How do I generate a new SSL certificate from my SonicWall firewall?

06/09/2022

1,912 People found this article helpful

161,247 Views

Description

Scenario

A network admin is trying to install a certificate, so that the web management of the device can be accessed without any certificate error.

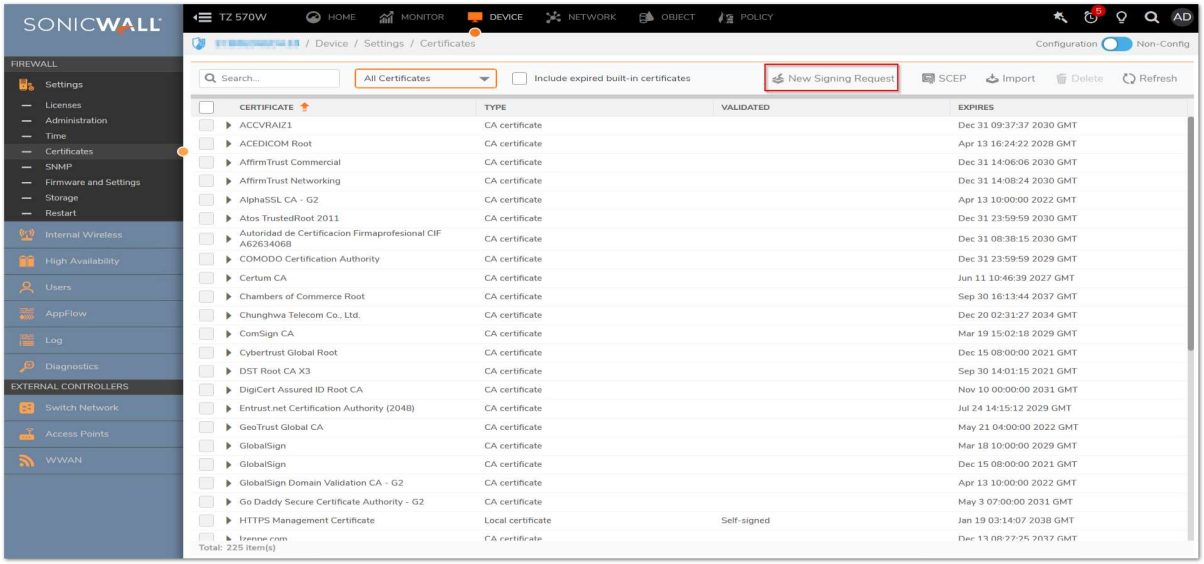
CAUTION: Will require a restart of the firewall.

In order to request and import a certificate from a certificate authority that will work on your appliance you will need to create a certificate signing request on the appliance.

Resolution for SonicOS 7.X

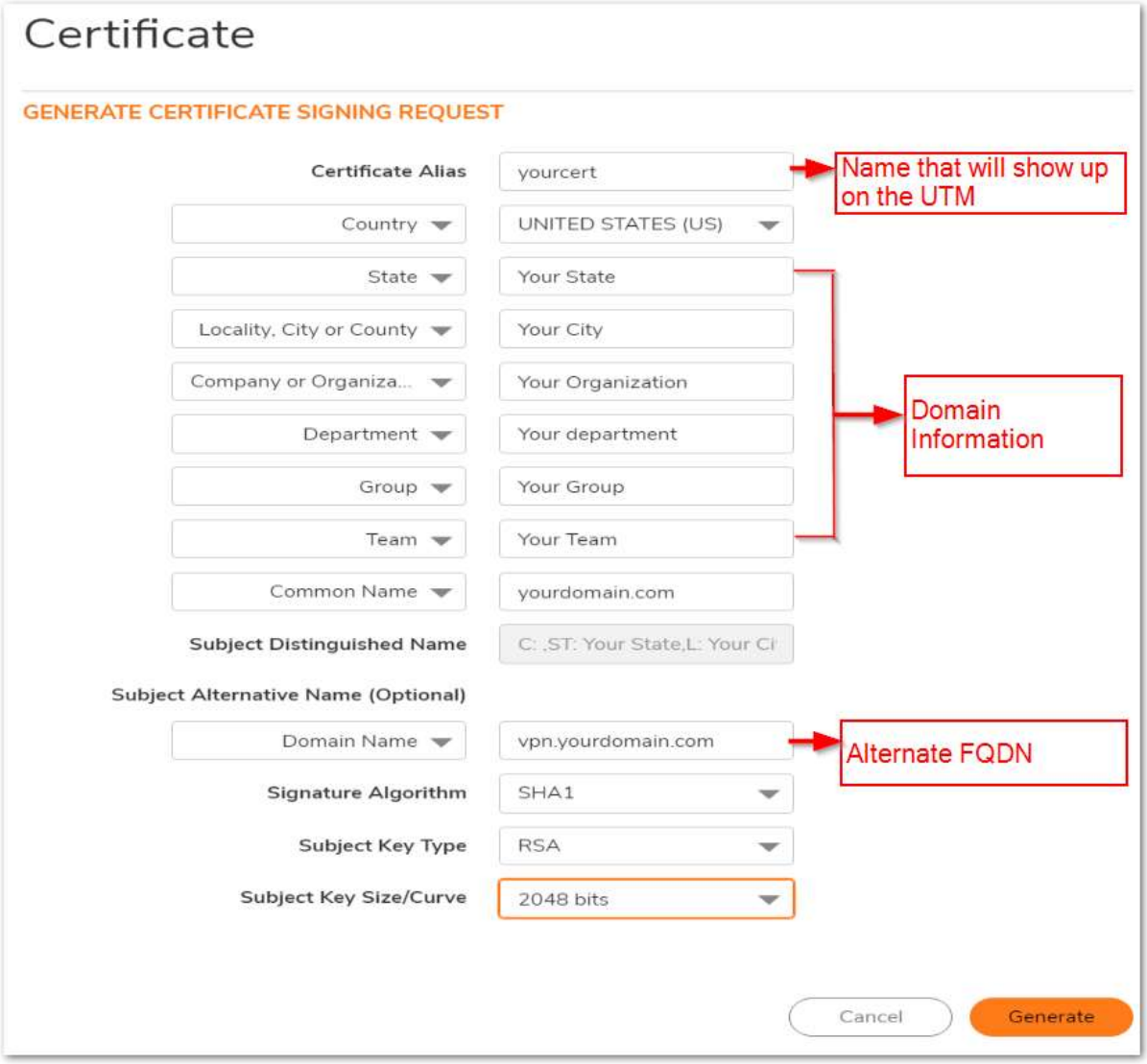
This release includes significant user interface changes and many new features that are different from the SonicOS 6.5 and earlier firmware. The below resolution is for customers using SonicOS 7.X firmware.

1. Log into the appliance and navigate to **Device | Settings | Certificates** and click **New Signing Request**.

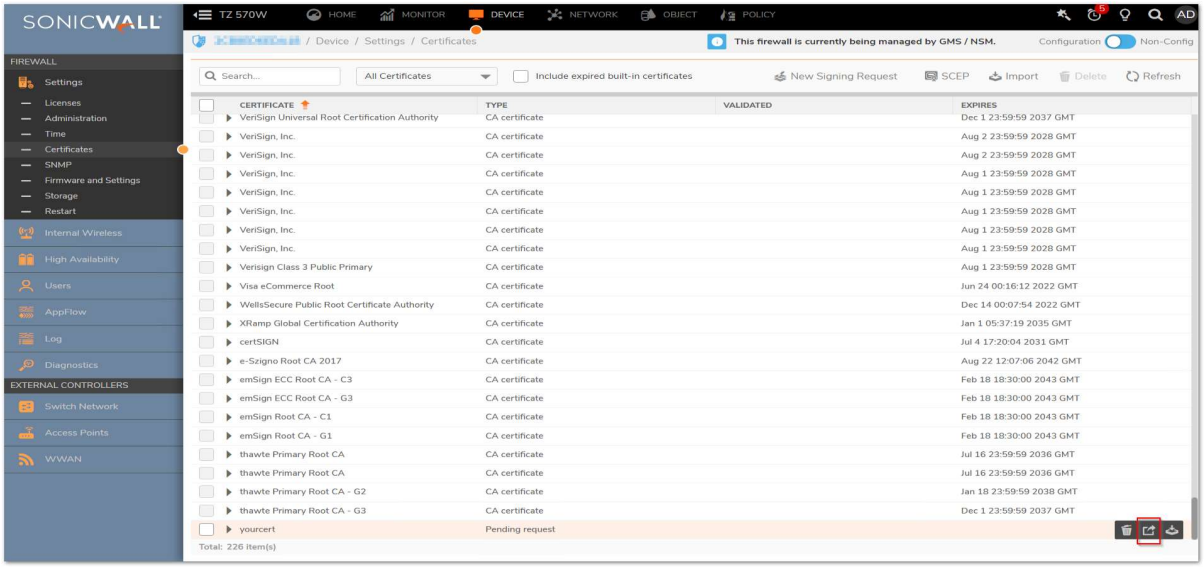


2. Fill out the **Certificate Signing Request** with information on the fully qualified domain name (FQDN) you will be using for the SSL.

📌 **TIP:** Wildcard for a domain would be *.yourdomain.com, Wildcard cost more but authenticate all subdomains on the domain.



3. Download the CSR. You can edit this with a text editor. Notepad ++ is a good option because it keeps the format that works best for copying a CSR request over to a certificate authority.



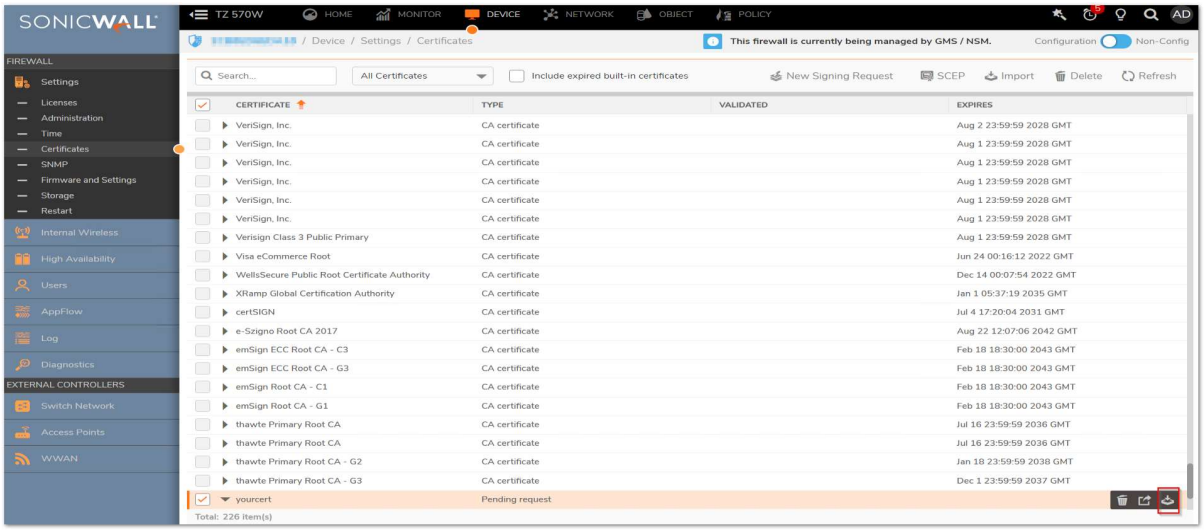
4. Request a SSL from your certificate authority providing this CSR text where they request.

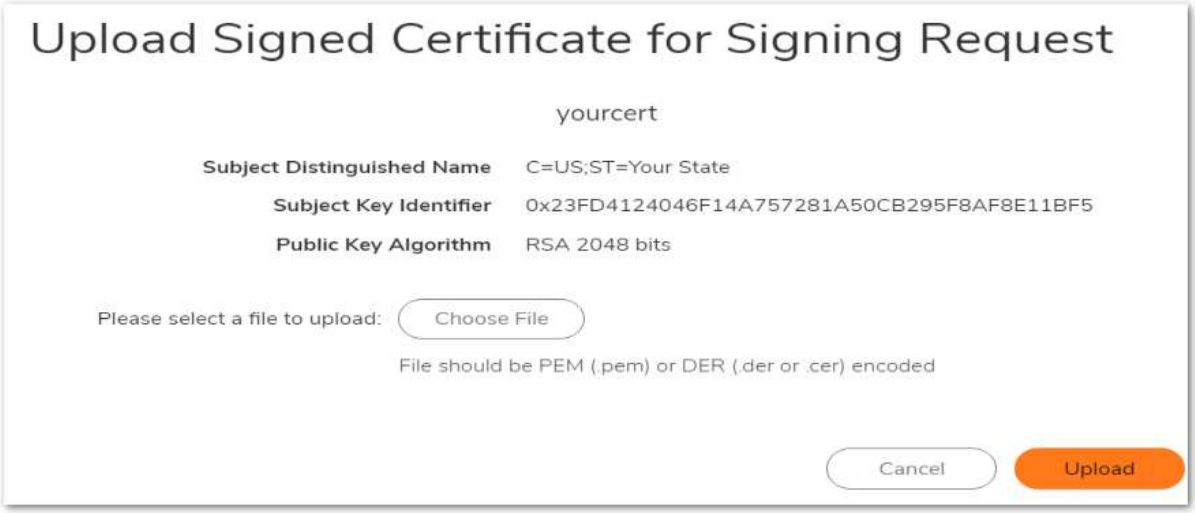
NOTE: When downloading the signed certificate from the certificate authority (such as GoDaddy or Thawte) select the server platform Apache SSL.

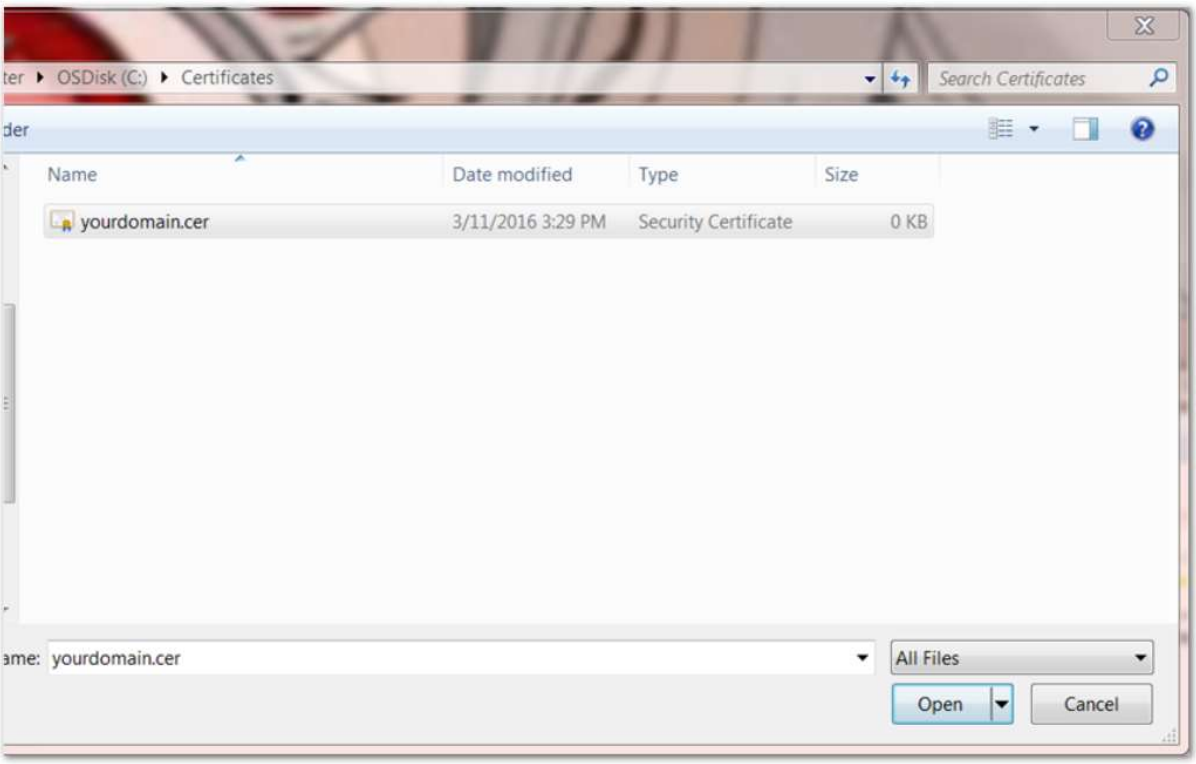
yourcert.p10

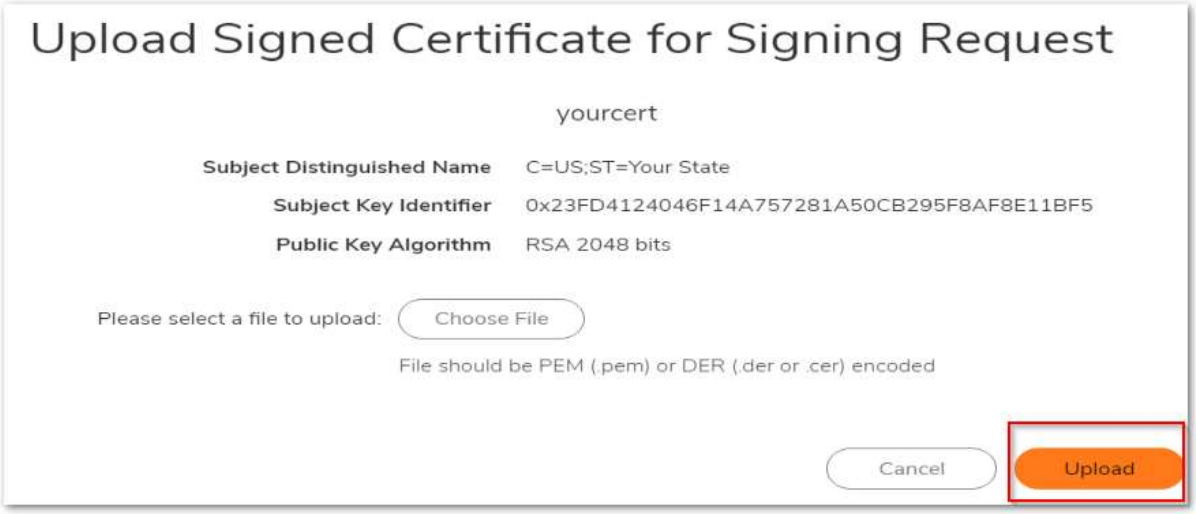
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDJDCCAgwCAQAwga4xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpZb3VyIFN0YXRl
MRIwEAYDVQQHEwlZb3VyIENpdHkxGjAYBgNVBAoTEVlvdXIgT3JnYW5pemF0aW9u
MRgwFgYDVQQLEw9Zb3VyIGRlcGFydG1lbnQxEzARBgNVBAsTCllvdXIgR3JvdXAx
EjAQBgNVBAsTCVlvdXIgVGVhbTEXMBUGA1UEAxMOeW91cmRvbWFpbi5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDMbHQL105FKAEuCGyD0pyXaHlz
efcvmbehMCrhRAdDOdLXxw09mA6L9pd+ElqORtLsrjAlITXb064ommp5Fa4gTYdQ
TATzcmKzrrqloXBwaZwK8W4A9OMI+iOx0J7rUERJpfaIVxRgcpRdG6k3z9JS/mIK
B0QZW2Oy/miO1Qpt6KValA/QFTEw1WnWpbVSACJcWVmQ22f64+9nd9odr6uW/uSh
5EOF1aqxt3nJfooRoYPx4prnTI63EAl16heDoNyr9KERIwBtd6pzsOBdILZ3msVk
2Vbi1SNgWKaIfB+C/szAa47AJ3pp/YlSmdHz92toeSjo12drYKKYSIh7WCK3AgMB
AAGgMDAuBgkqhkiG9w0BCQ4xITAfMB0GA1UdEQQWMBSCEnZwbi55b3VyZG9tYWlu
LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEARwceu7E96of9jxDKxFnOXvJYSt0e6Cvl
bBcRBqjlEf+F6rhDR3/1p4wdGGg7B6VoRpzquBFOhNUUhTFrs1QNFoWmwxDHgrJ6
EZD5/G4uIXGcYsyN5i0F3M74PwGRAsa12aILuH3REiJFZtuhavBq46Ya4jp5HJZv
QMbl2johSH2px0GO4dXM+0UtifvbzXafbmTW1XBBRhnOW4m5+6bdzEJaS8lhhZ8U
5aoO0UOaDkZ6tYsv9Tz3FGuUe9nN8l8jbhWdmzeGn8RpwQGQfxJLz9wUs++7ZEP1
xkJnmcZ5xKpYNpPQ/XIpSgyEPVZ4Wf+blp7uuYuuXR+ACfuvEHZ64A==
-----END CERTIFICATE REQUEST-----
```

5. Once you get the certificate back from the certificate authority upload the certificate to the pending request.




Upload Signed Certificate for Signing Request
yourcert
Subject Distinguished Name
C=US;ST=Your State
Subject Key Identifier
0x23FD4124046F14A757281A50CB295F8AF8E11BF5
Public Key Algorithm
RSA 2048 bits
Please select a file to upload:
Choose File
File should be PEM (.pem) or DER (.der or .cer) encoded
Cancel
Upload


OSDisk (C:)
Certificates
Search Certificates
Name
Date modified
Type
Size
yourdomain.cer
3/11/2016 3:29 PM
Security Certificate
0 KB
yourdomain.cer
All Files
Open
Cancel



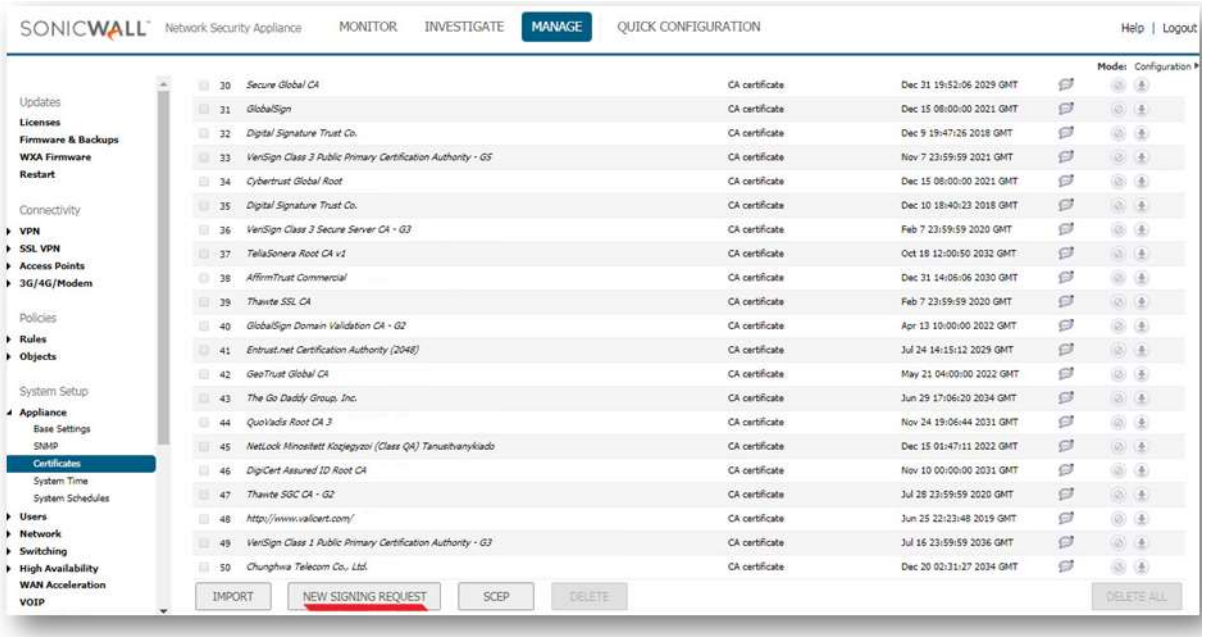
6. Restart the appliance to verify the certificate is installed and validated.

   📌 **TIP:** If the certificate shows "Validated No" use the following article to import the certificate chain to validate the SSL.

Resolution for SonicOS 6.5

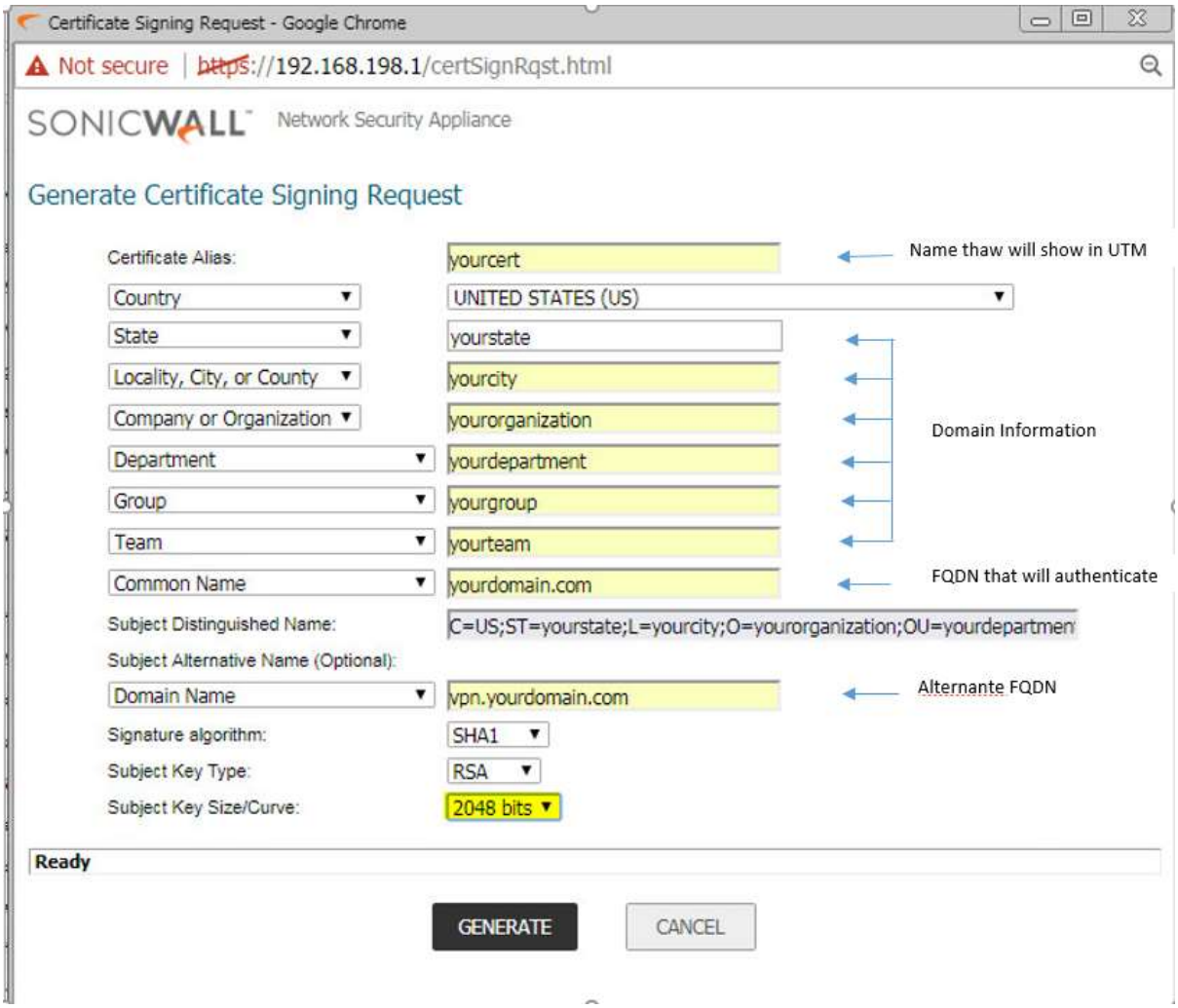
This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 firmware.

1. Log into the appliance and navigate to **Manage | Appliance | Certificates** and click **New Signing Request**.

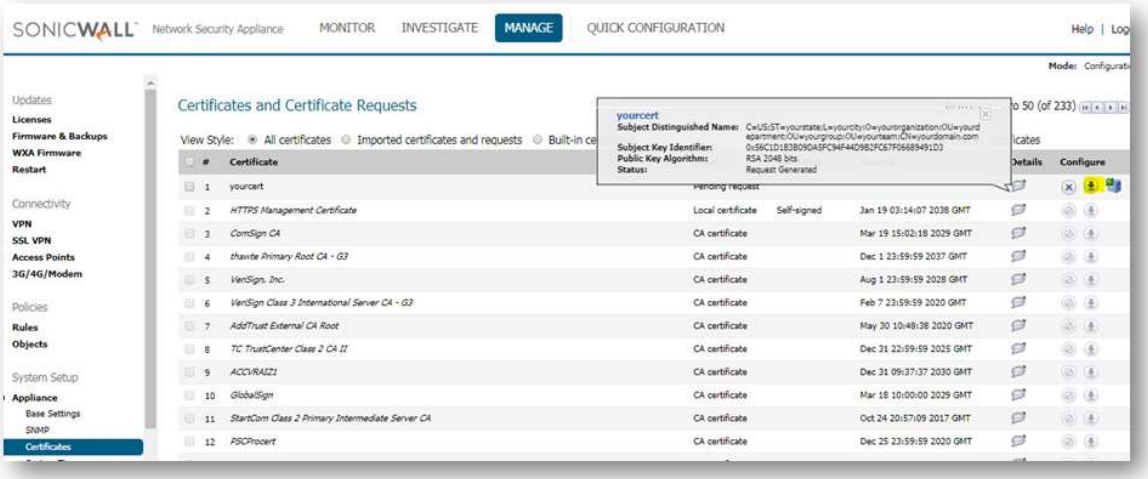


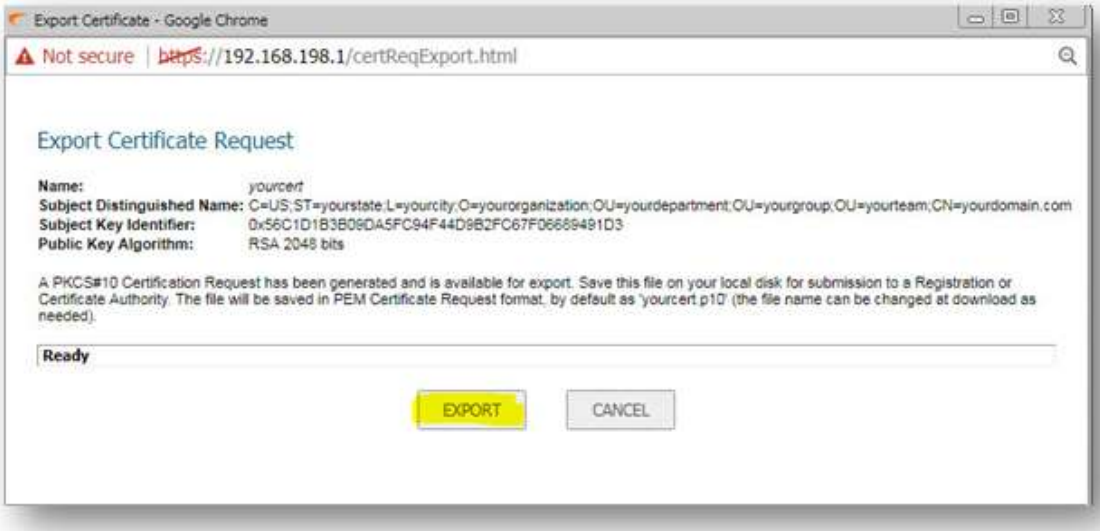
2. Fill out the **Certificate Signing Request** with information on the fully qualified domain name (FQDN) you will be using for the SSL.

📌 **TIP:** Wildcard for a domain would be *.yourdomain.com, Wildcard cost more but authenticate all subdomains on the domain.



3. Download the CSR. You can edit this with a text editor. Notepad ++ is a good option because it keeps the format that works best for copying a CSR request over to a certificate authority.





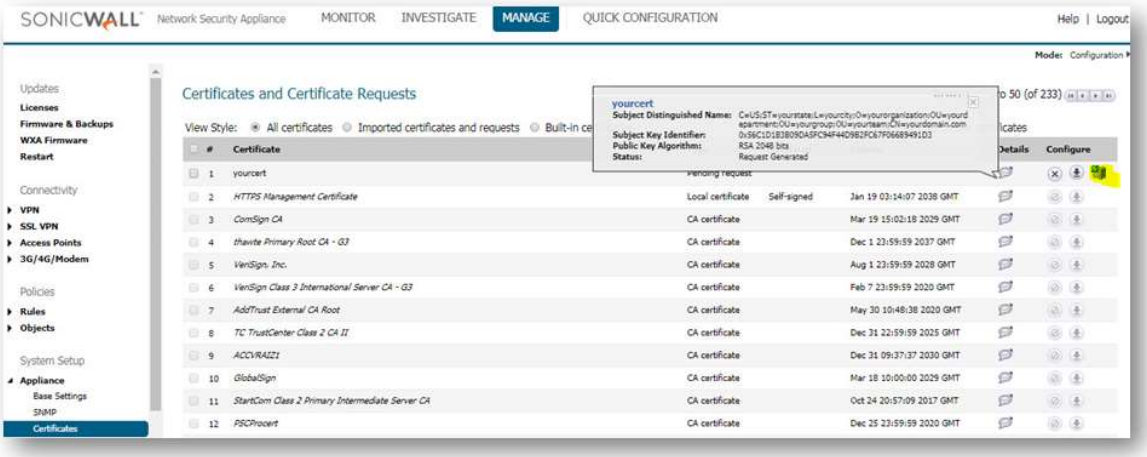
4. Request a SSL from your certificate authority providing this CSR text where they request.

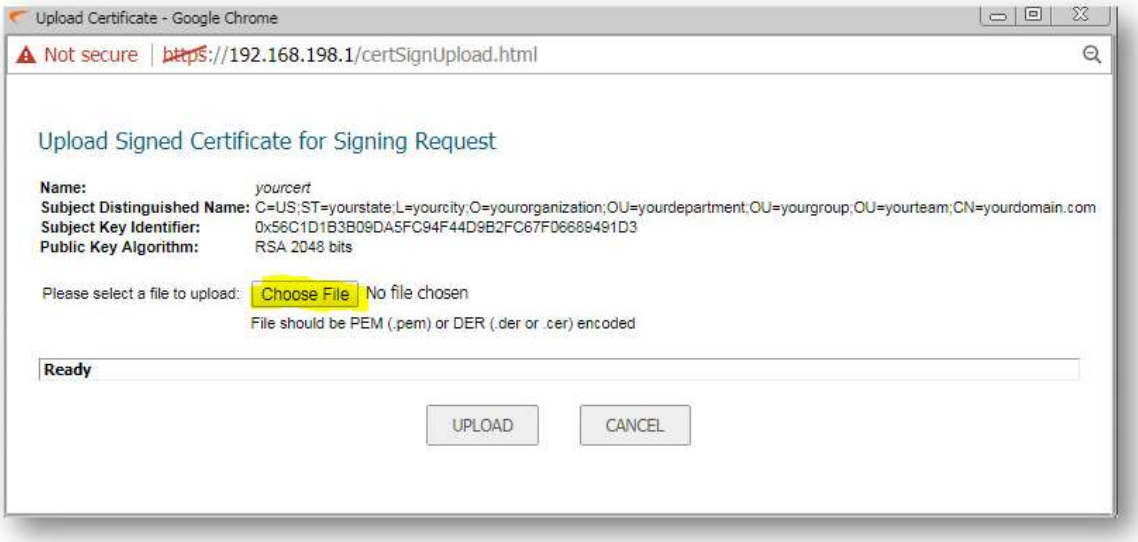
NOTE: When downloading the signed certificate from the certificate authority (such as GoDaddy or Thawte) select the server platform Apache SSL.

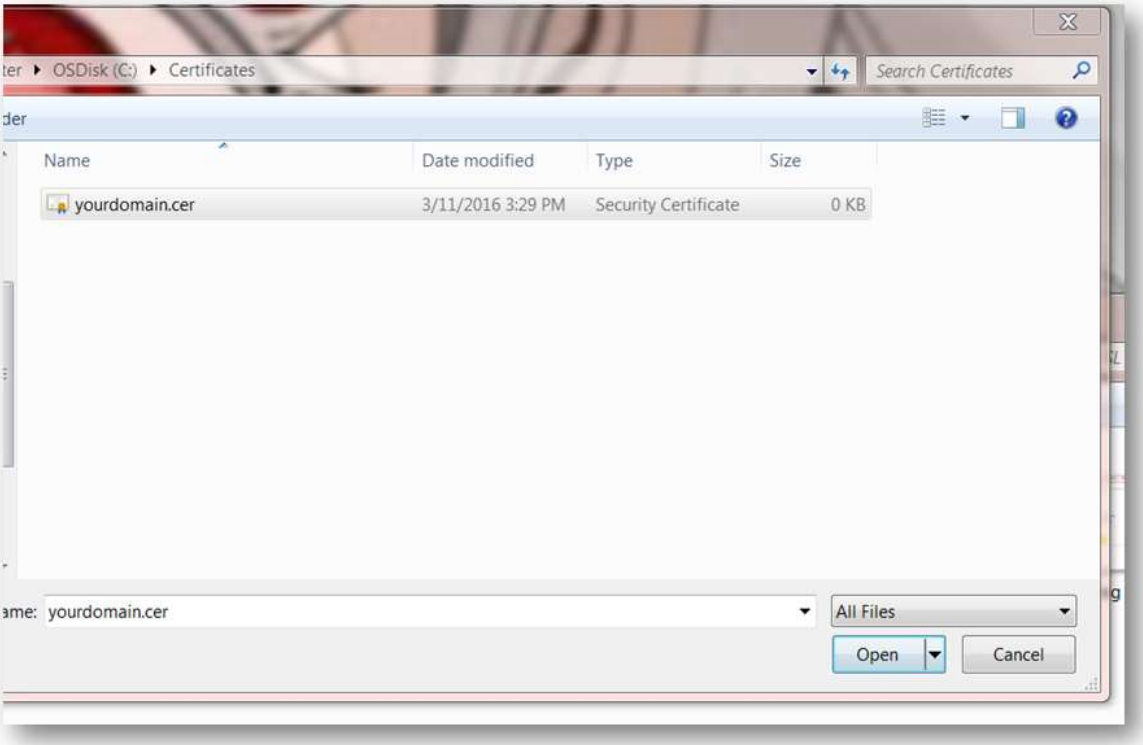
yourcert.p10

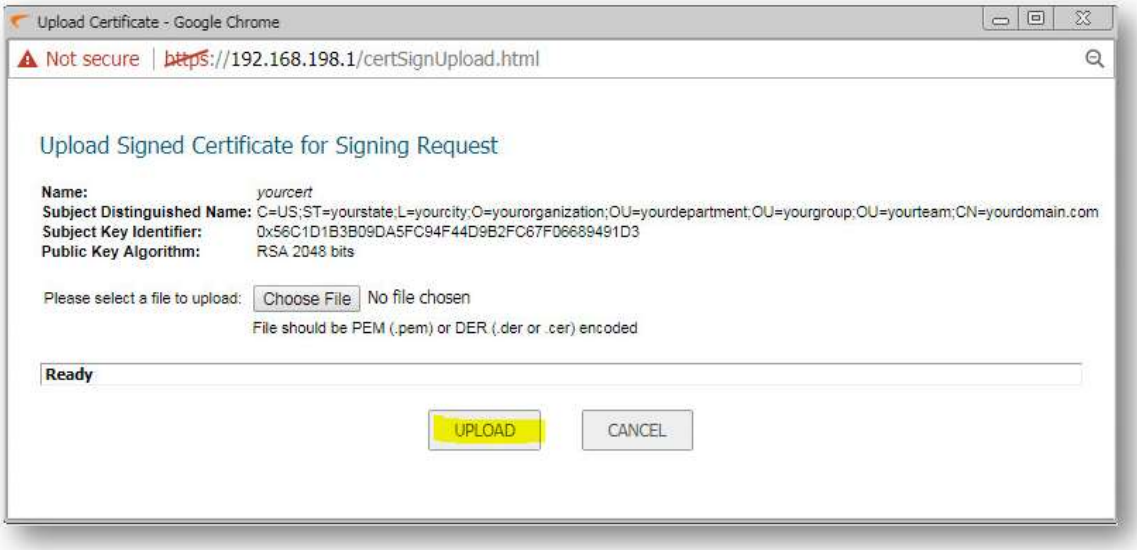
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDHjCCAgYCAQAwgagxCzAJBgNVBAYTAlVTMRIwEAYDVQQIEwl5b3Vyc3RhdGUx
ETAPBgNVBAcTCHlvdXJjaXR5MRkwFwYDVQQKExB5b3Vyb3JnYW5pemF0aW9uMRcw
FQYDVQQLEw55b3VyZGVwYXJ0bWVudDESMBAGA1UECxMJeW91cmdyb3VwMREwDwYD
VQQLEwh5b3VydGVhbTEXMBUGA1UEAxMOeW91cmRvbWFpbi5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCcR3q+N5XbTLK8E20VZnKQaFP70BYM0HvT
jkA3R3tJC3TpHiWC/bhA3B2DFb8JnrTTYO+2rPVYpB31y/IHW9VDYrLHxuoa5Vh7
BLN3jDX03EEuFmX0OvGn9rGFkeZ9KCgS4ZCcWzEixewqgU6jrVPn4wWJnJwERgPg
kdGu9dljBPZoAF4YFHZ4vlnzv6/qpLoiUYmlFZe9W+wLuKI8F0S/5Ozypa2qT1xZ
9hugubATTfeev1O2HCPSjmlPOyBIF4kFmWXnQxOabBkEoDexKyyDjwcwb+HZzoqX
OlvTDUMKxGJbq/kX+6QNNCEqKdPKNtORDRR9NQy7+c5mKib8OT0vAgMBAAGgMDAu
BgkqhkiG9w0BCQ4xITAfMB0GA1UdEQQWMBSCEnZwbi55b3VyZG9tYWluLmNvbTAN
BgkqhkiG9w0BAQsFAAOCAQEAHFfs+h76uta2boSOb/F4JKfNNqrnrbz1MN5yUXQm
R+LgBeJXoQus4ZW9xCu1R2/tPUTn3oOsBXVoHTQHxWAllefLQdUTWVKbq6xah0NR
gfiId4rxHcAD+9h9grxi8fEDmiVPmnH56pHn/t0s/jRitxCxjh0/7bgtfNKSrlNS
KZ32v1U5o9XTeFNqWA7QKtuTR7tIJ4DmHlt8RNXF5yLWPkqhEXqg3rSTzLmUN5Bc
Ml4e+xy8WGaI9maJc1zhe2ssHAH865Vkwi0YipOPPAFZ0J/jnPQRMylaFqR2Vga/
FHAaAowEjkTX/C+K7i0cgaqH9bgLFE1NFGeDIaXjW2rLhg==
-----END CERTIFICATE REQUEST-----
```

5. Once you get the certificate back from the certificate authority upload the certificate to the pending request.




Upload Certificate - Google Chrome
Not secure | https://192.168.198.1/certSignUpload.html
Upload Signed Certificate for Signing Request
Name: yourcert
Subject Distinguished Name: C=US;ST=yourstate;L=yourcity;O=yourorganization;OU=yourdepartment;OU=yourgroup;OU=yourteam;CN=yourdomain.com
Subject Key Identifier: 0x56C1D1B3B09DA5FC94F44D9B2FC67F06689491D3
Public Key Algorithm: RSA 2048 bits
Please select a file to upload:
Choose File
No file chosen
File should be PEM (.pem) or DER (.der or .cer) encoded
Ready
UPLOAD
CANCEL


OSDisk (C:) ▸ Certificates
Search Certificates
Name
Date modified
Type
Size
yourdomain.cer
3/11/2016 3:29 PM
Security Certificate
0 KB
yourdomain.cer
All Files
Open
Cancel



6. Restart the appliance to verify the certificate is installed and validated.

📌 **TIP:** If the certificate shows "Validated No" use the following article to import the certificate chain to validate the SSL: Importing Certificate Authority Chain.