Splunk® SOAR (On-premises)
Use Splunk SOAR (On-premises) 5.4.0

Generated: 10/28/2022 7:46 am

Table of Contents

Introduction.....1

About Splunk SOAR (On-premises).....1
Who should read this manual?.....3
Access Account Settings.....3

Get started using Splunk SOAR (On-premises).....5

Start with Investigation in Splunk SOAR (On-premises).....5
Manage the status, severity, and resolution of events in Splunk SOAR (On-premises).....6
Approve actions before they run in Splunk SOAR (On-premises).....7
Mark files and events as evidence in Splunk SOAR (On-premises).....9
View recommendations for mission experts, playbooks, and actions.....10
View and create notes in Splunk SOAR (On-premises).....11
Search within Splunk SOAR (On-premises).....11
View the list of configured playbooks in Splunk SOAR (On-premises).....12
Create Executive Summary reports and view all reports in Splunk SOAR (On-premises).....14
Create custom lists for use in Splunk SOAR (On-premises) playbooks.....15

Manage cases in Splunk SOAR (On-premises).....17

Overview of containers.....17
Overview of cases.....18
Create cases in Splunk SOAR (On-premises).....18
Add objects to a case in Splunk SOAR (On-premises).....19
Define a workflow in a case using workbooks in Splunk SOAR (On-premises).....20
Create case reports to download and share in Splunk SOAR (On-premises).....22

Use Splunk SOAR (On-premises) in a Connected Experiences App.....23

Use the Splunk Mobile app for Splunk SOAR (On-premises).....23
Run Splunk SOAR (On-premises) playbooks in Splunk AR workspaces.....24

Use Splunk SOAR (On-premises) with IT Service Intelligence.....25

Send IT Service Intelligence episodes to Splunk SOAR (On-premises).....25

Use the command line interface to perform tasks in Splunk SOAR (On-premises).....26

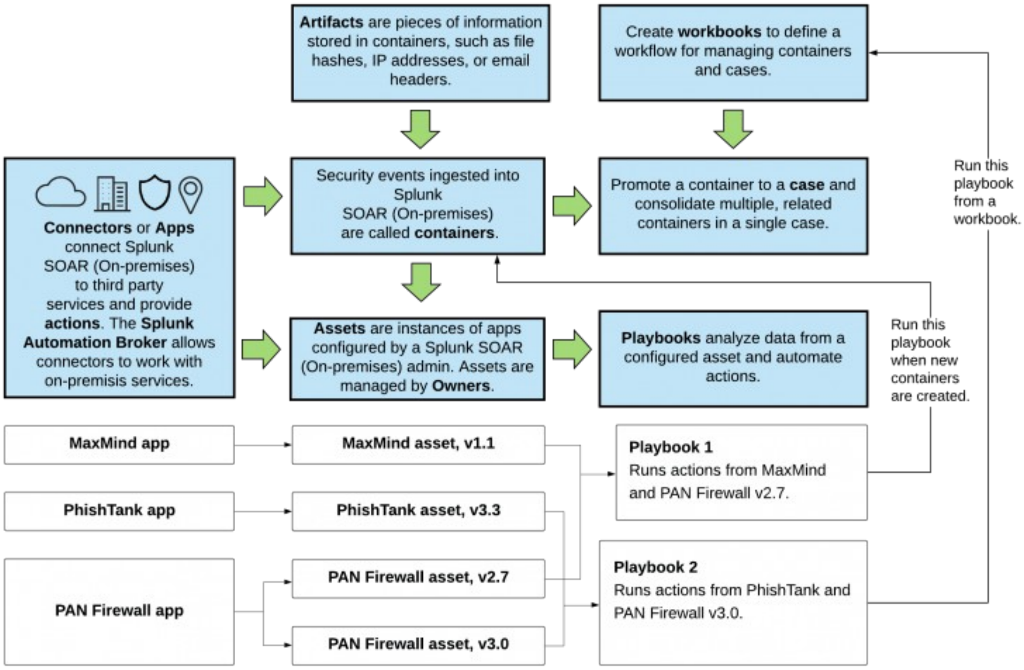
Splunk SOAR (On-premises) command-line interface overview.....26
Run an action in Splunk SOAR (On-premises).....28
Run a playbook in Splunk SOAR (On-premises).....29
Add a note in Splunk SOAR (On-premises).....30
Update or edit an event in Splunk SOAR (On-premises).....30
Use a datapath in Splunk SOAR (On-premises).....31

Introduction

About Splunk SOAR (On-premises)

Splunk SOAR (On-premises) is a Security Orchestration, Automation, and Response (SOAR) system. The Splunk SOAR (On-premises) platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.

This diagram shows the end-to-end flow of security automation in Splunk SOAR (On-premises). See the table immediately following the diagram for more information about each Splunk SOAR (On-premises) component in the diagram.



Artifacts are pieces of information stored in containers, such as file hashes, IP addresses, or email headers.
Create workbooks to define a workflow for managing containers and cases.
Connectors or Apps connect Splunk SOAR (On-premises) to third party services and provide actions. The Splunk Automation Broker allows connectors to work with on-premisis services.
Security events ingested into Splunk SOAR (On-premises) are called containers.
Promote a container to a case and consolidate multiple, related containers in a single case.
Run this playbook from a workbook.
Assets are instances of apps configured by a Splunk SOAR (On-premises) admin. Assets are managed by Owners.
Playbooks analyze data from a configured asset and automate actions.
Run this playbook when new containers are created.
MaxMind app
MaxMind asset, v1.1
Playbook 1
Runs actions from MaxMind and PAN Firewall v2.7.
PhishTank app
PhishTank asset, v3.3
PAN Firewall app
PAN Firewall asset, v2.7
Playbook 2
Runs actions from PhishTank and PAN Firewall v3.0.
PAN Firewall asset, v3.0

Component	Description
App	Adds connectivity to third-party security technologies. The connections allow Splunk SOAR (On-premises) to access and run actions that are provided by the third-party technologies. Some apps also provide a visual component such as widgets that can be used to render data produced by the app. The diagram shows three apps in a Splunk SOAR (On-premises) environment: • The MaxMind app provides an action to find the geographical location of an IP address. • The PhishTank app provides an action to find the reputation of a URL. • The Palo Alto Networks (PAN) Firewall app provides several actions, such as blocking and unblocking access to IP addresses, applications, and URLs. See Add and configure apps and assets to provide actions in Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.
Asset	A specific instance of an app. Each asset represents a physical or virtual device within your organization such as a server, endpoint, router, or firewall. For example, you might have a Palo Alto Network (PAN) firewall app that connects the firewall to Splunk SOAR (On-premises). You can configure an asset with the specific connection details for this firewall. If your environment has multiple firewalls, you can configure one asset for each firewall. The diagram shows one MaxMind asset, one PhishTank asset, and two PAN firewall assets. The PAN assets have different version numbers, which is the reason for having two assets. See Add and configure apps and assets to provide actions in Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.
Container	A security event that is ingested into Splunk SOAR (On-premises). Containers have the default label of Events. Labels are used to group related containers together. For example, containers from the same asset can all have the same label. You can then run a playbook against all containers with the same label. You can create custom labels in Splunk SOAR (On-premises) as needed. See Configure labels to apply to containers in the *Administer Splunk SOAR (On-premises)* manual.
Case	A special kind of container that can hold other containers. For example, if you have several closely related containers for a security incident, you can promote one of those containers to a case and then add the other related containers to the case. Doing this lets you consolidate your investigation rather than having to investigate each container individually. See Overview of cases.
Artifact	A piece of information added to a container, such as a file hash, IP address, or email header.
Indicator or Indicator of Compromise (IOC)	A piece of data such as an IP address, host name, or file hash that populates the Common Event Format (CEF) fields in an artifact. Indicators are the smallest unit of data that can be acted upon in Splunk SOAR (On-premises).
Playbook	Defines a series of automation tasks that act on new data entering Splunk SOAR (On-premises). For example, you can configure a playbook to run actions against all new containers with a specific label. Or you can configure running a playbook as part of the workflow in a workbook. In the diagram, two playbooks are configured:

Component	Description
	- Playbook 1 runs actions from the MaxMind and PAN Firewall version 2.7 assets whenever a new container is created in Splunk SOAR (On-premises). - Playbook 2 runs actions from the PhishTank and PAN Firewall version 3.0 assets whenever a specific workbook is used in a case. See Use playbooks to automate analyst workflows in Splunk SOAR (On-premises) in the *Build Playbooks with the Playbook Editor* manual.
Workbook	A template providing a list of standard tasks that analysts can follow when evaluating containers or cases. See Define a workflow in a case using workbooks in Splunk SOAR (On-premises).
Action	A high level primitive used throughout the Splunk SOAR (On-premises) platform, such as get process dump, block ip, suspend vm, or terminate process. Actions are run in playbooks or manually from the Splunk SOAR (On-premises) web interface. Actions are made available to Splunk SOAR (On-premises) by apps. See Add and configure apps and assets to provide actions in Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.
Owner	The person responsible for managing assets in your organization. Owners receive approvals, which are requests to run a particular action on an asset. Approvals are sent to the asset owners and contain a service level agreement (SLA) dictating the expected response time. SLAs can be set on events, phases, and tasks. - See Configure approval settings for a Splunk SOAR (On-premises) asset in the *Administer Splunk SOAR (On-premises)* manual. - See Configure the response times for service level agreements in the *Administer Splunk SOAR (On-premises)* manual for more information about configuring SLAs.

Who should read this manual?

This manual is intended for Security Operations Center (SOC) staff, analysts, and managers who are not primarily Splunk SOAR (On-premises) administrators.

Access Account Settings

Click your account name and select **Account Settings** to access your account settings.

The default admin account on a Splunk SOAR (On-premises) instance is a local account. Local accounts only exist in the database for the Splunk SOAR (On-premises) web interface and can't be used to log into the operating system or any external authentication server.

Each account must have at least one email address associated with it. Splunk SOAR (On-premises) uses this email address as part of the approval process workflow.

Splunk SOAR (On-premises) also supports single sign-on authentication from various identity providers. For more information, see Configuring single sign-on authentication for Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.

Account Settings

You can configure various settings through the account settings page. Use this page to configure user settings, notifications, and change your password.

User Settings

For a local account, the primary email is the username you log in with. You can change it at any time, but you must use the new email address the next time you log in. Your current login session continues until you log out, your session expires, or you switch browsers or machines.

Get started using Splunk SOAR (On-premises)

Start with Investigation in Splunk SOAR (On-premises)

Use the Splunk SOAR (On-premises) Investigation page as the starting point to understand, investigate, and act on events. Investigation provides you access to event activity history, contextual and interactive data views, secure file attachments, and automation and case management controls.

The activity feed displays current and historical action and playbook activity that has acted on the currently displayed event. It provides a summary of the success, ongoing execution, and results of all automation operations for the event. The activity feed also provides team collaboration capabilities that are integrated inline with automation details and other data, forming a record of all relevant event information.

You can use Splunk SOAR (On-premises) to promote a verified event to a case using the integrated case management capability. Case management supports tasks that map to your defined Standard Operating Procedures (SOPs). Case management also has full access to the Splunk SOAR (On-premises) Automation Engine, allowing you to launch actions and playbooks as part of a task.

Set your view in Investigation

Analyst and summary views enable different personas to quickly view information and perform actions. Toggle quickly between the summary and analyst views by clicking the **Summary** or **Analyst** view buttons in an event or case.

- The **Summary** view presents mostly non-actionable information about an event or case. This information is useful for individuals such as managers or executives who want to be able to view the status of an event or case without having to view the actionable items.
- The **Analyst** view contains the same information as the summary view along with all options to perform actions on the event or case, such as run a playbook, add and edit a workbook, or view and add artifacts.

HUD cards

The collapsible heads up display (HUD) helps you track important metrics and information. Splunk SOAR (On-premises) administrators control HUD card settings. Users can customize the HUD for an event or case by adding or removing cards, or configuring manual cards of their own design.

The following HUD card types are available:

- Preset Metrics
- Custom Fields
- Manual

Preset Metrics and Custom Fields cards are defined by a Splunk SOAR (On-premises) administrator and display one of the built-in metrics or the information from a custom field. You can add or remove these cards, but only an administrator can change the card options. Manual cards let you add a customized card to the HUD for an event or case.

Add a card to the HUD

Perform the following steps to add a card to the HUD:

1. From the Splunk SOAR (On-premises) **Home** menu, select either **Cases** or **Sources** > **My Events**.
2. Select an event or case.
3. Expand the HUD menu by clicking the downward-facing double chevron icon ⏬.
4. Click the gear icon to open the Configure HUD modal.
5. Click **+ HUD Card**.
6. Choose a HUD card type.
7. Configure the available card options. The following table describes the manual card options:

Setting	Description
Type	**Text** creates an input field where you can add a small amount of text. **Select** creates a card with a dropdown list of options.
Message	The name of the HUD card.
Color	The display color of the HUD card.

8. Click **Save**.

Manage the status, severity, and resolution of events in Splunk SOAR (On-premises)

You can manage the status, severity, and resolution of events in Splunk SOAR (On-premises) in order to best organize events.

Use status to represent the state of an event

Each event or case has a status. Use the status to indicate the state of an event or case.

Statuses are grouped into three types: New, Open, and Closed. You can create up to 10 additional custom statuses in each category as required by your business processes.

The status of an event or case is set when it is created or ingested from an asset.

Perform the following steps to change the status of an event or case:

1. In Investigation, click the downward arrow stack icon next to the **Playbook** button.
2. In the expanded section at the top of the page, click **Event Info**.
3. Select a status from the menu in the Status field.

You can also set the status of a case or event using actions inside of a playbook. See Set container parameters in Splunk SOAR (On-premises) using the API block with the classic playbook editor in *Build Playbooks with the Playbook Editor*.

Use severity to represent the importance of an event

Severity defines the impact or importance of an event or case. Different severities have their own service level agreements (SLAs) assigned to them.

Splunk SOAR (On-premises) ships with three severity names: High, Medium, and Low. Your organization might need additional levels of severity to match your business processes. A Splunk SOAR (On-premises) administrator can define additional severity names.

The severity of a case or event is set when it is created or ingested. You can change the severity assigned to a case or event in Investigation by clicking on the severity label.

Each severity label has a corresponding SLA which is defined as the number of minutes that can pass before an action or approval is considered late. Each severity name can be configured with its own SLA.

This table lists the default SLA settings for High, Medium, and Low.

Severity name	SLA
High	60 minutes (1 hour)
Medium	720 minutes (12 hours)
Low	1440 (24 hours)

Use SLAs for the following purposes in Splunk SOAR (On-premises):

- Track the amount of time an event or case has remaining before it is considered due.
- Track the amount of time an approver has to approve an action before the approval is escalated to another approver.

If an approver does not approve an action before the SLA time elapses, the action is escalated to the next level of approvers.

For more information about the approval and escalation process see Approve actions before they run in Splunk SOAR (On-premises).

Close or resolve events and cases

When all the tasks or actions associated with a case or event are complete, you can close or resolve the case or event by setting the status to a Closed type. You can change the status in Investigation, using the REST API, or by automation in a playbook.

Change the status of an event or case by selecting the status from the menu in **Investigation** > **Event Info** > **Status**. Playbooks can also set the status of a case or event.

An administrator can specify which tags are required before an event or case before you can resolve it. Selecting a status with a Closed type with a missing required tag generates an error.

Approve actions before they run in Splunk SOAR (On-premises)

Take action on an asset to either make it do something or retrieve information from it. For example, you can create an action to use a firewall to block a particular IP address, request a list of VMs from a VMware ESXi server, or look up a file hash on VirusTotal.

Action approval is controlled at the asset level. You can assign an asset to one or more approvers. If someone takes action on that asset, all approvers must approve the action before it runs. If an asset has no approvers, or if the actions are read-only, all actions taken on it run immediately. A read-only action is an action that does not change anything on the device or application with which it is communicating. For example, a read-only action from a firewall obtains information from the firewall without doing anything to change the firewall.

Take action on assets

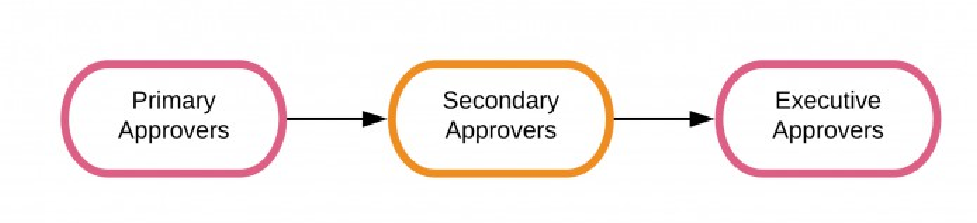
An asset doesn't need to have approvers. Approval is only required for actions that have a write component.

To start an action, perform the following steps:

1. From the **Home** menu, click **Sources**.
2. Select a label.
3. Select an event.
4. Click **Analyst** to make sure you are in analyst view.
5. Click **Action**.

For more information about how to assign approvers to assets, see Add and configure apps and assets to provide actions in Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.

The following diagram describes the approval escalation path in Splunk SOAR (On-premises):



Primary approvers

If an asset has primary approvers, the required number of approvers must approve the action within the action service level agreement (SLA) deadline. If any single primary approver denies the action, the action stops immediately and no further approvals are permitted.

Secondary approvers

If the minimum number of approvals by primary approvers isn't met within the SLA, but no one denied the action, it moves to secondary approvers and the action SLA clock starts over.

Executive approvers

If the action isn't approved or denied within the secondary SLA, it moves to the executive approvers. Executive approvers have the same amount of time to approve the action. If they fail to act on it, it expires and doesn't run.

Run actions using the Splunk SOAR (On-premises) API

You can also run actions using a call to the phantom.act API. See act in the *Python Playbook API Reference for Splunk SOAR (On-premises)* manual. The `reviewer` parameter is optional. If you specify this parameter, the action doesn't run until a reviewer approves or denies it. A reviewer is an analyst or member of the security operations team who reviews and decides if the action is allowed to run. After the reviewer approves the action, the approval process begins.

The first reviewer to approve or deny the action determines whether it runs or not. If the SLA expires before any reviewer approves it, the action fails.

Delegate actions to other users

When an approver receives a notification to approve an action, they can delegate the approval to one or more users or roles. Those users must approve or deny the action within the remaining SLA period or it moves to the next level of approval.

> If you delegate an action, you renounce your portion of the vote. All delegates must approve the action for it to count as a single vote from the original approver.

Delegation example

Users A, B, and C are primary approvers for an asset that requires two approvers. Users D and E are secondary approvers, and they all need to approve the action. Users F, G, H, and I also exist on the system. Someone takes an action on the asset and users A, B and C are notified.

If any two users approve the action within the SLA deadline, the action runs. Alternatively, user A might approve while user B delegates to users F and G. The action runs if users F and G both approve the action. While A approved directly, B effectively approved by being represented by F and G. The single-user veto still applies because users F or G can deny the action.

Alternatively, if users F or G don't approve but C does, the action runs because A and C make up the two approval votes needed.

A second level of delegation is allowed. When user B delegates to F and G, user F can then delegate to users H and I. The requirement that all delegates must approve still stands. To represent user B's original vote, G, H, and I must all approve. G has half a vote, and H and I each have a quarter of a vote.

Delegation restrictions

You can't delegate to other approvers that an action is currently waiting on. Primary approvers can delegate to secondary approvers, but not other primary approvers. You can delegate to primary approvers only once an action expires and moves to the secondary approvers.

Mark files and events as evidence in Splunk SOAR (On-premises)

When you discover information that's critical to your conclusions, you can mark it as evidence in your investigation. Evidence can include files, artifacts, action results, events, and notes. Tagging evidence helps to separate general information from information that's directly related to diagnosing an incident. All evidence appears on the **Evidence** tab within an investigation.

Mark a file as evidence

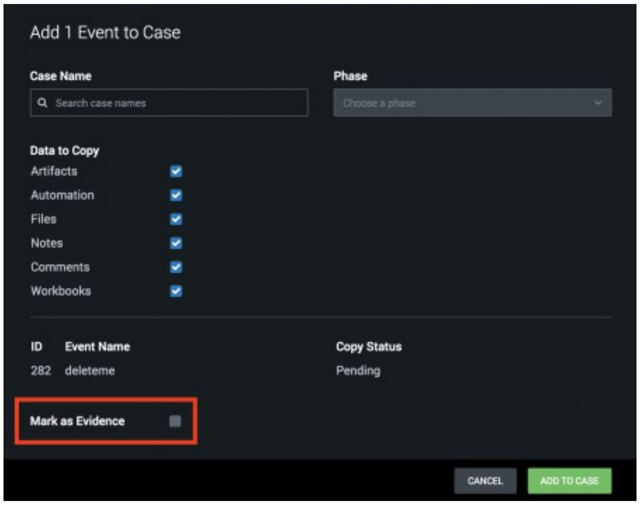
Perform the following steps to mark a file as evidence:

1. Navigate to a container in Splunk SOAR (On-premises).
2. Click **Analyst** to change the container to analyst view.
3. Click the **Files** tab.
4. Click the ⋯ more icon for the file.
5. Select **Mark as Evidence**.

6. Click **Confirm**.

Mark an event as evidence

To mark an event as evidence, select **Mark as Evidence** when adding the event to a case. For more information about adding events to cases, see Add objects to a case in Splunk SOAR (On-premises). The following screenshot illustrates how to mark an event as evidence.



Add 1 Event to Case

Case Name: Search case names

Phase: Choose a phase

Data to Copy

Artifacts	☑
Automation	☑
Files	☑
Notes	☑
Comments	☑
Workbooks	☑

ID	Event Name	Copy Status
282	deleteme	Pending

Mark as Evidence □

When you add an event to an existing case, it copies all the data from the existing event into the case you're adding it to while also maintaining the original event data. The information on the **Evidence** tab is a copy of the original event, not the actual event.

View recommendations for mission experts, playbooks, and actions

Use the **Guidance** tab to view recommended users, playbooks, and actions that can be used to resolve an event. The recommendations are provided by Splunk SOAR (On-premises) based on a variety of factors, including the following:

- Previous playbooks or actions run on a container, event, or case with the same label.
- The users working on that label.
- The frequency with which those previous entities were used. For example, a user that has frequently changed the state of all containers with the matching label would be considered an expert.
- How recently an entity has interacted with the event, case, or container. For example, a user is considered less of an expert as time goes on, assuming there is no activity from the user.

Perform the following tasks to view guidance information:

1. Navigate to a container or case in Splunk SOAR (On-premises).
2. Click **Analyst** to switch to Analyst view.
3. Click the **Guidance** tab.

The **Mission Experts** are the users who have taken action on containers, events, or cases with the same label. You can also view recommended **Playbooks** and **Actions** in their respective sections.

View and create notes in Splunk SOAR (On-premises)

You can create a note in Splunk SOAR (On-premises) when working with events, tasks, and cases. Use the **Notes** tab to view all of the notes, regardless of who created them.

Create a note

To create a note, follow these steps:

1. Navigate to an event, task, or case in Splunk SOAR (On-premises).
2. Click the **Notes** tab.
3. Enter a title and body text for your note.
4. (Optional) Add an attachment by clicking the paper clip icon. You can upload a new attachment of up to 20 MB. To upload a larger attachment, first upload it using the **Files** tab. You can then add the larger file to the note as an existing file using the paper clip icon.
5. (Optional) Click the image icon to add a new or existing image of up to 2 MB. Supported image file types include JPG, JPEG, PNG, GIF, BMP, and ICO. Images appear inline in the body of the note once the note is saved.
6. Click **Save**.

To edit, delete, or mark a note as evidence, click the ••• icon. Once your note is marked as evidence, it appears in the **Evidence** tab.

Filtering notes

You can filter notes by doing the following:

- In the **Show** field, select either **Task Notes**, **General Notes**, or **Artifact Notes** from the drop-down list. By default, all notes are displayed.
- In the **Sort** field, sort by the **Newest** or **Oldest** notes.

Using HTML and Markdown in notes

Splunk SOAR (On-premises) supports clickable links and inline images when notes are written in Markdown. Clickable links and inline images are not supported when notes are written in HTML.

Search within Splunk SOAR (On-premises)

Splunk SOAR (On-premises) includes an embedded copy of Splunk Enterprise for searching data in Splunk SOAR (On-premises).

You can also configure search using an external Splunk Enterprise instance, or distributed Splunk Enterprise deployment. For more information, see Configure search in Splunk SOAR (On-premises) in the *Administer Splunk SOAR (On-premises)* manual.

Searching in Splunk SOAR (On-premises)

There is a search box in the upper left of every Splunk SOAR (On-premises) screen. Most screens also have a section specific search box below the menu bar. Section specific search boxes display text indicating what it will search. For example, on the Indicators screen, the section specific search box contains "Search indicator values".

For non section specific searches, when you enter a search term, it appears as part of the URL in the address bar, so you can create a bookmark.

For example: `https://<Splunk SOAR URL>/search?query=events`

Search results can vary as changes in Splunk SOAR (On-premises) occur between visits to the search page.

Initial search results are returned without filters applied. The search results page has a row of checkboxes for the following predefined filters; **Containers**, **Artifacts**, **Actions**, **Assets**, **Apps**, or **Other** to narrow your search results. Click the checkbox next the the filter you want to apply.

Search results are displayed in groups of 10 results per page. Use the menu in the bottom center of the search results page to view a up to a maximum of 100 results per page.

The search directives in Splunk SOAR (On-premises) are limited to a subset of the Splunk Processing Language (**SPL**). If you're using an external Splunk Enterprise instance as your Splunk SOAR (On-premises) search engine, you can use all of the Splunk Enterprise features through the interface on that instance. For more information, see Understanding SPL syntax in the Splunk Enterprise *Search Reference* manual.

Available search operators in Splunk SOAR (On-premises) are:

- Boolean operators; AND, OR, and NOT. The NOT operator excludes an entire object from appearing in the search results, even if other terms within that object match.
- Parentheses to group terms into more complex boolean searches.
- Quotation marks to search for exact phrases.
- The wildcard character '*'.

Searching with multiple words creates an implied ALL condition. For example, the term `data path` returns results containing both `data` and `path`. Use `OR` to find results containing either `data` or `path`.

Search examples

Search for the exact phase "data path":

```
"data path"
```

Search for objects that contain both "data" and "path":

```
data AND path
```

Search for any objects that contain a match for "dat":

```
dat*
```

View the list of configured playbooks in Splunk SOAR (On-premises)

The playbooks list contains all your currently available Splunk SOAR (On-premises) playbooks and significant metadata about those playbooks. Use the playbooks list to sort, filter, and manage your playbooks.

To open the playbooks list, perform the following steps:

1. From the **Home** menu, select **Playbooks**.
2. Click the **Playbooks** tab if it's not already open.

3. (Optional) Use the search field to find specific playbooks. Searches are case-insensitive and partial-word matches are supported. This search does not support booleans, such as AND, NOT, or OR.

Use the buttons to reorder the playbooks on this page, configure source control, import playbooks, or create new playbooks:

> To help improve Splunk SOAR (On-premises), Splunk collects playbook names, playbook descriptions, and custom-function names in telemetry, so don't include any personally identifiable or sensitive information in playbook names, playbook descriptions, and custom-function names.

Button	Description
⇅	Set the order to run playbooks with a status of **Active**. • Playbooks with a status of **Inactive** are not run. When you change a playbook's status to **Inactive**, you are prompted to cancel the running playbook. • The next playbook in the list starts once the preceding playbook's `on_start()` function has completed. • If you want one playbook to depend on another playbook finishing completely before starting, use the `phantom.playbook()` function instead of the playbook list. See playbook in the *Python Playbook API Reference for Splunk SOAR (On-premises)*.
↻	Splunk SOAR (On-premises) stores playbooks in Git repositories. See Configure a source code repository for your playbooks in *Administer Splunk SOAR (On-premises)*. Click this button to open the **Update from Source Control** dialog. 1. Select a repository from the drop-down list in the **Source to update from** field. 2. Select either **Force Update** or **Preserve State** ♦ **Force Update** treats the remote repository as authoritative. Using this overwrites any local changes to playbooks. ♦ **Preserve State** retains the local metadata for changes to playbooks. Playbooks from the community repository always have a status of **Inactive**. If you have set the status of a community playbook to **Active** locally, updating from the community repository will set its status to **Inactive** unless you select **Preserve State**. 3. Click **Update**.
☰	Manage source control settings. See Configure a source code repository for your Splunk SOAR (On-premises) playbooks in *Administer Splunk SOAR (On-premises)*.
⇪	Import a playbook that was exported from another instance of Splunk SOAR (On-premises). 1. Click this button to import a playbook. 2. In the **Source to update** field, select a repository where you want to write the imported playbook. 3. (Optional) Click **Force Update** to overwrite existing versions of the same playbook. 4. Drag and drop a compressed playbook in `.tgz` format, or click and navigate to the playbook. 5. Click **Upload**.
+ PLAYBOOK	Open the Classic Playbook Editor to create a new playbook. See Create a new playbook in Splunk SOAR (On-premises) using the classic playbook editor in *Build Playbooks with the Playbook Editor*.

Click the vertical ellipsis (â ®) icon to toggle the display of the available columns in the playbook list. Items marked with a check mark (â) are displayed in the playbook list. When the space required to display the columns exceeds the width of the current window, a scroll bar appears at the bottom of the playbook list.

Edit, delete, export, or copy a playbook

Click the name of a playbook to open it in the Classic Playbook Editor. For more information, see Create a new playbook in Splunk SOAR (On-premises) using the classic playbook editor in *Build Playbooks with the Playbook Editor*.

Check the checkbox next to the playbook name to select one or more playbooks. After playbooks are selected, you can perform the following actions:

Button	Action
Edit	Set the properties of the selected playbooks, not the playbooks themselves. Set the status, logging mode, safe mode, which labels the playbook operates on, the category, and tags by selecting the property value you want from the drop-down list.
Delete	Delete the selected playbooks. A dialog box asks you to confirm your choice.
Export	Download the playbook as a .tgz extension archive. You can export only one playbook at a time.
Copy	Save the playbook to a repository that you have configured, such as Git. You can only copy one playbook at a time.

Create Executive Summary reports and view all reports in Splunk SOAR (On-premises)

View all reports created or generated in Splunk SOAR (On-premises) on the Reporting page. You can perform the following actions on this page:

- View all reports available in your Splunk SOAR (On-premises) instance.
- View only Event reports, which are reports generated inside a container.
- View only Case reports, which are reports generated inside a case.
- View and create Executive Summary reports. You can only create Executive Summary reports on this page. See Create an Executive Summary report in Splunk SOAR (On-premises).

View reports in Splunk SOAR (On-premises)

Perform the following tasks to view reports in Splunk SOAR (On-premises):

1. From the **Home** menu, select **Reporting**. Reports that are generated on-demand appear in the **Generated Reports** section, and reports that are scheduled for a specific time or interval appear in the **Scheduled Reports** section.
2. (Optional) Filter the reports you see on this page by selecting the **All Types** drop-down list.
    - Select **Executive Summary** to view only Executive Summary reports on this page.
    - Select **Event Report** to view only reports created inside a container.
    - Select **Case Report** to view only reports created inside a case.
3. (Optional) Click on any column header to sort the table. For example, click on **Report Name** to sort the reports in the table by report name.
4. (Optional) For any report on the page, download a PDF or view the report within Splunk SOAR (On-premises).

Create an Executive Summary report in Splunk SOAR (On-premises)

Perform the following tasks to create an Executive Summary report in Splunk SOAR (On-premises).

1. From the **Home** menu, select **Reporting**.
2. Click **+ Report** to create a new report.
3. Give the report a name.
4. The report **Type** is Executive Summary. This is the only type of report you can create on this page.
5. Select a **Source**.
6. In the **Period** field, select the period of time you want the report to cover.
7. In the **Schedule** field, select when or how often you want the report to be run.
    - Select **Run Now** to run the report immediately after it is saved. View the report in the **Generated Reports** section of the Reporting page.
    - Select another option such as **Daily**, **Weekly**, **Bi-Weekly**, **Monthly**, or **Quarterly** to schedule an interval for running the report. Specify a starting date in the **Starting On** field, which appears when you select any

option other than **Run Now**. View the report in the **Scheduled Reports** section of the Reporting page.

8. Click **Save**.

Create custom lists for use in Splunk SOAR (On-premises) playbooks

A custom list is a collection of values that you can use in a Splunk SOAR (On-premises) playbook, such as a list of banned countries, or blocked or allowed IP addresses. Custom lists are used to save information in a visual format that can be used to make decisions or track information about playbooks. In your **Filter** and **Decision** blocks, compare parameters against all the values in a custom list, rather than having to configure each comparison in the playbook.

Create or import a custom list in Splunk SOAR (On-premises)

To work with custom lists through the REST API, refer to the next section, Create a custom list using the REST API.

Create a custom list in Splunk SOAR (On-premises)

Custom lists have a size limit of 2GB.

Perform the following steps to create a custom list in Splunk SOAR (On-premises):

1. From the **Home** menu, select **Playbooks**.
2. Select the **Custom Lists** tab.
3. Click **+ List** to create a new list.
4. Enter a name for the list.
5. Enter or paste the list values in the table using one value per cell. For example, you can create a list of banned countries, or blocked or allowed IP addresses. Right-click in a cell to add or remove rows and columns.
6. Click **Save**.

Import a custom list to Splunk SOAR (On-premises) using a CSV file

Imported custom list files have a size limit of 1MB.

Perform the following tasks to import a CSV file to be used as a custom list.

1. From the **Home** menu, select **Playbooks**.
2. Select the **Custom Lists** tab.
3. Click the **Import Custom List CSV** icon (⬆) to import a custom list as a CSV file.
4. Enter a name for the list.
5. Drag and drop your CSV file to the window, or click the window to locate the CSV file on your file system.
6. Click **Upload**.

See Example of using a custom list in a filter in *Build Playbooks with the Visual Editor* for an example of how to use a custom list in a playbook.

Create a custom list using the REST API

See REST Lists in the *REST API Reference for Splunk SOAR (On-premises)* for information about how to manage custom lists using the REST API.

Export a custom list for use with third party products and services

You can use the REST API to export a custom list for use as an external deny list with third-party products and services. For example, you can publish a list of banned IP addresses that can be used in your Palo Alto Networks firewall products.

Perform the following tasks to export a Splunk SOAR (On-premises) custom list and use it in a third party product.

1. Review the formatting requirements that your third party product or service has for custom lists. For example, Palo Alto Networks products may have specific formatting requirements for their dynamic lists. Review these requirements so that the formatting in your Splunk SOAR (On-premises) custom lists match these formatting requirements of your third party product or service.
2. Provide a URI to the custom list in Splunk SOAR (On-premises) using the following format:

   ```
   https://username:password@[soar server]/rest/decided_list/[list
   name]/formatted_content?_output_format=csv
   ```

   For example, to provide a URI to the Splunk SOAR (On-premises) server **SOAR_server.example.com**, using **admin** as the user and **password** as the password, and a custom list named **blockdomains**:

   ```
   https://admin:password@SOAR_server.example.com/rest/decided_list/blockdomains/formatted_content?_output
   _format=csv
   ```

Manage cases in Splunk SOAR (On-premises)

Overview of containers

A container describes an object made of one or more artifacts that playbooks automate on. Objects are ingested from assets into containers. A container has the default label event and can be promoted to a case.

Create a container

Containers are created automatically during ingestion. You can also create a new container by following these steps:

1. From the **Home** menu, click **Sources**.
2. Click **+Event**.
3. Enter an event name.
4. The default label for a container is "events." If you have other labels, you can select one from the drop-down list in the **Label** field. See Configure labels to apply to containers in *Administer Splunk SOAR (On-premises)*.
5. (Optional) Click the **Advanced** drop-down menu to specify other information about the container.
    1. In the **Event Type** field, select if you want this event to be a container (Event) or a case.
    2. In the **Status** field, select a status. See Create custom status labels in Splunk SOAR (On-premises) in *Administer Splunk SOAR (On-premises)*.
    3. In the **Owner** field, select the owner or role for the event.
    4. In the **Severity** field, select the severity of the event to define its impact or importance. See Create custom severity names in *Administer Splunk SOAR (On-premises)*.
    5. In the **Sensitivity** field, select the sensitivity of the event to define who has access to the container. For example, if the machine of a high-ranking officer is compromised, you can assign a higher sensitivity to limit which analysts have access.
    6. In the **SLA Expires** field, configure the service level agreement for resolving the container. See Configure the response times for service level agreements in *Administer Splunk SOAR (On-premises)*.
    7. Enter a description of the container in the **Description** field.
    8. In the **Tags** field, select existing tags or type a new tag to create the tag. See Add tags to objects in Splunk SOAR (On-premises) in *Administer Splunk SOAR (On-premises)* for more information about how tags are used in Splunk SOAR (On-premises).
    9. Toggle the **Artifact Dependency** switch to the on position to prevent automation tasks from running on this container. By default, this dependency is off, meaning that automation tasks can run even when no artifacts are present.
6. Click **Save**.

Understanding container update time

After you have created a container, the **Event Info** tab provides information about the playbooks and actions run on it, artifacts, date and time information, authorized users, and the source ID and tags for the container. The time in the **Last Updated** field shows when the container was last updated. Performing the following actions updates the **Last Updated** time for the container:

- Creating, deleting, or editing a note.
- Creating, deleting, or editing a workbook task.
- Creating, deleting, or editing a workbook phase.
- Creating or deleting evidence.
- Creating or deleting a container attachment.

- Running an action on the container.
- Changing the status or severity.
- Changing the owner.
- Promoting a container to a case, or demoting it to an event.
- Editing the description of a container.
- Adding, deleting, or editing tags on the container.
- Adding a workbook.

Overview of cases

Containers can be promoted to cases. You can use cases to consolidate information from multiple containers.

- Cases have phases and tasks, which are organized into workbooks to track and manage all the actions taken.
- Tasks can have playbooks and actions associated with them, allowing you to automate these actions. Automating actions allows Splunk SOAR (On-premises) to be used to track policy and compliance, and to fulfill documentation requirements.

Create cases in Splunk SOAR (On-premises)

Once you have at least one case workbook, you can create cases to use that workbook.

Cases only contain the items from the workbook at the time the case was created. If you create a case from a workbook, and then later add a new phase to the workbook, the new phase is not available to the existing workbook. Only new cases created after the workbook is changed will have the new phase available to use. The case was a copy at the time it was created. There is no live link to the workbook. Items deleted from the workbook aren't deleted from cases created before the workbook change.

Promote a container to a case

Create a case by promoting a container.

1. From the **Home** menu, select **Sources**, and then select a container label.
2. Click the suitcase (💼) icon.
3. In the **Promote to Case** window, select the new workbook you want to use on this case. If you already added a workbook to the container, you do not have the option to select a workbook. The menu is inactive with the text "Keep current workbook".
4. Click **Save**.

A case looks similar to its container and has all of the same functions. The colored block with the word **Case** indicates that it is a case.

Select the **Workbook** tab to see the tasks defined in case workbook. The blue highlight indicates the current page and shows task completion progress within each phase.

Demote a case to change it back to a container

Perform the following steps to change a case back to a container:

1. In Splunk SOAR (On-premises), navigate to the case you want to demote.
2. Click the suitcase (💼) icon.

Delete a case in Splunk SOAR (On-premises)

Perform the following steps to delete a case:

1. In the **Home** menu, select **Cases**.
2. Select the cases you want to delete.
3. Click **Delete**.
4. Click **Delete** again to confirm that you want to delete the selected cases.

Add objects to a case in Splunk SOAR (On-premises)

Add objects to a case in one of the following ways:

- Promote a container to a new case. Everything in the container becomes a case object.
- Promote a container to an existing case. Choose the objects from the container to be copied to the existing case. The container itself remains a container and is not promoted to a case.
- Copy an individual object to an existing case with the Add to Case option.

Add objects from a container to an existing case

Perform the following steps to add objects from a container to an existing case:

1. Navigate to a container in Splunk SOAR (On-premises).
2. Click the suitcase (💼) icon.
3. Select the case in the **Add Event to Case** dialog box:
    1. Select **Existing Case**.
    2. In the **Case Name** field, select an existing case, or start typing to filter the case names before selecting a case.
    3. Select a phase from the case that you want to add objects to.
    4. Select the object type from the container that you want to add to the case. If the object is evidence, check the **Mark as evidence** checkbox.
4. Click **Save**.

You can add objects from a container to a case only once.

See Create cases in Splunk SOAR (On-premises) for information about promoting an entire container to a case.

Add artifacts from a container to a case

Perform the following steps to add artifacts from a container to a case:

1. Navigate to a container in Splunk SOAR (On-premises).
2. Click **Analyst** to change the container to the analyst view.
3. Click the **Artifacts** tab.
4. Click the **...** icon on the artifact line, and then select **Add To Case**.
5. Complete the **Add Artifact to Case** dialog box:

    1. Click the **Case Name** field and select an existing case, or start typing to filter the case names before selecting a case.
    2. Select a phase from the case that you want to add artifacts to.
    3. (Optional) Click **Include note** and add a note to accompany the artifact being added.
    4. (Optional) If the artifact is evidence, check the **Mark as evidence** checkbox.
6. Click **Save**.

Add files from a container to a case

Perform the following steps to add files from a container to a case:

1. Navigate to a container in Splunk SOAR (On-premises).
2. Click **Analyst** to change the container to analyst view.
3. Click the **Files** tab.
4. Click the **...** icon on the artifact line, and then select **Add To Case**.
5. Complete the **Add File to Case** dialog box:
    1. Click the **Case Name** field and select an existing case, or start typing to filter the case names before selecting a case.
    2. Select a phase from the case that you want to add the file to.
6. Click **Save**.

Add action results from a container to a case

Perform the following steps to add action results from a container to a case:

1. Navigate to a container in Splunk SOAR (On-premises).
2. Click **Analyst** to change the container to analyst view.
3. Click the **Activity** tab. Action run results appear near the bottom in the Activity tab.
4. Click the **...** icon on an action result and select **Add To Case**.
5. Complete the **Add Action Result to Case** dialog box:
    1. Click the **Case Name** field and select an existing case, or start typing to filter the case names before selecting a case.
    2. Select a phase from the case that you want to add the file to.
6. Click **Save**.

Define a workflow in a case using workbooks in Splunk SOAR (On-premises)

You can define a workflow in a case by using workbooks. Workbooks are lists of standard tasks that you follow when you evaluate events or cases. You can create workbooks to analyze events. You can also combine multiple workbooks to create a more comprehensive workbook for cumulative events, cumulative cases, or cases that start out as one type of incident but end up as a different type of incident.

Workbooks are available from Investigation in both Summary View and Analyst View.

Add a workbook to an event or case

Perform the following steps to add a workbook to an event or case:

1. Navigate to an event or case in Splunk SOAR (On-premises).
2. Click the **Workbook** tab.

3. Click **Add Workbook**.
4. Select the desired workbook from the drop-down list.
5. Click **Save**.

In Analyst View in Investigate, you can click **Add** to add additional workbooks to the event, or click **Edit** to make changes to the workbook. If you edit a workbook in this manner, the changes only apply to the current event, not for all events. You must edit a workbook on the Workbooks page to make global changes. See Define tasks using workbooks in *Administer Splunk SOAR (On-premises)*.

Use workbooks to track, edit, and complete tasks

Use workbooks in a case to track, edit, and complete tasks after you have added items to the case.

Perform the following tasks to view the workbook for a case:

1. Navigate to the case in Splunk SOAR (On-premises).
2. Click **Analyst** to switch to the Analyst View.
3. Select the **Workbook** tab.

Add new workbooks or edit phases and tasks

You can add existing workbooks to a case, add new phases to a workbook, or manage tasks.

1. Navigate to the case in Splunk SOAR (On-premises).
2. Click **Analyst** to switch to Analyst View.
3. Select the **Workbook** tab.
4. Click **Add** to add existing workbooks to the case.

If you have created self-contained workbooks to analyze certain types of incidents, adding multiple workbooks is useful for cases that start out like one type of incident but turn out to be a different type of incident. This helps you avoid any inconsistencies that might occur from adding individual phases or tasks during analysis. It is also possible to add individual phases or tasks.

Click **Edit** to add new phases or manage tasks. You can add, remove, or rename tasks, assign an owner to a task, assign authorized users, or configure whether or not a note is required for the task to be completed. If you edit a workbook in this manner, the changes only apply to the current event, not for all events. You must edit a workbook on the Workbooks page to make global changes.

Manage task details

Click on a task in the workbook column to open the task details in the main window area. You can view the task name and description supplied when the task was created.

1. Navigate to the case in Splunk SOAR (On-premises).
2. Click **Analyst** to switch to Analyst view.
3. Select the **Workbook** tab.
4. Click the name of the task.
5. Select a progress status from the drop-down list.

All tasks start with the status of Incomplete by default. As you complete tasks, additional options such as In-Progress or Complete become available. If configured to do so, some items require you to enter a note before you can mark it as complete.

A checkmark next to the task name indicates that it is complete. You can change the status of a task to Incomplete if the task requires additional information or action.

Create case reports to download and share in Splunk SOAR (On-premises)

Create a case report as a PDF file that can be downloaded and shared. You can generate a case report at any time from either Summary or Analyst view. The report contains all of the information in the case up to that point. You can have multiple reports per case.

Perform the following tasks to generate a case report:

1. Navigate to the case in Splunk SOAR (On-premises).
2. Click **+ Report**.
3. (Optional) Click **Include data** to generate an archive containing the PDF report file and copies of all the data in the case, such as files, action run results, copies of artifacts in JSON format, and notes. Including data in a case report can significantly increase the size of the report and the time it takes to generate the report.
4. Click **Generate**.

Use Splunk SOAR (On-premises) in a Connected Experiences App

Use the Splunk Mobile app for Splunk SOAR (On-premises)

Use the Splunk Mobile App to view and respond to notifications, view dashboards, view event details, or run a playbook in Splunk SOAR (On-premises).

Prerequisites

Before using the Splunk Mobile app for Splunk SOAR (On-premises), perform the required administrative tasks. See About the Splunk Mobile App for Splunk SOAR in the *Get Started with the Splunk Mobile App for Splunk SOAR (On-premises)* manual.

> The Splunk Mobile app for Splunk SOAR (On-premises) only works with iOS devices.

View a notification

View a notification by opening a push notification in the Splunk Mobile app. Or, you can open a notification in the Splunk Mobile UI.

1. In your Splunk SOAR (On-premises) instance in the Splunk Mobile app, navigate to the **Notifications** tab. You can filter notifications by type by tapping **All Types** at the top of the list.
2. Tap a notification to view its details.

Respond to a notification

You can also respond to notifications in the Splunk Mobile app.

1. In your Splunk SOAR (On-premises) instance in the Splunk Mobile app, navigate to the **Notifications** tab.
2. Select a notification.
3. To respond to the notification, complete the fields that the notification requests.

View dashboards

To view your Splunk SOAR (On-premises) dashboards, navigate to the **Dashboards** tab in the Splunk Mobile app.

Depending on the visualization type, you can scroll through or tap the visualization to get more details.

View event details

You can view event details from Splunk SOAR (On-premises) on your mobile device using the Splunk Mobile app.

To view an event, perform these steps:

1. In your Splunk SOAR (On-premises) instance in the Splunk Mobile app, navigate to the **Events** tab. You can filter events by owner and status at the top of the list.

2. Tap an event to view its information.

To run a playbook against the event, tap the **Playbook** button. See Run a playbook for more information about running playbooks on your mobile device.

Tap the **Activity** tab to view event activities or add a comment. Tap the **Artifacts** tab to view event artifacts. Tap the **Notes** tab to view and filter event notes.

Run a playbook

You can run a playbook that you create in Splunk SOAR (On-premises) on your mobile device using the Splunk Mobile app.

Follow these steps to run a playbook in the Splunk Mobile app:

1. Create playbooks in Splunk SOAR (On-premises). See Use playbooks to automate analyst workflows in Splunk SOAR (On-premises) in *Build Playbooks with the Visual Editor*.
2. In your Splunk SOAR (On-premises) instance in the Splunk Mobile app, navigate to the **Events** tab. You can filter events by owner and status at the top of the list.
3. Tap an event that you want to run a playbook in response to.
4. Tap the **Playbook** button.
5. Select the playbook you want to run.
6. Select the scope of the playbook. The scope indicates which artifacts that the playbook processes. New includes only artifacts from when this playbook was last run. All includes all artifacts. Artifact processes a specific artifact defined by the artifact ID.
7. Tap **Run Playbook**.

The Splunk Mobile app runs the playbook against the event you selected.

Run Splunk SOAR (On-premises) playbooks in Splunk AR workspaces

Workflow automation is a beta feature available in Splunk AR version 2.1.0. Workflow automation integrates Phantom playbooks into AR workspaces to guide users through real-world tasks. To use workflow automation, create playbooks in Phantom and then add them to your AR workspaces in the Splunk AR mobile app.

See Add Phantom playbooks to AR workspaces in Splunk AR to learn how to add playbooks to AR workspaces.

See Run a Splunk SOAR (On-premises) playbook in Splunk AR for instructions on how to run a playbook in Splunk AR.

Use Splunk SOAR (On-premises) with IT Service Intelligence

Send IT Service Intelligence episodes to Splunk SOAR (On-premises)

Integrate IT Service Intelligence (ITSI) and Splunk SOAR (On-premises) to automatically resolve issues in your IT environment.

With the ITSI integration with Splunk SOAR (On-premises), you can send episodes directly to Splunk SOAR (On-premises) and run custom playbooks to resolve issues in your IT environment. This functionality lets you automate simple and complex IT operations workflows to increase service availability and operational efficiency. For more information, see Resolve ITSI episodes automatically with Splunk SOAR (On-premises) in the Splunk IT Service Intelligence *Administration Manual*.

Use the command line interface to perform tasks in Splunk SOAR (On-premises)

Splunk SOAR (On-premises) command-line interface overview

Analysts can perform a number of tasks from either the command line of the *nix shell or from the comments field of a container through the PhBot CLI interpreter in Splunk SOAR (On-premises).

The command-line interface in Splunk SOAR (On-premises) supports a number of tasks:

- Run an action
- Run a playbook
- Add a note to a container
- Update or edit a container
- Get datapath information for use with other actions

Each task type has an associated slash command and arguments.

Use the CLI tool in Splunk SOAR (On-premises)

You can access the command line interface from the Linux shell by running a script with the required command and arguments. You can find the script in `<PHANTOM_HOME>/bin/run_slash_command.pyc`.

If you choose to use the CLI tool from a Linux shell, you are prompted to authenticate for each command unless the PH_AUTH_TOKEN or PHANTOM_USERNAME and PHANTOM_PASSWORD environment variables are set. Use the username and password for a valid Phantom user, which might be different from the Linux user account. User credentials are not cached.

You can set environment variables for the Linux user account using the `setenv` command or by editing the user account's profile.

You can also use the PH_AUTH_TOKEN environment variable for a temporary session as shown in the following example:

```
export PH_AUTH_TOKEN="<token>"

phenv python run_slash_command.pyc --help
```

> If you use sudo to use slash commands and want to use the PH_AUTH_TOKEN environment variable, use the -E argument to preserve the environment variable.

Anatomy of a slash command

A slash command is an instruction that begins with a forward slash (/) followed by a predefined command then any required or optional arguments. Each command has a series of arguments needed for the execution of the command. The order of arguments is important.

You can use the --help argument with a slash command to determine which arguments are needed and in what order they need to be listed.

Use the following format for the action slash command:

```
/action < action_name > < app > < required arguments > < --asset asset_name> < --optional arguments >
```

This example shows the slash command `/action` followed by the `action_name`, then the required app to run the action, and finally the required arguments.

/action geolocate_ip "MaxMind" 1.1.1.1

Slash command examples with the CLI tool

Run the `run_slash_command.pyc` script without arguments to get the help output.

Command:

```
phenv python run_slash_command.pyc
```

Output:

```
    run_slash_command.pyc USAGE: <container-id> <slash-command>

    You will be prompted for authentication. You can set the following environment
    variables to avoid this:

    Environment:
      PH_AUTH_TOKEN:    Authenticate using an auth token.
      PHANTOM_USERNAME: Authenticate with user name. Requires PHANTOM_PASSWORD set to avoid prompt.
      PHANTOM_PASSWORD: Authenticate with password.

    Hint: You can get the container ID from the phantom event UI, /mission/<container-id>/

    Examples:
      - phenv run_slash_command.pyc 1 /action geolocate_ip "MaxMind" 1.1.1.1
      - phenv run_slash_command.pyc 1 /playbook 12 all
      - phenv run_slash_command.pyc 1 /set name "My Container Name"
      - phenv run_slash_command.pyc 1 /note "Errant IPs" IPs encountered include
'artifact:*.network.src_ip'
      - phenv run_slash_command.pyc 1 /inspect 'artifact:*'
      - phenv run_slash_command.pyc 1 /inspect '[1, 2, 3, 4, 5]'
```

Use the CLI tool to add a note to a container.

Command:

phenv python run_slash_command.pyc <container ID> /note "Errant IPs" IPs encountered include 'artifact:*.network.src_ip'

Output:

```
[2019-12-12 00:02:08] Execution result was:
```

```
Command finished successfully!
```

The Splunk SOAR (On-premises) web interface has a new note for the container with the title "Errant IPs" and the body:

```
IPs encountered include 1.1.1.1
```

Use the CLI in the Splunk SOAR (On-premises) web interface

Analysts can use the CLI from the comments field on events or cases in Investigation. When using this method to run commands, slash commands run against the current container.

In the web-based interface, slash commands support auto-completion of options and arguments. Results are displayed in the activity sidebar.

Run an action in Splunk SOAR (On-premises)

Analysts can use the `/action` command to quickly run one of the actions Splunk SOAR (On-premises) supports.

Actions run with `/action` are the same actions that are found in the **Run Action** dialog box, but the names of the actions are formatted with underscores (_) instead of spaces. For example, the action `geolocate ip` becomes `geolocate_ip`.

The **Run Action** dialog box guides you through selecting the information an action requires. Using the command line interface requires you to provide the same information as arguments to the `/action` command.

When you type `/action` in the comment field of the activity sidebar, a tooltip-style dialog appears to guide you through adding arguments, or you can use the `--help` argument to get a message with help information as shown here:

```
/action geolocate_ip "MaxMind" --help
```

PhBot returns the following help message:

```
usage: /action geolocate_ip [app] <required arguments> [--asset asset...]
[--optional arguments]

Queries MaxMind for IP location info

required arguments:
ip IP to geolocate
```

The command-line interpreter validates arguments with the `/action` command. Incorrect arguments generate an error message to help you fix the arguments as shown in the following example:

```
/action whois_domain "WHOIS" splunk.com
```

The following error message is returned for the example:

```
/action whois_ip "WHOIS" a.b.not_an_ip
```

Use a list with the /action command

You can perform actions on lists of items by passing the list as an argument as shown in the following example:

```
/action geolocate_ip "MaxMind" ["1.1.1.1", "2.2.2.2"]
```

Lists must be presented in valid Python syntax, so individual items must be in quotation marks (").

> Passing the /action command multiple lists or datapaths, or a mix of lists and datapaths, results in a product. For example, [1, 2] [3, 4] results in four action runs: (1, 3), (1, 4), (2, 3), and (2, 4).

Run a playbook in Splunk SOAR (On-premises)

Analysts can use the `/playbook` command to run a playbook from the command line in Splunk SOAR (On-premises).

To run a playbook from the command line, you must supply the playbook_id or playbook_name and the scope. A playbook_name consists of a repository, followed by a slash (/), and the name of the playbook.

You can get a playbook_id or playbook_name by looking up the playbook from **Main Menu** > **Playbooks**, and clicking the playbook name from the list. The ID is the number in the playbook URL. See the following example:

```
https://<phantom.example.com/playbook/1
```

Or you can use the REST API to query `/rest/playbook`. See Query for Data in *REST API Reference for Splunk SOAR (On-premises)*.

Scope is one of the following values:

- `new` - Run the playbook for only artifacts added to the container since the last time the playbook was run.
- `all` - Run the playbook against all artifacts in the container.
- `<artifact ID>` - Run the playbook for either a specific artifact or a list of artifacts.

Example using the playbook ID

```
/playbook 1 new
```

Example using the playbook name

```
/playbook local/example_playbook all
```

You can also supply lists for IDs or scope to run multiple playbooks, to run a playbook for multiple specified artifacts or scopes, or multiple playbooks for multiple specified artifacts.

Example of multiple specified artifacts

```
/playbook 1 ["41", "43", "45"]
```

This example runs playbook 1, for artifact IDs 41, 43, and 45 in the container.

Example of multiple playbooks

```
/playbook ["1", "2", "3"] new
```

This example runs playbooks 1, 2, and 3 for new artifacts in the container.

Example of multiple playbooks and multiple scopes

```
/playbook ["1", "2"] ["new", "all"]
```

The example runs playbooks 1 and 2 for both the new and all scope.

Add a note in Splunk SOAR (On-premises)

Add a general note using the `/note` command in Splunk SOAR (On-premises). Only general notes are supported. Use the following format:

```
/note "<title>" <note body>
```

You can use a datapath with a note to add additional information to a note. See Use a datapath in Splunk SOAR (On-premises). This is shown in the following example:

```
/note "Attackers" Based on geolocate ip, attacks originated from artifact:*.ip
```

The above example results in a note added with the title "Attackers" and a body that looks like the following:

```
Based on geolocate ip, attacks originated from [2.2.2.2, 1.1.1.1]
```

Notes and datapaths

You can use a datapath anywhere in a note title or body. The datapath is evaluated as a Python style list, and creates a single note with the results listed in it.

See Use a datapath in Splunk SOAR (On-premises).

Update or edit an event in Splunk SOAR (On-premises)

You can edit or set several attributes of an event, also called a container, using the `/set` command.

You can set or edit these attributes:

- name
- label
- owner_id
- status
- severity
- sensitivity

Use the following format to set an attribute:

```
/set <attribute> <value>
```

You can use datapaths to set attributes for multiple events at a time. See Use a datapath in Splunk SOAR (On-premises).

Examples

Rename a container

```
/set <current name> <new name>
```

Set the severity of an event

```
/set severity high
```

Set the status of an event

```
/set status open
```

Use a datapath in Splunk SOAR (On-premises)

You can use a datapath as an argument with a slash command. This makes slash commands flexible and powerful. Use the `/inspect` command to get the datapath to use with other slash commands.

Datapaths

A datapath is a series of names, keywords, attributes, and wildcards that evaluates to a list of values. These values can be attributes of artifacts or action results.

A datapath is described using this format:

```
<type>:<path.to.value_name>
```

Example of a datapath for an artifact attribute:

```
artifact:*.ip
```

Artifacts are indexed by their common event format (CEF) data so only CEF data is available to use in datapaths. You cannot access other fields such as `label` or `description`.

Example of a datapath for action results:

```
action_result:data.*.longitude
```

For more information on datapaths, see collect in the *Python Playbook API Reference for Splunk SOAR (On-premises)*.

Use the /inspect command

Use the `/inspect` command to examine artifacts and to look for datapaths you want to use with another slash command.

See the following example:

Examine an artifact to see if it has IP addresses in its CEF data.

```
/inspect artifact:*
```

The above example returns the following:

```
{u'ip': u'2.2.2.2'}
{u'ip': u'1.1.1.1'}
```

Because there is IP information in the artifact, you can access that information in another command with a datapath.

```
/action whois_ip "WHOIS" artifact:*.ips.*
```

See the following example:

Examine an `action_run`.

```
/inspect action_run:1
```

Returns:

JSON formatted action run information.

```
{
    "comment": "",
    "node_guid": "d7c64d0f-fd0b-4d0b-8c68-34704ee91247",
    "playbook_run": null,
    "exec_order": null,
    "_pretty_owner": "admin",
    "creator": 1,
    "_pretty_undo": null,
    "assign_time": null,
    "create_time": "2019-12-12T00:32:20.600117Z",
    "playbook": null,
    "_pretty_playbook": "",
    "owner": 1,
    "message": "1 action succeeded",
    "action": "geolocate ip",
    "close_time": "2019-12-12T00:32:21.059521Z",
    "exec_delay_secs": 0,
    "container": 78,
    "_pretty_update_time": "17 minutes ago",
    "_pretty_has_app_runs": true,
    "id": 2,
    "targets": [
        {
            "app_id": 118,
            "parameters": [
                {
                    "ip": "115.249.247.26"
                }
            ],
            "assets": [
                2
            ]
        }
    ],
    "due_time": "2019-12-11T21:59:05.213705Z",
    "version": 1,
    "type": "investigate",
    "status": "success",
    "update_time": "2019-12-12T00:32:21.059521Z",
    "handle": null,
    "_pretty_close_time": "17 minutes ago",
    "_pretty_container": "ASN Transaction",
    "_pretty_creator": "admin",
    "ip_address": "10.26.96.21",
    "_pretty_due_time": "Yesterday at 09:59 PM",
    "name": "user initiated geolocate ip action",
    "_pretty_redo": true,
    "_pretty_create_time": "17 minutes ago",
    "cancelled": null,
    "cb_fn": null
}
```

See the following example:

Get a list of all `app_runs`.

```
/inspect app_run:*.id
```

Returns:

```
4

7

6

5

8
```

You can use these `app_run` IDs with other commands or REST API calls.