How to secure and harden your Splunk software installation

Use this checklist as a roadmap for this manual to help you secure your Splunk Enterprise configuration and protect your data.

Set up authenticated users and manage user access

- Administrator credentials provide unrestricted access to a Splunk Enterprise instance and should be the first thing you change and secure. See Secure your Admin password.
- Access control lists prevent unauthorized user access to your Splunk Enterprise instance. See Use Access Control Lists.
- Set up users and configure roles and capabilities to control user access. See About configuring role-based user access.
- Configure user authentication with one of the following methods:
  - The built-in authentication scheme. See Set up user authentication with Splunk's built-in system.
  - Splunk Enterprise authentication tokens, which are based on the native authentication scheme. Tokens let you provide access to the instance through web requests to Splunk Enterprise Representational State Transfer (REST) endpoints. See Set up authentication with tokens.
  - The Lightweight Directory Access Protocol (LDAP) authentication scheme. 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.
- Use one of the following to create secure one-step login, or single sign-on (SSO), for users:
  - Single Sign on with SAML
  - Multi-factor authentication
  - ProxySSO
  - Reverse-proxy SSO with Apache

Use certificates and encryption to secure communications for your Splunk Enterprise configuration

Splunk Enterprise comes with a set of default certificates and keys that demonstrate encryption. Where possible, deploy your own certificates and configure them to secure Splunk Enterprise communications. See About securing Splunk with SSL.

Harden your Splunk Enterprise instances to reduce vulnerability and risk

- Secure communication within indexer clusters and search head clusters. See Secure your indexer clusters and search head clusters.
- Ensure that credentials in a distributed deployment are consistent across individual instances. See Deploy secure passwords across multiple servers.
- Confirm that the credentials and access levels for the accounts that run Splunk Enterprise are secure. See Secure your service accounts.
- Where possible, limit access to the app key value store network port on any Splunk Enterprise instances. See Harden your KV store port.
- Disable automatic chart recovery in the analytics workspace. See Charts in the Splunk Analytics Workspace Using the Splunk Analytics Workspace manual.
Audit your system regularly

Audit events provide information about what has changed in your Splunk Enterprise configuration. It gives you the where and when, as well as the identity of the actor who implemented the change. Leveraging audit events provides better security and other benefits.

- Audit your system regularly to monitor user and administrator access, as well as other activities that could tip you off to unsafe practices or security breaches.
- Keep an eye on activities within Splunk Enterprise, such as searches or configuration changes. You can use this information for compliance reporting, troubleshooting, and attribution during incidence response.
- Audit events are especially useful in distributed Splunk Enterprise configurations for detecting configuration and access control changes across many Splunk Enterprise instances. To learn more, see Audit Splunk Enterprise activity.
- Use the file system-based monitoring available out of the box on most Splunk-supported operating systems. For more information about monitoring, see Monitor Files and Directories in the Getting Data In Manual.