KB009 Splunk – Adding a CA signed certificate to the restAPI HTTPS port

Affected release: All

Condition:

- Customer wants to use a CA signed certificate, to ensure the certificate issues by Splunk matches the hostname being used to access the restAPI which is a requirement for HTTPS / SSL to function.

http://docs.splunk.com/Documentation/Splunk/6.3.2/Security/Howtogetthird-partycertificates

How to get certificates signed by a third-party

This topic describes one way you can use the version of OpenSSL that ships with Splunk Enterprise to obtain third-party certificates that you can use to secure your forwarder-to-indexer and inter-Splunk communication.

Before you begin

In this discussion, $SPLUNK_HOME (%SPLUNK_HOME% on Windows) refers to the Splunk Enterprise installation directory. On Windows, you might need to set this variable at the command line or in the Environment tab in the System Properties dialog.

On Windows, the Splunk Enterprise directory is at C:\Program Files\Splunk by default. For most Unix platforms, the default installation directory is at /opt/splunk. For Mac OS, it is /Applications/splunk. See the Administration Guide to learn more about working with Windows and *nix.

Make sure that you are using the version of OpenSSL provided with Splunk Enterprise by setting your environment to the version in $SPLUNK_HOME/splunk/lib in *nix or %SPLUNK_HOME%/splunk/bin in Windows.

Create a new directory for your certificates

Create a new directory to work from when creating your certificates. In our example, we are using $SPLUNK_HOME/etc/auth/mycerts2:

mkdir E:\Program Files\Splunk\etc\auth\mycerts2

cd E:\Program Files\Splunk\etc\auth\mycerts2

Splunk strongly recommends that you make a new folder so that you do not overwrite the existing certificates in $SPLUNK_HOME/etc/auth for your new certificates and keys. Working in a new directory protects the certificates that ship with Splunk and lets you use them for other Splunk components as necessary.

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

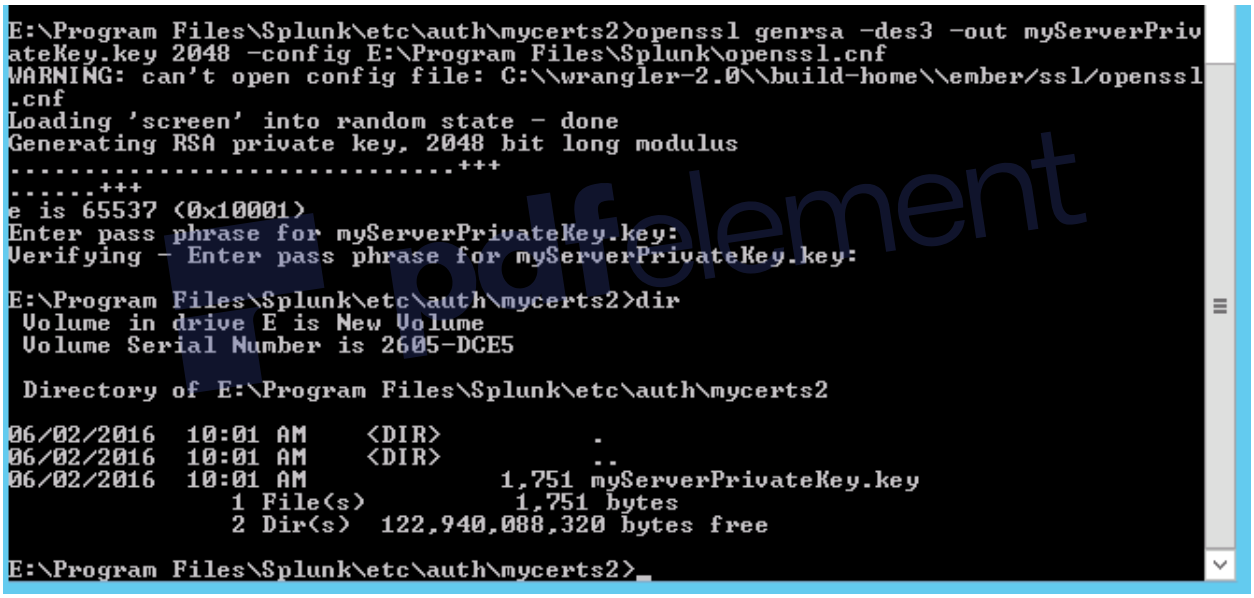
1. Create a new private key. The following example uses DES3 encryption and a 2048 bit key length, we recommend a key length of 2048 or higher.

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).



Generate a new Certificate Signing Request (CSR)

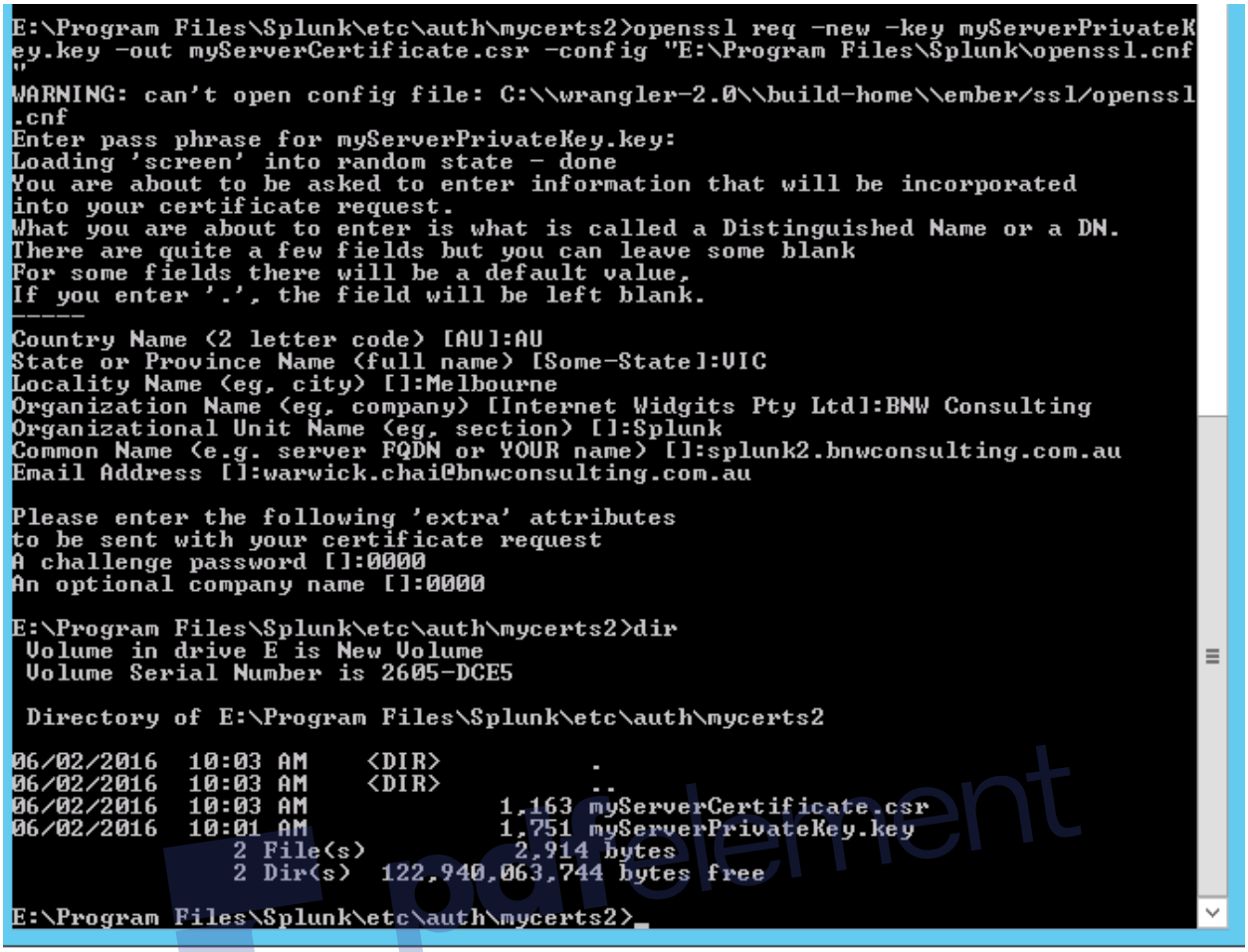
1. Use your private key myServerPrivateKey.key to generate a CSR for your server certificate:

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.



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.

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.

```
5F2dhEuF5Hw7V48DWw==
-----END CERTIFICATE-----

subject=/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA
issuer=/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
-----BEGIN CERTIFICATE-----
MIIGCDCCA/CgAwIBAgIQKy5u6tl1NmwUim7bo3yMBzANBgkqhkiG9w0BAQwFADCB
hTELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxKzApBgNV
```

new 1

```
subject=/OU=Domain Control Validated/OU=PositiveSSL/CN=splunk2.bnwconsulting.com.au
issuer=/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA
-----BEGIN CERTIFICATE-----
MIIFeTCCBGGgAwIBAgIRAI2C4w+7U3ORlTOy6fFLjZwwDQYJKoZIhvcNAQELBQAw
gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
```

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

subject=/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
issuer=/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
-----BEGIN CERTIFICATE-----
MIIFdDCCBFygAwIBAgIQJ2buVutJ846r13Ci/ITeIjANBgkqhkiG9w0BAQwFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFk
ZFRydXN0IEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
```

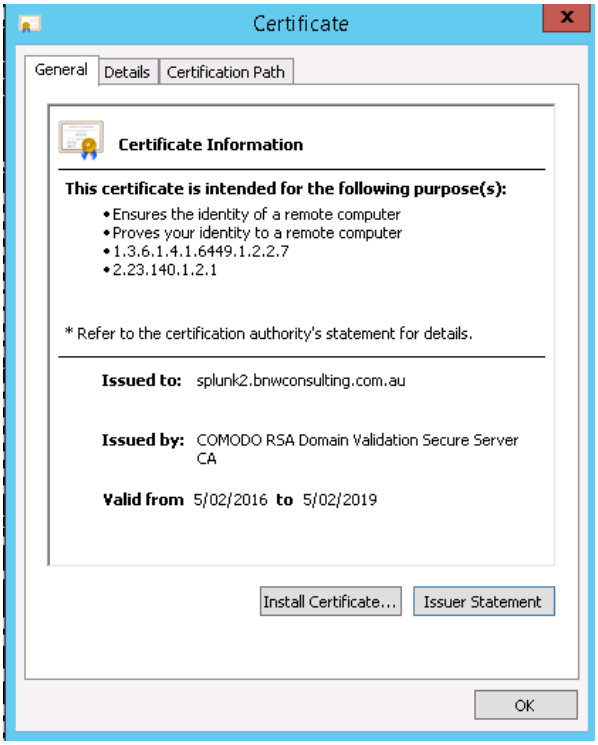
```
PUsE2JOAWVrgQSQdso8VYFhH2+9uRv0V9dlfmrPb2LjkQLPNlzmuhbsdjrzch5vR
pu/xO28QOG8=
-----END CERTIFICATE-----

subject=/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
issuer=/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
-----BEGIN CERTIFICATE-----
MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
MBIGA1UEChMLOWRkVHJ1c3OaOUIxJiAkBgNVBAsTHUFkZFRvdXN0IEV4dGVvbmFs
```

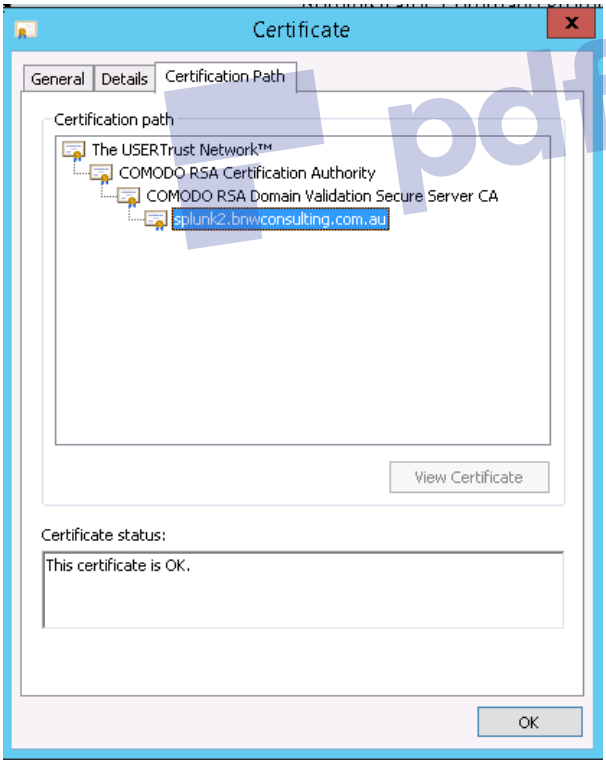

If your Certificate Authority does not provide you with certificates in PEM format, you must convert them using the OpenSSL command appropriate to your existing file type, consult your OpenSSL documentation for more information about converting different file types.

4. View the contents to make sure it has everything you need:

The “Issuer” entry should refer to your CA’s information.

The “Subject” entry should show the information (country name, organization name, Common Name, etc.) that you entered when creating the CSR earlier.





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:

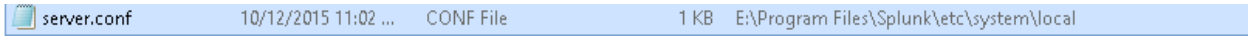
myServerCertificate.pem

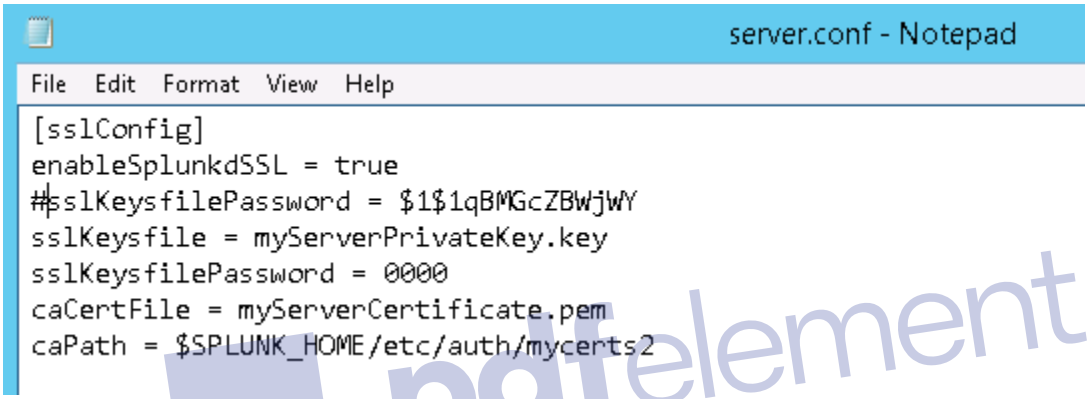
myServerPrivateKey.key

myCACertificate.pem

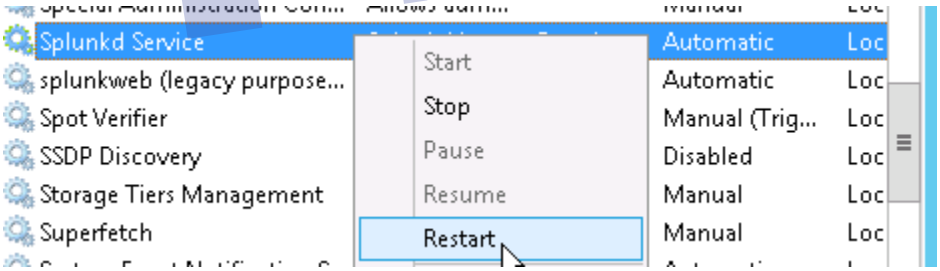
Now that you have the certificates you need, you must prepare your server certificate (including appending any intermediate certificates), and then configure Splunk to find and use your certificates:

Edit local server.conf





Restart Splunk



Hit the management port and check the certificate being presented

Open the local certificate and we can see the certificate chain