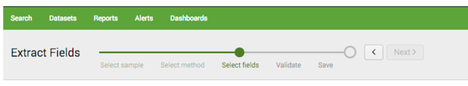
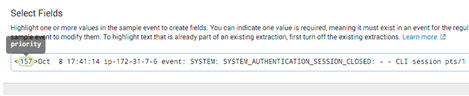
1. **Extract a field name or use an existing field name to map.**

I have Priority already extracted
Using all lower case for fields to be be uniform.



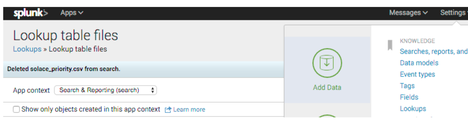


2. **Create CSV file.**

To simplify , use same source field name (severity) as you just extracted.

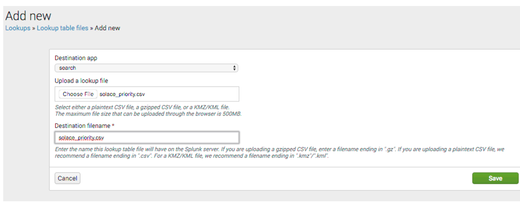
```
hermosa:Splunk$ head solace_priority.csv
priority,severity,facility
128,EMERGENCY,local0
129,ALERT,local0
130,CRITICAL,local0
131,ERROR,local0
132,WARNING,local0
133,NOTICE,local0
134,INFO,local0
135,DEBUG,local0
136,EMERGENCY,local1
```

3. **Create New Lookup**

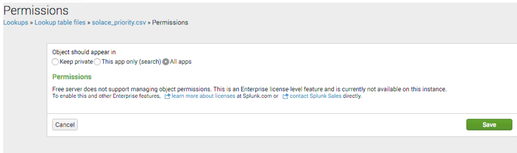


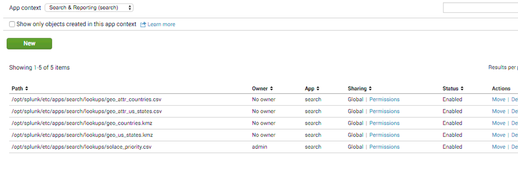
4. **Select CSV file.**

Using same name as file to simplify



5. **Change Permissions**





6. **Use search and pipe to lookup command**

You can map to multiple fields (priority -> severity, facility)
or search on new fields.

```
index=solace | lookup solace_priority.csv priority OUTPUT severity
index=solace | lookup solace_priority.csv PRI OUTPUT Severity | stats count by Severity
index=solace | lookup solace_priority.csv priority OUTPUTNEW severity,facility
```