Splunk® Enterprise Installation Manual 7.1.0

Uninstall Splunk Enterprise

Generated: 5/21/2018 2:03 am

Uninstall Splunk Enterprise

Learn how to remove Splunk Enterprise from a host by following the procedures in this topic.

Prerequisites

1. If you configured Splunk Enterprise to start on boot, remove it from your boot scripts before you uninstall.

   ```
   ./splunk disable boot-start
   ```
2. Stop Splunk Enterprise. Navigate to `$SPLUNK_HOME/bin` and type `./splunk stop` (or just `splunk stop` on Windows).

Uninstall Splunk Enterprise with your package management utilities

Use your local package management commands to uninstall Splunk Enterprise. In most cases, files that were not originally installed by the package will be retained. These files include your configuration and index files which are under your installation directory.

In these instructions, `$SPLUNK_HOME` refers to the Splunk installation directory. On Windows, this is `C:\Program Files\Splunk` by default. For most Unix platforms, the default installation directory is `/opt/splunk`. On Mac OS X, it is `/Applications/splunk`.

RedHat Linux

```
rpm -e splunk_product_name
```

Debian Linux

```
dpkg -r splunk
```

Remove all Splunk files, including configuration files

```
dpkg -P splunk
```

Other things you might want to delete

- If you created any indexes and did not use the Splunk Enterprise default path, you must delete those directories as well.
- If you created a user or group for running Splunk Enterprise, you should also delete them.

Windows

- Use the **Add or Remove Programs** option in the Control Panel. In Windows 7, 8.1, and 10, and Windows Server 2008 R2 and 2012 R2, that option is available under **Programs and Features.**
- (Optional) You can also uninstall Splunk Enterprise from the command line by using the `msiexec` executable against the Splunk installer package.

```
msiexec /x splunk-<version>-x64.msi
```

Under some circumstances, the Microsoft installer might present a reboot prompt during the uninstall process. You can safely ignore this request without rebooting.

Uninstall Splunk Enterprise manually

If you can't use package management commands, use these instructions to uninstall Splunk Enterprise.

1. Stop Splunk Enterprise.

```
$SPLUNK_HOME/bin/splunk stop
```
2. Find and `kill` any lingering processes that contain "splunk" in their name.
For Linux

```
kill -9 `ps -ef | grep splunk | grep -v grep | awk '{print $2;}'`
```

For Mac OS

```
kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'`
```
3. Remove the Splunk Enterprise installation directory, `$SPLUNK_HOME`.

```
rm -rf /Applications/splunk
```

You can also remove the installation directory by dragging the folder into the trash.

4. Remove any Splunk Enterprise datastore or indexes outside the top-level directory, if they exist.

```
rm -rf /opt/splunkdata
```

5. Delete the `splunk` user and group, if they exist.

For Linux
```
userdel splunk
groupdel splunk
```

For Mac OS
Use the **System Preferences > Accounts** panel to manage users and groups.

For Windows
Open a command prompt and run the command `msiexec /x` against the msi package that you used to install Splunk Enterprise. If you don't have that package, get the correct version from the download page.