splunk>

turn data into doing™

Splunk® Enterprise Security
Administer Splunk Enterprise Security 6.3.0 Cloud only

Generated: 10/03/2020 3:43 am

Table of Contents

Table of Contents

Asset and Identity Management

Table of Contents

Overview

Administering Splunk Enterprise Security

Splunk Enterprise Security administrators are responsible for configuring, maintaining, auditing, and customizing an instance of Splunk Enterprise Security. If you are not administering Splunk Enterprise Security, see *Use Splunk Enterprise Security* for an introduction to using this app as a security analyst.

Use the links below to learn more about administrative tasks in Splunk Enterprise Security.

Manage and support analyst workflows

To enable and customize the workflows for analysts in your organization, see:

- Managing Incident Review in Splunk Enterprise Security
- Customize Incident Review in Splunk Enterprise Security
- Customize notable event settings in Splunk Enterprise Security
- Manage investigations in Splunk Enterprise Security

Enrich data for Enterprise Security

Enrich Splunk Enterprise Security with data about the assets and identities in your environment and with additional data about known threats.

- See Add asset and identity data to Splunk Enterprise Security for a full list of tasks related to adding and managing asset and identity data in Splunk Enterprise Security.
- See Add threat intelligence to Splunk Enterprise Security for information on all tasks related to managing threat intelligence sources in Splunk Enterprise Security.

Manage and customize configurations

To perform ongoing configuration in Splunk Enterprise Security, see:

- Configure general settings for Splunk Enterprise Security
- Manage input credentials in Splunk Enterprise Security
- Manage permissions in Splunk Enterprise Security
- Customize the menu bar in Splunk Enterprise Security
- Configure advanced filtering in Splunk Enterprise Security

You can find additional configuration information in the *Install and Upgrade Manual*.

- Configure and deploy indexes
- Configure users and roles
- Configure data models for Splunk Enterprise Security

Create, manage, and export content

To create new content or manage and customize existing content, see:

- Create correlation searches in Splunk Enterprise Security
- Create and manage key indicator searches in Splunk Enterprise Security
- Create and manage saved searches in Splunk Enterprise Security
- Create and manage search-driven lookups in Splunk Enterprise Security
- Create and manage swim lane searches in Splunk Enterprise Security
- Create and manage views in Splunk Enterprise Security
- Create and manage lookups in Splunk Enterprise Security
- Create risk and edit risk objects in Splunk Enterprise Security

To share custom content with other ES instances, see Export content from Splunk Enterprise Security as an app.

Troubleshoot dashboards

- For tips and best practices useful for troubleshooting dashboards in Enterprise Security, see Troubleshoot dashboards in Splunk Enterprise Security.
- For information about data model datasets that populate Enterprise Security dashboards, see Dashboard requirements matrix for Splunk Enterprise Security.
- For an overview of all dashboards in Splunk Enterprise Security, see Introduction to the dashboards available in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Incident Review and Investigations

Managing Incident Review in Splunk Enterprise Security

Splunk Enterprise Security detects patterns in your data and automatically reviews events for security-relevant incidents using **correlation searches**. When a correlation search detects a suspicious pattern, the correlation search creates an alert called a **notable event**.

The Incident Review dashboard surfaces all notable events, and categorizes them by potential severity so analysts can quickly triage, assign, and track issues.

- For information about how analysts use the Incident Review dashboard, see Incident Review overview in *Use Splunk Enterprise Security*.
- To audit and review analyst activity on the Incident Review dashboard, see Incident Review Audit in *Use Splunk Enterprise Security*.
- To customize the display of the Incident Review dashboard, and also modify analyst capabilities and permissions, see Customize Incident Review in Splunk Enterprise Security.
- To manually create notable events, see Manually create a notable event in Splunk Enterprise Security.
- To customize settings for notable events, see Customize notable event settings in Splunk Enterprise Security.
- For more information about how notable events are populated and managed by the notable event framework, see Notable Event framework in Splunk Enterprise Security on the Splunk developer portal.

How risk scores display in Incident Review

Risk scores do not display in Incident Review for every asset or identity. Only assets or identities (risk objects) that have a risk score and a risk object type of "system," "user," or "other" display in Incident Review. Risk scores only show for the following fields: `orig_host`, `dvc`, `src`, `dest`, `src_user`, and `user`. The risk score for an asset or identity might not match the score on the Risk Analysis dashboard. The risk score is a cumulative score for an asset or identity, rather than a score specific to an exact username.

- For example, if a person has a username of "buttercup" that has a risk score of 40, and an email address of "buttercup@splunk.com" with a risk score of 60, and the identity lookup identifies that "buttercup" and "buttercup@splunk.com" belong to the same person, a risk score of 100 displays on Incident Review for both "buttercup" and "buttercup@splunk.com" accounts.
- As another example, if an IP of 10.11.36.1 has a risk score of 80 and an IP of 10.11.36.19 has a risk score of 30, and the asset lookup identifies that a range of IPs "10.11.36.1 - 10.11.36.19" belong to the same asset, a risk score of 110 displays on Incident Review for both "10.11.36.1" and "10.11.36.19" IP addresses.

Risk scores are calculated for Incident Review using the **Threat - Risk Correlation By <type> - Lookup Gen** lookup generation searches. The searches run every 7 days and update the `risk_correlation_lookup` lookup file. To see more frequent updates to the risk scores in Incident Review, update the `cron_schedule` of the saved searches.

Notify an analyst of untriaged notable events

You can use a correlation search to notify an analyst if a notable event has not been triaged.

1. Select **Configure > Content > Content Management**.
2. Locate the **Untriaged Notable Events** correlation search using the filters.
3. Modify the search, changing the notable event owner or status fields as desired.

4. Set the desired alert action.
5. Save the changes.
6. Enable the **Untriaged Notable Events** correlation search.

Customize Incident Review in Splunk Enterprise Security

As a Splunk Enterprise Security administrator, you can customize the way that analysts view and interact with notable events on the Incident Review dashboard.

Modify analyst capabilities and permissions

Configure whether analysts can override the calculated urgency of a notable event and choose whether to require an analyst to add a comment when updating a notable event on the **Incident Review Settings** page.

1. Select **Configure > Incident Management > Incident Review Settings** to view the Incident Review settings.
2. Allow or prevent analysts from overriding the calculated urgency of a notable event with the **Allow Overriding of Urgency** checkbox. Analysts are allowed to override urgency by default.
3. Require analysts to add a comment when updating a notable event by checking the **Required** checkbox under **Comments**.
4. If you require analysts to add a comment, enter the minimum character length for required comments. The default character length is 20 characters.

Configure the recommended capacity for analysts

Configure the recommended maximum number of notable events that should be assigned per security analyst on the **General Settings** page.

1. Select **Configure > General > General Settings** to view the General Settings.
2. Enter a preferred number of notable events that should be assigned to an analyst with the **Incident Review Analyst Capacity** setting. The default is 12.

This value is used for audit purposes, and does not prevent more than the default number of notable events from being assigned to an analyst.

Change Incident Review columns

You can change the columns displayed on the Incident Review dashboard.

1. Review the existing columns in **Incident Review - Table Attributes**.
2. Use the action column to edit, remove, or change the order of the available columns.
3. Add custom columns by selecting **Insert below** or selecting **More...**, then **Insert above**.

Troubleshoot an issue where analysts cannot edit notable events successfully on Incident Review

If analysts cannot edit notable events successfully on Incident Review, several issues could be the cause.

- The analyst might not have permission to make status transitions. See Manage notable event statuses.

- The analyst might be attempting to edit a notable event that is visible, but cannot be edited successfully due to the limited number of events that can be retrieved from a bucket.

If a correlation search creates a high number of notable events in a short period of time, such as 1000 in less than five minutes, the Incident Review dashboard can hit the `max_events_per_bucket` limit when attempting to retrieve notable events for display from the `notable` index.

If analysts are unable to edit a notable event for this reason, the analyst can use a smaller time range when reviewing notable events on Incident Review. For example, a time range that reduces the number of events on the Incident Review dashboard to less than 1000. 1000 is the default value of `max_events_per_bucket`, so search that produces less than 1000 events cannot produce this error.

To prevent this from happening at any time, you can modify the maximum number of events that can be returned from a bucket. However, modifying this setting can negatively affect the performance of your Splunk software deployment.

If you are running Splunk Enterprise Security on Splunk Cloud, file a support ticket for assistance with this setting.

1. Open `limits.conf` for editing. See How to edit a configuration file in the Splunk Enterprise *Admin Manual*.
2. Set `max_events_per_bucket` to a number above 1000.
3. Save.

See limits.conf for more about the `max_events_per_bucket` setting.

Add a navigation link to a filtered view of Incident Review

To help ES analysts with their workflows, you can add a link in the app navigation that loads a version of Incident Review with filters applied. See Add a link to a filtered view of Incident Review.

Manually create a notable event in Splunk Enterprise Security

You can manually create a notable event from an indexed event, or create one from scratch.

Note: By default, only administrators with the edit_reviewstatuses capability can manually create notable events. To grant other users this capability, see Configure users and roles in the *Installation and Upgrade Manual*.

Create a notable event from an existing event

You can create a notable event from any indexed event using the **Event Actions** menu. Do not create a notable event from notable events on the Incident Review dashboard.

1. From an event, view the event details and click **Event Actions**.
2. Select **Create notable event**.
3. Enter a **Title** for the event.
4. (Optional) Select a security **Domain**.
5. (Optional) Select an **Urgency** level.
6. (Optional) Select an **Owner**.
7. (Optional) Select a **Status**.
8. Enter a **Description** for the event that describes why you created the notable event or what needs to be investigated.
9. Save the new notable event. The **Incident Review** dashboard displays with your new notable event.

Note: A notable event created in this way includes tracking fields such as **Owner** and **Status**, but does not include the unique fields or links created when a notable event is generated by a correlation search alert action.

Create a notable event from scratch

Create a notable event based on observations, a finding from a security system outside Splunk, or something else.

1. Select **Configure > Incident Management > New Notable Event**.
2. Enter a **Title** for the event.
3. (Optional) Select a security **Domain**.
4. (Optional) Select an **Urgency** level.
5. (Optional) Select an **Owner**.
6. (Optional) Select a **Status**.
7. Enter a **Description** for the event that describes why you created the notable event or what needs to be investigated.
8. Save the new notable event. The **Incident Review** dashboard displays with your new notable event.

Use the owner field in a Splunk event to create a notable event with said owner

Normally in a correlation search, the `owner` field automatically maps to `orig_owner`. If you have some Splunk events, doesn't matter where they came from, and you want the owner field of the Splunk event to be the owner of the notable event, it is crucial that the value of the `owner` field is a Splunk username. To use the owner field in a Splunk event to create a notable event with said owner, remove the `owner` field from the list of notable `mapfields`.

Your correlation rule will look similar to the following in
`$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/savedsearches.conf`:

```
## savedsearches.conf
[Threat ? My Correlation ? Rule]
?
action.notable.param.mapfields =
rule_id,rule_name,rule_title,rule_description,security_domain,nes_fields,drilldown_name,drilldown
_search,governance,control,status,default_owner,drilldown_earliest_offset,drilldown_latest_offset,next
_steps,investigation_profiles,extract_artifacts,recommended_actions
?
```

For example, if you have a CSV lookup that contains the "owner" field for assigning the new owners, then you can dynamically update the owner of an event in incident review by updating the lookup using a search similar to this one:

```
| inputlookup es_notable_events | search owner=gleb | eval owner="george"| outputlookup es_notable_events
append=true key_field=owner
```

Pinpoint the original event via drill-down

If you are creating a notable event from a raw event, you can pinpoint the specific raw event that contributed to the notable event.

When certain fields exist such as `orig_event_hash`, a secondary drill-down link is automatically constructed for you called "View original event." If the correct fields are passed with the notable event you can construct a very performant search for getting back to the original event.

The following fields come into play:

- `orig_time` (optional)
- `orig_index` (optional)
- `orig_indexer_guid` (optional)
- `orig_event_hash` (required)

The `orig_time` and `orig_index` are automatically created if you pass `_time` and `index` respectively. This is because `_time` and `index` are included in the default set of `mapfields`. For `indexer_guid` and `event_hash` you will either need to manually rename to `orig_<field>` or add them to `mapfields` as appropriate.

Your correlation rule will look similar to the following in `$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/savedsearches.conf`:

```
## savedsearches.conf
[Threat ? My Correlation ? Rule]
?
action.notable.param.mapfields =
rule_id,rule_name,rule_title,rule_description,security_domain,nes_fields,drilldown_name,drilldown
_search,governance,control,status,owner,default_owner,drilldown_earliest_offset,drilldown_latest_offset,next
_steps,investigation_profiles,extract_artifacts,recommended_actions,indexer_guid,event_hash
?
```

Customize notable event settings in Splunk Enterprise Security

As a Splunk Enterprise Security administrator, you can make configuration changes to **notable events**.

- Change notable event fields.
- Manage notable event statuses.
- Create and manage notable event suppressions.

Change notable event fields

Make changes to the fields displayed on the Incident Review dashboard for notable events on the Incident Review Settings dashboard. For example, change the label of a field in the notable event details, remove a field, or add a field to the **Additional Fields** section of the notable event details. Changes that you make to notable event fields affect all notable events.

1. From the Splunk Enterprise Security menu bar, select **Configure > Incident Management > Incident Review Settings**.
2. Review the **Incident Review - Event Attributes**.
3. Click **Edit** to change a field or the label for a specific field that appears on Incident Review.
4. Click **Remove** to remove a field from the notable event details on the Incident Review dashboard.
5. Click **Save** to save your changes.

Add a field to the notable event details

A field appears in the **Additional fields** of the notable event details if the field exists in the correlation search results and Incident Review can display the field. To add a field to the notable event details, first make sure that the correlation search results include the field and then make sure that Incident Review can display the field.

1. Determine if the field you want to see is included in the correlation search results. Run the correlation search on the Search page to review the output or the search syntax.
    - If the field exists in the search results, go to step four.
    - If the field does not exist in the search results, go to step two.

2. Modify the correlation search to include the field.
    - If you can edit the search with the guided search editor, add the field as an aggregate function with an alias. Use the **values** function to return all possible values of a given field, or the **latest** function to return the most recent value for the field.
    - If you created the search manually, modify the search to extract the fields. Make sure that you do not modify the correlation criteria when you modify the search.
        - ◊ If the search does not include statistical transformations, add `| fields + newfieldname` to the end of the search, where `newfieldname` is the name of the new field you want to see in the additional details.
        - ◊ If the search does include statistical transformations, extract the fields when you perform the statistical transformation.
3. Verify changes to correlation searches on the Search page before saving them.
4. Add the field to the list of additional fields.
    1. From the Splunk Enterprise Security menu bar, select **Configure > Incident Management > Incident Review Settings**.
    2. Click **Add new entry** to add the new field to the **Additional Fields** section of the notable event details.
    3. Type a **Label** to use as the display name of the field in the notable event details.
    4. Type a **Field** to match the field that you want to appear in the notable event details.
    5. Click **Done**.
    6. Click **Save**.

SPL search to verify the additional fields

Use the following search to get a list of all of the active **Additional Fields**.

```
| rest splunk_server=local /servicesNS/-/-/configs/conf-log_review/incident_review | fields
event_attributes | eval d=split(event_attributes, "},") | rex field=d max_match=0
"field\"\s*:\s*\"(?<field>[^\"]+)" | rex field=d max_match=0 "label\"\s*:\s*\"(?<label>[^\"]+)" | eval
mv=mvzip(field,label) | fields mv | mvexpand mv | eval field=mvindex(split(mv,","), 0),
label=mvindex(split(mv,","), 1) | table field, label
```

A truncated example response follows.

field	label
action	Action
app	Application
bytes_in	Bytes In
bytes_out	Bytes Out
category	Category
change_type	Change Type
channel	Channel
command	Command
cpu_load_percent	CPU Load (%)
creator	Creator
creator_realname	Creator Realname
cve	CVE

field	label
decoration	Decoration
desc	Description
dest	Destination
dest_threatlist_category	Destination Threat List Category
dest_threatlist_description	Destination Threat List Description
dest_threatlist_name	Destination Threat List Name
dest_bunit	Destination Business Unit
dest_category	Destination Category

Manage notable event statuses

An analyst assigns a status to a notable event in the investigation workflow. The status aligns with the stages of an investigation, and can be used to review and report on the progress of a notable event investigation on the Incident Review Audit dashboard.

To see the available statuses for notable events, select **Configure > Incident Management > Status Configuration**.

Label	Description	Can be edited
Unassigned	Used by Enterprise Security when an error prevents the notable event from having a valid status assignment.	No
New (default)	The notable event has not been reviewed.	No
In Progress	An investigation or response to the notable event is in progress.	Yes
Pending	Closure of the notable event is pending some action.	Yes
Resolved	The notable event has been resolved and awaits verification.	Yes
Closed	The notable event has been resolved and verified.	Yes

Every notable event is assigned a status of **New** by default when it is created by a correlation search. You can customize notable event statuses to match an existing workflow at your organization.

Edit notable event statuses

Change the available statuses for notable events on the **Edit Notable Event Status** page.

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select a notable event status to open the **Edit Notable Event Status** page.
3. (Optional) Change the **Label** or **Description**.

You cannot edit the **Unassigned** and **New** statuses because they are defaults used when creating notable events.

Manage notable event status history

Notable events are associated with users, statuses, and comments. Changes made to status names only affect the name of a status, not the status ID assigned to the notable event in the notable index.

If you change the name of a default notable event status, the name changes for both past and future notable events. For example, if you rename "pending" to "waiting for customer", all notable events with a status of "pending" will then have a status of "waiting for customer". The status ID assigned to the notable events remains the same.

Notable event status transitions

Statuses represent the steps in investigating a notable event. Status transitions define the path of a notable event investigation.

An analyst changes the status of the notable event as the investigation progresses. To change the status of a notable event:

- The analyst must be a member of a role that has permission to change a status. The ability to change notable event statuses is available to the **ess_analyst** and **ess_admin** roles by default.
- The follow-on status must allow a transition from the current status. By default, every status can transition to any other status. For example, an analyst can change the status of a notable event with the **New** status to any other status, such as **Closed**.

Restrict notable event status transitions

You can define a status workflow and limit which statuses analysts can transition to other statuses, creating a path for a notable event investigation. By default, a notable event in any status can be changed to any other status.

Prerequisites

- You must have the **ess_admin** role or your role must be assigned the **Edit Statuses** capability. For more information about user roles and capabilities, see Configure users and roles in the *Installation and Upgrade Manual*.
- Define a status workflow for notable event investigations. Determine which statuses to require, and whether analysts must follow a specific sequence of statuses before completing the workflow. Determine whether any roles can bypass the full workflow.

Steps

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select a notable event status to open the Edit Notable Event Status page.
3. In Status Transitions, modify the **To Status** fields. These fields control which statuses analysts can transition a notable event to if it is in the status that you are editing.
    1. To define which roles are allowed to transition a notable event to the selected status, choose the **Authorization** field and add or remove roles.
    2. To remove a transition for an event to the selected status, choose **Unselect All**.
4. Click **Save**.

Example of restricting notable event status transitions

This example walks you through setting up restricting status transitions for analysts. Restrict status transitions so that analysts must follow a path from New, to In Progress or Pending, to Resolved, then to Closed.

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Restrict the transitions from the **New** status. Select the **New** status to open the Edit Investigation Status page.
3. In **Status Transitions**, select the roles for the **Resolved** status and deselect the check box for the ess_analyst role.

4. Select the roles for the **Closed** status and deselect the check box for the ess_analyst role.
5. Click **Save** to save the changes to the **New** status.
6. Restrict the transitions on the **In Progress** and **Pending** statuses to prevent the ess_analyst role from transitioning to **New** or to **Closed**.
7. Select the **In Progress** status.
8. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **Closed** status.
9. Click **Save** to save the changes to the **In Progress** status.
10. Repeat steps 8 and 9 for the **Pending** status.
11. Restrict the **Resolved** status. Click the **Investigation** tab and select the **Resolved** status.
12. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **In Progress** and **Pending** statuses.
13. Click **Save** to save the changes to the **Resolved** status.
14. Restrict the transitions for the **Closed** status. Select the **Closed** status.
15. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **In Progress**, **Pending**, and **Resolved** statuses.
16. Click **Save** to save the changes for the **Closed** status.

Create a status

Create a status for the notable event investigation workflow.

Prerequisites

If you restrict status transitions, determine where the new status is needed in the workflow and whether any roles can bypass the new status in the workflow.

Steps

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select **Create New Status > Notable**.
3. Type a **Label** that represents the status on the Incident Review dashboard.
   For example, Waiting on ITOps.
4. (Optional) Type a description that appears on the Status Configuration page.
   For example, Waiting on the IT operations department.
5. (Optional) Select the check box for **Default Status**. Select this check box if you want to replace the **New** status as the default status for newly-created notable events.
6. (Optional) Select the check box for **End Status**. Select this check box if you are adding an additional **Closed** status for notable events, such as **False Positive**.
7. (Optional) Deselect the check box for **Enabled**. Deselect this check box if you want to create this status without using it.
8. Update the status transitions by modifying the **To Status** fields. If you do not select any roles that can transition from this status to another one, no one will be able to move the notable event to a different status after transitioning the notable event to this status. If you do not restrict status transitions, select all roles for each status.
9. Click **Save**.

If you restrict status transitions based on user roles, modify the status transitions for each status that can transition to this new status.

Create and manage notable event suppressions

You can hide notable events from the Incident Review dashboard by creating a notable event suppression.

A suppression is a search filter that hides additional notable events from view, and is used to stop excessive or unwanted numbers of notable events from appearing on the Incident Review dashboard. Notable events that meet the search conditions are still created and added to the notable index. Suppressed notable events continue to contribute to notable event counts on the Security Posture and auditing dashboards.

To prevent notable events that meet certain conditions from being created, see Throttle the number of response actions generated by a correlation search.

You can create a suppression filter in two ways.

- Create a suppression from Incident Review. See Suppress a notable event.
- Create a suppression from the **Configure** menu. See Create a suppression from Notable Event Suppressions.

Create a suppression from Notable Event Suppressions

1. Select **Configure > Incident Management > Notable Event Suppressions**.
2. Click **Create New Suppression**.
3. Enter a **Name** and **Description** for the suppression filter.
4. Enter a **Search** to use to find notable events to be suppressed.
   The search goes directly into the eventtype stanza, so the use of pipes is limited. See eventtypes.conf in the Splunk Enterprise *Admin Manual*.
5. Set the **Expiration Time**. This defines a time limit for the suppression filter. The expiration time does not prevent the suppression from working, so events within the specified time range will continue to be suppressed until you disable the suppression. Notable events that fall outside the expiration time are not suppressed.

Edit notable event suppressions

1. Select **Configure > Incident Management > Notable Event Suppressions**.
2. Select a notable event suppression to open the **Edit Notable Event Suppression** page.
3. Edit the **Description** and **Search** fields used for the suppression filter.
4. Click **Save**.

Disable notable event suppressions

1. Select **Configure > Incident Management > Notable Event Suppressions**.
2. Select **Disable** in the **Status** column for the notable event suppression.

Remove a notable event suppression

1. From the Splunk platform toolbar, select **Settings > Event types**.
2. Search for the the suppression event: `notable_suppression-<suppression_name>`.
3. Select **delete** in the **Actions** column for the notable event suppression.

Audit notable event suppressions

Audit notable event suppressions with the **Suppression Audit** dashboard. See Suppression Audit in *Use Splunk Enterprise Security*.

Expand tokens in notable events using the expandtoken command

Tokens in notable event titles and descriptions automatically get expanded to include the values of the tokens on the Incident Review dashboard. With the `expandtoken` search command, you can expand the tokens in so that token replacement happens in your search results. The `expandtoken`search command is intended for use in Splunk Web.

Description

Expand the fields in notable events that contain tokens in the values, such as the title (`rule_name`) or description (`rule_description`) of a notable event. Tokens are automatically expanded on the Incident Review dashboard, but not within search.

Syntax

... | expandtoken [field],[field1],[field2]...

Optional argument

field

> **Description:** The name of a field in the notable event that contains a token to expand. Do not specify the name of the token. Specify additional fields separated by commas. If you do not specify a field, all fields are processed for tokens to expand. For a list of example fields in notable events, see Using notable events in search in the Splunk developer portal.

Usage

The `expandtoken` command is a **streaming command**.

Limitations

The search command does not support token delimiters in the middle of a field name.

If you have tokens dependent on the expansion of other tokens, those tokens might not be reliably expanded because you cannot specify the order in which tokens are expanded. For example, if you have a rule_description: "Brute force access behavior detected from $src$." and a drilldown_name: "See contributing events for $rule_description$", the following search might expand the $src$ token without expanding the $rule_description$ token.

```
`notable` | expandtoken
```

For more information about tokens, see Token usage in dashboards in the Splunk Enterprise *Dashboards and Visualizations Manual*.

Examples

The following examples show usage of the `expandtoken` search command in Splunk Web.

Expand tokens for all notable events

```
`notable` | expandtoken rule_title,rule_description,drilldown_name,drilldown_search
```

Expand tokens for a specific notable event

Expand tokens for a specific notable event based on the event_id field.

```
`notable` |where event_id="<event_id>" | expandtoken rule_title,rule_description
```

Expand tokens for a specific notable event based on the short ID field.

```
`notable` | where notable_xref_id="<short ID>" | expandtoken rule_title,rule_description
```

See also

For a list of example fields in notable events, see Using notable events in search in the Splunk developer portal.

For more information about tokens, see Token usage in dashboards in the Splunk Enterprise *Dashboards and Visualizations Manual*.

Manage investigations in Splunk Enterprise Security

As an Enterprise Security administrator, you can manage access to security investigations, and support analysts by troubleshooting problems with their action history.

For more information about the analyst investigation workflow, see Investigations in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Manage access to investigations

Users with the **ess_admin** role can create, view, and manage investigations by default. Users with the **ess_analyst** role can create and edit investigations. Make changes to capabilities with the Permissions dashboard.

- To allow other users to create or edit an investigation, add the **Manage Your Investigations** capability to their role. Users can only make changes on investigations on which they are a collaborator.
- To allow other users to manage, view, and delete all investigations, add the **Manage All Investigations** capability to their role.

See Configure users and and roles in the *Installation and Upgrade Manual*.

You can manage who can make changes to an investigation by setting write permissions for collaborators on a specific investigation. By default, all collaborators have write permissions for the investigations to which they are added, but other collaborators on the timeline can change those permissions to read-only. See Make changes to the collaborators on an investigation in *Use Splunk Enterprise Security*.

After a user creates an investigation, any user with the **Manage All Investigations** capability can view the investigation, but only the collaborators on the investigation can edit the investigation. You cannot view the investigation KV Store collections as lookups. Only users with the admin role can view or modify the KV store collections using the KV Store API endpoint. For details about using the KV Store API endpoint, see KV Store endpoint descriptions in the Splunk Enterprise

REST API Reference Manual.

Data sources for investigations

Splunk Enterprise Security stores investigation information in several KV Store collections. The investigations on the Investigations page, items added to the investigation, attachments added to notes on the investigation, and artifacts added to the investigation workbench each have their own collection. See **Investigations** in the Dashboard requirements matrix for Splunk Enterprise Security.

Investigation details from investigations created in versions earlier than 4.6.0 of Splunk Enterprise Security are stored in two KV Store collections, `investigative_canvas` and `investigative_canvas_entries`. Those collections are preserved in version 4.6.0 but the contents are added to the new investigation KV Store collections. So to restore, you may need to restore `investigation`, `investigation_attachment`, `investigation_event`, `investigation_lead`, `investigative_canvas`, and `investigative_canvas_leads`.

Troubleshoot investigation action history items

When an analyst selects a type of action history to add to an investigation, one of five searches run over the selected time range.

- Dashboard Views - Action History
- Search Tracking - Action History
- Per-Panel Filtering - Action History
- Notable Suppression - Action History
- Notable Status - Action History

View the searches by navigating to **Configure** > **Content** > **Content Management** and using the filters on the page. If you change these saved searches, action history items might fail to appear in your action history. To exclude a search from your action history, use the Action History Search Tracking Whitelist lookup. See Create and manage lookups in Splunk Enterprise Security.

Administer and customize the investigation workbench

The workbench extends existing investigation functionality in Splunk Enterprise Security by allowing analysts to perform investigative actions in one location. Analysts investigate artifacts, or assets and identities, using panels, tabs, and profiles on the workbench. You can customize the workbench by creating panels, tabs, and profiles to help analysts. You can also set up artifact extraction from notable events to accelerate investigations that start from notable events.

The workbench introduces a configuration file, `es_investigations.conf`, that is used to manage the metadata for panels, tabs, and profiles. You can make changes in the file system by adding stanzas to the `es_investigations.conf` file. Refer to `es_investigations.conf.spec` and `es_investigations.conf.example` for details.

Create panels and tabs for the investigation workbench

The investigation workbench can display any prebuilt panel that has a workbench panel reference and has been added to a workbench tab.

1. Create or modify a prebuilt panel. See Create or modify a prebuilt panel for the investigation workbench in this topic.

2. Create a workbench panel that references the prebuilt panel. See Create a tab for the investigation workbench in this topic.
3. Create a workbench tab that includes the workbench panel. See Create a tab for the investigation workbench in this topic.

For an example of this entire process, see Example panel conversion and workbench panel creation in this topic.

Create or modify a prebuilt panel for the investigation workbench

You can use any prebuilt panel on the investigation workbench. You can create one specifically for the workbench, or you can modify an existing panel. You can create or modify a prebuilt panel with Splunk Enterprise Security in several ways:

- Create a panel from Content Management.
    1. From the ES menu bar, select **Configure** > **Content** > **Content Management**.
    2. Select **Create New Content** > **Panel**.
    3. Type a **Prebuilt panel ID**.
    4. Select a **Destination App**.
    5. Type **Prebuilt panel XML**.
    6. Click **Save**.
- Convert a dashboard panel to a prebuilt panel. See Convert an existing panel to a prebuilt panel in *Dashboards and Visualizations*.
- Modify a panel in Splunk Settings.
    1. From the Splunk menu bar, select **Settings** > **User Interface**.
    2. Click **Prebuilt Panels** and click **Edit** > **Edit Panel** for the panel that you want to modify.

       If you modify an existing prebuilt panel, consider cloning it before you modify it. If you clone the panel, change the panel ID so that you remember which one is specific to the workbench.
- Create a panel in Splunk Settings. See Add panels to dashboards in *Dashboards and Visualizations*.

When creating or modifying a prebuilt panel for the workbench, follow these guidelines for the best user experience:

- Add one or more tokens to the panel search to limit your search results to the artifacts investigated on the workbench. Use multiple tokens to substitute more than one type of artifact. Define your token using the syntax `$token$`. You set up the format of the token when you create the workbench panel.
- Remove the panel name from the panel XML. If you do not do this, two panel titles appear on the workbench. Workbench panels get the title from the **Label** field when you create a workbench panel.
- Add a drilldown to the panel so that analysts can add artifacts from the panel. Add a drilldown using the syntax `<option name="drilldown">cell</option>` in the panel XML. The workbench replaces existing panel drilldowns, such as custom searches, with this ability to add artifacts to the workbench scope from the panel.
- Update the permissions on the panel to be shared with Splunk Enterprise Security. Confirm that the panel is **Shared in App** or set to **Display For: All Apps**.
- If you save your panel in a dedicated app, make sure that the objects in the app are set to export globally. See Set permissions for objects in a Splunk app in the Splunk dev portal.
- To make your panel use a different time range than the one set by the workbench, set a time range in the panel search or panel XML.

Then, follow the steps to create a panel for the investigation workbench. See Create a panel for the investigation workbench in this topic.

Create or modify a panel for the investigation workbench

Create a workbench panel.

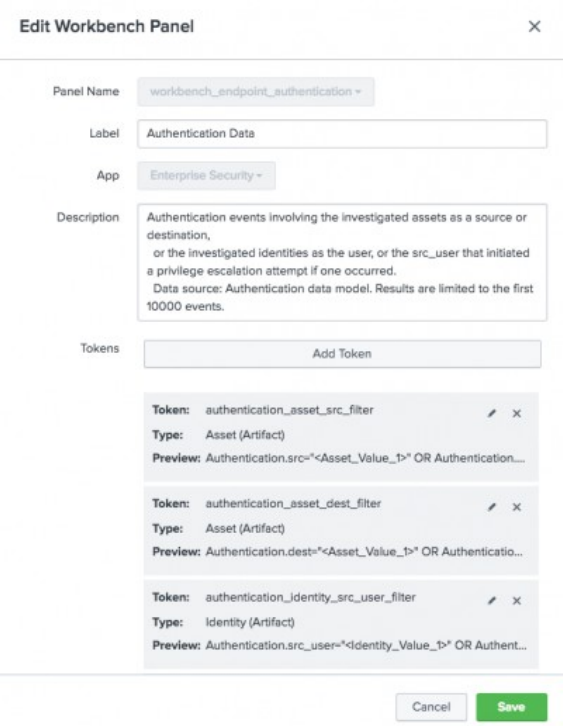
1. Select **Configure** > **Content** > **Content Management**.
2. Select **Create New Content** > **Workbench Panel**.
3. Select the prebuilt panel that you want to use on workbench from the drop-down list.
4. (Optional) Type a **Label** to replace the default panel title on the workbench.
5. (Optional) Type a **Description** to provide information about the panel.
6. Add a token to replace the token in the panel search. See Example panel conversion and workbench panel creation in this topic or see Define tokens for multiselect inputs in the Splunk Enterprise *Dashboards and Visualizations Manual*.
    1. Select the type of artifact from the **Type** drop-down menu: Identity, Asset, File, or URL.
    2. Click **Apply.**
7. Click **Save**.
8. Click **Save**.

Then add the panel to a tab so that it is visible on the workbench.

Modify a workbench panel.

1. Select **Configure** > **Content** > **Content Management**.
2. From the Type filter, select **Workbench Panel**.
3. Click the name of the panel.
4. Edit something, such as a token.

Tokens are now displayed in summary view instead of list view. The summary view displays each token name, type of artifact, and a preview of the token text that is generated out of the artifacts and put into place to run the search.



Edit Workbench Panel ×

Panel Name: workbench_endpoint_authentication ▾

Label: Authentication Data

App: Enterprise Security ▾

Description: Authentication events involving the investigated assets as a source or destination,
or the investigated identities as the user, or the src_user that initiated a privilege escalation attempt if one occurred.
Data source: Authentication data model. Results are limited to the first 10000 events.

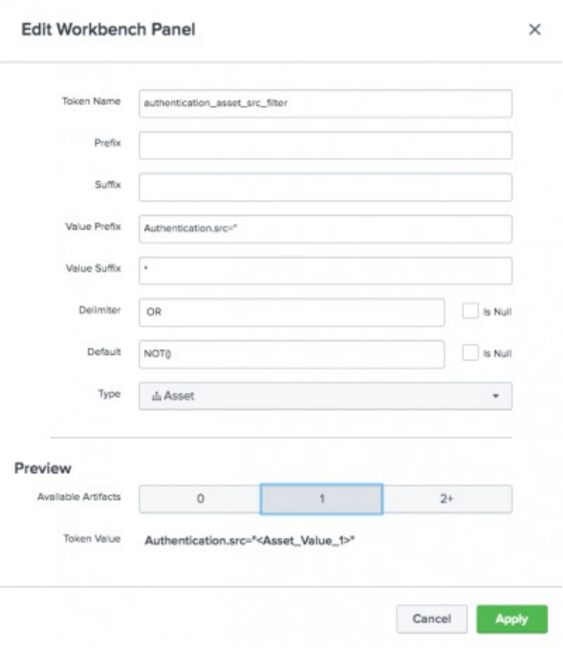
Tokens: Add Token

Token: authentication_asset_src_filter
Type: Asset (Artifact)
Preview: Authentication.src="<Asset_Value_1>" OR Authentication....

Token: authentication_asset_dest_filter
Type: Asset (Artifact)
Preview: Authentication.dest="<Asset_Value_1>" OR Authenticatio...

Token: authentication_identity_src_user_filter
Type: Identity (Artifact)
Preview: Authentication.src_user="<Identity_Value_1>" OR Authent...

When you click the pencil to edit a token in the summary view, it will slide open into edit mode. In the preview section at the bottom of the edit window, you can see how the token value changes as you edit the token parameters. This helps to simulate what you will see in the search under certain situations.



Edit Workbench Panel

Token Name: authentication_asset_src_filter

Prefix:

Suffix:

Value Prefix: Authentication.src="

Value Suffix: "

Delimiter: OR ☐ Is Null

Default: NOT() ☐ Is Null

Type: Asset

Preview

Available Artifacts: 0 | 1 | 2+

Token Value: Authentication.src="<Asset_Value_1>"

Create a tab for the investigation workbench

Create a tab to display information specific to a particular data type, use case, or something else.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Workbench Tab**.
3. Type a **Tab Name**. This name becomes part of the stanza name in `es_investigations.conf` and is used as the label if you do not specify a label.
4. (Optional) Type a **Label** to provide a user-facing name for the workbench tab.
5. In **Workbench Panels**, select the panels that you want to appear on this tab. The order in which you select the panels is the order in which they appear on this tab on the workbench.
6. (Optional) Select a workbench profile to associate with this tab. You can only associate a tab with one profile. Profiles allow analysts to load multiple tabs that relate to a use case on the workbench.
7. (Optional) Change the **Load by default** selection. Select **True** if you want this tab to load for all workbench investigations.
8. (Optional) Type a **Description** for the tab. This helps analysts determine what types of information and context they can gather using the panels on the tab.
9. Click **Save**.

Example panel conversion and workbench panel creation

Prerequisite

You must have the Splunk Add-on for Blue Coat ProxySG installed, and data from the add-on in your Splunk Enterprise Security deployment. You can download the Splunk Add-on for Blue Coat ProxySG from Splunkbase.

1. Clone a panel and modify the search to use an input token with the workbench.
    1. Select **Settings > User Interface**.
    2. Click **Prebuilt panels**.
    3. Click **Edit > Clone** for the `actions_by_destination_ip` for the `Splunk_TA_bluecoat-proxysg`.
    4. Type a Prebuilt panel ID. `workbench_actions_by_dest_ip`.
    5. Remove the title from the XML, unless you want two titles to appear on the workbench.
    6. Modify the query in the XML to include a token that limits the results to the investigated asset artifacts.
       ```
       sourcetype="bluecoat:proxysg:access*" $dest_token$ | iplocation dest | geostats count by
       action
       ```
    7. Decide whether to remove the `<earliest>` and `<latest>` time range for the panel. This time range takes precedence over the time range set on the workbench, so you likely want to remove it so that analysts can perform context-sensitive searches.
    8. Click **Save**.
2. Modify the permissions of the panel.
    1. Locate the panel that you just created, `workbench_actions_by_dest_ip`.
    2. Select **Edit > Edit Permissions**.
    3. For **Display for**, select **All apps**.
    4. Click **Save**.
3. Return to Splunk Enterprise Security and set up the panel to be used on the workbench.
    1. Select **Configure > Content > Content Management**.
    2. Select **Create New Content > Workbench Panel**.
    3. Select a **Panel Name** of **workbench_actions_by_dest_ip**.
    4. (Optional) Type a user-facing **Label** that appears on the workbench: **Proxy Actions by Destination**.
    5. (Optional) Type a user-facing description that appears on the workbench: **Displays a map that graphs the actions by destination IP, when possible, specific to the investigated assets.**
    6. Click **Add a Token** to add a token for the **$dest_token$** from the search.
    7. Type a **Token Name** that corresponds to the token name. **dest_token**
    8. Type a **Prefix** of **(**.
    9. Type a **Suffix** of **)**.
    10. Type a **Value Prefix** of **dest="**.
    11. Type a **Value Suffix** of **"**.
    12. Unselect the check box for **Is Null** for the **Delimiter** and type ` OR ` in the text box. Include the spaces on either side of the OR.
    13. Leave the check box for **Is Null** for the **Default** field selected. If this check box is selected, the search runs only when an artifact of the relevant type is selected on the workbench. In this case, the search runs only if you are exploring assets on the workbench.
    14. Select a **Type** of **Asset**, because the destination is an asset, not an identity or file or URL.
    15. Click the **Available Artifacts** buttons to see what the token value will look like if there are 0, 1, or 2 artifacts. For an example of two assets:
        ```
        (dest="<Asset_Value_1>" OR dest="<Asset_Value_2>")
        ```
    16. Click **Apply**.
    17. Click **Save**.
        This panel now contains a search that would be constructed as follows for two assets investigated on the workbench:

        ```
        sourcetype="bluecoat:proxysg:access*" (dest="<investigated_asset_1>" OR
        dest="<investigated_asset_2>") | iplocation dest | geostats count by action
        ```
4. Add the new panel to a new tab.
    1. On Content Management, select **Create New Content > Workbench Tab**.
    2. Type a **Tab Name** of **proxy_data**. This name becomes the stanza name in `es_investigations.conf` and is used as the label if the label is not specified.
    3. (Optional) Type a **Label** of **Proxy Data**.

4. In **Workbench Panels**, type and select the **Proxy Actions by Destination IP** panel.
5. For **Load by default**, leave it as **False**. Select True if you want this tab to load for all workbench investigations.
6. (Optional) Type a **Description** for the tab. **Proxy data related to investigated assets and identities.**
7. Click **Save**.

Analysts can then open a workbench and add the new tab to start investigating proxy data in the workbench.

Create a workbench profile

You can use profiles on the workbench to associate several tabs together that all fit a specific use case. For example, a DDoS Investigation profile might include a Firewall data tab and a general Network data tab. An analyst can then add the DDoS Investigation profile to an investigation to add both of those tabs to the workbench, rather than having to individually add tabs that fit the investigation.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Workbench Profile**.
3. Type a **Profile Name**. This name becomes the stanza name in `es_investigations.conf` and is used as the label if the label is not specified.
4. (Optional) Type a **Label** to provide a user-facing name for the workbench profile.
5. (Optional) Type a **Description** for the profile. This helps analysts determine what types of information and context they can gather by adding the profile to their investigation.
6. Click **Save**.

After creating a profile, update the tabs with the profile that you created. For the DDoS investigation example, edit the Firewall data and Network data tabs and select the new DDoS Investigation profile.

Set up artifact extraction for notable events

You can define the fields that are automatically extracted as identities or assets on the workbench when a notable event is added to an investigation. By default, the same fields that are used for asset and identity correlation are the fields extracted from the notable events created by included correlation searches. You must add fields to be extracted for any custom correlation searches.

When artifacts are extracted, duplicates are not created if they already exist in the investigation. You will see a notification that "the following artifacts already exist and have not been added." The existing artifact is not linked against the new notable event that would have caused the duplicate artifact to be created. This does not prevent you from manually adding a duplicate artifact.

Type of investigation artifact	Fields extracted for investigation scope
Asset	`dest`, `src`, `dvc`, `orig_host`
Identity	`src_user`, `user`, `src_user_id`, `src_user_role`, `user_id`, `user_role`, `vendor_account`
File and URL	These correspond to the artifact creation flow on the investigation workbench. Instead of creating a file or URL artifact on the workbench by hand, you can specify which fields should be used to create artifacts automatically when you add a notable to the investigation workbench.

If your correlation search does not use data models, or the search results contain different fields that you want to extract, you can specify the fields to extract into the investigation scope.

1. Select **Configure > Content > Content Management**.
2. Click the correlation search that you want to customize to open it for editing.
3. Select the notable event adaptive response action.
4. For **Asset Extraction**, type a field name from the correlation search results that identifies an asset. Press Enter to add the field name.
5. For **Identity Extraction**, type a field name from the correlation search results that identifies an identity. Press Enter to add the field name.
6. Click **Save**.
7. For **File Extraction**, type a field name from the correlation search results that identifies a file. Press Enter to add the field name.
8. Click **Save**.
9. For **URL Extraction**, type a field name from the correlation search results that identifies a URL. Press Enter to add the field name.
10. Click **Save**.

Manage and customize investigation statuses in Splunk Enterprise Security

Starting in version 5.0.0, you can add statuses to investigations. After upgrading to this version, investigations that did not have a status are assigned the **New** status.

To change the status of an investigation, an analyst must have the `transition_reviewstatus-<x>_to_<y>` capability for the statuses that they want to transition between. The ess_analyst role and the ess_admin role have those capabilities for all statuses by default. Modifying status transitions for investigations modifies these capabilities.

To make changes to statuses as an analyst, you must have the `edit_reviewstatuses` capability. The ess_admin role has this capability by default. See Configure users and roles in the *Installation and Upgrade Manual*.

Create an investigation status

Create a status for analysts to select when performing an investigation.

If you restrict status transitions, update status transitions after creating a status, otherwise analysts will be unable to select the new status. See Restrict status transitions for investigations in this topic.

1. From the Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. (Optional) Select the **Investigation** tab to review existing investigation statuses.
3. Select **Create New Status > Investigation**.
4. Type a **Label** that appears as the name of the status on the investigation.
   For example, Waiting on Desktop IT.
5. (Optional) Type a **Description** that appears on the **Status Configuration** page to describe the status.
   For example, Investigation is waiting for desktop IT to perform additional remediation or forensics steps.
6. (Optional) Select the check box for **Default Status** to set this status as the default for newly-created investigations.
7. (Optional) Select the check box for **End Status** to set this status as a possible last status for an investigation.
8. (Optional) Deselect the check box for **Enabled** to create the status without allowing anyone to use it yet.
9. Update the user roles that are able to transition an investigation from this new status, for example Waiting on Desktop IT, to another status, such as Closed. If you do not select any roles that can transition from this status to another one, no one will be able to move the investigation to a different status after transitioning the investigation to this status.
10. Click **Save**.

Restrict status transitions for investigations

The status transitions that can be made on an investigation define the path of an investigation. By default, an investigation in any status can be changed to any other status. For example, someone can change the status of an investigation in the **New** status to any other status, such as **Closed**.

You can restrict the statuses that analysts can choose when investigating. Determine which statuses to require, and whether analysts must follow a specific sequence of statuses before completing an investigation. Determine whether any roles can bypass the full sequence of statuses.

This example walks you through setting up restricting status transitions for analysts. Restrict status transitions so that analysts must follow a path from New, to In Progress or Pending, to Resolved, then to Closed.

1	2	3	4
New	In Progress Pending	Resolved	Closed

Prerequisites

- You must have the **ess_admin** role or your role must be assigned the **Edit Statuses** capability. For more information about user roles and capabilities, see Configure users and roles in the *Installation and Upgrade Manual*.

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Click the **Investigation** tab.
3. Restrict the transitions from the **New** status. Select the **New** status to open the Edit Investigation Status page.
4. In **Status Transitions**, select the roles for the **Resolved** status and deselect the check box for the ess_analyst role.
5. Select the roles for the **Closed** status and deselect the check box for the ess_analyst role.
6. Click **Save** to save the changes to the **New** status.
7. Restrict the transitions on the **In Progress** and **Pending** statuses to prevent the ess_analyst role from transitioning to **New** or to **Closed**.
8. Click the **Investigation** tab and select the **In Progress** status.
9. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **Closed** status.
10. Click **Save** to save the changes to the **In Progress** status. Repeat those steps for the **Pending** status.
11. Restrict the **Resolved** status. Click the **Investigation** tab and select the **Resolved** status.
12. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **In Progress** and **Pending** statuses.
13. Click **Save** to save the changes to the **Resolved** status.
14. Restrict the transitions for the **Closed** status. Click the **Investigations** tab and select the **Closed** status.
15. In **Status Transition**, select the roles for the **New** status and deselect the check box for the ess_analyst role. Repeat for the **In Progress**, **Pending**, and **Resolved** statuses.
16. Click **Save** to save the changes for the **Closed** status.

Create a workbench panel workflow action in Splunk Enterprise Security

Use an embedded workbench as workflow field action to get more context about specific values in Incident Review. The embedded workbench provides a simplified drill-down experience, reduces the number of open tabs, and makes it easier to determine notable event trends. Pre-built panels can be embedded in dashboards and investigations, as well as directly within Incident Review.

Do the following to create a workbench panel workflow action and use an embedded workbench:

1. Create a new panel or edit a prebuilt panel
2. (Optional) Create a workbench panel from a prebuilt panel
3. Create a workflow action
4. Click on the field workflow action in Incident Review
5. View the embedded workbench

Create a new prebuilt panel or edit a prebuilt panel

Create a new prebuilt panel, or edit of the existing prebuilt panels that ship with Enterprise Security.

Create a prebuilt panel

If you are interested in investigating data that is not already included in a prebuilt panel, you can create your own panel. See Create panels and tabs for the investigation workbench.

Edit an existing prebuilt panel

Editing an existing workbench panel allows you to add tokens to the panel, or view tokens that are already defined. This example starts with editing the existing prebuilt panel of **workbench_context_computer_inventory** for use in creating the workflow action in the next step.

From the Enterprise Security menu bar, modify the **workbench_context_computer_inventory** panel by performing the following steps:

1. Select **Configure > Content > Content Management**.
2. From the Type filter, select **Panel**.
3. Click the name of the panel, **workbench_context_computer_inventory**.
4. Edit something, such as a token.

The search that is tied to this workbench panel is defined as follows:

```
<panel>
  <table>
    <search>
      <query>| tstats latest(_time) as _time, latest("All_Inventory.OS.os") as os,
latest("All_Inventory.vendor_product") as vendor_product from datamodel="Compute_Inventory"."All_Inventory"
where nodename="All_Inventory.OS" ($inventory_asset_dest_filter$ OR $inventory_identity_user_filter$) by
"All_Inventory.dest" | head 10000 | `drop_dm_object_name("All_Inventory")` | fields _time, dest, os,
vendor_product</query>
    </search>
    <option name="drilldown">cell</option>
    <option name="wrap">false</option>
  </table>
```

```
</panel>
```

You can stack multiple tables or other visualizations inside of the `<panel>` tags. See panel in the Splunk Enterprise *Dashboards and Visualizations*.

Create a workbench panel from a prebuilt panel

This step is only required if you create a prebuilt panel in the first step. If you edit an existing prebuilt panel in the first step, then you skip this step.

See Create or modify a panel for the investigation workbench.

Create a workflow action

Create a workflow action that references the workbench panel. This example starts after editing the existing prebuilt panel of **workbench_context_computer_inventory** as the first step. However, if you create a new prebuilt panel and a new workbench panel, then you can create a workflow action for your workbench panel.

From the Splunk Enterprise menu bar, perform the following steps:

1. Go to **Settings** > **Fields** > **Workflow Actions**.
2. Click **New Workflow Action**.
3. Type the following in the corresponding fields:
    1. **Name**: Use a general name that is saved in workflow_actions.conf, for example, **`workbench_computer_inventory`**.
    2. **Label**: Use a token in the format of $tokenname$, such as the "dest" field in the notable event. Also append the string "inventory" after the token. For example, **`$dest$ Inventory`**.
    3. **Apply only to the following fields**: Use an asterisk to apply this to all the fields, for example **`*`**.
    4. **Show action in**: For displaying in Incident Review, use **`Fields menus`**.
    5. **URI**: Use the name of the prebuilt-panel that you created or edited, for example, panel=workbench_context_computer_inventory:
       ```
       /app/$@namespace$/ess_workbench_panel?type_asset=$@field_value$&panel=workbench_context_computer
       _inventory&drilldown_field=$@field_name$&use_drilldown_time=true
       ```
4. Click **Save**.

The URI is composed of a few special tokens and query parameters:

```
/app/$@namespace$/ess_workbench_panel?type_asset=$@field_value$&panel=workbench
_context_computer_inventory&drilldown_field=$@field_name$&use_drilldown_time=true
```

Tokens:

Token	Meaning
$@namespace$	This is the namespace of the app (such as SplunkEnterpriseSecuritySuite)
$@field_value$	This is the value of the field you selected from the workflow action, and is the value set to either type_asset, type_file, type_identity, type_url
$@field_name$	This is the name of the field you selected from the workflow action, and is the value set to drilldown_field for proper telemetry reporting. Has no impact on functionality otherwise.

Parameters:

	Optional	Meaning

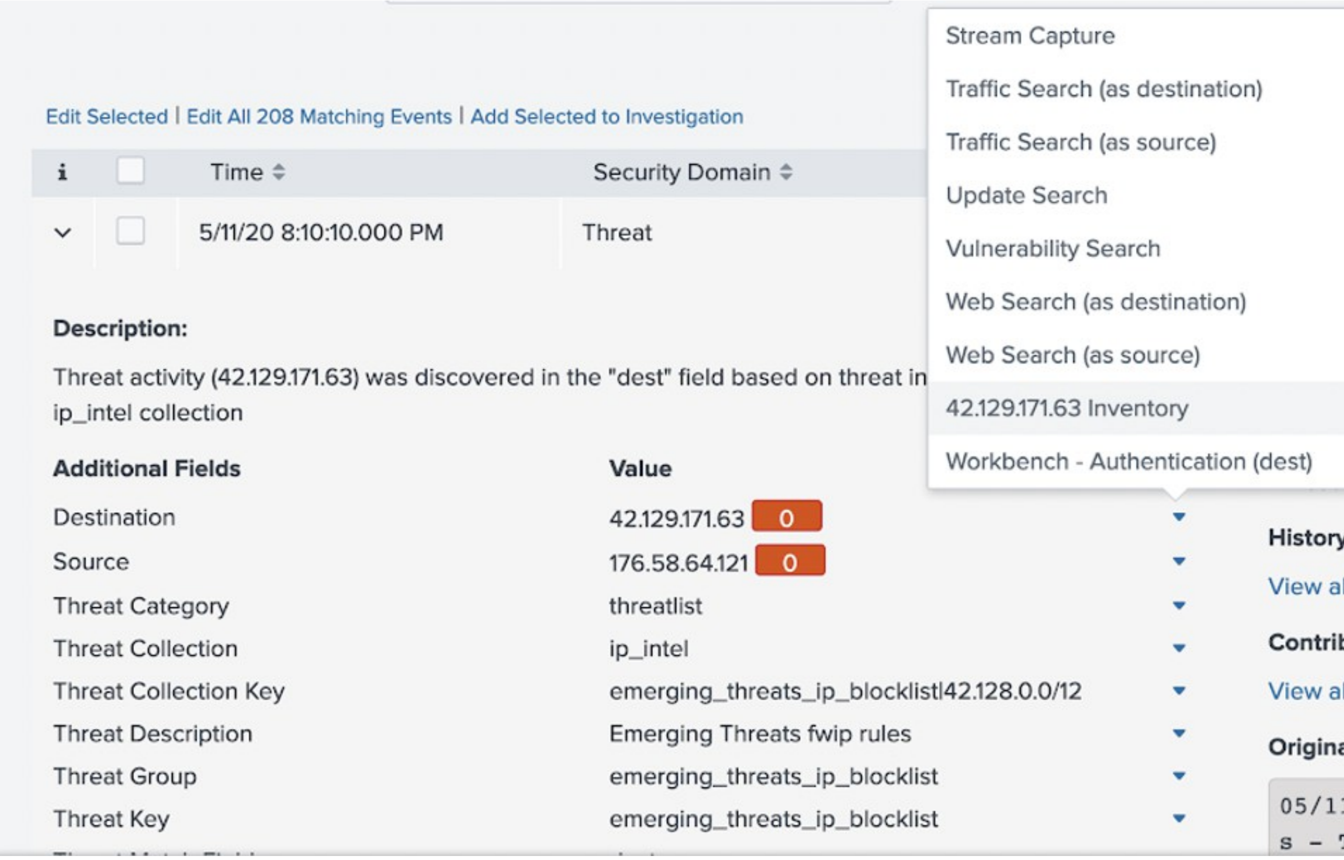
URL query parameter		
type_asset, type_file, type_identity, type_url	Optional, but most panels won't work	Query parameter to pass artifacts; it can also be used/defined multiple times in order to hand over multiple artifacts. Example: ?type_asset=127.0.0.1&type_asset=localhost&type_identity=admin
panel	required	Set this to the name of the workbench panel you created. See Create a workflow action.
use_drilldown_time	Optional	This defines if on Incident Review the time range defined by the notable event drilldown should be used. Otherwise earliest and latest will be used.
drilldown_field	Optional	This is being used for telemetry and indicates on which event field the workflow action is being invoked.
earliest	Optional	Timerange to be used for the panel, unless use_drilldown_time is set to true and the workflow action is being called on Incident Review, won't affect the search page.
latest	Optional	Timerange to be used for the panel, unless use_drilldown_time is set to true and the workflow action is being called on Incident Review, won't affect the search page.

For further details about tokens, see Token usage in dashboards in Splunk Enterprise *Dashboards and Visualizations*.

Click on the workflow field action in Incident Review

From the Enterprise Security menu bar, perform the following steps:

1. Go to **Incident Review**.
2. From a notable event that contains a **Destination** (dest) value:
   1. Click the info drop-down menu to view the event details.
   2. Click the new workflow in the destination field actions menu, complete with token substitution, such as **42.129.171.63 Inventory**.


Stream Capture
Traffic Search (as destination)
Traffic Search (as source)
Update Search
Vulnerability Search
Web Search (as destination)
Web Search (as source)
42.129.171.63 Inventory
Workbench - Authentication (dest)
Edit Selected | Edit All 208 Matching Events | Add Selected to Investigation
i
Time
Security Domain
History
View a
Contrib
View a
Origina

Time	Security Domain
5/11/20 8:10:10.000 PM	Threat

Description:

Threat activity (42.129.171.63) was discovered in the "dest" field based on threat in
ip_intel collection

Additional Fields	Value
Destination	42.129.171.63 0
Source	176.58.64.121 0
Threat Category	threatlist
Threat Collection	ip_intel
Threat Collection Key	emerging_threats_ip_blocklist|42.128.0.0/12
Threat Description	Emerging Threats fwip rules
Threat Group	emerging_threats_ip_blocklist
Threat Key	emerging_threats_ip_blocklist

```
05/1
s - 
```

View the embedded workbench

The embedded workbench pops up with the token passed into it for the artifact. This is the `dest` field value that you specified when creating the workflow action.

From here, you can drill-down into the data and investigate, without going back to the Enterprise Security menu bar and navigating to Incident Review. See Investigations in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

You can also use the embedded workbench with an existing default panel. See Example of using the embedded workbench in *Use Splunk Enterprise Security*.

Correlation Searches

Correlation search overview for Splunk Enterprise Security

A **correlation search** scans multiple data sources for defined patterns. When the search finds a pattern, it performs an **adaptive response action**.

Correlation searches can search many types of data sources, including events from any security domain (access, identity, endpoint, network), asset lists, identity lists, threat intelligence, and other data in Splunk platform. The searches then aggregate the results of an initial search with functions in SPL, and take action in response to events that match the search conditions with an adaptive response action.

- To create a correlation search, see Create a correlation search in *Splunk Enterprise Security Tutorials*.
- To set up or modify correlation searches in your environment, see Configuring correlation searches.

Examples of correlation searches

- Identify an access attempt from an expired account by correlating a list of identities and an attempt to authenticate into a host or device.
- Identify a high number of hosts with a specific malware infection, or a single host with a high number of malware infections by correlating an asset list with events from an endpoint protection system.
- Identify a pattern of high numbers of authentication failures on a single host, followed by a successful authentication by correlating a list of identities and attempts to authenticate into a host or device. Then, apply a threshold in the search to count the number of authentication attempts.

Create correlation searches in Splunk Enterprise Security

You can create your own correlation searches to create notable events, modify risk scores, and perform other adaptive response actions automatically based on a correlation in events. There are two ways to create correlation searches in Splunk Enterprise Security.

- Create a correlation search manually if you are an expert with SPL. You can review the included correlation searches for examples of the search methodology and available options. Test your correlation search ideas on the **Search** page before implementing them.
- For more assistance with the syntax of correlation searches, use the guided search creation wizard to create a correlation search. The guided search creation wizard allows you to create a correlation search that uses data models or lookups as the data source. The wizard takes your choices about the data source, time range, filtering, aggregate functions, split-by fields, and other conditions and builds the syntax of the search for you. See Create a correlation search in *Splunk Enterprise Security Tutorials* for a step-by-step tutorial of creating a correlation search.

For details about how to make sure that additional fields appear in the notable event details for a custom correlation search, see Change notable event fields.

See also

- Configure correlation searches in Splunk Enterprise Security
- List correlation searches in Splunk Enterprise Security

Configure correlation searches in Splunk Enterprise Security

Configure correlation searches to enable or disable them, update the settings associated with how they run, change the search logic, and throttle their resulting adaptive response actions. See Correlation search overview for Splunk Enterprise Security to learn more about **correlation searches**.

Enable correlation searches

Enable **correlation searches** to start running **adaptive response actions** and receiving **notable events**. Splunk Enterprise Security installs with all correlation searches disabled so that you can choose the searches that are most relevant to your security use cases.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. Filter the **Content Management** page by a **Type** of **Correlation Search** to view only correlation searches.
3. Review the names and descriptions of the correlation searches to determine which ones to enable to support your security use cases.
   For example, if compromised accounts are a concern, consider enabling the **Concurrent Login Attempts Detected** and **Brute Force Access Behavior Detected** correlation searches.
4. In the **Actions** column, click **Enable** to enable the searches that you want to enable.

Only enable correlation searches that you use. For example, don't enable Untriaged Notable Events in an unattended production environment.

After you enable correlation searches, dashboards start to display notable events, risk scores, and other data.

Change correlation search scheduling

Change the default search type of a correlation search from real-time to scheduled. Splunk Enterprise Security uses indexed real-time searches by default.

1. From the **Content Management** page, locate the correlation search you want to change.
2. In the **Actions** column, click **Change to scheduled**.

After changing a search to be scheduled, you can modify the schedule settings of the search.

1. From the **Content Management** page, click the name of the correlation search you want to change.
2. (Optional) Modify the search schedule.
   Correlation searches can run with a real-time or continuous schedule. Use a real-time schedule to prioritize current data and performance. Searches with a real-time schedule are skipped if the search cannot be run at the scheduled time. Searches with a real-time schedule do not backfill gaps in data that occur if the search is skipped. Use a continuous schedule to prioritize data completion, as searches with a continuous schedule are never skipped.
3. (Optional) Modify the cron schedule to control how frequently the search runs.
4. (Optional) Specify a schedule window for the search. Type **0** to not use a schedule window, type **auto** to use the automatic schedule window set by the scheduler, or type a number that corresponds with the number of minutes that you want the schedule window to last.
   When there are many scheduled reports set to run at the same time, specify a schedule window to allow the search scheduler to delay running this search in favor of higher-priority searches.
5. (Optional) Specify a schedule priority for the search. Change the default to **Higher** or **Highest** depending on how important it is that this search runs, and that it runs at a specific time.
   The schedule priority setting overrides the schedule window setting, so you do not need to set both.

If you manually convert a real-time search to a scheduled search, this does not automatically adjust the earliest or latest dispatch times. The time range default remains the same as the original real-time search, such as **-5m@m ~ +5m@m** which does discard events based on the extracted time being slightly in the future versus in the past. You will also need to evaluate the syntax of the converted search. This is because **| datamodel** is in use for real-time searches. However, if you are moving to a scheduled search, you can use **| tstats** for efficiency. If you use guided mode to convert the search, it can automatically switch the syntax from **| datamodel** to **| tstats** for you.

For information on search schedule priority, see the Splunk platform documentation.

- For tstats syntax, see Tstats in the Splunk Enterprise *Search Reference* .
- For Splunk Enterprise, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Enterprise *Reporting Manual*.
- For Splunk Cloud, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Cloud *Reporting Manual*.

Edit a correlation search

You can make changes to correlation searches to fit your environment. For example, modify the thresholds used in the search, change the response actions that result from a successful correlation, or change how often the search runs. Modifying a correlation search does not affect existing notable events.

1. From the **Content Management** page, locate the correlation search you want to edit.
2. Click the name of a correlation search on the **Content Management** page to edit it.
3. Modify the parameters of the search, then click **Save**.

If you modify the start time and end time for the correlation search, use **relative time modifiers**. See Specify time modifiers in your search in the Splunk Enterprise *Search Manual*.

Edit the correlation search in guided mode

You can edit some correlation searches in guided mode. Not all correlation searches support guided search editing. If a search appears grayed-out and has the option to **Edit search in guided mode**, the search was built in guided mode and can be edited in guided mode. If a search can be edited in the search box, you cannot edit it in guided mode. Attempting to switch to guided mode overwrites your existing search with a new search.

1. Click **Edit search in guided mode** to open the guided search creation wizard.
2. Review the search elements in the correlation search, making changes if you want.
3. Save the search.

Use security framework annotations in correlation searches

Use annotations to enrich your correlation search results with security framework mappings. You also see these annotations as field labels in Incident Review and Risk Analysis.

1. Select **Configure > Content > Content Management**.
2. Click the title of the correlation search you want to edit.
3. You can use annotations for industry-standard mappings or unmanaged annotations for custom mappings.

The annotations are stored in `action.correlationsearch.annotations` in JSON format in the savedsearches.conf file. MITRE ATT&CK definitions are pre-populated in the security_framework_annotations.csv file. You don't need to revise this unless you want to display non-default info in the annotations dropdown field.

When annotated, the correlation searches do not automatically display in the use case library for use with the Framework Mapping filter. To add correlation searches to analytic stories, see Edit or add Analytic Story details.

Annotations

Use annotations to enrich your correlation search results with the context from industry-standard mappings.

1. Scroll to **Annotations**.
2. Add annotations for the common framework names listed. These fields are for use with industry-standard mappings, but also allow custom values. Industry-standard mappings include values such as the following:

Security Framework	Five Random Mapping Examples
CIS 20	CIS 3, CIS 9, CIS 11, CIS 7, CIS 12
Kill Chain	Reconnaissance, Actions on Objectives, Exploitation, Delivery, Lateral Movement
MITRE ATT&CK	T1015, T1138, T1084, T1068, T1085 This field also contains mitre technique IDs for you to select from the **mitre_attack_lookup** lookup definition.
NIST	PR.IP, PR.PT, PR.AC, PR.DS, DE.AE

3. Click **Save**.

Consider MITRE ATT&CK annotations as an example. At search time, the **mitre_attack_enrichment** automatic lookup uses the mitre technique id that you selected, and it outputs additional industry-standard context as event fields. Some examples include, but are not limited to, the following: `annotations.mitre_attack.mitre_description`, `annotations.mitre_attack.mitre_detection`, `annotations.mitre_attack.mitre_software_name`, `annotations.mitre_attack.mitre_software_platform`, `annotations.mitre_attack.mitre_tactic`, `annotations.mitre_attack.mitre_technique`, `annotations.mitre_attack.mitre_technique_id`, `annotations.mitre_attack.mitre_url`.

Search your MITRE ATT&CK intelligence download data to verify the annotation details as follows:

```
| inputintelligence mitre_attack
```

Unmanaged Annotations

Unmanaged annotations won't be enriched with any industry-standard context.

1. Scroll to **Unmanaged Annotations**.
2. Click **+ Framework** to add your own framework names and their mapping categories. These are free-form fields.
3. Click **Save**.

Consider an unmanaged annotation as an example. In your events, you will see `annotations.<unmanaged_framework_name>=<unmanaged_tactic_id_value>`.

Add additional security frameworks to your annotations

While the MITRE ATT&CK framework annotations are available by default, you can also add other industry-standard frameworks. You can add them from scratch, but clone the existing mitre_attack for convenience.

Add the intelligence download by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Data inputs > Intelligence Downloads**.
2. Filter on **mitre**.
3. Click the **Clone** action for **mitre_attack**.
4. Type a name for the industry-standard framework.
5. Revise the description.
6. Leave **Is Threat Intelligence** unchecked.
7. Revise the type.
8. Revise the URL.
9. Click **Save**.

Add the lookup definition by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Lookups > Lookup definitions**.
2. Filter on **mitre**.
3. Click the **Clone** action for **mitre_attack_lookup**.
4. Leave **Type** as-is.
5. Type a name for the industry-standard framework.
6. Revise the **Supported fields**.
7. Click **Save**.

Add the automatic lookup by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Lookups > Automatic lookups**.
2. Filter on **mitre**.
3. Click the **Clone** action for **source::...- Rule : LOOKUP-mitre_attack_enrichment**.
4. Leave **Destination app** as-is.
5. Leave **Apply to** as-is. The named* **source::...- Rule** is necessary.
6. Type a name for the industry-standard framework.
7. Revise all the fields.
8. Click **Save**.

Define trigger conditions for adaptive response actions generated by a correlation search

You can modify the conditions that control when an adaptive response action is generated by a correlation search. Throttling is different from defining trigger conditions and happens after search results meet the trigger conditions. When you define trigger conditions, the correlation search results are evaluated to check if they match the conditions. If the search results match the conditions, throttling rules control whether an adaptive response action is generated.

You can set up trigger conditions to generate response actions per-result, based on the number of results returned by the correlation search, based on the number of hosts, number of sources, or based on custom criteria. For custom criteria, type a custom search string to create a condition. Trigger conditions act as a secondary search against the results of the correlation search.

For information on trigger conditions and configuring those conditions for a search, see the Splunk platform documentation.

- For Splunk Enterprise, see Configure alert trigger conditions in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud, see Configure alert trigger conditions in the Splunk Cloud *Alerting Manual*.

Throttle the number of response actions generated by a correlation search

Set up throttling to limit the number of response actions generated by a correlation search. When a correlation search matches an event, it triggers a response action.

By default, every result returned by the correlation search generates a response action. Typically, you may only want one alert of a certain type. You can use throttling to prevent a correlation search from creating more than one alert within a set period. To change the types of results that generate a response action, define trigger conditions. Some response actions allow you to specify a maximum number of results in addition to throttling. See Set up adaptive response actions in Splunk Enterprise Security.

1. Select **Configure** > **Content** > **Content Management**.
2. Click the title of the correlation search you want to edit.
3. Type a **Window duration**. During this window, any additional event that matches any of the **Fields to group by** will not create a new alert. After the window ends, the next matching event will create a new alert and apply the throttle conditions again.
4. Type the **Fields to group by** to specify which fields to use when matching similar events. If a field listed here matches a generated alert, the correlation search will not create a new alert. You can define multiple fields. Available fields depend on the search fields that the correlation search returns.
5. Save the correlation search.

Throttling applies to any type of correlation search response action and occurs before notable event suppression. See Create and manage notable event suppressions for more on notable event suppression.

If you have throttling set for an existing adaptive response action, such as a notable event alarm, editing the details of the alarm causes the throttling to be disregarded. The change to the alarm causes the throttle file, which notes how long to ignore events, to get removed. Therefore the throttling does not occur again until the next event is triggered.

Clone a correlation search

You can clone correlation searches to create your own, rather than starting from scratch.

1. From the Splunk ES menu bar, select **Configure** > **Content** > **Content Management**.
2. Filter the **Content Management** page by a **Type** of **Correlation Search** to view only correlation searches.
3. Scroll to find the name of the correlation search to clone.
4. In the Actions column of the correlation search, click **Clone**.
5. Type a unique name for the New Search Label. This field is case sensitive, so a name of **Account Deleted CLONE** is different than **Account Deleted Clone**.
6. (Optional) Chose an App from the drop-down list.
7. Click **Save**.
8. To edit the cloned correlation search immediately, click the link in the success message pop-up window. Alternately, you can close the pop-up window and edit the clone later.
9. Your cloned correlation search appears in **Content > Content Management** within a few minutes. The status is disabled by default.
10. Click **Enable** when you're ready to use it.

See also

- List correlation searches in Splunk Enterprise Security
- Set up adaptive response actions in Splunk Enterprise Security

List correlation searches in Splunk Enterprise Security

To obtain a list of correlation searches enabled in Splunk Enterprise Security, use a REST search to extract the information that you want in a table.

For example, create a table with the app, security domain, name, and description of all correlation searches in your environment.

```
| rest splunk_server=local count=0 /services/saved/searches | where
match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") | rename eai:acl.app as app, title as
csearch_name, action.correlationsearch.label as csearch_label, action.notable.param.security_domain as
security_domain | table csearch_name, csearch_label, app, security_domain, description
```

As another example, create a table with only the enabled correlation searches and the adaptive response actions associated with those searches in your environment. To see the adaptive response actions for all correlation searches, remove `| where disabled=0`.

```
| rest splunk_server=local count=0 /servicesNS/-/SplunkEnterpriseSecuritySuite/saved/searches | where
match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") | where disabled=0 | eval
actions=split(actions, ",") | table title,actions
```

Upgrade correlation searches in Splunk Enterprise Security

Starting in Splunk Enterprise Security version 4.6.0, `correlationsearches.conf` is no longer used to define correlation searches. Instead, `savedsearches.conf` uniquely identifies correlation searches using the `action.correlationsearch.enabled=1` parameter. The `correlationsearches.conf` file is deprecated.

Changes Splunk Enterprise Security makes at upgrade

When you upgrade to Splunk Enterprise Security 4.6.0, Splunk Enterprise Security migrates all correlation searches in your environment from `correlationsearches.conf` to `savedsearches.conf` using the `confcheck_es_correlationmigration.py` script. The migration can take up to five minutes to complete after the upgrade. In a search head cluster, the captain performs the migration.

During the upgrade, Splunk Enterprise Security continues to create notable events without interruption. This change does not prevent or delay notable events from appearing on Incident Review because the `Threat - Correlation Searches - Lookup Gen` saved search continues to use the contents of both `correlationsearches.conf` and `savedsearches.conf` to populate the `correlationsearches` KV Store collection used by Incident Review.

Changes you have to make after upgrade

After upgrading to Splunk Enterprise Security 4.6.0 or later, you have to make additional changes.

- Check `correlationsearches.conf` for search definitions that would indicate that a search did not migrate successfully. Migrated searches only exist in `savedsearches.conf`. If a search did not get migrated, migrate the `correlationsearches.conf` entries manually to `savedsearches.conf` using the parameter definitions below.
- Update searches that call the `correlationsearches` REST endpoint.
    - ♦ For example, a search that displays a list of correlation searches in your environment would change from

      ```
      | rest splunk_server=local /services/alerts/correlationsearches | rename eai:acl.app as app,
      title as csearch_name | table app security_domain csearch_name description
      ```

to

```
| rest splunk_server=local count=0 /services/saved/searches | where
match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") | rename eai:acl.app as
app, title as csearch_name, action.correlationsearch.label as csearch_label,
action.notable.param.security_domain as security_domain | table csearch_name, csearch_label,
app, security_domain, description
```

- See List correlation searches in Splunk Enterprise Security for more examples of updated searches.

Custom search macros that reference the `correlationsearches` KV Store collection continue to work as before, but consider updating them anyway.

`correlationsearches.conf` *parameter translation to* *`savedsearches.conf`*

All `correlationsearches.conf` parameters now exist in `savedsearches.conf` and the `correlationsearches.conf` file has been deprecated. Do not update it directly except to manually migrate correlation search definitions.

Identification parameters for correlation searches

New parameters identify whether a saved search is a correlation search and the name of the correlation search.

`correlationsearches.conf` parameter in pre-4.6.0 versions	`savedsearches.conf` parameter starting in 4.6.0	Notes
N/A	`action.correlationsearch=0`	This is an internal parameter and can be ignored.
A stanza for the search exists	`action.correlationsearch.enabled=1`	This parameter identifies a saved search as a correlation search.
`rule_name`	`action.correlationsearch.label`	This parameter provides the name of the correlation search.
`description`	`description`	This parameter provides the description of the correlation search.

Notable event parameters for correlation searches

The `action.notable` parameter identifies a notable event associated with a correlation search. The parameters that describe additional details associated with the notable event now exist in the `savedsearches.conf` file.

`correlationsearches.conf` parameter in pre-4.6.0 versions	`savedsearches.conf` parameter starting in 4.6.0
`security_domain`	`action.notable.param.security_domain`
`severity`	`action.notable.param.severity`
`rule_title`	`action.notable.param.rule_title`
`rule_description`	`action.notable.param.rule_description`
`nes_fields`	`action.notable.param.nes_fields`
`drilldown_name`	`action.notable.param.drilldown_name`
`drilldown_search`	`action.notable.param.drilldown_search`
`default_status`	`action.notable.param.default_status`

`correlationsearches.conf` parameter in pre-4.6.0 versions	`savedsearches.conf` parameter starting in 4.6.0
`default_owner`	`action.notable.param.default_owner`

Related search parameters for correlation searches

Searches related to a correlation search, such as the context-generating searches associated with a correlation search that uses extreme search, are now part of a JSON blob `action.correlationsearch.related_searches` parameter.

`correlationsearches.conf` parameter in pre-4.6.0 versions	`savedsearches.conf` parameter starting in 4.6.0

related_search_name = Endpoint - Emails By Source - Context Gen
related_search_name.0 = Endpoint - Emails By Destination Count - Context Gen
	`action.correlationsearch.related_searches = [\`
	`    "Endpoint - Emails By Source - Context Gen",\`
	`    "Endpoint - Emails By Destination Count - Context Gen"\`
	`]`

Example correlation search stanzas from this version and previous versions

The `savedsearches.conf` stanza for a correlation search looks as follows starting in 4.6.0.

```
[Access - Concurrent App Accesses - Rule]
action.correlationsearch = 0
action.correlationsearch.enabled = 1
action.correlationsearch.label = Concurrent Login Attempts Detected
action.email.sendresults = 0
action.notable = 0
action.notable.param.security_domain = access
action.notable.param.severity = medium
action.notable.param.rule_title = Concurrent Access Event Detected For $user$
action.notable.param.rule_description = Concurrent access attempts to $app1$ by $user$ from two different
sources( $src1$, $src2$ ) have been detected.
action.notable.param.nes_fields = user
action.notable.param.drilldown_name = View access attemps by $user$
action.notable.param.drilldown_search = | datamodel Authentication Authentication search | search
Authentication.user="$user$"
action.risk = 1
action.risk.param._risk_object = user
action.risk.param._risk_object_type = user
action.risk.param._risk_score = 20
alert.suppress = 1
alert.suppress.fields = user
alert.suppress.period = 86300s
alert.track = false
cron_schedule = 10 * * * *
description = Alerts on concurrent access attempts to an app from different hosts. These are good indicators
of shared passwords and potential misuse.
disabled = True
dispatch.earliest_time = -70m@m
dispatch.latest_time = -5m@m
enableSched = 1
is_visible = false
request.ui_dispatch_app = SplunkEnterpriseSecuritySuite
search = | tstats `summariesonly` count from datamodel=Authentication.Authentication by
_time,Authentication.app,Authentication.src,Authentication.user span=1s |
`drop_dm_object_name("Authentication")` | eventstats dc(src) as src_count by app,user | search src_count>1
| sort 0 + _time | streamstats current=t window=2 earliest(_time) as previous_time,earliest(src) as
previous_src by app,user | where (src!=previous_src) | eval time_diff=abs(_time-previous_time) | where
```

```
time_diff<300
```

In previous versions of Splunk Enterprise Security, the `savedsearches.conf` and `correlationsearches.conf` definitions for the same correlation search would look as follows. `savedsearches.conf`

```
[Access - Concurrent App Accesses - Rule]
action.email.sendresults            = 0
action.risk                         = 1
action.risk.param._risk_object      = user
action.risk.param._risk_object_type = user
action.risk.param._risk_score       = 20
alert.suppress                      = 1
alert.suppress.fields               = user
alert.suppress.period               = 86300s
alert.track                         = false
cron_schedule                       = 10 * * * *
disabled                            = True
dispatch.earliest_time              = -70m@m
dispatch.latest_time                = -5m@m
enableSched                         = 1
is_visible                          = false
request.ui_dispatch_app             = SplunkEnterpriseSecuritySuite
search                              = | tstats `summariesonly` count from
datamodel=Authentication.Authentication by _time,Authentication.app,Authentication.src,Authentication.user
span=1s | `drop_dm_object_name("Authentication")` | eventstats dc(src) as src_count by app,user | search
src_count>1 | sort 0 + _time | streamstats current=t window=2 earliest(_time) as
previous_time,earliest(src) as previous_src by app,user | where (src!=previous_src) | eval
time_diff=abs(_time-previous_time) | where time_diff<300
correlationsearches.conf
```

```
[Access - Concurrent App Accesses - Rule]
security_domain     = access
severity            = medium
rule_name           = Concurrent Login Attempts Detected
description         = Alerts on concurrent access attempts to an app from different hosts. These are good
indicators of shared passwords and potential misuse.
rule_title          = Concurrent Access Event Detected For $user$
rule_description    = Concurrent access attempts to $app1$ by $user$ from two different sources( $src1$,
$src2$ ) have been detected.
nes_fields          = user
drilldown_name      = View access attemps by $user$
drilldown_search    = | datamodel Authentication Authentication search | search
Authentication.user="$user$"
default_owner       =
default_status      =
```

Create sequence templates in Splunk Enterprise Security

The Event Sequencing Engine provides capabilities for threat detection that allow you to group correlation searches into batches of events, either in a specific sequence, by specific attributes, or both.

You create batches of events by defining a workflow to run correlation searches in an order of your choice, specifying what notable events would need to occur in order to advance to the next step.

The concept is similar to writing a script to automate the things that you might otherwise have to do manually when tracking a variety of notable events and variables through a variety of correlation searches. The concept is also similar to that of meta notable events or named multi-vector notables, which are alerts that are generated by correlation searches monitoring for multiple specific conditions prior to raising the alert.

How sequence templates work

The Event Sequencing Engine runs as a real-time search and listens for incoming notable events and risk modifiers that are triggered by correlation searches. Security analysts can provide specifications on how sequenced events are constructed by using sequence templates. Once you have created a sequence template, it is available for execution within 5 minutes.

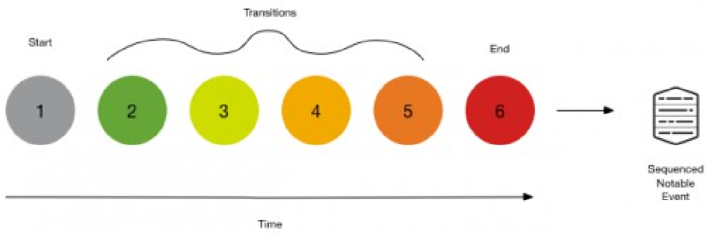
Sequence templates are stored in the `sequence_templates.conf` file.

The Event Sequencing Engine periodically stores information regarding the currently running sequence templates. This information can be viewed from the sequence lister page. See the status of a template.

Sequence template details

A sequence template defines the various constraints of constructing a sequence. It has three main components: start, transitions, and end. You can construct a sequence template using the editor.

The following diagram shows an example of the way that you can start with one correlation search (1), flow through any number of correlation searches in the transitions (2 through 5), and end with a final search (6).



Start

The start section defines match conditions for starting the execution of a template. Optionally, the start section can define state variables to store field values for the purpose of matching further notables or risk modifiers. State variables can also be used as outputs in the final sequenced event. Once the start condition is met, the event sequencing engine will start the execution of the corresponding sequence template.

Match conditions

The match condition defines the criteria for considering notable events or risk modifiers for transitioning through the phases in a template. The match condition has two parts that are evaluated successively, correlation search and expression.

Match Conditions	Description
Correlation Search	The correlation search to match the source of the incoming notable or risk modifier. Wildcard matching (*) is supported on this field.
Expression	The expression allows you to compare any field from an incoming event with a static value or a state variable (see state for further information). Expressions follow Splunk style syntax in the format of `<field> <comparator> <value>`. Note that while similar to SPL syntax, expressions in the event sequencing engine are more restricted

Match Conditions	Description

	than in standard SPL syntax. For example, SPL doesn't enforce AND/OR operators for field searches, but the event sequencing engine does. Wildcard matching (*) and regular expressions are not supported in the expression section.
	You can also use brackets for grouping. You must use the logical operators of AND or OR in your grouping, such as: `'host' = "127.0.0.1" AND ('dest' = "example.com" OR 'dest'="example.org").` The NOT operator is not supported.
	The expression is made up of field, comparison function, and value.
	Field
	The name of any SPL field in single quotes, such as: `'host'`, `'source'`, `'sourcetype'`, etc. Multivalue fields are supported, and an event is considered a match as long as one value matches.
	Comparison function
	The comparison function can be any of the following: =, !=, >, <, >=, <=.
	The following comparison functions force numeric comparisons: >=, <=, >, <.
	Value
	The field value in double quotes, which can be in string format or in state_variable notation, such as: `'host' = "127.0.0.1"` or `'host' = "$host$"`.
	Based on an example event in .csv format such as the following:
	`host, source, sourcetype`
	`127.0.0.1, "Threat Detected", "nginx"`
	• An expression for matching on the host is `'host' = "127.0.0.1"`.
	• An expression for matching on any other source is `'source' != "Threat Detected"`.
	If you want to use assets and identities in expressions, configure asset and identity correlation with the **enable for all sourcetypes** option selected. This makes sure that identity and asset information is enriched during search time when receiving contents from the risk or notable index. See Configure asset and identity correlation in Splunk Enterprise Security.

State

The state provides a way to store values from matched events for the lifetime of a sequence. State can be stored at the start section and at each transition if the enforce ordering check box is unchecked. You cannot save a new state at the end step. These values can then be used for matching expressions in consecutive transitions. State can also be an output in the final sequenced event. If a multivalue is the output in the final sequenced event, it will be returned in a comma separated format. Once stored, state variables can be referenced using `$variable_name$` syntax. State allows you to store important pieces of information for future matching. The state contains two parts, the field and the label.

State	Description
Field	The name of any SPL field that you want to capture for later use. State fields defined in the start section can be used in all transitions. But state fields defined in the transitions section will be available only to expressions in subsequent transitions.
Label	The label is the variable name for referring to the state field in a later search. The state_variable notation for referring to the label is similar to an SPL token in the way it is used to capture and pass values. The label is available only for use while the template is running. It does not persist when the template terminates or completes. The label cannot contain a dollar sign ($).

Transitions

The transitions section defines the sequence, either chronologically or in an order-independent way. You can define a series of match conditions to find the sequence. Each transition defines a title and a match condition.

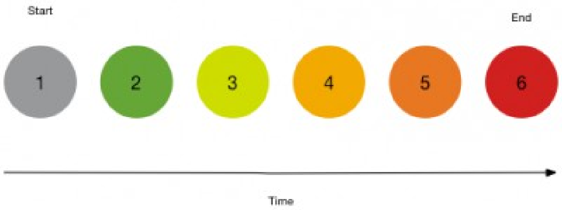
Chronological

Transitions are matched chronologically by default. With the **enforce order** check box checked, the Event Sequencing Engine will check if notable events or risk modifiers match the completed transitions in the order specified. A transition is completed by matching an incoming event with a match condition. Given a sequence of correlation searches in the following order, with the **enforce order** check box checked for example, the notable events will be matched in order:

Start
1. Brute Force Access Behavior Detected

Transitions
2. Uncommon Processes On Endpoint
3. Unusually Long Command Line
4. Suspicious Reg.exe Process
5. Web Uploads to Non-corporate Sites by Users

End
6. Abnormally High Number of Endpoint Changes By User



Transitions can only define state variables if the **enforce order** check box is checked. Enforcing the order provides a way to chronologically build a sequence. A state stored in an earlier transition is available for matching in later ones.

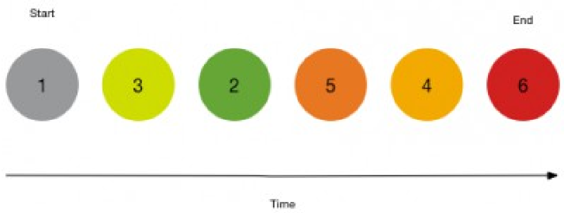
Not chronological

You can turn off chronological matching by unchecking the enforce order checkbox. With enforce order unchecked, the Event Sequencing Engine will check if notable events or risk modifiers match any of the incomplete transitions. Once matched, corresponding transitions will be considered complete. The order of events will not be considered. For example, given a sequence of correlation searches with the enforce order check box unchecked, you'll notice that notable events can match in any order:

Start
1. Brute Force Access Behavior Detected

Transitions
3. Unusually Long Command Line
2. Uncommon Processes On Endpoint
5. Web Uploads to Non-corporate Sites by Users
4. Suspicious Reg.exe Process

End
6. Abnormally High Number of Endpoint Changes By User



Wildcard

Transitions also support the same constructs for match conditions as in the start section. Since the correlation search field in the match condition allows wildcard match, it is possible to construct sequences that require forks. Transitions can define more than one next possible notable event or risk modifier. Given a wildcard correlation search sequence, for example:

The sequence can go in the following patterns:

Start

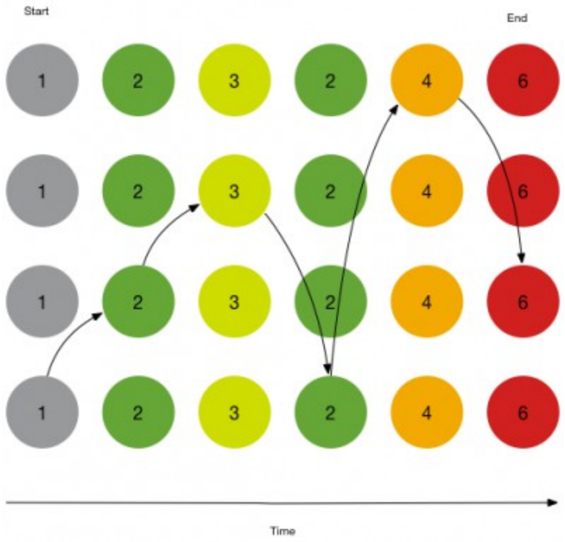
1. Brute Force Access Behavior Detected

Transitions

2. Option A or Option B, using a wildcard for two correlation searches. For example, a search of step_one or step_two by matching either one using the wildcard, such as `step*`.
4. Suspicious Reg.exe Process
5. Web Uploads to Non-corporate Sites by Users

End

6. Abnormally High Number of Endpoint Changes By User

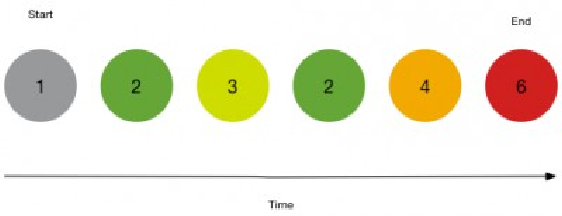


Aggregate

Transitions can also be configured to aggregate notable events or risk modifiers that may happen after a transition match is found. If the **aggregate matches** check box is checked, the Event Sequencing Engine will add any notable events or risk modifiers that satisfy the match condition for one of the completed transitions. This can be used to add more context to the final sequenced event.

Consider a sequence of correlation searches like the following, where we have one correlation search that fires multiple notable events (Uncommon Processes On Endpoint) during the lifetime of our sequence:

Start
 1. Brute Force Access Behavior Detected
Transitions
 2. Uncommon Processes On Endpoint
 3. Unusually Long Command Line
 2. Uncommon Processes On Endpoint
 4. Suspicious Reg.exe Process
End
 6. Abnormally High Number of Endpoint Changes By User



If aggregate matches is unchecked, then there will only be one match for Uncommon Processes On Endpoint in the final sequenced event, even though it matched multiple times. If **aggregate matches** is checked, the event sequencing engine will try to match all new incoming notables and risk modifiers with completed transitions. In this case, after finding the first Uncommon Processes On Endpoint, the sequencing engine re-evaluates the next two Uncommon Processes On Endpoint notable events with match conditions and adds them to the final sequenced event if true.

End

The end section defines the termination criteria for a sequence template. A template can terminate if either of these two conditions are true:

- All transitions are complete and the event satisfying match condition is found. The event sequencing engine will consider this outcome as a successful run of a template and will trigger the sequenced event creation.
- The template has reached the configured max time to live (max_ttl). As the template has not reached its end state in the desired time, the event sequencing engine will discard this run and no sequenced event will be created.

Sequenced event

After the successful termination of a template, the output is a sequenced event. This sequenced event is the result of a template run and holds the necessary information for identifying a sequence. Sequenced events are written to the `sequenced_events` index. Sequence templates can be configured to use any of the state variables or statically configured values as output in the final sequenced events. The variables are stored and available for use only during the runtime of a template.

Create a template

You can create a template to run any number of searches that match your criteria.

The sequence template does not require any special capability to view, but requires the `edit_sequence_template` capability to manage sequence templates. By default, ES assigns the `edit_sequence_template` capability to the `ess_admin` role. An admin can assign it to other roles from the Permissions setting.

In the following scenario, you know that you're interested in detecting a prohibited application spawning the cmd.exe process. Once you've detected the process, you're interested in knowing if it's happening on your favorite computer, particularly if it starts creating new local admin accounts. Finally, you want to know if the user is making an abnormally high number of changes elsewhere. Because each system involved is set for logging at a different time interval, you are not necessarily interested in chronological order.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management > Create New Content > Sequence Template**.
2. In the Sequence Template section, type a **Name** for your template, a **Description** for it, and select an **App** with which to run the search. If your template name has spaces, replace them with underscores.
3. In the Start section, add the following:
    1. Select the Correlation Search to begin with, such as **Detect Prohibited Applications Spawning cmd.exe**.
    2. Type the Expression to match on, such as `'dest' = "198.18.0.101"`
    3. Type a State to store for use in a later correlation search, such as:
        - ◊ **Field:** `user`
        - ◊ **Label:** `questionable_user`
4. In the Transition section, do the following:
    1. Uncheck the Enforce Ordering check box.
    2. Type a Title for this section, such as: `new local admin`
    3. Select the Correlation Search to run next, such as: **ESCU - Detect New Local Admin account - Rule**.
    4. Type the Expression to match on, such as the state you saved earlier: `'user' = "$questionable_user$"`.
5. In the End section, add the following:
    1. Select the Correlation Search to end with, such as **Change - Abnormally High Number of Endpoint Changes By User - Rule**.
    2. Type the Expression to match on, such as the state you saved earlier: `'user' = "$questionable_user$"`.
    3. Select the Time Limit when the search should expire, such as `2 days`.
6. In the Actions section, add the following:
    1. Type the Event Title that you want to see in the Incident Review, such as `Prohibited cmd, new local account, high endpoint changes`.
    2. Type the Description that you want to see in the Incident Review, such as `The questionable user on my favorite computer is $questionable_user$`.
    3. Select the Urgency that you want to see in the Incident Review, such as **High**.
    4. Select a Security Domain that you want to see in the Incident Review, such as **Access**.
7. Click **Save**.

Enable or Disable a template

Manage sequence templates individually by enabling or disabling each one. Enable or disable the template by performing the following steps:

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. From the Type filter, select the **Sequence Template** option.

3. Check the check box for your Sequence Template.
4. Click **Edit selection > Enable** or **Edit selection > Disable**.

Enable event sequencing

Manage sequence templates as a whole by enabling or disabling the Event Event Sequencing Engine. The sequence templates will run only if the Event Sequencing Engine is enabled. The Event Sequencing Engine is disabled by default.

Enable the Event Sequencing Engine by performing the following steps:

1. From the Splunk ES menu bar, select **Configure > General > General Settings**.
2. (Optional) Type `Event Sequencing Engine` in the filter field.
3. Click **Enable** to enable the Event Sequencing Engine.

Edit an existing template

The sequence template does not require any special capability to view, but requires `edit_sequence_template` to manage sequence templates. By default, ES assigns the `edit_sequence_template` capability to the `ess_admin` role. An admin can always assign it to other roles from the Permissions setting.

You can edit all templates, whether they're enabled or disabled.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. From the Type filter, select the **Sequence Template** option.
3. (Optional) Click **Disable** to disable an enabled template.
4. Click the name of the search to edit the template parameters.

See the status of a template

You can see which sequences are running or completed.

1. From the Splunk ES menu bar, select **Security Intelligence > Sequence Analysis**.
2. From the Showing filter, select the **Running Templates** or **Completed Templates**.
3. From the event information column, click the greater than (>) symbol to expand the display.

You can see which templates are running and their current status in terms of which events have been matched and how many transitions have been completed.

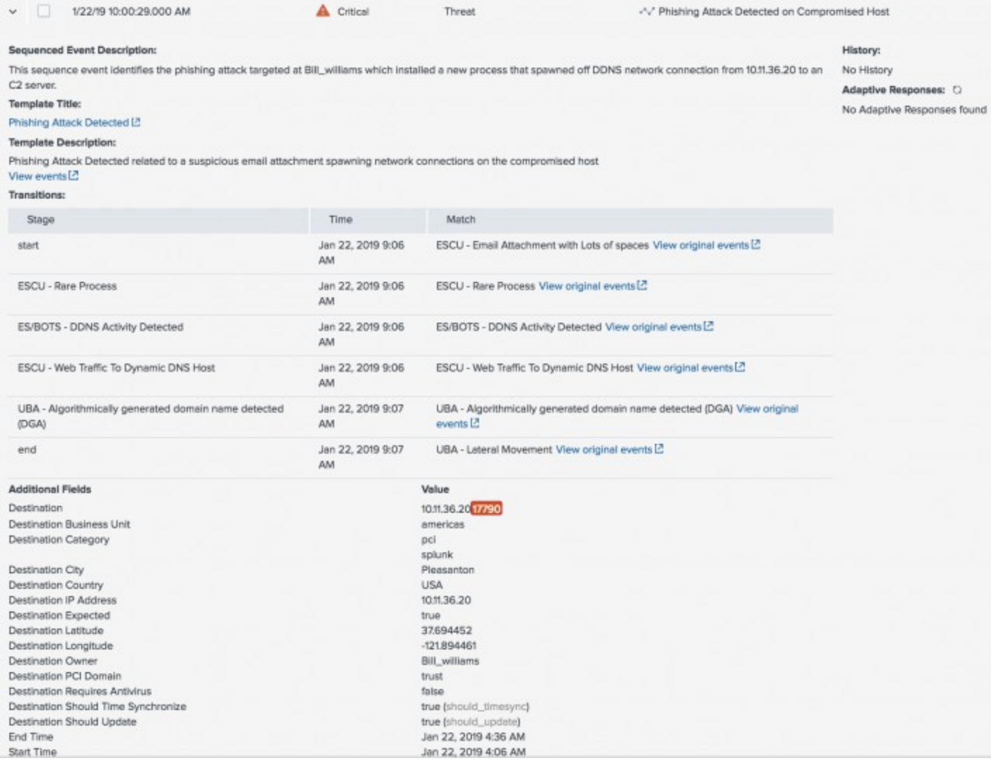
Find the sequenced events generated by the event sequence template

Once you create a sequence template and it reaches the end state, the output displays as a sequenced event in the Incident Review dashboard. See Incident Review overview for information about using the dashboard.

To find the output from the sequence template search, do the following:

1. From the Splunk ES menu bar, select **Incident Review**.
2. Click the **Sequenced Event** filter to show only sequenced events.
3. (Optional) Sort by **Title**.
4. You will see the Event Title that you typed in the editor as the title of your sequenced event.
5. From the event information column, click the greater than (>) symbol to expand the display.

ES displays information specific to that sequence of events, such as the name and description, the state of each transition in the sequence, and the sequence expiration date. For example when we see Rare Process, then DDNS Activity, then Web Traffic, then a UBA-triggered DGA alert.



1/22/19 10:00:29.000 AM Critical Threat Phishing Attack Detected on Compromised Host

Sequenced Event Description:

This sequence event identifies the phishing attack targeted at Bill_williams which installed a new process that spawned off DDNS network connection from 10.11.36.20 to an C2 server.

Template Title:

Phishing Attack Detected

Template Description:

Phishing Attack Detected related to a suspicious email attachment spawning network connections on the compromised host

View events

Transitions:

Stage	Time	Match
start	Jan 22, 2019 9:06 AM	ESCU - Email Attachment with Lots of spaces View original events
ESCU - Rare Process	Jan 22, 2019 9:06 AM	ESCU - Rare Process View original events
ES/BOTS - DDNS Activity Detected	Jan 22, 2019 9:06 AM	ES/BOTS - DDNS Activity Detected View original events
ESCU - Web Traffic To Dynamic DNS Host	Jan 22, 2019 9:06 AM	ESCU - Web Traffic To Dynamic DNS Host View original events
UBA - Algorithmically generated domain name detected (DGA)	Jan 22, 2019 9:07 AM	UBA - Algorithmically generated domain name detected (DGA) View original events
end	Jan 22, 2019 9:07 AM	UBA - Lateral Movement View original events

Additional Fields	Value
Destination	10.11.36.20 17790
Destination Business Unit	americas
Destination Category	pci splunk
Destination City	Pleasanton
Destination Country	USA
Destination IP Address	10.11.36.20
Destination Expected	true
Destination Latitude	37.694452
Destination Longitude	-121.894461
Destination Owner	Bill_williams
Destination PCI Domain	trust
Destination Requires Antivirus	false
Destination Should Time Synchronize	true (should_timesync)
Destination Should Update	true (should_update)
End Time	Jan 22, 2019 4:36 AM
Start Time	Jan 22, 2019 4:06 AM

History:

No History

Adaptive Responses:

No Adaptive Responses found

Execute the Event Sequencing Engine in an ad-hoc manner

When you create a template, the Event Sequencing Engine starts executing it within 5 minutes. Alternately, you can run the helper macro, `execute_sequence_template`. This macro takes two parameters: the template name and a Boolean expression indicating if a sequenced event is created or not. For example:

```
`execute_sequence_template(template_name, false)`
```

In this case, `false` means that the sequenced event will not be created.

This macro can be run over historical data, so you can find sequenced events in past notable events and risk modifiers. After running the macro, the Event Sequencing Engine returns sequenced events if any are found. You can only execute one template at a time. This macro is intended for explorations and fine tuning to manage sequence templates.

Set up Adaptive Response actions in Splunk Enterprise Security

Adaptive Response actions allow you to gather information or take other action in response to the results of a correlation search or the details of a notable event. Splunk Enterprise Security includes several Adaptive Response actions. See Included Adaptive Response actions.

You can add Adaptive Response actions and alert actions to correlation searches, or run Adaptive Response actions from notable events on the Incident Review dashboard. Collect information before you start your investigation to save time at triage by adding Adaptive Response actions to correlation searches. Take action at triage time by running Adaptive Response actions from the Incident Review dashboard.

The Adaptive Response actions that ship out of the box for ping, nbtstat, and nslookup are modified to support Splunk Cloud. Additional setup is required before configuring Adaptive Response actions from Splunk Cloud to on-premises infrastructure and services. See Set up an Adaptive Response relay from Splunk Cloud to an on-premises device.

Add new Adaptive Response actions

To add new Adaptive Response actions, you can install add-ons with Adaptive Response actions or create your own Adaptive Response actions. See Create an Adaptive Response action on the Splunk developer portal for information on creating Adaptive Response actions. See Deploy add-ons included with Splunk Enterprise Security in the *Install and Upgrade Manual*.

Audit Adaptive Response actions

Audit all Adaptive Response actions on the Adaptive Response Action Center.

Configure permissions for Adaptive Response actions

Restrict certain Adaptive Response actions to certain roles by adjusting the permissions for Adaptive Response actions in the alert actions manager. You can find information about the alert actions manager in the Splunk platform documentation.

- For Splunk Enterprise, see Using the alert actions manager in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud, see Using the alert actions manager in the Splunk Cloud *Alerting Manual*.

In order to run Adaptive Response actions from the Incident Review dashboard that have credentials stored in the credential manager, you must have the appropriate capability.

- For Splunk platform version 6.5.0 and later, `list_storage_passwords`.
- For earlier Splunk platform versions, `admin_all_objects`.

Add an Adaptive Response action to a correlation search

1. On the Splunk Enterprise Security menu bar, click **Configure > Content > Content Management**.
2. Click an existing correlation search, or click **Create New > Correlation Search**.
3. Click **Add New Response Action** and select the response action you want to add.
4. Complete the fields for the action. If you want, add another response action.
5. Click **Save** to save all changes to the correlation search.

For instructions on configuring each of the Adaptive Response actions included with Splunk Enterprise Security, see Configure Adaptive Response actions for a correlation search in Splunk Enterprise Security. For instructions on configuring a custom Adaptive Response action, see the documentation for the app or add-on that supplied the Adaptive Responsee action.

Troubleshoot why an Adaptive Response action is not available to select

If an Adaptive Response action is not available to select on the correlation search editor or Incident Review, several things could be the cause.

- Your role may not have permissions to view and use the Adaptive Response action. See Using the alert actions manager in the *Alerting Manual*.
- Check the alert actions manager to determine if the Adaptive Response actions exist in Splunk platform. See Using the alert actions manager in the *Alerting Manual*.
- If the Adaptive Response actions from an add-on do not appear in Splunk Enterprise Security, but do appear in the alert actions manager, make sure that the add-on is being exported globally. See Make Splunk knowledge objects globally available in the Splunk Enterprise *Admin Manual*.
- If you can select the Adaptive Response action on the correlation search editor, but not on Incident Review, the Adaptive Response action might be an ordinary alert action, or the response action does not support ad hoc invocation. See Determine whether your action supports ad hoc invocation on the Splunk developer portal.

Set up an Adaptive Response relay from a Splunk Cloud Enterprise Security search head to an on-premises device

Splunk Cloud customers can utilize Adaptive Response actions in Splunk Enterprise Security (ES) without exposing infrastructure controls and administration to the open internet. Adaptive response relay allows adaptive response actions to queue on the Splunk Cloud ES search head. These queued actions store metadata and search results that allow a separate proxy component to execute those adaptive response actions from within the on-premises environment.

You need to perform the following steps to set up Adaptive Response actions:

1. Install the technology add-on for Adaptive Response on your heavy forwarder.
2. Configure your Splunk Cloud ES search head with an API key.
3. Configure your on-premises heavy forwarder with an API key.
4. Configure your on-premises heavy forwarder with a modular action relay.
5. Configure your Splunk Cloud ES search head with a modular action worker.
6. Configure adaptive response actions for your Splunk Cloud ES search head.

Install the technology add-on for Adaptive Response on your heavy forwarder

For an on-premises heavy forwarder to perform Adaptive Response actions, you must install the actions on both the Splunk Cloud ES search head and the heavy forwarder. These actions are installed by default with ES in `$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence`, but you need to install them manually on your heavy forwarder.

1. From the Splunk ES menu bar of the Splunk Cloud ES search head, select **Configure > General > General Settings.**
2. Locate the **Distributed Configuration Management** item.
3. Click **Splunk_TA_AROnPrem** to download the app.
4. Install the app on the heavy forwarder.

Configure your Splunk Cloud ES search head with an API key

The API key allows you to authenticate from the KV Store collection and CAM queue. You must create and manage your own API key. The API key follows a specific format, and it does not support two-factor authentication. For a Splunk Cloud environment that requires two-factor authentication, turn off this feature by not setting an API key.

1. Retrieve the heavy forwarder's `serverName` value by running the following search on the heavy forwarder:

```
| rest /services/server/info | table serverName
```

Take note of this name because you will need it when you set up your heavy forwarder. In this example the `serverName` value is `hf1`.

2. Install the Common Information Model version 4.12 or higher on the Splunk Cloud ES search head, if you haven't done so already.
3. Generate an API key on the Splunk Cloud ES search head.
    1. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click the **Adaptive Response** tab.
    2. Under **Manage API Keys** do the following steps:
        1. In the **Key Name** field, type the `serverName` value that you retrieved: in this case, `hf1`.
        2. To generate the API key value, type the following URI into a browser window of your Splunk Cloud ES search head:
           `https://<yoursplunkserver>/en-US/splunkd/__raw/alerts/modaction_queue/key`
           This will return a random 128-character string in the valid format.
        3. Copy and paste the string into the **API Key** field.
           Take note of this string because you will use it when you configure your heavy forwarder.

Configure your on-premises heavy forwarder with an API key

An API key allows the heavy forwarder to authenticate against the Splunk Cloud ES search head. The API key on the heavy forwarder must match the API key on the Splunk Cloud ES search head.

1. Install the Common Information Model version 4.12 or higher on the heavy forwarder, if you haven't done so already.
2. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click the **Adaptive Response** tab.
3. Under **Manage API Keys** do the following steps:
    1. On the key management page, in the **Key Name** field, type the `serverName` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section.
    2. On the key management page, in the **API Key** field, paste the string that you took note of in the Configure your Splunk Cloud ES search head with an API key section.

Configure your on-premises heavy forwarder with a modular action relay

The modular action relay is where you set the heavy forwarder to retrieve queued search results from a Splunk Cloud correlation search so that it can execute adaptive response actions on premises.

1. From the Splunk ES menu bar, select **Settings > Data inputs**.
2. Scroll down to Modular Action Relay and click **+ Add new**.
    1. Type a **Name** for the relay, such as `relay1`.
    2. Type the **Remote Search Head URI** in the format of `protocol://servername:port`, such as:
       `https://10.224.62.249:8089`.
       8089 is the default port for Splunk Cloud.
    3. Type a **Description** for the relay, such as `remote search head`.
    4. Type the **Api Key Name** (the `serverName` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section), such as `hf1`.
    5. Type `True` in the **Verify** field to verify the certificates between the worker and the Splunk Cloud ES search head.
    6. (Optional) If your ES search head is using a privately signed SSL certificate, add your root CA certificate chain file to the `Splunk_SA_CIM/auth` directory on the heavy forwarder and provide its file name to this input in the **Client Certificate** field. If your search head is in Splunk Cloud, this is not an issue.

Configure your Splunk Cloud ES search head with a modular action worker

The modular action worker is where you specify the `serverName` value of the heavy forwarder that the Splunk Cloud ES search head will queue search results for.

1. From the Splunk ES menu bar of the Splunk Cloud ES search head, select **Configure > Content > Content Management**.
2. Type `Modular Action Workers` in the search filter.
3. Click the name of the **Modular Action Workers** lookup.
4. Add a worker set and the name of the worker. The `worker_set` value is used when running Adaptive Response actions from ES. The `cam_worker` is the actual name of the heavy forwarder that will execute the actions.
    1. Leave the row with **local** as-is because it allows for local execution of actions on the Splunk Cloud ES search head.
    2. In the **worker_set** column, type a descriptive name for the heavy forwarder: `onprem`.
    3. In the **cam_workers** column, type the `serverName` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section, such as `"["hf1"]"`.
       The format requires array-style notation of `"["nameofworker"]"` with each worker name in quotes and separated with commas in CSV encoded JSON. An example of multiple workers is `"[""hf1"",""hf2""]"`.

Configure Adaptive Response actions for your Splunk Cloud ES search head

See Configure Adaptive Response actions for a correlation search in Splunk Enterprise Security for information about configuring Adaptive Response actions in general.

The Worker Set drop-down menu is specific to Adaptive Response actions on a Splunk Cloud ES search head. After completing the in the Configure your Splunk Cloud ES search head with a modular action worker section, when you create or edit a correlation search to add an Adaptive Response action, the drop-down menu includes the `worker_set` that you created.

Select the `worker_set` to use for executing those Adaptive Response actions from within the on-premises environment.

The results of Adaptive Response actions, ping for example, are found in `"index=main source=ping"`.

Troubleshoot Adaptive Response relay from Splunk Cloud ES search head to an on-premises device

The Adaptive Response modular input runs on a default interval of 2 minutes. You can adjust this based on your needs. A more frequent execution time will place additional load on the Splunk Cloud ES search head. To avoid performance problems with the CAM queue, adjust the interval to run less frequently, and do not set it below 10 seconds.

Ensure that your heavy forwarder is configured to forward its data to your indexers. This includes forwarding data from the relayed modular actions. You can run a search similar to the following search on your ES search head to verify that data is forwarding, where `hf1` is the name of your heavy forwarder:

```
index="cim_modactions" host=hf1
```

If this search never returns results, then your heavy forwarder is experiencing issues connecting to the ES search head.

Related information about distributed Adaptive Response actions

See the following related information about distributed Adaptive Response actions.

- See Adaptive Response framework in Splunk ES on the Splunk Developer Portal.
- See Create an Adaptive Response action on the Splunk Developer Portal.
- See Example distributed Adaptive Response action on the Splunk Developer Portal.
- See Create an Adaptive Response action for Enterprise Security in the *Splunk Add-on Builder User Guide*.

Configure adaptive response actions for a correlation search in Splunk Enterprise Security

As a Splunk Enterprise Security admin, you can configure which adaptive response actions that a correlation search triggers.

Analysts can run some adaptive response actions on an ad hoc basis from Incident Review. See Included adaptive response actions with Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Splunk Enterprise Security includes several adaptive response actions, and you can obtain additional ones from add-ons available on Splunkbase.

Included adaptive response actions

Splunk Enterprise Security includes several adaptive response actions.

- Create a notable event.
- Modify a risk score with a risk modifier.
- Send an email.
- Run a script.
- Start a stream capture with Splunk Stream.
- Ping a host.
- Run Nbtstat.
- Run Nslookup.
- Add threat intelligence.
- Create a Splunk Web message.

Create a notable event

Create a **notable event** when the conditions of a correlation search are met.

1. On the Splunk Enterprise Security menu bar, click **Configure > Content > Content Management**.
2. Click an existing correlation search, or click **Create New > Correlation Search**.
3. Click **Add New Response Action** and select **Notable** to add a notable event.
4. Type a **Title** of the notable event on the **Incident Review** dashboard. Supports variable substitution from the fields in the matching event.
5. Type a **Description** of the notable event. Supports variable substitution from the fields in the matching event
6. Select the **Security Domain** of the notable event from the drop-down list.
7. Select the **Severity** of the notable event from the drop-down list. The severity is used to calculate the **Urgency** of a notable event.

8. (Optional) Change the default owner of the notable event from the system default, **unassigned**.
9. (Optional) Change the default status of the notable event from the system default, **New**.
10. Type a drill-down name for the **Contributing Events** link in the notable event.
11. Type a drill-down search for the **Contributing Events** link in the notable event.
12. In the **Drill-down earliest offset** field, type the amount of time before the time of the triggering event to look for related events for the **Contributing Events** link in the notable event.
    For example **2h** to look for contributing events 2 hours before the triggering event.
13. In the **Drill-down latest offset** field, type the amount of time after the time of the triggering event to look for related events for the **Contributing Events** link in the notable event.
    For example, **1h** to look for contributing events 1 hour after the triggering event.
14. (Optional) Add **Investigation Profiles** that apply to the notable event.
    For example, add an investigation profile that fits a use case of "Malware" to malware-related notable events.
15. (Optional) Add fields that contain assets in **Asset Extraction** to extract the field values and add them to the investigation workbench as artifacts when the notable event is added to an investigation.
16. (Optional) Add fields that contain identities in **Identity Extraction** to extract the field values and add them to the investigation workbench as an artifact when the notable event is added to an investigation.
17. Type **Next Steps** for an analyst to take after triaging a notable event. Type text or click **Insert Adaptive Response Action** to reference a response action in the text of the next steps. You can only type plain text and links to response actions in the next steps field. Use next steps if you want to recommend response actions that should be taken in a specific order.
    For example, ping a host to determine if it is active on the network. If the host is active, increase the risk score by 100, otherwise, increase the risk score by 50.
18. Select **Recommended Actions** to complement the next steps. From the list of all adaptive response actions, click the name of an action that you recommend as a triage or investigation step for this notable event to add it to the list of recommended actions that analysts can take for this notable event. You can add as many recommended actions as you like. Use recommended actions to recommend response actions that do not need to be taken in a specific order.
    For example, increase the risk score on a host and perform an nslookup on a domain name.

In Splunk Enterprise Security versions lower than 6.1.1, correlation searches can produce a notable event with an "invalid" severity, resulting in a less than ideal urgency calculation. In Splunk Enterprise Security 6.1.1 and higher, notable event severity is validated as one of "critical," "high," "medium," "low," or "informational." If it is not one of the aforementioned values, the severity is set to "unknown." From there, normal urgency calculations apply. See How urgency is assigned to notable events in Splunk Enterprise Security.

Modify a risk score with a risk modifier

Modify a risk score as a result of a correlation search or in response to notable event details with the **Risk Analysis** adaptive response action. The risk adaptive response action creates a risk modifier event. You can view the risk modifier events on the Risk Analysis dashboard in Enterprise Security.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Click **+** to add a risk modifier.
    1. Type a positive integer in the **Risk Score** field to assign a value to the risk object.
    2. In the **Risk Object Field**, type the name of a field that exists in the correlation search to apply the risk score to the field.
       For example, type **src** to specify the source field.
    3. In the **Risk Object Type** field, select the name of an object type to specify wether the entity is a system, user, or other. The list is shown based on results from the `` |`risk_object_types` `` macro. For example, **host_artifacts** for an asset.
3. Click **+** to add additional risk modifiers and follow the previous steps a-c to assign different risk scores to different

fields.

This view is unique to the correlation search editor. You do not see it, for example, in the adaptive response actions through Incident Review.

See Assign risk to an object in *Use Splunk Enterprise Security* for other ways to modify risk scores.

Send an email

Send an email as a result of a correlation search match.

Prerequisite

Make sure that the mail server is configured in the Splunk platform before setting up this response action.

- For Splunk Enterprise, see Configure email notification settings in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud, see Configure email notification settings in the Splunk Cloud *Alerting Manual*.

Steps

1. Click **Add New Response Action** and select **Send email**.
2. In the **To** field, type a comma-separated list of email addresses to send the email to.
3. (Optional) Change the priority of the email. Defaults to **Lowest**.
4. Type a subject for the email. The email subject defaults to "Splunk Alert: $name$", where $name$ is the correlation search **Search Name**.
5. Type a message to include as the body of the email. Defaults to "The scheduled report '$name$' has run."
6. Select the check boxes of the information you want the email message to include.
7. Select whether to send a plain-text or HTML and plain-text email message.

If you're using the **Override Email Alert Action** in the general settings, the `subject="$action.email.subject$"` is passed explicitly. The default `useNSSubject` for use in local savedsearches `$action.email.subject.alert$` and `$action.email.subject.report$` is ignored. See Configure general settings for Splunk Enterprise Security.

When using '''Send email''' from the adaptive response actions through Incident Review, token replacement is not supported based on event fields. For example, you cannot use an email subject such as "Splunk Alert: $name$", where $name$ is the correlation search name. Since this is an ad-hoc adaptive response action rather than a scheduled saved search, the $name$ token does not apply. Token replacement is supported from the adaptive response actions through the correlation search editor.

Run a script

Run a script stored in `$SPLUNK_HOME/bin/scripts`.

1. Click **Add New Response Action** and select **Run a script**.
2. Type the file name of the script.

More information about scripted alerts can be found in the Splunk platform documentation.

- For Splunk Enterprise, see Configure scripted alerts in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud, see Configure scripted alerts in the Splunk Cloud *Alerting Manual*.

Start a stream capture with Splunk Stream

Start a stream capture to capture packets on the IP addresses of the selected protocols over the time period that you select. You can view the results of the capture session on the Protocol Intelligence dashboards.

A stream capture will not work unless you integrate Splunk Stream with Splunk Enterprise Security. See Integrate Splunk Stream with Splunk Enterprise Security.

1. Click **Add New Response Action** and select **Stream Capture** to start a packet capture in response to a correlation search match.
2. Type a **Description** to describe the stream created in response to the correlation search match.
3. Type a **Category** to define the type of stream capture. You can view streams by category in Splunk Stream.
4. Type the comma-separated event fields to search for IP addresses for the Stream capture. The first non-null field is used for the capture.
5. Type the comma-separated list of protocols to capture.
6. Select a **Capture duration** to define the length of the packet capture.
7. Type a **Stream capture limit** to limit the number of stream captures started by the correlation search.

Ping a host

Determine whether a host is still active on the network by pinging the host.

1. Click **Add New Response Action** and select **Ping**.
2. Type the event field that contains the host that you want to ping in the **Host Field**.
3. Type the number of maximum results that the ping returns. Defaults to 1.
4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud ES search head. See Set up an adaptive response relay from a Splunk Cloud Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

Run nbtstat

Learn more about a host and the services that the host runs by running nbtstat.

1. Click **Add New Response Action** and select **Nbtstat**.
2. Type the event field that contains the host that you want to run the nbtstat for in the **Host Field**.
3. Type the number of maximum results that the nbtstat returns. Defaults to 1.
4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud ES search head. See Set up an adaptive response relay from a Splunk Cloud Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

Run nslookup

Look up the domain name of an IP address, or the IP address of a domain name, by running nslookup.

1. Click **Add New Response Action** and select **Nslookup**.
2. Type the event field that contains the host that you want to run the nslookup for in the **Host Field**.
3. Type the number of maximum results that the nslookup returns. Defaults to 1.
4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud ES search head. See Set up an adaptive response relay from a Splunk Cloud Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

Add threat intelligence

Create threat artifacts in a threat collection.

1. Click **Add New Response Action** and select **Add Threat Intelligence**.
2. Select the **Threat Group** to attribute this artifact to.
3. Select the **Threat Collection** to insert the threat artifact into.
4. Type the **Search Field** that contains the value to insert into the threat artifact.
5. Type a **Description** for the threat artifact.
6. Type a **Weight** associated with the threat list. Defaults to 1.
7. Type a number of **Max Results** to specify the number of results to process as threat artifacts. Each unique search field value counts as a result. Defaults to 100.

Asset and Identity Overview

Add asset and identity data to Splunk Enterprise Security

Splunk Enterprise Security uses an asset and identity system to correlate asset and identity information with events to enrich and provide context to your data. This system takes information from external data sources to populate **lookups**, which Enterprise Security correlates with events at search time.

You have choices for registering asset and identity data in ES:

- Manually register asset and identity data in Asset and Identity Manager
- Use LDAP to register data in Asset and Identity Manager
- Use cloud service provider data to register data in Asset and Identity Manager

Manually register asset and identity data in Asset and Identity Manager

Do the following to manually add asset and identity data to ES to take advantage of asset and identity correlation:

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.
4. Manage assets and identities in Splunk Enterprise Security.
5. Verify that your asset or identity data was added to Splunk Enterprise Security.

Use LDAP to register data in Asset and Identity Manager

Do the following to use LDAP to register asset and identity data in ES to take advantage of asset and identity correlation.

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. Create an asset lookup from your current LDAP data in Splunk Enterprise Security.
3. Create an identity lookup from your current LDAP data in Splunk Enterprise Security.
4. Verify that your asset or identity data was added to Splunk Enterprise Security.

Use your cloud service provider to register data in Asset and Identity Manager

Do the following to use your cloud service provider to register asset and identity data in ES to take advantage of asset and identity correlation.

1. Create an asset lookup from your current cloud service provider data in Splunk Enterprise Security.
2. Create an identity lookup from your current cloud service provider data in Splunk Enterprise Security.
3. Verify that your asset or identity data was added to Splunk Enterprise Security.

See also

Lookups that store merged asset and identity data

Asset and identity fields after processing in Splunk Enterprise Security

How Splunk Enterprise Security processes and merges asset and identity data

Manage asset and identity upon upgrade

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you may see the following issues:

- The Asset and Identity Management navigation bar and page does not display if you have customized the menu bar in Splunk Enterprise Security. See Restore the default navigation or Recover previous view of Assets and Identities Navigation page.
- The Asset and Identity page merges the data for your assets and identities after the upgrade. For more information on how to avoid merged rows to display, see Avoid merged assets and identities data.
- The asset and identity collections, search previews, and search results may display differently from before the upgrade. To restore the previous view that you had prior to the upgrade, see Recover previous view of Assets and Identities Navigation page.
- The Asset and Identity page does not enable access to some of your previously saved macros. You may no longer be able to access saved macros if they were not documented for public use.

Recover Asset and Identity Management page

You may not see the Asset and Identity Management page after you upgrade to Enterprise Security 6.0 or higher, especially if you customized the menu bar in the Splunk Enterprise Security app. You have the option to restore the default Assets and Identity Management page or revert to your previous Asset and Identity Management page.

For more information on how to restore the default navigation menu bar for assets and identities, see Restore the default navigation.

Avoid merged assets and identities data

When you upgrade to Splunk Enterprise Security 6.2 or higher, your asset collection may not retain the settings that were specified in your .csv files. Instead, your assets and identities may be merged into rows, which potentially contain overlapping or duplicate information. This happens because the app automatically overwrites the old assets and identity collections.

For example, consider a source file with duplicates in the key field of `nt_host`, such as the following:

```
192.0.2.2,,host1,,,,,,,,,,,,,,
192.0.2.120,,host1,,,,,,,,,,,,,,
192.0.2.135,,host1,,,,,,,,,, ,,,,
192.0.2.242,,host2,,,,,,,,,,,,,,
192.0.2.65,,host2,,,,,,,,,,,,,,
```

In this example, `host1` is assigned to three different IP addresses and `host2` assigned to two different IP addresses. In previous versions of Splunk Enterprise Security, the display of the Asset and Identity management page would retain the correlations established in the .csv files of the asset collection as follows:

asset	ip	nt_host	pci_domain
192.0.2.2 host1	192.0.2.2	host1	untrust
192.0.2.120 host1	192.0.2.120	host1	untrust

asset	ip	nt_host	pci_domain
192.0.2.135 host1	192.0.2.135	host1	untrust
192.0.2.242 host2	192.0.2.242	host2	untrust
192.0.2.65 host2	192.0.2.65	host2	untrust

However, post upgrade the three rows with `nt_host` of `host1` will be merged into one asset, and the two rows with `host2` may be merged into another asset as follows:

asset	ip	nt_host	pci_domain
192.0.2.2 192.0.2.120 192.0.2.135 host1	192.0.2.2 192.0.2.120 192.0.2.135	host1	untrust
192.0.2.242 192.0.2.65 host2	192.0.2.242 192.0.2.65	host2	untrust

To avoid merged rows from being displayed in the Assets and Identities page, you may clean up the source data. For more information on cleaning your source data, see Maintain data hygiene.

Alternatively, you have the option of disabling the merge so that the collection remains the same as the source file and you do not see merged rows in your display. However, you must upgrade to Splunk Enterprise Security 6.2.0 to disable the merge. For more information on enabling or disabling the merge, see Enable merge for assets or identities.

Finally, you may also limit the maximum number of merges for each row by upgrading to Splunk Enterprise Security versions 6.0.2 or 6.1.1. For more information on upgrading to Enterprise Security 6.0.2 or 6.1.1, see Upgrade to Splunk Enterprise Security 6. 0.2 or 6.1.1.

Maintain data hygiene by cleaning source data

Avoid merged rows and maintain data hygiene by cleaning asset and identity source data and removing duplicate fields or values. Long merged rows of data should be cleaned to avoid performance issues.

Splunk Enterprise Security versions 6.1.1 and higher may truncate the long merged rows of data based on the multivalue limits set for each field. However, for Splunk Enterprise Security versions 6.0.2 truncation may be possible without configuring the multivalue limits.

Rows may be merged when any of the following scenarios occur:

- If the source data has two separate rows, which contain `dns="splunk.com"`, then the rows are merged post upgrade.

- If you input any of the following values `"NULL"`, `"null"`, `"N/A"`, `"blank"`, or `"none"` in one of the four "key" fields `nt_host`, `ip`, `mac`, or `dns`, and if these values are not empty zero-byte string, the values are merged to avoid duplication.

For Splunk Enterprise Security 6.1.1 and 6.2.0, the following input values: `"null"`, `"n/a"`, `"unknown"`, `"undefined"` are not merged, but ignored.

- If there are multiple rows with `dns="undefined"` and other rows with `nt_host="undefined"`, all rows in the lookup may be merged even though the IP addresses are different. The resulting merged row may cause search performance issues.

Upgrade to Splunk Enterprise Security 6.0.2 or 6.1.1

If you do not have the option to clean you source data, you may limit the maximum number of merges for each row. You may do this by upgrading to Splunk Enterprise Security versions 6.0.2 or 6.1.1 and including the maximum limit values for the distributed lookups.

For more information on multivalue field limits for assets, see Multivalue field limits for assets. For more information on multivalue field limits for identities, see Multivalue field limits for identities.

For more information on Splunk Enterprise Security compatibility matrix, see Compatibility matrix.

Recover previous view of Assets and Identities Navigation page

If you do not wish to restore the default navigation menu, you can append the following path: `/app/SplunkEnterpriseSecuritySuite/ess_entity_management` to your Splunk server URL and revert to your previous Assets and Identity Management page.

Asset and Identity Manual Registration

Collect and extract asset and identity data in Splunk Enterprise Security

Collect and extract your asset and identity data in order to add it to Splunk Enterprise Security. In a Splunk Cloud deployment, work with Splunk Professional Services to design and implement an asset and identity collection solution.

1. Determine where the asset and identity data in your environment is stored.
2. Collect and update your asset and identity data automatically to reduce the overhead and maintenance that manual updating requires and improve data integrity.

    - Use Splunk DB Connect or another Splunk platform add-on to connect to an external database or repository.
    - Use scripted inputs to import and format the lists.
    - Use events indexed in the Splunk platform with a search to collect, sort, and export the data to a list.

Suggested collection methods for assets and identities.

Technology	Asset or Identity data	Collection methods
Active Directory	Both	SA-ldapsearch and a custom search.
	Both	SecKit Windows Add On for ES Asset and Identities *
LDAP	Both	SA-ldapsearch and a custom search.
CMDB	Asset	DB Connect for integrating with 3rd Party structured data sources, and a custom search.
ServiceNow	Both	Splunk Add-on for ServiceNow
Asset Discovery	Asset	Splunk for Asset Discovery *
Bit9	Asset	Splunk Add-on for Bit9 and a custom search.
Cisco ISE	Both	Splunk Add-on for Cisco ISE and a custom search.
Microsoft SCOM	Asset	Splunk Add-on for Microsoft SCOM and a custom search.
Okta	Identity	Splunk Add-on for Okta and a custom search. *
Sophos	Asset	Splunk Add-on for Sophos and a custom search.
Symantec Endpoint Protection	Asset	Splunk Add-on for Symantec Endpoint Protection and a custom search.
Amazon Web Services (AWS)	Asset	SecKit AWS Add On for ES Asset and Identities *
Configuration Management Database (CMDB)	Asset	SecKit SA Common tools for populating assets and identities in Enterprise Security and PCI apps *

* Not officially supported for use through a wizard setup, but available for manual setup.

Next step

Format an asset or identity list as a lookup in Splunk Enterprise Security

Format an asset or identity list as a lookup in Splunk Enterprise Security

Format your collected asset or identity data into a lookup file so that it can be processed by Splunk Enterprise Security.

Prerequisites

- Collect and extract asset and identity data for Splunk Enterprise Security

Steps

1. Create a plain text, CSV-formatted file with Unix line endings and a `.csv` file extension.
2. Use the correct headers for the CSV file. See Asset lookup header or Identity lookup header for the headers expected by Splunk Enterprise Security.
3. Populate the rows of the CSV with the asset or identity fields. The maximum number of characters per value in a field is 975. For a multivalue field, each value in the list can be 975 characters. See Asset lookup fields or Identity lookup fields for reference.

For an example asset list, review the Demonstration Assets lookup.

- Locate the list in Splunk Web by navigating to **Configure > Content > Content Management**.
- Locate the list in the file system, the `demo_assets.csv` file is located in the `SA-IdentityManagement/lookups/` directory.

If you use a custom search to generate a lookup, make sure that the lookup produced by the search results contains fields that match the headers.

Next step

Configure the new asset or identity list in Splunk Enterprise Security

Asset and identity lookup configurations

Enterprise Security manages specific `props.conf` settings as part of the asset and identity framework. In order for these files to be configured properly, all configurations need to be populated in the `SPLUNK_HOME/etc/apps/SA-IdentityManagement/`**`local`**`/props.conf` file. If there are existing identity correlation lookup definitions in the `SPLUNK_HOME/etc/apps/SA-IdentityManagement/`**`default`**`/props.conf` file, remove them so they can be managed by the asset and identity framework.

Asset lookup header

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av,cim_entity_zone
```

Asset lookup fields

Populate the following fields in an asset lookup.

To add multi-homed hosts or devices to the asset list, add each IP address to the `ip` field for the host, pipe-delimited. Multi-homed support is limited, and having multiple hosts with the same IP address on different network segments can cause conflicts in the merge process.

Field	Data type	Description	Example values
ip	pipe-delimited numbers	A pipe-delimited list of single IP address or IP ranges. An asset is required to have an entry in at least one of the key fields such as: **ip**, **mac**, **nt_host**, or **dns** fields. All of the key fields are multi-value fields.	2.0.0.0/8|1.2.3.4|192.168.15.9-192.169.15.27|5.6.7.8|10.11.12.13
mac	pipe-delimited strings	A pipe-delimited list of MAC address. An asset is required to have an entry in at least one of the key fields such as: **ip**, **mac**, **nt_host**, or **dns** fields. All of the key fields are multi-value fields.	00:25:bc:42:f4:60|00:50:ef:84:f1:21|00:50:ef:84:f1:20
nt_host	pipe-delimited strings	A pipe-delimited list of Windows machine names. An asset is required to have an entry in at least one of the key fields such as: **ip**, **mac**, **nt_host**, or **dns** fields. All of the key fields are multi-value fields.	ACME-0005|SSPROCKETS-0102|COSWCOGS-013
dns	pipe-delimited strings	A pipe-delimited list of DNS names. An asset is required to have an entry in at least one of the key fields such as: **ip**, **mac**, **nt_host**, or **dns** fields. All of the key fields are multi-value fields.	acme-0005.corp1.acmetech.org|SSPROCKETS-0102.spsp.com|COSWCOGS-013.cwcogs.com
owner	string	The user or department	f.prefect@acmetech.org, DevOps, Bill

Field	Data type	Description	Example values
		associated with the device	
priority	string	**Recommended.** The priority assigned to the device for calculating the **Urgency** field for notable events on Incident Review. An "unknown" priority reduces the assigned **Urgency** by default. For more information, see How urgency is assigned to notable events in Splunk Enterprise Security.	unknown, low, medium, high or critical.
lat	string	The latitude of the asset in decimal degrees, using +/- to indicate direction.	37.780080
long	string	The longitude of the asset in decimal degrees, using +/- to indicate direction.	-122.420170
city	string	The city in which the asset is located	Chicago
country	string	The country in which the asset is located	USA
bunit	string	**Recommended.** The business unit of the asset. Used for filtering by dashboards in Splunk Enterprise Security.	EMEA, NorCal
category	pipe-delimited strings	**Recommended.** A pipe-delimited list of logical classifications for assets. Used for	server|web_farm|cloud

Field	Data type	Description	Example values
		asset and identity correlation and categorization. See Asset/Identity Categories.	
pci_domain	pipe-delimited strings	A pipe-delimited list of PCI domains. See Configure assets in the Splunk App for PCI Compliance *Installation and Configuration Manual*.	cardholder, trust|dmz, untrust If left blank, defaults to untrust.
is_expected	boolean	Indicates whether events from this asset should always be expected. If set to true, the Expected Host Not Reporting correlation search performs an adaptive response action when this asset stops reporting events.	"true", or blank to indicate "false"
should_timesync	boolean	Indicates whether this asset must be monitored for time-sync events. It set to true, the Should Timesync Host Not Syncing correlation search performs an adaptive response action if this asset does not report any time-sync events from the past 24 hours.	"true", or blank to indicate "false"
should_update	boolean	Indicates whether this asset must be monitored for system update events.	"true", or blank to indicate "false"

Field	Data type	Description	Example values
requires_av	boolean	Indicates whether this asset must have anti-virus software installed.	"true", or blank to indicate "false"
cim_entity_zone	string	Required when entity zones are enabled. Lowercase word to use as a default zone name. For use in situations when you have mergers or acquisitions with other companies, for example, and you have similar IP address spaces that you need to keep separate. This word auto-populates in the cim_entity_zone fields if you do not specify your own values when formatting an asset or identity list as a lookup.	my_zone

You can also customize asset fields. See Manage asset field settings in Splunk Enterprise Security.

Identity lookup header

```
identity,prefix,nick,first,last,suffix,email,phone,managedBy,priority,bunit,category,watchlist,startD
ate,endDate,work_city,work_country,work_lat,work_long,cim_entity_zone
```

Identity lookup fields

Field	Data type	Description	Example
identity	pipe-delimited strings	**Required**. A pipe-delimited list of username strings representing the identity. After the merge process completes, this field includes generated values based on the identity lookup configuration settings.	a.vanhelsing|abraham.vanhelsing|a.vanhelsing@acmetech.org
prefix	string	Prefix of the identity.	Ms., Mr.
nick	string	Nickname of an identity.	Van Helsing

Field	Data type	Description	Example
first	string	First name of an identity.	Abraham
last	string	Last name of an identity.	Van Helsing
suffix	string	Suffix of the identity.	M.D., Ph.D
email	string	Email address of an identity.	a.vanhelsing@acmetech.org
phone	string	A multi-value field for telephone number of an identity.	123-456-7890
managedBy	string	A username representing the manager of an identity.	phb@acmetech.org
priority	string	**Recommended.** The priority assigned to the identity for calculating the **Urgency** field for notable events on Incident Review. An "unknown" priority reduces the assigned **Urgency** by default. For more information, see How urgency is assigned to notable events in Splunk Enterprise Security.	unknown, low, medium, high or critical.
bunit	string	**Recommended.** A group or department classification for identities. Used for filtering by dashboards in Splunk Enterprise Security.	Field Reps, ITS, Products, HR
category	pipe-delimited strings	**Recommended.** A pipe-delimited list of logical classifications for identities. Used for asset and identity correlation and categorization. See Asset/Identity Categories.	Privileged|Officer|CISO
watchlist	boolean	Marks the identity for activity monitoring.	Accepted values: "true" or empty. See User Activity Monitoring in this manual.
startDate	string	The start or hire date of an identity.	Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M, %s
endDate	string	The end or termination date of an identity.	Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M, %s
work_city	string	The primary work site City for an identity.	
work_country	string	The primary work site Country for an identity.	
work_lat	string	The latitude of primary work site City in decimal degrees, using +/- to indicate direction.	37.780080
work_long	string	The longitude of primary work site City in decimal degrees using +/- to indicate direction.	-122.420170
cim_entity_zone	string	Required when entity zones are enabled. Lowercase word to use as a default zone name. For use in situations when you have mergers or acquisitions with other companies, for example, and you have similar identities that you need to keep separate. This word auto-populates in the cim_entity_zone fields if you do not specify your own values when formatting an asset	my_zone

Field	Data type	Description	Example
		or identity list as a lookup.	

You can also customize identity fields. See Manage identity field settings in Splunk Enterprise Security.

Configure a new asset or identity list in Splunk Enterprise Security

Configure a new asset or identity lookup in Splunk Enterprise Security. This multistep process adds the lookup in Splunk Enterprise Security and defines the lookup for the merge process.

Prerequisites

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. Assets and identities framework supports only exact-matching of IPv6 addresses.

Steps

1. Add the new lookup table file
2. Set permissions on the lookup table file to share it with Splunk Enterprise Security
3. Add a new lookup definition
4. Set permissions on the lookup definition to share it with Splunk Enterprise Security

Add the new lookup table file

These lookup table files are consumed by the asset and identity framework and merged together. The product of the merge is called an "expanded lookup."

1. From the Splunk menu bar, select **Settings > Lookups > Lookup table files**.
2. Click **New**.
3. Select a **Destination App** of **SA-IdentityManagement**.
4. Select the lookup file to upload.
5. Type the **Destination filename** that the lookup table file should have on the search head. The name should include the filename extension.
   For example, `network_assets_from_CMDB.csv`
6. Click **Save** to save the lookup table file and return to the list of lookup table files.

In a distributed environment, these lookup table files are not replicated from the search heads to the indexers. Only the expanded lookup is replicated to the indexers. However, these lookup files are still replicated between search heads. If an asset or identity lookup table file grows in excess of 1GB+, it should be broken down into smaller files (for example, by location or by type or by easily identifiable category). When making changes to lookup files, only the updated files are replicated across search heads, reducing bundle sizes.

Set permissions on the lookup table file to share it with Splunk Enterprise Security

1. From **Lookup table files**, locate the new lookup table file and select **Permissions**.
2. Set **Object should appear in** to **All apps**.
3. Set **Read** access for **Everyone**.
4. Set **Write** access for `admin` or other roles.
5. Click **Save**.

Add a new lookup definition

1. From the Splunk menu bar, select **Settings > Lookups > Lookup definitions**.
2. Click **New**.
3. Select a **Destination App** of **SA-IdentityManagement**.
4. Type a name for the lookup source. This name must match the name defined later in the input stanza definition on the **Identity Management** dashboard.
   For example, `network_assets_from_CMDB`.
5. Select a **Type** of **File based**.
6. Select the lookup table file created.
   For example, select `network_assets_from_CMDB.csv`.
7. Click **Save**.

Set permissions on the lookup definition to share it with Splunk Enterprise Security

1. From **Lookup definitions**, locate the new lookup definition and select **Permissions**.
2. Set **Object should appear in** to **All apps**.
3. Set **Read** access for **Everyone**.
4. Set **Write** access for `admin` or other roles.
5. Click **Save**.

Next step

Manage assets and identities in Splunk Enterprise Security.

Asset and Identity LDAP and Cloud Service Provider Registration

Create an asset lookup from your current LDAP data in Splunk Enterprise Security

Use LDAP to register your assets, create a lookup, and schedule a search to run on a regular basis.

Prerequisites
This requires the Splunk Supporting Add-on for Active Directory for access to the `| ldapsearch` command. See Collect and extract asset and identity data in Splunk Enterprise Security.

To get started with the Asset and Identity Builder, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Asset and Identity Management**.
2. Click the **Asset Lookup Configuration** tab.
3. Click **New**.
4. Select the **LDAP Lookup** from the drop-down menu.

Search

In the search section, do the following to name the lookup generating search:

1. Provide a unique name for the search.
2. Provide your LDAP domain.

Once you have provided your LDAP domain, you will see messages in the custom search builder preview, such as "InvalidLDAPSearchSpec: Valid LDAP search specifications must supply a lookup." This message is normal at this point.

Lookup

In the lookup section, do the following:

1. Provide a lookup label for your search-driven lookup.
2. Provide a unique lookup name and/or transform name.
3. The lookup filename .csv will auto-complete based on the name you provided for the lookup name.

Search schedule

Once you have completed the lookup fields, the custom search builder preview will show the search it has created. Click **Run search** to verify if the search returns results.

In the search schedule section, do the following to run the search on a regular basis:

1. Enter a cron schedule.
2. Select **Real-time** or **Continuous** scheduling.
3. Click **Save**.

This saves two things:

- Saved searches that you can find in **Configure** > **Content** > **Content Management**
- Lookup table and lookup definition that you can find in **Settings** > **Lookups**

Asset management

The next step is where you begin to create the settings stored in the `input.conf` file that points to the lookup and pulls the data every 5 minutes to make updates to the asset or identity collections.

Since this example is for an asset, the next window that pops up is the New Asset Manager.

1. The **Source** is auto-populated with the name of the lookup that you provided.
2. See Asset Lookup Configuration.

Create an identity lookup from your current LDAP data in Splunk Enterprise Security

Use LDAP to register your identities, create a lookup, and schedule a search to run on a regular basis.

Prerequisites
This requires the Splunk Supporting Add-on for Active Directory for access to the `| ldapsearch` command. See Collect and extract asset and identity data in Splunk Enterprise Security.

To get started with the Asset and Identity Builder, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Asset and Identity Management**.
2. Click the **Identity Lookup Configuration** tab.
3. Click **New**.
4. Select the **LDAP Lookup** from the drop-down menu.

Search

In the search section, do the following to name the lookup generating search:

1. Provide a unique name for the search.
2. Provide your LDAP domain.

Once you have provided your LDAP domain, you will see messages in the custom search builder preview, such as "InvalidLDAPSearchSpec: Valid LDAP search specifications must supply a lookup." This message is normal at this point.

Lookup

In the lookup section, do the following:

1. Provide a lookup label for your search-driven lookup.
2. Provide a unique lookup name and/or transform name.
3. The lookup filename .csv will auto-complete based on the name you provided for the lookup name.

Search schedule

Once you have completed the lookup fields, the custom search builder preview will show the search it has created. Click **Run search** to verify if the search returns results.

In the search schedule section, do the following to run the search on a regular basis:

1. Enter a cron schedule.
2. Select **Real-time** or **Continuous** scheduling.
3. Click **Save**.

This saves two things:

- Saved searches that you can find in **Configure > Content > Content Management**
- Lookup table and lookup definition that you can find in **Settings > Lookups**

Identity management

The next step is where you begin to create the settings stored in the `input.conf` file that points to the lookup and pulls the data every 5 minutes to make updates to the asset or identity collections.

Since this example is for an identity, the next window that pops up is the New Identity Manager.

1. The **Source** is auto-populated with the name of the lookup that you provided.
2. See Identity Lookup Configuration.

Create an asset lookup from your cloud service provider data in Splunk Enterprise Security

Use cloud service provider data to register your identities, create a lookup, and schedule a search to run on a regular basis. Creating a cloud provider lookup automatically adds specific fields into the asset list, such as:

`image_id, instance_type, network_interface_id, subnet_id, vendor_account, vendor_region`
.

After saving the lookup search, you can edit or delete the fields from the **Asset Fields** tab of Asset and Identity Management. See Manage identity field settings in Splunk Enterprise Security.

Create an asset lookup

Prerequisites

- You must already have a cloud service provider.
- You must already be ingesting data from the cloud service provider into the Splunk platform.

Steps

Use the Asset and Identity Builder page to perform the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Asset Lookup Configuration** tab.
3. Click **New**.
4. Select the **Cloud Services Lookup** from the drop-down menu.

Name the asset lookup search

Steps

In the **Search** section of the Asset and Identity Builder page, perform the following steps:

1. In the **Search Name** field, type a unique name for the search.
2. From the **Cloud data source** drop-down menu, select one of the following options:
    - Select the name of a cloud service provider. These are listed by provider name and also by the event type used for the corresponding search, such as AWS (aws_description_ec2_instances).
    - Select **Custom** and when the **Custom event type** field appears, do one of the following:
        - Choose an event type. These are all the available event types in the Splunk platform, regardless of whether that type of data is populating in your environment.
        - Type a custom value of your own. Use this option if you have an alternate cloud source data type that you have not yet installed. See eventtypes.conf in the Splunk Enterprise *Admin Manual*.

After you have provided your cloud service provider, you will see messages in the custom search builder preview, such as "Valid search specifications must specify the 'lookup'." This message is normal at this point.

Auto-generate the lookup fields

Steps

In the **Lookup** section of the Asset and Identity Builder page, perform the following steps:

1. In the **Label** field, type a lookup label for your search-driven lookup.
2. In the **Lookup** field, type a unique lookup name or transform name.

The lookup CSV filename auto-completes based on the name you provided for the lookup name.

Create a search schedule

After you have completed generating the lookup fields, the custom search builder preview displays the search it has created. Click **Run search** to verify if the search returns results.

Steps

In the **Search Schedule** section of the Asset and Identity Builder page, perform the following steps:

1. Enter a cron schedule.
2. Select **Real-time** or **Continuous** scheduling.
3. Click **Save**.

After creating a search schedule, you can access the following searches in the Enterprise Security app:

- Saved searches in **Configure** > **Content** > **Content Management**.
- Lookup tables and lookup definitions in **Settings** > **Lookups**.

Make auto-updates to the assets

Create the settings that are stored in the input.conf file that points to the lookup and pulls the data every 5 minutes to make updates to the asset collections. To make auto-updates to assets, access the **New Asset Manager**. The **Source** is auto-populated with the name of the lookup that you provided. For more information, see Manage identity lookup configuration policies in Splunk Enterprise Security.

Create an identity lookup from your cloud service provider data in Splunk Enterprise Security

Use cloud service provider data to register your identities, create a lookup, and schedule a search to run on a regular basis.

Create an identity lookup

Prerequisites

- You must already have a cloud service provider.*
- You must already be ingesting data from the cloud service provider into the Splunk platform.

Steps

Use the Asset and Identity Builder page to perform the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Asset and Identity Management**.
2. Click the **Asset Lookup Configuration** tab.
3. Click **New**.
4. Select the **Cloud Services Lookup** from the drop-down menu.

Name the identity lookup search

Steps

In the **Search** section of the Asset and Identity Builder page, perform the following steps:

1. In the **Search Name** field, type a unique name for the search.
2. From the **Cloud data source** drop-down menu, select one of the following options:
    - ♦ Select the name of a cloud service provider. These are listed by provider name and also by the event type used for the corresponding search, such as AWS (aws_description_ec2_instances).
    - ♦ Select **Custom** and when the **Custom event type** field appears, do one of the following:
        - ◊ Choose an event type. These are all the available event types in the Splunk platform, regardless of whether that type of data is populating in your environment.
        - ◊ Type a custom value of your own. Use this option if you have an alternate cloud source data type that you have not yet installed. See eventtypes.conf in the Splunk Enterprise *Admin Manual*.

After you have provided your cloud service provider, you will see messages in the custom search builder preview, such as "Valid search specifications must specify the 'lookup'." This message is normal at this point.

Auto-generate the lookup fields

Steps

In the **Lookup** section of the Asset and Identity Builder page, perform the following steps:

1. In the **Label** field, type a lookup label for your search-driven lookup.
2. In the **Lookup** field, type a unique lookup name or transform name.

The lookup CSV filename auto-completes based on the name you provided for the lookup name.

Create a search schedule

After you have completed generating the lookup fields, the custom search builder preview displays the search it has created. Click **Run search** to verify if the search returns results.

Steps

In the **Search Schedule** section of the Asset and Identity Builder page, perform the following steps:

1. Enter a cron schedule.
2. Select **Real-time** or **Continuous** scheduling.
3. Click **Save**.

After creating a search schedule, you can access the following searches in the Enterprise Security app:

- Saved searches in **Configure** > **Content** > **Content Management**.
- Lookup tables and lookup definitions in **Settings** > **Lookups**.

Make auto-updates to assets or identities

Create the settings that are stored in the input.conf file that points to the lookup and pulls the data every 5 minutes to make updates to the identity collections. To make auto-updates to identitiess, access the **New Identity Manager**. The **Source** is auto-populated with the name of the lookup that you provided. For more information, see Identity Lookup Configuration.

Asset and Identity Management

Manage assets and identities in Splunk Enterprise Security

Use the Asset and Identity Management page to enrich and manage asset and identity data using lookups. The Asset and Identity Management interface replaces the previously separate menus for Identity Management, Identity Correlation, and Identity Lookup Configuration. You need to have the edit_modinput_identity_manager capability to use it. See Configure users and roles in the *Installation and Upgrade Manual*.

When the identity manager runs, it processes all of the asset and identity input configurations that have changed. If the source has been updated, the identity manager dispatches the SPL created by a custom-built search.

The SPL search uses a custom search command that handles the merging and updating of new data to existing data. The custom search command merges data based on key fields and policies that you define here.

Assets and identities that need to be deleted are updated in the KV store with a `_delete` flag set to `True` so that the delete operation can persist and be completed at a later time.

The custom search command returns the merged data, which is updated or inserted to the KV store using `outputlookup append=T`. The identity manager checks and processes rows that are marked for deletion.

If you have customized the menu bar in Splunk Enterprise Security, the Asset and Identity Management navigation and page do not display. See Restore the default navigation to restore them.

Prerequisites

Perform the following prerequisite tasks before starting any of the tasks listed in the table:

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.

Asset and identity management tasks

Complete the following tasks to manage configuration settings for assets and identities. These tasks do not need to be performed in any particular order.

Task	Description	Documentation
Configure global settings	Configure the global settings of the identity manager modular input to revise the way the identity manager works by default. You can change settings such as the following: • Disable merge for assets and identities • Enable entity zones for assets and identities • Ignore values for assets and identities • Revise the enforcements used by the identity manager framework • Revise the miscellaneous settings used by the identity manager framework • Revise asset and identity lookup memory usage behavior • Reset asset and identity collections immediately	Manage global settings for assets and identities in Splunk Enterprise Security

Task	Description	Documentation
Configure asset lookup configuration	The asset lookup configuration settings create the policy that updates the inputs.conf file to point to a lookup and update your assets. You can change settings such as the following: • Add an asset input stanza for the lookup source • Rank the order for merging assets • Disable or enable asset lookups • Modify asset lookups • Manually add static asset data • Disable the demo asset lookups	Manage asset lookup configuration policies in Splunk Enterprise Security
Configure asset field settings	Configure asset field settings for lookup matching. You can change settings such as the following: • Add or edit an asset field • Enable case-sensitive matching for asset fields • Revise multivalue field limits for assets	Manage asset field settings in Splunk Enterprise Security
Create identity lookup configuration	Create an identity lookup configuration policy to update and enrich your identities. You can change settings such as the following: • Add an identity input stanza for the lookup source • Rank the order for merging identities • Modify identity lookups	Manage identity lookup configuration policies in Splunk Enterprise Security
Configure identity field settings	Configure identity settings for lookup matching. You can change settings such as the following: • Add or edit an identity field • Enable case-sensitive matching for identity fields • Revise multivalue field limits for identities	Manage identity field settings in Splunk Enterprise Security
Configure Correlation setup	When asset and identity correlation is enabled, Splunk Enterprise Security compares indexed events with asset and identity data in the asset and identity lists to provide data enrichment and context. You can change settings such as the following: • Disable correlation for all sourcetypes • Enable correlation selectively by sourcetype • Enable correlation for all sourcetypes • Correlation and entity zones	Manage correlation setup in Splunk Enterprise Security
Search preview	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 test the following: • asset_lookup_by_str • asset_lookup_by_cidr • identity_lookup_expanded	Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security

Manage global settings for assets and identities in Splunk Enterprise Security

Configure the global settings of the identity manager modular input to revise the way the identity manager works by default.

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.

Enable merge for assets or identities

The merge process is enabled for assets and identities by default. However, in situations when you have a source file with duplication in the key fields, and you can't groom the file to make sure that the information belongs to the same asset or identity, then you have the option to disable the merge process.

Use the global settings to enable or disable merge 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 **Enable Merge for Assets or Identities** panel.
4. Use the toggle to enable or disable for **Assets** or **Identities**.

Using assets as an example, consider a source file with duplicates in the key field of `nt_host`, such as the following:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires _av
192.0.2.2,,host1,,,,,,,,,,,,,,
192.0.2.120,,host1,,,,,,,,,,,,,,
192.0.2.135,,host1,,,,,,,,,,,,,,
192.0.2.242,,host2,,,,,,,,,,,,,,
192.0.2.65,,host2,,,,,,,,,,,,,,
```

The default is to merge the three rows with `nt_host` of `host1` into one asset, and merge the two rows with `host2` into another asset.

asset	ip	nt_host	pci_domain
192.0.2.2 192.0.2.120 192.0.2.135 host1	192.0.2.2 192.0.2.120 192.0.2.135	host1	untrust
192.0.2.242 192.0.2.65 host2	192.0.2.242 192.0.2.65	host2	untrust

If you disable the merge, then the collection remains the same as the source file, and assets are not merged.

asset	ip	nt_host	pci_domain
192.0.2.2 host1	192.0.2.2	host1	untrust
192.0.2.120 host1	192.0.2.120	host1	untrust

asset	ip	nt_host	pci_domain
192.0.2.135 host1	192.0.2.135	host1	untrust
192.0.2.242 host2	192.0.2.242	host2	untrust
192.0.2.65 host2	192.0.2.65	host2	untrust

When you do a lookup on an non-merged collection, there is no context for how to resolve the overlapping key field values. For example, the asset_lookup_by_str lookup in transforms.conf has `max_matches = 1`, so the first host it matches in the assets_by_str collection is the only one you'll see in your search results.

Enable entity zones for Assets or Identities

Entity zones are disabled for assets and identities by default. You can enable entity zones in situations when you have mergers or acquisitions with other companies, for example, and you have similar IP address spaces that you need to keep separate.

Enable entity zones in the global settings 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 **Enable Zones for Assets or Identities** panel.
4. Use the toggle to enable for **Assets** or **Identities**.
5. Type a lowercase word to use as a default zone name. This word auto-populates in the `cim_entity_zone` fields if you do not specify your own values when formatting an asset or identity list as a lookup.
6. (Optional) Click **Configure Zones** to build a clause and specify a condition.
   The conditions may be as follows:
   - Matches an event
   - Assigns a specified zone to the `cim_entity_zone` field

     In situations where you have a default value specified for your known entities, a default `cim_entity_zone` value is not assigned if a similar event occurs from an unknown entity.

   1. In the **Condition** field, type a boolean that returns true or false for an eval statement in SPL. See Eval in the Splunk Enterprise *Search Reference*.
   2. In the **Zone** field, type the name of a zone to assign when the match is made.
   3. Click **+Add Clause** to add additional clauses.
   4. Click **x** to delete clauses.
   5. Click **Confirm** to save the clauses.
   6. Click **Save**.

   Any events that do not have a specified `cim_entity_zone`, or do not match any clauses, are assigned the default zone.

Disable entity zones for Assets and Identities

Disable entity zones in the global settings 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 **Enable Zones for Assets or Identities** panel.
4. Use the toggle to disable for **Assets** or **Identities**. Any previously existing default zone is disabled, not deleted.
5. Click **Save**.

See Format an asset or identity list as a lookup in Splunk Enterprise Security.

Example

Using assets as an example, consider a default zone name of **my_zone** and a source file with the same `ip` of 10.0.2.109, `nt_host` of host1 and host2 in different zones, a `cim_entity_zone` defined as an asset lookup header, and one empty `cim_entity_zone` value such as the following:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av,cim_entity _zone
192.0.2.94,,host1,,,,,,,,,,,,,,,
192.0.2.155,,host1,,,,,,,,,,,,,,,zone2
192.0.2.90,,host2,,, ,,,,,,,,,,,,zone1
192.0.2.39,,host2,,,,,,,,,,,,,,,zone1
10.0.2.109,,host2,,,,,,,,,,,,,,,zone1
10.0 .2.109,,host3,,,,,,,,,,,,,,,zone3
10.0.2.109,,host4,,,,,,,,,,,,,,,zone3
```

If you enable entity zones, the behavior is to use the default zone name for the empty `cim_entity_zone` value and not to merge key fields such as `ip` and `nt_host` that are in different zones.

cim_entity_zone	asset	ip	nt_host	pci_domain
my_zone	192.0.2.94 host1	192.0.2.94	host1	untrust
zone2	192.0.2.155 host1	192.0.2.155	host1	untrust
zone1	192.0.2.90 192.0.2.39 10.0.2.109 host2	192.0.2.90 192.0.2.39 10.0.2.109	host2	untrust
zone3	10.0.2.109 host3 host4	10.0.2.109	host3 host4	untrust

If you disable entity zones, the behavior is to merge key fields such as `ip` and `nt_host` as usual.

asset	ip	nt_host	pci_domain
192.0.2.94	192.0.2.94 192.0.2.155	host1	untrust

asset	ip	nt_host	pci_domain
192.0.2.155 host1			
192.0.2.90 192.0.2.39 10.0.2.109 host2 host3 host4	192.0.2.90 192.0.2.39 10.0.2.109	host2 host3 host4	untrust

Ignored values for Assets or Identities

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.

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.

Revise the enforcements used by the identity manager framework

Every five minutes when the identity manager runs, it automatically enforces configuration file settings used by the framework, including inputs.conf, props.conf, macros.conf, transforms.conf, and identityLookup.conf (deprecated).

With these enforcements enabled, if there are accidental changes made to your conf files, the settings are reverted back to the way they were. If you're doing manual testing or making changes on purpose to your conf files and you do not want the settings checked or reverted back, you can disable these enforcements.

Use the global settings to enable or disable enforcements as follows. For the majority of users who configure settings through the Splunk Web UI, there is no need to disable these 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 **Enforcements** panel.
4. Use the toggle to enable or disable.

Using the example of **Enforce props**, you experience the following by default. If you add a custom field in **Identity Settings**, the field is automatically added to the props.conf file because the settings check occurs to sync and reload props to be consistent with the identity manager.

Using the example of **Enforce props**, you experience the following by disabling it. If you add a custom field in **Identity Settings**, then you have to add that custom field to the props.conf file manually because the settings check no longer occurs. With enforce props disabled, any manual identity settings changes made without using the Splunk Web UI are also ignored.

After upgrading to Enterprise Security 6.2.0, you need to enable the **Enforce props** setting if you want the identity manager to automatically enforce configuration file settings. On a fresh installation, Enterprise Security 6.2.0 has **Enforce props** set to enabled by default and the setting is enforced continuously. However, prior versions only enforce once and then switch the setting to false right away. If you're already using a previous version of ES with assets and identities, the `/local/inputs.conf` file already has `enforce_props=false` and it needs to be set back to true after you upgrade, if you want to ensure that settings are managed for you. The majority of users who configure settings through the Splunk Web UI will benefit from enabling the setting.

Revise the miscellaneous settings used by the identity manager framework

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

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.

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,cim_entity_zone
192.187.2.94,,,,owner1,,,,,,,,,,,,,zone1
192.187.0.0 /16,,,,cidr_owner1,,,,,,,,,,,,,zone1
10.0.2.109,,,,owner2,,,,,,,,,,,,,zone1
10.0.2.0/24,,,,cidr _owner2,,,,,,,,,,,,,zone1
```

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
192.187.2.94	192.187.2.94	untrust
10.0.2.109	10.0.2.109	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.

Revise asset and identity lookups memory usage behavior

Prior to the release of Splunk Cloud 8.0.2004, KV Store backed lookups do not respect the `max_memtable_bytes` setting. This means that KV Store backed lookups are always stored in memory on the indexer.

With the release of Splunk Cloud 8.0.2004, KV Store backed lookups do respect the `max_memtable_bytes` setting. This means that a KV Store backed lookup is stored in memory until it exceeds the definition in the `max_memtable_bytes` setting.

You might experience the following behavior after upgrading. Using Splunk Enterprise 8.0 as an example, consider a KV Store lookup of 1 GB in size that is used as an automatic lookup, with `max_memtable_bytes=25MB`. If you upgrade to a Splunk Cloud version of 8.0.2004 or higher, the 1 GB size exceeds the `max_memtable_bytes` setting, so an index file is created and the lookup occurs on disk, which is slower.

The default setting in Splunk Cloud is `max_memtable_bytes=100MB`. Splunk Cloud customers need to contact technical support if necessary to revise this behavior.

To revise this behavior in an on-premises environment, increase your `max_memtable_bytes` in the `$SPLUNK_HOME/etc/system/local/limits.conf` file. See lookup of limits.conf in the Splunk Enterprise *Admin Manual*.

Reset your collections immediately

All the asset and identity source files that are enabled in the Asset and Identity Management page get merged into the following default collections in the collections.conf file: assets_by_str, assets_by_cidr, or identities_expanded.

If your collections get into an undesirable state, you can reset your collections at any time, rather than waiting for the automated process to clear out the KV store collection. It's similar to clearing cache manually.

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click **Reset Collections**. The button is globally available regardless if you are configuring in a particular tab.

When the identity manager runs again in 5 minutes, it rebuilds the collections based on which source files are enabled in the Asset Lookup Configuration or the Identity Lookup Configuration.

Manage asset lookup configuration policies in Splunk Enterprise Security

Create an asset lookup configuration policy to update and enrich your assets. The asset lookup configuration settings create the policy that updates the inputs.conf file to point to a lookup and update your assets. 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 asset input stanza for the lookup source

To add a new asset input source, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Asset Lookup Configuration** tab.
3. Click **New**.
4. In the New Asset 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 asset list stanza, but matching the source file name is a good idea.
    3. Enter a descriptive category for this asset list, such as web_servers or west_coast_servers.
    4. Enter a detailed description of the contents of this asset 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**, **asset** is selected for you.
7. In **Lookup Field Exclusion List**, select fields for the merge process to ignore. This excludes the fields and those 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.
8. Click **Save**.

Rank the order for merging assets

Any new asset list gets added to the bottom of the list by default. You can rank the order of this list to determine priority for merging assets. If an asset 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 asset fields are as follows:

- is_expected
- priority
- requires_av
- should_timesync
- should_update

These are the fields where the rank takes effect. For example, If you're merging two assets and they both have the is_expected 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 from the **Asset 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** field. The merge process combines all the values into the field, and then removes the duplicates.

Key fields are `dns`, `ip`, `mac`, and `nt_host`. If you store extra information in your key fields, such as the same IP address assigned to multiple systems, these duplicate IP addresses are now merged together as one asset. Make sure that the information in your key fields either belongs to the same asset or does not overlap.

Disable or enable asset lookups

You can disable or enable an asset lookup input. Disabling an input does not delete the data from the associated lookup from Splunk Enterprise Security. Disabling prevents the contents of the corresponding list from being included in the merge process. Enabling a disabled input allows the associated list to be merged at the next scheduled merge of the asset or identity data.

To disable an asset lookup, do the following from the **Asset Lookup Configuration** tab:

1. Navigate to the **Status** column.
2. Do one of the following options:
    - ♦ Click **Disable** to disable an input.
    - ♦ Click **Enable** to enable a disabled input.

Starting with version 5.0.0, asset and identity lookup inputs are disabled by default after a new installation. However, local settings are respected after an upgrade.

Modify asset lookups

Make changes to the asset lookups in Splunk Enterprise Security to add new assets 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 asset or 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 asset data

Manually add new static asset data to Splunk Enterprise Security by editing the Assets 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 asset data, click the **Assets** lookup 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_assets or static_identities or in **Configure > Data Enrichment > Asset and Identity Management**.

Disable the demo asset lookups

The demo asset lookups are disabled by default. Enable them if needed for testing. Disable the demo asset 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_assets lookups.
3. Click **Disable**.

Manage asset field settings in Splunk Enterprise Security

You can add a new asset field, enable case sensitive matching, revise multivalue field limits for assets.

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 asset field

Asset fields are added both by default and by entering custom fields manually. You can add up to 20 custom fields for your lookups. Default key fields are `dns`, `ip`, `mac`, `nt_host`. You can configure whether a field is a key field, a tag field, a multivalue field, or all of the above.

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

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Asset Settings** tab.
3. Click **Add New Field**.
4. In the **New Asset Field** dialog box, do the following:
    1. Enter a 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. The minimum number of key fields is one.
    3. 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.
    4. Check the **Multivalue** check box if the field can output multiple values.
    5. (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.
    6. Click **Save**.

The Save button is disabled when the limit is reached and is 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 `dns`, `ip`, `mac`, `nt_host`, you can edit the default key fields. To edit an asset field, do the following:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Asset Settings** 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.
    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 asset fields

Case sensitive matching is globally available across all fields.

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 that 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 **Asset Settings** tab.
3. Enable the **Enable case sensitive asset matching** switch.
4. Click **Update** to trigger the merge process and rewrite the `asset_lookup_by_str` and `asset_lookup_by_cidr` KV store collections.

Revise multivalue field limits for assets

The default number of multivalue asset fields that display after merging is 6 for key fields and 25 for non-key fields.

To revise multivalue field limits, perform the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Asset Settings** 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 a non-key multivalue field is 1 - 100. The field value range for a key multivalue field is 1 - 25. The reason that the default multivalue key field limit is 6 for assets is because there are 4 key fields. If each key field contains 6 values, the merge process results in an asset field with 24 key values. Performance issues can occur when a resulting asset field contains 25 key values. You can set a key multivalue field to 25, but performance issues can also occur if multiple key fields have 25 values.

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 key multivalue fields to 25, and non-key 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 to spread out those values so that they seem to be part of different assets, by making sure that there are no duplicate values in the key fields.

Key fields are `dns`, `ip`, `mac`, and `nt_host`. If you store extra information in your key fields, such as the same IP address assigned to multiple systems, these duplicate IP addresses are now merged together as one asset. Make sure that the information in your key fields either belongs to the same asset or does not overlap.

Example of revising multivalue field limits

As an example, you have a source CSV file that contains 9 values in the `mac` key field and 7 values in the `bunit` field, such as the following:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av
192.0.2.2,mac1|mac2|mac3|mac4|mac5|mac6|mac7|mac8|mac9,host1,dns1,owner1,,,,,,bunit1|bunit2|bunit3|bunit4|buni
t5|bunit6|bunit7,,,,,,
```

Using the default limit of 6 for the `mac` multivalue key field and revising the limit to 5 for the `bunit` multivalue field, these are merged into an asset where the `mac` key field values are truncated to 6 and the `bunit` non-key values are truncated to 5.

bunit	pci_domain	nt_host	ip	asset	asset_tag	mac	dns	owner
bunit1 bunit2 bunit3 bunit4 bunit5	untrust	host1	192.0.2.2	dns1 192.0.2.2 mac1 mac2 mac3 mac4 mac5 mac6 host1	bunit1 bunit2 bunit3 bunit4 bunit5	mac1 mac2 mac3 mac4 mac5 mac6 mac7 mac8 mac9	dns1	owner1

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 values from the KV store collections. This excludes the fields and those 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.

5. (Optional) Configure the conventions that the identity lookup can use to uniquely identify identities in your data. When an email convention check box is checked, the email address is used as an additional primary key for identity. The **Email** and **Email Short** conventions are 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**.

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 Settings** 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 Settings** 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

Case-sensitive matching is globally available across all fields.

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 Settings** 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 Settings** 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	medium	americas	3/2/88 2:39	3/8/01 6:21
dr.j	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-1554	medium	americas	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	medium	americas	3/2/88 2:39	3/8/01 6:21
Latoyia.Journot	Dr.	Latoyia	Journot	ljournot@acmetech.com		medium	americas	3/2/88 2:39	3/8/01 6:21

identity	prefix	first	last	email	phone	managedBy	priority	watchlist	startDate
					+1 (800)555-3481 | +1 (800)555-1556				
Latoyia.J	Dr.	Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3482 | +1 (800)555-1557	medium	americas	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	medium	americas	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	medium	americas	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	medium	americas	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	medium	americas	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
ljournot@acmetech.com	984050460.000000	3/2/88 2:39	journot	latoyia	medium	dr.	dr.l ljournot@acmetech.com ljournot l.journot latoyia.journot latoyia.j	americas

Manage correlation setup in Splunk Enterprise Security

When asset and identity correlation is enabled, Splunk Enterprise Security compares indexed events with asset and identity data in the asset and identity lists to provide data enrichment and context. The comparison process uses automatic lookups in the props.conf file. You can find information about automatic lookups in the Splunk platform documentation:

- For Splunk Enterprise, see Make your lookup automatic in the Splunk Enterprise *Knowledge Manager Manual*.
- For Splunk Cloud, see Make your lookup automatic in the Splunk Cloud *Knowledge Manager Manual*.
- See Modify priority and rank in the Asset and Identity Framework in the *Use Splunk Enterprise Security* manual for further information about how ranks, correlations, and automatic lookups affect notable event urgency.

Asset and identity correlation enriches events with asset and identity data at search time in the following ways:

- Asset correlation compares events that contain data in any of the `src`, `dest`, or `dvc` fields against the merged asset lists for matching IP address, MAC address, DNS name, or Windows NT host names. Asset correlation no longer occurs automatically against the `host` or `orig_host` fields.
- Identity correlation compares events that contain data in any of the `user` or `src_user` fields against the merged identity lists for a matching identity.
- Enterprise Security adds the matching output fields to the event. For example, correlation on the asset `src` field results in additional fields such as `src_is_expected` and `src_should_timesync`.

Asset and identity correlation lets you determine whether multiple events can relate to the same asset or identity. You can also perform actions on the identity and asset fields added to events to open additional searches or dashboards scoped to the specific asset or identity. For example, you can open the Asset Investigator dashboard on a `src` field.

You can choose from the following options:

- Disable for all sourcetypes
- Enable selectively by sourcetype
- (Not available for for Splunk Cloud) Enable for all sourcetypes

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.

Disable correlation for all sourcetypes

Disabling asset and identity correlation completely prevents events from being enriched with asset and identity data from the asset and identity lookups. This might prevent correlation searches, dashboards, and other functionality from working as expected. Consult with Splunk Professional Services or Splunk Support before disabling asset and identity correlation. If in doubt, keep asset and identity correlation enabled.

To disable correlation for all sourcetypes, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Disable for all sourcetypes** radio button.
4. Click **Save**.

Enable correlation selectively by sourcetype

Enable correlation selectively by sourcetype if you know the specific sourcetypes and corresponding lookups that you need for populating your correlation searches, dashboards, and other functionality. To enable correlation selectively by sourcetype, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Enable selectively by Source Type** radio button.
4. To add asset sourcetypes, navigate to **Add Asset Sourcetypes** and do one of the following:
    - Click the drop-down menu and check the checkbox for each existing sourcetype to add.
    - Type free-form text for the name of a sourcetype that you plan to add later.
5. To add identity sourcetypes, navigate to **Add Identity Source Types** and do one of the following:
    - Click the drop-down menu and check the checkbox for each existing sourcetype to add.
    - Type free-form text for the name of a sourcetype that you plan to add later.
6. Click **Save**.

Enable correlation for all sourcetypes

Enable correlation for all sourcetypes for ease of management if you don't have performance concerns and if you don't know specifically which sourcetypes you need for populating your correlation searches, dashboards, and other functionality. To enable correlation for all sourcetypes, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Enable for all sourcetypes** radio button.
4. Click **Save**.

Enable correlation and entity zones

When correlation and entity zones are both enabled, the `cim_entity_zone` field is used to find the correct asset in the correct zone. Identifying the correct asset in the correct zone enables you to more accurately enrich your search results and notable events fields. For details about entity zones, see Enable entity zones for Assets or Identities.

Using assets as an example, consider the following source file with the same `ip`, `mac`, and `nt_host` in different zones:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av,cim_entity _zone
192.0.2.94,00:00:5e:16:a7:7a,host,splunk.com,owner1,priority1,,,city1,country1,bunit1,,,,,,,zone1
192.0.2.94,00:00:5e:16:a7:7a,host,splunk.com,owner2,priority2,,,city2,country2,bunit2,,,,,,,zone2
```

With entity zones enabled, the behavior is not to merge key fields such as `ip`, `mac`, and `nt_host` that are in different zones.

You may use the search preview for **asset_lookup_by_str** that returns results as shown in the following table:

asset	cim_entity_zone	ip	mac	nt_host	dns	owner	priority	city	country	bunit
00:00:5e:16:a7:7a host	zone1	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner1	priority1	city1	country1	bunit1
	zone2	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner2	priority2	city2	country2	bunit2

asset	cim_entity_zone	ip	mac	nt_host	dns	owner	priority	city	country	bunit
00:00:5e:16:a7:7a host										

For more information on how to use the search preview to test the merge of assets and identities, see Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security.

With correlation and entity zones both enabled, search results are displayed with the events enriched by the `cim_entity_zone` field.

The following search:

```
index="main" sourcetype="sourcetype_you_enabled_for_correlation"
```

displays the following search results:

i	Time	Event
>	6/9/2020 6:06:05.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone1" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1" dvc_priority="priority1" dvc_country="country1" dvc_city="city1" dvc_bunit="bunit1" asset_tag="bunit1" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"
>	6/9/2020 7:06:07.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone2" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner2" dvc_priority="priority2" dvc_country="country2" dvc_city="city2" dvc_bunit="bunit2" asset_tag="bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"

The results display two devices of 192.0.2.94 in two different `cim_entity_zone` zones with events that occurred an hour apart. The `cim_entity_zone` field is used to find the correct asset in the correct zone.

Disable entity zones

When entity zones are disabled, With entity zones disabled, the default behavior is to merge by the key fields, such as `ip`, `mac`, and `nt_host`.

You may use the search preview for **asset_lookup_by_str** that returns results as shown in the following table:

asset	ip	mac	nt_host	dns	owner	priority	city	country	bunit	asset_tag
00:00:5e:16:a7:7a host	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner1 owner2	priority2	city1 city2	zone1_country zone2_country	bunit1 bunit2	bunit1 bunit2

For more information on how to use the search preview to test the merge of assets and identities, see Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security.

With correlation and entity zones both disabled, the merged search results are displayed with the events that are not enriched by the `cim_entity_zone` field.

The following search:

```
index="main" sourcetype="sourcetype_you_enabled_for_correlation"
```

displays the following search results: The results display the same device 192.0.2.94 enriched with the same multivalue fields in events that occurred an hour apart. The `cim_entity_zone` field is in the raw event (if defined). However, with entity zones disabled, it is not used in correlation searches, saved searches, or dashboards.

i	Time	Event
>	6/9/2020 6:06:05.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone1" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1 | owner2" dvc_priority="priority2" dvc_country="country1 | country2" dvc_city="city1 | city2" dvc_bunit="bunit1 | bunit2" asset_tag="bunit1 | bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"
>	6/9/2020 7:06:07.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone2" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1 | owner2" dvc_priority="priority2" dvc_country="country1 | country2" dvc_city="city1 | city2" dvc_bunit="bunit1 | bunit2" asset_tag="bunit1 | bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"

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. From each drop-down list, 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 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.

Asset and Identity Validation

Verify that your asset and identity data was added to Splunk Enterprise Security

Verify that your asset or identity data was added to Splunk Enterprise Security by searching and viewing dashboards.

Prerequisites

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.
4. Manage assets and identities in Splunk Enterprise Security.

Steps

Verify asset lookup data.

1. Verify that a specific asset record exists in the asset lookup.
    1. Choose an asset record with data in the `ip`, `mac`, `nt_host`, or `dns` fields from an asset list.
    2. Search for it in Splunk Web.

```
| makeresults | eval src="1.2.3.4" | `get_asset(src)`
```

- View all available assets in your instance using one of the following methods. Compare the number of rows with your asset data sources to verify the number of asset records matches your expectations, or spot check specific records.
    - View the Asset Center dashboard. See Asset Center dashboard in *Use Splunk Enterprise Security.*.
    - Use the assets macro.

```
| `assets`
```

- Search the data model.

```
|`datamodel("Identity_Management", "All_Assets")` |`drop_dm_object_name("All_Assets")`
```

Verify identity lookup data.

1. Verify that a specific identity record exists in the identity lookup.
    1. Choose an identity record with data in the `identity` field.
    2. Search for it in Splunk Web.

```
| makeresults | eval user="VanHelsing" | `get_identity4events(user)`
```

- View all available identities in your instance using one of the following methods. Compare the number of rows with your identity data sources to verify the number of identity records matches your expectations, or spot check specific records.
    - View the Identity Center dashboard. See Identity Center dashboard in *Use Splunk Enterprise Security*.
    - Use the identities macro.

```
| `identities`
```

- Search the data model.

```
|`datamodel("Identity_Management", "All_Identities")` |`drop_dm_object_name("All_Identities")`
```

How Splunk Enterprise Security processes and merges asset and identity data

Splunk Enterprise Security takes the asset and identity data that you add as lookups and generates combined lookup files. Splunk Enterprise Security uses the generated lookup files to correlate asset and identity data with events using automatic lookups. The following steps describe this process at a high level.

1. You collect asset and identity data from data sources using an add-on and a custom search or manually with a CSV file. See Collect and extract asset and identity data.
2. The Splunk Enterprise Security identity manager modular input updates settings in the `transforms.conf` stanza `identity_lookup_expanded`.
3. You format the data as a lookup, using a search or manually with a CSV file. See Format the asset or identity list as a lookup.
4. You configure the list as a lookup table, definition, and input. See Configure a new asset or identity list.
5. You create an identity lookup configuration. See Create an identity lookup configuration.
6. The Splunk Enterprise Security identity manager modular input detects two things:
   - Changed size of the CSV source file.
   - Changed update time of the CSV source file.
7. The Splunk Enterprise Security identity manager modular input updates the macros used to identify the input sources based on the currently enabled stanzas in `inputs.conf`.
8. The Splunk Enterprise Security identity manager modular input dispatches custom dynamic searches if it identifies changes that require the asset and identity lists to be merged.
9. The custom search dispatches a merge process to merge all configured and enabled asset and identity lists.
10. The custom searches concatenate the lookup tables referenced by the identity manager input, generate new fields, and output the concatenated asset and identity lists into target lookup table files: asset_lookup_by_str, asset_lookup_by_cidr, identity_lookup_expanded.
11. You verify that the data looks as expected. See Verify that your asset or identity data was added to Splunk Enterprise Security.

The merging of identity and asset lookups does not validate or de-duplicate input. Errors from the identity manager modular input are logged in `identity_manager.log`. This log does not show data errors.

Lookups that store merged asset and identity data in Splunk Enterprise Security

After the asset and identity merging process completes, four lookups store your asset and identity data.

Current

Function	Table name	Lookup name
String-based asset correlation	assets_by_str KV store collection	LOOKUP-zu-asset_lookup_by_str-dest LOOKUP-zu-asset_lookup_by_str-dvc LOOKUP-zu-asset_lookup_by_str-src
CIDR subnet-based asset correlation	assets_by_cidr KV store collection	LOOKUP-zv-asset_lookup_by_cidr-dest LOOKUP-zv-asset_lookup_by_cidr-dvc LOOKUP-zv-asset_lookup_by_cidr-src

Function	Table name	Lookup name
String-based identity correlation	identities_expanded KV store collection	LOOKUP-zy-identity_lookup_expanded-src_user LOOKUP-zy-identity_lookup_expanded-user
Default field correlation	identity_lookup_default_fields.csv asset_lookup_default_fields.csv	LOOKUP-zz-asset_identity_lookup_default_fields-dest LOOKUP-zz-asset_identity_lookup_default_fields-dvc LOOKUP-zz-asset_identity_lookup_default_fields-src LOOKUP-zz-asset_identity_lookup_default_fields-src_user LOOKUP-zz-asset_identity_lookup_default_fields-user

The main difference now is that three out of four tables are migrated from .csv files to KV store, and can store custom fields. The default field correlation is not migrated over to KV store at this time. The automatic lookups still remain in `props.conf`.

5.3.1 and earlier

Function	Table name	Saved search	Lookup name
String-based asset correlation	assets_by_str.csv	Identity - Asset String Matches - Lookup Gen	LOOKUP-zu-asset_lookup_by_str-dest LOOKUP-zu-asset_lookup_by_str-dvc LOOKUP-zu-asset_lookup_by_str-src
CIDR subnet-based asset correlation	assets_by_cidr.csv	Identity - Asset CIDR Matches - Lookup Gen	LOOKUP-zv-asset_lookup_by_cidr-dest LOOKUP-zv-asset_lookup_by_cidr-dvc LOOKUP-zv-asset_lookup_by_cidr-src
String-based identity correlation	identities_expanded.csv	Identity - Identity Matches - Lookup Gen	LOOKUP-zy-identity_lookup_expanded-src_user LOOKUP-zy-identity_lookup_expanded-user
Default field correlation	identity_lookup_default_fields.csv asset_lookup_default_fields.csv		LOOKUP-zz-asset_identity_lookup_default_fields-dest LOOKUP-zz-asset_identity_lookup_default_fields-dvc LOOKUP-zz-asset_identity_lookup_default_fields-src LOOKUP-zz-asset_identity_lookup_default_fields-src_user LOOKUP-zz-asset_identity_lookup_default_fields-user

Asset and identity fields after processing in Splunk Enterprise Security

The following tables describe the fields that exist in the asset and identity lookups after Splunk Enterprise Security finishes processing the source lookup files. These fields are the fields present in the lookups that store merged asset and identity data. See Lookups that store merged asset and identity data in Splunk Enterprise Security.

The tables below list the default asset and identity fields in the KV store collections after the merge process completes. However, take note that it is possible to revise fields from multivalue to single, and tag or untag fields. It is also possible to add custom fields.

Asset fields after processing

Asset fields of the asset lookup after the saved searches perform the merge process.

Field	Action taken by ETL
bunit	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
city	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.

Field	Action taken by ETL
country	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
dns	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
lat	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
long	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
mac	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
nt_host	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
owner	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
priority	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
asset_id	Generated from the values of dns, ip, mac, and nt_host fields. Accepts all values and converts them to a multivalue field.
asset_tag	By default, generated from the values of category, pci_domain, is_expected, should_timesync, should_update, requires_av, and bunit fields. Also custom generated from assets that have been tagged. See Asset Settings.
category	Appends "pci" if the value contains "cardholder". Accepts all values and converts them to a multi-value field.
ip	Validates and splits the field into CIDR subnets as necessary. Accepts all values and converts them to a multi-value field.
pci_domain	Appends "trust" or "untrust" based on certain field values. Accepts all values and converts them to a multi-value field.
is_expected	Normalized to a boolean. Accepts all values and converts them to a multivalue field.
should_timesync	Normalized to a boolean. Accepts all values and converts them to a multivalue field.
should_update	Normalized to a boolean. Accepts all values and converts them to a multivalue field.
requires_av	Normalized to a boolean. Accepts all values and converts them to a multivalue field.
key	Generated by the ip, mac, nt_host, and dns fields after the original fields are transformed. Accepts all values and converts them to a multivalue field.
cim_entity_zone	Not processed if entity zones are disabled.

Identity fields after processing

Identity fields of the identity lookup after the saved searches perform the merge process.

Field	Action taken by ETL
bunit	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
email	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
endDate	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.

Field	Action taken by ETL
first	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
last	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
managedBy	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
nick	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
phone	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
prefix	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
priority	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
startDate	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
suffix	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
work_city	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
work_country	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
work_lat	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
work_long	Unchanged if configured as a single value field. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
watchlist	Normalized to a boolean. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
category	Appends "pci" if the value contains "cardholder". Accepts all values and converts them to a multi-value field.
identity	Generated based on values in the input row and conventions specified in the Identity Lookup Configuration. Accepts all values and converts them to a multi-value field.
identity_id	Generated from the values of identity, first, last, and email. Accepts all values and converts them to a multivalue field if configured as a multivalue field.
identity_tag	By default, generated from the values of bunit, category, and watchlist. Also custom generated from assets that have been tagged. See Identity Settings.
cim_entity_zone	Not processed if entity zones are disabled.

Overwrite asset or identity data with entitymerge in Splunk Enterprise Security

After you add assets and identities to Splunk Enterprise Security, you can use the `entitymerge` command to merge or overwrite asset or identity data based on matched foreign keys. See Add asset and identity data to Splunk Enterprise Security.

Description

Use the `entitymerge` command to merge or overwrite asset or identity data based on matched foreign keys. Primarily, you use it by default in the Search Preview tab of Asset and Identity Management. You can use it manually for debugging. See Search Preview.

Syntax

entitymerge <entitymerge-target>

Required arguments

entitymerge-target

> **Syntax:** [asset|identity]
> **Description:** Required target of the entitymerge command.

Example

You can see examples of the `entitymerge` command in the Search Preview tab of Asset and Identity Management.

One example is the search preview for **asset_lookup_by_str**, the asset table that uses string matching to enrich events:

```
| `add_entity_source("demo_asset_lookup","demo_assets")` |
`add_entity_source("frothly_assets_2018","frothly_assets_2018")` |
`add_entity_source("seckit_idm_assets_aws_ec2","frothly_aws_assets_2018")` |
`add_entity_source("simple_asset_lookup","static_assets")` | table "_source","cim_entity
_zone","bunit","category","city","country","dns"," ip","is_expected","lat","long","mac","nt
_host","owner","pci_domain","priority","requires_av","should _timesync","should_update" | `make_ip_str` |
inputlookup append=T "asset_lookup_by_str" | entitymerge "asset"
```

Threat Intelligence

Add threat intelligence to Splunk Enterprise Security

As an ES administrator, you can correlate indicators of suspicious activity, known threats, or potential threats with your events by adding threat intelligence to Splunk Enterprise Security. Adding threat intelligence enhances your analysts' security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a selection of threat intelligence sources. Splunk Enterprise Security also supports multiple types of threat intelligence so that you can add your own threat intelligence.

ES administrators can add threat intelligence to Splunk Enterprise Security by downloading a feed from the Internet, uploading a structured file, or inserting the threat intelligence directly from events in Splunk Enterprise Security.

Prerequisite

Review the types of threat intelligence that Splunk Enterprise Security supports. See Supported types of threat intelligence in Splunk Enterprise Security.

Steps

1. Configure the threat intelligence sources included with Splunk Enterprise Security.
2. For each additional threat intelligence source not already included with Splunk Enterprise Security, follow the procedure to add threat intelligence that matches the source and format of the intelligence that you want to add.
    - Download a threat intelligence feed from the Internet
    - Upload a STIX or OpenIOC structured threat intelligence file
    - Upload a custom CSV file of threat intelligence
    - Add threat intelligence from Splunk events in Splunk Enterprise Security
    - Add and maintain threat intelligence locally in Splunk Enterprise Security
    - Add threat intelligence with a custom lookup file in Splunk Enterprise Security
3. Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

See also

Change existing threat intelligence in Splunk Enterprise Security

Add threat intelligence with an adaptive response action.

Threat Intelligence API reference in *REST API Reference*.

Threat Intelligence framework in Splunk ES on the Splunk developer portal

Supported types of threat intelligence in Splunk Enterprise Security

Splunk Enterprise Security supports several types of threat intelligence. The supported types of threat intelligence correspond to the KV Store collections in which the threat intelligence is stored.

The threat intelligence manager modular input parses downloaded and uploaded files and adds indicators to these collections. Files can contain any combination of indicators.

Threat collection in KV Store	Supported IOC data types	Local lookup file	Required headers in lookup file with no spaces after commas
certificate_intel	X509 Certificates	Local Certificate Intel	`certificate_issuer,certificate_subject,certificate_issuer_organization,certificat _organization,certificate_serial,certificate_issuer_unit,certificate_subject_unit`
email_intel	Email	Local Email Intel	`description,src_user,subject,weight`
file_intel	File names or hashes	Local File Intel	`description,file_hash,file_name,weight`
http_intel	URLs	Local HTTP Intel	`description,http_referrer,http_user_agent,url,weight`
ip_intel	IP addresses	Local IP Intel	`description,ip,weight`
	domains	Local Domain Intel	`description,domain,weight`
process_intel	Processes	Local Process Intel	`description,process,process_file_name,weight`
registry_intel	Registry entries	Local Registry Intel	`description,registry_path,registry_value_name,registry_value_text,weight`
service_intel	Services	Local Service Intel	`description,service,service_file_hash,service_dll_file_hash,weight`
user_intel	Users	Local User Intel	`description,user,weight`

The `collections.conf` file in the `DA-ESS-ThreatIntelligence` subdirectory lists these KV Store collections.

The `inputs.conf.spec` file in the `SA-ThreatIntelligence` subdirectory lists the specifications for headers, such as weight:

```
weight = <integer>
* [Required]
* The weight assigned to the intelligence.
* Between 1 and 100.
* A higher weight will result in higher risk scores for corresponding intelligence matches.
* Defaults to 60.
```

Configure the intelligence sources included with Splunk Enterprise Security

Splunk Enterprise Security includes several intelligence sources that retrieve information across the Internet.

None of these intelligence sources are enabled by default. Review the types of intelligence provided by the sources, and determine if the included intelligence is useful to your team before enabling specific sources.

Prerequisites

- Your Splunk Enterprise deployment must be connected to the Internet. If your deployment is not connected to the Internet, disable these sources or source them in an alternate way.
- To set up firewall rules for these sources, you might want to use a proxy server to collect the intelligence before forwarding it to Splunk Enterprise Security and allow the IP address for the proxy server to access Splunk Enterprise Security. The IP addresses for these sources can change.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Review the **Description** field for all defined intelligence sources to learn more about the types of information or threat indicators that can be correlated with your events.
3. Enable the intelligence sources that fit your security use cases.
4. Configure the enabled intelligence sources that fit your security use cases, using the links to the source websites to review the source provider's documentation. Each source website provides suggestions for polling intervals and other configuration requirements separate from Splunk Enterprise Security.

Splunk Enterprise Security expects all intelligence sources to send properly-formatted data and valuable intelligence information. Feed providers are responsible for malformed data or false positives that might be identified in your environment as a result.

If you determine that your Splunk Enterprise Security installation is retrieving data from unexpected IP addresses, perform a WHOIS or nslookup to determine if the IP address matches that of one of the intelligence sources configured in your environment.

Next step

To add a custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding intelligence sources, see Verify that you have added intelligence successfully in Splunk Enterprise Security.

Included threat intelligence sources

The threat intelligence sources are parsed for threat indicators and added to the relevant KV Store collections.

Threat source	Threat list provider	Website for the threat source
Emerging Threats compromised IPs blocklist	Emerging Threats	https://rules.emergingthreats.net/blockrules
Emerging Threats firewall IP rules	Emerging Threats	https://rules.emergingthreats.net/fwrules
Malware domain host list	Hail a TAXII.com	http://hailataxii.com
iblocklist Logmein	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Piratebay	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Proxy	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Rapidshare	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Spyware	I-Blocklist	https://www.iblocklist.com/lists

Threat source	Threat list provider	Website for the threat source
iblocklist Tor	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Web attacker	I-Blocklist	https://www.iblocklist.com/lists
Malware Domain Blocklist	Malware Domains	https://mirror1.malwaredomains.com
abuse.ch Palevo C&C IP Blocklist	abuse.ch	https://palevotracker.abuse.ch
Phishtank Database	Phishtank	https://www.phishtank.com/
SANS blocklist	SANS	https://isc.sans.edu
abuse.ch ZeuS blocklist (bad IPs only)	abuse.ch	https://zeustracker.abuse.ch
abuse.ch ZeuS blocklist (standard)	abuse.ch	https://zeustracker.abuse.ch

Included generic intelligence sources

Splunk Enterprise Security also includes generic intelligence that is not added to the threat intelligence KV Store collections and are instead used to enrich data in Splunk Enterprise Security.

Data list	Data provider	Website for data provider
Cisco Umbrella 1 Million Sites	Cisco	https://umbrella.cisco.com/blog/2016/12/14/cisco-umbrella-1-million/
Alexa Top 1 Million Sites	Alexa Internet	https://s3.amazonaws.com/alexa-static
ICANN Top-level Domains List	IANA	https://data.iana.org/TLD/
MaxMind GeoIP ASN IPv4 database	MaxMind	https://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database/
MaxMind GeoIP ASN IPv6 database	MaxMind	https://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database/
Mozilla Public Suffix List	Mozilla	https://publicsuffix.org

You can configure the generic intelligence source to use for top one million sites:

1. From the Splunk ES menu bar, select **Configure** > **General** > **General Settings**
2. Scroll down to Top 1M Site Source and select **Cisco**.

Download a threat intelligence feed from the Internet in Splunk Enterprise Security

Splunk Enterprise Security can periodically download a threat intelligence feed available from the Internet, parse it, and add it to the relevant KV Store collections.

1. (Optional) Configure a proxy for retrieving threat intelligence.
2. Follow the procedure that matches the format of the threat source:
   - Add a URL-based threat source
   - Add a TAXII feed

If you manually disable a threat artifact in a collection, but the threat intelligence source provides the same indicator in a download again, then the entry in KVStore gets overwritten, and does not preserve your flag.

Configure a proxy for retrieving threat intelligence

If you use a proxy server to send threat intelligence to Splunk Enterprise Security, configure the proxy options for the threat source.

The user must correspond to the name of a Splunk secure stored credential in Credential Management. If you remove an existing proxy user and password in the Intelligence Download Setting editor, the download process no longer references the stored credentials. Removing the reference to the credential does not delete the stored credentials from Credential Management. See Manage credentials in Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment > Intelligence Downloads**.
2. Select the threat download source or add a new threat download source. See Add a URL-based threat source or Add a TAXII feed.
3. Configure the proxy options.
    1. Type a proxy server address. The **Proxy Server** cannot be a URL. For example, `10.10.10.10` or `server.example.com`.
    2. Type a proxy server port to use to access the proxy server address.
    3. Type a proxy user credential for the proxy server. Only basic and digest authentication methods are supported. The user must correspond to the name of a credential stored in Credential Management.
    4. (Optional) Type a proxy user realm for the proxy user credential. Use this to specify a proxy user realm for the user credential.
4. Save your changes.

Add a URL-based threat source

Add a non-TAXII source of intelligence that is available from a URL on the Internet. For an example of adding a URL-based threat intelligence source, see Example: Add a ransomware threat feed to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Click **New** to add a new intelligence source.
3. Type a **Name** for the threat download. The name can only contain alphanumeric characters, hyphens, and underscores. The name cannot contain spaces.
4. Select or deselect the check box for **Is Threat Intelligence**.
5. (Optional) Select or deselect the check box for **Sinkhole**. Select the check box to delete the downloaded file after processing.
6. Type a **Type** for the threat download. The type identifies the type of threat indicator that the feed contains.
7. Type a **Description**. Describe the indicators in the threat feed.
8. Type an integer to use as the **Weight** for the threat indicators. Enterprise Security uses the weight of a threat feed to calculate the risk score of an asset or identity associated with an indicator on the threat feed. A higher weight indicates an increased relevance or an increased risk to your environment.
9. (Optional) Change the default download **Interval** for the threat feed. Defaults to 43200 seconds, or every 12 hours.
10. (Optional) Type POST arguments for the threat feed. You can use POST arguments to retrieve user credentials from Credential Management. Use the format `key=$user:<username>$` or `key=$user:<username>,realm:<realm>$` to specify a username and realm.
11. (Optional) Type a **Maximum age** to define the retention period for this threat source, defined in relative time. Enable the corresponding saved searches for this setting to take effect. See Configure threat source retention. For example, `-7d`. If the time that the feed was last updated is greater than the maximum age defined with this setting, the threat intelligence modular input removes the data from the threat collection.
12. (Optional) If you need to specify a custom **User agent** string to bypass network security controls in your environment, type it in the format `<user-agent>/<version>`. For example, `Mozilla/5.0` or `AppleWebKit/602.3.12`.

The value in this field must match this regex: `([A-Za-z0-9_.-]+)/([A-Za-z0-9_.-]+)`. Check with your security device administrator to ensure the string you type here is accepted by your network security controls.

13. Fill out the **Parsing Options** fields to make sure that your threat list parses successfully. You must fill out either a delimiting regular expression or an extracting regular expression. You cannot leave both fields blank.

Field	Description	Example
Delimiting regular expression	A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.	`,` or `:` or `\t`
Extracting regular expression	A regular expression used to extract fields from individual lines of a threat source document. Use to extract values in the threat source.	`^(\S+)\t+(\S+)\t+\S+\t+\S+\t*(\S*)`

Fields	Required if your document is line-delimited. Comma-separated list of fields to be extracted from the threat list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the `DA-ESS-ThreatIntelligence/collections.conf` file. Defaults to `description:$1,ip:$2`.	`<fieldname>:$<number>,<field name>.$<number>`
		`ip:$1,description:domain_blocklist`

Ignoring regular expression	A regular expression used to ignore lines in a threat source. Defaults to ignoring blank lines and comments beginning with #.	`^\s*$)`
Skip header lines	The number of header lines to skip when processing the threat source.	`0`
Intelligence file encoding	If the file encoding is something other than ASCII or UTF8, specify the encoding here. Leave blank otherwise.	latin1

14. (Optional) Change the **Download Options** fields to make sure that your threat list downloads successfully.

Field	Description	Example
Retry interval	Number of seconds to wait between download retry attempts. Review the recommended poll interval of the threat source provider before changing the retry interval.	60
Remote site user	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The user name you add in this field must match the name of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	buttercup
Remote site user realm	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The realm you add in this field must match the realm of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	paddock
Retries	The maximum number of retry attempts.	3
Timeout	Number of seconds to wait before marking a download attempt as failed.	30

15. (Optional) If you are using a proxy server, fill out the **Proxy Options** for the threat feed. See Configure a proxy for retrieving threat intelligence.
16. Save your changes.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add a TAXII feed

Add threat intelligence provided as a TAXII feed to Splunk Enterprise Security.

Prerequisite

Determine whether the TAXII feed requires certificate authentication. If it does, add the certificate and keys to the same app directory in which you define the TAXII feed. For example, DA-ESS-ThreatIntelligence.

1. Follow the steps to add a new certificate to Splunk Enterprise Security to add both the certificate and the private key files. See Manage credentials in Splunk Enterprise Security.
2. Follow the steps for adding a TAXII feed to Splunk Enterprise Security, using the `cert_file` and `key_file` POST arguments to specify the file names of the certificate and private key file.

Steps

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment > Intelligence Downloads**.
2. Click **New** to add a new TAXII feed.
3. Type a **Name** for the threat intelligence feed.
4. Select the check box for **Is Threat Intelligence**.
5. (Optional) Select or deselect the check box for **Sinkhole**. Select the check box to delete the downloaded file after processing. The sinkhole option works for anything in the pickup directory that has been processed. The pickup directories follow:
   ```
   $SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel
   $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel
   $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel
   $SPLUNK_HOME/etc/apps/<custom>
   ```
6. Type a **Type** of **taxii**.
7. Type a **Description** for the threat intelligence feed.
8. Type a URL to use to download the TAXII feed.
9. (Optional) Change the default **Weight** for the threat intelligence feed. Increase the weight if the threats on the threat feed are high-confidence and malicious threats that should increase the risk score for assets and identities that interact with the indicators from the threat source.
10. (Optional) Adjust the interval at which to download the threat intelligence. Defaults to 43200 seconds, or twice a day.
11. Type TAXII-specific space-delimited **POST arguments** for the threat intelligence feed.
    ```
    <POST argument>="<POST argument value>"
    ```

Example POST argument	Description	Example
collection	Name of the data collection from a TAXII feed.	`collection="A_TAXII_Feed_Name"`
earliest	The earliest threat data to pull from the TAXII feed.	`earliest="-1y"`
taxii_username	An optional method to provide a TAXII feed username.	`taxii_username="user"`
taxii_password	An optional method to provide a TAXII feed password. If you provide a username without providing a password, the threat intelligence modular input attempts to find the password in Credential Management. See Manage credentials in Splunk Enterprise Security.	`taxii_password="password"`
taxii_username_realm	An optional method to provide a realm for the TAXII feed username. Used with the `taxii_username` to locate the user credential password in Credential Management.	`taxii_username_realm="realm"`

Example POST argument	Description	Example
cert_file	Add the certificate file name if the TAXII feed uses certificate authentication. The file name must match exactly and is case sensitive.	`cert_file="cert.crt"`
key_file	Add the key file name for the certificate if the TAXII feed uses certificate authentication. The file name must match exactly and is case sensitive.	`key_file="cert.key"`

12. TAXII feeds do not use the **Maximum age** setting. To configure file retention for TAXII files, see Configure intelligence file retention.
13. TAXII feeds do not use the **User agent** setting.
14. TAXII feeds do not use the **Parsing Options** settings.
15. (Optional) Change the **Download Options**.
16. (Optional) Change the **Proxy Options**. See Configure a proxy for retrieving threat intelligence.
17. Save the changes.

You cannot use an authenticated proxy with a TAXII feed because the libtaxii library used by Enterprise Security does not support authenticated proxies. If possible, use an unauthenticated proxy instead.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security

Upload threat intelligence in a STIX or OpenIOC file to Splunk Enterprise Security using one of the following methods:

- Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface
- Add STIX or OpenIOC files using the REST API
- Add STIX or OpenIOC files using the file system

Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface

Splunk Enterprise Security supports adding the following file types directly in the Splunk Enterprise Security interface:

- OpenIOC 1.0 and 1.1
- STIX 1.0, 2.0, and 2.1
- CSV

To add a file in the Splunk Enterprise Security interface, complete the following steps:

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Threat Intelligence Uploads**.

2. Type a file name for the file you want to upload. The file name you type becomes the name of the file saved to `$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel`. The file name cannot include spaces or special characters.
3. Upload an OpenIOC or STIX-formatted file.
4. Type a **Weight** for the threat intelligence file. The weight of a threat intelligence file increases the risk score of objects associated with threat intelligence on this list.
5. (Optional) Type a **Threat Category**. If you leave this field blank and a category is specified in the OpenIOC or STIX file, Splunk Enterprise Security uses the threat category specified in the file.
6. (Optional) Type a **Threat Group**. If you leave this field blank and a group is specified in the OpenIOC or STIX file, Splunk Enterprise Security uses the threat group specified in the file.
7. (Optional) Select the **Overwrite** check box. If you have previously uploaded a file with the same file name, select this check box to overwrite the previous version of the file.
8. (Optional) Select the **Sinkhole** check box. This deletes the file after the intelligence from the file is processed.
9. Click **Save**.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add STIX or OpenIOC files using the REST API

The Splunk Enterprise Security REST API supports uploading threat intelligence files in OpenIOC, STIX, or CSV format. See Threat Intelligence API reference.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add STIX or OpenIOC files using the file system

You can also add threat intelligence to Splunk Enterprise Security by adding a properly-formatted file to a file system folder.

1. Add a STIX-formatted file with a `.xml` file extension or an OpenIOC file with a `.ioc` file extension to the `$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel` folder on your Splunk Enterprise Security search head or make it available to that file directory on a mounted local network share. The `.ioc` file extension is not required.
2. By default, the `da_ess_threat_local` modular input processes those files and places the threat intelligence found in the relevant KV Store collections.
3. By default, after processing the intelligence in the files, the modular input deletes the files because the sinkhole setting is enabled by default.

Change the da_ess_threat_local inputs settings

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Threat Intelligence Management**.
2. Click the `da_ess_threat_local` modular input.
3. Review or change the settings as required.

Do not change the default `da_ess_threat_default` input.

Configure a custom folder and input monitor for threat sources

You can also add threat intelligence to Splunk Enterprise Security by adding a properly-formatted file to a custom file directory. The file directory must match the pattern `$SPLUNK_HOME/etc/apps/<app_name>/local/data/<directory_name>`, and you must create an input monitor to monitor that file directory for threat intelligence.

Create an input monitor for threat sources to add threat intelligence to a different folder than the one monitored by the **da_ess_threat_local** modular input.

1. From the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Threat Intelligence Management**.
2. Click **New**
3. Type a descriptive name for the modular input. The name cannot include spaces.
4. Type a path to the file repository. The file repository must be `$SPLUNK_HOME/etc/apps/<app_name>/local/data/<directory_name>`
5. (Optional) Type a maximum file size in bytes.
6. (Optional) Select the **Sinkhole** check box. If selected, the modular input deletes each file in the directory after processing the file.
7. (Optional) Select the **Remove Unusable** check box. If selected, the modular input deletes a file after processing it if it has no actionable threat intelligence.
8. (Optional) Type a number to use as the default weight for all threat intelligence documents consumed from this directory.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Upload a custom CSV file of threat intelligence in Splunk Enterprise Security

You can add a custom file of threat intelligence to Splunk Enterprise Security.

Prerequisite

Format the custom CSV file by adding headers for each type of intelligence in the file. The custom file can contain multiple types of intelligence, but you must include headers for each column in the CSV file. See Supported types of threat intelligence in Splunk Enterprise Security for the headers relevant for each type of threat intelligence.

Add the custom file to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Threat Intelligence Uploads**.
2. Type a file name for the file you want to upload. The file name you type becomes the name of the file saved to `$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel`. The file name cannot include spaces or special characters.
3. Upload the CSV-formatted file.
4. Type a **Weight** for the threat list. The weight of a threat file increases the risk score of objects associated with threat intelligence on this list.
5. (Optional) Type a **Threat Category**.
6. (Optional) Type a **Threat Group**.
7. (Optional) Select the **Overwrite** check box. If you have previously uploaded a file with the same file name, select this check box to overwrite the previous version of the file.
8. (Optional) Select the **Sinkhole** check box. This deletes the file after the intelligence from the file is processed.
9. Click **Save**.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add threat intelligence from Splunk events in Splunk Enterprise Security

You can add threat intelligence from Splunk events to the local threat intelligence lookups.

1. Write a search that produces threat indicators.
2. Add `| outputlookup local_<threat intelligence type>_intel append=t` to the end of the search.

For example, write a search that produces a list of IP addresses that are testing a web server for vulnerabilities and add them to the `local_ip_intel` lookup to be processed by the modular input and added to the `ip_intel` KV Store collection.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add and maintain threat intelligence locally in Splunk Enterprise Security

Each threat collection has a local lookup file that you can use to manually add threat intelligence.

1. On the Enterprise Security menu bar, select **Configure** > **Content** > **Content Management**.
2. Find the local lookup that matches the type of threat indicator you want to add. For example, **Local Certificate intel** to add information about malicious or spoofed certificates.
3. Click the lookup name to edit the lookup.
4. Add indicators to the lookup. Right-click and select **Insert Row Below** to add new rows as needed.

5. (Optional) Type a numeric **Weight** to change the risk score for objects associated with indicators on this threat intelligence source.
6. Click **Save**.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add threat intelligence with a custom lookup file in Splunk Enterprise Security

You can add threat intelligence to Splunk Enterprise Security as a custom lookup file. Add a custom lookup file in this way if you want to edit the lookup file in Splunk Enterprise Security. If you want to add a lookup file to have the intelligence in it extracted once, upload the CSV file instead. See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security.

A lookup-based threat source can add data to any of the supported threat intelligence types, such as file or IP intelligence. See Supported types of threat intelligence in Splunk Enterprise Security.

Prerequisite

Create the custom CSV file. The custom file can contain multiple types of intelligence, but you must include headers for each column in the CSV file. See Supported types of threat intelligence in Splunk Enterprise Security for the headers relevant for each type of threat intelligence.

Steps

First, add the lookup to Splunk Enterprise Security.

1. Select **Configure** > **Content** > **Content Management**.
2. Select **Create New Content** > **Lookup**.
3. Click **Create New**.
4. Select the lookup file to upload.
5. Select an **App** of **SA-ThreatIntelligence**.
6. (Optional) Modify the file name. For example, type `threatindicatorszerodayattack.csv`.
7. (Optional) Modify the definition name. For example, `zero_day_attack_threat_indicators_list`.
8. Leave the default lookup type of **Manual editing**.
9. Type a label for the lookup. The label appears as the name for the lookup on the Content Management page. For example, Zero Day Threat Indicators.
10. Type a description for the lookup. For example, File-based threat indicators from zero day malware.
11. Save.

Next, add a threat source input stanza that corresponds to the lookup file so that ES can parse the threat intelligence.

1. Select **Configure** > **Data Enrichment** > **Intelligence Downloads**.
2. Click **New**.

3. Type a **Name**. The name cannot include spaces. For example, zero_day_attack_threat_indicators.
4. Type a **Type**. For example, zero_day_IOCs.
5. Type a **Description**. For example, File-based threat indicators from zero day malware.
6. Type a **URL** that references the lookup definition you created. For example, `lookup://zero_day_attack_threat_indicators_list`
7. (Optional) Change the default **Weight** for the threat data.
8. (Optional) Change the default **Retry interval** for the lookup.
9. If your lookup contains multiple types of threat intelligence, type the headers in the **Fields** section.
10. Save.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Verify that you have added intelligence successfully to Splunk Enterprise Security

After you add new intelligence sources or configure included intelligence sources, verify that the intelligence is being parsed successfully and that threat indicators are being added to the threat intelligence KV Store collections. The modular input responsible for parsing intelligence runs every 60 seconds.

Verify that the intelligence source is being downloaded

This verification procedure is relevant only for URL-based sources and TAXII feeds.

1. From the Enterprise Security menu bar, select **Audit > Threat Intelligence Audit**.
2. Find the intelligence source and confirm that the **download_status** column states **threat list downloaded**.
3. Review the **Intelligence Audit Events** to see if there are errors associated with the lookup name.

If the download fails, attempt the download directly from the terminal of the Splunk server using a curl or wget utility. If the intelligence source can be successfully downloaded using one of these utilities, but is not being downloaded successfully in Splunk Enterprise Security, ask your system administrator whether you need to specify a custom user-agent string to bypass network security controls in your environment. See step 12 in Add a URL-based threat source.

Verify that threat indicators exist in the threat collections

For threat intelligence sources, verify that the threat intelligence was successfully parsed and threat indicators exist in the threat collections.

1. Select **Security Intelligence > Threat Intelligence > Threat Artifacts**.
2. Search for the threat source name in the **Intel Source ID** field.
3. Confirm that threat indicators exist for the threat source.

Troubleshoot parsing errors

Review the following log files to troubleshoot errors that can occur when parsing intelligence sources in order to add them to Enterprise Security.

Problem	Suggestion
Issues related to downloading intelligence sources.	Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the `threatlist.log` file with the `threatintel:download` sourcetype.
Issues related to parsing or processing.	Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the `threat_intelligence_manager.log` file with the `threatintel:manager` sourcetype.
Errors result from uploading a file.	Review the `threat_intel_file_upload_rest_handler.log` file.
Other parsing errors.	Verify that the modular inputs are running as expected. See `python_modular_input.log` for errors associated with modular input failures.

Troubleshoot FSISAC threat sources

If you are having trouble with your FSISAC threat source, it appears to be stuck, and you're seeing the following in your traceback log:

```
2020-06-03 18:36:12,461+0000 INFO pid=6580 tid=MainThread file=threatlist.py:download_taxii:361 |
status="TAXII feed polling starting" stanza="FS_TEST"
2020-06-03 18:36:12,516+0000 INFO pid=6580 tid=MainThread file=__init__.py:_poll_taxii_11:49 | Certificate
information incomplete - falling back to AUTH_BASIC.
2020-06-03 18:36:12,516+0000 INFO pid=6580 tid=MainThread file=__init__.py:_poll_taxii_11:68 | Auth Type:
AUTH_BASIC
```

It could be due to a bug in libtaxii that requires version 1.1.113 or higher to support the vendor's requirement of including the Server Name Indication System (SNI). Libtaxii 1.1.113.x is only available in versions of Enterprise Security 6.x and higher.

Change existing intelligence in Splunk Enterprise Security

After you add intelligence to Splunk Enterprise Security, you can make changes to the settings to make sure the intelligence you correlate with events is useful.

Disable an intelligence source

Disable an intelligence source to stop downloading information from the source. This also prevents new threat indicators from the disabled source from being added to the threat intelligence collections.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Find the intelligence source.
3. Under **Status**, click **Disable**.

Disable individual threat artifacts

To prevent individual threat artifacts on a threat list from creating notable events if they match events in your environment, disable individual threat artifacts. If you have command line access to the Enterprise Security search head, you can disable individual threat artifacts using the REST API. See Threat Intelligence API reference in Splunk Enterprise Security *REST API Reference*.

Edit an intelligence source

Change information about an existing intelligence source, such as the retention period or the download interval for the source.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Click the name of the intelligence source you want to edit.
3. Make changes to the fields as needed.
4. Save your changes.

By default, only administrators can edit intelligence sources. To allow non-admin users to edit intelligence sources, see Adding capabilities to a role in the *Installation and Upgrade Manual*.

Configure threat source retention

Remove threat intelligence from the KV Store collections in Splunk Enterprise Security based on the date that the threat intelligence was added to Enterprise Security.

The default maximum age is `-30d` for 30 days of retention in the KV Store. To remove the data more often, use a smaller number such as `-7d` for one week of retention. To keep the data indefinitely, use a blank field. However, if the KV Store collection is stored indefinitely, the .csv files that result from lookup-generating searches can grow large enough to impact search head cluster replication performance. If you manually delete the data from the .csv file, the maximum age timer does not reset based on the edit date, and the data is still removed from the KV Store after the maximum age expires.

1. If the threat intelligence source is not a TAXII feed, define the maximum age of the threat intelligence. This field is not used for TAXII feeds.
    1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
    2. Select an intelligence source.
    3. Change the **Maximum age** setting using a relative time specifier.
2. Enable the retention search for the collection.
    1. From the Splunk platform menu bar, select **Settings** and click **Searches, reports, and alerts**.
    2. Search for "retention" using the search filter.
    3. Enable the retention search for the collection that hosts the threat source. All retention searches are disabled by default.

Configure threat intelligence file retention

Configure how long files are stored by Splunk Enterprise Security after processing. Modular inputs managed on the Threat Intelligence Management page handle file parsing of intelligence sources. Modify the settings of the local modular inputs to manage global file retention for intelligence sources, or modify individual settings for each download or upload to more granularly control file retention.

Use the following table to determine the conditions under which Splunk Enterprise Security deletes a file after processing. For files placed into a directory by a script, for example, use the modular input sinkhole.

Sinkhole set for modular input	Sinkhole set for individual file	Result
False	False	File not deleted.
False	True	File deleted.
True	True	File deleted.
True	False	File deleted.

Remove files managed by a specific modular input

Use the sinkhole or the remove unusable settings to selectively remove files managed by a modular input.

1. From the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Threat Intelligence Management**.
2. Select the modular input for the file retention settings that you want to modify.
    1. For downloaded files, select the `sa_threat_local` modular input.
    2. For uploaded files, select the `da_ess_threat_local` modular input.
3. Select the **Sinkhole** check box so that the modular input deletes each file in the directory after processing.
4. Select the **Remove Unusable** check box so that the modular input deletes a file after processing if it has no actionable intelligence.
5. Save your changes.

Remove files associated with a specific download

Use the sinkhole check box to remove files associated with a threat intelligence download.

1. From the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Intelligence Downloads**.
2. Locate the threat intelligence download.
3. Select the **Sinkhole** check box.
4. Save your changes.

Remove files associated with a specific upload

When you upload the file, select the sinkhole check box to delete the file after processing.

- See Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security.
- See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security.

Example: Add a ransomware threat feed to Splunk Enterprise Security

This example describes how to add a list of blocked domains that could host ransomware to Splunk Enterprise Security to better prepare your organization for a ransomware attack. Replace the feed used in this example with a feed of your choice.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Intelligence Downloads**.
2. Click **New** to add a new threat intelligence source.
3. Type a **Name** of **ransomware_tracker** to describe the threat download source.
4. Type a **Type** of **domain** to identify the type of threat intelligence contained in the threat source.

5. Type a **Description** of **Blocked domains that could host ransomware**.
6. Type a **URL** of `https://v.firebog.net/hosts/Shalla-mal.txt`.
7. (Optional) Change the default **Weight** of 1 to **2** because ransomware is a severe threat and you want an extra risk score multiplier for assets or identities associated with blocked ransomware domains.
8. Leave the default **Interval** of 43200 seconds, or every 12 hours.
9. Leave the **POST arguments** field blank because this type of feed does not accept POST arguments.
10. Decide whether to define a **Maximum age** for the threat intelligence. According to the ransomware tracker website, items on the blocklist stay on the blocklist for 30 days. To drop items off the blocklist in Enterprise Security sooner than that, set a maximum age of less than 30 days. Type a maximum age of `-7d`.
11. Determine whether you need to specify a **User agent** string due to security controls in your environment. If not, leave this field blank.
12. Type a default **Delimiting regular expression** of `:` so that you can enrich the threat indicators by adding fields.
13. Leave the **Extracting regular expression** field blank because the domain names do not need to be extracted because they are line-delimited.
14. Type **Fields** of `domain:$1,description:ransomware_domain_blocklist` to define the fields in this blocklist.
15. (Optional) Leave the default **Ignoring regular expressions** field.
16. Change the **Skip header lines** field to 0 because the ignoring regular expression ignores the comments at the top of the feed.
17. Leave the **Retry interval** at the default of 60 seconds.
18. (Optional) Leave the **Remote site user** and **Remote site user realm** fields blank because this feed does not require any form of authentication.
19. Leave the **Retries** field at the default of **3**.
20. Leave the **Timeout** field at the default of 30 seconds.
21. Ignore the **Proxy Options** section unless you are using a proxy server to add threat intelligence to Splunk Enterprise Security.
22. Click **Save**.
23. From the Splunk platform menu bar, select **Apps > Enterprise Security** to return to Splunk Enterprise Security.
24. From the Enterprise Security menu bar, select **Audit > Threat Intelligence Audit**.
25. Fiind the **ransomware_tracker** stanza in the **Threat Intelligence Downloads** panel and verify that the **status** is **threat list downloaded**.
26. From the Enterprise Security menu bar, select **Security Intelligence > Threat Intelligence > Threat Artifacts**.
27. Type an **Intel Source ID** of **ransomware_tracker** to search for domains added to Splunk Enterprise Security from the new threat feed.
28. Click **Submit** to search.
29. Click the **Network** tab and review the **Domain Intelligence** panel to verify that threat intelligence from the `ransomware_tracker` threat source appears.

Generic Intelligence

Add intelligence to Splunk Enterprise Security

As an ES administrator, you can use the threat intelligence framework in Splunk Enterprise Security to download and parse other forms of intelligence that you can use to correlate with events or enrich dashboards using search. Adding these generic forms of intelligence enhances your analysts' security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a few intelligence sources. Splunk Enterprise Security also supports adding other generic intelligence sources.

ES administrators can add generic intelligence to Splunk Enterprise Security by downloading a feed from the Internet.

1. Configure the intelligence sources included with Splunk Enterprise Security.
2. Download an intelligence feed from the Internet.
3. Verify that you have added intelligence successfully in Splunk Enterprise Security.
4. Use generic intelligence in search with inputintelligence.

Download an intelligence feed from the Internet in Splunk Enterprise Security

Splunk Enterprise Security can periodically download an intelligence feed available from the Internet and store it in the `$SPLUNK_DB/modinput/threatlist` directory. You can then use the `inputintelligence` search command to use the intelligence in reports, searches, or dashboards. See Example: Add a generic intelligence source to Splunk Enterprise Security.

1. (Optional) Configure a proxy for retrieving intelligence.
2. Add a URL-based intelligence source.

Configure a proxy for retrieving intelligence

If you use a proxy server to send intelligence to Splunk Enterprise Security, configure the proxy options for the intelligence source.

The user must correspond to the name of a Splunk secure stored credential in Credential Management. If you remove an existing proxy user and password in the Intelligence Download Setting editor, the download process no longer references the stored credentials. Removing the reference to the credential does not delete the stored credentials from Credential Management. For more information, see Manage credentials in Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment > Intelligence Downloads**.
2. Select the download source.
3. Configure the proxy options.
    1. Type a proxy server address. The **Proxy Server** cannot be a URL. For example, `10.10.10.10` or `server.example.com`.
    2. Type a proxy server port to use to access the proxy server address.
    3. Type a proxy user credential for the proxy server. Only basic and digest authentication methods are supported. The user must correspond to the name of a credential stored in Credential Management.

    4. (Optional) Type a proxy user realm for the proxy user credential. Use this to specify a proxy user realm for the user credential.
4. Save your changes.

Add a URL-based intelligence source

Add a non-TAXII source of intelligence that is available from a URL on the Internet. For an example of adding a URL-based generic intelligence source, see Example: Add a generic intelligence source to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment** > **Intelligence Downloads**.
2. Type a **Name** for the download. The name can only contain alphanumeric characters, hyphens, and underscores. The name cannot contain spaces.
3. Click **New** to add a new intelligence source.
4. Do not select the check box for **Sinkhole**.
5. Deselect the check box for **Is Threat Intelligence**.
6. Type a **Type** for the download. The type identifies the type of information that the feed contains.
7. Type a **Description**. Describe the information in the feed.
8. Leave the default **Weight** because the field does not matter for the generic intelligence source.
9. (Optional) Change the default download **Interval** for the feed. Defaults to 43200 seconds, or every 12 hours.
10. (Optional) Type POST arguments for the feed. You can use POST arguments to retrieve user credentials from Credential Management. Use the format `key=$user:<username>$` or `key=$user:<username>,realm:<realm>$` to specify a username and realm.
11. Do not use the **Maximum age** setting.
12. (Optional) If you need to specify a custom **User agent** string to bypass network security controls in your environment, type it in the format `<user-agent>/<version>`. For example, `Mozilla/5.0` or `AppleWebKit/602.3.12`. The value in this field must match this regex: `([A-Za-z0-9_.-]+)/([A-Za-z0-9_.-]+)`. Check with your security device administrator to ensure the string you type here is accepted by your network security controls.
13. Fill out the **Parsing Options** fields to make sure that your list parses successfully. You must fill out either a delimiting regular expression or an extracting regular expression. You cannot leave both fields blank.

Field	Description	Example
Delimiting regular expression	A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.	`,` or `:` or `\t`
Extracting regular expression	A regular expression used to extract fields from individual lines of an intelligence source document. Use to extract values in the intelligence source.	`^(\S+)\t+(\S+)\t+\S+\t+\S+\t*(\S*)`

Fields	Required if your document is line-delimited. Comma-separated list of fields to be extracted from the intelligence list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the `DA-ESS-ThreatIntelligence/collections.conf` file. Defaults to `description:$1,ip:$2`.	`<fieldname>:$<number>,<field name>.$<number>`
		`ip:$1,description:domain_blocklist`

Ignoring regular expression	A regular expression used to ignore lines in an intelligence source. Defaults to ignoring blank lines and comments that begin with #.	`^\s*$)`
Skip header lines	The number of header lines to skip when processing the intelligence source.	`0`
Intelligence file encoding	If the file encoding is something other than ASCII or UTF8, specify the encoding here. Leave blank otherwise.	latin1

Field	Description	Example

14. (Optional) Change the **Download Options** fields to make sure that your list downloads successfully.

Field	Description	Example
Retry interval	Number of seconds to wait between download retry attempts. Review the recommended poll interval of the intelligence source provider before changing the retry interval.	60
Remote site user	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The user name you add in this field must match the name of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	buttercup
Remote site user realm	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The realm you add in this field must match the realm of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	paddock
Retries	The maximum number of retry attempts.	3
Timeout	Number of seconds to wait before marking a download attempt as failed.	30

15. (Optional) If you are using a proxy server, fill out the **Proxy Options** for the feed. See Configure a proxy for retrieving intelligence.
16. Save your changes.

If you are finished adding intelligence sources, see Verify that you have added intelligence successfully in Splunk Enterprise Security.

Use generic intelligence in search with inputintelligence

After you add generic intelligence to Splunk Enterprise Security, you can use the `inputintelligence` command to make use of the intelligence. See Add generic intelligence to Splunk Enterprise Security.

Description

Use the `inputintelligence` command to add intelligence from the threatlist directory to your search results. When downloaded, generic intelligence is parsed and stored in the `$SPLUNK_DB/modinputs/threatlist$` directory.

Syntax

| inputintelligence <threatlist_stanza_name> [fields=<string>] [delim_regex=<string>] [extract_regex=<string>] [ignore_regex=<string>] [skip_header_lines=<int>] [include_raw=<bool>] [append=<bool>] [no_parse=<bool>]

Required arguments

threatlist_stanza_name

Syntax: <string>
Description: The stanza of the intelligence download. Matches the **Name** field on the Intelligence Downloads page. You can include multiple stanza names in your search. See Download an intelligence feed from the Internet in Splunk Enterprise Security.

Optional arguments

fields

Syntax: <string>
Description: Overrides the default fields setting for the intelligence download defined in the Intelligence Download page. Required if your document is line-delimited. Comma-separated list of fields to be extracted from the intelligence list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the DA-ESS-ThreatIntelligence/collections.conf file. Defaults to description:$1,ip:$2.

delim_regex

Syntax: <string>
Description: Overrides the default delimiting regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.

extract_regex

Syntax: <string>
Description: Overrides the default extracting regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression used to extract fields from individual lines of an intelligence source document. Use to extract values in the intelligence source.

ignore_regex

Syntax: <string>
Description: Overrides the default ignore regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression used to ignore lines in an intelligence source. Defaults to ignoring blank lines and comments that begin with #.

skip_header_lines

Syntax: <int>
Description: Overrides the default skip header lines setting for the intelligence download defined in the Intelligence Download page. The number of header lines to skip when processing the intelligence source.
Default: 0

include_raw

Syntax: <bool>
Description: If 1, t, or true, adds the original line content to an additional column called raw.
Default: 0

append

Syntax: <bool>
Description: If 1, t, or true, appends the results of the `inputintelligence` command to an existing set of search results instead of replacing it.
Default: 0

no_parse

Syntax: <bool>
Description: If 1, t, or true all other options are ignored and the raw contents of the intelligence file is returned one line per row.
Default: 0

Usage

The `inputintelligence` command is a **transforming command**.

Examples

1. View the top one million sites

View the top one million sites according to Cisco.

```
inputintelligence cisco_top_one_million_sites
```

2. Further examples

See Example: Add a generic intelligence source to Splunk Enterprise Security.

See also

inputlookup

Example: Add a generic intelligence source to Splunk Enterprise Security

As a security analyst, you want to compare hosts seen in your network with the hosts associated with Spotify advertisements so that you can assess the risk that listening to Spotify Free during the work day poses to your network. The hosts associated with Spotify ads are not malicious, and you do not want to add them to Splunk Enterprise Security as threat intelligence. Instead, you can add them as generic intelligence.

Download the generic intelligence

First, create a download configuration for the list.

1. Select **Configure > Data Enrichment > Intelligence Downloads**.
2. Click **New**.
3. Type a **Name** of `spotify_ads`.
4. Deselect the check box for **Is Threat Intelligence**.
5. Type a **Type** of `spotify_ads`.
6. Type a **Description** of Hostnames of machines hosting Spotify ads.
7. Type a URL of `https://raw.githubusercontent.com/FadeMind/hosts.extras/master/StreamingAds/hosts`.
8. (Optional) Change the default **Weight**.
9. (Optional) Change the default **Interval**.
10. Type a delimiting regular expression of `\s`.
11. Type **Fields** of `url:$2`.
12. Type an **Ignoring regular expression** of `(^#|^\s*$)`.

13. Save.

Verify that the intelligence downloads successfully

Using search, verify that the modular input is downloading information from the source.

```
| inputintelligence no_parse=1 spotify_ads
```

Verify that the intelligence parses correctly

Use the custom search command `inputintelligence` to verify that the intelligence parses correctly.

```
| inputintelligence spotify_ads
```

If the intelligence does not seem to be parsing correctly, review `search.log` for any error messages. In addition, you can change the parsing settings for the download using the optional arguments for the `inputintelligence` command to determine the correct settings. See Use generic intelligence in search with inputintelligence.

Use the new intelligence source in a search

You can use the new intelligence source in many ways in searches.

Use Spotify ads in a subsearch

To return 100 URLs used by Spotify ads in a list with the following subsearch:

```
| search [| inputintelligence spotify_ads | return 100 url]
```

Use Spotify ads in join

Join the hosts in the Spotify ads intelligence source with another set of data with `join`:

```
... | join url [| inputintelligence spotify_ads | eval spotify_ad="true"] | search spotify_ad="true"
```

Add Spotify ads to a lookup table file

Add the hosts from Spotify ads to a lookup table file using a lookup generating search:

```
| inputintelligence spotify_ads | eval spotify_ad="true" | outputlookup spotify_ads.csv
```

After creating the lookup, use it in search with the following example search:

```
... | lookup spotify_ads.csv url OUTPUT spotify_ad | search spotify_ad="true"
```

Managing Content

Managing content in Splunk Enterprise Security

As a Splunk Enterprise Security administrator, you can use the Content Management page to display, create, configure, and edit content that is unique to Splunk Enterprise Security, such as correlation searches, key indicators, saved searches, and swim lane searches.

- Create correlation searches in Splunk Enterprise Security
- Create and manage data models in Splunk Enterprise Security
- Create and manage key indicator searches in Splunk Enterprise Security
- Create and manage lookups in Splunk Enterprise Security
- Create and manage saved searches in Splunk Enterprise Security
- Create and manage search-driven lookups in Splunk Enterprise Security
- Create and manage swim lane searches in Splunk Enterprise Security
- Create and manage views in Splunk Enterprise Security
- Export content from Splunk Enterprise Security as an app
- Create and edit risk objects in Splunk Enterprise Security

Create and manage data models in Splunk Enterprise Security

Create and manage data models using the Content Management page in Splunk Enterprise Security.

- Review the list of data models in Splunk Enterprise Security.
- Review the next scheduled time, acceleration status, and choose whether or not to accelerate a data model.
- Click a data model name to edit the data model.

Create a data model

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Data Model**.
3. Create a data model following the instructions in the Splunk platform documentation.
   - ♦ For Splunk Enterprise, see Create a data model in the Splunk Enterprise *Knowledge Manager Manual*.
   - ♦ For Splunk Cloud, see Design data models in the Splunk Cloud *Knowledge Manager Manual*.

Create and manage key indicator searches in Splunk Enterprise Security

Configure key indicator searches on Content Management in Splunk Enterprise Security. Use the filters to select a type of key indicator to view only key indicator searches.

Create a custom key indicator search

Create a key indicator search to create a key indicator that you can add to a dashboard or glass table as a security metric.

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Key Indicator Search**.

3. Type a key indicator name.
   In order for the key indicator to show up in the list of security metrics on glass table, type a category or security domain at the beginning of the key indicator name followed by a hyphen. For example, **APT - Example Key Indicator** or **Access - Sample Key Indicator**.
4. Type a search, and other details.
   The key indicators that come with Enterprise Security use data models to accelerate the return of results.
5. (Optional) Select **Schedule** to use data model acceleration for your custom key indicator.
6. Type the name of the field that corresponds to the value of the key indicator in the **Value** field.
7. Type the name of the field that corresponds to the change in the key indicator in the **Delta** field.
8. (Optional) Type a **Threshold** for the key indicator. The threshold controls whether the key indicator changes color. You can also set the threshold in dashboards and on glass tables.
9. Type a **Value Suffix** to indicate units or another word to follow the key indicator.
10. Select the **Invert** check box to invert the colors of the key indicator. Select this check box to indicate that a high value is good and a low value is bad.
11. Click **Save**.

Schedule a key indicator search

Key indicators included with Splunk Enterprise Security use data model acceleration. Enable acceleration and schedule the search to run as a **scheduled report**. Scheduled report results are cached, allowing the indicator to display results on the dashboard more quickly.

1. Select **Configure > Content > Content Management**.
2. Locate the key indicator search that you want to accelerate.
3. Click **Accelerate** in the **Actions** column.
4. In the **Edit Acceleration** window, select the **Accelerate** check box.
5. Select a **Refresh Frequency** for how often Enterprise Security should update the cached results.
6. Click **Save**.

After a key indicator is accelerated, the **Next Scheduled Time** populates on the **Content Management** page and the lightning bolt for that indicator changes from grey to yellow.

Edit a key indicator search

Make changes to a key indicator search.

1. From the ES menu bar, select **Configure > Content > Content Management**
2. Select a key indicator search.
3. (Optional) Change the search name.
4. (Optional) Change the destination app where the search is stored.
5. (Optional) Change the title of the key indicator. The title appears above the key indicator on a dashboard, or next to the security metric on a glass table.
6. (Optional) Change the sub-title of the key indicator that is used to describe the type of the key indicator function on dashboards.
7. (Optional) Change the search string that populates the key indicator.
8. (Optional) Add a drilldown URL such as a custom search or dashboard link to override the default drilldown behavior. By default, the key indicator drilldown opens the search results that produced the key indicator value. For key indicators on glass tables, you can set a custom drilldown when you add the key indicator to the glass table.
9. (Optional) Select the **Schedule** check box to enable acceleration for a key indicator and allow it to load faster on a dashboard.

10. (Optional) Change the **Cron Schedule** frequency using standard cron notation.
11. (Optional) Change the **Threshold** behavior to determine the color assigned to the value indicator. By default, no threshold produces a black value indicator, a threshold number higher than the count of a value indicator produces a green value indicator, and a threshold number lower than the count of a value indicator produces a red value indicator.
12. (Optional) Add a **Value suffix** to describe the value indicator. For example, specify units. On dashboards, the value suffix appears between the value indicator and the trend indicator.
13. (Optional) Select the **Invert** check box to change the default colors of the trend indicator threshold. If this check box is selected, a threshold number higher than the count of a value indicator produces a red value indicator, and a threshold number lower than the count of a value indicator produces a green value indicator.
14. Click **Save**.

Create and manage saved searches in Splunk Enterprise Security

Create a saved search, also called a scheduled report, in Splunk Enterprise Security.

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Saved Search**.
3. Create a saved search, also called a scheduled report, following the instructions in the Splunk platform documentation.
    - For Splunk Enterprise, see Create a new report in the Splunk Enterprise *Reporting Manual*.
    - For Splunk Cloud, see Create a new report in the Splunk Cloud *Reporting Manual*.
4. Modify the permissions of the report to share it with Enterprise Security so that you can view and manage the search in Enterprise Security, following the instructions in the Splunk platform documentation.
    - For Splunk Enterprise, see Set report permissions in the Splunk Enterprise *Reporting Manual*.
    - For Splunk Cloud, see Set report permissions in the Splunk Cloud *Reporting Manual*.

Create and manage search-driven lookups in Splunk Enterprise Security

A search-driven lookup lets you create a lookup based on the results of a search that runs at regular scheduled intervals. The search can run only against data stored in data models or in an existing lookup. Lookups created as search-driven lookups are excluded from bundle replication and are not sent to the indexers.

When to use search-driven lookups

Create a search-driven lookup if you want to know when something new happens in your environment, or need to consistently update a lookup based on changing information from a data model or another lookup.

The search-driven lookup collects and stores information from data models or other lookups. The data stored in the lookup represents a historical summary of selected fields gathered from events. You can view changes on a dashboard or use a correlation search to compare data from the search-driven lookup with new events, and alert if there is a match. For example, to find out when a new user logs in to a web server.

1. Search for user data in the Authentication data model and filter by the web server host name with the `where` command.
2. Verify the search results match the known hosts and users in your environment.
3. Create a guided search-driven lookup to collect and store information on a recurring schedule about users logging in to the web servers.

4. Create a correlation search that alerts you when a user logs in to one of the web servers that he or she has not accessed in the past, based on the historical information in the search-driven lookup.

Create a search-driven lookup

When you create a search-driven lookup, two knowledge objects are created. One knowledge object is the lookup that is generated by the search, while the other knowledge object is the search that drives the lookup.

Create a search-driven lookup as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Content> Content Management**.
2. Click **Create New Content** and select **Search-Driven Lookup**.
3. (Optional) Select an **App**. The default app is SplunkEnterpriseSecuritySuite. You can create the lookup in a specific app, such as SA-NetworkProtection, or a custom app. You cannot change the app after you save the search-driven lookup.
4. (Optional) Type a description for the search.
5. Type a label for the lookup. This is the name of the search-driven lookup that appears on **Content Management**.
6. Type a name for the lookup. After you save the lookup, the name cannot be changed.
7. Type a cron schedule to define how often you want the search to run.
8. Select real-time or continuous scheduling for the search. Real-time scheduling prioritizes search performance, while continuous scheduling prioritizes data integrity.
9. Type a **Search Name** to define the name of the saved search. After you save the lookup, the name cannot be changed.
10. Select a mode of **Guided** to create a search without having to write the search syntax yourself, or select **Manual** to write your own search. See the example for help building a search with the guided search editor.
11. If you create a search in manual mode, type a search.
12. (Optional) Use the **Enabled** toggle to enable retention.
    1. In the **Time field** list, type a valid time field for retention. Note that this is a free-form text field, and there is no validation on this field.
    2. In the **Earliest Time** field, type the time specifier such as **-1y** to retain data for one year.
    3. In the **Time Format** field, type the time format such as **%s** for seconds.
       See Date and time format variables in the Splunk Enterprise *Search Reference*.
13. Click **Save** to save the search.

Example search-driven lookup

In this example search-driven lookup included with Splunk Enterprise Security, you want to track attacks identified by your intrusion detection system (IDS). You can then be notified of new attacks with a correlation search, or determine whether an attack is new to your environment or not. The Intrusion Center dashboard uses this search-driven lookup for the New Attacks - Last 30 Days panel. See Intrusion Center dashboard.

1. From the Splunk Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Search-Driven Lookup**.
3. (Optional) Select an **App** of SA-NetworkProtection. You cannot change the app after you save the search-driven lookup.
4. Type a description of "Maintains a list of attacks identified by an IDS and the first and last time that the attacks were seen."
5. Type a label of **IDS Attack Tracker Example** for the lookup. This is the name of the search-driven lookup that appears on **Content Management**.
6. Type a unique and descriptive name for the lookup of **ids_attack_tracker_example**. After you save the lookup, the name cannot be changed.

7. Type a cron schedule to define how often you want the search to run. If your IDS collects data often, type a cron schedule of `25 * * * *` to run the search at 25 minutes every hour every day.
8. Select a Continuous Schedule because the lookup must track all data points.
9. Type a **Search Name** of **Network - IDS Attack Tracker - Example Lookup Gen**.
10. Select guided mode to use the guided search editor to create the search.
11. Click **Open guided search editor** to start creating the search.
12. Select a data source of **Data Model** because the IDS Attack data is stored in a data model.
13. Select a data model of **Intrusion_Detection** and a data model dataset of **IDS_Attacks**.
14. Select **Yes** for the summaries only field to run the search against only the data in the accelerated data model.
15. Select a time range that uses Relative time that begins with an earliest time of 70 minutes ago, starting at the beginning of the minute, and ends now. Click **Apply** to save the time range.
16. Click **Next**.
17. (Optional) Type a where clause to filter the data from the data model to only the data from a specific IDS vendor and click **Next**.
18. Add aggregate values to track specific statistics about the data and store that information in the lookup. At least one aggregate is required.
    1. To track the first time that an IDS attack was seen in your environment, add a new aggregate with a function of **min** and a field of **_time** and save it as **firstTime**.
    2. Track the last time an attack was seen by adding another aggregate with a **max** function and a field of **_time** and saving it as **lastTime**. This creates two columns in the lookup, firstTime and lastTime.
19. Add split-by clauses to track more data points in the lookup. All split-by clauses appear as columns in the lookup.
    1. Add a split-by clause of **IDS_Attacks.ids_type** and rename it as **ids_type** to monitor the IDS type in the lookup.
    2. Add a split-by clause to rename IDS_Attacks.signature as **signature**.
    3. Add a split-by clause to rename IDS_Attacks.vendor_product as **vendor_product**.
20. Click **Next**.
21. Select a retention period that defines the age of the data to be stored in the lookup. For example, you want to keep 5 years of IDS attack evidence stored in this lookup. Select a time field of **lastTime** to base the retention on the last time an attack was identified by the IDS. Type an earliest time of **-5y** and indicate the format of the time value that you entered: **%s**. You can find guidance on the time format in the Splunk platform documentation.
    - For Splunk Enterprise, see Date and time format variables in the Splunk Enterprise *Search Reference* manual.
    - For Splunk Cloud, see Date and time format variables in the Splunk Cloud *Search Reference* manual.
22. Click **Next**.
23. Review the search created by the wizard and click **Done** to finish using the guided search editor.
24. Click **Save** to save the search.

Modify a search-driven lookup

Since a search-driven lookup contains the two knowledge objects of search and lookup, there are two ways to modify it. Both ways will open the search-driven lookup editor.

Modify the search-driven lookup as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Select a **Type** of **Search-Driven Lookup**.
3. Click the lookup that you want to edit.
4. Make changes and click **Save**.

Modify the lookup generating search as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Select a **Type** of **Lookup Generating Search**.
3. Click the lookup that you want to edit.
4. Make changes and click **Save**.

Modify retention settings for a search-driven lookup

You can modify search-driven lookup retention settings for performance purposes.

As of Enterprise Security 6.3.0, retention settings are no longer handled in the custom search builder specification of the savedsearches.conf file. The search-driven lookup retention is managed by the lookup_retention.py modular input using `managed_configurations` settings. Therefore, you no longer use the guided search builder to revise the retention settings in the search processing language (SPL). With retention settings migrated into `managed_configurations`, the retention is no longer impacted if you use `outputlookup append=T` in the SPL of a search driven lookup, so the change delta does not get ignored. In addition, for CSV only, the `outputlookup override_if_empty` is set to true by default and allows an outputlookup to delete the output file if the result set is empty. If you have existing retention settings, they remain as you set them.

Modify the retention settings as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Select a Type of **Search-Driven Lookup**.
3. Click the lookup that you want to edit.
4. Scroll to **Retention**.
5. If disabled, use the **Enabled** toggle to enable retention.
6. In the **Time field** list, type a valid time field for retention.
   Time fields are defined in the transforms.conf file. Examples include the following:
   - _time
   - lastTime
7. In the **Earliest Time** field, type the time specifier such as **-1y** to retain data for one year.
8. In the **Time Format** field, type the time format such as **%s** for seconds.
   For Splunk Enterprise, see Date and time format variables in the Splunk Enterprise *Search Reference* manual.
   For Splunk Cloud, see Date and time format variables in the Splunk Cloud *Search Reference* manual.

The default search-driven lookup retention settings are as follows. Those listed as **N/A** are not available for modifying through the Splunk Web UI.

Search Driven Lookup Label	Search Driven Lookup Description	Time Field	Retention Period
Access App Tracker	Maintains a list of Authentication app values and the first and last time they have been seen.	_time	5 years
Access Tracker	Maintains a list of users that have authenticated to each system and the first, second to last, and last time they have been seen.	lastTime	1 year
Asset/Identity Categories	Maintains a list of categories that apply to assets and identities.	N/A	N/A
Correlation Searches Lookup	Maintains correlation search enrichment for notable events.	N/A	N/A
ES Notable Events		N/A	N/A

Search Driven Lookup Label	Search Driven Lookup Description	Time Field	Retention Period
	Maintains a list containing pertinent information for the last 48 hours of notable events.		
Firewall Rule Tracker	Maintains a list of Traffic rule values by device and vendor and the first and last time they were seen. See Firewall Rule Tracker Retention	year	2 years
IDS Attack Tracker	Maintains a list of IDS attacks by vendor and the first and last time they were seen.	lastTime	5 years
IDS Category Tracker	Maintains a list of IDS attack categories by vendor and the first and last time they were seen.	lastTime	5 years
Licensing - Events Per Day	Maintains a list of event counts per day per index.	_time	1 year
Listening Ports Tracker	Maintains a list of all port and protocol combinations listening on each system and the first and last time they were seen.	lastTime	5 years
Local Processes Tracker	Maintains a list of all processes on each system and the first and last time they were seen.	lastTime	1 month
Malware Operation Tracker	Maintains a list of anti-malware product and signature versions for each system.	_time	1 year
Malware Tracker	Maintains a list of all detections (regardless of status) for each system and the first and last time they were seen.	lastTime	5 years
PCI Domain Lookup	Maintains a list of pci domains that apply to assets and identities.	N/A	N/A
Port/Protocol Tracker	Maintains a list of allowed Traffic by unique transport protocol and destination port combination and the first and last time they were seen.	lastTime	5 years
Registry Tracker	Maintains a list of registry paths, keys, and value information by system and the first and last time they were seen.	lastTime	1 year
Services Tracker	Maintains a list of all services (and the most recent startmode) for each system and the first and last time they were seen.	lastTime	1 month
System Version Tracker	Maintains a list of the most recent operating system version for each system and the time we got this information.	_time	5 years
Traffic Bytes Tracker	Maintains Traffic byte statistics.	N/A	N/A
Update Signature Reference	Maintains a list of all updates by vendor and the first and last time they were seen.	lastTime	1 year
URL Length Tracker	Maintains Web user agent length statistics.	N/A	N/A
User Accounts Tracker	Maintains a list of all local user accounts on each system and the first and last time they were seen (not accelerated).	lastTime	1 year
User Agent Length Tracker	Maintains Web url length statistics.	N/A	N/A
Vulnerability Signature Reference	Maintains a list of vulnerability signatures by vendor (including external reference information such as cve) and the first and last time they were seen.	lastTime	1 year
Vulnerability Tracker	Maintains a list of Vulnerabilities by signature, destination and the first and last time they were seen.	lastTime	5 years
Whois Tracker	Maintains a list of whois scan data including the resolved_domain (if domain was an IP) and the date the domain was created.	_time	5 years

Global settings for search-driven lookup retention is handled by the data_retention_manager in **Settings > Data Inputs > Lookup Retention**.

Firewall rule tracker retention

The Firewall Rule Tracker retention works differently from the others. It uses only the year field in its retention spec, which means that a relative time is used that's based off the beginning of the year. The default retention period is set to two years, in order to preserve data quantity. For example, if today is 06/20/2020 and your retention period is "-1y", then all rows in your lookup where the year is less than or equal to 2019 are deleted.

Do not set the Firewall Rule Tracker retention period to less than two years, unless you accept the possibility of data loss.

Enable or disable the search populating a search-driven lookup

You can enable or disable the search of a search-driven lookup to prevent the search from updating the lookup. If you disable the search that populates a search-driven lookup, the search stops updating the lookup and the data in the lookup will stop being updated. Correlation searches or dashboards that rely on the data inside the lookup will be out-of-date.

1. Select **Configure > Content > Content Management**.
2. Filter on a type of search-driven lookup and open the search-driven lookup that you want to enable or disable.
3. Find the **Search name** of the search-driven lookup.
4. From the Splunk platform menu bar, select **Settings > Searches, reports, alerts**.
5. (Optional) Filter by Type and App of **All**.
6. Find the search and enable or disable it.

Create and manage swim lane searches in Splunk Enterprise Security

Create a swim lane search to create a swim lane that you can add to the Asset Investigator or Identity Investigator dashboard. Swim lanes on the investigator dashboards help you profile activity by a specific asset or identity over time.

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Swim Lane Search**.
3. Type a **Search Name**.
4. Select a **Destination App**.
5. Type a **Title** for the swim lane that appears on the dashboard.
6. Type a **Search** that populates the swim lane.
7. Type a **Drilldown Search** that runs when a user clicks a swim lane item. By default, the swim lane item drilldown shows the raw events.
8. Select a color.
9. Select an **Entity Type** of **Asset** or **Identity**.
10. Type **Constraint Fields**. Type a field to specify constraints on the search. Your search must contain `where $constraints$` to use these constraint fields in the search. Only specific constraints are valid for each type of swim lane search.
    For example, an Asset Investigator swim lane search using the Malware data model and the Malware_Attacks data model dataset could specify the `Malware_Attacks.user` field as a constraint.
11. Click **Save**.

Example

For example, create a swim lane to identify all authentication events involving a specific asset.

1. Type a **Search Name** of **Authentication by Asset - Example**
2. Select a **Destination App** of **DA-ESS-AccessProtection**.
3. Type a **Title** for the swim lane that appears on the dashboard. **All Authentication**.
4. Type a **Search** that populates the swim lane.

   ```
   | tstats `summariesonly` values(Authentication.action) as action,values(Authentication.app) as
   app,values(Authentication.src) as src,values(Authentication.dest) as
   dest,values(Authentication.user) as user,count from datamodel=Authentication.Authentication where
   $constraints$ by _time span=$span$
   ```
5. Type a **Drilldown Search**.

   ```
   | `datamodel("Authentication","Authentication")` | search $constraints$
   ```
6. Select the color **Purple**.
7. Select an entity type of **Asset** because you want to investigate all authentication events by asset and be able to add this swim lane to the Asset Investigator dashboard. With this specified, all constraints specified as constraint fields perform a reverse lookup against the other fields that identify an asset.
8. Type constraint fields of **Authentication.src** and **Authentication.dest** to identify authentications originating from or targeting a specific asset.

Assuming an asset lookup entry with an IP address of `1.2.3.4`, `dns` of `server.example.com`, and `nt_host` of `server1`, the search for this swim lane searches for all authentication events where the source or destination of the authentication event is 1.2.3.4, server.example.com, or server1.

```
... Authentication.src=1.2.3.4 OR Authentication.src=server.example.com OR Authentication.src=server1 OR
Authentication.dest=1.2.3.4 OR Authentication.dest=server.example.com OR Authentication.dest=server1
```

Create and manage views in Splunk Enterprise Security

Create a new view or dashboard using Simple XML from Content Management.

Prerequisite

Creating new views and dashboards from Content Management requires familiarity with Simple XML. For an overview of building and editing dashboards, including working with Simple XML, see the Splunk platform documentation.

- For Splunk Enterprise, see Dashboard overview in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Enterprise, see Dashboard overview in Splunk Enterprise *Dashboards and Visualizations*.

Task

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **View**.
3. Create a new dashboard with Simple XML.
4. Modify the permissions to share the new view with Enterprise Security so that you can view and manage it in Enterprise Security.
   1. From the Splunk bar, select **Settings > User interface > Views**.
   2. Locate the **View name** that you created.

3. Click **Permissions** and modify the permissions to share the view with Enterprise Security.
4. Click **Save**.

You can also create a new dashboard with the interactive dashboard editor. Select **Search** > **Dashboards** to open the Dashboards page. You can find information about the Dashboard Editor in the Splunk platform documentation.

- For Splunk Enterprise, see Open the Dashboard Editor in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Cloud, see Open the Dashboard Editor in Splunk Cloud *Dashboards and Visualizations*.

Use the Navigation editor to change which dashboards are visible on the menu in your deployment. For more information, see Customize the menu bar in Splunk Enterprise Security.

Export content from Splunk Enterprise Security as an app

Export content from Splunk Enterprise Security as an app from the Content Management page. Use the export option to share custom content with other ES instances, such as migrating customized searches from a development or testing environment into production. You can export any type of content on the Content Management page, such as correlation searches, glass tables, data models, and views.

By default, only admin users can export content. To add the export capability to another role, see Adding capabilities to a role in the *Installation and Upgrade Manual*.

1. From the ES menu bar, select **Configure** > **Content** > **Content Management**.
2. Select the check boxes of the content you want to export.
3. Click **Edit Selection** and select **Export**.
4. Type an **App name**. This will be the name of the app in the file system.
   For example, SOC_custom.
5. Select an **App name prefix**. If you want to import the content back into Splunk Enterprise Security without modifying the default app import conventions, select **DA-ESS-**. Otherwise, select **No Prefix**.
6. Type a **Label**. This is the name of the app.
   For example, Custom SOC app.
7. Type a **Version** and **Build number** for your app.
8. Click **Export**.
9. Click **Download app now** to download the app package to the search head at the location `$SPLUNK_HOME/etc/apps/SA-Utils/local/data/appmaker/*`.
10. Click **Close** to return to **Content Management**.

Limitations to exported content

Exported content may not work on older versions of Enterprise Security. The following items are included or not included in exported content.

Exported item	Included in export	Not included in export
Data models	`datamodels.conf` and data model JSON definition.	N/A

Saved searches, including correlation, key indicator, and swim lane searches	`savedsearches.conf`
	`governance.conf`
	Alert actions and response actions, including risk assignments, script names, and email addresses.
		Macros, script files, lookups, or any binary files referenced by the search object. Extreme Search objects, such as the context generating search, the contexts, or the concepts referenced by the search object.

Exported item	Included in export	Not included in export

Search-driven lookups	`savedsearches.conf`
	`governance.conf`
	`managed_configurations.conf`
	`collections.conf`
	`transforms.conf`
		Macros, script files, lookups, or any binary files referenced by the search object.

Managed lookups	The lookup CSV file.
	`managed_configurations.conf`
	`collections.conf`
	`transforms.conf`
		N/A

Views	The XML or HTML, CSS, and JS files for the view.	N/A
Sequence Template	`app.conf` and `sequence_templates.conf` for all the selected templates.	The sequenced events themselves are not exported, but saved in the `sequenced_events` index.

Create and manage lookups in Splunk Enterprise Security

Splunk Enterprise Security provides **lookups** to manage asset and identity correlation with events, match threat indicators with events, and enrich dashboards and panels with information.

As an administrator, you can add lookups to Splunk Enterprise Security. After you add lookups to Splunk Enterprise Security, you can use the lookups in searches, edit them, add descriptions, and export them.

Add a lookup to Splunk Enterprise Security

Upload and create a lookup in Splunk Enterprise Security.

1. Select **Configure > Content > Content Management**.
2. Click **Create New Content > Managed Lookup**.
3. Click **Create New**.
4. Select a lookup file to upload.
5. (Optional) Change the default **App** for the file.
6. (Optional) Modify the file name.
7. (Optional) Modify the definition name.
8. (Optional) Change the default lookup type.
9. Type a label for the lookup. The label appears as the name for the lookup on the **Content Management** page.
10. Type a description for the lookup.
11. (Optional) Change the option to allow editing of the lookup file.
12. Click **Save**.

Add an existing lookup to Splunk Enterprise Security

If the lookup file and definition already exists in the Splunk platform, you can add it to Splunk Enterprise Security so that you can edit it.

1. Select **Configure > Content > Content Management**.
2. Click **Create New Content > Managed Lookup**.
3. Click **Select Existing**.
4. Select the lookup definition from the drop-down list.
5. (Optional) Modify the lookup type.
6. Type a label for the lookup. The label appears as the name for the lookup on the **Content Management** page.

7. Type a description for the lookup.
8. (Optional) Change the option to allow editing of the lookup file.
9. Click **Save**.

Verify that you added a lookup successfully

Confirm that you added a lookup file successfully by using the `inputlookup` search command to display the list. For example, to review the application protocols lookup:

```
| inputlookup append=T application_protocol_lookup
```

Edit a lookup in Splunk Enterprise Security

Only users with appropriate permissions can edit lookups. See Manage permissions in Splunk Enterprise Security. Lookups do not accept regular expressions, and the lookup editor does not validate the accuracy of your entries. You cannot save a lookup file with empty header fields.

Stop managing a lookup

You can stop managing a lookup on the Content Management page by clicking **Stop managing**. When you stop managing a lookup, you can no longer edit the lookup from Splunk Web but the lookup is not deleted.

Export a lookup in Splunk Enterprise Security

1. On Content Management, locate the lookup that you want to export.
2. Under the Actions column, click **Export** to export a copy of the file in CSV format.

You can export multiple lookup files and other knowledge objects as part of an app. See Export content from Splunk Enterprise Security as an app in *Administer Splunk Enterprise Security*.

Audit changes made to lookup files

To review the last time a lookup file was edited and by whom, use a search. For example:

```
index=_internal uri_path="/splunk-es/en-US/app/SplunkEnterpriseSecuritySuite/ess_lookups_edit"
```

Manage internal lookups in Splunk Enterprise Security

Splunk Enterprise Security provides and maintains internal lookups to support dashboards, searches, and other internal processes.

These lookups are created in several ways.

- Populated by a static lookup table
- Populated internally by search commands, called a search-driven lookup
- Populated with information from the Internet

The internal lookups populated with information from the Internet are used by some correlation searches to identify hosts that are recognized as malicious or suspicious according to various online sources, such as the SANS Institute. If Splunk Enterprise Security is not connected to the Internet, these lookup files are not updated and the correlation searches that rely on the lookups might not function correctly. Most of the internal lookups populated by the Internet are threat intelligence sources. See Configure the threat intelligence sources included with Splunk Enterprise Security in this manual.

Select **Configure** > **Content** > **Content Management** to view the existing lookups that you can edit in Splunk Enterprise Security.

Splunk Enterprise Security uses the internal lookups in different ways.

Lookup type	Description	Example
List	Small, relatively static lists used to enrich dashboards.	Categories
Asset or identity list	Maintained by a modular input and searches. See How Splunk Enterprise Security processes and merges asset and identity data.	Assets
Threat intelligence collections	Maintained by several modular inputs. See Threat intelligence framework in Splunk ES on the Splunk developer portal.	Local Certificate Intel
Tracker	Search-driven lookups used to supply data to dashboard panels.	Malware Tracker
Per-panel filter lookup	Used to maintain a list of per-panel filters on specific dashboards.	HTTP Category Analysis Filter

Internal lookups that you can modify

Some lookups are managed by searches (search-driven lookups), and others you update manually. This table lists the lookups that you might need to modify in Splunk Enterprise Security.

Lookup name	Type	Description	Usage details
Action History Search Tracking Whitelist	List	Add searches to this whitelist to prevent them from creating action history items for investigations.	Type a **start_time** of 1 to whitelist the search. Type a **start_time** and an **end_time** to whitelist the search for a specific period of time.
Administrative Identities	List	You can use this lookup to identify privileged or administrative identities on relevant dashboards such as the Access Center and Account Management dashboards.	Modify the **category** column to indicate the privileged status of an account. Specify privileged default accounts with `default|privileged`, or type `privileged` for privileged accounts that are not default accounts, or `default` for default accounts that are not privileged.
Application Protocols	List	Used by the Port and Protocol dashboard.	See Application Protocols.
Asset/Identity Categories	List	You can use this to set up categories to use to organize an asset or identity. Common categories for assets include compliance and security standards such as PCI or functional categories such as server and web_farm. Common categories for identities include titles and roles.	See Asset/Identity Categories.
Assets	Asset list	You can manually add assets in your environment to this lookup to be included in the asset lookups used for asset correlation.	See Manually add static asset or identity data.
Demonstration Assets	Asset list	Provides sample asset data for demonstrations or examples.	Disable the lookup for use in production environments. See Disable the demo asset and identity lookups.
Demonstration Identities	Identity list	Provides sample identity data for demonstrations or examples.	Disable the lookup for use in production environments. See Disable the demo asset and identity lookups.

Lookup name	Type	Description	Usage details
ES Configuration Health Filter	Per-panel filter lookup	Per-panel filtering for the ES Configuration Health dashboard.	See Configure per-panel filtering in Splunk Enterprise Security.
Expected Views	List	Lists Enterprise Security views for analysts to monitor regularly.	See Expected Views.
HTTP Category Analysis Filter	Per-panel filter lookup	Per-panel filtering for the HTTP Category Analysis dashboard	See Configure per-panel filtering in Splunk Enterprise Security.
HTTP User Agent Analysis	Per-panel filter lookup	Per-panel filtering for the HTTP User Agent Analysis dashboard	See Configure per-panel filtering in Splunk Enterprise Security.
Identities	Identity list	You can manually edit this lookup to add identities to the identity lookup used for identity correlation.	See Manually add static asset or identity data.
IIN Lookup	List	Static list of Issuer Identification Numbers (IIN) used to identify likely credit card numbers in event data.	Used to detect Personally-Identifiable Information (PII) in your events.
Interesting Ports	List	Used by correlation searches to identify ports that are relevant to your network security policy.	See Interesting Ports.
Interesting Processes	List	Used by a correlation search to identify processes running on hosts relevant to your security policy.	See Interesting Processes.
Interesting Services	List	Used by a correlation search to identify services running on hosts relevant to your security policy.	See Interesting Services.
Local * Intel	Threat intelligence lookup	Used to manually add threat intelligence.	See Add and maintain threat intelligence locally in Splunk Enterprise Security.
Modular Action Categories	List	Used to categorize the types of adaptive response actions available to select.	Add a custom category to categorize a custom adaptive response action on Incident Review or the correlation search editor.
New Domain Analysis	Per-panel filter lookup	Per-panel filtering for the New Domain Analysis dashboard.	See Configure per-panel filtering in Splunk Enterprise Security.
PCI Domain Lookup	Identity list	Used by the Splunk App for PCI Compliance to enrich the `pci_domain` field. Contains the PCI domains relevant to the PCI standard.	See Set up asset categories.
Primary Functions	List	Identifies the primary process or service running on a host. Used by a correlation search.	See Primary Functions.
Prohibited Traffic	List	Identifies process and service traffic prohibited in your environment. Used by a correlation search.	See Prohibited Traffic.
Risk Object Types	List	The types of risk objects available.	Edit the lookup to create a custom risk object type. You can then filter on the new risk object type or add a new risk entry on the Risk Analysis dashboard. See Create risk and edit risk objects in Splunk Enterprise Security.
Security Domains	List	Lists the security domains that you can use to categorize notable events when created and on Incident Review.	Edit the lookup and add a custom security domain.
Threat Activity Filter	Per-panel filter lookup	Per-panel filtering for the Threat Activity dashboard.	See Configure per-panel filtering in Splunk Enterprise Security.

Lookup name	Type	Description	Usage details
Traffic Size Analysis	Per-panel filter lookup	Per-panel filtering for the Traffic Size Analysis dashboard.	See Configure per-panel filtering in Splunk Enterprise Security.
Urgency Levels	List	Urgency Levels contains the combinations of priority and severity that dictate the urgency of notable events.	See How urgency is assigned to notable events in Splunk Enterprise Security in *Use Splunk Enterprise Security*.
URL Length Analysis	Per-panel filter lookup	Per-panel filtering for the URL Length Analysis dashboard.	See Configure per-panel filtering in Splunk Enterprise Security.

Application Protocols

The Application Protocols list is a list of port and protocol combinations and their approval status in your organization. This list is used by the Port & Protocol Tracker dashboard. See Port & Protocol Tracker dashboard.

The following fields are available in this file.

Field	Description
`dest_port`	The destination port number. Must be a number from 0 to 65535.
`transport`	The protocol of the network traffic. For example, icmp, tcp, or udp.
`app`	The name of the application using the port.

Asset/Identity Categories

The category list can contain any set of categories you choose for organizing an asset or an identity. A category is logical classification or grouping used for assets and identities. Common choices for assets include compliance and security standards such as PCI, or functional categories such as server and web_farm. Common choices for identities include titles and roles. For more examples, see Format an asset or identity list as a lookup in Splunk Enterprise Security.

To enrich events with category information in asset and identity correlation, you must maintain the `category` field in the asset and identity lists instead of in the Asset/Identity Categories list. See Format an asset or identity list as a lookup in Splunk Enterprise Security.

There are two ways to maintain the Asset/Identity Categories list.

Run a saved search to maintain a list of categories

Splunk Enterprise Security includes a saved search that takes categories defined in the asset and identity lists and adds them to the Asset/Identity Categories list. The search is not scheduled by default.

1. From the Splunk platform menu bar, select **Settings > Searches, reports, alerts**.
2. Locate the `Identity - Make Categories - Lookup Gen` search-driven lookup or lookup generating search.
3. Click **Edit > Enable**.

Manually maintain a list of categories

Maintain the Categories list manually by adding categories to the lookup directly. By default, you must maintain the list manually.

1. Select **Configure > Content > Content Management**.
2. Click the **Asset/Identity Categories** list.

3. Add new categories to the list.
4. Click **Save**.

Expected Views

The Expected Views list specifies Splunk Enterprise Security views that are monitored on a regular basis. The View Audit dashboard uses this lookup. See View Audit for more about the dashboard.

The following table describes the fields in this file.

Field	Description
`app`	The application that contains the view. This is usually set to SplunkEnterpriseSecuritySuite.
`is_expected`	Either "true" or "false". If not specified, Splunk Enterprise Security assumes by default that the view is not expected to be monitored.
`view`	The name of the view. Available in the URL or on the Content Management dashboard.

To find the name of a view:

1. Navigate to the view in Enterprise Security.
2. Look at the last segment of the URL to find the view name.

For example, the view in the following URL below is named `incident_review`:

```
https://127.0.0.1:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review
```

Interesting Ports

Interesting Ports contains a list of TCP and UDP ports determined to be required, prohibited, or insecure in your deployment. Administrators can set a policy defining the allowed and disallowed ports and modify the lookup to match that policy. To get alerts when those ports are seen in your environment, enable the correlation search that triggers an alert for those ports, such as Prohibited Port Activity Detected.

The following table describes the fields in this file.

Field	Description	Example
`app`	The application or service name using the port.	Win32Time
`dest`	The destination host for the network service. Use a wildcard `*` to match all hosts.	DARTH*, 10.10.1.100, my_host.
`dest_pci_domain`	An optional PCI domain. Accepts a wildcard.	trust, untrust
`dest_port`	The destination port number. Accepts a wildcard.	443, 3389, 5900
`transport`	The transport protocol. Accepts a wildcard.	tcp or udp
`is_required`	If you require the service to be running, and want the correlation search to create an alert if it is not running, set to true.	true or false
`is_prohibited`	If you do not want the port to be used in your network, and want the correlation search to create an alert if it is in use, set to true.	true or false
`is_secure`	If the traffic sent through the port is secure, set to true.	true or false
`note`	Describe the service using the port and the explanation for the port policy.	

Field	Description	Example
		Unencrypted telnet services are insecure.

Interesting Processes

Interesting Processes contains a list of processes and whether you consider the processes required, prohibited, or secure to be running in your environment. Splunk Enterprise Security uses this list in the Prohibited Process Detected correlation search.

The following table describes the fields in this file.

Field	Description
app	Application name
dest	Destination of the process
dest_pci_domain	PCI domain, if available
is_required	If the process is required to be running on the destination host, set to true. Possible values are true or false.
is_prohibited	If the process is prohibited on the destination host, set to true. Possible values are true or false.
is_secure	If the process is secure, set to true. Possible values are true or false.
note	Describe any additional information about this process. For example, The telnet application is prohibited due to insecure authentication.

Interesting Services

Interesting Services contains a list of services in your deployment. The correlation search Prohibited Service Detected uses this lookup to determine whether a service is required, prohibited, and/or secure.

The following table describes the fields in this file.

Field	Description
app	Application name
dest	Destination host that the service is running on.
dest_pci_domain	PCI domain of the host, if available
is_required	If the service is required to be running on the host, set to true. Possible values are true or false.
is_prohibited	If the service is prohibited from running on the host, set to true. Possible values are true or false.
is_secure	If the service is secure, set to true. Possible values are true or false.
note	Any additional information about this service.

Primary Functions

Primary Functions contains a list of primary processes and services and their function in your deployment. Use this list to define which services are primary and the port and transport to be used by the services. This lookup is used by the Multiple Primary Functions Detected correlation search.

The following table describes the fields in this file.

Field	Description
`process`	Name of the process
`service`	Name of the service
`dest_pci_domain`	PCI domain of the destination host, if available
`transport`	Protocol used for transport by the process. Possible values are tcp or udp.
`port`	The port number used by the process.
`is_primary`	If the process is the primary process on the host, set to true. Possible values are true or false.
`function`	The function that the process performs. For example, proxy, authentication, database, Domain Name Service (DNS), web, or mail.

Prohibited Traffic

Prohibited Traffic lists processes that, if seen in your network traffic, could indicate malicious behavior. This list is used by the System Center dashboard and is useful for detecting software that is prohibited by your security policy, such as IRC, data destruction tools, file transfer software, or known malicious software, such as malware that was recently implicated in an outbreak.

The following table describes the fields in this file.

Field	Description
`app`	The name of the process (such as echo, chargen, etc.)
`is_prohibited`	If the process is prohibited in your environment, set to true. Possible values are true or false.
`note`	Add a description about why the process is prohibited.

Create risk and edit risk objects in Splunk Enterprise Security

As an ES Admin, you can create and edit risk objects.

Create a new risk object

1. From the Enterprise Security menu, select **Configure** > **Content** > **Content Management**.
2. From the Type drop-down filter, select **Lookup**.
3. (Optional) In the Search filter, type `risk object types`.
4. Select the **Risk Object Types** list.
5. Highlight the last **risk_object_type** cell in the table and right-click to see the table editor.
6. Insert a new row into the table.
7. Double-click in the new row to edit it, then add the new object type name.
8. Save the changes.

Edit an existing risk object

1. From the Enterprise Security menu, select **Configure** > **Content** > **Content Management**.
2. From the Type drop-down filter, select **Lookup**.
3. (Optional) In the Search filter, type `risk object types`.
4. Select the **Risk Object Types** list.
5. Highlight the risk object type and change the name.
6. Save the changes.

Expand Content Management searches to view dependency and usage information in Splunk Enterprise Security

In Content Management, it is possible to see more details about the knowledge objects such as data models, correlation searches, lookups, investigations, key indicators, glass tables, and reports.

Additional details

With these additional details, you can verify health status, statistics, associated knowledge objects, and that the proper technical add-ons are populating within each of objects.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. (Optional) From the Type filter, select a type such as **Search** or **Data Model**.
3. From the event information column of a search or data model, click the greater than (**>**) symbol to expand the display.

   Not every Type will include the greater than (>) symbol, and each different Type will show different details.

The following table describes the additional usage details and dependencies:

Name	Description
Status	Icon to show the overall health. If the icon is not a green checkmark, then you are not ingesting enough data for this content to report accurately.
Statistics	For searches, if the saved search is scheduled, this shows execution statistics from the _audit index. For data models, if the data model is accelerated, the execution statistics are also returned for the acceleration search.
Associated Searches	The saved searches that use this object or dataset.
Associated Panels	The panels that use this object or dataset.
Indexes	The indexes that this object or dataset uses. If the icon is a green checkmark, then the index has events for the past 24 hours.
Lookups	The lookups that this object or dataset uses. If the icon is a green checkmark, then the row counts for the csv or kvstore lookup files are not empty.
Sourcetypes	The sourcetypes that this object or dataset uses. For example, if you have Unix in your environment and you would expect to see that sourcetype listed here, but you don't see it, then you would know that you need to revise the way you're getting that data into Splunk. If the icon is a green checkmark, then the index has events for the past 24 hours.
Tags	The tags that this object or dataset uses.

Associated objects are only visible if there is data to populate them. If there is no data to populate them, then you will see a message such as "No associated objects or datasets found."

Use Analytic Stories through the use case library in Splunk Enterprise Security

The Splunk Security Research team writes Analytic Stories that provide actionable guidance for detecting, analyzing, and addressing security threats. An Analytic Story contains the searches you need to implement the story in your own Splunk Enterprise Security (ES) environment. It also provides an explanation of what the search achieves and how to convert a search into adaptive response actions, where appropriate.

The Splunk Enterprise Security Content Update (ESCU) delivers Analytic Stories to customers as part of a content subscription service. Analytic Stories give you advice on how to use Splunk ES to investigate and take action on new threats that Splunk ES detects in your environment.

The ESCU Analytic Story content is available directly in Splunk ES through the use case library. If you do not have ESCU installed, you will see some Analytic Stories by default as well as a message prompting you to download and install the ESCU add-on for access to common security Analytic Stories. When new Analytic Stories are published in newer versions of ESCU, you need to upgrade the ESCU add-on to get the new content.

Prerequisites for using the use case library include the following:

- Data is ingested via your forwarders and technical add-ons.
- The CIM add-on is installed.
- (Optional) The ESCU add-on is installed so you can access more Analytic Stories.

You can explore, activate, bookmark, and configure common searches in the use case library.

Determine which Analytic Stories to use

You can use common industry use cases to determine which Analytic Stories and searches are useful to you. There are a variety of ways to determine if an Analytic Story contains the searches you need:

- by industry use case
- by framework
- by data

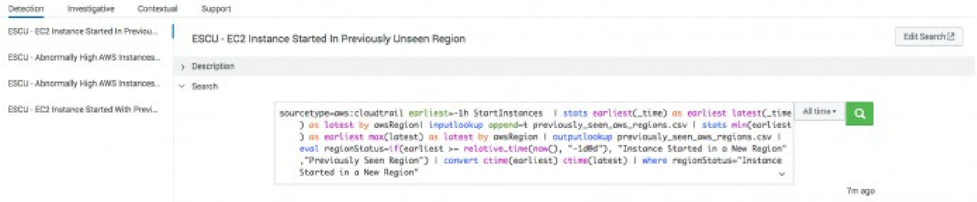
In the following scenario, you know that you're interested in common AWS-related security issues, so you start by filtering on known use cases for cloud security.

1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.
2. From the use cases filters on the left, click **Cloud Security**.
3. From an Analytic Story, such as Suspicious AWS EC2 Activities, click the greater than (>) symbol to expand the display.
4. You will see the detection searches that are related to this use case.
5. You will also see your data sources, data models, and lookups that these searches use.

Data Sources	Description
Recommended Data Sources	The type of data sources that are likely to provide valuable data.
Sourcetypes	Your sourcetypes that are in use by the detection searches for this Analytic Story. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
Data Models	Your data that is in use by the detection searches for this Analytic Story as mapped to the Splunk data models via the CIM add-on. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
Lookups	Your lookups that are in use by the detection searches for this Analytic Story. If the status icon shows a red exclamation mark, hover over the icon to see the reason.

6. Click the name of the Analytic Story. In this case, click **Suspicious AWS EC2 Activities**.
   The Analytic Story Details page opens for the story.
7. You will see the searches related to the stages of detecting, investigating, assessing, and mitigating issues.
   1. From the Detection section, select a search, such as **ESCU - EC2 Instance Started In Previously Unseen Region**.
   2. From the Search section, click the greater than (>) symbol to expand the display.

3. Revise the time picker and click **Search**.



Detection
Investigative
Contextual
Support
ESCU - EC2 Instance Started In Previou...
ESCU - Abnormally High AWS Instances...
ESCU - Abnormally High AWS Instances...
ESCU - EC2 Instance Started With Previ...
ESCU - EC2 Instance Started In Previously Unseen Region
Edit Search
Description
Search
All time
7m ago

```
sourcetype=aws:cloudtrail earliest=-1h StartInstances  | stats earliest(_time) as earliest latest(_time
    ) as latest by awsRegion| inputlookup append=t previously_seen_aws_regions.csv | stats min(earliest
    ) as earliest max(latest) as latest by awsRegion | outputlookup previously_seen_aws_regions.csv |
    eval regionStatus=if(earliest >= relative_time(now(), "-1d@d"), "Instance Started in a New Region"
    ,"Previously Seen Region") | convert ctime(earliest) ctime(latest) | where regionStatus="Instance
    Started in a New Region"
```

4. From the How to Implement section, click the greater than (**>**) symbol to expand the display for tips on implementation.
5. From the Known False Positives section, click the greater than (**>**) symbol to expand the display for tips on when the results might not indicate a problem.

If you want to run this search automatically on a regular basis, see Enable and schedule the Analytic Story.

Enable and schedule the Analytic Story

Once you determine that an Analytic Story will help you detect, investigate, assess, or mitigate an issue, you can enable and schedule it. An Analytic Story is considered "in use" when at least one search is enabled and scheduled. By default, all stories are disabled. If a search is enabled but not scheduled, or if it is run manually, then it is not considered in use.

1. From the Splunk ES menu bar, select **Configure** > **Content** > **Use Case Library**.
2. From the event information column, click the greater than (**>**) symbol to expand the display.
    1. Click the name of an ESCU detection search.
       A new content management window opens.
    2. Click **Enable**.
3. To edit the correlation search schedule, click the name of the search.
4. Click **Save**.

To modify correlation searches in your environment, see Create correlation searches in Splunk Enterprise Security.

Bookmark the Analytic Story

Bookmarks persist per user, so individual analysts can bookmark the Analytic Stories that are specific to their duties.

1. From the Splunk ES menu bar, select **Configure** > **Content** > **Use Case Library**.
2. Find the name of the Analytic Story.
3. Toggle the **Bookmark** switch to enable it.
4. From the drop-down filters, select **Bookmarked** > **True** to find your bookmarked stories.

Configure the library

You can revise how the preconfigured use case library displays your most frequently used Analytic Stories and searches.

The use case library does not require any special capability to view Analytic Stories, but it does require the `edit_analyticstories` capability to edit and add them. By default, ES assigns the `edit_analyticstories` capability to the `ess_admin` and `ess_analyst` roles. An admin can assign other roles from the Permissions setting.

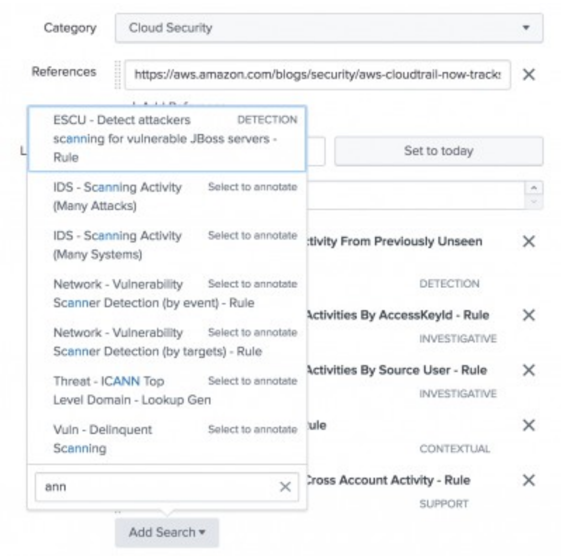
Edit or add Analytic Story details

To edit the displayed descriptions, narratives, references, or searches:

1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.
2. From the use case library, click the name of an Analytic Story to see the Analytic Story Details page, which contains all the default information that is provided by the ESCU content.
3. From the top-right of the Analytic Story Details page, click **Edit**.
4. A new browser window opens so you can change the story descriptions, narratives, or references to fit your specific usage. These changes are global, not per user, so everyone sees the same updates.
5. You can also add existing searches that do not display by default in this Analytic Story.
    1. Scroll to the Searches section.
    2. Click **Add Search**.
    3. Select the search to include in this story.
6. Click **Save**.

Search types

When you add a search in the Edit Analytic Stories window, the type of search appears to the right of the search name. By default you will see detection, investigative, contextual, support, or select to annotate.


Category
Cloud Security
References
https://aws.amazon.com/blogs/security/aws-cloudtrail-now-tracks
Set to today
ESCU - Detect attackers scanning for vulnerable JBoss servers - Rule
DETECTION
IDS - Scanning Activity (Many Attacks)
Select to annotate
IDS - Scanning Activity (Many Systems)
Select to annotate
Network - Vulnerability Scanner Detection (by event) - Rule
Select to annotate
Network - Vulnerability Scanner Detection (by targets) - Rule
Select to annotate
Threat - ICANN Top Level Domain - Lookup Gen
Select to annotate
Vuln - Delinquent Scanning
Select to annotate
ann
tivity From Previously Unseen
DETECTION
Activities By AccessKeyId - Rule
INVESTIGATIVE
Activities By Source User - Rule
INVESTIGATIVE
ule
CONTEXTUAL
Cross Account Activity - Rule
SUPPORT
Add Search ▾

Only annotated searches are associated with an Analytic Story. When you add an annotated search, the search is immediately added to the Analytic Story. In those added searches, you can click **Edit Search** to revise the annotations of that search.

If the search is not annotated, do the following to annotate it:

1. From the right side of the search name, click **Select to annotate**.
2. In the annotation editor, type the name of an existing search type or type the name a new search type in the Type field. This is the only mandatory field.
3. (Optional) If you want analysts to see information when deciding which stories and searches to use, fill in information for Description, How to Implement, Known False Positives, Providing Technologies (also known as data sources or technology add-ons).
4. (Optional) In the Annotations field, click **Add row** to add Framework names and their Mapping categories. These are free-form fields. You can use them for either industry-standard frameworks, such as National Institute of Standards and Technology issues for detecting and continuous monitoring of vulnerabilities (NIST + DE.CM), or you can use them for frameworks of your own.
   You can find these later from the Framework Mapping filter.
   1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.
   2. From the drop-down filters, click **Framework Mapping**.
   3. Type the name of a Framework or scroll to find it.
   4. Click the check box to select a Framework. The filter is using OR logic, so the more check boxes you select, the more results you will see.

The `savedsearches.conf` file is used to annotate existing saved searches.

Create an Analytic Story

You can create your own Analytic Story and map it to the searches of your choice.

The use case library does not require any special capability to view Analytic Stories, but requires the `edit_analyticstories` capability to edit and create new ones. By default, ES assigns the `edit_analyticstories` capability to the `ess_admin` and `ess_analyst` roles. An admin can assign it to other roles from the Permissions setting.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content > Analytic Story**.
3. Fill in the required fields to create your analytics story.
4. Scroll down to the **Searches** field.
5. From the Add Search drop-down menu, you can select any of the searches that have been annotated.
6. Click **Save**.

Install Analytic Stories from other apps

While ESCU content is imported automatically, you can also import Analytic Stories from apps other than ESCU into the use case library.

Install the app to see the Analytic Stories in the use case library.

1. Install the app onto the same search head as Splunk ES.
2. Export the app to other apps or globally.
3. Review the new knowledge objects. If the Analytic Stories are visible in the use case library, the export is successful.

4. Use the new Analytic Stories.

If you do not see the new Analytic Stories in the use case library, it's because of one of the following reasons:

- Make sure that the app is being exported globally. See Make Splunk knowledge objects globally available in the Splunk Enterprise *Admin Manual*.
- If the app does not contain compatible use cases, it does not contain an `analyticstories.conf` file.

Configuration and Troubleshooting

Configure general settings for Splunk Enterprise Security

As a Splunk Enterprise administrator, you can make configuration changes to your Splunk Enterprise Security installation. Change threshold values, macro definitions, search filters, and other commonly changed values on the General Settings page.

On the Enterprise Security menu bar, select **Configure** > **General** > **General Settings**.

Setting	Description
Auto Pause	Type the time in seconds before a drilldown search will pause. A value of 0 means never auto-pause. This is a search macro for performance purposes.
Default Watchlist Search	Define a search string for the `tag=watchlist` of Threat Intelligence events in the 'Watchlisted Event Observed' correlation search.
Distributed Configuration Management	Download Splunk "helper" applications for distributed deployments.
Domain Analysis	Enable or disable WHOIS tracking for Web domains. This is a search macro and when enabled, the search macro expands to **outputcheckpoint modinput=whois** by default when it is referenced in another search. When disabled, the default is **noop**.
Domain From URL Extraction Regex	A regular expression used to extract domain (url_domain) from a URL.
Event Sequencing Engine	Enables the main Event Sequencing Engine. See Create sequence templates in Splunk Enterprise Security.
Generic Error Search	A search filter for defining events that indicate an error has occurred.
HTTP Category Analysis Sparkline Earliest	Set the start time for sparklines displayed on the **HTTP User Category Analysis** dashboard.
HTTP Category Analysis Sparkline Span	Set the time span for sparklines displayed on the **HTTP User Category Analysis** dashboard.
HTTP User Agent Analysis Sparkline Earliest	Set the start time for sparklines displayed on the **HTTP User Agent Analysis** dashboard.
HTTP User Agent Analysis Sparkline Span	Set the time span for sparklines displayed on the **HTTP User Agent Analysis** dashboard.
Incident Review Analyst Capacity	Estimated maximum capacity of notable events assigned to an analyst. Relative measure of analyst workload.
Indexed Realtime	Enable/Disable Indexed Realtime. Enabling your real-times searches to run after the events are indexed can greatly improve indexing performance. Use indexed real-time search when up-to-the-second accuracy is not needed.
IRT Disk Sync Delay	Set the number of seconds for Enterprise Security to wait for a disk flush to finish. Built into indexed real-time searches is a sync (synchronizing) delay. The sync delay is a precaution so that none of the data is missed.
Large Email Threshold	An email that exceeds this size in bytes is considered large.
Licensing Event Count Filter	Define the list of indexes to exclude from the "Events Per Day" summarization.
Max running sequences	Maximum number of ongoing sequences allowed in event sequencing engine. Increasing this limit will result in additional memory overhead.

Setting	Description
Maximum Documents Per Batch Save (kvstore)	The maximum number of documents that can be saved in a single batch to a KV Store collection.
New Domain Analysis Sparkline Span	Set the time span for sparklines displayed in the **New Domain Analysis** dashboard.
Notable Modalert Pipeline	SPL for the notable event adaptive response action.
Override Email Alert Action	Override the email alert action settings to allow users to send notable events via email through adaptive response actions on the Incident Review dashboard.
PCI Compliance History Span	The bucket time span for the "Compliance History" panel on the "PCI Posture" view.
PCI Scorecard Single Value	Controls the logic for determining the color of single value visualizations on PCI Posture and Scorecards
Risk Modalert Pipeline	SPL for the risk modifier adaptive response action.
Search Disk Quota (admin)	Set the maximum amount of disk space in MB that an admin user can use to store search job results.
Search Jobs Quota (admin)	Set the maximum number of concurrent searches allowed for admin users.
Search Jobs Quota (power)	Set the maximum number of concurrent searches for power users.
Short Lived Account Length	An account creation and deletion record that falls within this threshold is anomalous.
Threat Artifacts Max	The maximum number of threat artifacts to return for unfiltered queries on the Threat Artifacts dashboard. The default is 10000, and is managed in the `` `threat_artifacts_max` `` macro editor.
Threat Intelligence Wildcard Minimum Length	Filter out wildcard intelligence that doesn't meet the minimum requirement.
Top 1M Site Source	A macro definition to indicate source to be used for Top 1M sites.
TSTATS Local	Determine whether or not the TSTATS macro will be distributed.
TSTATS Summaries Only	Determine whether or not the TSTATS or summariesonly macro will only search accelerated events.
Use Other	Enable or disable the term OTHER on charts that exceed default series limits.
Website Watchlist Search	A list of watchlisted websites used by the "Watchlisted Events" correlation search.

See also

Manage input credentials in Splunk Enterprise Security

Manage permissions in Splunk Enterprise Security

Customize the menu bar in Splunk Enterprise Security

Configure per-panel filtering in Splunk Enterprise Security

Manage credentials in Splunk Enterprise Security

Use the **Credential Management** page to store credentials for scripted or modular inputs. Input configurations that reference credentials use the credentials stored in Credential Management. You can store credentials such as usernames and passwords, or certificates used for authentication with third-party systems. Do not use this page to manage certificates used to encrypt server-to-server communications.

Your role must have the appropriate capabilities to add, modify, and view credentials and certificates. See Configure users and roles in the *Installation and Upgrade Manual*.

Add a new credential for an input

1. On the Enterprise Security menu bar, select **Configure > General > Credential Management**.
2. Click **New Credential** to add a new user credential.
3. Type a **Username**.
4. (Optional) Type a **Realm** field to differentiate between multiple credentials that have the same username.
5. Type the **Password** for the credential, and type it again in **Confirm password**.
6. Select the **App** for the credential.
7. Click **Save**.

Add a new credential for UBA input

Splunk ES uses a specific local UBA username and password authentication to integrate with Splunk User Behavior Analytics.

1. On the Enterprise Security menu bar, select **Configure > General > Credential Management**.
2. Click **New Credential** to add a new user credential.
3. Type a **Username** of **ubaesuser**.
4. Type a **Realm** of **uba**.
5. Type the same **Password** for the credential that is used in UBA for this user, and type it again in **Confirm password**.
6. Select the **App** of **SA-UEBA** for the credential.
7. Click **Save**.

For the integration to work correctly, this user needs to exist in both UBA and Splunk ES. If the password for this user needs to be changed, it needs to be the same in both places.

Edit an existing input credential

You can edit passwords of existing input credentials.

1. On the Enterprise Security menu bar, select **Configure > General > Credential Management**.
2. In the **Action** column of a credential, click **Edit**.
3. Type a new **Password** for the credential, and type it again in **Confirm password**.
4. Click **Save**.

Add a new certificate

You cannot add a new certificate using Credential Management on a search head cluster (SHC). To add a new certificate to Splunk Enterprise Security on a SHC, add the certificate to `$SPLUNK_HOME/etc/shcluster/apps/<app_name>/auth` on the deployer and deploy the certificate to the SHC members.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Credential Management**.
2. Click **New Certificate** to add a new certificate.
3. Type a **File name** for the certificate. This is the file name that the certificate is saved as in the `$SPLUNK_HOME/etc/apps/<app_name>/auth` directory.
4. Add **Certificate text** for the certificate. Paste the contents of an existing certificate file here to add the certificate to Splunk Enterprise Security.
5. Select an **App** to save the certificate in.
6. Click **Save**.

Edit an existing certificate

You can edit the certificate text of existing certificates in Credential Management. You cannot edit certificates on a search head cluster.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Credential Management**.
2. In the **Action** column of a certificate, click **Edit**.
3. Type a new **Certificate text** for the certificate.
4. Click **Save**.

Delete an existing input credential or certificate

You cannot delete certificates on a search head cluster.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Credential Management**.
2. In the **Action** column of a credential or certificate, click **Delete**.
3. Click **OK** to confirm.

Manage permissions in Splunk Enterprise Security

Use the Permissions page to view and assign Enterprise Security capabilities to non-admin roles.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Permissions**.
2. Select the checkbox for the role and permissions for that role.
3. Click **Save**.

For more information about ES capabilities, see Configure users and roles in the *Installation and Upgrade Manual*.

Manage permissions for custom roles in Splunk Enterprise Security

If you create a custom role for Enterprise Security and you want to manage it in the general permissions along with the default ES components, do the following.

1. On the Splunk Enterprise menu bar, select **Configure** > **Settings** > **Data inputs**.
2. Click **App Permissions Manager**.
3. Click **enforce_es_permissions**.
4. Add your custom role to the comma separated list of roles to be managed.
5. Click **Save**.
6. Now you can manage the role in the general permissions.

Customize the menu bar in Splunk Enterprise Security

Customize the menu bar in Splunk Enterprise Security with the Edit Navigation view. Add new **dashboards**, reports, **views**, links to filtered dashboards, or links to the web to your menu bar. You must have Enterprise Security administrator privileges to make changes to the menu bar navigation.

You can add views to the menu bar as part of a collection that groups several views together or as an individual item on the menu bar. For example, Incident Review is an individual dashboard in the menu bar, and Audit is a collection of the audit dashboards.

Splunk Enterprise Security persists customizations you made to the navigation from previous versions.

Check for updated views

Views and collections that are new, updated, or deprecated in the version of the app that you have installed are highlighted with small icons that indicate the relevant changes.

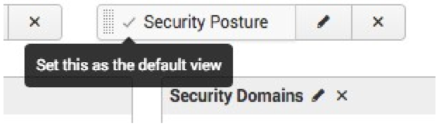
After installing a new version of Splunk Enterprise Security or a new version of an app that provides views and collections for use in Enterprise Security, visit the Edit Navigation view to check for updates in those views and collections.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Navigation**.
2. If any content has been updated, the message "Some content updates available" appears at the top of the navigation editor.
3. Look for icons on the views on the editor pane to find content that has been added, updated, or deprecated. These same icons also appear in the **Add a New View** and **Add a New Collection** menus.

Set a default view for Splunk Enterprise Security

To see a specific view when you or other users open Splunk Enterprise Security, set a default view.

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Navigation**.
2. Locate the view that you want to be the default view.
3. Click the checkmark icon that appears when you mouse over the view to **Set this as the default view**.



4. Click **Save** to save your changes
5. Click **OK** to refresh the page and view your changes.

Only views can be selected as default views.

Edit the existing menu bar navigation

1. On the Enterprise Security menu bar, select **Configure** > **General** > **Navigation**.
2. Click and drag views or collections of views to change the location of the views or collections of views in the menu.
3. Click the **X** next to a view or collection to remove it from the menu.
4. Click the ✎ icon to edit the name of a collection.
5. Click the − icon to add a divider and visually separate items in a collection.

6. Click **Save** to save your changes
7. Click **OK** to refresh the page and view your changes.

Add a single view to the menu bar

You can add a new view to the menu bar without adding it to a collection.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Click **Add a New View**.
3. Leave **View Options** set to the default of **View**.
4. Click **Select a View** from **Unused Views**.
5. Select a dashboard or view from the list.
6. Click **Save**. The dashboard appears on the navigation editor.
7. If you are finished adding items to the menu, click **Save** to save your changes
8. Click **OK** to refresh the page and view your changes.

Add a collection to the menu bar

Use a collection to organize several views or links together in the menu bar.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Click **Add a New Collection**.
3. Type a **Name**. For example, **Audit**.
4. Click **Save**. The collection appears on the navigation editor.

You must add a view or link to the collection before it appears in the menu navigation.

Add a view to an existing collection

Add views to an existing collection.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Locate the collection that you want to add views to.
3. Click the icon.
4. Leave **View Options** set to the default of **View**.
5. Click **Select a View** from **Unused Views**.
6. Select a view from the list.
7. Click **Save**. The view appears on the navigation editor.
8. If you are finished adding items to the menu, click **Save** to save your changes
9. Click **OK** to refresh the page and view your changes.

Add a link to the menu bar

You can add a link to the menu bar of Splunk Enterprise Security. For example, add a link to a specifically-filtered view of Incident Review or to an external ticketing system.

Create a link in the menu to an external system or webpage

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Click **Add a New View** to add it to the menu, or locate an existing collection and click the icon to add the link to an existing collection of views.

3. Select **Link** from **View Options**.
4. Type a **Name** to appear on the Splunk Enterprise Security menu. For example, Splunk Answers.
5. Type a link. For example, https://answers.splunk.com/
6. Click **Save**.
7. If you are finished adding items to the menu, click **Save** to save your changes
8. Click **OK** to refresh the page and view your changes.

Add a link to a filtered view of Incident Review

A common link to add to the menu bar is a filtered view of Incident Review.

1. Filter Incident Review with your desired filters. When you filter the dashboard, the URL updates with query string parameters matching your filters.
2. In the web browser address bar, copy the part of the URL that starts with `/app/SplunkEnterpriseSecuritySuite/` and paste it in a plain text file for reference.
   For example, if you filtered the dashboard to show only critical notable events, the part of the URL that you copy looks like `/app/SplunkEnterpriseSecuritySuite/incident_review?form.selected_urgency=critical`.
3. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
4. Click **Add a New View** to add it to the menu, or locate an existing collection and click the **Add View** icon to add the link to an existing collection of views.
5. Select **Link** from **View Options**.
6. Type a **Name** to appear on the Splunk Enterprise Security menu. For example, **IR - Critical**.
7. In the **Link** field, paste the URL section. For example,
   `/app/SplunkEnterpriseSecuritySuite/incident_review?form.selected_urgency=critical`
8. Click **Save**.
9. If you are finished adding items to the menu, click **Save** to save your changes.
10. Click **OK** to refresh the page and view your changes.

If you add a link with multiple parameters you must modify the query string parameters by adding `&`. For example, type the link for a filtered view of Incident Review that shows new and unassigned notable events as `/app/SplunkEnterpriseSecuritySuite/incident_review?form.status_form=1&form.owner_form=unassigned< /font>`.

You can also construct a URL manually using the parameters in the following table. Use an asterisk to show all results for a specific parameter. Not all parameters are required.

Parameter	Description	Possible values
`form.selected_urgency`	Display notable events with the urgency specified by this parameter.	critical, high, medium, low, informational
`form.status_form`	Display notable events with the status specified by this parameter. An integer corresponds to each status value.	0 for unassigned, 1 for new, 2 for in progress, 3 for pending, 4 for resolved, 5 for closed
`form.owner_form`		usernames

Parameter	Description	Possible values
	Display notable events owned by the user specified by this parameter.	
form.source	Display notable events created by the correlation search specified by this parameter. HTML-encode spaces in the correlation search name and use the name that appears in the notable event rather than the name that appears on Content Management.	Endpoint - Host With Multiple Infections - Rule
form.rule_name	Display notable events created by the correlation search specified by this parameter. HTML-encode spaces in the correlation search name. Use the name that appears on Content Management.	Host With Multiple Infections
form.tag	Displays notable events with the tag specified by this paramter.	malware, any custom tag value
form.srch	Displays notable events that match the SPL specified in this parameter. HTML-encode special characters such as = for	dest=127.0.0.1

Parameter	Description	Possible values
	key-value pairs.	
`form.security_domain_form`	Displays notable events in the security domain specified by this parameter.	access, endpoint, network, threat, identity, audit
`earliest=` and `latest=`	Displays notable events in the time range specified by these parameters. Specify a relative time range. HTML-encode special characters such as @.	-24h@h, now
`form.new_urgency_count_form`	Displays notable events that do not have the urgency specified by this parameter.	critical, high, medium, low, informational
`form.selected_urgency`	Displays notable events that have the urgency specified by this parameter. Use multiple instances of this parameter to select multiple urgency settings.	critical, high, medium, low, informational
`event_id`	Displays the notable event that matches the specified `event_id`.	3C84A9D8-87F6-4066-8659-C7DD680F98E6@@notable@@80e0f89da83cad6665dd1de7447ced
`form.association_type` `form.association_id`	Used together, displays the notable events associated with a short ID or an investigation.	short_id, investigation EYIYNW, 5a4be2b8cdc9736b2352c7c3

Restore the default navigation

To restore the default navigation of the Splunk Enterprise Security menu bar:

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. In the upper right corner, click **Restore Default Configuration**.
3. Click **OK** to confirm.
4. Scroll to the bottom of page and click **Save**.

Configure per-panel filtering in Splunk Enterprise Security

Some dashboards in Splunk Enterprise Security include the per-panel filter option, which can filter items out of dashboard views, making it easier to find those events that require investigation.

- If you determine that an event is a threat, use the per-panel filter to add the item to your deny list of known threats.
- If you determine that an event is not a threat, you can add it to your allow list to remove it from the dashboard view.

The per-panel filter button appears only if the user has permission. To configure this permission, see Configure users and roles in the *Installation and Configuration* manual.

Allow events

After you determine that an event is not a threat, you can allow the event in order to hide it from the dashboard view. After you allow an event, the summary statistics continue to calculate allowed items, but these items are not displayed in the dashboard.

Allow an event

Use the per-panel filter to allow, or filter, events on a dashboard.

For example, to allow traffic events on the **Traffic Size Analysis** dashboard:

1. Use the checkboxes to select the items to filter.
2. Click **Per-panel Filter** in the top right corner to display options for events that can be filtered in this dashboard.
3. Select the radio button to filter events on this dashboard.
   For example, on the **Traffic Size Analysis** dashboard, you can either filter events so that they no longer appear or highlight them so that they are flagged as important.
4. Click **Save** when you are done.

In this example, after an item is added to the allow list, it is no longer considered a threat and no longer appears on the **Traffic Size Analysis** dashboard.

Remove an item from the allow list

1. Click **Per-panel Filter**, then **View/edit lookup file** to see the list of entries currently being filtered.
2. Right-click a cell in the table to view the context menu.
3. Select **Remove row** to remove the row containing the allowed item.
4. Click **Save**.

Exclude events

An event can also be excluded. Excluding an item means that you have identified an event that is known to be malicious, or thought to communicate with a command and control server that is known to be malicious. Anytime the event or string shows up in the data, you will want to investigate the system, the user associated with the system, and the web activity to understand the nature and possible proliferation of the threat.

Excluding an event or string is similar to allowing it. Events can only be excluded after they have been filtered from the dashboard.

To exclude a traffic event on, for example, the **Traffic Size Analysis** dashboard, do the following:

1. Click **Per-panel Filter**, then **View/edit lookup file** to see the list of entries currently being filtered.
2. Locate the entry you want to add to the exclusion list. Under the **filter** column, double-click the word **whitelist** to edit the cell. Delete **whitelist** and type **blacklist**.
3. Click **Save**.

Edit the per-panel filter list

To see a current list of per-panel filters by dashboard, select **Configure > Content > Content Management**. Lookups with a description indicating that they are a per-panel filter show the current per-panel filters for the dashboard in the lookup name. Events added to the allow list for a dashboard are listed in that lookup.

For example, the **Threat Activity Filter** lookup displays the filters for the **Threat Activity** dashboard.

Edit the per-panel filter lookup.

1. Open the filter list for the relevant dashboard. The name of the filter, for example `ppf_threat_activity`, shows in the upper left-hand corner.
2. To edit a field, select a cell and begin typing.
3. To insert or remove a row or column in the filter, right-click the field for edit options. Removing a row adds that item back to the dashboard panel view and removes it from the allow list.
4. To exclude an item, use the editor to add a new row to the table and use **blacklist** in the **filter** column.
5. Click **Save** to save your changes.

Audit per-panel filters

Changes made to the per-panel filters are logged in the per-panel filtering audit logs. The lookup editor and the per-panel filter module modify per-panel filters. Use the Per-Panel Filter Audit dashboard to audit per-panel filters.

Create a Splunk Web message in Splunk Enterprise Security

Create a message in Splunk Web based on the results of a search using the **Create Splunk messages** alert action. Only administrators can create messages using this alert action.

The message that you create with this alert action must already exist in `messages.conf`. See Customize Splunk Web messages in the Splunk Enterprise *Admin Manual* for more about creating messages.

1. You can create Splunk Web messages from a search or from a correlation search:

Option	Steps
Create a new alert	From the **Search** page in the **Search and Reporting** app, select **Save As** > **Alert**. Type and select alert details and configure triggering and throttling as needed.
Create or edit a correlation search	From the ES menu bar, select **Configure** > **Content** > **Content Management**. Select **Create New Content** > **Correlation Search**. Type and select correlation search configurations as needed.
Edit a correlation search	From the ES menu bar, select **Configure** > **Content** > **Content Management**. Select the correlation search.

2. Click **Add Actions** and select **Create Splunk messages**.
3. Select a **Name**. The name corresponds to a stanza in `messages.conf` of an existing message.
   For example, `DISK_MON:INSUFFICIENT_DISK_SPACE_ERROR`.
4. (Optional) Type a **Message ID** that identifies the message.
   For example, `insufficient_diskspace`.
5. (Optional) If a message uses field substitution, type the **Fields** to use. The fields used for argument substitution must be returned in the search results to be included in the message. Type the fields in the order that they must be substituted in the message.
   For example, for a message `Host %s has free disk space %d, below the minimum 5GB.`, type the fields `src,FreeMBytes`.
6. (Optional) Select **Yes** for **Keep Only Latest** and keep only the latest message produced by a search.
   For example, if the host has low disk space for three days, rather than get daily messages for three days, select **Yes** for this setting to only see one message.
7. Click **Save**.

Troubleshoot script errors in Splunk Enterprise Security

Troubleshoot script errors from modular inputs in Splunk Enterprise Security. If you see a message about a script exiting abnormally or a script that is in an unknown state, investigate the script and stanza that produced the error.

The `Audit - Script Errors` search replaces a configuration check script and creates Splunk messages to warn about non-zero exit codes that result from scripts in your Splunk deployment.

Possible root cause	Verification	Mitigation
The script did not run successfully.	Review the log files for the script. Run the script manually to see if it runs successfully, and review the exit code that results.	Address the reasons why the script exited with a non-zero exit code.
The script ran successfully with a non-zero exit code.	Run the script manually to see if it runs successfully, and review the exit code that results.	Include the script in the suppression for the search so that it does not display messages for this script.
The script is in an unknown state. There is a stop time for the script, but no exit status or start time.	Check the modular input settings to confirm they are correct.	Correct the modular input settings.

See Configure a script for an alert action in the Splunk Enterprise *Alerting Manual* and What Splunk software logs about itself in the Splunk Enterprise *Troubleshooting Manual*.

Prevent messages about specific scripts

If needed, you can prevent messages about specific scripts by modifying the match syntax in the `` `script_error_msg_ignore` `` macro.

If you had locally-defined script suppression regex in the `[configuration_check://confcheck_script_errors]` stanza, you can replicate it in the macro. For example, the suppression stanza includes the following regular expression:

```
suppress = ((streamfwd|splunk
-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.exe|regmon\.exe|winprintmon\.exe|admon\.exe)).*
with code 1)
```

The macro replicates this suppression with the following definition:

```
match(script, "(streamfwd|splunk
-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.exe|regmon\.exe|winprintmon\.exe|admon\.exe|pow
AND exit_status=1
```

To reduce the frequency of messages about specific scripts rather than prevent them from appearing, throttle the alerts. Set up alert throttling for the `Audit - Script Errors` search based on the necessary values, such as the `script` field.

- For Splunk Enterprise, see Throttle alerts in the *Alerting Manual*.
- For Splunk Cloud, see Throttle alerts in the *Alerting Manual*.

Disable the configuration checker

To stop the messages by disabling the configuration checks, such as `confcheck_app_exports.py`, do the following:

1. On the Enterprise Security menu bar, select **Configure > General > Configuration Checker**.
2. Find the name of the script and click **Disable.**

Though in the case of `confcheck_app_exports.py` specifically, see Export apps globally to verify if you want to export the apps or disable the configuration checker.

Export apps globally

Splunk Enterprise Security no longer selectively imports apps and add-ons based on the name of the app or add-on. Knowledge objects in apps and add-ons that are installed on the same search head as Splunk Enterprise Security and exported to other apps or globally are visible in Splunk Enterprise Security. Apps that are not exported globally are flagged by the `confcheck_app_exports.py` health check.

To verify a global export from the search head, check the `local.meta` file of the app or add-on for `export = system`. For further details, see the "Make Splunk knowledge objects globally available" section of App architecture and object ownership in the Splunk Enterprise *Admin Manual*.

Or when installing ES in a search head cluster environment, verify that your `server.conf shclustering` configuration is in `$SPLUNK_HOME/etc/system/local/server.conf` or is in an app that exports the server configuration globally via metadata:

[server]
export = system
See Prerequisites for installing Enterprise Security in a search head cluster environment in the Splunk Enterprise *Installation and Upgrade Manual*.

Troubleshoot messages about default indexes searched by the admin role

Troubleshoot Splunk messages about default indexes searched by the admin role in the Splunk platform.

Default admin searches include summary indexes

When the admin role searches summary indexes by default, you can see decreased performance. You can stop seeing messages about this setting by limiting the indexes searched by the admin role or by disabling the search.

Limit the indexes searched by the admin role

Prevent the admin role from searching summary indexes. You can identify summary index names because the index names end in `_summary`, such as `endpoint_summary`.

1. Select **Settings > Access controls**.
2. Click **Roles**.
3. Click **admin**.
4. From **Indexes** click any summary index to remove it from the selected indexes.
5. Click **Save**.

Disable the search to prevent messages

If you do not want to limit the indexes searched by the admin role, but you want to stop seeing messages, disable the search.

1. Select **Settings > Searches, reports, and alerts**.
2. Locate the **Audit - Default Admin Search Indexes** search.
3. Select **Edit > Disable**.
4. Click **Disable**.

Default admin searches include all non-internal indexes

When the admin role searches all non-internal indexes by default, you can see decreased performance. You can stop seeing messages about this setting by limiting the indexes searched by the admin role or disabling the search.

Limit the indexes searched by the admin role

Prevent the admin role from searching all non-internal indexes.

1. Select **Settings > Access controls**.
2. Click **Roles**.
3. Click **admin**.
4. From **Indexes** click **All non-internal indexes** to remove it from the selected indexes.
5. Click **Save**.

Disable the search to prevent messages

If you do not want to limit the indexes searched by the admin role, but you want to stop seeing messages, disable the search.

1. Select **Settings > Searches, reports, and alerts**.
2. Locate the **Audit - Default Admin Search All Non-Internal** search.
3. Select **Edit > Disable**.
4. Click **Disable**.

Troubleshoot messages about unnecessary read or write access to investigation KV store collections

Troubleshoot Splunk Web messages about roles that have unnecessary read or write access to the investigation KV store collections.

You might see the following error messages in Splunk Web:

Health Check: Review roles for unnecessary read or write access to the investigation_attachment collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigation_event collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigative_canvas_entries collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the files collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigation collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigative_canvas collection and remove access if possible

These messages are produced by the `Audit - Investigation Collection ACLs` saved search. The search looks for non-admin permissions to the investigation KV store collections.

Remove the unnecessary read or write access from the collections

If you see these messages, remove the corresponding `[collections/<stanza_name>]` collections from `$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/metadata/local.meta`. Access to these collections by non-admin roles is not recommended. After making the changes, refresh the file cache from Splunk Web: `http://<yoursplunkserver>:8000/en-us/debug/refresh?`.

In a search head cluster environment, make these changes to the `local.meta` file on each member in the cluster, via the deployer if applicable. Then refresh the file cache from Splunk Web for each search head: `http://<yoursplunkserver>:8000/en-us/debug/refresh?`. Alternately, if there are more than a few members in the cluster, a rolling restart can be used instead of the debug/refresh command.

Troubleshoot failed intelligence downloads in Splunk Enterprise Security

If you receive the message that a threat list failed to download, there are several possible root causes.

Possible root cause	Verification	Mitigation
The threat or intelligence source is no longer available at the IP address or URL.	Attempt to visit the URL or curl the threat source manually.	Disable the intelligence source if it is no longer available to

Possible root cause	Verification	Mitigation
		download.
Firewall or proxy settings are preventing the intelligence source from being accessed.	Test if you can visit the URL or curl the intelligence source manually on a different machine.	Modify the firewall or proxy settings to allow access to the intelligence source.

Troubleshoot dashboards in Splunk Enterprise Security

Each dashboard in Enterprise Security references data from various data models. Without the relevant data, the dashboards will remain empty. If you expect data to appear, or if the data appearing is older than you expect, follow these troubleshooting steps.

1. Perform a search against the data model. Click **Open in Search** in the lower left corner of a dashboard view to perform a direct search against the data model. The **New Search** dashboard also exposes the search commands and objects used to populate a particular view.
2. If the search yields no results, determine if any data required for a dashboard is available in the data model.
    1. See the Dashboard requirements matrix in this manual to determine the data model datasets used by a dashboard.
    2. Use the data model and data model dataset to search for events in the data model.

Action	Search	Expected Result
Verify the data is normalized to the Common Information Model	| datamodel **data_model_name root_object_name** search | table _time, sourcetype, **root_object_name.*** For example, `| datamodel Network_Traffic All_Traffic search	dedup sourcetype	table _time, sourcetype, All_Traffic.*`	Returns a list of sourcetypes and the data model objects and fields populated by that sourcetype.

3. If no data is available, confirm the data model is being accelerated.
    1. In Enterprise Security, browse to **Audit** > **Data Model Audit**.
    2. Review the **Acceleration Details** panel for information about the data model acceleration status, such as when the latest data model acceleration occurred, or whether it is 100% complete. See Configure data models for Splunk Enterprise Security in the *Installation and Upgrade Manual*.
4. If the data model acceleration status is as expected, validate that additional required data sources are available. For example, the **User Activity** dashboard uses additional data sources.

Dashboard Name	Data type	Data source
User Activity	Lookups	The **Cloud Domains**, **Corporate Email Domains**, and **Corporate Web Domains** lookup files.
	Identities	The Identity fields: `bunit`, `email`, `watchlist`, `work_city`, `work_country`, `work_lat`, and `work_long`. For more details, see Identity lookup fields in this manual.
	Correlation Searches	* High Volume Email Activity with Non-corporate Domains * Watchlisted Event Observed * Web Uploads to Non-corporate Sites by Users
Access Anomalies	Correlation Searches	* Impossible Travel Events Detected For Users

Troubleshoot lookups in Splunk Enterprise Security

Troubleshoot Splunk issues regarding lookups and available memory.

Lookups not respecting ASCII name order

Splunk Enterprise does not honor lexicographical order of automatic search-time lookups when some of the lookups in a set are configured to execute in-memory versus when some of the lookups in the set are configured to be indexed.

For instance, if you have `max_memtable_bytes` set to 50MB, `assets_by_cidr` lookup set to 25MB, and `assets_by_str` lookup set to 75MB. This would cause `assets_by_str` to be indexed and `assets_by_cidr` to run in memory, resulting in `assets_by_cidr` inadvertently executing prior to `assets_by_str`.

Increase the `max_memtable_bytes` of the `lookup` stanza in the `$SPLUNK_HOME/etc/system/default/limits.conf` file. See limits.conf in the Splunk Enterprise *Admin Manual*.

Lookup tables exceeding the maximum length

Lookup table files that exceed the HTTP `httpServer:max_content_length` in `server.conf` will not be replicated across search head cluster members.

Increase the `max_content_length` of the `http_input` stanza in the `$SPLUNK_HOME/etc/system/default/server.conf` file. See server.conf in the Splunk Enterprise *Admin Manual*.

Lookup files growing in excess of 1GB

Lookup table files involved in special search matches, such as CIDR or Wildcard, are required to run in memory. This can lead to running out of memory when using these features.

Increase the `max_memtable_bytes` of the `lookup` stanza in the `$SPLUNK_HOME/etc/system/default/limits.conf` file. See limits.conf in the Splunk Enterprise *Admin Manual*.

Dashboard requirements matrix for Splunk Enterprise Security

The Enterprise Security dashboards rely on events that conform to the Common Information Model (CIM), and are populated from data model accelerations unless otherwise noted.

Dashboard panel to data model

A - E

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Access Anomalies	Geographically Improbable Accesses	Relies on the **gia_summary** summary index, which is populated by the **Access - Geographically Improbable**	Authentication.app, .src, .user

Dashboard Name	Panel Title	Data Model	Data Model Dataset
		Access - Summary Gen search. That search references the Authentication data model.	
	Concurrent Application Accesses	Authentication	Authentication.app, .src, .user
Access Center	Access Over Time By Action	Authentication	Authentication.action
	Access Over Time By App		Authentication.app
	Top Access By Source		Authentication.src
	Top Access By Unique User		Authentication.user,.src
Access Search			Authentication.action, .app, src, .dest, .user, src_user
Access Tracker	First Time Access - Last 7 days	None. Calls access_tracker lookup	
	Inactive Account Usage - Last 90 days		
	Completely Inactive Accounts - Last 90 days		
	Account Usage For Expired Identities - Last 7 days	Authentication	Authentication.dest
Account Management	Account Management Over Time	Change	All_Changes.Account_Management, .action
	Account Lockouts		All_Changes.Account_Management, .result
	Account Management By Source User		All_Changes.Account_Management, .src_user
	Top Account Management Events		All_Changes.Account_Management, .action
Asset Center	Assets By Priority	Assets And Identities	All_Assets.priority, .bunit, .category, .owner
	Assets By Business Unit		
	Assets By Category		
	Asset Information		
Asset Investigator	Asset Investigator	Based on swim lane selection	
Dashboard Name	**Panel Title**	**Data Model**	**Data Model Dataset**
Data Protection	Data Integrity Control By Index	Incident Management	
	Sensitive Data	None. Calls a REST search on indexes checking for data integrity controls.	
Default Account Activity	Default Account Usage Over Time By App	Authentication	Authentication.Default_Authentication, .action, .app
	Default Accounts In Use		Authentication.user_category, .dest, .user
	Default Local Accounts	None. Calls useraccounts_tracker lookup	
DNS Activity	Top Reply Codes By Unique Sources	Network Resolution DNS	DNS.message_type, DNS.reply_code
	Top DNS Query Sources		DNS.message_type, DNS.src

Dashboard Name	Panel Title	Data Model	Data Model Dataset
	Top DNS Queries		DNS.message_type, DNS.query
	Queries Per Domain		DNS.message_type, DNS.query
	Recent DNS Queries		DNS.message_type
DNS Search			DNS.message_type, DNS.reply_code, DNS.dest, DNS.src ,DNS.query_type, DNS.query, DNS.answer

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Email Activity	Top Email Sources	Email	All_Email.src
	Large Emails		All_Email.size, src, .src_user, .dest
	Rarely Seen Senders		All_Email.protocol, .src, .src_user, .recipient
	Rarely Seen Receivers		All_Email.protocol, .src, .recipient
Email Search			All_Email.protocol, .recipient, .src, .src_user, .dest
Endpoint Changes	Endpoint Changes By Action	Change	All_Changes.Endpoint_Changes, .action
	Endpoint Changes By Type		All_Changes.Endpoint_Changes, .object_category
	Endpoint Changes By System		All_Changes.Endpoint_Changes, .object_category, .dest

F - M

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Forwarder Audit	Event Count Over Time By Host	None. Calls host_eventcount macro and search.	
	Hosts By Last Report Time		
	Splunkd Process Utilization	Endpoint	Endpoint.Processes.cpu_load_percent, .mem_used, .process_exec, Endpoint_Ports_ fillnull_dest.dest
	Splunk Service Start Mode		All_Application_State.Services.start_mode, .status, .service
HTTP Category Analysis	Category Distribution	Web	Web.src, .category
	Category Details		Web.src, .dest, .category,
HTTP User Agent Analysis	User Agent Distribution	Web	Web.http_user_agent_length, .http_user_agent
	User Agent Details		Web.http_user_agent_length, .src, .dest, .http_user_agent

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Identity Center	Identities By Priority	Assets and Identities	All_Identities.priority, .bunit, .category
	Identities By Business Unit		

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Identity Investigator	Identities By Category	Based on swim lane selection	
	Identity Information		
	Identity Investigator		
Incident Review Audit	Review Activity By Reviewer	None. Calls a search over the es_notable_events KV Store collection.	
	Top Reviewers		
	Notable Events By Status - Last 48 hours		
	Notable Events By Owner - Last 24 hours		
	Recent Review Activity		
Indexing Audit	Events Per Day Over Time	None. Calls a search over the licensing_epd KV Store collection.	
	Events Per Day		
	Events Per Index (Last Day)		
Intrusion Center	Attacks Over Time By Severity	Intrusion Detection	IDS_Attacks.severity
	Top Attacks		IDS_Attacks.dest, .src, .signature
	Scanning Activity (Many Attacks)		IDS_Attacks.signature
	New Attacks		IDS_Attacks.ids_type
Intrusion Search			IDS_Attacks.severity, .category, .signature, .src, .dest
Investigations	Investigations	None. Calls a search over the investigation KV Store collection.	
	Investigation timelines	None. Calls a search over the investigation_event KV Store collection.	
	Investigation note attachments	None. Calls a search over the investigation_attachment KV Store collection.	
	Action history	None. Calls one of five different searches. See Manage investigations in Splunk Enterprise Security.	
	Investigation workbench artifacts	None. Calls a search over the investigation_leads KV Store collection.	
Investigation workbench	Authentication Data	Authentication	Authentication.app, .action, .src, .src_user, .dest, .user
	Certificate Activity	Certificates	Certificates.SSL, .src, .src_port, .dest, .dest_port, .ssl_is_valid, .ssl_validity_window, .ssl_hash, .ssl_serial, .ssl_subject, .ssl_start_time, .ssl_end_time
	Computer Inventory	Inventory	Compute_Inventory.All_Inventory, .os, .vendor_product, .user, .dest
	DNS Data	Network Resolution DNS	Network_Resolution.DNS, DNS.dest, .query, .query_count, .message_type, .answer, .reply_code
	Email Data	Email	Email.All_Email, .src, .dest, .src_user, .action, .recipient, .recipient_count, .subject

	Panel Title	Data Model	Data Model Dataset
Dashboard Name	Filesystem Changes	Change	Change.All_Changes, .user, .dest, .action, .status, All_Changes.Endpoint_Changes.Filesystem_Changes, .file_name, .file_hash, .file_path, .file_size, .file_create_time, .file_modify_time, .file_access_time
	IDS Alerts	Intrusion Detection	Intrusion_Detection.IDS_Attacks, .user, .src, .dest, .severity, .category, .signature, .ids_type, .vendor_product, .dvc
	Latest OS Updates	Updates	Updates.status, .dest, .signature_id, .signature, .vendor_product
	Network Session Data	Network Sessions	Network_Sessions.All_Sessions, .src_ip, .dest_ip, .dest_nt_host, .tag, .action, .vendor_product
	Network Traffic Data	Network Traffic	Network_Traffic.All_Traffic, .packets, .src_ip, .dest_ip, .user, .transport, .action, .src, .src_port, .dest, .dest_port
	Notable Events	Incident Management	Incident_Management.Notable_Events, .user, .src, .dest, .rule_name, .severity, .urgency, .security_domain, .status_label, .owner, .savedsearch_description
	Port Activity	Endpoint	Endpoint.Ports, .dest_port, .transport, .process_id
	Process Activity	Endpoint	Endpoint_Application_State, .dest, .user, .process_name, .process
	Registry Activity	Change	Change.All_Changes, .user, .dest, .action, .status, .object, object_path, .object_attrs, .object_id, .Endpoint_Changes.Registry_Changes
	Risk Scores	Risk Analysis	Risk.All_Risk, .risk_score, .risk_object_type, .risk_object
	Service Activity	Endpoint	Endpoint.Processes, .user_id, .process_exec, .process_id
	System Vulnerabilities	Vulnerabilities	Vulnerabilities.Vulnerabilities, .user, .dest, .severity, .signature, .category, .vendor_product
	User Account Changes	Change	Change.All_Changes, .user, .dest, .action, .status, .object, .object_path, .object_attrs, .object_id, .Account_Management
	Web Activity	Web	Web.Web, .src, .dest, .user, .action, .http_method, .url, .http_referrer, .http_user_agent, .http_content_type, .status

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Malware Center	Malware Activity Over Time By Action	Malware	Malware_Attacks.action
	Malware Activity Over Time By Signature		Malware_Attacks.signature
	Top Infections		Malware_Attacks.signature, .dest
	New Malware - Last 30 Days	None. Calls malware_tracker lookup.	
Malware Operations	Clients By Product Version	None. Calls malware_operations_tracker lookup.	
	Clients By Signature Version		

Dashboard Name	Panel Title	Data Model	Data Model Dataset
	Oldest Infections		
Malware Search	Repeat Infections	Malware	Malware_Attacks.action, .signature, .dest
			Malware_Attacks.action, .file_name, .user, .signature, .dest
Managed Lookups Audit	Lookups	None. Calls | rest /services/data/transforms/managed_lookups	
	Action Invocations Over Time By Name	Splunk Audit Logs	Modular_Actions.Modular_Action_Invocations, .action_name
Modular Action Center	Top Actions By Name		Modular_Actions.Modular_Action_Invocations, .action_mode, .user, .duration, .search_name, .rid, .sid
	Top Actions By Search		Modular_Actions.Modular_Action_Invocations, .action_name, .action_mode, .user, .search_name, .rid, .sid

N - S

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Network Changes	Network Changes By Action	Change	All_Changes.Network_Changes, .action
	Network Changes By Device		All_Changes.Network_Changes, .dvc
New Domain Analysis	New Domain Activity	Web	Web.dest
	New Domain Activity By Age		
	New Domain Activity By TLD		
	Registration Details	None	

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Port & Protocol Tracker	Port/Protocol Profiler	Network Traffic	All_Traffic.transport, .dest_port
	Prohibited Or Insecure Traffic Over Time - Last 24 Hours		All_Traffic.src_category, .dest_category, .src, .dest, .transport, .dest_port
	Prohibited Traffic Details - Last 24 Hours		All_Traffic.src_category, .dest_category, .src, .dest, .transport, .dest_port
	New Port Activity - Last 7 Days	None. Calls the application protocols lookup.	
Protocol Center	Connections By Protocol	Network Traffic	All_Traffic.app
	Usage By Protocol		All_Traffic.app, .bytes
	Top Connection Sources		All_Traffic.src
	Usage For Well Known Ports		All_Traffic.bytes, .dest_port
	Long Lived Connections		All_Traffic.src, .src_port, .duration, .dest, .dest_port, .transport
Risk Analysis	Risk Modifiers Over Time	Risk Analysis	All_Risk.risk_score

Dashboard Name	Panel Title	Data Model	Data Model Dataset
	Risk Score By Object		All_Risk.risk_score
	Most Active Sources		All_Risk.risk_score, .risk_object
	Recent Risk Modifiers		All_Risk.*

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Security Posture	Notable Events By Urgency	None. Calls a search over the es_notable_events KVStore collection.	
	Notable Events Over Time		
	Top Notable Events		
	Top Notable Event Sources		
Session Center	Sessions Over Time	Network Sessions	All_Sessions.Session_*
	Session Details		All_Sessions.*
SSL Activity	SSL Activity By Common Name	Certificates	All_Certificates.SSL.ssl_subject_common_name
	SSL Cloud Sessions		All_Certificates.SSL.ssl_subject_common_name, .src,
	Recent SSL Sessions		
SSL Search			All_Certificates.src, .dest, .ssl_subject_common_name, .ssl_subject_email, .ssl_issuer_common_name, .ssl_issuer_organization, .ssl_start_time, .ssl_end_time, .ssl_validity_window, .ssl_is_valid
Suppression Audit	Suppressed Events Over Time - Last 24 Hours	None	Calls a macro to search on notable events.
	Suppression History Over Time - Last 30 Days		Calls a macro and a search on Summary Gen information.
	Suppression Management Activity		Calls a search by eventtype.
	Expired Suppressions		Calls a search by eventtype.
System Center	Operating Systems	None. Calls system_version_tracker lookup.	
	Top-Average CPU Load By System	Performance	All_Performance.CPU.cpu_load_percent, All_Performance.dest
	Services By System Count	Endpoint	Endpoint.Services
	Ports By System Count		Endpoint.Ports

T - Z

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Threat Activity	Threat Activity Over Time	Intrusion Detection, Network Traffic, and Web. For more details, see Threat Activity Data Sources.	
	Most Active Threat Collections		
	Most Active Threat Sources		
	Threat Activity Details		
Threat Artifacts	Threat Overview		

Dashboard Name	Panel Title	Data Model	Data Model Dataset
		None. Calls the threat intelligence KV Store collections. For a list of threat intelligence collections, see Supported types of threat intelligence in Splunk Enterprise Security.	
	Endpoint Artifacts		
	Network Artifacts		
	Email Artifacts		
	Certificate Artifacts		
Threat Intelligence Audit	Threat Intelligence Downloads	None. Calls a search by REST endpoint.	
	Threat Intelligence Audit Events	None. Calls a search by eventtype.	
Time Center	Time Synchronization Failures	Performance	All_Performance.OS.Timesync, All_Performance.dest, .dest_should_timesync, OS.Timesync.action
	Systems Not Time Synching		
	Indexing Time Delay	None. Calls the results of a Summary Gen search.	
	Time Service Start Mode Anomalies	Endpoint	Endpoint_Services_fillnull_start_mode, Endpoint_Services_fillnull_status, Endpoint_Services_fillnull_dest .dest_should_timesync, .tag
Traffic Center	Traffic Over Time By Action	Network Traffic	All_Traffic.action
	Traffic Over Time By Protocol		All_Traffic.transport
	Scanning Activity (Many Systems)		All_Traffic.dest, .src
	Top Sources		All_Traffic.src
Traffic Search			All_Traffic.action, .src_port, .src, .dest, .transport, .dest_port
Traffic Size Analysis	Traffic Size Anomalies Over Time	Network Traffic	All_Traffic.transport, .src
	Traffic Size Details		All_Traffic.bytes, .dest, .src
Dashboard Name	**Panel Title**	**Data Model**	**Data Model Dataset**
Update Center	Top Systems Needing Updates	Updates	Updates.status, .dest, .signature_id, .vendor_product
	Top Updates Needed		Updates.status, .dest, .signature_id, .vendor_product
	Systems Not Updating - Greater Than 30 Days		Updates.dest_should_update, .dest, .signature_id, .vendor_product, .status
	Update Service Start Mode Anomalies	Endpoint	Endpoint_Services_fillnull_start_mode, Endpoint_Services_fillnull_status, .Services.service_exec, .tag
Update Search		Updates	Updates.dest_should_update, .status, .dest, .signature_id, .vendor_product
URL Length Analysis	URL Length Anomalies Over Time	Web	Web.http_method, .url
	URL Length Details		Web.url_length, .src, .dest, .url
User Activity	Users By Risk Scores	Risk Analysis	All_Risk.risk_object
	Non-corporate Web Uploads	Web	Web.bytes, .user, .http_method, .url

Dashboard Name	Panel Title	Data Model	Data Model Dataset
	Non-corporate Email Activity	Email	All_Email.size, .recipient, .src_user,
	Watchlisted Site Activity	Web	Web.src, .url
	Remote Access	Authentication	Authentication.src, .user
	Ticket Activity	Ticket Management	All_Ticket_Management.description, .priority, . severity, .src_user

Dashboard Name	Panel Title	Data Model	Data Model Dataset
View Audit	View Activity Over Time	Splunk Audit Logs	View_Activity.app, .view
	Expected View Activity		View_Activity.app, .view, .user
Vulnerability Center	Top Vulnerabilities	Vulnerabilities	Vulnerabilities.signature, .dest
	Most Vulnerable Hosts		Vulnerabilities.signature, .severity, .dest
	Vulnerabilities By Severity		Vulnerabilities.signature, .severity, .dest
	New Vulnerabilities	Calls vuln_signature_reference lookup.	
Vulnerability Operations	Scan Activity Over Time	Vulnerabilities	Vulnerabilities.dest
	Vulnerabilities By Age	Calls vulnerability_tracker lookup.	
	Delinquent Scanning	Vulnerabilities	Vulnerabilities.dest
Vulnerability Search			Vulnerabilities.category, .signature, .dest, .severity, .cve,
Web Center	Events Over Time By Method	Web	Web.http_method
	Events Over Time By Status		Web.status
	Top Sources		Web.dest, .src
	Top Destinations		Web.dest, .src
Web Search			Web.http_method, .status, .src, .dest, .url

Dashboards to Add-on

Add-on dashboards are included in Splunk Enterprise Security. Use the navigation editor to add or rearrange dashboards on the menu bar. For more information about using the navigation editor, see Customize the menu bar in Splunk Enterprise Security.

To view the entire list of dashboards in Enterprise Security, select **Search** > **Dashboards**.

To review the list of dashboards in Enterprise Security by add-on, use Content Management and filter by app or data model. See Expand Content Management searches to view dependency and usage information in Splunk Enterprise Security.

Enable Debug Logging in Splunk Enterprise Security

You can enable debug logging for each component in Splunk Enterprise Security. See Enable debug logging in the Splunk Enterprise *Troubleshooting Manual* for general information about debug logging.

Enable Debug Logging for Adaptive Response Actions

Adaptive Response Actions have a global `param.verbose` setting that can be applied to the alert_actions.conf file to affect all invocations of the action. You can also use the savedsearches.conf file to place the action in "debug mode" for action invocations specific to that saved search.

To enable debug logging through the CLI, edit the savedsearches.conf file as follows:

```
## $SPLUNK_HOME/etc/apps/<app>/local/savedsearches.conf
[<search_name>]
...
action.<action_name>.param.verbose = true
...
```

After changing the parameter, reload savedsearches from the UI.

To enable debug logging through the GUI, set verbose to true in the following location:

1. From the Splunk platform menu bar, select **Settings** and click **Searches, Reports, and Alerts**.
2. Search for the name of saved search using the search filter.
3. Click **Edit > Advanced Edit**.
4. Scroll to **action.<action_name>.param.verbose**
5. Set it to **true**.
6. Click **Save**.

See Set up adaptive response actions in Splunk Enterprise Security in the *Administer Splunk Enterprise Security* manual for general information about adaptive response actions.

Enable Debug Logging for Custom Search Commands protocol, Version 2

See Create custom search commands for apps in Splunk Cloud or Splunk Enterprise in the Developer Guide on the Developer Portal for information about version 2 of the Custom Search Command protocol.

You can use the "| noop log_DEBUG=*" command to set the Version 2 Custom Search Command protocol, or chunked, logging level to debug. This works due to a stream handler that sends the logging output to the sys.stderr stream, which is used by searches and displayed in the search.log.

To set the noop command, append it to the end of your chunked custom search, for example:

```
| ... | <chunked_search_command> | noop log_DEBUG=*
```

Enable Debug Logging for Custom Search Command protocol, Version 1

Version 1 of the Custom Search Command protocol, or Intersplunk search command, currently does not respect "| noop log_DEBUG=*". Log levels can only be modified by altering the command python script at your own risk. Intersplunk search commands currently log to their own explicit log files instead of search.log.

See Create a custom search command using Intersplunk.py for information about version 1 of the Custom Search Command protocol.

Enable Debug Logging for Extensible Administration Interface Handlers

Extensible Administration Interface (EAI) handlers log levels can be modified by altering the handler python script at your own risk.

See `[admin_external:<uniqueName>]` from restmap.conf in the Splunk Enterprise *Admin Manual* for general information about EAI handlers.

Enable Debug Logging for Modular Inputs

Modular inputs use a globally defined "debug" setting" that can be toggled in the inputs.conf file.

To enable debug logging through the CLI, edit the inputs.conf file as follows:

```
## $SPLUNK_HOME/etc/apps/<app>/local/inputs.conf
[<modular_input_name>://<module_input_instance>]
debug = true
```

To enable debug logging through the UI for most modular inputs, it is similar to the following:

1. From the Splunk platform menu bar, select **Settings** and click **Data inputs**.
2. Select a modular input such as **Threat Intelligence Manager**.
3. Click an input such as **da_ess_threat_local**.
4. Check the check box for **Debug**.
5. Click **Save**.

To enable debug logging through the UI for Asset and Identity Management:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.
3. Enable the toggle switch for **Debug Mode**.
4. Click **Save**.

See Modular inputs overview in the Splunk Enterprise *Developing Views and Apps for Splunk Web* manual for information about modular inputs.

Enable Debug Logging for Script Handlers

Script handlers can use the `script.args.<N> = debug` setting in the restmap.conf file to enable debug mode (N here is an integer). Please note that the `scripttype` setting must be set to "persist" for this to work.

You cannot currently edit script.args in the restmap.conf file through the GUI.

To enable debug logging through the CLI, edit the restmap.conf file as follows:

```
## $SPLUNK_HOME/etc/apps/<app>/local/restmap.conf
[script:<script_handler_name>]
...
script.arg.<N> = debug
...
```

See restmap.conf in the Splunk Enterprise *Admin Manual* for general information about script handlers.

Enable Debug Logging for Scripted Lookups

No UI or CLI methods are available for enabling debug logging of scripted lookups.

See Configure external lookups in the Splunk Enterprise *Knowledge Manager Manual* for general info about scripted lookups.

Log files in Splunk Enterprise Security

Splunk Enterprise Security uses many custom log files to log errors and activity specific to the application.

Use the log files to check for activity

You can check the log files for errors and activity. The path for all log files is `$SPLUNK_HOME/var/log/splunk/`.

analyticstory_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
analyticstory_rest_handler	Analytic Stories: REST Handler	SA-ThreatIntelligence	Logs create, read, update, and delete (CRUD) operations for analytics stories.

app_certs_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
app_certs_rest_handler	Application Certificates: REST Handler	SA-Utils	Logs CRUD options for certificates uploaded via the "Credential Management" page.

app_imports_update.log

Sourcetype	Component	Eai:acl.app	Description
app_imports_update	App Imports Update: REST Handler	SA-Utils	Checks if apps, which had previously been imported, are not exporting their knowledge objects globally so that they are visible within ES. The output is complementary to the configuration_check.log file.

app_permissions_manager.log

Sourcetype	Component	Eai:acl.app	Description
app_permissions_manager	App Permissions: Modular Input	SplunkEnterpriseSecuritySuite	Logs when permissions policies are changed or enforced.

app_permissions_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
app_permissions_rest_handler	App Permissions: REST Handler	SplunkEnterpriseSecuritySuite	Persistent rest handler for returning a list of ES permissions related to the the ess_permissions page.

appmaker_base_class.log

Sourcetype	Component	Eai:acl.app	Description
appmaker:base_class	App Maker: Base	SA-Utils	Super class for all the appmaker scripts. The make_on_prem.py script is used on Distributed Conf Management, which also has its own log file. The make_index_time_properties.py script is used by Distribute Conf Download. Th make_content_pack.py script is used on Content Management when exporting knowledge objects.

appmaker_make_content_pack.log

Sourcetype	Component	Eai:acl.app	Description
appmaker:make_content_pack	App Maker: Make Content Pack	SA-Utils	Logs when exporting from Content Management into an app.

appmaker_make_on_prem.log

Sourcetype	Component	Eai:acl.app	Description
appmaker:make_on_prem	App Maker: Make On Prem	SA-Utils	Logs when downloading the distributed configuration management application "Splunk_TA_AROnPrem" in General Settings.

appmaker_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
appmaker:rest_handler	App Maker: REST Handler	SA-Utils	Logs export requests from the Content Management page, including the export package name as well as the download requests for exported packages.

apps_shc_es_deployer_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
apps_shc_es_deployer_rest_handler	SHC Installer: REST Handler	SplunkEnterpriseSecuritySuite	Persistent rest handler for managing apps on a search head cluster deployer.

configuration_check.log

Sourcetype	Component	Eai:acl.app	Description
configuration_check	Configuration Check: Modular Input	SA-Utils	Logs output messages of the confcheck migration scripts, such as when migration from correlationsearches.conf to savedsearches.conf fails.

contentinfo.log

Sourcetype	Component	Eai:acl.app	Description
contentinfo	ContentInfo: Search Command	SA-Utils	Logs the data sources referenced by contentinfo search-related objects.

contentinfo_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
contentinfo_rest_handler	ContentInfo: REST Handler	SA-Utils	Logs errors and successful operations to the contentinfo REST handler and associated components, as used mostly by the Use Case Library and Analytic Story pages.

correlationmigration_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
correlationsearches:migration_rest_handler	Correlation Migration: REST Handler	SA-ThreatIntelligence	Logs when migration from correlationsearches.conf to savedsearches.conf fails.

customsearchbuilder_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
customsearchbuilder:rest_handler	Custom Search Builder: REST Handler	SA-ThreatIntelligence	Logs when the search syntax of a correlation search, a lookup generating search, or an Assets and Identities LDAP search cannot be created or is incorrect.

data_migrator.log

Sourcetype	Component	Eai:acl.app	Description
data_migrator	Data Migrator: Modular Input	SA-Utils	Logs migration operations during ES upgrades. For example, when searches are executed as first-time run tasks or when a CSV lookup table is migrated to a KV store collection during an app upgrade.

datamodelsimple.log

Sourcetype	Component	Eai:acl.app	Description
datamodelsimple	Data Model Simple: Search Command	Splunk_SA_CIM	Logs when datamodelsimple starts and finishes processing in a search command.

entity_merge.log

Sourcetype	Component	Eai:acl.app	Description
identity_correlation:merge	Identity Correlation Merge: Search Command	SA-IdentityManagement	Logs the status of the search process during asset and identity merge.

es_investigations_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
es_investigations_rest_handler	ES Investigations Conf: REST Handler	SplunkEnterpriseSecuritySuite	Returns knowledge objects and handles change request for them, also enforces schemas and other stanza-specific prefixes and so on.

esconfighealth.log

Sourcetype	Component	Eai:acl.app	Description
esconfighealth	ES Configuration Health: Search Command	SplunkEnterpriseSecuritySuite	For installation and upgrade, logs the health of ES configurations against a manifest file that ships with each ES release. This typically logs as a result of running a config health check through the ES Configuration Health custom search command feature.

ess_configured_handler.log

Sourcetype	Component	Eai:acl.app	Description
ess_configured_handler		SplunkEnterpriseSecuritySuite	

Sourcetype	Component	Eai:acl.app	Description
	ES Configured: REST Handler		Logs current configured version state of search head cluster captains and search head cluster members for ES during setup and reset.

ess_content_importer.log

Sourcetype	Component	Eai:acl.app	Description
ess_content_importer	ES Content Importer: Modular Input	SplunkEnterpriseSecuritySuite	Logs when importing content from installed apps.

essinstaller2.log

Sourcetype	Component	Eai:acl.app	Description
essinstall2	ES Installer: Search Command	SplunkEnterpriseSecuritySuite	Logs installation status after setup completes.

event_sequencing_engine.log

Sourcetype	Component	Eai:acl.app	Description
event_sequencing_engine_log	Event Sequencing Engine: Search Command	SplunkEnterpriseSecuritySuite	Logs event sequencing engine operations such as terminate for sequence templates.

expectedactivity.log

Sourcetype	Component	Eai:acl.app	Description
expectedactivity	Expected Activity: Search Command	SA-Utils	Pertains to the Expected Activity custom search command. Logs when filling in gaps in results in preparation for use in statistical calculations. For example in stats, chart, or timechart.

governance_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
governance:rest_handler	Governance: REST Handler	SA-ThreatIntelligence	Logs when handling governance configurations and collections.

identdelete.log

Sourcetype	Component	Eai:acl.app	Description
identity_correlation:delete	Identity Correlation Delete: Search Command	SA-IdentityManagement	Logs when pruning identities marked for deletion from the assets_by_str, assets_by_cidr, or identities_expanded collections.

identity_correlation_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
identity_correlation:rest_handler	Identity Correlation: REST Handler	SA-IdentityManagement	Logs when creating, editing, validating, and deleting correlations for automatic lookups.

identity_manager.log

Sourcetype	Component	Eai:acl.app	Description
identity_correlation:modular_input	Identity Correlation: Modular Input	SA-IdentityManagement	Logs when asset and identity information is merged into Splunk asset and identity lookup tables.

Sourcetype	Component	Eai:acl.app	Description

identitymapper.log

Sourcetype	Component	Eai:acl.app	Description
identity_correlation:identitymapper	Identity Mapper: REST Handler	SA-IdentityManagement	Logs during reverse lookup searches for assets or identities.

investigation_handler.log

Sourcetype	Component	Eai:acl.app	Description
investigation_rest_handler	Investigation Workbench: REST Handler	SplunkEnterpriseSecuritySuite	Logs errors and such related to investigations, such as investigation data, entries, attachments, and cross-references to investigations from the Incident Review dashboard.

log_review_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
log_review_rest_handler	Log Review Conf: REST Handler	SA-ThreatIntelligence	Logs management information for REST changes made to log_review.conf, which is used by the Incident Review dashboard and Incident Review Settings page.

lookup_table_custom_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
lookup_table_custom_rest_handler	Lookup Table Custom: REST Handler	SA-Utils	Logs interactions with ES-managed csv lookups, including uploading new lookups through content management, as well as editing lookups in the lookup editor.

managed_lookups_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
managed_lookups_rest_handler	Managed Lookups: REST Handler	SA-Utils	Logs internal operations such as settings checks for managed lookups.

managed_nav_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
managed_nav_rest_handler	Managed Navigation: REST Handler	SA-Utils	Logs CRUD operations for the ES navigation menu, typically through the Navigation editor page.

modaction_adhoc_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
modaction:adhoc_rest_handler	Modular Action Adhoc: REST Handler	Splunk_SA_CIM	CIM: Adaptive Response actions execution. Logs when ad hoc searches result in adaptive response actions.

modaction_invocations_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
modaction:invocations_rest_handler		Splunk_SA_CIM	

Sourcetype	Component	Eai:acl.app	Description
	Modular Action Invocations: REST Handler		CIM: Adaptive Response actions execution

modaction_queue_handler.log

Sourcetype	Component	Eai:acl.app	Description
modaction:queue_handler	Modular Action Queue: REST Handler	Splunk_SA_CIM	Logs when handling the queue for Common Action Model properties.

notable_event_suppression.log

Sourcetype	Component	Eai:acl.app	Description
notable_event_suppression	Notable Event Suppression: Base	SA-ThreatIntelligence	Logs when managing notable event suppressions.

notable_event_suppression_autoDisable.log

Sourcetype	Component	Eai:acl.app	Description
notable_event_suppression:autoDisable	Notable Event Suppression: Auto Disable	SA-ThreatIntelligence	Logs on auto-disable for notable event suppressions of Adhoc Risk Events.

notable_update_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
notable_update_rest_handler	Notable Event Update: REST Handler	SA-ThreatIntelligence	Logs when changing notable events in Incident Review.

outputcheckpoint.log

Sourcetype	Component	Eai:acl.app	Description
outputcheckpoint	Output Checkpoint: Search Command	SA-Utils	Logs when outputting the results of the previous search pipeline to a modular input checkpoint directory.

per_panel_filtering.log

Sourcetype	Component	Eai:acl.app	Description
per_panel_filtering	Per Panel Filtering	SA-Utils	Logs per panel filtering changes.

relaymodaction.log

Sourcetype	Component	Eai:acl.app	Description
relaymodaction	Modular Action Relay: Modular Input	Splunk_SA_CIM	Logs when managing remote Splunk instance modular actions.

reviewstatuses_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
reviewstatuses:rest_handler	Reviewstatuses: REST Handler	SA-ThreatIntelligence	Logs when handling knowledge objects for configuring notable statuses and investigation statuses.

sequence_instance_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
sequence_instance_rest_handler	Sequence Instance: REST Handler	SplunkEnterpriseSecuritySuite	Logs when handling an instance of a running sequenced event.

sequence_templates_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
sequence_templates_rest_handler	Sequence Templates: REST Handler	SplunkEnterpriseSecuritySuite	Logs when making CRUD operations to the configuration of sequence templates.

sorttimecols.log

Sourcetype	Component	Eai:acl.app	Description
sorttimecols	Sort Time Columns: Search Command	SA-Utils	Pertains to the sorttimecols custom search command. Logs when using the sorttimecols commands to sort columns in a result set by time.

suppressions_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
notable_event_suppression:rest_handler	Notable Event Suppression: REST Handler	SA-ThreatIntelligence	REST handler for notable suppression create and edit. For use in conjunction with the notable_event_suppression.log file.

threat_intel_file_upload_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
threatintel:file_upload_rest_handler	Threat Intel Upload: REST Handler	DA-ESS-ThreatIntelligence	rest handler for uploading threat intelligence files

threat_intelligence_manager.log

Sourcetype	Component	Eai:acl.app	Description
threatintel:manager	Threat Intel Manager: Modular Input	DA-ESS-ThreatIntelligence	Logs when the modular input parses the threat sources and updates the KV Store threat collections with any new intelligence.

threat_intelligence_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
threatintel:rest_handler	Threat Intel: REST Handler	DA-ESS-ThreatIntelligence	Logs activity of threat intel endpoints.

threatlist.log

Sourcetype	Component	Eai:acl.app	Description
threatintel:download	Intelligence Download: Modular Input	SA-ThreatIntelligence	Logs the status of threat intel downloads, including success and failure.

transitioners_rest_handler.log

Sourcetype	Component	Eai:acl.app	Description
transitioners_rest_handler	Transitioners: REST Handler	SA-ThreatIntelligence	notable status handler, checking permission who can change status, also migrates from authorize.conf to reviewstatuses.conf.

uba_rest.log

Sourcetype	Component	Eai:acl.app	Description
uba:rest_handler	UBA: REST Handler	SA-UEBA	Pertains to the UBA Integration rest handler.

whois_manager.log

Sourcetype	Component	Eai:acl.app	Description
whois_manager	Whois Manager: Modular Input	SA-NetworkProtection	Logs when executing the whois modular input data.

Use search to check for activity

You can use search to check for errors and activity. The majority of sourcetypes can be searched in the _internal index. The notable_update_rest_handler can also be searched for as a source in the _audit index.

Searching the _internal index for notable_update_rest_handler will show you, for example, what happens during the handler review process. **Example search:**

```
index=_internal sourcetype="notable_update_rest_handler"
```

Example response:

i	Time	Event

>	12/2/19 3:07:16.525 PM	`2019-12-02 20:07:16,525+0000 INFO pid=8649 tid=MainThread file=rest_handler.py:handle:728 NotableEventUpdate.handle_post duration=4.474`
		host = hostname = /usr/local/bamboo/splunk-install/current/var/log/splunk/notable_update_rest_handler.log sourcetype = notable_update_rest_handler

>	12/2/19 3:07:16.524 PM	`2019-12-02 20:07:16,524+0000 INFO pid=8649 tid=MainThread file=notable_update_rest_handler.py:setStatuses:957 Done editing events matching search admin__admin__SplunkEnterpriseSecuritySuite__RMD57f02abc0263583b0`
		_1575317218.11939
		host = hostname = /usr/local/bamboo/splunk-install/current/var/log/splunk/notable_update_rest_handler.log sourcetype = notable_update_rest_handler

>	12/2/19 3:07:16.524 PM	`2019-12-02 20:07:16,524+0000 INFO pid=8649 tid=MainThread file=cim_actions.py:message:425 I sendmodaction - worker="soln-esnightly1" signature="Successfully created splunk events" action_name="notable_event_edit" digest_mode="1" action_mode="adhoc" event_count="1"`
		host = hostname source = /usr/local/bamboo/splunk-install/current/var/log/splunk/notable_update_rest_handler.log sourcetype = notable_update_rest_handler

Searching the _audit index for the source of notable_update_rest_handler will show you, for example, what was saved to the KV Store during the handler processing. This is not necessarily for troubleshooting, but more specific to incident review activity.

Example search:

```
index=_audit sourcetype="incident_review"
```

Example response:

i	Time	Event

>	12/2/19
	3:07:13.090
	PM
		`1575317233.09,19E67472-762C-4636-9A91-E4CF6B4BD885@@notable@@15c339addb8d09e6d8a24176beafd9792bd84f45,`
		`With Multiple Infections,4,esadmin,high,comment,admin,True`
		host = hostname source = notable_update_rest_handler sourcetype = incident_review

Machine Learning Toolkit

Machine Learning Toolkit Overview in Splunk Enterprise Security

The Splunk Machine Learning Toolkit (MLTK) is replacing Extreme Search (XS) as a model generation package in Enterprise Security (ES). MLTK can scale at larger volume and also can identify more abnormal events through its models. See Welcome to the Machine Learning Toolkit in the Splunk Machine Learning Toolkit *User Guide*.

In an effort to improve performance and save space as compared to XS, MLTK behaves differently. As an example, XS runs on a schedule, such as daily, over a short time window. Then XS stores its models, and many of the searches merge daily data into those models, so that the historical data grows bigger over the course of a year. MLTK also runs on a schedule, such as daily, but over a bigger time window. MLTK does not merge the daily data, but replaces it with every run. The MLTK data does not grow as large, and remains more relevant to the current timeframe.

Fit and apply commands

The main commands that are replacing the XS commands are `fit` and `apply`. The default correlation searches that use XS in ES are updated for you. If you have any custom correlation searches that are using XS commands, you need to revise them accordingly. See Convert Extreme Searches to Machine Learning Toolkit.

Creating models and finding anomalies

XS and MLTK are similar in many ways:

- Both XS and MLTK create models.
- Both XS and MLTK represent distributions in their models.
- Both XS and MLTK in ES use "low", "medium", "high" and "extreme" to represent threshold values. For details about threshold values, see Machine Learning Toolkit Macros in Splunk Enterprise Security.
- XS and MLTK both use their models to find outliers.
- Both use thresholds like "above high" to define what values to consider as outliers.

Creating models with `xscreateddcontext` versus with `fit`

XS uses both `xscreateddcontext` and `xsupdateddcontext` to build models. MLTK uses `fit` to build models.

The `xscreateddcontext` command creates a new model each time the context gen search is run. The following example shows a context gen search that uses `xsupdateddcontext`:

```
tstats summariesonly=true allow_old_summaries=true count as web_event_count from datamodel=Web.Web by Web.src, Web.http_method, _time span=24h | rename "Web.*" as * | where match(http_method, "^[A-Za-z]+$") | stats count(web_event_count) as count min(web_event_count) as min max(web_event_count) as max avg(web_event_count) as avg median(web_event_count) as median stdev(web_event_count) as size by http_method | eval min=0 | eval max=median*2 | xscreateddcontext name=count_by_http_method_by_src_1d container=web class="http_method" app="SA-NetworkProtection" scope=app type=domain terms="minimal,low,medium,high,extreme" | stats count
```

The `xsupdateddcontext` command merges the new results into the existing model each time the context gen search is run. The following example shows a context gen search that uses `xsupdateddcontext`:

```
tstats `summariesonly` count as failures from datamodel=Authentication.Authentication where authentication.action="failure" by authentication.src,_time span=1h | stats median(failures) as median, min(failures) as min, count as count | eval max = median*2 |
xsupdateddcontext app="sa-accessprotection" name=failures_by_src_count_1h container=authentication scope=app | stats count
```

The `fit` command builds a model, replacing the data each time the model gen search is run, and the `apply` command lets you use that model later. The following example shows a model gen search that uses `fit`:

```
tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where Authentication.action="failure" by
Authentication.src,_time span=1h | fit DensityFunction failure dist=norm into app:failures_by_src_count_1h
```

Finding anomalies with `xswhere` versus `apply`

XS and MLTK both use their models to find outliers. Both use thresholds like "above high" to define what values to consider as outliers. For example, if you use "above high", then `xswhere` or `apply` functions show all values that are above the highest 5% (0.05). If you change this to "above extreme", then the values are above the highest 1% (0.01).

The following example shows a search that uses `xswhere`:

```
tstats `summariesonly` count as web_event_count from datamodel=web.web by web.src, web.http_method | `drop_dm_object_name("web")` |
xswhere web_event_count from count_by_http_method_by_src_1d in web by http_method is above high
```

The following example shows a search that uses `apply`:

```
tstats `summariesonly` count as web_event_count from datamodel=Web.Web by Web.src, Web.http_method | `drop_dm_object_name("Web")` |
`mltk_apply_upper("app:count_by_http_method_by_src_1d", "extreme", "web_event_count")`
```

To verify the qualitative IDs and thresholds, use the following search: `| inputlookup qualitative_thresholds_lookup`

qualitative_id	qualitative_label	threshold
extreme	extreme	0.01
high	high	0.05
medium	medium	0.1
low	low	0.25
minimal	minimal	0.5

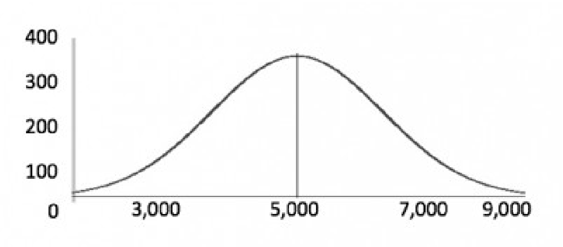
Finding outliers with DensityFunction

Anomalies and outliers are not necessarily bad, they're just different. As you gather data over time, you'll start to recognize what's standard. You might notice deviation from past behavior or you might notice deviation from peers. As you think about the deviation, then you'll start to consider upper and lower bounds from the standard. Outside of the bounds is where you'll find your anomalies and outliers.

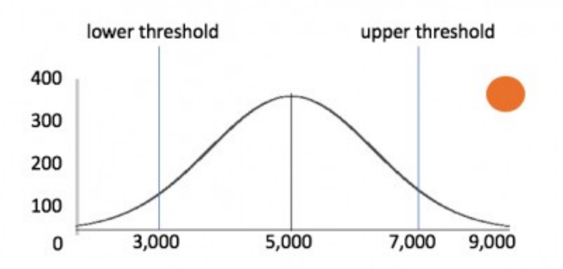
The DensityFunction's distribution is normal, exponential, or gaussian. ES searches are explicitly configured with the normal DensityFunction setting of `dist=norm` for those that use `fit`. You can modify the type of distribution for each MTLK model when using the `fit` command. Valid values for the dist parameter include: norm (normal distribution), expon (exponential distribution), gaussian_kde (Gaussian Kernel Density Estimation distribution), and auto (automatic selection). See Anomaly Detection in the Splunk Machine Learning Toolkit *User Guide*.

The threshold parameter is the center of the outlier detection process. It represents the percentage of the area under the density function and has a value between 0.000000001 (refers to ~0%) and 1 (refers to 100%). The threshold parameter guides the DensityFunction algorithm to mark outlier areas on the fitted distribution. For example, if threshold=0.01, then 1% of the fitted density function will be set as the outlier area.

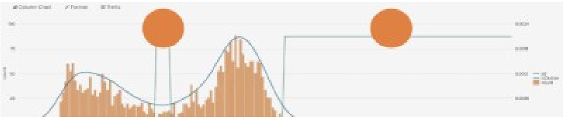
The shape of a normal distribution is that of a bell curve. Consider the scenario of network traffic volume over time. Maybe most of the traffic occurs during certain cycles. The data is naturally in a normal bell curve.



The x-axis is values. The y-axis is the number of times you see that particular value. If you see a slight increase compared to the number of times you usually see a value, it's not necessarily an outlier that you need to investigate. But if you see a large spike compared to the number of times you usually see a value, then it's probably important to investigate because it's outside the normal bounds of your upper or lower threshold.



Not all data is naturally in the shape of a bell curve, so you might need to use the "auto" dist parameter to help you find the accurate shape of your data. For example, your data might be in a Gaussian Kernel Density Estimation shape. In this case, your outliers might not be outside of upper and lower thresholds, but beyond a percentage of standard deviation.



When you're exploring your data, sometimes you already have known outliers. In some cases, you want to clean up those outliers before you train your model. For example, if you have a device on your network that is doing active or passive vulnerability scans, then you want to remove that from the results. You don't need to limit this to only known outliers. For example, if you have test servers generating data that fits in the middle of the distribution curve, this will change your curve to put more weight in the middle of the curve. This is also undesirable.

Regular search:

```
| tstats `summariesonly` count as total_count from datamodel=Network_Traffic.All_Traffic by _time span=30m
| fit DensityFunction total_count dist=norm into app:network_traffic_count_30m
```

Search with outliers removed from the source:
Notice filtering out the CIDR range of the test servers by using `.src!=10.11.36.0/24`.

```
|tstats `summariesonly` count as total_count from datamodel=Network_Traffic.All_Traffic where
All_Traffic.src !=10.11.36.0/24 by _time span=30m | fit DensityFunction total_count dist=norm into
app:network_traffic_count_30m
```

You can also filter out those results when you apply the data to your model.

Most people are used to analyzing with eventstats or streamstats, gathering data just in time for analysis. The difference with MLTK is that the probability density function uses averages and standard deviations for building a model. Then you can send your data as input into the model, and then output the outliers.

Machine Learning Toolkit Searches in Splunk Enterprise Security

Extreme Search (XS) context generating searches with names ending in "Context Gen" are revised to use Machine Learning Toolkit (MLTK) and are renamed to end with "Model Gen" instead. Other saved searches, correlation searches, key indicator searches, and rules that used XS keep their names but are also revised to use MLTK. If you have any locally modified XS searches, you need to port them over to use MLTK.

Since XS correlation searches no longer use XS, the corresponding Model Gen searches must first be run to generate a model. As mentioned in the overview, MLTK does not merge daily data into the model, but replaces it with every run. If you want to experiment with running and tuning a model without overwriting it, see Machine Learning Toolkit Troubleshooting in Splunk Enterprise Security.

Searches migrating from XS to MLTK

The list of default searches, correlation searches, key indicators, and rules that are revised from XS to MLTK follows.

DA-ESS-AccessProtection

XS: Access - Total Access Attempts

```
| tstats `summariesonly` count as current_count from datamodel=authentication.authentication where
earliest=-24h@h latest=+0s | appendcols [| tstats `summariesonly` count as historical_count from
datamodel=authentication.authentication where earliest=-48h@h latest=-24h@h] |
`get_ksi_fields(current_count,historical_count)` | xsfindbestconcept current_count from count_1d in
authentication as current_count_qual | xsfindbestconcept delta from percentile in default as delta_qual
```

MLTK: Access - Total Access Attempts

```
| tstats `summariesonly` count as current_count from datamodel=Authentication.Authentication where
earliest=-24h@h latest=+0s | appendcols [| tstats `summariesonly` count as historical_count from
datamodel=Authentication.Authentication where earliest=-48h@h latest=-24h@h] |
`get_ksi_fields(current_count,historical_count)` | `mltk_findbest("app:authentication_count_1d")` |
`get_percentage_qualitative(delta, delta_qual)`
```

DA-ESS-EndpointProtection

XS: Change - Abnormally High Number of Endpoint Changes By User - Rule

```
| `tstats` count from datamodel=endpoint.filesystem where filesystem.tag="change" by filesystem.user |
eval change_type="filesystem",user='filesystem.user' | `tstats` append=t count from
datamodel=endpoint.registry where registry.tag="change" by registry.user | eval
change_type=if(isnull(change_type),"registry",change_type),user=if(isnull(user),'registry.user',user) |
`tstats` append=t count from datamodel=change.all_changes where nodename="all_changes.endpoint_changes" by
all_changes.change_type,all_changes.user | eval
change_type=if(isnull(change_type),'all_changes.change_type',change_type),user=if(isnull(user),
'all _changes.user',user) | stats count as change_count by change_type,user | xswhere change_count from
change_count_by_user_by_change_type_1d in change_analysis by change_type is above high
```

MLTK: Change - Abnormally High Number of Endpoint Changes By User - Rule

```
| `tstats` count from datamodel=Endpoint.Filesystem where Filesystem.tag="change" by Filesystem.user |
eval change_type="filesystem",user='Filesystem.user' | `tstats` append=T count from
datamodel=Endpoint.Registry where Registry.tag="change" by Registry.user | eval
change_type=if(isnull(change_type),"registry",change_type),user=if(isnull(user),'Registry.user',user) |
`tstats` append=T count from datamodel=Change.All_Changes where nodename="All_Changes.Endpoint_Changes" by
All_Changes.change_type,All_Changes.user | eval
change_type=if(isnull(change_type),'All_Changes.change_type',change_type),user=if(isnull(user),
'All _Changes.user',user) | stats count as change_count by change_type,user |
`mltk_apply_upper("app:change_count_by_user_by_change_type_1d", "extreme", "change_count")`
```

XS: Endpoint - Host Sending Excessive Email - Rule

```
| tstats `summariesonly` sum(all_email.recipient_count) as count,dc(all_email.dest) as dest_count from
datamodel=email.all_email where not all_email.src_category="email_servers" by "all_email.src",_time
span=1h | `drop_dm_object_name("all_email")` | xswhere count from recipients_by_src_1h in email is above
medium or dest_count from destinations_by_src_1h in email is above medium
```

MLTK: Endpoint - Host Sending Excessive Email - Rule

```
| tstats `summariesonly` sum(All_Email.recipient_count) as recipient_count,dc(All_Email.dest) as
dest_count from datamodel=Email.All_Email where NOT All_Email.src_category="email_servers" by
"All_Email.src",_time span=1h | `drop_dm_object_name("All_Email")` | apply app:recipients_by_src_1h
[|`get_qualitative_upper_threshold(high)`] | apply app:destinations_by_src_1h
[|`get_qualitative_upper_threshold(high)`] | search "IsOutlier(recipient_count)"=1 OR
"IsOutlier(dest_count)"=1
```

XS: Malware - Total Infection Count

```
| tstats `summariesonly` dc(malware_attacks.signature) as infection_count from
datamodel=malware.malware_attacks where earliest=-24h@h latest=+0s malware_attacks.action=allowed by
malware_attacks.dest | stats sum(infection_count) as current_count | appendcols [| tstats `summariesonly`
dc(malware_attacks.signature) as infection_count from datamodel=malware.malware_attacks where
earliest=-48h@h latest=-24h@h malware_attacks.action=allowed by malware_attacks.dest | stats
sum(infection_count) as historical_count] | `get_ksi_fields(current_count,historical_count)` |
xsfindbestconcept current_count from count_1d in malware as current_count_qual | xsfindbestconcept delta
from percentile in default as delta_qual
```

MLTK: Malware - Total Infection Count

```
| tstats `summariesonly` dc(Malware_Attacks.signature) as infection_count from
datamodel=Malware.Malware_Attacks where earliest=-24h@h latest=+0s Malware_Attacks.action=allowed by
Malware_Attacks.dest | stats sum(infection_count) as current_count | appendcols [| tstats `summariesonly`
dc(Malware_Attacks.signature) as infection_count from datamodel=Malware.Malware_Attacks where
earliest=-48h@h latest=-24h@h Malware_Attacks.action=allowed by Malware_Attacks.dest | stats
sum(infection_count) as historical_count] | `get_ksi_fields(current_count,historical_count)` |
`mltk_findbest("app:malware_infection_count_by_1d")` | `get_percentage_qualitative(delta, delta_qual)`
```

DA-ESS-IdentityManagement

XS: Identity - High Volume Email Activity with Non-corporate Domains - Rule

```
| tstats `summariesonly` sum(all_email.size) as bytes, values(all_email.recipient) as recipient from
datamodel=email.all_email where not `cim_corporate_email_domain_search("all_email.recipient")` by
all_email.src_user | `drop_dm_object_name("all_email")` | xsfindbestconcept bytes from
email_volume_1h_noncorp | eval
risk_score=case(bestconcept="extreme",80,bestconcept="high",50,bestconcept="medium",20, 1==1, 0) | search
risk_score>0
```

MLTK: Identity - High Volume Email Activity with Non-corporate Domains - Rule

```
| tstats `summariesonly` sum(All_Email.size) as bytes, values(All_Email.recipient) as recipient from
datamodel=Email.All_Email where NOT `cim_corporate_email_domain_search("All_Email.recipient")` by
All_Email.src_user, All_Email.src_user_bunit | `drop_dm_object_name("All_Email")` |
`mltk_apply_upper("app:email_activity_to_non_corporate_by_user_1h", "medium", "bytes")`
```

XS: Identity - Web Uploads to Non-corporate Domains - Rule

```
| tstats `summariesonly` sum(web.bytes) as bytes from datamodel=web.web where (web.http_method="post" or
web.http_method="put") not (`cim_corporate_web_domain_search("web.url")`) by web.user |
`drop_dm_object_name("web")` | xsfindbestconcept bytes from web_volume_1h_noncorp | eval
risk_score=case(bestconcept="extreme",80,bestconcept="high",50,bestconcept="medium",20, 1==1, 0) | search
risk_score>0
```

MLTK: Identity - Web Uploads to Non-corporate Domains - Rule

```
| tstats `summariesonly` sum(Web.bytes) as bytes from datamodel=Web.Web where (Web.http_method="POST" OR
Web.http_method="PUT") NOT (`cim_corporate_web_domain_search("Web.url")`) by Web.user, Web.user_bunit |
`drop_dm_object_name("Web")` | `mltk_apply_upper("app:web_upload_to_non_corporate_by_user_1h", "medium",
"bytes")`
```

DA-ESS-NetworkProtection

XS: Network - Unusual Volume of Network Activity - Rule

```
| tstats `summariesonly` dc(all_traffic.src) as src_count,count from datamodel=network_traffic.all_traffic
| localop | xswhere count from count_30m in network_traffic is extreme or src_count from src_count_30m in
network_traffic is extreme | eval const_dedup_id="network - unusual volume of network activity - rule"
```

MLTK: Network - Unusual Volume of Network Activity - Rule

```
| tstats `summariesonly` dc(All_Traffic.src) as src_count,count as total_count from
datamodel=Network_Traffic.All_Traffic | localop | apply network_traffic_src_count_30m
[|`get_qualitative_upper_threshold(extreme)`] | apply network_traffic_count_30m
[|`get_qualitative_upper_threshold(extreme)`] | search "IsOutlier(src_count)"=1 OR
"IsOutlier(total_count)"=1
```

XS: Web - Abnormally High Number of HTTP Method Events By Src - Rule

```
| tstats `summariesonly` count as web_event_count from datamodel=web.web by web.src, web.http_method |
`drop_dm_object_name("web")` | xswhere web_event_count from count_by_http_method_by_src_1d in web by
http_method is above high
```

MLTK: Web - Abnormally High Number of HTTP Method Events By Src - Rule

```
| tstats `summariesonly` count as web_event_count from datamodel=Web.Web by Web.src, Web.http_method |
`drop_dm_object_name("Web")` | `mltk_apply_upper("app:count_by_http_method_by_src_1d", "extreme",
"web_event_count")`
```

SA-AccessProtection

XS: Access - Authentication Failures By Source - Context Gen

```
| tstats `summariesonly` count as failures from datamodel=authentication.authentication where
authentication.action="failure" by authentication.src,_time span=1h | stats median(failures) as median,
min(failures) as min, count as count | eval max = median*2 | xsupdateddcontext app="sa-accessprotection"
name=failures_by_src_count_1h container=authentication scope=app | stats count
```

MLTK: Access - Authentication Failures By Source - Model Gen

```
| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where
Authentication.action="failure" by Authentication.src,_time span=1h | fit DensityFunction failure
```

```
dist=norm into app:failures_by_src_count_1h
```

XS: Access - Authentication Failures By Source Per Day - Context Gen

```
| tstats `summariesonly` count as failures from datamodel=authentication.authentication where
authentication.action="failure" by authentication.src,_time span=1d | stats median(failures) as median,
min(failures) as min, count as count | eval max = median*2 | xscreateddcontext app="sa-accessprotection"
name=failures_by_src_count_1d container=authentication scope=app type=domain
terms=`xs_default_magnitude_concepts` | stats count
```

MLTK: Access - Authentication Failures By Source Per Day - Model Gen

```
| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where
Authentication.action="failure" by Authentication.src,_time span=1d | fit DensityFunction failure
dist=norm into app:failures_by_src_count_1d
```

XS: Access - Authentication Volume Per Day - Context Gen

```
| tstats `summariesonly` count as count_1d from datamodel=authentication.authentication by _time span=1d |
stats count, median(count_1d) as median, stdev(count_1d) as size | search size>0 | xscreateddcontext
name=count_1d container=authentication type=median_centered scope=app app=sa-accessprotection
terms=`xs_default_magnitude_concepts` | stats count
```

MLTK: Access - Authentication Volume Per Day - Model Gen

```
| tstats `summariesonly` count as current_count from datamodel=Authentication.Authentication by _time
span=1d | fit DensityFunction current_count dist=norm into app:authentication_count_1d
```

XS: Access - Brute Force Access Behavior Detected - Rule

```
| from datamodel:"authentication"."authentication" | stats values(tag) as tag,values(app) as
app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src |
search success>0 | xswhere failure from failures_by_src_count_1h in authentication is above medium
```

MLTK: Access - Brute Force Access Behavior Detected - Rule

```
| from datamodel:"Authentication"."Authentication" | stats values(tag) as tag,values(app) as
app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src |
search success>0 | `mltk_apply_upper("app:failures_by_src_count_1h", "high", "failure")`
```

XS: Access - Brute Force Access Behavior Detected Over 1d - Rule

```
| tstats `summariesonly` values(authentication.app) as app,count from
datamodel=authentication.authentication by authentication.action,authentication.src |
`drop_dm_object_name("authentication")` | eval
success=if(action="success",count,0),failure=if(action="failure",count,0) | stats values(app) as
app,sum(failure) as failure,sum(success) as success by src | where success > 0 | xswhere failure from
failures_by_src_count_1d in authentication is above medium
```

MLTK: Access - Brute Force Access Behavior Detected Over 1d - Rule

```
| tstats `summariesonly` values(Authentication.app) as app,count from
datamodel=Authentication.Authentication by Authentication.action,Authentication.src |
`drop_dm_object_name("Authentication")` | eval
success=if(action="success",count,0),failure=if(action="failure",count,0) | stats values(app) as
app,sum(failure) as failure,sum(success) as success by src | where success > 0 |
`mltk_apply_upper("app:failures_by_src_count_1d", "medium", "failure")`
```

SA-EndpointProtection

XS: Change - Total Change Count By User By Change Type Per Day - Context Gen

```
| `tstats` count from datamodel=endpoint.filesystem where filesystem.tag="change" by _time,filesystem.user
span=24h | eval change_type="filesystem",user='filesystem.user' | `tstats` append=t count from
datamodel=endpoint.registry where registry.tag="change" by _time,registry.user span=24h | eval
change_type=if(isnull(change_type),"registry",change_type),user=if(isnull(user),'registry.user',user) |
`tstats` append=t count from datamodel=change.all_changes by
_time,all_changes.change_type,all_changes.user span=24h | eval
change_type=if(isnull(change_type),'all_changes.change_type',change_type),user=if(isnull(user),'all
_changes.user',user) | stats count as change_count by _time,change_type,user |
`context_stats(change_count, change_type)` | eval min=0 | eval max=median*2 | xsupdateddcontext
name=change_count_by_user_by_change_type_1d container=change_analysis class=change_type type=domain
app="sa-endpointprotection" scope=app terms=`xs_default_magnitude_concepts` | stats count
```

MLTK: Change - Total Change Count By User By Change Type Per Day - Model Gen

```
| `tstats` count from datamodel=Endpoint.Filesystem where Filesystem.tag="change" by _time,Filesystem.user
span=24h | eval change_type="filesystem",user='Filesystem.user' | `tstats` append=T count from
datamodel=Endpoint.Registry where Registry.tag="change" by _time,Registry.user span=24h | eval
change_type=if(isnull(change_type),"registry",change_type),user=if(isnull(user),'Registry.user',user) |
`tstats` append=T count from datamodel=Change.All_Changes by
_time,All_Changes.change_type,All_Changes.user span=24h | eval
change_type=if(isnull(change_type),'All_Changes.change_type',change_type),user=if(isnull(user),'All
_Changes.user',user) | stats count as change_count by _time,change_type,user | fit DensityFunction
change_count by change_type dist=norm into app:change_count_by_user_by_change_type_1d
```

XS: Endpoint - Emails By Destination Count - Context Gen

```
| tstats summariesonly=false dc(all_email.dest) as dest_count from datamodel=email.all_email where not
all_email.src_category="email_servers" by "all_email.src",_time span=1h | stats avg(dest_count) as avg,
count | eval min=0 | eval max=avg * 2 | xsupdateddcontext app=sa-endpointprotection
name=destinations_by_src_1h container=email type=domain scope=app | stats count
```

MLTK: Endpoint - Emails By Destination Count - Model Gen

```
| tstats summariesonly=false dc(All_Email.dest) as dest_count from datamodel=Email.All_Email where NOT
All_Email.src_category="email_servers" by "All_Email.src",_time span=1h | fit DensityFunction dest_count
dist=norm into app:destinations_by_src_1h
```

XS: Endpoint - Emails By Source - Context Gen

```
| tstats summariesonly=false sum(all_email.recipient_count) as recipient_count from
datamodel=email.all_email where not all_email.src_category="email_servers" by "all_email.src",_time
span=1h | stats avg(recipient_count) as avg, count | eval min=0 | eval max=avg * 2 | xsupdateddcontext
app=sa-endpointprotection name=recipients_by_src_1h container=email type=domain scope=app | stats count
```

MLTK: Endpoint - Emails By Source - Model Gen

```
| tstats summariesonly=false sum(All_Email.recipient_count) as recipient_count from
datamodel=Email.All_Email where NOT All_Email.src_category="email_servers" by "All_Email.src",_time
span=1h | fit DensityFunction recipient_count dist=norm into app:recipients_by_src_1h
```

XS: Endpoint - Malware Daily Count - Context Gen

```
| tstats `summariesonly` dc(malware_attacks.signature) as infection_count from
datamodel=malware.malware_attacks where earliest=-31d@d latest=-1d@d malware_attacks.action=allowed by
malware_attacks.dest,_time span=1d | stats sum(infection_count) as total_infection_count by _time | stats
count,median(total_infection_count) as median by _time | eval min=0 | eval max=median*2 |
xscreateddcontext name=count_1d container=malware type=domain terms="minimal,small,medium,large,extreme"
```

```
scope=app app=sa-networkprotection | stats count
```

MLTK: Endpoint - Malware Daily Count - Model Gen

```
| tstats `summariesonly` dc(Malware_Attacks.signature) as infection_count from
datamodel=Malware.Malware_Attacks where earliest=-31d@d latest=-1d@d Malware_Attacks.action=allowed by
Malware_Attacks.dest,_time span=1d | stats sum(infection_count) as current_count by _time | fit
DensityFunction current_count dist=norm into app:malware_infection_count_by_1d
```

SA-IdentityManagement

XS: Identity - Email Activity to Non-corporate Domains by Users Per 1d - Context Gen

```
| tstats `summariesonly` sum(all_email.size) as bytes, values(all_email.recipient) as recipient from
datamodel=email.all_email where not `cim_corporate_email_domain_search("all_email.recipient")` by _time,
all_email.src_user, all_email.src_user_bunit span=1h | `drop_dm_object_name("all_email")` | stats
avg(bytes) as avg, stdev(bytes) as stdev, count by src_user_bunit | eval min=0 | eval max=avg + 3*stdev |
xsupdateddcontext name="email_volume_1h_noncorp" class=src_user_bunit scope=app
terms=`xs_default_magnitude_concepts` uom="email_volume_bytes" type=domain app=sa-identitymanagement |
stats count
```

MLTK: Identity - Email Activity to Non-corporate Domains by Users Per 1d - Model Gen

```
| tstats `summariesonly` sum(All_Email.size) as bytes, values(All_Email.recipient) as recipient from
datamodel=Email.All_Email where NOT `cim_corporate_email_domain_search("All_Email.recipient")` by _time,
All_Email.src_user, All_Email.src_user_bunit span=1h | `drop_dm_object_name("All_Email")` | fit
DensityFunction bytes by src_user_bunit dist=norm into app:email_activity_to_non_corporate_by_user_1h
```

XS: Identity - Web Uploads to Non-corporate Domains by Users Per 1d - Context Gen

```
| tstats `summariesonly` sum(web.bytes) as bytes from datamodel=web.web where
not(`cim_corporate_web_domain_search("web.url")`) (web.http_method="post" or web.http_method="put") by
_time, web.user, web.user_bunit span=1h | `drop_dm_object_name("web")`| stats avg(bytes) as avg,
stdev(bytes) as stdev, count by user_bunit | eval min=0 | eval max=avg + 3*stdev | xsupdateddcontext
name="web_volume_1h_noncorp" class=user_bunit scope=app terms=`xs_default_magnitude_concepts`
uom="web_volume_bytes" type=domain app=sa-identitymanagement | stats count
```

MLTK: Identity - Web Uploads to Non-corporate Domains by Users Per 1d - Model Gen

```
| tstats `summariesonly` sum(Web.bytes) as bytes from datamodel=Web.Web where
NOT(`cim_corporate_web_domain_search("Web.url")`) (Web.http_method="POST" OR Web.http_method="PUT") by
_time, Web.user, Web.user_bunit span=1h | `drop_dm_object_name("Web")` | fit DensityFunction bytes by
user_bunit dist=norm into app:web_upload_to_non_corporate_by_user_1h
```

SA-NetworkProtection

XS: Network - Event Count By Signature Per Hour - Context Gen

```
| tstats `summariesonly` count as count_by_signature_1h from datamodel=intrusion_detection.ids_attacks by
_time,ids_attacks.signature span=1h | `drop_dm_object_name("ids_attacks")` |
`context_stats(count_by_signature_1h, signature)` | search size>0 | xscreateddcontext
name=count_by_signature_1h class=signature container=ids_attacks type=median_centered
terms="minimal,low,medium,high,extreme" scope=app app=sa-networkprotection | stats count
```

MLTK: Network - Event Count By Signature Per Hour - Model Gen

```
| tstats `summariesonly` count as ids_attacks from datamodel=Intrusion_Detection.IDS_Attacks by
_time,IDS_Attacks.signature span=1h | `drop_dm_object_name("IDS_Attacks")` | fit DensityFunction
ids_attacks by signature dist=norm into app:count_by_signature_1h
```

XS: Network - Port Activity By Destination Port - Context Gen

```
| tstats `summariesonly` count as dest_port_traffic_count from datamodel=Network_Traffic.All_Traffic by
All_Traffic.dest_port,_time span=1d | `drop_dm_object_name("All_Traffic")` |
`context_stats(dest_port_traffic_count, dest_port)` | search size>0 | xscreateddcontext
name=count_by_dest_port_1d class=dest_port container=network_traffic type=median_centered
terms="minimal,low,medium,high,extreme" width=3 scope=app app=SA-NetworkProtection | stats count
```

MLTK: Network - Port Activity By Destination Port - Model Gen

```
| tstats `summariesonly` count as dest_port_traffic_count from datamodel=Network_Traffic.All_Traffic by
All_Traffic.dest_port,_time span=1d | `drop_dm_object_name("All_Traffic")` | fit DensityFunction
dest_port_traffic_count by dest_port dist=norm into app:count_by_dest_port_1d
```

XS: Network - Substantial Increase In Intrusion Events - Rule

```
| tstats `summariesonly` count,values(ids_attacks.tag) as tag from
datamodel=intrusion_detection.ids_attacks by ids_attacks.signature | `drop_dm_object_name("ids_attacks")`
| xswhere count from count_by_signature_1h in ids_attacks by signature is above medium
```

MLTK: Network - Substantial Increase In Intrusion Events - Rule

```
| tstats `summariesonly` count as ids_attacks,values(IDS_Attacks.tag) as tag from
datamodel=Intrusion_Detection.IDS_Attacks by IDS_Attacks.signature | `drop_dm_object_name("IDS_Attacks")`
| `mltk_apply_upper("app:count_by_signature_1h", "high", "ids_attacks")`
```

XS: Network - Substantial Increase in Port Activity - Rule

```
| tstats `summariesonly` count,values(all_traffic.tag) as tag from datamodel=network_traffic.all_traffic
by all_traffic.dest_port | `drop_dm_object_name("all_traffic")` | xswhere count from count_by_dest_port_1d
in network_traffic by dest_port is extreme
```

MLTK: Network - Substantial Increase in Port Activity - Rule

```
| tstats `summariesonly` count as dest_port_traffic_count,values(All_Traffic.tag) as tag from
datamodel=Network_Traffic.All_Traffic by All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")` |
`mltk_apply_upper("app:count_by_dest_port_1d", "extreme", "dest_port_traffic_count")`
```

XS: Network - Traffic Source Count Per 30m - Context Gen

```
| tstats `summariesonly` dc(all_traffic.src) as src_count from datamodel=network_traffic.all_traffic by
_time span=30m | stats count, median(src_count) as median, stdev(src_count) as size | search size>0 |
xsupdateddcontext name=src_count_30m container=network_traffic terms="minimal,low,medium,high,extreme"
type=median_centered width=3 app=sa-networkprotection scope=app | stats count
```

MLTK: Network - Traffic Source Count Per 30m - Model Gen

```
| tstats `summariesonly` dc(All_Traffic.src) as src_count from datamodel=Network_Traffic.All_Traffic by
_time span=30m | fit DensityFunction src_count dist=norm into app:network_traffic_src_count_30m
```

XS: Network - Traffic Volume Per 30m - Context Gen

```
| tstats `summariesonly` count as total_count from datamodel=network_traffic.all_traffic by _time span=30m
| stats count, median(total_count) as median, stdev(total_count) as size | search size>0 |
xsupdateddcontext name=count_30m container=network_traffic terms="minimal,low,medium,high,extreme"
type=median_centered width=3 app=sa-networkprotection scope=app | stats count
```

MLTK: Network - Traffic Volume Per 30m - Model Gen

```
| tstats `summariesonly` count as total_count from datamodel=Network_Traffic.All_Traffic by _time span=30m
| fit DensityFunction total_count dist=norm into app:network_traffic_count_30m
```

XS: Web - Web Event Count By Src By HTTP Method Per 1d - Context Gen

```
| tstats `summariesonly` count as web_event_count from datamodel=web.web by web.src, web.http_method,
_time span=24h | `drop_dm_object_name("web")` | where match(http_method, "^[a-za-z]+$") |
`context_stats(web_event_count, http_method)` | eval min=0 | eval max=median*2 | xscreateddcontext
name=count_by_http_method_by_src_1d container=web class=http_method app="sa-networkprotection" scope=app
type=domain terms=`xs_default_magnitude_concepts` | stats count
```

MLTK: Web - Web Event Count By Src By HTTP Method Per 1d - Model Gen

```
| tstats `summariesonly` count as web_event_count from datamodel=Web.Web by Web.src, Web.http_method,
_time span=24h | `drop_dm_object_name("Web")` | where match(http_method, "^[A-Za-z]+$") | fit
DensityFunction web_event_count by http_method dist=norm into app:count_by_http_method_by_src_1d
```

SA-ThreatIntelligence

XS: Risk - Aggregated Other Risk

```
| tstats `summariesonly` sum(all_risk.risk_score) as current_count from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="other" by all_risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(all_risk.risk_score) as historical_count from datamodel=risk.all_risk where
earliest=-48h@h latest=-24h@h all_risk.risk_object_type="other" by all_risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept
current_count from total_risk_by_object_type_1d in risk by risk_object_type as current_count_qual |
xsfindbestconcept delta from percentile in default as delta_qual
```

MLTK: Risk - Aggregated Other Risk

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="other" by All_Risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(All_Risk.risk_score) as historical_count from datamodel=Risk.All_Risk where
earliest=-48h@h latest=-24h@h All_Risk.risk_object_type="other" by All_Risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:total_risk_by_object_type_1d")` | `get_percentage_qualitative(delta, delta_qual)`
```

XS: Risk - Aggregated Risk

```
| tstats `summariesonly` sum(all_risk.risk_score) as current_count from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s | appendcols [| tstats `summariesonly` sum(all_risk.risk_score) as
historical_count from datamodel=risk.all_risk where earliest=-48h@h latest=-24h@h] |
`get_ksi_fields(current_count, historical_count)` | xsfindbestconcept current_count from
total_risk_by_object_type_1d in risk as current_count_qual | xsfindbestconcept delta from percentile in
default as delta_qual
```

MLTK: Risk - Aggregated Risk

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s | appendcols [| tstats `summariesonly` sum(All_Risk.risk_score) as
historical_count from datamodel=Risk.All_Risk where earliest=-48h@h latest=-24h@h] |
`get_ksi_fields(current_count, historical_count)` | `mltk_findbest("app:total_risk_1d")` |
`get_percentage_qualitative(delta, delta_qual)`
```

XS: Risk - Aggregated System Risk

```
| tstats `summariesonly` sum(all_risk.risk_score) as current_count from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="system" by all_risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(all_risk.risk_score) as historical_count from datamodel=risk.all_risk where
earliest=-48h@h latest=-24h@h all_risk.risk_object_type="system" by all_risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept
current_count from total_risk_by_object_type_1d in risk by risk_object_type as current_count_qual |
xsfindbestconcept delta from percentile in default as delta_qual
```

MLTK: Risk - Aggregated System Risk

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="system" by All_Risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(All_Risk.risk_score) as historical_count from datamodel=Risk.All_Risk where
earliest=-48h@h latest=-24h@h All_Risk.risk_object_type="system" by All_Risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:total_risk_by_object_type_1d")` | `get_percentage_qualitative(delta, delta_qual)`
```

XS: Risk - Aggregated User Risk

```
| tstats `summariesonly` sum(all_risk.risk_score) as current_count from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="user" by all_risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(all_risk.risk_score) as historical_count from datamodel=risk.all_risk where
earliest=-48h@h latest=-24h@h all_risk.risk_object_type="user" by all_risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept
current_count from total_risk_by_object_type_1d in risk by risk_object_type as current_count_qual |
xsfindbestconcept delta from percentile in default as delta_qual
```

MLTK: Risk - Aggregated User Risk

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="user" by All_Risk.risk_object_type | appendcols [|
tstats `summariesonly` sum(All_Risk.risk_score) as historical_count from datamodel=Risk.All_Risk where
earliest=-48h@h latest=-24h@h All_Risk.risk_object_type="user" by All_Risk.risk_object_type] |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:total_risk_by_object_type_1d")` | `get_percentage_qualitative(delta, delta_qual)`
```

XS: Risk - Median Object Risk Per Day - Context Gen

```
| tstats `summariesonly` sum(all_risk.risk_score) as object_risk from datamodel=risk.all_risk by
_time,all_risk.risk_object,all_risk.risk_object_type span=1d | `drop_dm_object_name("all_risk")` |
`context_stats(object_risk, risk_object_type)` | eval min=0 | eval max=median*2 | xsupdateddcontext
app=sa-threatintelligence name=median_object_risk_by_object_type_1d container=risk class=risk_object_type
type=domain scope=app | stats count
```

MLTK: Risk - Median Object Risk Per Day - Model Gen

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk by
_time,All_Risk.risk_object,All_Risk.risk_object_type span=1d | `drop_dm_object_name("All_Risk")` | fit
DensityFunction current_count dist=norm into app:median_object_risk_1d
```

XS: Risk - Median Object Risk Per Day by Object Type - Context Gen

N/A. The original Risk - Median Object Risk Per Day - Context Gen became two: Risk - Median Object Risk Per Day - Model Gen and Risk - Median Object Risk Per Day by Object Type - Model Gen.

MLTK: Risk - Median Object Risk Per Day by Object Type - Model Gen

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk by
_time,All_Risk.risk_object,All_Risk.risk_object_type span=1d | `drop_dm_object_name("All_Risk")` | fit
DensityFunction current_count by risk_object_type dist=norm into app:median_object_risk_by_object_type_1d
```

XS: Risk - Median Risk Score

```
| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s by all_risk.risk_object | stats median(accum_risk) as current_count |
appendcols [| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk
where earliest=-48h@h latest=-24h@h by all_risk.risk_object | stats median(accum_risk) as
historical_count] | `get_ksi_fields(current_count, historical_count)` | xsfindbestconcept current_count
from median_object_risk_by_object_type_1d in risk as current_count_qual | xsfindbestconcept delta from
percentile in default as delta_qual
```

MLTK: Risk - Median Risk Score

```
| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s by All_Risk.risk_object | stats median(accum_risk) as current_count |
appendcols [| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk
where earliest=-48h@h latest=-24h@h by All_Risk.risk_object | stats median(accum_risk) as
historical_count] | `get_ksi_fields(current_count, historical_count)` |
`mltk_findbest("app:median_object_risk_1d")` | `get_percentage_qualitative(delta, delta_qual)`
```

XS: Risk - Median Risk Score By Other

```
| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="other" by all_risk.risk_object,
all_risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where earliest=-48h@h
latest=-24h@h all_risk.risk_object_type="other" by all_risk.risk_object, all_risk.risk_object_type | stats
median(accum_risk) as historical_count] | eval risk_object_type="other" | `get_ksi_fields(current_count,
historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept current_count from
median_object_risk_by_object_type_1d in risk by risk_object_type as current_count_qual | xsfindbestconcept
delta from percentile in default as delta_qual
```

MLTK: Risk - Median Risk Score By Other

```
| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="other" by All_Risk.risk_object,
All_Risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-48h@h
latest=-24h@h All_Risk.risk_object_type="other" by All_Risk.risk_object, All_Risk.risk_object_type | stats
median(accum_risk) as historical_count] | eval risk_object_type="other" | `get_ksi_fields(current_count,
historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:median_object_risk_by_object_type_1d")` | `get_percentage_qualitative(delta,
delta_qual)`
```

XS: Risk - Median Risk Score By System

```
| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="system" by all_risk.risk_object,
all_risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where earliest=-48h@h
latest=-24h@h all_risk.risk_object_type="system" by all_risk.risk_object, all_risk.risk_object_type |
stats median(accum_risk) as historical_count] | eval risk_object_type="system" |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept
current_count from median_object_risk_by_object_type_1d in risk by risk_object_type as current_count_qual
| xsfindbestconcept delta from percentile in default as delta_qual
```

MLTK: Risk - Median Risk Score By System

```
| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="system" by All_Risk.risk_object,
All_Risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-48h@h
latest=-24h@h All_Risk.risk_object_type="system" by All_Risk.risk_object, All_Risk.risk_object_type |
stats median(accum_risk) as historical_count] | eval risk_object_type="system" |
`get_ksi_fields(current_count, historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:median_object_risk_by_object_type_1d")` | `get_percentage_qualitative(delta,
delta_qual)`
```

XS: Risk - Median Risk Score By User

```
| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where
earliest=-24h@h latest=+0s all_risk.risk_object_type="user" by all_risk.risk_object,
all_risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk where earliest=-48h@h
latest=-24h@h all_risk.risk_object_type="user" by all_risk.risk_object, all_risk.risk_object_type | stats
median(accum_risk) as historical_count] | eval risk_object_type="user" | `get_ksi_fields(current_count,
historical_count)` | `drop_dm_object_name("all_risk")` | xsfindbestconcept current_count from
median_object_risk_by_object_type_1d in risk by risk_object_type as current_count_qual | xsfindbestconcept
delta from percentile in default as delta_qual
```

MLTK: Risk - Median Risk Score By User

```
| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where
earliest=-24h@h latest=+0s All_Risk.risk_object_type="user" by All_Risk.risk_object,
All_Risk.risk_object_type | stats median(accum_risk) as current_count | appendcols [| tstats
`summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-48h@h
latest=-24h@h All_Risk.risk_object_type="user" by All_Risk.risk_object, All_Risk.risk_object_type | stats
median(accum_risk) as historical_count] | eval risk_object_type="user" | `get_ksi_fields(current_count,
historical_count)` | `drop_dm_object_name("All_Risk")` |
`mltk_findbest("app:median_object_risk_by_object_type_1d")` | `get_percentage_qualitative(delta,
delta_qual)`
```

XS: Risk - Total Risk By Risk Object Type Per Day - Context Gen

```
| tstats `summariesonly` sum(all_risk.risk_score) as accum_risk from datamodel=risk.all_risk by
_time,all_risk.risk_object_type span=1d | `drop_dm_object_name("all_risk")` | `context_stats(accum_risk,
risk_object_type)` | eval min=0 | eval max=median*2 | xsupdateddcontext app=sa-threatintelligence
name=total_risk_by_object_type_1d container=risk class=risk_object_type type=domain scope=app | stats
count
```

MLTK: Risk - Total Risk By Risk Object Type Per Day - Model Gen

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk by
_time,All_Risk.risk_object_type span=1d | `drop_dm_object_name("All_Risk")` | fit DensityFunction
current_count by risk_object_type dist=norm into app:total_risk_by_object_type_1d
```

XS: Risk - Total Risk Per Day - Context Gen

N/A. The original Risk - Total Risk By Risk Object Type Per Day - Context Gen became two: Risk - Total Risk By Risk Object Type Per Day - Model Gen and Risk - Total Risk Per Day - Model Gen.

MLTK: Risk - Total Risk Per Day - Model Gen

```
| tstats `summariesonly` sum(All_Risk.risk_score) as current_count from datamodel=Risk.All_Risk by _time
span=1d | `drop_dm_object_name("All_Risk")` | fit DensityFunction current_count dist=norm into
app:total_risk_1d
```

SA-Utils

XS: ESS - Percentile - Context Gen

```
| xscreateudcontext scope=app container=default name=percentile
terms="extreme,high,medium,low,minimal,low,medium,high,extreme" type=domain uom="percentage" min=-100
max=100 count=1 | stats count
```

Audit searches using an MLTK Model

There is a savedsearch to help audit your model generating searches and the corresponding rules that apply them.

For example, the following savedsearch finds the search called "Network - Traffic Source Count Per 30m - Model Gen" that builds the model for `network_traffic_src_count_30m` with `fit densityfunction`. Then it also finds the rule called "Network - Unusual Volume of Network Activity - Rule" that applies data to the model and finds the outliers using `apply` and the `` `get_qualitative_upper_threshold(extreme)` `` macro.

Example search:

```
| savedsearch "Audit - Searches using an MLTK Model" model_name=network_traffic_src_count_30m
```

Example results:

eai:acl.app	title	search
SA-NetworkProtection	Network - Traffic Source Count Per 30m - Model Gen	tstats `summariesonly` dc(all_traffic.src) as src_count from datamodel=network_traffic.all_traffic by _time span=30m | fit densityfunction src_count dist=norm into app:network_traffic_src_count_30m
DA-ESS-NetworkProtection	Network - Unusual Volume of Network Activity - Rule	tstats `summariesonly` dc(all_traffic.src) as src_count,count as total_count from datamodel=network_traffic.all_traffic | localop | apply network_traffic_src_count_30m [|`get_qualitative_upper_threshold(extreme)`] | apply network_traffic_count_30m [|`get_qualitative_upper_threshold(extreme)`] | search "isoutlier(src_count)"=1 or "isoutlier(total_count)"=1

Machine Learning Toolkit Macros in Splunk Enterprise Security

Machine Learning Toolkit macros act as shortcuts and wrappers. The macros are found from the Splunk Enterprise menu at **Settings > Advanced Search > Search macros**.

An example of using a macro to apply data to model=app:failures_by_src_count_1d for qualitative_id=medium, and field=failure:

```
... | `mltk_apply_upper("app:failures_by_src_count_1d", "medium", "failure")`
```

Versus doing it without the macro:

```
... | apply app:failures_by_src_count_1d [| inputlookup append=T qualitative_thresholds_lookup where
qualitative_id="medium" | rename threshold as upper_threshold | return upper_threshold | eval
search=replace(search,"\"","")] | search "IsOutlier(failure)"=1
```

Macros used in SPL

You might use the following macros to apply data to your models.

[mltk_apply]

This is approximately equivalent to the xsWhere command, for applying to either upper or lower bounds.

```
[mltk_apply(3)]
args       = model,qualitative_id,field
definition = apply $model$ [| `get_qualitative_threshold($qualitative_id$)`] | search
"IsOutlier($field$)"=1
```

The macro takes the following arguments:

model
: The name of the model for applying data and comparing against standards to find outliers, such as `app:failures_by_src_count_1d`.

qualitative_id

The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

field

The name of the field that you're searching or counting to find outliers, such as `failure`.

[mltk_apply_lower]

This is approximately equivalent to the xsWhere command, for applying to lower bounds.

```
[mltk_apply_lower(3)]
args       = model,qualitative_id,field
definition = apply $model$ [| `get_qualitative_lower_threshold($qualitative_id$)`] | search
"IsOutlier($field$)"=1
```

The macro takes the following arguments:

model

The name of the model for applying data and comparing against standards to find outliers, such as `app:failures_by_src_count_1d`.

qualitative_id

The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

field

The name of the field that you're searching or counting to find outliers, such as `failure`.

[mltk_apply_upper]

This is approximately equivalent to the xsWhere command, for applying to upper bounds.

```
[mltk_apply_upper(3)]
args       = model,qualitative_id,field
definition = apply $model$ [| `get_qualitative_upper_threshold($qualitative_id$)`] | search
"IsOutlier($field$)"=1
```

The macro takes the following arguments:

model

The name of the model for applying data and comparing against standards to find outliers, such as `app:failures_by_src_count_1d`.

qualitative_id

The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

field

The name of the field that you're searching or counting to find outliers, such as `failure`.

[mltk_findbest]

This is approximately equivalent to the xsFindBestConcept command. For each value, this macro tells you in which threshold range the value falls on the distribution curve.

```
[mltk_findbest(1)]
args       = model
```

```
definition = apply $model$ as findbest [| `get_findbest_thresholds`] | eval [| `get_findbest_qualitative`]
| fields - BoundaryRanges,findbest*
```

The macro takes the following arguments:

model
: The name of the model for applying data and comparing against standards to find outliers, such as `app:failures_by_src_count_1d`.

Note that the threshold doesn't take a field parameter like the other macros. It performs the `findbest` operation on the exact field that the Model Gen `fit` command was performed on. For example:

- If the Model Gen performed: `... | fit DensityFunction current_count dist=norm into app:total_risk_1d`, the `mltk_findbest()` search will only match on the `current_count` field.
- This means that the portion of the search that comes before the `mltk_findbest()` command must contain the `current_count` field.

Macros used by other macros

These macros are in use by the macros used in SPL.

[get_qualitative_threshold]

This is a building block for [mltk_apply]. You might not use this one by itself.

```
[get_qualitative_threshold(1)]
args       = qualitative_id
definition = inputlookup append=T qualitative_thresholds_lookup where qualitative_id="$qualitative_id$" |
return threshold | eval search=replace(search,"\"","")
```

The macro takes the following arguments:

qualitative_id
: The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

[get_qualitative_lower_threshold]

This is a building block for [mltk_apply_upper]. You might not use this one by itself.

```
[get_qualitative_lower_threshold(1)]
args       = qualitative_id
definition = inputlookup append=T qualitative_thresholds_lookup where qualitative_id="$qualitative_id$" |
rename threshold as lower_threshold | return lower_threshold | eval search=replace(search,"\"","")
```

The macro takes the following arguments:

qualitative_id
: The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

[get_qualitative_upper_threshold]

This is a building block for [mltk_apply_upper]. You might not use this one by itself.

```
[get_qualitative_upper_threshold(1)]
args       = qualitative_id
definition = inputlookup append=T qualitative_thresholds_lookup where qualitative_id="$qualitative_id$" |
rename threshold as upper_threshold | return upper_threshold | eval search=replace(search,"\"","")
```

The macro takes the following arguments:

qualitative_id

> The default IDs that correspond to percentages of deviation, representing where on the distribution curve to start looking for the outliers, such as `medium`.

[get_findbest_thresholds]

This is a building block for [mltk_findbest]. You might not use this one by itself.

```
[get_findbest_thresholds]
definition = inputlookup append=T qualitative_thresholds_lookup | stats values(threshold) as search | eval
search="threshold=\"".mvjoin(mvsort(search), ",")."\""
```

[get_findbest_qualitative]

This is a building block for [mltk_findbest]. You might not use this one by itself.

```
[get_findbest_qualitative]
definition = inputlookup append=T qualitative_thresholds_lookup | eval
threshold_id="findbest_th=".threshold | sort threshold | eval
subcase="'".threshold_id."'=\"1.0\",\"".qualitative_label."\"" | stats values(subcase) as search | eval
search="qualitative=case(".mvjoin(search, ",").")"
```

Convert Extreme Searches to Machine Learning Toolkit in Splunk Enterprise Security

If you need to convert any locally modified XS searches to MLTK, use the following information to help guide your decisions.

Converting XS commands

The most common common XS commands that have MLTK equivalents in ES follow.

xsWhere

The `xsWhere` command is approximately equivalent to the `` `mltk_apply` `` macro. These apply data to a model, compare against thresholds, and find outliers for a field. For each value, given the provided threshold, the macros tell you if the value is an outlier. See Abnormally High Number of HTTP Method Events By Src - Rule in DA-ESS-NetworkProtection.

xsFindBestConcept

The `xsFindBestConcept` command is approximately equivalent to the `` `mltk_findbest` `` macro. They are almost the opposite of the `xsWhere` and `apply`commands. For each value, these tell you in which threshold range the value falls on the distribution curve. For example: the high range is between 0.05 - 0.01, and the extreme range is between 0.01 -

0.000000001. See Access - Total Access Attempts in DA-ESS-AccessProtection.

xsCreateDDContext

The `xsCreateDDContext` command is approximately equivalent to the `fit` command. These both generate a new model each time the search is run. See Access - Authentication Failures By Source in SA-AccessProtection

xsUpdateDDContext

Each time this is run, it will combine the new training with the existing model. There is no `xsUpdateDDContext` equivalent in MLTK at this time. There are no models/contexts that are updated additively. All model-generation searches wipe out the old model and produce a new model based on the data retrieved in the dispatch window.

To accommodate this change, the dispatch times of the Model Gen searches that were converted from `xsUpdateDDContext` XS searches have been increased to generate the model from more data, to get more reliable models.

Converting a Context Gen Search

As an example of converting a context gen search, consider Access - Authentication Failures By Source - Context Gen as three lines.

Line	SPL
1.	`| tstats `summariesonly` count as failures from datamodel=Authentication.Authentication where Authentication.action="failure" by Authentication.src,_time span=1h`
2.	`| stats median(failures) as median, min(failures) as min, count as count | eval max = median*2`
3.	`| xsUpdateDDContext app="SA-AccessProtection" name=failures_by_src_count_1h container=authentication scope=app | stats count`

Line one
Line one starts by counting the authentication failures per hour:
`` | tstats `summariesonly` count as failures from datamodel=Authentication.Authentication where Authentication.action="failure" by Authentication.src,_time span=1h ``.

Line two
Line two contains `stats median(failures) as median, min(failures) as min, count as count | eval max = median*2`, which is putting the results of the search into the input format that the XS `xsUpdateDDContext` command requires. In some searches you see the macro `` `context_stats` `` used instead, such as `` `context_stats(web_event_count, http_method)` ``.

Line three
Line three uses the XS `xsUpdateDDContext` command to build a data-defined historical view context, puts it in an `app` context, gives it a `name`, assigns a `container`, and a `scope`.

Consider the MLTK version of the search is Access - Authentication Failures By Source - Model Gen as two lines.

Line	SPL
1.	`| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where Authentication.action="failure" by Authentication.src,_time span=1h`
2.	`| fit DensityFunction failure dist=norm into app:failures_by_src_count_1h`

The steps for converting this search from a context gen search to a model gen search follow:

1. Line one starts the same way for both searches, by counting the authentication failures per hour. Keep this when converting to MLTK.
2. The fit command takes tables as inputs, thus it is not necessary to include
   `| stats median(failures) as median, min(failures) as min, count as count | eval max = median*2`
3. In line two for the MLTK version of the search, do the following:
    1. Replace the XS command `xsUpdateDDContext` with the approximate equivalent of `fit DensityFunction`.
    2. Include the `failure` field that you're counting in the first part of the search.
    3. Add the `dist=norm` to represent the normal distribution bell curve of the density function.
    4. Use `into` for passing the data into the model.
    5. Keep the `name` from the original search because it is also the model name for MLTK.
        1. All MLTK model names should include the `app:` prefix, which properly saves the model into the shared application namespace.
        2. In this example, append it to the name "failures_by_src_count_1h" so that it resembles `app:failures_by_src_count_1h`.

Converting a Correlation Search

As an example of converting a correlation search, consider Access - Brute Force Access Behavior Detected - Rule as four lines.

Line	SPL
1.	`| from datamodel:"Authentication"."Authentication"`
2.	`| stats values(tag) as tag,values(app) as app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src`
3.	`| search success>0`
4.	`| xswhere failure from failures_by_src_count_1h in authentication is above medium`

Line one

Line one starts by searching the authentication data model:
`| from datamodel:"Authentication"."Authentication"`

Line two

Line two contains `| stats values(tag) as tag,values(app) as app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src`, which is counting authentication failures followed by success.

Line three

Line three searches for successes greater than 0.

Line four

Line four uses the XS `xswhere` command to match a concept within a specified context and determine compatibility, in this case `authentication is above medium`.

Consider the MLTK version of the search Access - Brute Force Access Behavior Detected - Rule as four lines.

Line	SPL

Line	SPL
1.	| from datamodel:"Authentication"."Authentication"
2.	| stats values(tag) as tag,values(app) as app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src
3.	| search success>0
4.	`mltk_apply_upper("app:failures_by_src_count_1h", "medium", "failure")`

The steps for converting this search to MLTK:

1. Keep line 1 as-is.
2. Keep line 2 as-is.
3. Keep line 3 as-is.
4. In line four, do the following:
    1. Replace the XS command xswhere with the approximate equivalent of the `` `mltk_apply_upper` `` macro.
        1. The macro wraps the MLTK apply function and filters the results based on whether the values are above or below a certain threshold.
    2. Include the argument for the model name app:failures_by_src_count_1h from the model gen search that builds the model.
    3. Include the argument for the qualitative_id of medium.
    4. Include the argument for the failure field that you're counting in the first part of the search.

Converting a Key Indicator Search

To convert a Key Indicator search to use MLTK, you have to first convert the corresponding Model Gen search. The Key Indicator search references the ML model name created by the Model Gen search.

As an example of converting a correlation search, consider Risk - Median Risk Score as seven lines.

Line	SPL
1.	| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-24h@h latest=+0s by All_Risk.risk_object | stats median(accum_risk) as current_count | appendcols
2.	[| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-48h@h latest=-24h@h by All_Risk.risk_object | stats median(accum_risk) as historical_count]
3.	| `get_ksi_fields(current_count, historical_count)`
4.	| xsfindbestconcept current_count FROM median_object_risk_by_object_type_1d IN risk as current_count_qual
5.	| xsfindbestconcept delta FROM percentile in default as delta_qual

Line one
Line one starts by searching for data from the current day.

Line two
Line two starts by searching data from the previous day.

Line three
Line three calculates the delta as a percentage between current_count and historical_count (today's value and yesterday's value). So if yesterday's value was 100 and today's is 125, then the delta = 25% and the direction = increasing.

Line four
Line four evaluates the statistics counts.

Line five
Line five finds the delta percentage for the key indicator in the risk analysis dashboard.

Converting Risk - Median Risk Score to MLTK.

Line	SPL
1.	| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-24h@h latest=+0s by All_Risk.risk_object | stats median(accum_risk) as current_count | appendcols
2.	[| tstats `summariesonly` sum(All_Risk.risk_score) as accum_risk from datamodel=Risk.All_Risk where earliest=-48h@h latest=-24h@h by All_Risk.risk_object | stats median(accum_risk) as historical_count]
3.	| `get_ksi_fields(current_count, historical_count)`
4.	| `mltk_findbest("app:median_object_risk_by_object_type_1d")`
5.	| `get_percentage_qualitative(delta, delta_qual)`

Lines one through three remain as-is. The last two lines are replaced with the MLTK equivalent:

1. In line four, replace the `xsfindbestconcept current_count` with the approximate equivalent of `` `mltk_findbest` `` macro. This is a macro that wraps the MLTK `apply` function. For each value, this macro tells you in which threshold range the value falls on the distribution curve. Notice that this model doesn't need a field name for a specific field that you're applying it on. This is because the field is determined during the `fit`, so you only need to make sure that the field exists in the results when doing the `apply`.
2. In line five, replace the `xsfindbestconcept delta` with the approximate equivalent of the `` `get_percentage_qualitative` `` macro. This applies a qualitative term to the delta between the current count and the historical count, such as extremely, moderately, greatly. You will see these as indicators in the risk analysis dashboard.

You cannot rename current_count, as this is expected.

Machine Learning Toolkit Troubleshooting in Splunk Enterprise Security

Troubleshoot MLTK in Splunk Enterprise Security. There are some known issues and potential workarounds.

Error messages

MLTK errors are found in the `mlspl.log` file. The errors themselves are not necessarily enough to troubleshoot the issues. The Machine Learning Audit dashboard helps to correlate MLTK errors with the corresponding failed searches. See Machine Learning Audit Dashboard.

Testing and training models overwrites them

MLTK replaces the models with every run if you're not using `partial_fit=true`. Even if you are using `partial_fit=true`, MLTK updates the original model, which you might not want. You can test in your user space without overwriting or updating the original model. MLTK model names with the app: prefix are saved into the shared application namespace, for example: `./apps/SA-AccessProtection/lookups/failures_by_src_count_1d.csv`. If you are the admin user and you revise the search to remove the app: prefix, then it will save in the admin user space, such as `./users/admin/SplunkEnterpriseSecuritySuite/lookups/recipients_by_src_1h.csv`, and it will not overwrite the original. The user and app name spaces depend on the user that is logged in and the app currently running. You can also revise the name of the model to avoid overwriting the original while testing.

Original model name:

```
| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where
Authentication.action="failure" by Authentication.src,_time span=1h | fit DensityFunction failure dist=norm
into app:failures_by_src_count_1h
```

Model name revised to save in non-app space:

```
| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where
Authentication.action="failure" by Authentication.src,_time span=1h | fit DensityFunction failure dist=norm
into failures_by_src_count_1h
```

Model name revised to include testing:

```
| tstats `summariesonly` count as failure from datamodel=Authentication.Authentication where
Authentication.action="failure" by Authentication.src,_time span=1h | fit DensityFunction failure dist=norm
into app:testing_failures_by_src_count_1h
```

Maximum group limit

There is a limit of 1024 on the maximum number of groups that can be created when using the MLTK DensityFunction with a `by` clause. If you have custom searches that you're converting to MLTK, depending what you use to split your searches, the results will not display if the number of groups is too large to split with the `by` clause. To change the limit, change the value of the `max_groups` field in the DensityFunction stanza of the `mlspl.conf` file in the Machine Learning Toolkit app.

Example search

```
| tstats `summariesonly` count as dest_port_traffic_count from datamodel=Network_Traffic.All_Traffic by
All_Traffic.dest_port,_time span=1d | `drop_dm_object_name("All_Traffic")` | fit DensityFunction
dest_port_traffic_count by dest_port dist=norm into app:count_by_dest_port_1d
```

Example error message

Error in 'fit' command: Error while fitting "DensityFunction model: The number of groups cannot exceed <abc>; the current number of groups is <xyz>."

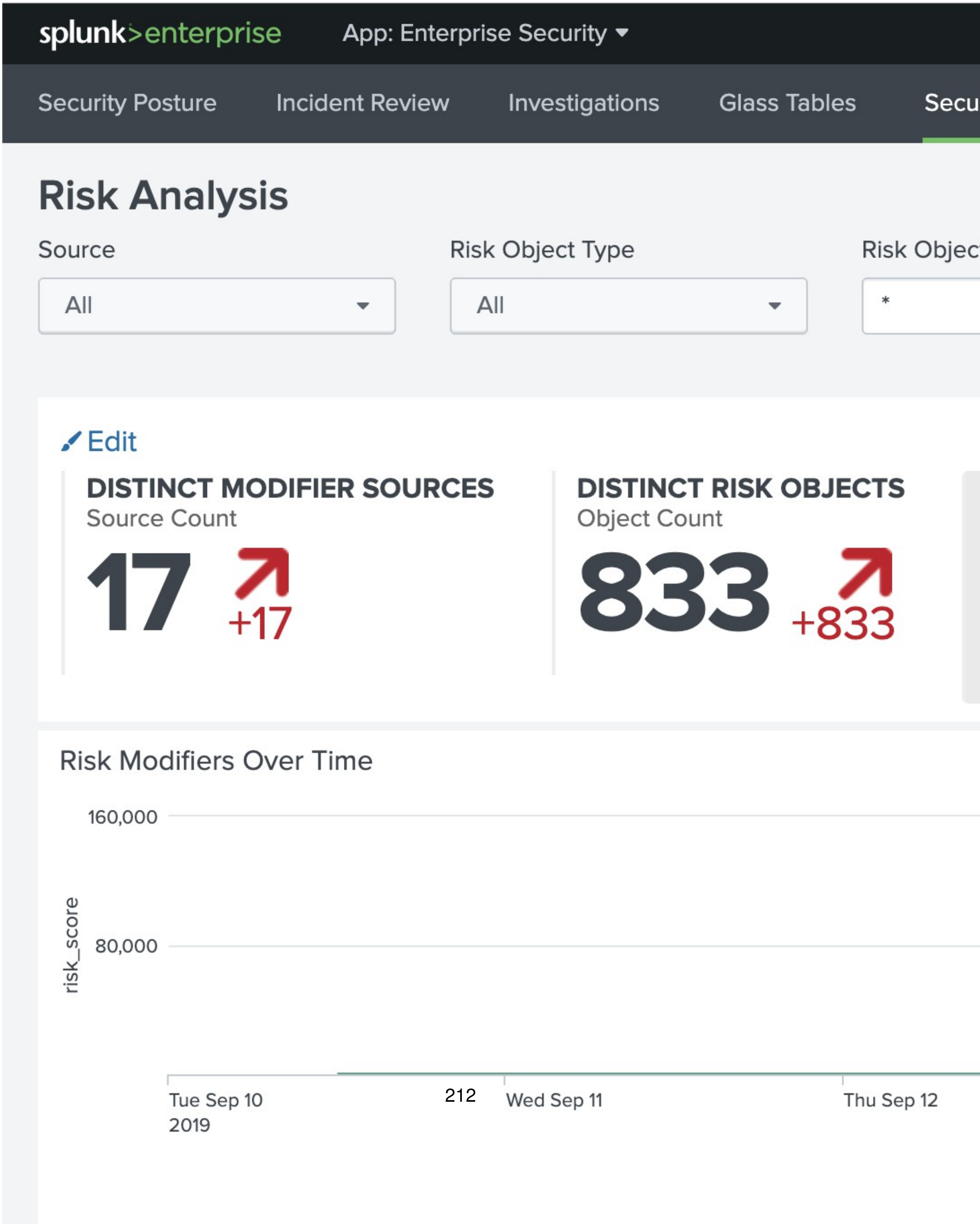
See the syntax constraints of the Density Function in the Splunk Machine Learning Toolkit *User Guide*.

CSV required

There's a lookup table file at `$SPLUNK_HOME/etc/apps/SA-Utils/lookups/qualitative_thresholds.csv` that's required for using the qualitative_id thresholds. If the CSV file is missing, then you can't use the qualitative_id thresholds for extreme, high, medium, low, and minimal.

MLTK-backed key performance indicator errors

The Risk Analysis page shows risk scores that are "unable to load results" for up to one day after a risk modifier has been created.



splunk>enterprise App: Enterprise Security ▾

Security Posture Incident Review Investigations Glass Tables Secu

Risk Analysis

Source: All ▾

Risk Object Type: All ▾

Risk Objec: *

Edit

DISTINCT MODIFIER SOURCES
Source Count
17 ↗ +17

DISTINCT RISK OBJECTS
Object Count
833 ↗ +833

Risk Modifiers Over Time

This occurs because the key security indicator searches have been updated to MLTK, and the corresponding MLTK models of these qualitative key indicators haven't been generated yet.

To load these results, manually run the following searches from **Configure > Content > Content Management**:

- `Risk - Median Object Risk Per Day - Model Gen`
- `Risk - Total Risk By Risk Object Type Per Day - Model Gen`

Python3 and MLTK 5.x

When the Python2 to Python3 cut-off happens, such as in MLTK 5.x, the previously generated models from MLTK 4.x will not be compatible and will have to be regenerated. This may not be an issue since the model-gen searches run on a daily basis anyway. However, you will have to re-run models immediately after upgrading to MLTK 5.x if you want to use MLTK searches.

See Update Splunk MLTK models for Python 3 in the Splunk Enterprise *Python 3 Migration* guide.