
-rw-r----- 1 admin root 1.7K Jul 29 07:05 www_rkmillets_tk.key
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# cat www_rkmillets_tk.crt ca-bundle-client.crt >> rkmillets_combined_cert.crt
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# ls -lh
total 28K
-rw-r----- 1 admin root 5.7K Jul 24 16:32 ca-bundle-client.crt
-rw-rw---- 1 admin root 8.2K Jul 29 07:07 rkmillets_combined_cert.crt
-rw-r----- 1 admin root 2.6K Jul 24 16:32 www_rkmillets_tk.crt
-rw-r----- 1 admin root 1.7K Jul 29 07:05 www_rkmillets_tk.key
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# cpopenssl pkcs12 -export -out rkmillets_final.p12 -in rkmillets_combined_cert.crt -inkey www_rkmillets_tk.key
Enter Export Password:
Verifying - Enter Export Password:
[Expert@RK-FW-BNG:0]#
[Expert@RK-FW-BNG:0]# ls -lh
total 36K
-rw-r----- 1 admin root 5.7K Jul 24 16:32 ca-bundle-client.crt
-rw-rw---- 1 admin root 8.2K Jul 29 07:07 rkmillets_combined_cert.crt
-rw-rw---- 1 admin root 7.6K Jul 29 07:09 rkmillets_final.p12
-rw-r----- 1 admin root 2.6K Jul 24 16:32 www_rkmillets_tk.crt
-rw-r----- 1 admin root 1.7K Jul 29 07:05 www_rkmillets_tk.key
[Expert@RK-FW-BNG:0]#
```

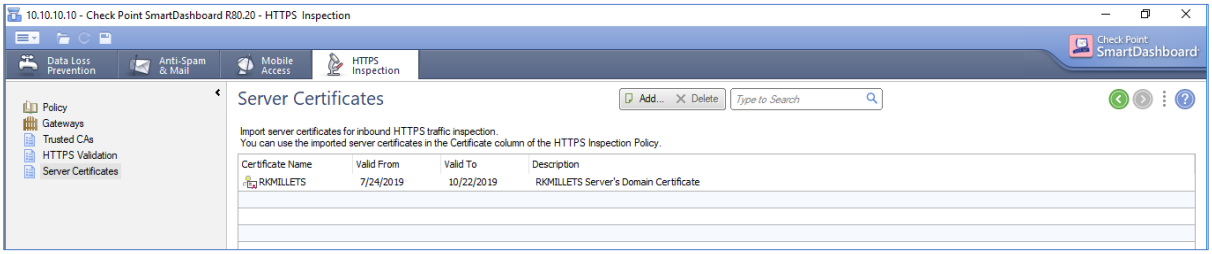
- Copy the Server's ***.p12*** certificate to your local machine and then import it on the Gateway.



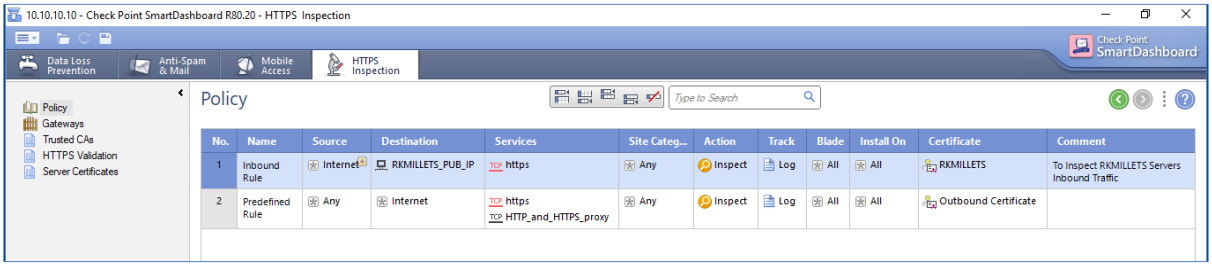








7. Define the Inbound HTTPS Inspection Rule on the Gateway by using the Server's Certificate that we have imported.



8. Install the Database on the Management Server & then Install the Policy on the Gateway and you are done with the configuration to inspect the Server's Inbound traffic.