



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**.

CERTIFICATE	TYPE	VALIDATED	EXPIRES
▶ ACCVRAIZ1	CA certificate		Dec 31 09:37:37 2030 GMT
▶ ACEDICOM Root	CA certificate		Apr 13 16:24:22 2028 GMT
▶ AffirmTrust Commercial	CA certificate		Dec 31 14:06:06 2030 GMT
▶ AffirmTrust Networking	CA certificate		Dec 31 14:08:24 2030 GMT
▶ AlphaSSL CA - G2	CA certificate		Apr 13 10:00:00 2022 GMT
▶ Alotus TrustedRoot 2011	CA certificate		Dec 31 23:59:59 2030 GMT
▶ Autoridad de Certificacion Firmaprofesional CIF A626344968	CA certificate		Dec 31 08:38:15 2030 GMT
▶ COMODO Certification Authority	CA certificate		Dec 31 23:59:59 2029 GMT
▶ Certum CA	CA certificate		Jun 11 10:46:39 2027 GMT
▶ Chambers of Commerce Root	CA certificate		Sep 30 16:13:44 2037 GMT
▶ Chunghwa Telecom Co., Ltd.	CA certificate		Dec 20 02:31:27 2034 GMT
▶ ComSign CA	CA certificate		Mar 19 15:02:18 2029 GMT
▶ Cybertrust Global Root	CA certificate		Dec 15 08:00:00 2021 GMT
▶ DST Root CA X3	CA certificate		Sep 30 14:01:15 2021 GMT
▶ DigiCert Assured ID Root CA	CA certificate		Nov 10 00:00:00 2031 GMT
▶ Entrust.net Certification Authority (2048)	CA certificate		Jul 24 14:15:12 2029 GMT
▶ GeoTrust Global CA	CA certificate		May 21 04:00:00 2022 GMT
▶ GlobalSign	CA certificate		Mar 18 10:00:00 2029 GMT
▶ GlobalSign	CA certificate		Dec 15 08:00:00 2021 GMT
▶ GlobalSign Domain Validation CA - G2	CA certificate		Apr 13 10:00:00 2022 GMT
▶ Go Daddy Secure Certificate Authority - G2	CA certificate		May 3 07:00:00 2031 GMT
▶ HTTPS Management Certificate	Local certificate	Self-signed	Jan 19 03:14:07 2038 GMT
▶ Itranse.com	CA certificate		Dec 13 08:27:25 2017 GMT

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.

Certificate

GENERATE CERTIFICATE SIGNING REQUEST

Certificate Alias	<input type="text" value="yourcert"/>	→ Name that will show up on the UTM
Country	<input type="text" value="UNITED STATES (US)"/>	
State	<input type="text" value="Your State"/>	→ Domain Information
Locality, City or County	<input type="text" value="Your City"/>	
Company or Organiza...	<input type="text" value="Your Organization"/>	
Department	<input type="text" value="Your department"/>	
Group	<input type="text" value="Your Group"/>	
Team	<input type="text" value="Your Team"/>	
Common Name	<input type="text" value="yourdomain.com"/>	
Subject Distinguished Name	<input type="text" value="C:.,ST: Your State,L: Your Ci"/>	
Subject Alternative Name (Optional)		
Domain Name	<input type="text" value="vpn.yourdomain.com"/>	→ Alternate FQDN
Signature Algorithm	<input type="text" value="SHA1"/>	
Subject Key Type	<input type="text" value="RSA"/>	
Subject Key Size/Curve	<input type="text" value="2048 bits"/>	

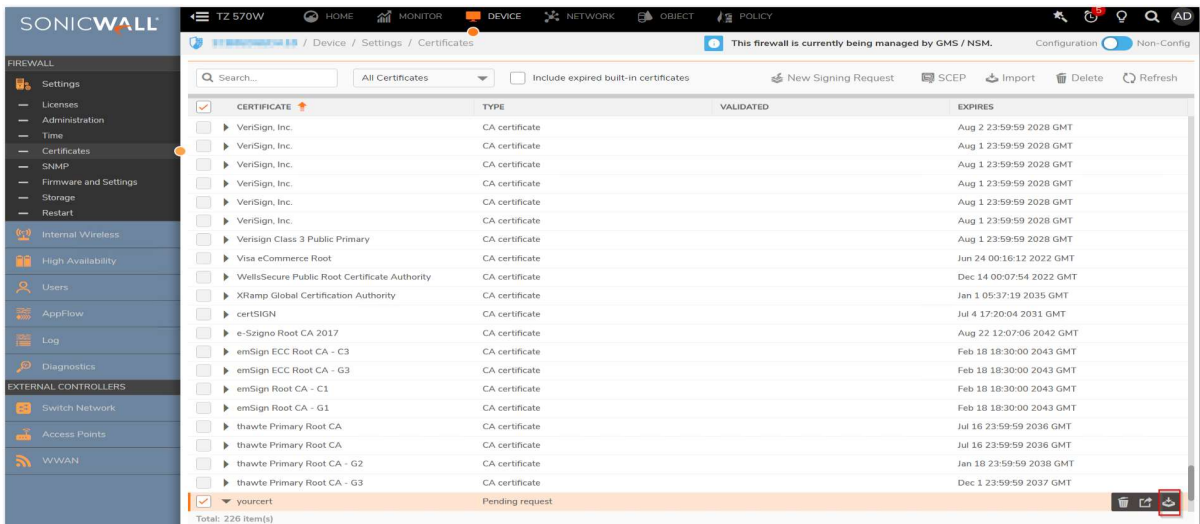
3. Download the CSR. You can edit this with a text editor. Notepad ++ is a good option because it keeps the format that works best for copying a CSR request over to a certificate authority.


```

yourcert.p10
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIDJDCCAgwCAQAwga4xCzAJBgNVBAYTA1VTMRMwEQYDVQQLIEwpcZb3VyIFN0YXRl
3 MRIwEAYDVQQHEwlZb3VyIENpdHkxGjAYBgNVBAoTEVlvdXIgT3JnYW5pemF0aW9u
4 MRgwFgYDVQQLEw9Zb3VyIGRlcGFydG11bnQxEzARBgNVBAsTC1lvdXIgR3JvdXAx
5 EjAQBgNVBAstCVlvdXIgVGhvbGVhbnRlcG91cmRvdWVpbi5jb20wgG91cmRvdWVp
6 MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQMhQ105FKAEuCGyD0pyXaHlz
7 efcvmbehMCRhRADdDdLXxw09mA6L9pd+ElqOrtLsrjAlITXb064ommp5Fa4gTYdQ
8 TATzcmKzrrqloXBwaZwK8W4A9OMI+iOx0J7rUERJpfaIVxRgcpRdG6k3z9JS/mIK
9 B0QZ2W0y/miO1Qpt6KValA/QFTewlWnWpbVSACJcWVmQ22f64+9nd9odr6uW/uSh
10 5EOf1aqxt3nJfooRoYPx4prnTI63EAl16heDoNyr9KERIwBtd6pzsOBdILZ3msVk
11 2Vbi1SNgWKAIfB+C/szAa47AJ3pp/YlSmdHz92toeSjo12drYKKYSih7WCK3AgMB
12 AAGMDAuBgkqhkiG9w0BCQ4xITAFMB0GA1UdEQQWMBSCEnZwbi55b3VyZG9tYWlu
13 LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEARwceu7E96of9jxDKxFnOXvJYSt0e6Cv1
14 bBcRBqj1Ef+F6rhDR3/1p4wdGGg7B6VoRpzquBFOhNUUHTFrslQNFoWmwxDHgrJ6
15 EZD5/G4uIXGcYsyN5i0F3M74PwGRAsal2aILuH3REiJFZtuhavBq46Ya4jp5HJZv
16 QMb12johSH2px0GO4dXM+0UtifvzbXafbmTW1XBBRhnOW4m5+6bdzEJaS8lhhZ8U
17 5ao0UOaDkZ6tYsv9Tz3FGuE9nN818jbhWdmzeGn8RpWQGFxJLz9wUs++7ZEP1
18 xkJnmcZ5xKpYNpPQ/XIpSgyEPVZ4Wf+blp7uuYuuXR+ACfuvEHZ64A==
19 -----END CERTIFICATE REQUEST-----
20

```

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



Upload Signed Certificate for Signing Request

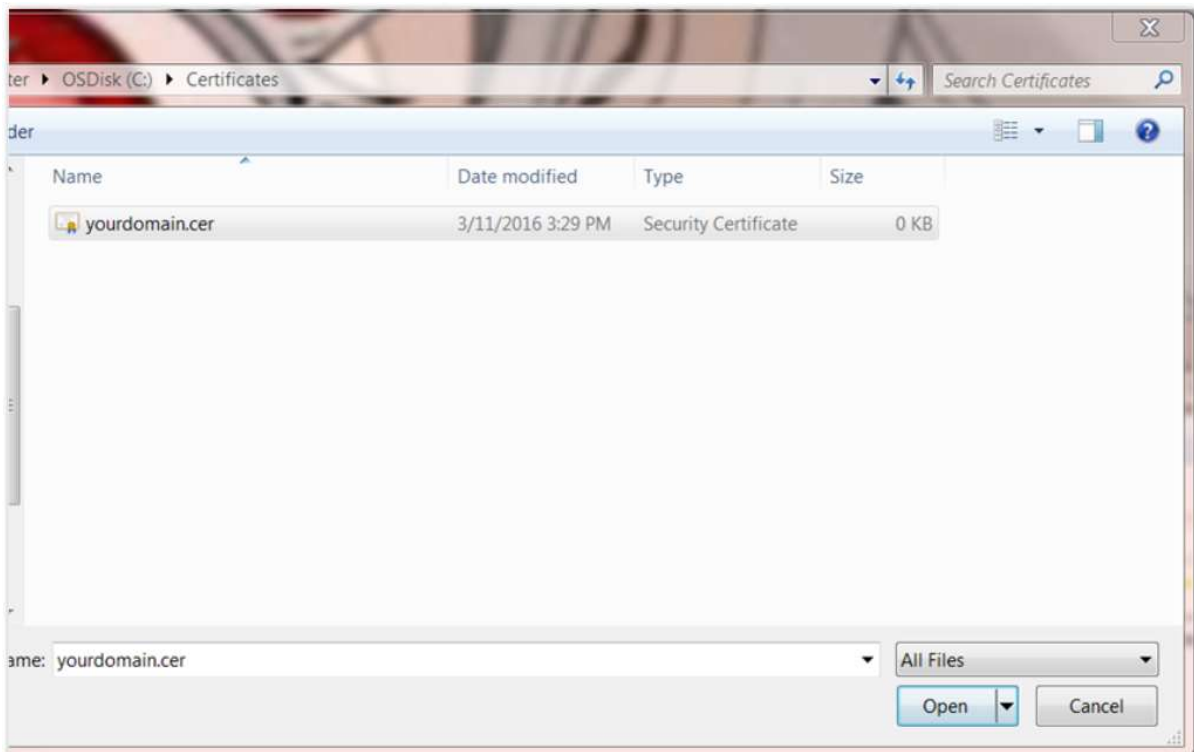


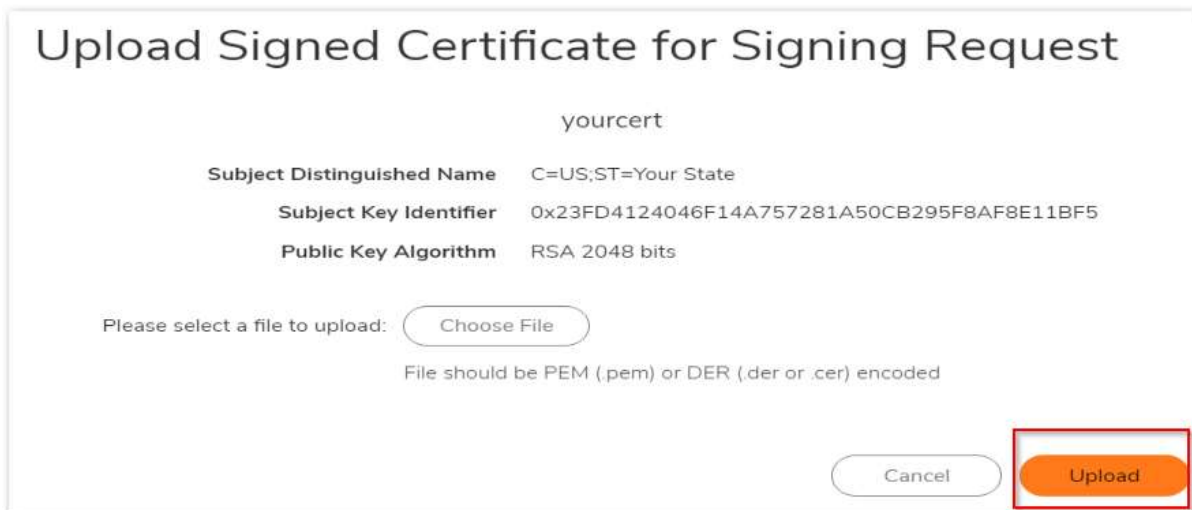
yourcert

Subject Distinguished Name C=US;ST=Your State
Subject Key Identifier 0x23FD4124046F14A757281A50CB295F8AF8E11BF5
Public Key Algorithm RSA 2048 bits

Please select a file to upload:

File should be PEM (.pem) or DER (.der or .cer) encoded





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:

File should be PEM (.pem) or DER (.der or .cer) encoded

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**.

SONICWALL Network Security Appliance MONITOR INVESTIGATE **MANAGE** QUICK CONFIGURATION Help | Logout

Updates
Licenses
Firmware & Backups
WXA Firmware
Restart

Connectivity
VPN
SSL VPN
Access Points
3G/4G/Modem

Policies
Rules
Objects

System Setup
Appliance
Base Settings
SNMP
Certificates
System Time
System Schedules

Users
Network
Switching
High Availability
WAN Acceleration
VOIP

ID	Name	Type	Expiration	Mode	Configuration
30	Secure Global CA	CA certificate	Dec 31 19:52:06 2029 GMT		
31	GlobalSign	CA certificate	Dec 15 08:00:00 2021 GMT		
32	Digital Signature Trust Co.	CA certificate	Dec 9 19:47:26 2018 GMT		
33	VeriSign Class 3 Public Primary Certification Authority - G5	CA certificate	Nov 7 23:59:59 2021 GMT		
34	Cybertrust Global Root	CA certificate	Dec 15 08:00:00 2021 GMT		
35	Digital Signature Trust Co.	CA certificate	Dec 10 18:40:23 2018 GMT		
36	VeriSign Class 2 Secure Server CA - G3	CA certificate	Feb 7 23:59:59 2020 GMT		
37	TeliaSonera Root CA v1	CA certificate	Oct 18 12:00:50 2032 GMT		
38	AffirmTrust Commercial	CA certificate	Dec 31 14:06:06 2030 GMT		
39	Thawte SSL CA	CA certificate	Feb 7 23:59:59 2020 GMT		
40	GlobalSign Domain Validation CA - G2	CA certificate	Apr 13 10:00:00 2022 GMT		
41	Entrust.net Certification Authority (2048)	CA certificate	Jul 24 14:15:12 2029 GMT		
42	GeoTrust Global CA	CA certificate	May 21 04:00:00 2022 GMT		
43	The Go Daddy Group, Inc.	CA certificate	Jun 29 17:06:20 2034 GMT		
44	QuoVadis Root CA 3	CA certificate	Nov 24 19:06:44 2031 GMT		
45	NetLock Minostett Kozjegyzoi (Class QA) Tanusitvanykiado	CA certificate	Dec 15 01:47:11 2022 GMT		
46	DigiCert Assured ID Root CA	CA certificate	Nov 10 00:00:00 2031 GMT		
47	Thawte SSC CA - G2	CA certificate	Jul 28 23:59:59 2020 GMT		
48	http://www.valicert.com/	CA certificate	Jun 25 22:23:48 2019 GMT		
49	VeriSign Class 1 Public Primary Certification Authority - G3	CA certificate	Jul 16 23:59:59 2026 GMT		
50	Chunghwa Telecom Co., Ltd.	CA certificate	Dec 20 02:31:27 2034 GMT		

IMPORT **NEW SIGNING REQUEST** SCEP DELETE DELETE ALL

- 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.



Certificate Signing Request - Google Chrome
Not secure | https://192.168.198.1/certSignRqst.html

SONICWALL Network Security Appliance

Generate Certificate Signing Request

Certificate Alias: yourcert ← Name that will show in UTM

Country: UNITED STATES (US)

State: yourstate

Locality, City, or County: yourcity

Company or Organization: yourorganization

Department: yourdepartment

Group: yourgroup

Team: yourteam

Common Name: yourdomain.com ← FQDN that will authenticate

Subject Distinguished Name: C=US;ST=yourstate;L=yourcity;O=yourorganization;OU=yourdepartment

Subject Alternative Name (Optional): Domain Name: ypn.yourdomain.com ← Alternante FQDN

Signature algorithm: SHA1

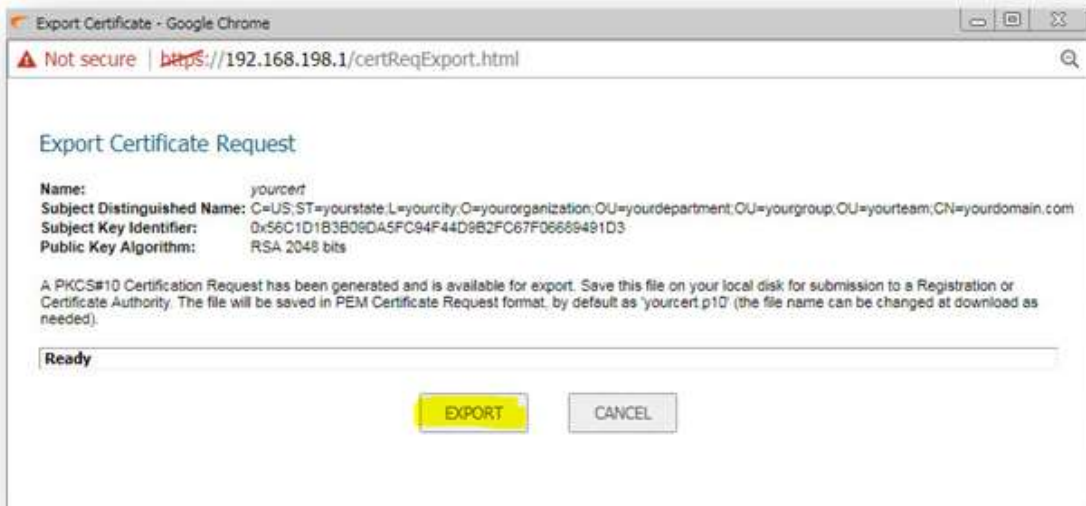
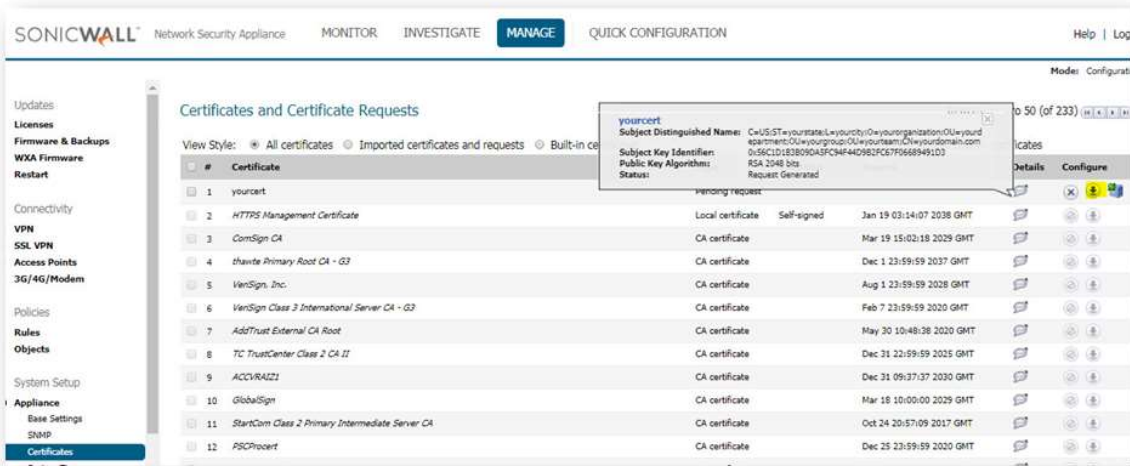
Subject Key Type: RSA

Subject Key Size/Curve: 2048 bits


Ready

GENERATE CANCEL

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.

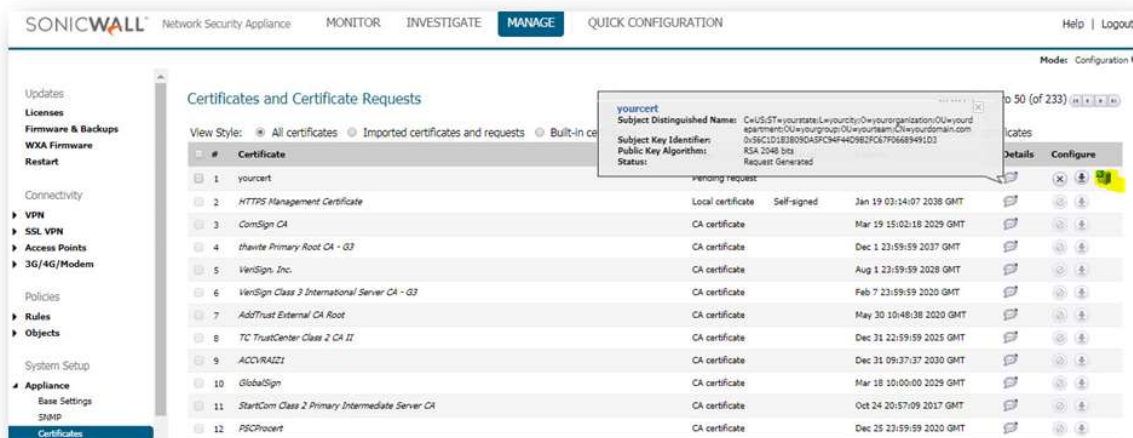
 **NOTE:** When downloading the signed certificate from the certificate authority (such as GoDaddy or Thawte) select the server platform Apache SSL.

```

1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIDHjCCAgyCAQAwgagxCzAJBgNVBAYTA1VTMRIWEAYDVQQIEw15b3Vyc3RhdGUx
3 ETAPBgNVBACrTCH1vdXJjaXR5MRkwFwYDVQQKEwB5b3Vyb3JnYW5pemF0aW9uMRcw
4 FQYDVQQLew55b3Vyc2VwYXJ0bWVudDESMBAGA1UECzMJeW91cmdyb3VwMREwDwYD
5 VQQLewh5b3VydGVhbTEwMREwDwYDZSMBAGA1UEAxMOeW91cmRvbWVwYXJ0bWVudE
6 SIb3DQEBAAQAA4IBDwAwggEKAoIBAQCc3q+N5XbTLK8E20VznKQaFP70BYM0HvT
7 jkA3R3tJC3TPHiWC/bhA3B2DFb8JnrTTYO+2rPVYpB31y/IHW9VDYrLHxuoA5Vh7
8 BLN3jDX03EEuFmX0OvGn9rGFkeZ9KCgS4ZCcWzEixewqGU6jrVPn4wWJnJwERgPg
9 kdGu9dljBPZoAF4YFHZ4vlnzv6/gpLoiUYmlFZe9W+wLuKI8F0S/5Ozypa2qT1xZ
10 9hugubATTfeevlO2HCPSjmlPOyBIF4kFmWXnQxOabBkEoDexKyyDjwcbw+HzzoqX
11 OlvTDUMKxGJbq/kX+6QNNCEqKdPKntORDRR9NQy7+c5mKib8OT0vAgMBAAGgMDAu
12 BgkqhkiG9w0BCQ4xITAFMB0GA1UdEQQWMBSCEnZwbi55b3Vyc2VwYXJ0bWVudE
13 BgkqhkiG9w0BAQsFAAOCAQEAHffs+h76uta2boSob/F4JKfNNqnrnbz1MN5yUXQm
14 R+LgBeJXoQus4Zw9xCu1R2/tPUTn3oOsBXVoHTQHxWallefLQdUTVWkbq6xah0NR
15 gfiId4rxHcAD+9h9grxi8fEDmiVPmnh56pHn/t0s/jRitxCxjh0/7bgtfNKSrlNS
16 KZ32v1U5o9XTeFNqWA7QktuTR7tIJ4DmH1t8RNXF5yLWPkqhEXqg3rSTzLmUN5Bc
17 M14e+xy8WGaI9maJc1zhe2ssSHAH865VkwI0YipOPPAFZ0J/jnPQRMyLaFqR2Vga/
18 FHAAaOweJkTX/C+K7i0cgaqH9bgLFE1NFGeDIaXjW2rLhg==
19 -----END CERTIFICATE REQUEST-----
20

```

- 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

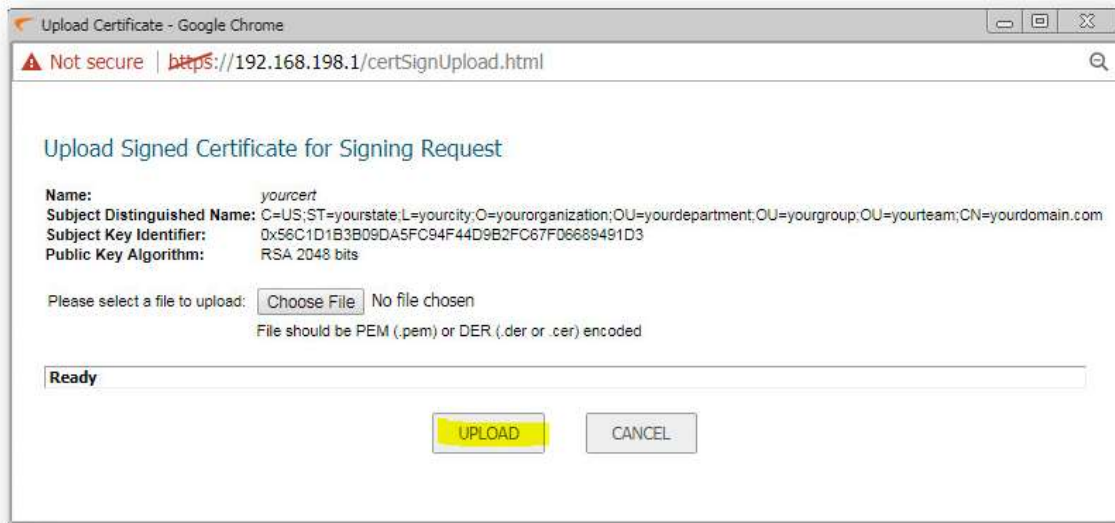
OSDisk (C:) > Certificates

Search Certificates

Name	Date modified	Type	Size
yourdomain.cer	3/11/2016 3:29 PM	Security Certificate	0 KB

Name: yourdomain.cer All Files

Open Cancel



- 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](#).
-