Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security

You can test the asset and identity merge process if you want to confirm that the data produced by the merge process is expected and accurate. You can run the search previews to determine what the merge will do with your data without actually performing the merge. These steps aren't required, but can be performed to validate the merge works as expected.

If you used previous versions of ES, note that the search preview shows you the dynamic custom search that replaces the following correlation searches:

- Identity - Asset CIDR Matches - Lookup Gen
- Identity - Asset String Matches - Lookup Gen
- Identity - Identity Matches - Lookup Gen

To preview all your asset and identity searches, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Search Preview** tab.
3. You can run the search preview for each collection, the lookups of which are located in the transforms.conf file:
    - asset_lookup_by_str is the lookup for the assets_by_str collection.
    - asset_lookup_by_cidr is the lookup for the assets_by_cidr collection.
    - identity_lookup_expanded is the lookup for the identities_expanded collection.

The search preview looks into all your lookup tables and creates custom-built searches with what is currently in your inputs.conf file. The search is dynamic and generates the search each time you refresh or load the page. The results of these searches are the delta since the last merge. If nothing has changed in the source files since the last merge, you do not see any output.

If you want to see some output regardless if anything has changed, you can remove the `inputlookup append=T` SPL from the search. For example, in the case of identities, you would remove: `| inputlookup append=T "identity_lookup_expanded"` from the identity_lookup_expanded search.