



# **Splunk® Enterprise Security**

## **Administer Splunk Enterprise Security 7.0.1**

**Ignore values for assets and identities in Splunk Enterprise Security**

Generated: 6/13/2022 8:38 am

# Ignore values for assets and identities in Splunk Enterprise Security

In situations when you want values to be ignored in your fields, you might want to use special words to represent null values. The default behavior is to merge rows of source data based on a match in any one of the key fields. In many cases your source data might have placeholder values that span multiple rows, which causes them to get merged into one large multivalue row. To avoid this, you can define the placeholder values, and clean them during the merge process, so that independent rows are still maintained in the final lookups.

## 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.

## Set null values

Use the global settings to set your null values 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 **Asset Ignored Values** tab or the **Identity Ignored Values** tab.  
The default values that are ignored are null, n/a, unknown, and undefined.
  1. For assets, in the **Asset Ignored Values** section, click **Add Row**.
  2. Type a word that you want ignored and not displayed in the merge results. This field is case-sensitive.
  3. For identities, in the **Identity Ignored Values** section, click **Add Row**.
  4. Type a lowercase word that you want ignored and not displayed in the merge results. This field is case-sensitive.
4. Click **Save**.

The ignored values setting applies to any type of field, such as multivalue field or single value field or key field or non-key field. The strings are saved as `ignored_values` in `SplunkHome/etc/apps/SA-IdentityManagement/local/inputs.conf`.

## Remove null values

Use the global settings to remove your null values as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.  
The default values that are ignored are null, n/a, unknown, and undefined.
3. Scroll to the **Asset Ignored Values** tab or the **Identity Ignored Values** tab.
4. Find the value and click the **x** to delete it.