Splunk® Enterprise Securing Splunk Enterprise 7.0.1

About securing Splunk Enterprise with SSL

Generated: 12/13/2019 9:52 am
About securing Splunk Enterprise with SSL

This section describes the types of Splunk configurations that you might want to secure with SSL.

About the default certificates

Splunk software ships with, and is configured to use, a set of default certificates. These certificates discourage casual snoopers but could still leave you vulnerable, because the root certificate is the same in every Splunk download and anyone with the same root certificate can authenticate.

The default certificates are generated and configured at startup and can be found in \$SPLUNK_HOME/etc/auth/. They are set to expire three years after they are generated and new certificates must be created and configured at that time.

- For information about the default certificate for Splunk Web, see "Turn on encryption (https) with Splunk Web." or "Turn on encryption (https) using web.conf."
- For information about SSL for forwarding with the default certificate, see "Configure Splunk forwarding to use the default certificate."

Ways you can secure Splunk Enterprise

You can apply encryption and/or authentication using your own certificates for:

- Communications between the browser and Splunk Web
- Communication from Splunk forwarders to indexers
- Other types of communication, such as communications between Splunk instances over the management port

The table below describes the most common scenarios and the default SSL settings:

<table>
<thead>
<tr>
<th>Type of exchange</th>
<th>Node A function</th>
<th>Node B function</th>
<th>Encryption</th>
<th>Certificate Authentication</th>
<th>Common Name checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser to Splunk Web</td>
<td>Browser</td>
<td>Splunk Web</td>
<td>NOT enabled by default</td>
<td>dictated by client (browser)</td>
<td>dictated by client</td>
</tr>
<tr>
<td></td>
<td>Splunk Web</td>
<td></td>
<td>enabled by default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of exchange</td>
<td>Node A function</td>
<td>Node B function</td>
<td>Encryption</td>
<td>Certificate Authentication</td>
<td>Common Name checking</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>-----------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Splunk Web to search head</td>
<td>splunkd as a search head</td>
<td>splunkd as a search head</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Forwarding</td>
<td>splunkd as a forwarder</td>
<td>splunkd as an indexer</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Deployment server to deployment clients</td>
<td>splunkd as a deployment client</td>
<td>splunkd as deployment server</td>
<td>enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Distributed search</td>
<td>splunkd as search peer</td>
<td>splunkd as a search head</td>
<td>Enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Search head clusters</td>
<td>splunkd as cluster members</td>
<td>splunkd as cluster members</td>
<td>Not enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Search head cluster deployer</td>
<td>splunkd as cluster members</td>
<td>splunkd as cluster deployer</td>
<td>Enabled by default</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
<tr>
<td>Indexer cluster peer nodes</td>
<td>splunkd as indexer cluster peer nodes</td>
<td>splunkd as indexer cluster peer nodes</td>
<td>NOT enabled by default. You must use the replication_port-ssl</td>
<td>NOT enabled by default</td>
<td>NOT enabled by default</td>
</tr>
</tbody>
</table>
Setting in `server.conf` to enable replication of data over SSL:

<table>
<thead>
<tr>
<th>Type of exchange</th>
<th>Node A function</th>
<th>Node B function</th>
<th>Encryption</th>
<th>Certificate Authentication</th>
<th>Common Name checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexer cluster master</td>
<td>splunkd as peer and search head nodes</td>
<td>splunkd as a master node</td>
<td>Enabled by default</td>
<td>NOT enabled by default</td>
<td>use Pass4SymmKey instead</td>
</tr>
</tbody>
</table>

**Communications between the browser and Splunk Web**

Browser to Splunk Web data most commonly consists of search requests and returned data.

Data encryption (HTTPS) can be easily turned on using Splunk Web, or by editing the `configuration files`. Keep in mind that encryption with the default certificate protects against casual listening but is not fully secure.

For better security, replace the default certificates with certificates signed by a trusted CA. We strongly recommend using CA certs rather than signing your own in this case. Unless you have the ability to add your CA to the certificate stores in every browser that will access Splunk Web, a self-signed certificate is considered untrusted by users' browsers. For more information, see "About securing Splunk Web."

**Splunk forwarders to indexers**

Data sent from forwarders to indexers is the data that your indexers use for searches and reports. Depending upon your organization and the nature and format of the data being transmitted and Splunk configuration, this data may or may not be readable or sensitive.

Securing sensitive raw data helps to avoid snooping and man-in-the-middle attacks.

You can turn on SSL encryption using the default certificate to provide encryption and compression. However, communication using the default certificate does not provide secure authentication, as the certificate password is supplied with every
installation of Splunk software. The default certificates are set to expire three years after initial startup, and forwarder to indexer communications will fail at this point.

For better security, require certificate authentication using a self- or CA-signed certificate. A certificate signed by a known and mutually trusted Certificate Authority is considered more secure by outside parties than a certificate you sign yourself. For more information about using certificates with Splunk forwarders and indexers, see "About securing data from forwarders."

**Other SSL communications**

Other Splunk communications happen between different instances of Splunk software over the management port, usually but not always in a distributed environment. An example of this is configuration data sent by a deployment server to clients. This type of SSL encryption is enabled by default. For most configurations this is adequate and is the recommended security method. However, if you do need to secure your communications with SSL authentication, we’ve provided some guidelines to help you in "About securing Splunk to Splunk communication" in this manual.

To learn about more ways to use TLS certificates, see the following topics:

- Secure LDAP with TLS certificates
- Secure SSO with TLS certificates

**Getting your certificates**

If you are experienced with SSL certificates, you can create them as you normally would and go straight to configuring your Splunk instances to use them.

If you need help getting your certificates together, we’ve provided very simple examples using OpenSSL commands. (OpenSSL ships with Splunk software)

- How to self-sign certificates
- How to get third-party certificates
- How to self-sign certificates for Splunk Web
- How to get third-party certificates for Splunk Web
What to do when you have your certificates

The following topics provide more information about configuring Splunk software to use your certificates once you have them:

- Secure Splunk Web with your own certificate
- Configure Splunk forwarding to use your own certificates
- About securing inter-splunk communication