Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Revise the miscellaneous settings used by the identity manager framework in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Revise the miscellaneous settings used by the identity manager framework in Splunk Enterprise Security

You can revise miscellaneous settings that are specific to the identity manager.

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.

Revise how often the identity manager runs

The identity manager runs every 300 seconds (5 minutes) by default. For performance purposes, you can change this to a larger value so it does not run so frequently.

Use the global settings to change the time:

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 **Miscellaneous Settings** panel.
4. Type a number of seconds in the **Time(s)** field.

Revise the master host where the identity manager runs

The identity manager runs on the search head captain by default. If you want to separate search head responsibilities, or if the search head is experiencing performance issues due to resource consumption, then you can change the master host.

Use the global settings to change the master host if search head clustering is enabled:

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 **Miscellaneous Settings** panel.
4. Type a name in the **Master host** field that matches the name of a server in the cluster pool.

See System requirements and other deployment considerations for search head clusters.

Add additional context to string lookups based on CIDR blocks

By default, the `asset_lookup_by_str` lookup does not combine Classless Inter-Domain Routing (CIDR) enrichment in the output results. You can add additional enrichment to your asset and identity lookups based on CIDR blocks. This does not take away any functionality from your `asset_lookup_by_cidr` lookup.

Automatic lookups run in a certain order to populate enrichment data into empty fields. The order starts with `asset_lookup_by_str` first, and then `asset_lookup_by_cidr` is next. Once the string enrichment data is populated into a field, the field is no longer empty, so it does not get filled with CIDR data. Normally your CIDR data is only returned by `asset_lookup_by_cidr`, but sometimes that results in CIDR enrichment being lost because `asset_lookup_by_str` runs and matches first. With overlay CIDR enabled, your `asset_lookup_by_str` will include the CIDR data as well. For more information about automatic lookups and correlation setup, see Manage correlation setup in Splunk Enterprise Security.

To overlay CIDR enrichment into your string lookup results, use the global settings:

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 **Miscellaneous Settings** panel.
4. Toggle the **Overlay CIDR** setting to enable.

Examples of overlay CIDR

Using assets as an example, consider a source file with an `ip` address of 192.187.2.94, which is also a match for a CIDR range of 192.187.0.0/16 that has values in the `owner` field:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av
192.187.2.94,,,,owner1,,,,,,,,,,,,
192.187.0.0/16,,,,cidr _owner1,,,,,,,,,,,,
10.0.2.109,,,,owner2,,,,,,,,,,,,
10.0.2.0/24,,,,cidr_owner2,,,,,,,,,,,,
```

With overlay CIDR enabled, the behavior is to include CIDR field values within the string lookup's output results. When an event comes in that matches both an asset by string and also an asset by CIDR, you see the exact match data for the IP address and the most specific CIDR block data.

Using the search preview for `asset_lookup_by_str` returns results similar to the following:

asset	ip	owner	pci_domain
192.187.2.94	192.187.2.94	owner1 cidr_owner1	untrust
10.0.2.109	10.0.2.109	owner2 cidr_owner2	untrust

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

With overlay CIDR disabled, the behavior is not to include any enrichment for CIDR field values in the string lookup's output results.

Using the search preview for `asset_lookup_by_str` returns results similar to the following:

asset	ip	owner	pci_domain
192.187.2.94	192.187.2.94	owner1	untrust
10.0.2.109	10.0.2.109	owner2	untrust

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

The asset enrichment specific to CIDR fields is still available in the CIDR lookup's output results, just not in the string lookup's output results.

Using the search preview for `asset_lookup_by_cidr` returns results similar to the following:

asset	ip	owner	pci_domain
192.187.0.0/16	192.187.0.0/16	cidr_owner1	untrust
10.0.2.0/24	10.0.2.0/24	cidr_owner2	untrust

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

The `overlay_cidr` setting is stored in the `[identity_manager]` stanza of the inputs.conf file.