



# Splunk® Enterprise Installation Manual

## 7.1.0

### More ways to secure Splunk Enterprise

Generated: 5/20/2018 4:14 pm

## More ways to secure Splunk Enterprise

After you install Splunk Enterprise, you have more options to secure your configuration.

### Configure user authentication and role-based access control

Set up your users and use roles to control access. Splunk Enterprise lets you configure users in several ways. See the following information in *Securing Splunk Enterprise*.

- The built-in authentication system. See Set up user authentication with Splunk Enterprise native authentication.
- LDAP. See Set up user authentication with LDAP.
- A scripted authentication API for use with an external authentication system, such as Pluggable Authentication Modules (PAM) or Remote Access Dial-In User Server (RADIUS). See Set up user authentication with external systems.

After you configure users, you can assign roles in Splunk Enterprise that determine and control capabilities and access levels. See About role-based user access.

### Use SSL certificates to configure encryption and authentication

Splunk Enterprise comes with a set of default certificates and keys that, when enabled, provide encryption and data compression. You can also use your own certificates and keys to secure communications between your browser and Splunk Web as well as data sent from forwarders to a **receiver**, such as an indexer.

See "About securing Splunk with SSL" in this manual.

### Audit Splunk Enterprise

Splunk Enterprise includes audit features that let you track the reliability of your data.

- Monitor files and directories in *Getting Data In*
- Search for audit events in *Securing Splunk Enterprise*

## **Harden your Splunk Enterprise installation**

See the following topics in *Securing Splunk Enterprise* to harden your installation.

- Deploy secure passwords across multiple servers
- Use Splunk Enterprise Access Control Lists
- Secure your service accounts
- Disable unnecessary Splunk Enterprise components
- Secure Splunk Enterprise on your network