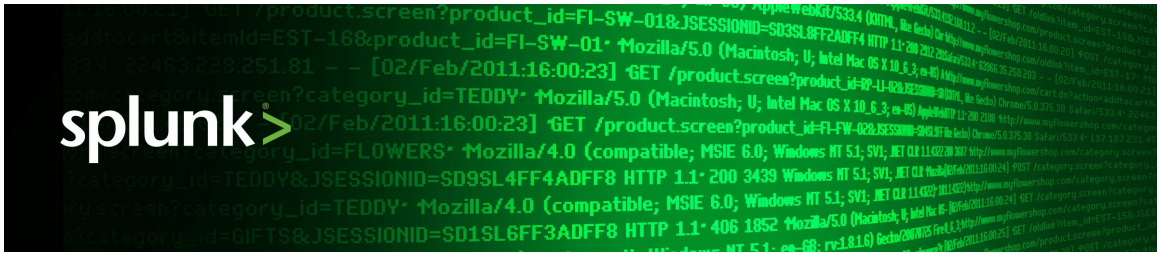

Splunk® Enterprise Installation Manual 7.1.0

Run Splunk Enterprise as a different or non-root user

Generated: 5/21/2018 4:49 pm

Run Splunk Enterprise as a different or non-root user

On *nix based systems, you can run Splunk Enterprise as a user other than root. This is a Splunk best practice and you should configure your systems to run the software as a non-root user where possible.

If you run Splunk software as a non-root user, confirm that the software can perform the following:

- Read the files and directories that you configure it to monitor. Some log files and directories might require root or superuser access to be indexed.
- Write to the Splunk Enterprise directory and execute any scripts configured to work with your alerts or scripted input. See Configure a script for an alert action in the *Alerting Manual* or Get data from APIs and other remote data interfaces through scripted inputs in *Getting data in*.
- Bind to the network ports it is listening on. Network ports below 1024 are reserved ports that only the root user can bind to.

Because network ports below 1024 are reserved for root access only, Splunk software can only listen on port 514 (the default listening port for syslog) if it runs as root. You can, however, install another utility (such as syslog-ng) to write your syslog data to a file and have Splunk monitor that file instead.

Set up Splunk software to run as a non-root user

1. Install Splunk software as the root user, if you have root access. Otherwise, install the software into a directory that has write access for the user that you want Splunk software to run as.
2. Change the ownership of the `$SPLUNK_HOME` directory to the user that you want Splunk software to run as.
3. Start the Splunk software.

Example instructions on how to install Splunk software as a non-root user

In this example, `$SPLUNK_HOME` represents the path to the Splunk Enterprise installation directory.

1. Log into the machine that you want to install Splunk software as root.
2. Create the `splunk` user and group.
   On Linux:
   ```
   useradd splunk
   ```

```
groupadd splunk
```

On Mac OS: You can use the **System Preferences > Accounts** System Preferences panel to add users and groups.

3. Install the Splunk software, as described in the installation instructions for your platform. See [Chooseyourplatform|Installation instructions].

   Do not start Splunk Enterprise yet.
4. Run the `chown` command to change the ownership of the `splunk` directory and everything under it to the user that you want to run the software.

   ```
   chown -R splunk:splunk $SPLUNK_HOME
   ```

   If the `chown` binary on your system does not support changing group ownership of files, you can use the `chgrp` command instead. See the `man` pages on your system for additional information on changing group ownership.
5. Become the non-root user.

   ```
   su - <user>
   ```

   You can also log out of the root account and log in as that user.
6. Start the Splunk software.

   ```
   $SPLUNK_HOME/bin/splunk start
   ```

Use sudo to start or stop Splunk software as a different user

If you want to start Splunk Enterprise as the `splunk` user while you are logged in as a different user, you can use the `sudo` command.

```
sudo -H -u splunk $SPLUNK_HOME/bin/splunk start
sudo -H -u splunk $SPLUNK_HOME/bin/splunk stop
```

This example command assumes the following:

- That Splunk Enterprise has been installed in the default installation directory. If Splunk Enterprise is in an alternate location, update the path in the command accordingly.
- That your system has the `sudo` command available. If this is not the case, use `su` or get and install `sudo`.
- That you have already created the user that you want Splunk software to run as.

- That the `splunk` user has access to the `/dev/urandom` device to generate the certificates for the product.

Further reading

- To configure Splunk software to run at boot time as a non-root user, see Enable boot-start as a non-root user in the *Admin* Manual.
- To learn how to install Splunk Enterprise on Windows using a user that is not an administrator, see Choose the user Splunk Enterprise should run as.
- To learn how to change the Windows user that Splunk Enterprise services use, see Change the user selected during Windows installation.