Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Manage identity field settings in Splunk Enterprise Security

Generated: 5/11/2022 7:11 pm

Manage identity field settings in Splunk Enterprise Security

Configure identity settings for lookup matching. Identity fields are added both by default and by entering custom fields manually. You can add up to 20 custom fields for your lookups. The default key field is `identity`. You are able to configure whether a field is a tag field, a **multivalue field**, or both.

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.

Add or edit an identity field

To add a new custom identity field, do the following:

1. From the Splunk ES menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Identity Fields** tab.
3. Click **Add New Field**.
4. In the New Identity Field window, do the following:
    1. Enter a lookup field name.
    2. Check the **Key** check box to make this field a key. When merge is enabled, assets with the same values for this field are merged.
    3. Check the **Tag** check box if the field can be used as an identity tag. This is a helper field for holding additional values that you want to look up, in addition to the key fields. This is not the same as tagging in Splunk Enterprise.
    4. Check the **Multivalue** check box if the field can output multiple values.
    5. Click **Save**.

The **Add New Field** button is disabled when the limit is reached and enabled again when any custom field is deleted using the **Delete** action link.

If you want the merge process to merge on something other than `identity`, you can edit the default key fields. To edit an identity field, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Identity Fields** tab.
3. Click the field name that you want to edit.
    1. Check the **Key** check box to make this field a key. When merge is enabled, assets with the same values for this field are merged. The minimum number of key fields is one.
    2. Check the **Tag** check box if the field can be used as an asset tag. This is a helper field for holding additional values that you want to look up, in addition to the key fields. This is not the same as tagging in Splunk Enterprise.
    3. Check the **Multivalue** check box if the field can output multiple values.
    4. (Optional) Revise the **Limit** if you want to change the number of values that display in a multivalue field merge. See Revise field limits for assets.
    5. Click **Save**.

Enable case-sensitive matching for identity fields

You can match identity collections to raw event data. Case-sensitive matching determines how to match the raw event with the identity collections. Case-sensitive matching is globally available across all fields.

For example, if you have a raw event with the field `dest="ThisIsAnExample"` and the identity data also has the same field, enabling case-sensitive matching allows a match only when spelling and capitalization is an exact match. Therefore, the following values `thisisanexample`, `thisISANEXAMPLE`, or `THISISANExAMPLE` do not match.

If case-sensitive matching is disabled, these examples produce a match because their values are the same. When case-sensitive matching is disabled, we match a word in lower case to another word in lower case.

Note that searches using `| inputlookup ... where <filter>` are case sensitive. Asset and Identity Management pages might use searches that contain `where` clauses. When case sensitivity is set to false, the merge process stores the values as lowercase so the case insensitive matches can be performed. To avoid this, you can toggle the case sensitive settings to true.

To use case-sensitive matching, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Identity Fields** tab.
3. Enable the **Enable case sensitive identity matching** switch.
4. Click **Update** to trigger the merge process and rewrite the `identity_lookup_expanded` KV store collection.

Revise multivalue field limits for identities

The default number of multivalue identity fields that display after merging is 25.

To revise multivalue field limits, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Identity Fields** tab.
3. Scroll to find the field name that you're looking for and do the following:
    1. Click on the link.
    2. Change the **Field Limit** value.
4. Click **Save**.

The field value range for both key and non-key multivalue fields is 1 - 100.

If your source CSV file contains more values in a multivalue field than the limit, these values are truncated during the merge process. This means that in addition to not being displayed in the results, they also are removed from the data altogether. If you search or lookup on the truncated values, you will not find them because they do not exist.

If your data gets truncated, you can revise multivalue fields to 100. Raising the limits has the potential to impact performance.

If your data still gets truncated, but you want to see more than the maximum values, then you need to revise your source CSV files. Spread out the values so that they seem to be part of different assets, by making sure that there are no duplicate values in the key fields.

The key field is identity and the default merge convention is email. If you store extra information in your key fields, such as the same identity or email address assigned to multiple people, these duplicates are now merged together as one identity. Make sure that the information in your key or email fields either belongs to the same person or does not overlap.

Example of revising multivalue field limits

If you have a source CSV file that contains 9 values in the identity key field and 16 values in the phone field, such as the following:

identity	prefix	first	last	email	phone	managedBy	priority	watchlist	startDate
journot	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3479	americas	medium	3/2/88 2:39	3/8/01 6:21
dr.j	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-1554	americas	medium	3/2/88 2:39	3/8/01 6:21
Dr.L	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3480 | +1 (800)555-1555	americas	medium	3/2/88 2:39	3/8/01 6:21
Latoyia.Journot	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3481 | +1 (800)555-1556	americas	medium	3/2/88 2:39	3/8/01 6:21
Latoyia.J	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3482 | +1 (800)555-1557	americas	medium	3/2/88 2:39	3/8/01 6:21
L.Journot	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3483 | +1 (800)555-1558	americas	medium	3/2/88 2:39	3/8/01 6:21
Latoyia	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3484 | +1 (800)555-1559	americas	medium	3/2/88 2:39	3/8/01 6:21
toyia	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3485 | +1 (800)555-1560	americas	medium	3/2/88 2:39	3/8/01 6:21
dr.toyia	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3486 | +1 (800)555-1561	americas	medium	3/2/88 2:39	3/8/01 6:21

Using the default email convention, the default limit of 6 for the identity multivalue key field, and revising the limit to 5 for the phone multivalue field, these are merged into an asset where the identity key field values are truncated to 6 and the phone non-key values are truncated to 5.

email	startDate	identity_tag	last	first	managedBy	prefix	identity	priority	wa
ljournot@acmetech.com	3/8/01 6:21	984050460.000000	journot	latoyia	americas	dr.	dr.l ljournot@acmetech.com ljournot l.journot latoyia.journot latoyia.j	medium	3/2/