Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Disable merge for assets and identities in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Disable merge for assets and identities in Splunk Enterprise Security

The merge process is enabled for assets and identities by default. However, in situations when you have a source file with duplication in the key fields, and you can't groom the file to make sure that the information belongs to the same asset or identity, then you have the option to disable the merge process.

Prerequisites

Perform the following prerequisite tasks before starting on these settings:

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. Format the asset or identity list as a lookup in Splunk Enterprise Security.
3. Configure a new asset or identity list in Splunk Enterprise Security.

Disable the merge process

Use the global settings to enable or disable merge as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.
3. Scroll to the **Enable Merge for Assets or Identities** panel.
4. Use the toggle to enable or disable for **Assets** or **Identities**.

Example

Using assets as an example, consider a source file with duplicates in the key field of `nt_host`, such as the following:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires _av
192.0.2.2,,host1,,,,,,,,,,,,,,
192.0.2.120,,host1,,,,,,,,,,,,,,
192.0.2.135,,host1,,,,,,,,,,,,,,
192.0.2.242,,host2,,,,,,,,,,,,,,
192.0.2.65,,host2,,,,,,,,,,,,,,
```

The default is to merge the three rows with `nt_host` of `host1` into one asset, and merge the two rows with `host2` into another asset.

asset	ip	nt_host	pci_domain
192.0.2.2 192.0.2.120 192.0.2.135 host1	192.0.2.2 192.0.2.120 192.0.2.135	host1	untrust
192.0.2.242 192.0.2.65 host2	192.0.2.242 192.0.2.65	host2	untrust

If you disable the merge, then the collection remains the same as the source file, and assets are not merged.

asset	ip	nt_host	pci_domain
192.0.2.2 host1	192.0.2.2	host1	untrust
192.0.2.120 host1	192.0.2.120	host1	untrust
192.0.2.135 host1	192.0.2.135	host1	untrust
192.0.2.242 host2	192.0.2.242	host2	untrust
192.0.2.65 host2	192.0.2.65	host2	untrust

When you do a lookup on an non-merged collection, there is no context for how to resolve the overlapping key field values. For example, the asset_lookup_by_str lookup in transforms.conf has `max_matches = 1`, so the first host it matches in the assets_by_str collection is the only one you'll see in your search results.