

Request your server certificate

Create and sign a Certificate Signing Request (CSR) to send to your Certificate Authority.

Generate a private key for your server certificate

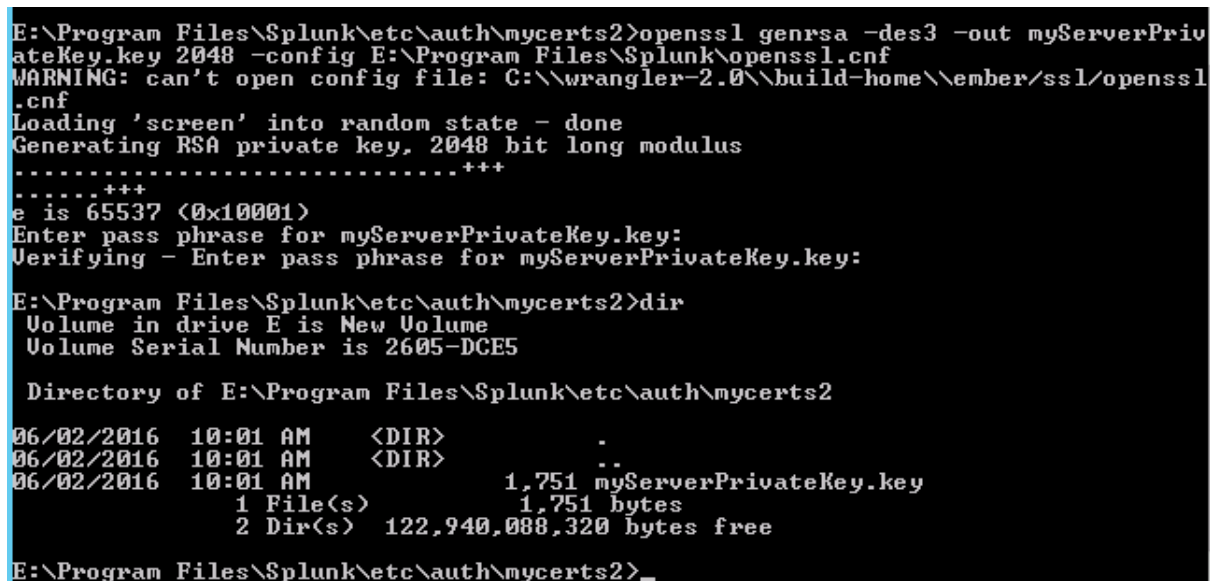
1. Create a new private key. The following example uses DES3 encryption and a 2048 bit key length, we recommend a key length of 2048 or higher.

In Windows:

```
openssl genrsa -des3 -out myServerPrivateKey.key 2048 -config E:\Program Files\Splunk\openssl.cnf
```

2. When prompted, create a password for your key.

When you are done, a new private key myServerPrivateKey.key is created in your directory. You will use this key to sign your Certificate Signing Request (CSR).



```
E:\Program Files\Splunk\etc\auth\mycerts2>openssl genrsa -des3 -out myServerPrivateKey.key 2048 -config E:\Program Files\Splunk\openssl.cnf
WARNING: can't open config file: C:\wrangler-2.0\build-home\ember\ssl\openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for myServerPrivateKey.key:
Verifying - Enter pass phrase for myServerPrivateKey.key:

E:\Program Files\Splunk\etc\auth\mycerts2>dir
Volume in drive E is New Volume
Volume Serial Number is 2605-DCE5

Directory of E:\Program Files\Splunk\etc\auth\mycerts2

06/02/2016  10:01 AM    <DIR>          .
06/02/2016  10:01 AM    <DIR>          ..
06/02/2016  10:01 AM                1,751 myServerPrivateKey.key
               1 File(s)                1,751 bytes
               2 Dir(s)  122,940,088,320 bytes free

E:\Program Files\Splunk\etc\auth\mycerts2>
```

Generate a new Certificate Signing Request (CSR)

1. Use your private key myServerPrivateKey.key to generate a CSR for your server certificate:

In Windows:

```
openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr -config "E:\Program Files\Splunk\openssl.cnf"
```

2. When prompted, provide the password you created for your private key myServerPrivateKey.key.

3. Provide the requested information for your certificate. To use common-name checking, make sure to provide a Common Name when entering your certificate details.

```
E:\Program Files\Splunk\etc\auth\mycerts2>openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr -config "E:\Program Files\Splunk\openssl.cnf"
WARNING: can't open config file: C:\wrangler-2.0\build-home\ember\ssl\openssl.cnf
Enter pass phrase for myServerPrivateKey.key:
Loading 'screen' into random state - done
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]:AU
State or Province Name (full name) [Some-State]:VIC
Locality Name (eg, city) []:Melbourne
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BNW Consulting
Organizational Unit Name (eg, section) []:Splunk
Common Name (e.g. server FQDN or YOUR name) []:splunk2.bnwconsulting.com.au
Email Address []:warwick.chai@bnwconsulting.com.au

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0000
An optional company name []:0000

E:\Program Files\Splunk\etc\auth\mycerts2>dir
Volume in drive E is New Volume
Volume Serial Number is 2605-DCE5

Directory of E:\Program Files\Splunk\etc\auth\mycerts2

06/02/2016  10:03 AM    <DIR>          .
06/02/2016  10:03 AM    <DIR>          ..
06/02/2016  10:03 AM                1,163 myServerCertificate.csr
06/02/2016  10:01 AM                1,751 myServerPrivateKey.key
                2 File(s)      2,914 bytes
                2 Dir(s)  122,940,063,744 bytes free

E:\Program Files\Splunk\etc\auth\mycerts2>
```

When you are done, a new CSR myServerCertificate.csr appears in your directory.

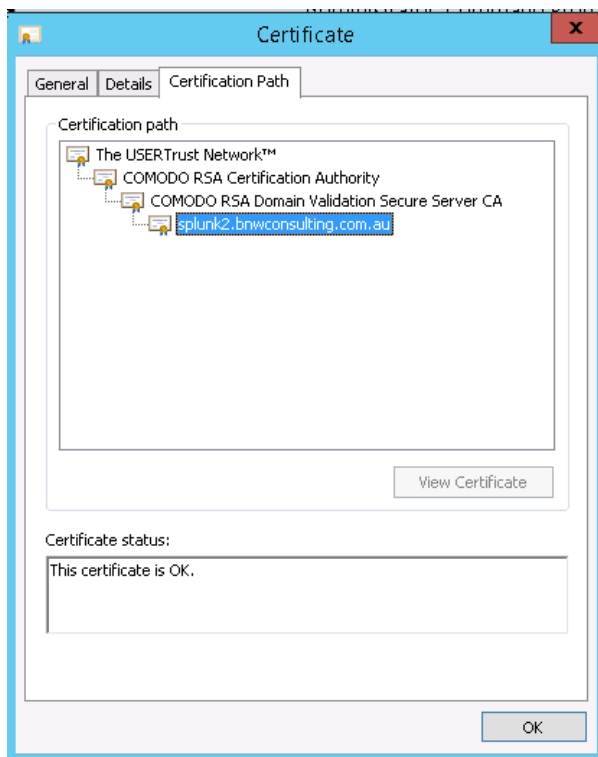
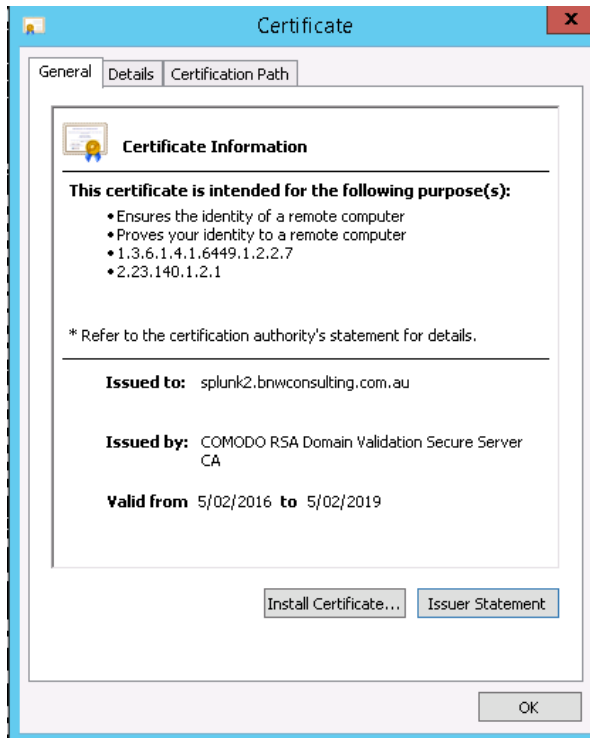
Download and verify the server certificate and public key

- 1. Send your CSR to your Certificate Authority (CA) to request a new server certificate. The request process varies based on the Certificate Authority you use.
- 2. When it's ready, download the new server certificate from your Certificate Authority. For the examples in this manual, let's call this myServerCertificate.pem.

```
06/02/2016  10:44 AM                8,378 myServerCertificate.pem
```

- 3. Also download your Certificate Authority's public CA certificate. For the examples in this manual, let's call this myCACertificate.pem.

We received a pksc7 from our provider file so this already contains the entire chain, if the entire chain is not present you will need to add the certificates in the chain to the file.



Next steps

You should now have the following files in the directory you created, which is everything you need to configure indexers, forwarders, and Splunk instances that communicate over the management port:

myServerCertificate.pem

myServerPrivateKey.key

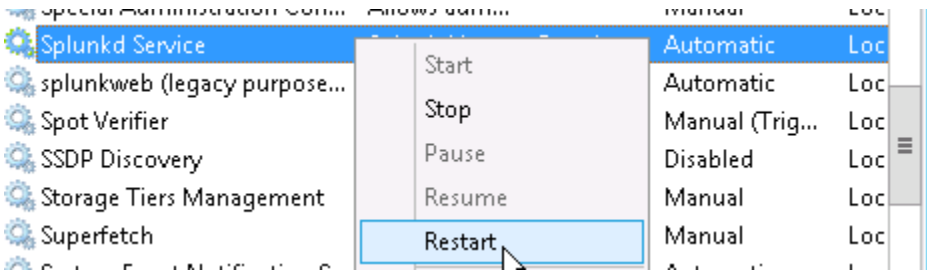
myCACertificate.pem

Now that you have the certificates you need, you must prepare your server certificate (including appending any intermediate certificates), and then configure Splunk to find and use your certificates:

Edit local server.conf

```
[sslConfig]
enableSplunkdSSL = true
#sslKeysfilePassword = $1$1qBMGcZBWjWY
sslKeysfile = myServerPrivateKey.key
sslKeysfilePassword = 0000
caCertFile = myServerCertificate.pem
caPath = $SPLUNK_HOME/etc/auth/mycerts2
```

Restart Splunk



Hit the management port and check the certificate being presented

Open the local certificate and we can see the certificate chain

Browser address bar: <https://localhost:8080> Certifi... splunkd - Splunk

Splunk Certificate

Updated: 2016-02-07T22:00:00

- [rpc](#)
- 2016-02-07T22:00:00
- [services](#)
- 2016-02-07T22:00:00
- [servicesNS](#)
- 2016-02-07T22:00:00
- [static](#)
- 2016-02-07T22:00:00

General Details Certification Path

Certification path

- The USERTrust Network™
- COMODO RSA Certification Authority
- COMODO RSA Domain Validation Secure Server CA
- splunk2.bnwconsulting.com.au

View Certificate

Certificate status:

This certificate is OK.

OK