Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Manage identity lookup configuration policies in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Manage identity lookup configuration policies in Splunk Enterprise Security

Create an identity lookup configuration policy to update and enrich your identities. Identity lookup settings create the configuration that updates the inputs.conf file to point to a lookup and update your identities. When you add new items, or update current items, the change takes effect in 5 minutes.

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 an identity input stanza for the lookup source

To add a new identity input source, do the following:

1. From the Splunk ES menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Identity Lookup Configuration** tab.
3. Click **New**.
4. In the New Identity Manager, do the following:
    1. Select the transforms.conf definition from the **Source** drop-down list that corresponds to the CSV source file of assets you uploaded in the prerequisite step.
    2. You can provide a name for the identity list stanza, but matching the source name is a good idea.
    3. Enter a descriptive category for this identity list, such as east_coast_employees or strategic_executives.
    4. Enter a detailed description of the contents of this identity list.
    5. Check the **Blacklist** check box to exclude the lookup file from bundle replication.

        The asset and identity source lookup files are excluded from bundle replication in an indexer cluster by default. The merged lookup files are still included in bundle replication to support asset and identity correlation. Changing the default to include asset and identity lookup files in bundle replication might reduce system performance. See Knowledge bundle replication overview in the Splunk Enterprise Distributed Search manual.

    6. In **Lookup List Type**, **identity** is selected for you.
    7. In **Lookup Field Exclusion List**, select fields for the merge process to ignore. This excludes the fields and their values from the KV store collections for that particular lookup. You might use this in the case where you have a field in your source file that you don't want to rely on for information.

        Do not use identity in the field exclusion list if you want to use the optional conventions that follow. The conventions are extracted from the identity field.
5. (Optional) Configure the conventions that the identity lookup can use to create a common unique key between different identity sources that might otherwise lack the same field.
   When an email convention check box is checked, the email address is used as an additional primary key for identity. The **Email** convention is enabled by default.
    1. Click **Email** to use the full email address.
    2. Click **Email Short** to use the email username.
    3. Click **+ Add a new convention** to add a custom convention:
       You can identify users by the first few letters of their first name and the first few letters of their last name, based on the columns in the Identities Table. Use the convention of identity_first(n)middle(n)last(n) where identity, first, and last are any columns from the Identities Table, and where n is a number starting with 0.

For example:
    - ◊ "Claudia Maria Garcia" using the convention first(3)last(3) is "clagar"
    - ◊ "Rutherford Michael Sullivan" using the convention first(1)middle(1).last() is "rm.sullivan"
    - ◊ "Vanya Patel" using the convention ADMIN_first(1)last() is "ADMIN_vpatel"
    - ◊ Multiple matches are resolved automatically by taking the first match in the table or manually by specifying **identity** values.
6. Click **Save**.

Rank the order for merging identities

Any new identity list gets added to the bottom of the page by default. You can rank the order of this list to determine priority for merging identities. If an identity exists in multiple source files as a single value, or exists multiple times in the same source file, this ranking is the weighted order for merging them. By default, the single value identity fields are as follows:

- endDate
- priority
- startDate
- watchlist

These are the fields where the rank takes effect. For example, if you're merging two identities, that both have the priority field value, you need to choose one to take precedence. The row at the top of the list takes precedence and the merge process uses that value, as opposed to the row that's ranked second.

To change the rank, do the following under the **Identity Lookup Configuration** tab:

1. Drag and drop the rows of the table into a new order.
2. When finished reordering, click **Save Ranking**.

Ranking is not considered for a multivalue field. The merge process combines all the values into the field, and then removes the duplicates.

Modify identity lookups

Make changes to the identity lookups in Splunk Enterprise Security to add new identities or change existing values in the lookup tables. You can also disable or enable existing lookups.

1. In Enterprise Security, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Find the name of the identity list you want to edit, and select the corresponding lookup from the Source column. The list opens in an interactive editor.
3. Use the scroll bars to view the columns and rows in the table. Double-click a cell to add, change, or remove content.
4. Click **Save** when you are finished.

Manually add static identity data

Manually add new static identity data to Splunk Enterprise Security by editing the Identities lookups. For example, add internal subnets, IP addresses to be whitelisted, and other static asset and identity data.

1. From the Splunk Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. To add identity data, click the **Identities** list to edit it.

3. Use the scroll bars to view the columns and rows in the table. Double-click in a cell to add, change, or remove content.
4. Save your changes.

Then you can see the lookup registered as static_identities or in **Configure > Data Enrichment > Asset and Identity Management**.

Disable the demo identity lookups

The demo identity lookups are disabled by default. Enable them if needed for testing. Disable the demo identity lookups to prevent the demo data from being added to the primary asset and identity lookups used by Splunk Enterprise Security for asset and identity correlation.

1. In Enterprise Security, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Locate the demo_identities lookups.
3. Click **Disable**.

Delete the identity lookup

Delete the source file configuration of an identity lookup configuration if you do not want a specific identity lookup source file to be processed when the Identity Manager modular input runs.

1. In Enterprise Security, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Locate the identity lookup that you created.

   You may not delete the identities that are available by default.
3. In the **Edit Identity Manager** dialog, click **Delete**.