Splunk® Enterprise Security Administer Splunk Enterprise Security 4.7.4

Generated: 11/30/2017 1:29 pm

Table of Contents

Table of Contents

Assets and Identities

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" or "user" 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 - Lookup Gen** lookup generation search. The search runs every 30 minutes and updates 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 search.

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 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.

Note: 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 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.

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 new 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 review 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. For example, if your search includes a stats search `| stats count by src | where count>5`, the `src` and `count` fields appear in the notable event details. To add the `dest` field to the notable event details, you might change the search to the following: `| stats values(dest) as dest,count by src`.
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**.

Manage notable event statuses

An analyst assigns a status to a notable event to communicate the state of the 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 > Notable Event Statuses**

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)	A notable event has not been reviewed.	No
In Progress	An investigation or response to the notable event is in progress.	Yes
Pending	A notable event closure is pending some action.	Yes
Resolved	A notable event has been resolved and awaits verification.	Yes
Closed	A 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 > Notable Event Statuses**.
2. Select a notable event status to open the **Edit Notable Event Status** page.
3. Change the **Label** or **Description** as desired.

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 affect only 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 will change 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 will remain the same.

Notable event status transitions

The status names represent the steps required in investigating a notable event. Status transitions define the path of a notable event investigation.

An analyst assigned a notable event will change the status of the notable event as the investigation progresses. To change the current status on a notable event:

- The analyst must be a member of a role that has permission to change a status. Notable event status transitions are available to the **ess_analyst** and **ess_admin** roles by default.
- The follow-on status must allow a transition from the current status. Every status can transition to any other status by default. For example, a notable event in a **New** status can transition directly to any other status including **Closed**.

Restrict status transitions

You can define a transition workflow and limit which status can transition to another status, creating a predefined path for the notable event investigation workflow. By default, no transition path is defined or required and every status can transition to every other status.

Prerequisites

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

Restrict notable event status transitions

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Notable Event Statuses**.
2. Select a notable event status to open the Edit Notable Event Status page.
3. In Status Transitions, modify the **To Status** fields.
    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 an event to the selected status, choose **Unselect All**.
4. Save the changes.
5. Test the changes to the status workflow. If any transitions required adding or removing roles, test with credentials assigned to each role.

Add a new status

Add a new status to the notable event investigation workflow. If you restrict status transitions, determine where this status fits in the workflow.

1. Define the status workflow for notable events.
    1. Determine where the new status is needed in the workflow.
    2. Determine whether any roles (e.g. **ess_admin**) will be allowed to bypass the new status in the workflow.
2. On the Splunk Enterprise Security toolbar, open **Configure > Incident Management** and select **Notable Event Statuses**.
3. Select **New**.
4. Add a label. This is the **Status** field value used on the Incident Review dashboard and for notable event status reporting. Example: Waiting on ITOps
5. Add a description. The description is only referenced in the Notable Event Status page. Example: Waiting on another department.
6. (Optional) Select **Default status**. Choose only if you are replacing the **New** status for notable events
7. (Optional) Select **End status**. Choose when adding an additional **Closed** status for notable events.
8. Define the Status Transitions by modifying the **To Status** fields.
    1. Review the status workflow and determine which statuses a notable event can transition to.
    2. Choose the **Authorization** field and add the roles allowed to transition a notable event to the selected status.
9. Save the changes.
   Example: In our workflow, the "Waiting on ITOps" status occurs after "New" and "In Progress", but before "Pending." It is not a required status and can be skipped over to choose "Pending." Edit the Status Transitions

in "Waiting on ITOps" for "Pending," "Resolved," and "Closed" and add the roles **ess_admin** and **ess_analyst** added under Authorization.

10. Edit the statuses that will precede the new status in the workflow, and add the roles allowed to perform the transition.
    Example: In our workflow, a notable event can be given a status of "Waiting on ITOps" from a status of "New" and "In Progress." Edit the Status Transitions in both "New" and "In Progress" adding the **ess_admin** and **ess_analyst** roles under Authorization for "Waiting on ITOps".
11. Test to ensure the status can be assigned and that any status transitions involving it work.

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.
5. Set the **Expiration Time**. This defines a time limit for the suppression filter. If the time limit is met, the suppression filter is disabled.

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.

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.

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 **Use 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.

Data sources for investigations

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

Investigation details from investigations created in pre-4.6.0 versions 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.

Troubleshoot investigation action history items

Action history items do not immediately appear in your action history after you perform an action. You can only view action history items and add them to an investigation after the saved searches that create action history items run. By default, the searches run every two minutes. Five saved searches create action history items.

- 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 Management** and using the filters on the page. If you change these saved searches, action history items might stop appearing 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.

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.

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 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.

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.

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

- 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.

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 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.

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*.

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`
`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      =
```

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.

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 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 response 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 imported by Splunk Enterprise Security. See Import custom apps and add-ons to Splunk Enterprise Security in the *Install and Upgrade 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.

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.

Note: Analysts can trigger selected 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 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 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. 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.
15. 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.

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. Type the score to assign to the risk object.
3. Type a field in the search to apply the risk score to for the **Risk Object Field**.
   For example, type "src" to specify the source field.
4. Select the **Risk Object Type** to apply the risk score to.

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.

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 filename 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.

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.

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.

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.

Assets and Identities

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.

Add asset and identity data to Splunk Enterprise Security to take advantage of asset and identity correlation.

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. (Optional) Define identity formats on the identity configuration page in Splunk Enterprise Security.
3. Format the asset or identity list as a lookup in Splunk Enterprise Security.
4. Configure a new asset or identity list in Splunk Enterprise Security.
5. Verify that your asset or identity data was added to Splunk Enterprise Security.
6. Configure asset and identity correlation in Splunk Enterprise Security.

See also

How Splunk Enterprise Security correlates, processes, and merges asset and identity data

Lookups that store merged asset and identity data

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. For examples of adding asset and identity data, see Example methods of adding asset and identity data to Splunk Enterprise Security.

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.
LDAP	Both	SA-ldapsearch and a custom search.
CMDB	Asset	DB Connect and a custom search.
ServiceNow	Both	Splunk Add-on for ServiceNow
Asset Discovery	Asset	Asset Discovery App
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.
Splunk platform	Asset	Add asset data from indexed events in Splunk platform.

Next step

(Optional) Define identity formats in Splunk Enterprise Security

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

Define identity formats in Splunk Enterprise Security

Define the identity formats that identify users in your environment on the Identity Lookup Configuration page. Changes made on the Identity Lookup Configuration page modify the `identityLookup.conf` file.

Prerequisite

Collect and extract asset and identity data in Splunk Enterprise Security

Steps

1. From the Splunk ES menu bar, select **Configure > Data Enrichment > Identity Lookup Configuration**.
2. (Optional) Deselect the check box for **Email** if email addresses do not identify users in your environment.
3. (Optional) Deselect the check box for **Email short** if the username of an email address does not identify users in your environment.
4. (Optional) Select the check box for **Convention** if you want to define custom conventions to use to identify users. Click **Add a new convention** to add a custom convention.
   For example, identify users by the first 3 letters of their first name and last name with the convention `first(3)last(3)`.
5. (Optional) Select the check box for **Case Sensitive** to require case sensitive identity matching. Case sensitive identity matching produces fewer matches.
6. Click **Save**.

Next step

Format the 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
- (Optional) Define identity formats in 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. 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 > Data Enrichment > Lists and Lookups**.
- Locate the list in the file system, the `demo_assets.csv` file is located in `SA-IdentityManagement/package/lookups`.

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 lookup header

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_ex
```

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	Exa
ip	pipe-delimited numbers	A pipe-delimited list of single IP address or IP ranges. An asset is required to have an entry in the **ip**, **mac**, **nt_host**, or **dns** fields. Do not use pipe-delimiting for more than one of these fields per asset.	2.0.0.0/8|1.2.3.4|192.168.15.9-192.169.15.2
mac	pipe-delimited strings	A pipe-delimited list of MAC address. An asset is required to have an entry in the **ip**, **mac**, **nt_host**, or **dns** fields. Do not use pipe-delimiting for more than one of these fields per asset.	00:25:bc:42:f4:60|00:50:ef:84:f1:21|00:50:ef:
nt_host	pipe-delimited strings	A pipe-delimited list of Windows machine names. An asset is required to have an entry in the **ip**, **mac**, **nt_host**, or **dns** fields. Do not use pipe-delimiting for more than one of these fields per asset.	ACME-0005|SSPROCKETS-0102|COSWC

dns	pipe-delimited strings	A pipe-delimited list of DNS names. An asset is required to have an entry in the **ip**, **mac**, **nt_host**, or **dns** fields. Do not use pipe-delimiting for more than one of these fields per asset.	acme-0005.corp1.acmetech.org|SSPROCKE
owner	string	The user or department associated with the device	f.prefect@acmetech.org, DevOps, Bill
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	41.040855
long	string	The longitude of the asset	28.986183

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 asset and identity correlation and categorization. See Categories.	server|web_farm|cloud
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	"true", or blank to indicate "false"

		correlation search performs an adaptive response action when this asset stops reporting events.	
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"
requires_av	boolean	Indicates whether this asset must have anti-virus software installed.	"true", or blank to indicate "false"

Identity lookup header

```
identity,prefix,nick,first,last,suffix,email,phone,phone2,managedBy,priority,bunit,cate
```

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@
prefix	string	Prefix of the identity.	Ms., Mr.
nick	string	Nickname of an identity.	Van Helsing
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 telephone number of an identity.	123-456-7890
phone2	string	A secondary telephone number of an identity.	012-345-6789
managedBy	string	A username representing the	phb@acmetech.org

		manager of an identity.	
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	Privileged|Officer|CISO

		categorization. See Categories.	
watchlist	boolean	Marks the identity for activity monitoring.	Accepted values: "true" or empty. See User Acti in this manual.
startDate	string	The start or hire date of an identity.	Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:
endDate	string	The end or termination date of an identity.	Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:
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 DD with compass direction.	37.78N
work_long	string	The longitude of primary work site City in DD with compass direction.	122.41W

Configure the new asset or identity list in Splunk Enterprise Security

Configure the 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.

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

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
5. Add an input stanza for the lookup source
6. (Optional) Force a merge

Add the new lookup table file

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.

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**.

Add an input stanza for the lookup source

1. Return to Splunk Enterprise Security.
2. From the Splunk ES menu bar, select **Configure > Data Enrichment > Identity Management**.
3. Click **New**.
4. Type the name of the lookup.
   For example, `network_assets_from_CMDB`.
5. Type a **Category** to describe the new asset or identity list.
   For example, CMDB_network_assets.
6. Type a **Description** of the contents of the list.
   For example, network assets from the CMDB.
7. Type **asset** or **identity** to define the type of list.
8. Type a **Source** that refers to the lookup definition name.
   For example, `lookup://network_assets_from_CMDB`.
9. Click **Save**.
10. Wait five minutes. Splunk Enterprise Security merges the asset and identity lists every five minutes with a saved search. For an explanation of this process, see How Splunk Enterprise Security processes and merges asset and identity data.

Force a merge

You can also run the primary saved searches directly to force a merge immediately without waiting the five minutes for the scheduled search to run.

1. Open the Search page.
2. Run the primary saved searches.

```
| from savedsearch:"Identity - Asset String Matches -
Lookup Gen"
| from savedsearch:"Identity - Asset CIDR Matches - Lookup
Gen"
| from savedsearch:"Identity - Identity Matches - Lookup
Gen"
```

Next step

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

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.

Prerequisite

Configure the new asset or identity list 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")`
    ```

Next step

Configure asset and identity correlation in Splunk Enterprise Security

Configure asset and identity correlation in Splunk Enterprise Security

After you add your asset and identity data to Splunk Enterprise Security, configure asset and identity correlation in Splunk Enterprise Security.

Prerequisite

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

Steps

1. Choose whether to enable asset and identity correlation, disable it, or restrict correlation to occur only for select source types. If in doubt, keep asset and identity correlation enabled. See How asset and identity correlation works for more information about how the correlation enriches events at search time.
2. From the Splunk ES menu bar, select **Configure > Data Enrichment > Identity Correlation**.
3. **Enable correlation** is selected by default. You can change this to **Disable correlation** (not recommended) or **Enable selectively by sourcetype**.
4. If you choose **Enable selectively by sourcetype**, type a source type and select the check box for asset and/or identity.
5. Click **Save**.

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.

How asset and identity correlation works

To effectively detect security intrusions, an organization must be able to correlate events in log data with specific assets and identities that may be responsible for, or affected by the intrusion. 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. 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*.

Asset and identity correlation enriches events with asset and identity data at search time.

- 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 NetBIOS 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 user or session.
- 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 allows you to 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, open the Asset Investigator dashboard on a `src` field.

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. You configure any settings in the identity lookup configuration setup. See Define identity formats on the identity configuration page.
3. The Splunk Enterprise Security identity manager modular input updates settings in the `transforms.conf` stanza `identity_lookup_expanded`.
4. 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.
5. You configure the list as a lookup table, definition, and input. See Configure a new asset or identity list.
6. The Splunk Enterprise Security identity manager modular input detects two things:
    - ♦ Changed content in the `identity_manager://<input_name>`.
    - ♦ Changes to stanzas in the input.

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`. For example, the `` `generate_identities` `` macro dynamically updates based on the conventions specified on the Identity Lookup Configuration page.
8. The Splunk Enterprise Security identity manager modular input dispatches lookup generating saved searches if it identifies changes that require the asset and identity lists to be merged.
9. The lookup generating saved searches merge all configured and enabled asset and identity lists.
    - The primary saved 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.
    - Secondary saved searches generate lookup tables for asset categories, identity categories, and asset PCI domains (in the Splunk App for PCI Compliance).
10. 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.

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-d LOOKUP-zu-asset_lookup_by_str-d LOOKUP-zu-asset_lookup_by_str-s
CIDR subnet-based	assets_by_cidr.csv	Identity - Asset	LOOKUP-zv-asset_lookup_by_cidr- LOOKUP-zv-asset_lookup_by_cidr-

asset correlation		CIDR Matches - Lookup Gen	LOOKUP-zv-asset_lookup_by_cidr-s
String-based identity correlation	identities_expanded.csv	Identity - Identity Matches - Lookup Gen	LOOKUP-zy-identity_lookup_expand LOOKUP-zy-identity_lookup_expand
Default field correlation	identity_lookup_default_fields.csv asset_lookup_default_fields.csv		LOOKUP-zz-asset_identity_lookup_ LOOKUP-zz-asset_identity_lookup_ LOOKUP-zz-asset_identity_lookup_ LOOKUP-zz-asset_identity_lookup_ LOOKUP-zz-asset_identity_lookup_

For more information about the asset and identity merge process, see How Splunk Enterprise Security processes and merges asset and identity data.

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.

For more information about the merge process, see How Splunk Enterprise Security processes and merges asset and identity data.

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
city	unchanged
country	unchanged

dns	Accepts pipe-delimited values and converts them to a multi-value field.
lat	unchanged
long	unchanged
mac	Accepts pipe-delimited values and converts them to a multi-value field.
nt_host	Accepts pipe-delimited values and converts them to a multi-value field.
owner	unchanged
priority	unchanged
asset_id	Generated from the values of dns, ip, mac, and nt_host fields.
asset_tag	Generated from the values of category, pci_domain, is_expected, should_timesync, should_update, requires_av, and bunit fields.
category	Appends "pci" if the value contains "cardholder". Accepts pipe-delimited values and converts them to a multi-value field.
ip	Validates and splits the field into CIDR subnets as necessary. Accepts pipe-delimited values and converts them to a multi-value field.
pci_domain	Appends "trust" or "untrust" based on certain field values. Accepts pipe-delimited values and converts them to a multi-value field.
is_expected	Normalized to a boolean.
should_timesync	Normalized to a boolean.
should_update	Normalized to a boolean.
requires_av	Normalized to a boolean.
key	Generated by the ip, mac, nt_host, and dns fields after the original fields are transformed.

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
email	unchanged
endDate	unchanged
first	unchanged
last	unchanged
managedBy	unchanged
nick	unchanged
phone	unchanged
phone2	unchanged
prefix	unchanged
priority	unchanged
startDate	unchanged
suffix	unchanged
work_city	unchanged
work_country	unchanged
work_lat	unchanged
work_long	unchanged
watchlist	Normalized to a boolean.
category	Appends "pci" if the value contains "cardholder". Accepts pipe-delimited 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 pipe-delimited values and converts them to a multi-value field.
identity_id	Generated from the values of identity, first, last, and email.
identity_tag	Generated from the values of bunit, category, and watchlist.

Test the asset and identity merge process in Splunk Enterprise Security

Test the asset and identity merge process to confirm that the data produced by the merge process is expected and accurate. Run the saved searches that perform the merge process without outputting the data to the merged lookups to determine what the merge will do with your data without actually performing the merge.

Test the merge process without performing a merge and outputting the data to a lookup.

1. From the Splunk ES menu bar, select **Configure > Content Management**.
2. Locate the first of the three primary saved searches **Identity - Asset CIDR Matches - Lookup Gen**.
3. Click the search name to open it.
4. Copy the search from the **Search** field.
5. Open the **Search** page.
6. Paste the search and remove the `` `output_*` `` macro. For example, change `` | `asset_sources` | `make_assets_cidr` | `output_assets("SA-IdentityManagement", "assets_by_cidr.csv")` `` to `` | `asset_sources` | `make_assets_cidr` ``.
7. Run the search.
8. Repeat steps 2-7 for the other two searches, **Identity - Asset String Matches - Lookup Gen** and **Identity - Identity Matches - Lookup Gen**.

Customize the asset and identity merge process in Splunk Enterprise Security

You can modify the saved searches that perform the asset and identity merge process to perform additional field transformations or data sanitization. Add any operations that you want to change in the merge process to the search before the `` `output_*` `` macro.

Certain modifications to the saved searches are unsupported and could break the merge process or asset and identity correlation.

- Do not add or delete fields from the output.
- Do not change the output location to a different lookup table or a KV store collection.
- Do not replace the `` `output_*` `` macros with the `outputlookup` command.

Modify asset and identity lookups in Splunk Enterprise Security

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

Edit asset and identity lookups

Edit an asset or identity lookup in the Identity Management dashboard.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Find the name of the asset or identity list you want to edit, and select **Source**. 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.

Changes made to an asset or identity list will be reflected in search results after the next scheduled merge. See How Splunk Enterprise Security processes and merges asset and identity data.

Disable or enable asset and identity lookups

Disable or enable an asset or identity lookup table file. Disable a list to prevent the contents of that list from being included in the merge process. Enable a disabled list to allow the list to be merged at the next scheduled merge of the asset or identity data. Disabling a list does not delete the data from Splunk Enterprise Security.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Locate the asset or identity lookup you want to disable.
3. Click **Disable** or **Enable**.

Disable the demo asset and identity lookups

Disable the demo asset and 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. Splunk Enterprise Security enables the demo asset and identity lookups after installation or upgrade. After you disable the demo data lookups, saved searches update the primary asset and identity lookups and removes the data from the disabled lookups from the primary lookups.

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

Include or exclude asset or identity lookups from bundle replication

Starting in version 4.7.0, 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. See Lookups that store merged asset and identity data in Splunk Enterprise Security for the lookup files that continue to be included in bundle replication.

Changing the default to include asset and identity lookup files in bundle replication might reduce system performance.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Click the lookup that you want to include or exclude from bundle replication.
3. Select or deselect the check box for **Blacklist**. If selected, the lookup file is excluded from bundle replication.

You can only make this change if the "Enable Identity Generation Autoupdate" setting is set to "true". See Configure general settings for Splunk Enterprise Security.

Example methods of adding asset and identity data in Splunk Enterprise Security

These example methods cover some common ways to add asset and identity data to Splunk Enterprise Security. You can work with Splunk Professional Services to find the best solution for your environment.

Add asset and identity data from Active Directory

This example describes how to add asset and identity data from Active Directory.

Set up the Splunk Support for Active Directory app

Collect asset and identity data with the Splunk Support for Active Directory app. For information about installing and configuring the app, see Install the Splunk Supporting Add-on for Active Directory.

Collect asset and identity data from Active Directory

Collect asset and identity data from Active Directory by searching the data in SA-ldapsearch.

1. Follow the steps to configure a new asset or identity list. See Configure a new asset or identity list in Splunk Enterprise Security.
2. Disable the lookup file you created until you finish setting up the saved search to prevent the asset or identity data from merging with incomplete or inaccurate data. See Disable or enable asset and identity lookups.
3. Create a saved search in SA-IdentityManagement to populate the lookup table file with the `ldapsearch` command. The exact syntax of this search varies depending on your AD configuration. See Example search for collecting identity data from Active Directory and Example search for collecting asset data from Active Directory for two examples.
4. Test the merge process. See Test the asset and identity merge process in Splunk Enterprise Security.

Example search for collecting identity data from Active Directory

This example search assigns static values for `suffix`, `endDate`, `category`, `watchlist`, and `priority`. Use it as a guide to construct and test a working search, then replace the static values with information from your AD environment. Rename the lookup `my_identity_lookup` to something appropriate for your environment.

```
|ldapsearch domain=<domain_name>
search="(&(objectclass=user)(!(objectClass=computer)))"
|makemv userAccountControl
|search userAccountControl="NORMAL_ACCOUNT"
|eval suffix=""
|eval priority="medium"
|eval category="normal"
|eval watchlist="false"
```

```
|eval endDate=""
|table
sAMAccountName,personalTitle,displayName,givenName,sn,suffix,mail,telephoneNumber,mobil
|rename sAMAccountName as identity, personalTitle as prefix,
displayName as nick, givenName as first, sn as last, mail as email,
telephoneNumber as phone, mobile as phone2, manager as managedBy,
department as bunit, whenCreated as startDate
|outputlookup my_identity_lookup
```

Example search for collecting asset data from Active Directory

This example search assigns static values for several fields. Use it as a guide to construct and test a working search, then replace the static values with information from your AD environment. Rename the lookup `my_asset_lookup` to something appropriate for your environment.

```
|ldapsearch domain=<domain name> search="(&(objectClass=computer))"
|eval city=""
|eval country=""
|eval priority="medium"
|eval category="normal"
|eval dns=dNSHostName
|eval owner=managedBy
|rex field=sAMAccountName mode=sed "s/\$//g"
|eval nt_host=sAMAccountName
|makemv delim="," dn
|rex field=dn "(OU|CN)\=(?<org>.+)"
|table
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_ex
| outputlookup create_empty=false createinapp=true my_asset_lookup
```

Add asset data from indexed events in the Splunk platform

This example demonstrates how to identify hosts that appear in indexed events that are not currently associated with existing asset data and add those hosts to your asset lookup.

Use this example search to compare hosts communicating with the Splunk platform to the set of existing asset information and review the table of unmatched hosts. You can then export the table as an asset list.

```
| `host_eventcount`
| search host_is_expected=false NOT host_asset_id=*
| fields - firstTime,recentTime,lastTime,_time,
host_owner_*,host_asset_tag,host_asset_id
| sort -totalCount,dayDiff
| table
host,ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,
```

Manually add new asset or identity data

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

1. From the Splunk ES menu bar, select **Configure > Data Enrichment > Lists and Lookups**.
2. To add asset data, click the **Assets** list to edit it. 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. Click **Save**.

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.

Threat collection in KV Store	Supported IOC data types	Local lookup file	Required headers in lookup file
certificate_intel	X509 Certificates	Local Certificate Intel	`certificate_issuer, certificate_subject, certificate_issuer_organization, certificate_subject_organization, certificate_serial, certificate_issuer_unit, certificate_subject_unit, description, weight`
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.

Configure the threat intelligence sources included with Splunk Enterprise Security

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

Some of these threat intelligence sources are enabled by default.

Prerequisites

- Your Splunk Enterprise deployment must be connected to the Internet. If your deployment is not connected to the Internet, disable these threat sources or source them in an alternate way.
- To set up firewall rules for these threat sources, you might want to use a proxy server to collect the threat 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 threat sources can change.

Steps

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

Threat source	Threat list provider	Website about the threat source
Emerging Threats compromised IPs blocklist	Emerging Threats	http://rules.emergingthreats.net/blockrules
Emerging Threats firewall IP rules	Emerging Threats	http://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
iblocklist Tor	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Web attacker	I-Blocklist	https://www.iblocklist.com/lists
Malware Domain Blocklist	Malware Domains	http://mirror1.malwaredomains.com
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

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

Some lists included in Splunk Enterprise Security are not added to the threat intelligence collections and are instead used to enrich data in Enterprise Security.

Data list	Data provider	Website for data provider
Alexa Top 1 Million Sites	Alexa Internet	http://www.alexa.com/topsites
Mozilla Public Suffix List	Mozilla	https://publicsuffix.org
ICANN Top-level Domains List	IANA	http://www.iana.org/domains/root/db

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

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

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 Threat 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 input credentials in Splunk Enterprise Security.

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.

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment > Threat 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.
4. Save your changes.

Add a URL-based threat source

Add a non-TAXII source of threat intelligence that is available from a URL on the Internet.

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Downloads**.
2. Click **New** to add a new threat 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. Type a **Type** for the threat download. The type identifies the type of threat indicator that the feed contains.

5. Type a **Description**. Describe the indicators in the threat feed.
6. 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.
7. (Optional) Change the default download **Interval** for the threat feed. Defaults to 43200 seconds, or every 12 hours.
8. (Optional) Type POST arguments for the threat feed.
9. (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.
10. (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.
11. 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 delimiter used to split lines in a threat source. Delimiters must be a single character. For more 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+`

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	`<fieldname>:$<number>,<fiename>.$<number>`
		`ip:$1,description:domain_b`

	the local lookup files or the `DA-ESS-ThreatIntelligence/collections.conf` file. Defaults to `description:$1,ip:$2`.	
Ignoring regular expression	A regular expression used to ignore lines in a threat source. Defaults to ignoring blank lines and comments.	`^\s*$)`
Skip header lines	The number of header lines to skip when processing the threat source.	`0`

12. (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.	admin
Retries	The maximum number of retry attempts.	3
Timeout	Number of seconds to wait before marking a download attempt as failed.	30

13. (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.
14. 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.

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. The feed used in this example is from abuse.ch

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat 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://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.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** field 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.

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.

You need file system access to add the certificates needed for certificate authentication. In a Splunk Cloud deployment, work with Splunk Support to add or change files on cloud-based nodes.

1. Add the certificate to the `$SPLUNK_HOME/etc/apps/<app_name>/auth` directory.
2. Add the private key for the certificate to the same `/auth` directory.
3. 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 > Threat Intelligence Downloads**.

2. Click **New** to add a new TAXII feed.
3. Type a **Name** for the threat intelligence feed.
4. Type a **Type** of **taxii**.
5. Type a **Description** for the threat intelligence feed.
6. Type a URL to use to download the TAXII feed.
7. (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.
8. (Optional) Adjust the interval at which to download the threat intelligence. Defaults to 43200 seconds, or twice a day.
9. 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.	`taxii_password="password"`
cert_file	Add the certificate file name if the TAXII feed uses	`cert_file="cert.crt"`

	certificate authentication. The file name must match exactly and is case sensitive.	
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"`

10. TAXII feeds do not use the **Maximum age** setting.
11. TAXII feeds do not use the **User agent** setting.
12. TAXII feeds do not use the **Parsing Options** settings.
13. (Optional) Change the **Download Options**.
14. (Optional) Change the **Proxy Options**. See Configure a proxy for retrieving threat intelligence.
15. Save the 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.

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 OpenIOC, STIX, and CSV file types directly in the Splunk Enterprise Security interface.

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. 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.
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/threat_intel`, 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/threat_intel`
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. If you add threat indicators in a CSV file, they must all be the same type. For example, the file can only include one type of intelligence. If you want to mix types of indicators in one file, create an OpenIOC or STIX file instead using an editor available on the web and follow the instructions to Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security.

Identify whether your custom file contains certificate, domain, email, file, HTTP, IP, process, registry, service, or user threat intelligence and make sure that the custom CSV file is properly formatted.

1. Select **Configure > Data Enrichment > Lists and Lookups**.

2. Find the lookup file that matches the local threat intel you are providing. For example, **Local File Intel**.
3. Open the relevant lookup to view the required headers.
4. Create a new `.csv` file with a header row containing the required fields.
5. Add the threat data to the `.csv` file.

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. 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 > Data Enrichment > Lists and Lookups**.
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. 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

- Identify whether the custom threat source is certificate, domain, email, file, HTTP, IP, process, registry, service, or user intelligence.
- Identify the headers for the CSV file that correspond to the type of threat intelligence that you want to add by reviewing the Supported types of threat intelligence in Splunk Enterprise Security.

Steps

Based on the type of intelligence you add to Splunk Enterprise Security and the required headers, create a CSV file.

1. Create a `.csv` file with a header row with the required fields.
2. Add the threat data to the `.csv` file.

After you create the lookup file, you must add it to Splunk Enterprise Security.

1. On the Splunk platform menu bar, select **Settings > Lookups**
2. Next to **Lookup table files**, click **Add New**.
3. Select a **Destination App** of **SA-ThreatIntelligence**.
4. Upload the `.csv` file you created.
5. Type a **Destination filename** for the file. For example, `threatindicatorszerodayattack.csv`.
6. Save.

After adding the threat intel lookup to Enterprise Security, set appropriate permissions so Enterprise Security can use the file.

1. Open **Lookup table files**.

2. Find the lookup file that you added and select **Permissions**.
3. Select **All apps** for the **Object should appear in** field.
4. Select **Read** access for **Everyone**.
5. Select **Write** access for **admin**.
6. Save.

Define the lookup so that Splunk ES can import it and understand what type of intelligence you are adding.

1. On the Splunk platform menu bar, select **Settings > Lookups**.
2. Next to **Lookup definitions**, click **Add New**.
3. Select a **Destination App** of **SA-ThreatIntelligence**.
4. Type a name for the threat source. The name you enter here is used to define the threatlist in the input stanza. For example, `zero_day_attack_threat_indicators_list`.
5. Select a **Type:** of **File based**.
6. Select the **Lookup File:** that you added in step one. For example, `threatindicatorszerodayattack.csv`.
7. Save.

Set permissions on the lookup definition so that the lookup functions properly.

1. Open **Lookup definitions**
2. Find the definition you added in step four and select **Permissions**.
3. Set **Object should appear in** to **All apps**.
4. Set **Read** access for **Everyone**.
5. Set **Write** access for **admin**.
6. Save.

Add a threat source input stanza that corresponds to the lookup file so that ES knows where to find the new threat intelligence.

1. Select **Configure > Data Enrichment > Threat Intelligence Downloads**.
2. Choose a threat source input that matches your new content. For example, `local_file_intel`.
3. Click **Clone** in the **Actions** column.
4. Type a **Name**. The name cannot include spaces. For example, zero_day_attack_threat_indicators.
5. Type a **Type**. For example, zero_day_IOCs
6. Type a **Description**. For example, File-based threat indicators from zero day malware.
7. Type a **URL** that references the lookup definition you created in step three. `lookup://zero_day_attack_threat_indicators_list`.

8. (Optional) Change the default **Weight** for the threat data.
9. (Optional) Change the default **Retry interval** for the lookup.

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 threat intelligence successfully to Splunk Enterprise Security

After you add new or configure included threat intelligence sources, verify that the threat 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 threat intelligence runs every 60 seconds.

Verify that the threat 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 threat intelligence source and confirm that the **download_status** column states **threat list downloaded**.
3. Review the **Threat 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 threat 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 10 in Add a URL-based threat source.

Verify that threat indicators exist in the threat collections

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 threat intelligence sources in order to add them to Enterprise Security.

Problem	Suggestion
Issues related to downloading threat intelligence sources.	Look at the Threat 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 Threat 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.

Change existing threat intelligence in Splunk Enterprise Security

After you add threat intelligence to Splunk Enterprise Security, you can make changes to the settings to make sure the threat intelligence you correlate with events is useful.

Enable or disable a threat intelligence source

Enable or disable a threat intelligence source to prevent your events from matching data in the collections of threat intelligence.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Downloads**.
2. Find the threat intelligence source.
3. Under **Status**, click **Enable** or **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 a threat source

Change information about an existing threat source, such as the retention period or the download interval for a threat source.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Downloads**.
2. Click the name of the threat source you want to edit.
3. Make changes to the fields as needed.
4. Save your changes.

By default, only administrators can edit threat sources. To allow non-admin users to edit threat 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 intelligence was added to Enterprise Security.

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 > Threat Intelligence Downloads**.
    2. Select a threat source.
    3. Change the **Maximum age** setting using a relative time specifier.

For example, `-7d` or `-30d`.

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 threat intelligence sources. Modify the settings of the local modular inputs to manage file retention for intelligence sources.

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 Unusuable** check box so that the modular input deletes a file after processing if it has no actionable intelligence.
5. Save your changes.

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 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
- Export content from Splunk Enterprise Security as an app

See also

Create and manage lookups in Splunk Enterprise Security

Create and edit risk objects in Splunk Enterprise Security

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 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 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 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 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

Create a search-driven lookup.

1. From the Splunk Enterprise Security menu bar, select **Configure > 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. 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 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

1. From the Splunk Enterprise Security menu bar, select **Configure > 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**.

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 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. 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 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 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, 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 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. For example, the following items are included or not included in exported content.

Included in exported content

- Saved searches exported from the **Content Management** page include only the `savedsearches.conf` and `governance.conf` settings for the selected objects.
- Alert actions and response actions, including risk assignments, script names, and email addresses.

Not included in exported content

- 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.

Create and manage lookups in Splunk Enterprise Security

To configure or edit the lists or lookup files used with the Splunk Enterprise Security, select **Configure > Data Enrichment > Lists and Lookups**. Use **Lists and Lookups** to view and edit the default lists and lookups in Enterprise Security.

Click the name of a list to view or edit it. Click **Export** to export a copy of the file in CSV format.

Internal lookups

Splunk Enterprise Security maintains internal lookups to provide information for dashboards or to create notable events. See Available internal lookups for more details on the lookups included with Splunk Enterprise Security.

These lookups are created in three 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, the 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.

Edit lists and lookups

From the ES menu bar, select **Configure > Data Enrichment > Lists and Lookups** to view the list of current lookup files. Click a file name to open that lookup file in the lookup editor.

The name of the CSV file is shown in the upper left-hand corner of the panel, `assets.csv` in this example. The lookup fields are shown at the top of the table, the values for the fields are displayed in the rows below that. Positive numbers are in green, negative numbers are shown in red. The priority values in this file are color-coded. Each CSV file looks slightly different depending on the fields it contains. Lookups do not accept regular expressions.

Only users with appropriate permissions can edit lookups. See Manage permissions in Splunk Enterprise Security in this manual to edit permissions for a user role.

Edit lookup content

1. From the ES menu bar, select **Configure > Data Enrichment > Lists and Lookups** to view the list of current lookup files.
2. Click a file name to open that lookup file in the lookup editor.
3. Change a value in a cell by selecting the cell and typing the new value.
4. Right-click the table to open a context menu that you can use to add columns or rows to the file.
5. Click **Save** to save your changes or **Cancel** to return to the list of lookups without saving.

Note: You cannot save a lookup file that contains empty header fields.

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"
```

Add new lookup files

An admin might add new CSV files to support new functions and data enrichment in the application. CSV files used as lookups must be created with Unix-style line endings (`\n`).

Note: CSV files used as lookups must be created with Unix-style line endings ("`\n`"). Splunk will not correctly read lookup files saved using Macintosh ("`\r`") or Windows line endings ("`\r\n`").

1. From the Splunk platform system menu, select **Settings > Lookups**.
2. Next to **Lookup table files**, click **Add New**.
3. Verify that **SplunkEnterpriseSecuritySuite** is selected as the **Destination app**.
4. Upload a lookup file.
5. Type a **Destination filename** to be displayed in the lookup list.
6. Click **Save**.

By default, lookups are saved as **Private**. To share the information with other users, searches, and upgrade events, change the file permissions.

1. Click **Permissions** next to the newly imported CSV file.
2. Select the appropriate level and type of permissions for this file. Set access to **This app only** to limit access to Splunk Enterprise Security or select **All apps** to allow all apps in this Splunk instance to access the lookup.
3. Click **Save**.

Verify lookup files

Confirm that you added a lookup file successfully by using the `inputlookup` search command to display the list.

```
inputlookup append=T application_protocol_lookup
```

Search-driven lookups

See Create and manage search-driven lookups in Splunk Enterprise Security.

Available internal lookups

The following lookups are available by default in Splunk Enterprise Security. Select **Configure > Data Enrichment > Lists and Lookups** to view the internal lookups.

Administrative Identities

An account that is known to have administrator or super-user access, such as root or administrator accounts, is considered privileged. Splunk Enterprise Security allows you to identify these privileged accounts so that you can filter to them in relevant dashboards, such as the Access Center dashboard and the Account Management dashboard.

Configure the list of privileged accounts with the **Administrative Identities** lookup.

1. Navigate to **Configure > Data Enrichment > Lists and Lookups** and select the **Administrative Identities** lookup.
2. The list categorizes privileged default accounts as **default|privileged**. Select the field and begin typing to make changes.

Application Protocols

The Application Protocols list is a list of port/protocol combinations and their approval status in the 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 0-65535)
transport	The protocol of the network traffic (icmp, tcp, udp).
app	application name
status	The approval status of the port (approved, pending, unapproved). By default, the port is considered approved.

Assets

The Assets lookup contains information about the assets in your environment. This list of assets is matched to incoming events. See Add asset and identity data to Splunk Enterprise Security.

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.

Note: To enrich events with category information in asset and identity correlation, you must maintain the category field in the asset and identity lists rather than the Categories list. See Format an asset or identity list as a lookup in Splunk Enterprise Security.

There are two ways to maintain the 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. Enable the `Identity - Make Categories - Lookup Gen` saved search.

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 > Data Enrichment > Lists and Lookups**.
2. Click the **Asset/Identity Categories** list.
3. Add new categories to the list.
4. Save your changes.

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 shows the fields in this file.

Field	Description
app	The application that contains the view (SplunkEnterpriseSecuritySuite)
is_expected	Either "true" or "false". If not specified, Splunk Enterprise Security assumes by default that activity is not expected.
view	The name of the view. Available in the URL.

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 URL below is named `incident_review`:

Identities

The Identities lookup contains a list of identities that are matched to incoming events. See Add asset and identity data to Splunk Enterprise Security in this manual.

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.

If you open the lookup file `interesting_ports.csv` in the lookup editor, the header of the file describes the fields in the file and also described in this table.

Field	Description	Example
app	The application or service name	Win32Time
dest	The destination host for the network service. Accepts a wildcard.	DARTH*, 10.10.1.100, my_host, etc. Using just a wildcard `*` will match all hosts.
dest_pci_domain	An optional PCI Domain. Accepts a wildcard.	trust, untrust, etc.
dest_port	The destination port number. Accepts a wildcard.	443, 3389, 5900, etc.
transport	The transport protocol. Accepts a wildcard.	tcp or udp
is_required	Is the service required to be running? Alert if not present.	true or false
is_prohibited	Is the service/traffic/port prohibited from running? Alert if present.	true or false
is_secure	Is the service traffic encrypted?	true or false
note	A brief description of the service and use-case	Unencrypted telnet services are insecure.

Interesting Processes

Interesting Processes contains a list of processes. This list is used to determine whether a process is required, prohibited, and/or secure. Use the List and Lookup editor to modify or add to this list. The Interesting Processes lookup is named `interesting_processes.csv`.

The following table shows the fields in this file.

Column	Description
app	application name
dest	destination of process
dest_pci_domain	PCI domain, if available
is_required	true or false
is_prohibited	true or false
is_secure	true or false
note	Any additional information about this process

Interesting Services

Interesting Services contains a list of services in your deployment. This list is used to determine whether a service is required, prohibited, and/or secure. Use the List and Lookup editor to modify or add to this list. The Interesting Services is named `interesting_services.csv`.

The following table shows the fields in this file.

Column	Description
app	application name
dest	destination of process
dest_pci_domain	PCI domain, if available
is_required	true or false
is_prohibited	true or false
is_secure	true or false
note	Any additional information about this process

Primary Functions

Primary Functions contains a list of primary processes and services, and their function in your deployment. Use this list to designate which services are primary and the port and transport to use. The Primary Functions lookup file is named `primary_functions.csv`.

The following table shows the fields in this file.

Column	Description
process	name of process
service	name of service
dest_pci_domain	PCI domain, if available from the asset lookup. See Configure assets in the Splunk App for PCI Compliance *Installation and Configuration Manual*.
transport	tcp or udp
port	port number
is_primary	true or false
function	function of this process (for example, Proxy, Authentication, Database, Domain Name Service (DNS), Web, Mail)

Prohibited Traffic

Prohibited Traffic lists processes that will generate an alert if they are detected. This list is used by the System Center dashboard and is useful for detecting software that is prohibited by the security policy, such as IRC or data destruction tools, or for software that is known to be malicious, such as malware that was recently implicated in an outbreak.

The Prohibited Traffic file is named `prohibited_traffic.csv`.

The following table shows the fields in this file.

Field	Description
app	The name of the process (such as echo, chargen, etc.)
is_prohibited	Either "true" or "false"
note	A text description of why the process is rejected

Urgency Levels

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*.

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 > Data Enrichment > Lists and Lookups** and select the **Risk Object Types** list.
2. Highlight the last **risk_object_type** cell in the table and right-click to see the table editor.
3. Insert a new row into the table.
4. Double-click in the new row to edit it, then add the new object type name.
5. Save the changes.

Edit an existing risk object

1. From the Enterprise Security menu, select **Configure > Data Enrichment > Lists and Lookups**
2. Select the **Risk Object Types** list.
3. Highlight the risk object type and change the name.
4. Save the changes.

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
Asset Sources	A search macro that enumerates the lookup tables that contain asset information used for asset correlation.
Auto Pause	Type the time in seconds before a drilldown search will pause.
Default Watchlist Search	Define the watchlisted events for the 'Watchlisted Events' correlation search
Domain Analysis	Enable or disable WHOIS tracking for Web domains.
Domain From URL Extraction Regex	A regular expression used to extract domain (url_domain) from a URL.
Enable Identity Generation Autoupdate	If true, permit the Identity Manager to auto-update asset_sources, identity_sources, and generate_identities macros. True by default.
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	Set the start time for sparklines displayed on the **HTTP User Agent Analysis** dashboard.

Earliest	
HTTP User Agent Analysis Sparkline Span	Set the time span for sparklines displayed on the **HTTP User Agent Analysis** dashboard.
IRT Disk Sync Delay	Set the number of seconds for Enterprise Security to wait for a disk flush to finish. Relevant to indexed real time searches.
Identity Generation	Defines the transformations used to normalize identity information. See How Splunk Enterprise Security processes and merges asset and identity data
Identity Generation Timeout	Number of seconds the Identity Manager waits before warning of slow search completion in identity_manager.log.
Identity Sources	Enumerates the source lookup tables that contain identity information.
Incident Review Analyst Capacity	Estimated maximum capacity of notable events assigned to an analyst. Relative measure of analyst workload.
Indexed Realtime	Enable or disable indexed real-time mode for searches.
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.
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.
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 exceeds this threshold is anomalous.
TSTATS Allow Old Summaries	Enable or disable searching of data model accelerations containing fields that do not match the current data model configuration.
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 input credentials in Splunk Enterprise Security

The Credential Management page displays stored credentials for objects, such as threat lists or lookups, that run as scripted or modular inputs. An input configuration that references a credential will attempt to find the credential values here.

Add a new credential for an input

1. On the Enterprise Security menu bar, select **Configure > General** and open **Credential Management**.
2. Click **New Credential** to add a new user credential.

3. Use the edit panel to add the username and password for the new credential.
4. (Optional) Use the **Realm** field to differentiate between multiple credentials that have the same username.
5. Select the Application for the credential.
6. Click **Save**.

Edit an existing input credential

1. On the Enterprise Security menu bar, select **Configure > General** and open **Credential Management**.
2. In the **Action** column of a credential, select **Edit**.
3. Use the editor to change the username, password, or application for the credential. You cannot change the realm after it has been applied to a credential. You must create a new credential to change the realm.
4. Click **Save**.

Delete an existing input credential

1. On the Enterprise Security menu bar, select **Configure > General** and open **Credential Management**.
2. In the **Action** column of a credential, select **Delete**.

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*.

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 or link when you or another user opens Splunk Enterprise Security, set a default view.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Locate the view or link 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.

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 encoding the `&` separating the parameters as `&amp;`. 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&amp;form.owner_fo`

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.selected_urgency=critica`
`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.status_form=0`
`form.owner_form`	Display notable events owned by the user specified by this parameter.	usernames	`form.owner_form=admin`
`form.source`	Display notable events created by the correlation search specified by this parameter. HTML-encode	Endpoint - Host With Multiple Infections - Rule	`form.source=Endpoint%20-%20Ho`

	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.		
`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.rule_name=Host%20With%2`
`form.tag`	Displays notable events with the tag specified by this paramter.	malware, any custom tag value	`form.tag=malware`
`form.srch`	Displays notable events that match the SPL specified in this parameter. HTML-encode special characters	dest=127.0.0.1	`form.srch=dest%3D127.0.0.1`

	such as = for key-value pairs.		
form.security_domain_form	Displays notable events in the security domain specified by this parameter.	access, endpoint, network, threat, identity, audit	form.security_domain_form=enc
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	earliest=-24h%40h&latest=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.new_urgency_count_form=
form.selected_urgency	Displays notable events that have the urgency specified by this parameter. Use multiple instances of this parameter to select multiple	critical, high, medium, low, informational	form.selected_urgency=critica

	urgency settings.		

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 editor to add the item to your blacklist of known threats.

- If you determine that an event is not a threat, you can add it to your whitelist to remove it from the dashboard view.

Note: 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.

Whitelist events

After you determine that an event is not a threat, you can whitelist the event to hide it from the dashboard view. The summary statistics will continue to calculate whitelisted items, but they will not be displayed in the dashboard.

Whitelist an event

Use the Per-panel Filter to whitelist, or filter, events on a dashboard.

For example, to whitelist 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.

Note: Filtered events are not removed from the calculations for this dashboard, only removed from view.

In this example, after an item is added to the whitelist, it is considered good (not a threat) and will no longer show up on the **Traffic Size Analysis** dashboard.

Remove an item from the whitelist

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 whitelisted item.
4. Click **Save**.

Blacklist events

An event can also be blacklisted. Blacklisting 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.

Blacklisting an event or string is similar to whitelisting. Events can only be blacklisted after they have been filtered from the dashboard.

To blacklist a traffic event on, for example, the **Traffic Size Analysis** dashboard, do the following:

1. From the Advanced Filter page, click **View/edit lookup files** to see the list of entries currently being filtered.
2. Locate the entry you want to add to the blacklist. 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, navigate to **Configure > Data Enrichment > Lists and Lookups**. Lists with a description indicating that they are a dashboard filter will show the current per-panel filters for that dashboard. Events added to the whitelist for a dashboard will be listed here.

For example, the **Threat Activity Filter** list displays the filters for the **Threat Activity** dashboard.

Edit the per-panel filter list.

1. Open the filter list for the relevant dashboard. The name of the filter, for example `ppf_threat_activity`, is shown 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 whitelist.
4. To "blacklist" an item, use the editor to add a new row to the table and use "blacklist" in the "filter" column.
5. Click **Save** when you are finished.

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.

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

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	Authentication	Authentication.app, .src, .user_bunit
	Concurrent Application Accesses		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	First Time	None. Calls access_tracker lookup	

Tracker	Access - Last 7 days		
	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 Analysis	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
		Incident Management	

Data Protection	Data Integrity Control By Index		
	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
	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
	Panel Title		**Data Model Dataset**

Dashboard Name		Data Model	
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 Analysis	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	Application State	All_Application_State.Processes.cpu_load_percent, .mem_used, .process, All_Application_State.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		
	Identities By Category		
	Identity Information		
Identity Investigator	Identity Investigator	Based on swim lane selection	
Incident Review Audit	Review Activity By Reviewer	None. Calls a search over the es_notable_events KVStore 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 KVStore 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 KVStore collection.	
	Investigation timelines	None. Calls a search over the investigation_event KVStore collection.	
	Investigation attachments	None. Calls a search over the investigation_attachment KVStore collection.	
	Action history	None. Calls a search over the action_history KVStore collection.	

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		
	Oldest Infections		
	Repeat Infections	Malware	Malware_Attacks.action, .signature, .dest
Malware Search			Malware_Attacks.action, .file_name, .user, .signature, .dest
Modular Action Center	Action Invocations Over Time By Name	Splunk Audit Logs	Modular_Actions.Modular_Action_Invocations, .action_name
	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 Analysis	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
	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	Application State	All_Application_State.Services
	Ports By System Count		All_Application_State.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	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	Application State	All_Application_State.Services.start_mode, .Services.status, .dest_should_timesync, .tag, .dest
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	Application State	All_Application_State.Services.start_mode, .Services.status, .Services.service, .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
	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

These 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, see the Content Profile dashboard. See Content Profile.

Dashboard name	Security Domain	Part of Add-on
Access Anomalies	Access	DA-ESS-AccessProtection
Access Center	Access	DA-ESS-AccessProtection
Access Search	Access	DA-ESS-AccessProtection
Access Tracker	Access	DA-ESS-AccessProtection
Account Management	Access	DA-ESS-AccessProtection
Asset Center	Asset	SA-IdentityManagement
Asset Investigator	Asset	SA-IdentityManagement
Content Profile	Audit	SplunkEnterpriseSecuritySuite
Data Model Audit	Audit	Splunk_SA_CIM

Default Account Activity	Access	DA-ESS-AccessProtection
DNS Activity	Network	DA-ESS-NetworkProtection
DNS Search	Network	DA-ESS-NetworkProtection
Email Activity	Network	DA-ESS-NetworkProtection
Email Search	Network	DA-ESS-NetworkProtection
Endpoint Changes	Endpoint	DA-ESS-EndpointProtection
Forwarder Audit	Audit	SA-AuditAndDataProtection
HTTP Category Analysis	Network	DA-ESS-NetworkProtection
HTTP User Agent Analysis	Network	DA-ESS-NetworkProtection
Identity Center	Identity	SA-IdentityManagement
Identity_investigator	Identity	SA-IdentityManagement
Incident Review	Threat	SA-ThreatIntelligence
Incident Review Audit	Threat	SA-ThreatIntelligence
Indexing Audit	Audit	SA-AuditAndDataProtection
Intrusion Center	Network	DA-ESS-NetworkProtection
Intrusion Search	Network	DA-ESS-NetworkProtection
Malware Center	Endpoint	DA-ESS-EndpointProtection
Malware Operations	Endpoint	DA-ESS-EndpointProtection
Malware Search	Endpoint	DA-ESS-EndpointProtection
Network Changes	Network	DA-ESS-NetworkProtection
New Domain Analysis	Network	DA-ESS-NetworkProtection
Per-Panel Filter Audit	Audit	SA-Utils
Port & Protocol Tracker	Network	DA-ESS-NetworkProtection
Predictive Analytics		Splunk_SA_CIM
Protocol Center	Network	DA-ESS-NetworkProtection

REST Audit	Audit	SA-Utils
Risk Analysis	Threat	SA-ThreatIntelligence
Search Audit	Audit	SA-AuditAndDataProtection
Security Posture		SplunkEnterpriseSecuritySuite
Session Center	Identity	SA-IdentityManagement
SSL Activity	Network	DA-ESS-NetworkProtection
SSL Search	Network	DA-ESS-NetworkProtection
Suppression Audit	Threat	SA-ThreatIntelligence
System Center	Endpoint	DA-ESS-EndpointProtection
Threat Activity	Threat	DA-ESS-ThreatIntelligence
Threat Artifacts	Threat	DA-ESS-ThreatIntelligence
Threat Intelligence Audit	Audit	DA-ESS-ThreatIntelligence
Time Center	Endpoint	DA-ESS-EndpointProtection
Traffic Center	Network	DA-ESS-NetworkProtection
Traffic Search	Network	DA-ESS-NetworkProtection
Traffic Size Analysis	Network	DA-ESS-NetworkProtection
Update Center	Endpoint	DA-ESS-EndpointProtection
Update Search	Endpoint	DA-ESS-EndpointProtection
URL Length Analysis	Network	DA-ESS-NetworkProtection
User Activity	Identity	DA-ESS-IdentityManagement
View Audit	Audit	SplunkEnterpriseSecuritySuite
Vulnerability Center	Network	DA-ESS-NetworkProtection
Vulnerability Operations	Network	DA-ESS-NetworkProtection
Vulnerability Search	Network	DA-ESS-NetworkProtection
Web Center	Network	DA-ESS-NetworkProtection
Web Search	Network	DA-ESS-NetworkProtection

Extreme Search

How Splunk Enterprise Security uses extreme search

Extreme search enhances the Splunk platform search language with a set of commands. For a list of extreme search commands, see Extreme search commands.

As implemented in Splunk Enterprise Security, you can use the extreme search commands to:

- Build dynamic thresholds based on event data.
- Provide context awareness by replacing event counts with natural language.

For example, in the Enterprise Security Malware Center dashboard, the Key Security Indicator Total Infections displays the total number of systems with malware infections over the last 48 hours.

Splunk ES determines the displayed rate of change by comparing the current count of infections against the count of infected systems from the day before. There is no automatic determination of a normal daily range for infected systems in your environment. The threshold is entirely user-configured. Infections have increased by three, but the value has no context to indicate whether it is a notable increase.

The same indicator using extreme search displays the relevant information, but includes a depth of information that was not available with the default Total Infections indicator.

Using extreme search, Splunk ES calculates the infection count and rate of new infections using a dynamically-updating model. The key security indicator uses contextual and easy-to-understand language. In this case, you know that the total malware infection count is not higher than it would be any other day, and the rate of change in infections is not alarming.

The use of context and concept in extreme search

The core ideas of **context** and **concept** are critical to the understanding of extreme search. These ideas are responsible for the data model used for dynamic thresholds by an extreme search command.

1. **Context**: A context defines a relationship to a field or data in numerical terms. The data to be modeled must be represented by numerical values as the result of a search. Example contexts include total network throughput over the last 24 hours or network latency over the last 24 hours.
2. **Concept**: A term that applies to data, representing a qualitative rather than quantitative description. Example concepts include the terms "extreme," "high," "medium," "low," and "minimal".

By combining context and concept, extreme search adds meaning and value to the data.

- The total network throughput over the last 24 hours was Extreme, high, medium, low, or minimal.
- The network latency over the last 24 hours was extreme, high, medium, low, or minimal.

The concept terms describe network activity in both examples, but have different meanings based on the context they are applied to. If your environment reports that total network throughput is minimal, it is a warning. If the environment reports that network latency is minimal, the network is operating normally.

Data models and extreme search

After you choose a context and concept to represent your data, Splunk ES creates a data model. Using the extreme search commands, the data model maps the context and event statistics by concept. Extreme search commands refer to this combined model as a context.

Saved searches update contexts, such as the dynamic threshold context. The saved search searches event data for statistics to update the context. For a list of the saved searches that update contexts, see Containers, contexts, and saved searches in this topic.

Configuring extreme search for Enterprise Security

The use of extreme search commands in Enterprise Security requires no additional configuration. The default installation of ES provides all contexts used by the extreme search commands and enables the saved searches that maintain them.

- For a list of the contexts and saved searches implemented in Enterprise Security, see Containers, contexts, and saved searches in this topic.
- For a list of the key security indicators that use extreme search, see Extreme search key security indicators in this topic.
- For a list of the correlation searches that use extreme search, see Correlation searches that use extreme search in this topic. All correlation searches are disabled by default.

Correlation searches that use extreme search

All correlation searches in Enterprise Security are disabled by default. See Enable correlation searches in this manual.

Guided Search Creation is not available for correlation searches that use extreme search commands. These correlation searches use extreme search.

Search Name	Context
Brute Force Access Behavior Detected	failures_by_src_count_1h
Brute Force Access Behavior Detected Over One Day	failures_by_src_count_1d
Abnormally High Number of Endpoint Changes By User	change_count_by_user_by_change_type_1d
Host Sending Excessive Email	recipients_by_src_1h
Substantial Increase in Events	count_by_signature_1h
Substantial Increase in Port Activity	count_by_dest_port_1d
Unusual Volume of Network Activity	count_30m

Abnormally High Number of HTTP Method Events By Src	count_by_http_method_by_src_1d

Extreme search key security indicators

You can easily identify the key indicators that use extreme search by their use of semantic language instead of numerical values. The key security indicators on each dashboard are enabled by default.

Search Name	Contexts
Access - Total Access Attempts	authentication: count_1d, percentile
Malware - Total Infection Count	malware: count_1d, percentile
Risk - Median Risk Score	median_object_risk_by_object_type_1d, percentile
Risk - Median Risk Score By System	median_object_risk_by_object_type_1d, percentile
Risk - Median Risk Score By User	median_object_risk_by_object_type_1d, percentile
Risk - Median Risk Score By Other	median_object_risk_by_object_type_1d, percentile
Risk - Aggregated Risk	total_risk_by_object_type_1d, percentile
Risk - Aggregated System Risk	total_risk_by_object_type_1d, percentile
Risk - Aggregated User Risk	total_risk_by_object_type_1d, percentile
Risk - Aggregated Other Risk	total_risk_by_object_type_1d, percentile

Containers, contexts, and saved searches

Enterprise Security stores contexts in objects called containers. A container is both an object in the file system and a logical configuration used to classify contexts. In Enterprise Security, the containers are files with the `.context` extension. A container can contain multiple contexts. You can view the saved searches that generate contexts on the Content Management view in Enterprise Security. See Create and manage saved searches in Splunk Enterprise Security for more information.

Note: Enterprise Security enables the dynamic context saved searches by default.

Container name	Context name	App location	s
authentication	failures_by_src_count_1h	SA-AccessProtection	Ac Au Fa So Co
	failures_by_src_count_1d		Ac Au Fa So Da Ge
	count_1d		Ac Au Vo Da Ge
change_analysis	change_count_by_user_by_change_type_1d	SA-EndpointProtection	Ch Ch By Ch Pe Co
email	destinations_by_src_1h	SA-EndpointProtection	En En De Co Co
	recipients_by_src_1h		En En So Co
malware	count_1d	SA-NetworkProtection	En Ma Co Co
ids_attacks	count_by_signature_1h	SA-NetworkProtection	

			Ne Ev By Pe Co
network_traffic	count_by_dest_port_1d	SA-NetworkProtection	Ne Ac De Po Ge
	src_count_30m		Ne Tr Co 30 Ge
	count_30m		Ne Tr Pe Co
web	count_by_http_method_by_src_1d	SA-NetworkProtection	W Ev By HT Pe Co
risk	median_object_risk_by_object_type_1d	SA-ThreatIntelligence	Ri Ol Pe Co
	total_risk_by_object_type_1d		Ri Ri Ol Pe Co
default	percentile	SA-Utils	ES Pe Co
default	height	Splunk_SA_ExtremeSearch	No
	trendchange		No

	compatibility		No

Extreme search example in Splunk Enterprise Security

You can convert existing correlation searches to use extreme search commands. You do not need to make any configuration changes or modifications to use searches converted to use extreme search commands. For a list of extreme search commands, see Extreme search commands.

This example demonstrates how to convert the existing "Brute Force Access Behavior Detected" correlation search to use extreme search commands.

This example is for illustration purposes only. The "Brute Force Access Behavior Detected" correlation search included in Splunk Enterprise Security has already been converted to use extreme search commands.

The Brute Force Access Behavior Detected search

The correlation search "Brute Force Access Behavior Detected" searches for an excessive number of failed login attempts, followed by a successful attempt. The base search finds relevant events, counts the events by type "failure" and looks for a trailing "success" event for every host authentication over the last hour. If the identified events meet a threshold, the search triggers an alert action to create a notable event or other alert types.

"Brute Force Access Behavior Detected" correlation search without extreme search commands:

```
| `datamodel("Authentication","Authentication")` | stats
values(Authentication.tag) as
tag,count(eval('Authentication.action'=="failure")) as
failure,count(eval('Authentication.action'=="success")) as success by
Authentication.src | `drop_dm_object_name("Authentication")` | search
failure>6 success>0 | `settags("access")`
```

Without extreme search commands, the search defines a static threshold for the "success" events with the string `| search failure>6`. The Enterprise Security administrator has to select a threshold value, or accept the default value. If the administrator sets the threshold too low, the search creates a storm of notable events. If they set the threshold too high, the search could miss notable events, creating a potential blind spot to a security threat.

A search that implements extreme search removes the static value and uses, in this example, the authentication data ingested by Splunk Enterprise to determine a notable level of authentication failures in your environment.

1. Examine the data

To use extreme search, you must build a data model for the commands to rely on. To build the data model, you must understand what the data represents and what question you are trying to answer.

In this example, the "Brute Force Access Behavior Detected" correlation search, you know that the count of authentication failures will not go below zero, and may range much higher. A scale of magnitude represents the authentication values being searched.

2. Choose a context

You can choose one of three types of contexts, each requiring three data points.

- Mean average: requires a mean value, a standard deviation, and a total count of events.
- Median average: requires a median value, a standard deviation, and a total count of events.
- Domain: requires a minimum, a maximum, and a total count of events.

In this example, the count of authentication events does not include a negative value and is progressive, so a domain is the best fit for the authentication data.

3. Choose a concept

A concept represents a qualitative description of the data. Splunk Enterprise Security includes predefined concepts for interpreting change, direction, and magnitude as a qualitative value. Concepts are differentiated by the terms used.

- Change uses the terms: "minimally, slightly, moderately, greatly, extremely."
- Direction uses the terms: "decreasing, unchanged, increasing"
- Magnitude uses the terms: "minimal, low, medium, high, extreme"

In this case, the magnitude concept best represents the behavior of authentication failures.

4. Create the context

As described in How Splunk Enterprise Security uses extreme search in this manual, a context has both a name and a container, with the container residing in an app. The "Brute Force Access Behavior Detected" search runs against authentication events, so the context container is called "authentication." The "authentication" container is located in the "SA-AccessProtection" app along with the authentication searches and other objects.

ES includes a pre-initialized authentication context. This context will not represent your environment unless a saved search updates it with events. Splunk Enterprise Security contains this context so that updates will carry a greater weight than the values used during the creation of the context. The domain for this authentication context is defined with a min=0, max=10, and count=0.

For the "Brute Force Access Behavior Detected" search, the context name is chosen to facilitate quick identification: `failures_by_src_count_1h`.

Create the initial context using example data.

```
| xsCreateUDContext app="SA-AccessProtection"
name=failures_by_src_count_1h container=authentication scope=app
terms=`xs_default_magnitude_concepts` min=0 max=10 count=0 type=domain
```

This context is a user-defined context because you are specifying the data in the search to make sure that the context works. In the final search, the context is data-defined because it relies on data from the search results of the earlier search.

Display the context, once created:

```
| xsdisplaycontext failures_by_src_count_1h in authentication
```

Before implementing extreme search, the static threshold for authentication failures was six. Using the context `failures_by_src_count_1h`, a count of six is modeled at the end of the term "medium". The model will change after the updated "Brute Force Access Behavior Detected" search searches the authentication data and the saved search that updates the `failures_by_src_count_1h` runs.

List the terms used in a context:

```
| xslistconcepts failures_by_src_count_1h in authentication
```

5. Apply the context in the search

You can use the search command `xsWhere` to evaluate a data value against a context. This correlation search uses `xsWhere` to compare the count of authentication failures against the context `failures_by_src_count_1h` to determine if the count represents a value above "medium."

In this example, a concept of medium represents the range of values that change after the context is updated with data. A saved search updates the context. If the count of events identified by the saved search is greater than medium, the correlation search using extreme search will trigger an alert action and create a notable event.

"Brute Force Access Behavior Detected" with extreme search capabilities

```
| `datamodel("Authentication","Authentication")` | stats
values(Authentication.tag) as
tag,count(eval('Authentication.action'=="failure")) as
failure,count(eval('Authentication.action'=="success")) as success by
Authentication.src | `drop_dm_object_name("Authentication")` | search
success>0 | xswhere failure from failures_by_src_count_1h in
authentication is above medium | `settags("access")`
```

6. Update the context

A search threshold can be dynamic because it uses a saved search to update a context. The saved searches included with ES that generate context information for extreme search end with "Context Gen" to provide easy identification.

The domain context used by the "Brute Force Access Behavior" correlation search requires values for minimum, maximum, and count. Those values are drawn from the authentication data model. The "Access - Authentication Failures By Source - Context Gen" saved search that generates the `failures_by_src_count_1h` context for the "Brute Force Access Behavior" correlation search.

For the `failures_by_src_count_1h` context, the results of the context generating search change the maximum value to a multiple of the median to prevent outliers from skewing the underlying context and potentially introducing oversights.

"Access - Authentication Failures By Source - Context Gen" saved search

```
| tstats `summariesonly` count as failures from
datamodel=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
```

This search updates the `failures_by_src_count_1h` context with `xsUpdateDDContext`. In this case, the data from the search is added to the context, creating a historical trend that informs the context. This is different from the context search in step 4 that used `xsUpdateUDContext`, because the first part of the search supplies the data used by the context, rather than being supplied by the user.

Both the correlation search and the saved search "Access - Authentication Failures By Source - Context Gen" are scheduled to run hourly by default.

7. Use hedges to modify the results

Hedges are semantic terms that modify the range represented by a concept. Use a hedge to limit, shrink, or modify the shape of the curve that a concept term uses to model the data. The hedges "above" and "below" are useful for alerting searches as they redefine the range of values that will match.

The "Brute Force Access Behavior Detected" correlation search using extreme search applies a hedge so an alert action triggers only when the count of failures is "above medium."

Examples of a concept with various hedges applied:

Hedge example	Image
| xsDisplayConcept medium from failures_by_src_count_1h in authentication	
| xsDisplayConcept very medium from failures_by_src_count_1h in authentication	

| xsDisplayConcept above medium from failures_by_src_count_1h in authentication	
| xsDisplayConcept below medium from failures_by_src_count_1h in authentication	
| xsDisplayConcept around medium from failures_by_src_count_1h in authentication	

The `synonyms.csv` lookup file in the Splunk_SA_ExtremeSearch app contains the extreme search hedges.

Summary

The "Brute Force Access Behavior Detected" correlation search using extreme search is included with Splunk Enterprise Security. The context generation search runs and updates the context on a recurring interval. The correlation search references the context, and the concept within the context sets the threshold. The concept is hedged to "above medium" so that the correlation search will only create a notable event when the count of failed authentications followed by a successful authentication is "high" or "extreme."

In plain language, extreme search transformed the "Brute Force Access Behavior Detected" correlation search from "find all authentication attempts where X count of failed authentications are followed by a successful authentication" to "find all authentication attempts where a high or extreme number of failed authentications are followed by a successful authentication."

Extreme search commands

Search command	Description
xsWhere	Used to match a concept within a specified context, and determine compatibility.
xsFindBestConcept	Used when evaluating a search count and comparing the count to a context. The closest match returns the term used by the concept. The key security indicators use this command.
xsUpdateDDContext	Used to update a data-defined context. A scheduled report that calls "xsUpdateDDContext" builds a context that represents a historical view. `|xsUpdateDDContext in app=<app> name=<context> container=<container> scope=app`

xsListContexts	Used to list all contexts in a container | `xsListContexts in <container>`
xsListConcepts	Used to list all concepts in a context | `xsListConcepts from <context> in <container>`
xsDisplayContext	Used to display the range of values in a context, including the terms used in the concept: | `xsDisplayContext <context> IN <container>`
xsDisplayConcept	Used to display the range of values used for a concept: | `xsDisplayConcept <concept> from <context> in <container>` | `xsDisplayConcept <hedge> <concept> from <context> in <container>`