Splunk® Enterprise
Securing Splunk Enterprise 8.0.4

About securing Splunk software

Generated: 5/29/2020 6:58 pm
About securing Splunk software

During and after your Splunk Enterprise installation, you must take steps to secure both your configuration and your data. Securing your Splunk Enterprise installation reduces its attack surface and mitigates the risk and impact of most vulnerabilities. Some procedures are simple, such as confirming that your servers are physically secure and that your properly manage your credentials. Others, such as configuring encryption, are more complex, but are equally as important to the integrity of your data.

Read this manual to learn about all of the areas of security that you should consider:

- Secure installation of Splunk Enterprise
- Management of users and role-based access control using your chosen form of authentication
- Usage of certificates to secure indexers, forwarders, and Splunk Web, where data is most vulnerable
- Usage of encryption to secure your configuration information
- Usage of auditing to keep track of activity in your system.

Use the How to secure and harden your Splunk software installation as a checklist and roadmap to ensure that you make your configuration and data as secure as possible.