Splunk® Enterprise
Securing Splunk Enterprise 8.0.3

Secure Splunk Web with your own certificate

Generated: 4/05/2020 2:15 am
Secure Splunk Web with your own certificate

This example assumes that you have already generated self-signed certificates or purchased third-party certificates. If you have not done this and are unsure how to proceed, we've provided some simple examples:

- Self-sign certificates for Splunk Web.
- Get a certificates signed by a third-party for Splunk Web.

Before you begin: make sure your certificate and key are available from your folder. In this example we are using $SPLUNK_HOME/etc/auth/mycerts/:

- $SPLUNK_HOME/etc/auth/mycerts/mySplunkWebCertificate.pem
- $SPLUNK_HOME/etc/auth/mycerts/mySplunkWebPrivateKey.key

Configure Splunk Web to use the key and certificate files

1. In $SPLUNK_HOME/etc/system/local/web.conf (or any other applicable location, if you are using a deployment server), make the following changes to the [settings] stanza:

   The following is an example of an edited settings stanza:

   [settings]
   enableSplunkWebSSL = true
   privKeyPath = </home/etc/auth/mycerts/mySplunkWebPrivateKey.key >
   serverCert = </home/etc/auth/mycerts/mySplunkWebCertificate.pem >

   Absolute paths may be used. non-absolute paths are relative to $SPLUNK_HOME

2. Restart Splunk:

   # $SPLUNK_HOME/bin/splunk restart splunkd