General Settings Quick Reference Guide

The table below details the general setting items and their current value within the Splunk Enterprise Security application as it is configure in the QA-Lab. To access these settings, log onto the Splunk Enterprise Security application and:

* **Single click** on the ***Configure*** menu option
* **Single click** on the ***General*** menu option
* **Single click** on the ***General*** Settings option.

General Settings Table

| Setting | Description | Current Configuration |
| --- | --- | --- |
| Auto Pause | Set the time in seconds before a drilldown search will pause. | 120 seconds |
| Domain Analysis | Enable or disable WHOIS tracking for Web domains. | NOOP |
| HTTP Category Analysis Sparkline Earliest | Set the start time for sparklines displayed on the **HTTP User Category Analysis** dashboard | -24h@h |
| HTTP Category Analysis Sparkline Span | Set the time span for sparklines displayed on the **HTTP User Category Analysis** dashboard. | 1 |
| HTTP User Agent Analysis Sparkline Earliest | Set the start time for sparklines displayed on the **HTTP User Agent Analysis** dashboard. | -24h@h |
| HTTP User Agent Analysis Sparkline Span | Set the time span for sparklines displayed on the **HTTP User Agent Analysis** dashboard. | 1 |
| IRT Disk Sync Delay | Set the number of seconds for Splunk ES to wait for a disk flush to finish. | 60 seconds |
| Incident Review Analyst Capacity | Set the maximum number of notable events that can be assigned to an analyst. | 12 |
| Indexed Realtime | Enable or disable Indexed Realtime. | Enabled |
| Large Email Threshold | An email that exceeds this size in bytes is considered large. | 2097152 bytes |
| Licensing Event Count Filter | Define the list of indexes to exclude from the “Events Per Day” summarization. | (index!=notable index!=risk index!= \*summary\*) |
| New Domain Analysis Sparkline Span | Set the time span for sparklines displayed in the **New Domain Analysis** dashboard. | 1 |
| Search Disk Quota (admin) | Set the maximum amount of disk space in MB that an admin user can use to store search job results. | 25000MB |
| Search Jobs Quota (admin) | Set the maximum number of concurrent searches allowed for admin users. | 50 |
| Search Jobs Quota (power) | Set the maximum number of concurrent searches for power users. | 10 |
| Short Lived Account Length | An account creation and deletion record that exceeds this threshold is anomalous. | 3600 |
| TSTATS Allow Old Summaries | Enable or disable searching of data model accelerations containing fields that do not match the current data model configuration. | Enabled |
| TSTATS Local | Determine whether or not the TSTATS macro will be distributed. | No |
| TSTATS Summaries Only | Determine whether or not the TSTATS or summaries only macro will on search accelerated events. | Yes |
| Use Other | Enable or disable the OTHER on charts that exceed default series limits. | Enable |
| Website Watchlist Search | A list of watchlisted websites used by the “Watchlisted Events” correlation search. | (indeed.com OR simplyhired.com OR monster.com) |