Splunk® Enterprise Installation Manual 9.0.0

Start Splunk Enterprise for the first time

Generated: 7/06/2022 3:50 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Start Splunk Enterprise for the first time

Before you begin using your new Splunk Enterprise upgrade or installation, take a few moments to make sure that the software and your data are secure.

As part of the initial startup process, Splunk Enterprise prompts you to create credentials for the administrator user. You can choose a username or use the default of `admin`. You can also enter a password. You must complete both steps for Splunk Enterprise to start and operate normally.

See the following topics in the *Securing Splunk* manual for more information:

- Hardening Standards
- Create secure administrator credentials

If you start Splunk Enterprise for the first time with the --no-prompt CLI argument, then the software does not prompt you to create the administrator credentials. If you do not create the credentials then Splunk Enterprise displays a message on login that there is no user. You must then manually create the credentials and restart Splunk Enterprise before you can log in. See "Create admin credentials manually" later in this topic for instruction on creating the credentials.

On Windows

You can start Splunk Enterprise on Windows using either the command line or the Services control panel. Using the command line offers more options.

From a command prompt or PowerShell window, run the following commands:

```
cd <Splunk Enterprise installation directory>\bin
splunk start
```

(For Windows users: in subsequent examples and information, replace `$SPLUNK_HOME` with `C:\Program Files\Splunk` if you have installed Splunk in the default location. You can also add `%SPLUNK_HOME%` as a system-wide environment variable by using the Advanced tab in the System Properties dialog box.)

On UNIX

1. Use the Splunk Enterprise command-line interface (CLI):

   ```
   cd <Splunk Enterprise installation directory>/bin
   ./splunk start
   ```
2. Create the Splunk Enterprise admin username. This is the user that you log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.

   ```
   This appears to be your first time running this version of Splunk.

   Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
   Create credentials for the administrator account.
   Characters do not appear on the screen when you type in credentials.

   Please enter an administrator username:
   ```

3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.
```
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
```
4. If the default management and Splunk Web ports are already in use (or are otherwise not available), Splunk Enterprise offers to use the next available ports. You can either accept this option or specify a port to use.
5. You can optionally set the `SPLUNK_HOME` environment variable to the Splunk Enterprise installation directory. Setting the environment variable lets you refer to the installation directory later without having to remember its exact location:

```
export SPLUNK_HOME=<Splunk Enterprise installation directory>
cd $SPLUNK_HOME/bin
./splunk start
```
6. Splunk Enterprise displays the license agreement and prompts you to accept before the startup sequence continues.

On Mac OS X

Start Splunk Enterprise from the Finder

1. Double-click the **Splunk** icon on the Desktop to launch the helper application, entitled "Splunk's Little Helper".
2. Click **OK** to allow Splunk to initialize and set up the trial license.
3. (Optional) Click **Start and Show Splunk** to start Splunk Enterprise and direct your web browser to open a page to Splunk Web.
4. (Optional) Click **Only Start Splunk** to start Splunk Enterprise, but not open Splunk Web in a browser.
5. (Optional) Click **Cancel** to quit the helper application. This does not affect the Splunk Enterprise instance itself, only the helper application.

After you make your choice, the helper application performs the requested application and terminates. You can run the helper application again to either show Splunk Web or stop Splunk Enterprise.

The helper application can also be used to stop Splunk Enterprise if it is already running.

Start Splunk Enterprise from the command line

1. On macOS, the default Splunk Enterprise installation directory is `/Applications/splunk`.

```
cd <Splunk Enterprise installation directory>/bin
./splunk start
```
2. Create the Splunk Enterprise admin username. This is the user that you log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.
```
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```
3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.
```
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
```

Other start options

Accept the Splunk license automatically when starting for the first time

1. Add the `--accept-license` option to the `start` command:
   `$SPLUNK_HOME/bin/splunk start --accept-license`
2. Create the Splunk Enterprise admin username. This is the user that you log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.
```
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```
3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.
```
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
```
4. The startup sequence displays:
```
Splunk>

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration...  Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _blocksignature _internal _introspection _thefishbucket history
main msad msexchange perfmon sf_food_health sos sos_summary_daily summary windows wineventlog
winevents
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                                [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://localhost:8000
```

Start Splunk Enterprise without prompting, or by answering "yes" to any prompts

There are two other `start` options: `no-prompt` and `answer-yes`.

- If you run `$SPLUNK_HOME/bin/splunk start --no-prompt`, Splunk Enterprise proceeds with startup until it has to

ask a question. Then, it displays the question and why it has to quit, and quits. In this scenario, it does not prompt for administrator credentials. You must manually create the credentials and restart before you can log in. See "Create administrator credentials manually" later in this topic for the procedure.
- If you run `SPLUNK_HOME/bin/splunk start --answer-yes`, Splunk Enterprise proceeds with startup and automatically answers "yes" to all yes/no questions that it encounters during startup. It displays each question and answer as it continues.

If you run start Splunk Enterprise with all three options in one line, the following happens:

- The software accepts the license automatically and does not ask you to accept it.
- The software answers "yes" to any "yes/no" question.
- The software quits if it encounters a question that cannot be answered "yes" or "no".

Change where and how Splunk Enterprise starts

To learn how to change system environment variables that control how Splunk Enterprise starts and operates, see "Set or change environment variables" in the Admin manual.

Create administrator credentials manually

If you start Splunk Enterprise for the first time and use the `--no-prompt` CLI argument, Splunk Enterprise can start without an administrator user, which prevents login. To fix this problem, you must create the credentials and then restart Splunk Enterprise.

1. Stop Splunk Enterprise:
   `./splunk stop`
2. With a text editor, create `$SPLUNK_HOME/etc/system/local/user-seed.conf`, substituting `$SPLUNK_HOME` for where you installed the software.
3. Within the file, add the following lines, substituting a password for `your new password`:
   ```
   [user_info]
   USERNAME = admin
   PASSWORD = <your new password>
   ```
4. Save the file and close it.
5. Restart Splunk Enterprise by following the instructions shown earlier in this topic.

For more information on administrator credential creation, including password management for automated installations, see Create a secure administrator password in *Securing Splunk Enterprise*.

Troubleshoot Splunk Enterprise not starting the first time

If you encounter a situation where Splunk Enterprise does not start, especially after an upgrade, confirm that you have not passed any illegal arguments to the Splunk CLI as part of the start process. If you have passed illegal arguments, rerun the `splunk start` command without the arguments.

Launch Splunk Web

With a supported web browser, navigate to:

```
http://<host name or ip address>:8000
```

Use whatever host and port you chose during installation.