

# Splunk Configuration File Folder Precedence

Any discussion of Splunk configuration files must be considered in the context of directory location 'precedence', which is the hierarchy in which Splunk assigns the various .conf file entry values to memory during startup and utilizes them during its operation.

When the configuration file context is global, directory priority descends in this order:

1. System local directory — highest priority
2. App local directories
3. App default directories
4. System default directory — lowest priority

By way of further explanation, there are a number of .conf files, including a server.conf file, located in the \$SPLUNK\_HOME/etc/system/default folder. Each of these .conf files contain a large number of default configuration settings. When you make configuration changes that affect the operation of Splunk either via Splunk Web or from the command line, deviations from the default settings in server.conf in the default folder will be stored in another server.conf file located in the \$SPLUNK\_HOME/etc/system/local folder. You'll note from the directory precedence outlined above those settings that reside in a file in the local folder will take precedence over those in the default folder.

For example, one of the stanzas and entries in the /etc/system/default/server.conf file on a Splunk server that is part of a clustered solution with a License Manager is:

```
[license]
manager_uri = self
```

In the /etc/system/local/server.conf file on this server we find this setting that points to the License Manager to obtain licensing - this setting takes precedence over the default setting:

```
[license]
manager_uri = https://10.2.6.36:8089
```

This folder precedence convention is a convenient way of managing a complex environment but is also why Splunk docs always warn against making any changes to .conf files in default folders – the local folder settings take precedence and will be preserved in the case of a Splunk version upgrade. Said another way, any changes made to a .conf file in the \$SPLUNK\_HOME/etc/system/default folder will be overwritten during an upgrade. Any changes you manually enter that will alter or

supplement default settings should therefore be placed in a same-named .conf file residing in a /local folder, for both system and app level configurations.

A final consideration is that while you could place system-level configuration settings into .conf files located in the /default or /local folder of an app folder in \$SPLUNK\_HOME/etc/apps/, this will result in these significant server settings being scattered all over the server such that it is difficult to determine what the total/final configuration really is without using btool or a lot of hunt-and-peck searching. Best practice suggests that non-default system level .conf files should be kept in \$SPLUNK\_HOME/etc/system/local, with very few exceptions.