Splunk® SOAR (Cloud)
Administer Splunk SOAR (Cloud) current

Generated: 3/11/2025 9:29 pm

Table of Contents

Table of Contents

Introduction to Splunk SOAR (Cloud)

Administer Splunk SOAR (Cloud)

Splunk SOAR (Cloud) is a cloud-based Security Orchestration, Automation, and Response (SOAR) system that is delivered as a SaaS (software-as-a-service) solution hosted and managed by Splunk.

The Splunk SOAR (Cloud) 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 manual is intended to be used by the person or team administering the Splunk SOAR (Cloud) system.

The following topics are discussed in this manual:

Feature	Description
Company Settings	Information about your company, contacts, and your Splunk SOAR (Cloud) license.
Administration Settings	All the settings to configure the behavior and appearance of Splunk SOAR (Cloud).
Product Settings	Settings for the Splunk SOAR (Cloud) product that apply to your deployment, such as clickable URLs, aggregation, and workbooks.
Event Settings	Settings to configure the organization, handling, and presentation.
User Management	Settings related to user accounts, permissions, and authentication.
View how much data is ingested in Splunk SOAR (Cloud) using ingestion summary	Information and reports for monitoring the activity of your Splunk SOAR (Cloud) deployment.
Apps and Assets	How to add and configure apps and assets to provide actions in Splunk SOAR (Cloud).
Telemetry	Information about sharing data from Splunk SOAR (Cloud).

Splunk Technical Support

Splunk Standard Support is included in every Splunk SOAR (Cloud) subscription. For details about the levels of technical support provided, read Support Programs. Only authorized support contacts from your company can open cases. Your Splunk support agreement specifies who your authorized contacts are. Your Support contract specifies a number of authorized contacts, and an expiration date. One of your contacts is a Support portal administrator, who can update the list. Only an authorized contact can open a case and track its status. An authorized contact can file a case by logging in to splunk.com, then navigating to the **Support Portal**.

Splunk Support portal

Designated Splunk SOAR (Cloud) users can manage operational contacts for their account and file support cases using the Support portal. Operational contacts are the people in your organization who are notified when their Splunk SOAR (Cloud) environment undergoes maintenance or experiences an event that affects performance.

To manage operational contacts:

1. Go to **My Operational Contacts** in the Support portal.

2. Follow the instructions on the page to add, edit, and remove operational contacts for your Splunk SOAR (Cloud) environment.

To file a case on the Support portal:

1. From the **Splunk installation is?** dropdown, select the state of your deployment.
2. In **Subject**, summarize your issue. Splunk Support sees the first 250 characters in this field.
3. In **What Product are you having trouble with?** select **Splunk SOAR (Cloud)**.
4. In **What OS are you using?** select **Linux**.
5. Leave **What OS Version are you using?** blank.
6. In **I need help with...** select a category that applies to your issue.
7. In **What is the impact...** explain briefly how this issue disrupts your work.
8. In the **Problem Description**, be thorough. For issues (as opposed to enhancement requests), include the exact time of the issue and its duration, the type of Splunk instance experiencing the issue (for example, forwarder, search head, or indexers), and any relevant screen shots.
9. Include **Steps to reproduce** if you've found a specific scenario that triggers the issue.
10. Click **Submit**. The portal directs you to a screen with a case number and sends you an email containing the case number.

Splunk Support replies to the case creator by email. You can update the case by replying to the email (be sure to keep the tracking ID in the email subject line). You can also update the case, check on its status, or close a case using the support portal.

Splunk community

The Splunk user community is a great resource. Check out Splunk Answers, where you can ask and answer questions about the product. There are also a number of other ways to get involved in the Splunk community, such as user groups or the Splunk Trust. For more information about getting involved with the Splunk community, see the Community portal.

See also

- Use playbooks to automate analyst workflows in Splunk SOAR (Cloud) in the *Build Playbooks with the Playbook Editor* manual.
- About Splunk Automation Broker in the *Set Up and manage the Splunk SOAR Automation Broker* manual.

Pair Splunk SOAR (Cloud) with Splunk Enterprise Security

Pair your Splunk SOAR (Cloud) instance with your Splunk Enterprise Security (Cloud) version 8.x instance to add the automation capabilities of Splunk SOAR (Cloud) to the security analytics of Splunk Enterprise Security (Cloud) version 8.x .

Coordinate with your Splunk Enterprise Security administrator and Splunk administrator to perform the pairing.

Provide the administrators with the following Splunk SOAR (Cloud) information:

- IP address, for the Splunk Cloud Platform IP allow list
- Base URL (https://example.soar.splunk.com)
- Login credentials (username and password)

The Splunk Enterprise Security admin might contact you about an error in the pairing process. Possible issues include:

- The Splunk SOAR (Cloud) version is not compatible with this version of Splunk Enterprise Security (Cloud) version 8.x . You might need to upgrade your Splunk SOAR (Cloud) deployment.
- The credentials entered for pairing were not correct. You might need to verify the Splunk SOAR (Cloud) credentials.
- The Splunk Enterprise Security (Cloud) version 8.x IP address is not included in the Splunk SOAR (Cloud) allow list. Contact Splunk Support to update the allow list.

The following users and roles manage the pairing of Splunk SOAR (Cloud) and Splunk Enterprise Security (Cloud) version 8.x. Do not assign the roles to user accounts or modify these users; es_soar_integration_role, es_automation_user, es_integration_user

See also

For details on the pairing process, see Pair Splunk Enterprise Security with Splunk SOAR in the *Administer Splunk Enterprise Security* documentation.

For information on troubleshooting pairing in Enterprise Security, see Troubleshoot pairing Splunk Enterprise Security with Splunk SOAR in the *Troubleshoot Splunk Enterprise Security* documentation.

Reset the admin password

The initial provisioning password is sent to the registered admin in an email. To reset the password, complete the following steps:

1. Navigate to the login page of your Splunk SOAR (Cloud) instance.
2. Click **forgot password**.
3. Type the user name of **soar_local_admin**.

An email will be sent to the registered admin. If you don't receive the email, contact Splunk support to find out who your registered admin is. See Splunk Technical Support.

Take a tour of Splunk SOAR (Cloud) and perform product onboarding when you log in for the first time

When you log in to Splunk SOAR (Cloud) for the first time, there are several screens you must navigate before arriving at the home page. The screens appear in the following order:

- Read and accept the Splunk End User License Agreement.
- Review and understand how Splunk collects and uses aggregated product usage data.
- (Optional) Take a tour of Splunk SOAR (Cloud)and create some sample data.
- (Optional) Configure basic settings for your Splunk SOAR (Cloud) instance, data sources, playbooks, and apps and assets.

Read and accept the Splunk End User License Agreement

When you log in to Splunk SOAR (Cloud) for the first time, you must read and accept the Splunk End User License Agreement.

1. Scroll to the bottom of the End User License Agreement.
2. Click **I Accept**.

Review and understand how Splunk collects and uses aggregated product usage data

Splunk collects and sends anonymized usage data to Splunk. This behavior is enabled by default. Read the text on the **Helping You Get More Value from Splunk Software** page and click **Got it**.

See Share data from Splunk SOAR (Cloud) for information about how to opt out, what information is shared, and how it is used.

Take a tour of Splunk SOAR (Cloud) and create some sample data

Generate some sample data and get a guided tour of Splunk SOAR (Cloud)'s main pages.

Click **Exit Tour** at any time to leave the tour and go to the onboarding tutorial, where you can Configure basic settings for your Splunk SOAR (Cloud) instance, data sources, playbooks, and apps and assets.

Perform the following tasks to create some sample data and take the guided tour:

1. Click **Get Started** to begin the product tour and create sample events.
2. Generate some sample events. Click the number of sample events you want to generate. After the events are generated, the **Sources** page shows you the sample events.
3. Click **View Event** to view the details for an event on the Investigation page.
4. Click **Run Playbook** to run a playbook against this event. In Investigation, the **Activity** tab shows the automated actions taken against the event by the playbook.
5. Click **View Playbook** to view the playbook in the Playbook Editor. Playbooks run from the **Start** block and perform the actions up to the **End** block.
6. Click **Configure Splunk SOAR (Cloud)** to complete the tour and go to the onboarding tutorial, where you can Configure basic settings for your Splunk SOAR instance, data sources, playbooks, and apps and assets.

Configure basic settings for your Splunk SOAR (Cloud) instance, data sources, playbooks, and apps and assets

Click **Skip on-boarding** at any time to go directly to the Splunk SOAR (Cloud) home page. See Log in and navigate Splunk SOAR (Cloud) in *Use Splunk SOAR (Cloud)*.

- Configure basic settings.
- Configure a data source.
- Run a demo playbook.
- Configure apps and assets.

Configure basic settings

Configure basic administrative and email settings for your Splunk SOAR (Cloud) instance.

1. Configure the administrative password, company name, IT contact email address, system time zone, and the base URL for this Splunk SOAR (Cloud) instance. If you skip the on-boarding, you can configure these fields later. See Configure your company settings in Splunk SOAR (Cloud) for more information about these fields.
2. Configure email server settings. Splunk SOAR (Cloud) requires an email server to send users email for action approvals, when SLAs are breached, and when items that they are tracking change. If you skip the on-boarding,

you can configure the email server and asset later. See Add and configure apps and assets to provide actions in Splunk SOAR (Cloud).

1. Use **smtp** as the default asset name, or enter a new name.
2. Enter the IP address or hostname of the email server.
3. Select the SSL method that your Splunk SOAR (Cloud) instance should use to connect to the email server.
4. Complete the email asset configuration by providing a tag, username, password, sender address, and port.
5. Click **Enable Unicode Support** to enable Splunk SOAR (Cloud) to properly display Unicode characters in the emails.

Splunk SOAR (Cloud) comes preconfigured with an SMTP asset called internal_smtp. The sender address of the internal_smtp asset cannot be changed. If you want Splunk SOAR (Cloud) to send emails from another address and domain, configure an SMTP asset using the previous instructions.

Configure a data source

Configure a data source from which Splunk SOAR (Cloud) can ingest data. In this on-boarding procedure, you can add one data source. You can add additional data sources later at any time. See Add and configure apps and assets to provide actions in Splunk SOAR (Cloud).

Perform the following tasks to configure a data source during the on-boarding procedure.

1. Select a data source. For example, you can configure your email server as a data source.
2. Select or specify an asset name. For example, "office365-phishing-inbox".
3. Select or specify a container name. For example, "FW: Spam Quarantine Notification".
4. (Optional) Click **Additional Information** to expand the section.
    1. Enter one or more **Tags** to attach to the objects from this data source. With the email server example, you might want to add tags that specify the inbox name the email came from, or the backing service, such as "office365".
    2. Enter a description for the asset. For example, "Data ingested from Office 365".
    3. Complete other fields specific to the asset type. The fields may vary depending on the data source you selected. With this example, you might want to configure the **Mailbox folder to be Polled** and the **Maximum Emails to Poll First Time for Scheduled Polling**.
5. Click **Save**.
6. In some cases, you are asked to perform additional tasks. For example, if you configure a Splunk data source, you must record the authorization token that is provided and also download a separate app from Splunkbase in order for the integration between Splunk SOAR (Cloud) and the Splunk platform to work.
7. Click **Continue**.

Run a demo playbook

A list of playbooks is available based on the data source you configured. Select a playbook you want to run, then click **Save and Continue**.

Configure apps and assets

Configure apps and assets that will provide actions for your playbooks.

1. Select the apps that will provide the actions for the selected playbook.

    - If you selected the **investigate** playbook, select one app in each of the Information Services, File Reputation Services, Domain Reputation Services, Sandbox, and Threat Intel.
    - If you selected the **hunting** playbook, select one app in each of the Information Services, Endpoint Services, File Reputation Services, and Sandbox.
2. In the **Select Apps to Configure** section, select each app and provide the required information to configure an instance of the app, called an asset.
3. Select **Additional Information** to expand the section and provide additional information.
4. Select **Save and Test Connectivity** to verify the configuration of each asset.

Splunk SOAR (Cloud) security information

This topic explains the fundamentals of the Splunk SOAR (Cloud) system design and base security measures, as well as the parameters and limitations for that design.

Operating System

Splunk SOAR (Cloud) users do not have access to the operating system of their Splunk SOAR (Cloud) deployment.

Splunk SOAR (Cloud) does not monitor or control the operating system on which it is deployed.

Basic OS privilege separation is utilized, partitions are mounted with limited capabilities, and for privileged deployments SELinux is on.

Processes and daemons

Splunk SOAR (Cloud) runs multiple processes and daemons:

- The web-based user interface runs in the http process as the nginx user. Splunk SOAR (Cloud) uses a custom httpd configuration. Use caution if you update http.
- In a privileged deployment the watchdogd daemon runs as root and is responsible for starting or stopping other processes, collecting system and process information, and installing RPMs.
- In an unprivileged deployment the watchdogd daemon runs as the phantom user and some of its abilities that require root permissions are removed.
- All other daemons run as the phantom user.

Start up

This section provides a brief overview of what happens when Splunk SOAR (Cloud) starts.

- In cloud deployments Splunk SOAR (Cloud) does not have root level access to configure systemd items. Therefore the user account that runs Splunk SOAR (Cloud) has its crontab modified to run <$PHANTOM_HOME>/bin/start_phantom.sh at system boot time.

Access to the operating system

Splunk SOAR (Cloud) users do not have access to the operating system of their Splunk SOAR (Cloud) deployment.

Privileged vs unprivileged deployments

Splunk SOAR (Cloud) is always deployed as an unprivileged installation.

Authentication

Splunk SOAR (Cloud) uses its own authentication database, independent of the linux operating system.

There are several options for web UI authentication. The local user database uses the default Django PBKDF2 hash. See the Wikipedia article https://en.wikipedia.org/wiki/PBKDF2 for more information. Other options include:

- OAUTH
- SAML

Splunk SOAR (Cloud) supports password complexity for its local accounts. Users that require the most advanced account security features are encouraged to use an external identity provider.

Splunk SOAR (Cloud) does use a certificate store for authenticating the LDAPS authentication server.

For more on information configuring users, two-factor authentication, and passwords, see the section Manage your Splunk SOAR (Cloud) users and accounts in *Administer Splunk SOAR (Cloud)*.

SSL and TLS

Splunk SOAR (Cloud) has a certificate store used to validate certificates when opening connections to other servers.

The certificates in the store are trusted certificate authority (CA) certificates from mkcert.org. In almost all cases, Splunk SOAR (Cloud) can use its certificate store to validate any certificate issued by a commercial certificate authority (CA).

If an asset uses TLS and has a self-signed certificate, or if you have an in-house certificate authority, then those certificates must be imported into the store for verification to work.

This includes any necessary intermediate certificates. Note that the requirement for the Common Name to match still applies, so if the certificate is for server.example.com, then the Splunk SOAR (Cloud) asset must also be configured to connect to it as server.example.com, and not a different form of the name such as "server", or an IP address.

TLS versions and ciphers

Splunk SOAR (Cloud) supports TLS versions TLSv1.2 and TLSv1.3. The ciphers supported by Splunk SOAR (Cloud) are those supported by FIPS 140-2 level 2.

The following shows a list of the supported ciphers.

```
TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256
```

Embedded git client

The git client uses the OpenSSL certificate store, which includes most commercial CAs. Git repositories can be configured to use an HTTPS URI if that repository uses a signed certificate from a commercial certificate authority.

If you need to connect to a git repo that uses an unrecognized CA, you have to disable git certificate checking system-wide.

Playbooks, apps, and Python code

Splunk SOAR (Cloud) uses user-supplied Python code in several ways.

- Apps are collections of Python code and JSON configuration files that allow Splunk SOAR (Cloud) to connect to, use, and control other products or services. Apps provide Actions to Splunk SOAR (Cloud), to make controlling your security infrastructure easy.
- Playbooks are specially-crafted Python code that utilize Splunk SOAR (Cloud) Python libraries to run actions, use apps, or run custom code.

Apps and playbooks are available from several sources:

- Splunk provides several apps and playbooks from Splunkbase and a GitHub repository.
- You can develop apps and playbooks yourself.
- You can get apps or playbooks from third parties, such as other Splunk SOAR (Cloud) users.

When running, the python code from Apps and Playbooks are running as either the linux user account phantom, or the specified account that runs Splunk SOAR (Cloud).

It is critical that any untrusted code you obtain from other sources be examined thoroughly.

Python code runs without restrictions other than that it is running as a user account without any special privileges. There is no sandbox of any kind. Anything that the Python language with common libraries can do can be done from an app's or playbook's code. If apps, or assets have configured credentials, obtaining those credentials is possible from an app or playbook's code.

Splunk SOAR (Cloud) FedRAMP Moderate environments have additional restrictions on playbook code:

- Playbooks cannot share information between playbook runs by using the host's file system.
- The directories /tmp and /opt/phantom/tmp cannot be used to share information between playbook runs. These directories can still be used to share information in the context of a single playbook run.
- Playbooks cannot read or modify the directory /opt/phantom/vault by using the file system. Playbooks that interact with the vault must use the Vault automation API.
- Playbooks cannot open direct connections to the PostgreSQL database.

Malicious apps can also introduce hostile HTML into the web user interface in two places:

- App documentation can include HTML.
- Apps often include widgets which render HTML in the web user interface.

Any sort of attack that one could typically perform with an XSS exploit could also be performed by a malicious app. This can allow complete control of the Splunk SOAR (Cloud) UI for a logged-in administrator account.

In addition to malicious behavior, it's also possible for app authors to inadvertently introduce security holes.

For example, an app author may make a system call to run a command, and pass user-supplied data to the shell without properly sanitizing the inputs, potentially leading to a command injection vulnerability. Worse, they might pick up input from a security alert that ultimately came from an outside attacker, and do the same.

User accounts, roles, and privileges

Splunk SOAR (Cloud) supports multiple types of users, has a number of built-in roles which can be assigned to users, and the ability to define custom roles with customized individual privileges.

See also:

- Manage Splunk SOAR (Cloud) users
- Manage roles and permissions in Splunk SOAR (Cloud)

Noteworthy user privileges and roles

When auditing your Splunk SOAR (Cloud) deployment's security, these user accounts and privileges which are especially important. While these roles privileges are expected to be given only to trusted users, it is vitally important to know what capabilities you are trusting them with before doing so.

Administrator role

Administrators can perform any function in the web UI. They can modify users, roles, edit or install apps, manage assets, edit or manage playbooks, change system settings, and more.

Administrators can manipulate users and assets.

- Local user accounts have passwords associated with them. Once the password is set, the UI will not display it to any account. However, an Administrator can simply change passwords.
- Assets can have stored credentials configured. Once credentials are stored, the UI will not display them to any account.

Edit Users and Roles

A user with the "Edit Users and Roles" permission, even if that is the only permission they have, can grant themselves any and all other privileges. Any user or role with this permission is effectively an administrator.

Edit Apps and/or Edit Playbooks

Users with these permissions can edit apps or playbooks, which gives them the ability to execute arbitrary Python code. This means they could leverage Python code to get access to the system shell and attempt other attacks or privilege escalations.

Edit Assets

This permission does not provide a direct path to escalate privileges on Splunk SOAR (Cloud) itself. With this permission a malicious actor could change an asset to connect to a different IP address or hostname for malicious server to obtain asset credentials.

Edit System Settings

The Edit System Settings privilege allows a user to modify system settings. One set of system settings are the identity providers in use. A malicious user with the Edit System Settings privilege could redirect authentication requests to an authentication server they control to obtain user credentials.

Splunk SOAR (Cloud) in restricted environments

Splunk SOAR (Cloud) is available for restricted environments, such as FedRAMP Moderate (IL2), Health Insurance Portability and Accountability Act (HIPAA), Information Security Registered Assessors Program (IRAP), and Payment Card Industry Data Security Standard (PCI DSS).

- For a description of the Splunk SOAR (Cloud) service, see the Splunk SOAR (Cloud) Service Description.
- For current compliance information, see Compliance at Splunk.

Splunk SOAR (Cloud) FedRAMP Moderate

This section applies only to Splunk SOAR (Cloud) in FedRAMP Moderate environments.

Splunk SOAR (Cloud) is available for customers who must meet United States Federal Information Processing Standard (FIPS) 199 Moderate Impact Level requirements.

Splunk SOAR (Cloud) FedRAMP Moderate is different from Splunk SOAR (Cloud) in these areas:

Area	Difference
Hosting	Splunk SOAR (Cloud) FedRAMP Moderate is hosted in AWS GovCloud (US) regions.
FIPS mode	FIPS mode is turned on for all Splunk SOAR (Cloud) FedRAMP Moderate deployments. **Note:** Any Splunk SOAR Automation Brokers that you use in conjunction with your deployment must also run in FIPS mode.
Playbooks	Splunk SOAR (Cloud) FedRAMP Moderate playbooks have additional restrictions over Splunk SOAR (Cloud) or Splunk SOAR (On-premises) instances. • Playbooks cannot modify declared global variables. • Playbooks cannot open direct connections to the the PostgreSQL database. Playbooks must use the playbook automation APIs. • Playbooks cannot share information between playbook runs by using the host's file system. • The directories /tmp and /opt/phantom/tmp cannot be used to share information between playbook runs. These directories can still be used to share information in the context of a single playbook run. • Playbooks cannot read or modify the directory /opt/phantom/vault by using the file system. Playbooks that interact with the vault must use the Vault automation API. • Playbooks should not create subprocesses, either by using the built-in `os.system` python function or the built-in `subprocess` python module.
Automation isolation	Playbook code run in Splunk SOAR (Cloud) FedRAMP Moderate environments is run in isolation using dynamically managed containers. These containers are connected to Splunk SOAR (Cloud) FedRAMP Moderate through an internal automation broker.
Internal automation broker	Splunk SOAR (Cloud) FedRAMP Moderate uses an internal Splunk SOAR Automation Broker to run actions. • The internal automation broker is called soar_internal_ab, and cannot be edited or deleted.

Area	Difference
	• You can see the status of the internal automation broker from the **Home** menu, **Administration**, **Product settings**, **Automation Broker**. For more information about the Splunk SOAR Automation Broker, see About Splunk SOAR Automation Broker.
Restoring from Splunk SOAR (On-premises) or Splunk SOAR (Cloud)	Splunk SOAR (Cloud) FedRAMP Moderate does not currently allow migration of any native data from Splunk SOAR (On-premises) or existing Splunk SOAR (Cloud) instances. This data includes containers, artifacts, notes, comments, and playbook and action runs data. A recommended alternative method is to use the Splunk App for SOAR to move relevant data to Splunk Cloud Platform for retention.

About automation isolation in Splunk SOAR

This feature is only available in Splunk SOAR (Cloud) FedRAMP Moderate environments.

Splunk SOAR (Cloud) has implemented a feature called Automation Isolation to further secure actions.

How playbooks and playbook blocks are run

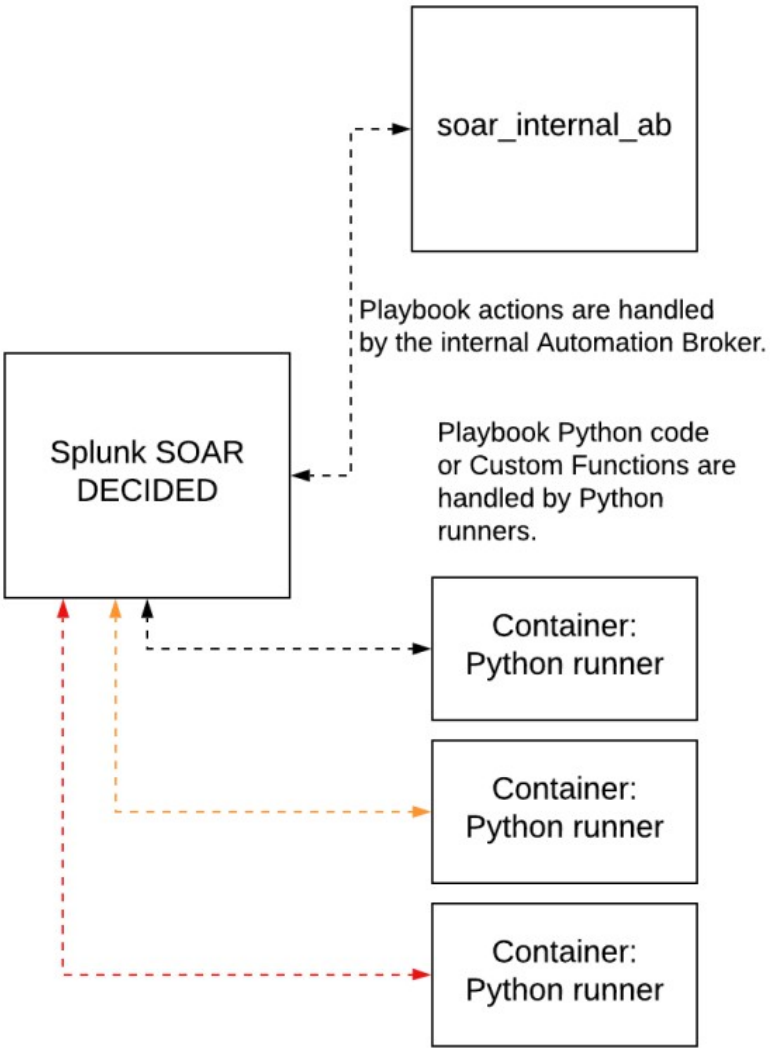
When you run a playbook, the blocks are run sequentially by a Python runner. A playbook block or custom function must be completed before the runner executes the next playbook or custom function in sequence.

Automation isolation

In deployments of Splunk SOAR (Cloud) FedRAMP Moderate your playbook's blocks can be run by multiple Python runners, each python runner in its own isolated container.

When a Playbook run is started, the DECIDED daemon assigns playbook actions or python code either to the internal Automation Broker or to a Python runner.

- Playbook actions are assigned to an internal automation broker named **soar_internal_ab** to be run.
- The playbook's Python code or custom function blocks are assigned to an available Python runner in a round-robin fashion.
- The number of Python runners is automatically scaled up or down as needed. When additional Python runners are required, new containers are launched. When a Python runner is no longer required, its container is destroyed.
- Blocks from the same playbook run are run sequentially. A single playbook run will only run one block at a time.
- Previous releases of Splunk SOAR (Cloud) guaranteed that all the blocks of a playbook run would be run by the same Python runner. Now, playbook blocks can be run by any available Python runner.


soar_internal_ab
Playbook actions are handled by the internal Automation Broker.
Splunk SOAR DECIDED
Playbook Python code or Custom Functions are handled by Python runners.
Container: Python runner
Container: Python runner
Container: Python runner

Additional information about playbook code when using automation isolation

The following changes in playbook behavior occur:

- The playbook API **save_data** may return incorrect results when playbook blocks are run different runners if the key:value pairs are not unique across playbook runs. Use the **save_object()** API instead of the **save_data()** API.
- The playbook API **save_object** may return incorrect results if the same playbook is run against the same container multiple times. Use the optional **playbook_name** and **container_id** parameters with **save_object** to make sure that saved objects are unique across multiple runs of the same playbook.
- The directories /tmp and /opt/phantom/tmp cannot be used to share information between playbook runs. These directories can still be used to share information in the context of a single playbook run.
- Playbooks cannot share information between playbook runs by using the host's file system.
- If you need to save information specifically about a playbook run, use the **save_run_data()** and **get_run_data()** APIs.
- Playbooks cannot read or modify the directory /opt/phantom/vault by using the file system. Playbooks that interact with the vault must use the Vault automation API.
- Playbooks should not create subprocesses, either by using the built-in `os.system` python function or the built-in `subprocess` python module.

See also

- Write better playbooks by following these guidelines
- Splunk SOAR (Cloud) in restricted environments

Configure your company's settings in Splunk SOAR (Cloud)

Configure your company settings in Splunk SOAR (Cloud)

Set the Company Name, IT Contact email address, System Time Zone, and the appliance Base URL for this Splunk SOAR (Cloud) instance. The settings are described in the following table:

Setting	Description
Company Name	The name of the company used in emails sent by Splunk SOAR (Cloud).
IT Contact	The email address of the OS system administrator for Splunk SOAR (Cloud). System-level alerts are sent to this email address.
Instance Name	A unique name used to identify a certain instance of Splunk SOAR (Cloud). Instance names are randomly generated and can be changed if desired, but changing the instance name is not required.
System Time Zone	The time zone for the host system of the virtual appliance that the Splunk SOAR (Cloud) instance runs on.
Base URL for Splunk SOAR (Cloud)	The URL used to access Splunk SOAR (Cloud). This field is set for you when your Splunk SOAR (Cloud) instance is created.

Configure the ROI Settings dashboard

Configure the parameters used to estimate the data displayed in the Automation ROI Summary dashboard.

To configure the ROI Summary dashboard, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Company Settings**, then **Dashboard**.
3. Configure the settings described in the following table.

Setting	Description
FTE Gained	Turn on to make the **FTE Gained** widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk SOAR (Cloud) divides the number of actions run by automation (calculated in Splunk SOAR (Cloud)) by the number of expected actions an analyst would take, based on minutes per action and analyst hours per day (configured on the ROI settings page).
Time Saved	Turn on to make the **Time saved** widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk SOAR (Cloud) sums the difference between the Analyst Minutes Per Action (configured on the ROI settings page) and the actual minutes per action (calculated in Splunk SOAR (Cloud)) over all actions for the past 24 hours.
Money Saved	Turn on to make the **Dollars saved** widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk SOAR (Cloud) multiplies the average time an analyst spends per action and the average analyst salary (configured on the ROI settings page) by the number of actions run by automation (calculated in Splunk SOAR (Cloud)).

Setting	Description
Annual analyst salary	Enter the average annual salary paid to each analyst.
Currency	Select the national currency value you want to use in the display.
Analyst hours per day	Enter the typical number of hours each analyst works per day.
Minutes per action	Enter the average number of minutes an analyst typically spends on any action in a case.

Use Splunk App for SOAR to view more granular breakdowns of individual action runtimes. Splunk App for SOAR sends Splunk SOAR (Cloud) log data back to the Splunk platform. You can use this data to generate or modify reports as needed. For details on Splunk App for SOAR, see Learn about Splunk App for SOAR. To download Splunk App for SOAR, go to Splunkbase.

View your Splunk SOAR (Cloud) license

From the main menu, select **Administration > Company Settings > License** to view information about the license on your system.

Seat-based license

Splunk SOAR (Cloud) is licensed by the number of user accounts that can log in to Splunk SOAR (Cloud). This number includes local accounts in Splunk SOAR (Cloud) and accounts authenticated or managed by external services. The built-in user accounts for the automation and the admin users do not count against a seat-based license. Other users assigned the admin role still count against a seat-based license.

Seat limits must be purchased in increments of five.

For Splunk Cloud customers who license Splunk Enterprise Security (Cloud) and SOAR (Cloud) directly from Splunk, use of Splunk Mission Control does not affect your Splunk SOAR seats or the licensed number of users allowed to log in to Splunk SOAR (Cloud). If you're a Splunk Mission Control user, see Access Splunk Mission Control in the *Splunk Mission Control Service Description* manual for details on how your Splunk SOAR license works with Splunk Mission Control.

Obtaining a license

You obtain a license when you purchase Splunk SOAR (Cloud).

Configure administration settings in Splunk SOAR (Cloud)

Configure a source control repository for your Splunk SOAR (Cloud) playbooks

You can save your Splunk SOAR (Cloud) playbooks in Git repositories. By default, playbooks are managed in a Git repository called `local`. You can create additional Git repositories as needed, so you can perform the following tasks:

- Import and export playbooks and share facilities among Splunk SOAR (Cloud) instances. For example, you can use Git to publish playbooks from a development Splunk SOAR (Cloud) environment to a separate production environment.
- Edit playbooks using a tool of your choice instead of the Splunk SOAR (Cloud) web interface.

If you edit a playbook outside of the Visual Playbook Editor (VPE), you can no longer use drag and drop blocks in the VPE to edit that playbook. After that, you can only perform subsequent edits in the VPE by editing the full playbook. This is not recommended.

Splunk SOAR (Cloud) also uses a Git repository to publish company-authored playbooks for you to download. This repository is called the community repository and is configured on Splunk SOAR (Cloud) by default. You can restore this repository if you accidentally remove it. See Restore the community playbook repository.

You can transfer playbooks to Git using HTTP, HTTPS, or Git. Other protocols can be authenticated or anonymous if supported by the server.

Access the source control settings in Splunk SOAR (Cloud)

To access the Splunk SOAR (Cloud) source control settings, perform the following steps:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **Source Control**.

You can also access the source control settings from any Playbooks page by selecting **Manage source control**.

Set up a playbook repository using HTTP, HTTPS, or Git

To set up a Git repository using HTTP, HTTPS, or Git protocols, perform the following steps:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **Source Control**.
3. Select **Configure a new repository** from the Repositories drop-down list.
4. Provide a repository URL, repository name, and branch name. The repository name can be any name that describes your repository. If you are using a subdirectory, its path must already exist. This configuration panel does not create new subdirectories.
   For details on creating a new subdirectory, see the next section, *Move playbooks to a different or new subdirectory*.
5. Provide the path to the playbooks directory within the repository. The path must end with a slash (/). To store playbooks at the root level, leave this field blank.

6. For HTTP and HTTPS, specify a username and password. Splunk SOAR (Cloud) attempts to connect anonymously if no username or password is provided. When crafting the URI, Splunk SOAR (Cloud) converts https://server... to https://username:password@server.... The Git protocol is not authenticated and does not require a username or password.
7. Select **Save Changes**.

Note the following important points:

- You cannot edit a repository after it is added to Splunk SOAR (Cloud). If you need to make a change, for example, if you change the subdirectory where the playbooks are stored, you must create a new source control repository in Splunk SOAR (Cloud) using the process described above. Delete unused repositories, as described later in this article.
- The repository must contain at least one commit in order to be added to Splunk SOAR (Cloud).

The username and password strings are separated so that the password can be encrypted and stored and not displayed to other administrators. However, passwords are stored as clear text in the Git configuration file for that repository.

Move playbooks to a different or new subdirectory

You might choose to move your organization's playbooks to their own subdirectory, separating them from other files in a repository. This involves updating the Git repository, using any Git client. The steps below are similar to the process described in the GitHub documentation for moving a file to a new location.

If you use multiple branches of the repository, repeat these steps for each branch.

To update the Git repository for your playbook storage path, follow these steps:

1. Create the new directory where you want to store playbooks, if it does not already exist in the Git repository. For example `mkdir playbooks`.
2. Move all existing playbook files to the directory where you want to store them. For example, `mv *.py playbooks/` followed by `mv *.json playbooks/`.
3. Run `git add --all`.
4. Run `git commit -m "Moving playbooks to new folder"`.
5. Run `git push origin <branch-name>`.
6. Return to the Splunk SOAR (Cloud) Administration page.
7. Complete the steps described in the previous section to configure a new source control repository, using the new path to the playbooks.
8. Delete the original, now unused, source control repository, as described in the next section of this article, *Delete a source control repository in Splunk SOAR (Cloud)*.

Delete a source control repository in Splunk SOAR (Cloud)

Delete unused source control repositories to avoid confusion and clutter.

To delete a source control repository in Splunk SOAR (Cloud), follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **Source Control**.
3. In the **Repositories** list, select the repository you want to delete.

4. Select **Delete**.

Git hooks and the Splunk SOAR Playbook Editor

Splunk SOAR (Cloud) does not directly support Git hooks. If you choose to use Git hooks in your system, be aware of the following:

- There is a risk that the playbook editor will not be able to save or push changes because the Git configuration rejects a commit.
- To avoid this issue, direct Splunk SOAR (Cloud) to push to a staging repository or branch that will not reject pushes. This prevents the playbook editor from being blocked from saving and pushing changes. Handle merge conflicts or other issues manually when pushing from the staging repository to the original repository.

If your playbook editor is blocked from pushing to the remote repository, follow these steps:

1. Delete the repository in Git and recreate it in Splunk SOAR (Cloud), using the steps described in the *Set up a playbook repository using HTTP, HTTPS, or Git* section of this article. The playbook reverts to the last successful push and removes all changes made after the last successful push.
2. Recreate your changes and try to push again.

Use repositories from the Playbooks page

You can make use of configured repositories on the Playbooks page. See View the list of configured playbooks for more information.

Restore the community playbook repository

The community playbook repository is a collection of playbooks vetted by the Splunk SOAR (Cloud) community. This repository is configured by default when Splunk SOAR (Cloud) is installed. Follow the procedure to restore the community repository if it is accidentally altered or deleted.

1. From the **Home** menu, select **Administration**.
2. Select **Source Control**.
3. In the Repositories drop-down list, select **Configure a new repository**.
4. In the Repo URL field, enter the URL: https://github.com/phantomcyber/playbooks.git
5. In the Repo Name field, enter **community**.
6. In the Branch Name field, enter the version of Splunk SOAR (Cloud) you are running, up to the second set of digits. For example, if you are running version 6.1.1 enter **6.1** in this field.
7. Select the **Read Only** check box.
8. Select **Save Changes**.

Customize email templates in Splunk SOAR (Cloud)

Customize email templates in Splunk SOAR (Cloud) by inserting real-time information into the emails using special variables. For example, to use the name of the incident in the email, use the `{name}` variable where you want the incident name to appear. Variables can be used in both the subject and body of the email.

1. From the **Home** menu, select **Administration**.

2. Select **Administration Settings > Email Settings**.
3. Select a template from the drop-down list. Templates provided by default are **New Incident Assigned** and **Approvals**.
4. Modify the email template for your use. You can use the variables listed in the following table.

The term **container** refers to the type of object generating the email. Incidents are the only container used for generating emails. See Add and configure apps and assets to provide actions in Splunk SOAR (Cloud) for more information about containers.

Variable	Description
`{name}`	The name of the container or incident.
`{label}`	The label of the container, such as "incident" or "vulnerability," which is configured on the asset.
`{container_url}`	The URL to view the container.
`{first_name}`	The first name of the user being notified.
`{from_first_name}`	The first name of the user who was the previous owner.
`{from_email}`	The email address of the previous owner. This is not a template, but can be configured in settings.
`{due_time}`	The due time of the container in the respective time zone.
`{severity}`	The severity of the container, such as high, medium, or low.
`{your_expired_containers}`	The details of the expired containers assigned to the user.
`{your_expiring_containers}`	The details of the containers assigned to the user that are about to expire.
`{your_closed_containers}`	The details of the containers assigned to the user that have been closed.
`{all_expired_containers}`	The details of all containers that have expired.
`{all_expiring_containers}`	The details of all containers that are about to expire.
`{all_closed_containers}`	The details of all containers that have been closed.
`{task_count}`	The amount of tasks assigned to you.
`{task_list}`	The list of tasks associated with the case.
`{phase}`	The case management phase associated with the task.
`{ownership_type}`	Denotes the owner type as either user or role.
`{invitee_first_name}`	The first name of the person receiving the email.
`{inviter_first_name}`	The first name of the person sending the email.
`{user_message}`	A custom message that can be written and added as part of the notification.
`{from_first_name}`	The name of the person the incident was reassigned to.
`{action_name}`	The name of the action that will be run on the asset.
`{action_executor}`	The rule name or name of the user running or executing the action.
`{asset_name}`	The name of the asset.
`{user_owner_type}`	This denotes whether the owner is the primary or secondary approver.
`{approval_due_time}`	The time in which the action to be run on an asset must be approved by.
`{approval_url}`	Use this URL to navigate to a place where you can approve, deny, delegate or change the action parameters.

Variable	Description
`{approval_message}`	A custom message that can be added to a manual action sent with the approval request.
`{task_name}`	The name of an assigned task.

Configure search in Splunk SOAR (Cloud)

In earlier releases of Splunk SOAR (Cloud) search was handled by an embedded version of Splunk Enterprise. Beginning with release 6.2.0, Splunk SOAR (Cloud) uses PostgreSQL full-text search, which has been modified to accept the `*` wildcard. For search syntax and examples, see Search within Splunk SOAR (Cloud).

To improve the ability to get Splunk SOAR (Cloud) data into a Splunk Cloud Platform, support was added for Universal Forwarders. For information about configuring forwarders, see Configure forwarders to send SOAR data to your Splunk deployment.

Configure Splunk SOAR (Cloud) to forward data to Splunk Cloud Platform

Integrating with Splunk Cloud Platform requires the following actions:

- Configure Universal Forwarders and a Universal Forwarder Credentials Package. See Configure forwarders to send SOAR data to your Splunk deployment.

Configure the scope of global search using the REST API

You can control the scope used by global search in Splunk SOAR (Cloud), using the `/rest/feature_flag/restrict_global_search` REST API endpoint. See /rest/feature_flag/<feature_flag_name> for details of the /rest/feature_flag REST API, the parameters it accepts, and examples for changing settings using the endpoint.

In the interest of performance, **restrict_global_search** defaults to "on" and has the following settings applied:

- Searching the database tables app_run, action_run, and playbook_run are turned off.
- The maximum age of database table entries will be searched is 30 days.

Configure forwarders to send SOAR data to your Splunk deployment

Universal forwarders replaced the embedded instance of Splunk Enterprise in Splunk SOAR (Cloud) release 6.2.0. These universal forwarders allow for better scaling, better performance, and reduced resource usage for getting your SOAR data into your Splunk deployment.

Configure data forwarding

Before you can forward data from your Splunk SOAR (Cloud) deployment to a Splunk Cloud Platform or Splunk Enterprise deployment, you must configure Splunk SOAR (Cloud) for forwarding.

This section applies if you are forwarding data from Splunk SOAR (Cloud) to either an external instance of Splunk Enterprise or Splunk Cloud Platform.

1. In your Splunk Cloud Platform deployment, get a Universal Forwarder Credentials Package.
   For details, see Install and configure the Splunk Cloud Platform universal forwarder credentials package in the

Splunk Universal Forwarder documentation.
    1. In Splunk Cloud Platform, select **Apps**, then **Universal Forwarder**.
    2. Select **Download Universal Forwarder Credentials**.
2. (Conditional) If your Splunk Cloud Platform deployment is in a restricted access category such as HIPPA, DCI/PCS, or FedRAMP Moderate, you must request that TCP port 9997 be opened on your Splunk Cloud Platform.
3. In Splunk SOAR (Cloud), upload the credentials package from Step 1.
    1. From the **Home** menu, select **Administration,** then **Administration Settings**. Then select **Forwarder Settings**.
    2. Select the **+Install Credentials Package** button.
    3. Drag and drop, or select the link to navigate to your credentials package.
    4. Set a name for your forwarder group.
    5. Select the data types you want forwarded to your Splunk Cloud Platform or Splunk Enterprise deployment.
    6. Select the **Save** button.

You will need to make sure that logging levels are set for the appropriate logs in order to forward useful information. For more information about configuring logs and logging levels see Configure the logging levels for the Splunk SOAR (Cloud) action daemon. If you choose to forward the Playbook run data type, you must first create the phantom_playbook_run index in your destination Splunk Enterprise or Splunk Cloud Platform instance. See Create Events Indexes in the Splunk Enterprise documentation or Create a Splunk Cloud Platform events index in the Splunk Cloud Platform documentation.

Update a Universal Forwarder Credentials Package

You may need to update the credentials package associated with your forwarder group. For example, the certificates in the package may need to be refreshed due to an approaching expiration date.

First, obtain an updated Universal Forwarder Credentials Package.

1. In your Splunk Cloud Platform deployment, get a Universal Forwarder Credentials Package.
   For details, see Install and configure the Splunk Cloud Platform universal forwarder credentials package in the Splunk Universal Forwarder documentation.
2. In Splunk Cloud Platform, select **Apps**, then **Universal Forwarder**.
3. Select **Download Universal Forwarder Credentials**.

You can only use a Universal Forwarder Credentials Package that matches the existing stack for your forwarder group.

Once you have obtained an updated Universal Forwarder Credentials Package, apply it to your forwarder group.

1. From the **Home** menu, select **Administration,** then **Administration Settings**. Then select **Forwarder Settings**.
2. Locate the forwarder group whose credential package you want to update.
3. Select the edit icon at the right-hand edge of the table entry for the forwarder group.
4. Select the **Update Credentials Package** button.
5. Drag and drop, or click the large box to select and upload the Splunk Universal Forwarder Credentials Package associated with your Splunk Cloud Platform instance.
6. Select **Save**.

Configure forwarding to a Splunk Enterprise deployment

If your organization forwards Splunk SOAR (Cloud) data to a Splunk Enterprise deployment, you need to configure your forwarders. To configure data forwarding follow these steps:

1. From the **Home** menu, select **Administration,** then **Administration Settings**. Then select **Forwarder Settings**.
2. Select **+New Group**.
3. In the **Add a new forwarder group** dialog do the following:
    1. In the **Name** field, type a name for your forwarder group (do not use the name `splunk`). This name is displayed on the **Forwarder Settings** page.
    2. (Conditional) If you use a TCP token to authenticate to your Splunk Enterprise deployment, add it to the **Token** field.
    3. In the **Indexers** field, add the address for your indexer. Click the **Add Another** if you have more indexers to add. You can remove an indexer from the list by using the **-** button at the end of the indexer's address field.
    4. Select the Data types you want to ingest into Splunk Cloud Platform or Splunk Enterprise.
4. Make sure the **Enabled** slider button is in the on position.
5. Select **Save**.

After you complete these steps, data will begin to stream from Splunk SOAR (Cloud) to your Splunk Enterprise deployment.

Configure transport layer security between your Splunk SOAR (Cloud) universal forwarder and the receiving indexer

You can now use transport layer security (TLS) certificates to secure connections between Splunk SOAR (Cloud)'s forwarders and the receiving indexers.

To add a TLS certificate, you will need a valid TLS certificate in your certificate bundle.

To use a certificate bundle it must include;

- the client certificate
- the matching private key
- the CA certificate that was used to sign the client certificate
- (Conditional) If the private key in your certificate bundle is encrypted, you will need the client certificate password.

For more information on preparing your TLS certificates for use with the Splunk platform, see How to prepare TLS certificates for use with the Splunk platform in *Securing Splunk Enterprise*.

To add a TLS certificate for your Universal Forwarder, or to edit the TLS configuration, do the following steps:

1. From the **Home** menu, select **Administration**, **Administration Settings**, **Forwarder Settings**.
2. On the **Forwarder Settings** page, click the edit icon on the right-hand end of the forwarder group's entry.
3. Click the **Certificate configuration** tab.
4. Add your client certificate bundle either by dragging and dropping it onto the box provided, or by clicking the box and navigating to the bundle on your filesystem.
    1. (Conditional) If your Client certificate bundle includes an encrypted private key, type your client certificate password in the **Client certificate password** box.
5. Add your TLS certificate by dragging and dropping the certificate onto the box provided, or by clicking the box and navigating to the certificate on your filesystem.
6. (Optional) Select options as needed:

    1. Verify server certificate
    2. Verify server name
    3. Use client SSL compression
7. (Optional) If you use common names or Subject Alt names for your servers, add them as comma-separated lists to the **Allowed common names** or **Allowed Subject Alt names** fields.
8. Click **Save**.

Reindexing

You can reindex all of your Splunk SOAR (Cloud) data.

Reindexing will send all your SOAR data to your Splunk Enterprise or Splunk Cloud Platform deployment again, which can result in duplicated data. To prevent duplicates, make sure to delete existing objects from all forwarder groups before reindexing. See How indexing works in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

To reindex your Splunk SOAR (Cloud) data, do these steps:

1. From the **Home** menu, select **Administration**, **Administration Settings**, **Forwarder Settings**.
2. From the **Forwarder Settings** screen, select the **Reindex** tab.
3. Use the dropdown menu to select the data type you would like to reindex.
4. (Optional) Set a start time from which to reindex data.
5. (Optional) Set an end time, after which data should not be reindexed.
6. Click **Reindex**.

Data types and corresponding indexes

This table shows the connection between the forwarded Data type and the index it corresponds to in Splunk Enterprise or Splunk Cloud Platform.

Splunk SOAR Data type	Index in Splunk Enterprise/Splunk Cloud Platform
Action run	phantom_action_run
App	phantom_app
App run	phantom_app_run
Artifact	phantom_artifact
Asset	phantom_asset
Audit log	_audit
Container	phantom_container
Container attachment	phantom_container_attachment
Container comment	phantom_container_comment
Custom function	phantom_custom_function
Custom list	phantom_decided_list
Note	phantom_note
Playbook	phantom_playbook
Playbook run	phantom_playbook_run You must create this index before forwarding data.

Splunk SOAR Data type	Index in Splunk Enterprise/Splunk Cloud Platform
SOAR logs	splunk_app_soar
Splunk addon for Linux logs	os

Configure forwarding a data type to a specific Splunk index

Do the following steps to change or customize the target Splunk Cloud Platform or Splunk Enterprise index for a data type.

1. From the **Home** menu, select **Administration**, then select **Administration Settings**, then **Forwarder Settings**.
2. From the **Forwarder Settings** page, click the **Settings** button.
3. Type the Splunk Cloud Platform or Splunk Enterprise index in the input box next to the data type you want to customize.
4. When your customizations are complete, click the **Submit** button.

You must make sure the target index exists in your Splunk Cloud Platform or Splunk Enterprise deployment before you change the setting in Splunk SOAR (Cloud).

See Also

For more information about getting data into Splunk Enterprise or Splunk Cloud Platform see these additional resources.

- What data can I index? in the Splunk Enterprise *Getting Data In* manual.
- Use forwarders to get data into Splunk Cloud Platform in the Splunk Enterprise *Getting Data In* manual.
- Use forwarders to get data into Splunk Enterprise in the Splunk Enterprise *Getting Data In* manual.
- Set up the universal forwarder using Splunk SOAR version 6.2.0 and later in the *Install and Configure Splunk App for SOAR* manual.
- How to prepare TLS certificates for use with the Splunk platform in the *Securing Splunk Enterprise* manual.

Customize your forwarder configuration

This topic covers customizations or additional configurations you can use when setting up forwarders for your Splunk SOAR (Cloud) deployment.

Use an HTTP load balancer for your Splunk SOAR (Cloud) forwarders

It is possible to configure the universal forwarders for your Splunk SOAR (Cloud) to use an HTTP load balancer.

You may either use Splunk to Splunk (S2S) service over TCP or HTTP forwarders on your deployment, not both. If you already have a forwarder group using the S2S service over TCP, you will need to remove it before you can configure an HTTP forwarder group.

Before you configure an HTTP forwarder group, you will need to obtain an HEC token from your Splunk Enterprise or Splunk Cloud Platform administrator. See Set up and use HTTP Event Collector in Splunk Web in *Getting Data In*.

To add an HTTP forwarder group, follow these steps:

1. From the **Home** menu, select **Administration,** then **Administration Settings**. Then select **Forwarder Settings**.
2. Select **+New Group**.
3. Select the HTTP forwarder type.

   You cannot create an HTTP forwarder group if you have an existing TCP forwarder group.
4. In the **Add a new forwarder group** dialog do the following:
   1. In the **Name** field, type a name for your forwarder group. This name is displayed on the **Forwarder Settings** page.
   2. Add your HEC token to the **HEC token** field.
   3. In the **Indexer** field, add the address for your for your HTTP load balancer. HTTP forwarders can only have a single indexer set.
   4. Select the Data types you want to ingest into Splunk Cloud Platform or Splunk Enterprise.
5. If you do not want to test the connection before the configuration is saved, check the **Skip connection check** box.
6. Make sure the **Enabled** slider button is in the on position.
7. Click **Save**.

After you complete these steps, data will begin to stream from Splunk SOAR (Cloud) to your Splunk Enterprise deployment through your load balancer.

Adding TLS configuration to your HTTP forwarder group

You can add TLS certificate configuration for a HTTP forwarder group the same way as you would for a TCP forwarder group.

1. On the **Forwarder Settings** page, click the edit icon on the right-hand end of the forwarder group's entry.
2. Click the **Certificate configuration** tab.
3. Add your client certificate bundle either by dragging and dropping it onto the box provided, or by clicking the box and navigating to the bundle on your filesystem.
4. (Conditional) If your Client certificate bundle includes an encrypted private key, type your client certificate password in the **Client certificate password** box.
5. Add your TLS certificate by dragging and dropping the certificate onto the box provided, or by clicking the box and navigating to the certificate on your filesystem.
6. (Optional) Select options as needed:
   - Verify server certificate
   - Verify server name
   - Use client SSL compression
7. (Optional) If you use common names or Subject Alt names for your servers, add them as comma-separated lists to the **Allowed common names** or **Allowed Subject Alt names** fields.
8. Click **Save**.

For more information on configuring universal forwarders to use HTTP, see Configure the universal forwarder to send data over HTTP in the *Forwarder Manual*.

Configure Google Maps for visual geolocation data

The MaxMind app provides a `geolocate_IP` action that uses Google Maps functionality to show a world map with a marker indicating the approximate location of the IP under investigation. You must provide a Google Maps API key to enable this functionality. See the Maps JavaScript API page in the Google Maps Platform documentation for more information about obtaining a Google Maps API key.

After obtaining an API key, perform the following steps:

1. From the **Home** Menu, select **Administration**.
2. Select **Administration Settings > Google Maps**.
3. Enter your API key into the field.
4. Click **Save Changes**.

With a proper API key applied, MaxMind Geolocate IP displays a map with searches.

Manage your organization's credentials with a password vault

Use credential vaults to centrally manage and monitor credential usage in your organization. Splunk SOAR (Cloud) supports the following password vaults:

- CyberArk Vault Privileged Access Manager
- Hashicorp Vault
- Thycotic Secret Server

As an administrator, you can configure Splunk SOAR (Cloud) to retrieve credentials from these vaults and use them with in assets.

- When used in conjunction with the Splunk SOAR Automation Broker, the Automation Broker will authenticate directly with your supported privileged access manager and retrieve credentials to use with assets.
- If an asset is configured on the Splunk SOAR instance and does not require the Automation Broker, then Splunk SOAR will authenticate with the supported privileged access manager and retrieve credentials to use with assets.

Use CyberArk Vault Privileged Access Manager with Splunk SOAR (Cloud)

Integrate Splunk SOAR (Cloud) with CyberArk's Vault cloud-based Privileged Access Manager feature to retrieve passwords or other fields for assets. This allows you to utilize CyberArk account management features to change passwords on managed products and services without having to manually update Splunk SOAR (Cloud) assets after a password change.

Before you begin, you need to be or be working with your organization's CyberArk administrator. Collect the following items:

- The URL to your organizations CyberArk Vault.
- Your organizations CyberArk Vault username and password.
- The pkcs12 certificate and certificate password for your organizations CyberArk Vault.
    - This certificate file must be located on the Splunk SOAR (Cloud) file system.

To use CyberArk Vault with Splunk SOAR (Cloud), perform the following steps:

1. From the main menu, select **Administration**.
2. Select **Administration Settings**, then **Password Vault**.
3. In the **Manager** field, select **CyberArk Vault**.
4. Type the entries for the following fields:
    1. URL
    2. Username
    3. Password

    4. Certificate password
5. Upload your certificate file:
    1. Click **Choose File** then select the pkcs12 certificate file from your filesystem.
6. Click **Save Changes**.

Use Hashicorp Vault with Splunk SOAR (Cloud)

Splunk SOAR (Cloud) supports Hashicorp Vault's KV store REST API version 2.

To use Hashicorp Vault with Splunk SOAR (Cloud), perform the following steps:

1. From the main menu, select **Administration**.
2. Select **Administration Settings**, then **Password Vault**.
3. In the **Manager** field, select **Hashicorp Vault**.
4. Get the URL and Token from your Hashicorp administrator.
5. Select the **Verify server certificate** check box to verify that the HTTPS certificate is trusted.
6. Click **Save Changes**.

Once you have Hashicorp access configured, you need to know the paths and names of the secrets you want to use from the Hashicorp Vault.

Use Hashicorp Vault to provide credentials with assets

You can use Hashicorp to automatically supply credentials when working with assets.

1. From the main menu, select **Apps**.
2. In the list of apps, find one to configure such as the Palo Alto Networks Firewall and click **Configure New Asset**.
3. Open the **Asset Settings** tab for that asset.
4. Click **Advanced** to expand the advanced configuration section.
5. In the Credential Management section, select the fields you want to get from Hashicorp Vault, and the path and key to use. For example, you can specify /**secret/autofocus** in the Path field and **apikey** in the Key field to retrieve an API key used to authenticate to the AutoFocus service.
6. Click **Save**.

Use Thycotic Secret Server with Splunk SOAR (Cloud)

Splunk SOAR (Cloud) can use Thycotic's API to access secrets managed by Secret Server. Usernames and passwords can be stored in Thycotic Secret Server for both users and assets which require a login to use.

Splunk SOAR (Cloud) does not support Delinea Secret Server, a product which replaces Thycotic Secret Server.

In order for Splunk SOAR (Cloud) to use secrets managed by Thycotic Secret Server you must provide:

- The URL to your organization's Thycotic Secret Server. You only need to include a port number in the URL if the Thycotic Secret Server is unreachable without a port number. Certain network and server configurations might require you to include port numbers in the URL.`https://<your.organization's.secret.server>:<port number>`
- The username and password of the account which will retrieve secrets using the API.
- Optional: The Organization ID set in Secret Server for use in the Thycotic Secret Server API.

These values are used to make an oauth2 token for Thycotic Secret Server. Once authenticated, Splunk SOAR (Cloud) uses the `SearchSecretsByFolder` API to access the managed secrets.

Set the login secret in Thycotic Secret Server

You must set up the login information in Secret Server before you can use it to access Splunk SOAR (Cloud). For more information on Thycotic Secret Server, see the documentation on the Thycotic website.

1. Create the required folders.
2. Use the **Create Secret** widget, selecting the template as **Password**.
3. Enter the required items in the mandatory fields of **secret** and **Password**.

Set the Thycotic Secret Server settings in Splunk SOAR (Cloud)

Add the required information to create the oauth2 token for Thycotic Secret Server in Splunk SOAR (Cloud)'s administration settings. This token is for connecting to Thycotic Secret Server.

1. From the Main Menu, select **Administration**.
2. Select **Administration Settings** > **Password Vault**.
3. Select **Thycotic Secret Server** from the drop-down list in the **Manager** field.
4. Set the URL fpr your Thycotic Secret Server instance.
5. Specify the username and password Splunk SOAR (Cloud) will use to access secrets.
6. Optional: Set the organization id.
7. Click **Save Changes**.

If you have assets that require logins, and those logins are managed by Thycotic Secret Server, then you must set credential management in the asset's configuration, in **Apps** > **<Asset Name>** > **Asset Settings** > **Advanced**.

Set global environment settings for Splunk SOAR (Cloud)

You can set and manage settings that will apply to the Splunk SOAR (Cloud) environment, such as a global environment variable or the global action limit.

Set global environment variables

You can set environment variables that apply globally across the Splunk SOAR (Cloud) runtime environment to manage proxies or other features. You can also override or provide these variables on a per-app basis in the app advanced configuration. Changes to global environment settings will not be applied until the Splunk SOAR (Cloud) platform is restarted.

To make changes to the global environment:

1. From the Splunk SOAR (Cloud) main menu, select **Administration**.
2. Click **Administration Settings > Environment Settings**.
3. Click **+Variable** to add a new environment variable.
4. In the **Name** field, specify **HTTP_PROXY**, **HTTPS_PROXY**, or **NO_PROXY** depending on the type of proxy connection. These environment variables are read by all Splunk SOAR (Cloud) processes and affect the entire product including external search connections, app and asset connections, and requests made from within playbooks.

These variable names are case sensitive and must be entered as HTTP_PROXY, HTTPS_PROXY, or NO_PROXY.

5. In the **Value** field, include the following depending on the type of proxy configuration. Wildcards are not supported.
    1. HTTP and HTTPS proxy configurations: protocol, hostname or IP address, and the port of the proxy server. For example, `<protocol>://<hostname/IP>:<port>`
    2. NO_PROXY configurations: IP address, hostname, or domain of the asset.
    3. (Conditional) If the proxy server requires authentication, consider the following items:
        - `<scheme>://[<username>[:<password>]@]<host>[:port]>` is the scheme (http or https), optional username and password, host name or IP address, and optional port number used to connect to the proxy server.
        - The scheme and host are required.
        - If using a proxy server that requires authentication Splunk SOAR (Cloud) may need a service account on the proxy server.
        - If authentication credentials (username/password) are specified, the "secret" box should be selected so that the username and password are stored in encrypted format.
        - If port is not specified it defaults to port 80 when the scheme is http, and port 443 when the scheme is https.
6. Check **Secret** to encrypt the **Value** field and stop it from being displayed.

When configuring the system to use an HTTP or HTTPS proxy, Splunk SOAR (Cloud) requires that you except calls to the loopback interface from the proxy list. You must set the environment variable NO_PROXY to include 127.0.0.1, localhost, and localhost.localdomain so that REST calls can be made on the loopback interface without being diverted to the proxy.

Apply environment variables to individual assets

You can also apply environment variables to configured assets individually. If you are using NO_PROXY, the asset configuration takes precedence over the global environment variable. However, if you are using HTTPS_PROXY, the global environment variable takes precedence over the asset configuration. For more information, see Add and configure apps and assets to provide actions in Splunk SOAR (Cloud).

Set the global action concurrency limit

The global action concurrency limit designates the maximum number of concurrent actions across all assets on the Splunk SOAR (Cloud) platform.

- The default setting is 50 concurrent actions on the SOAR platform.
- Cisco Talos connector, Splunk Enterprise Security (Mission Control), and SMTP each have a concurrency limit of 50.
- The Splunk Automation Broker has a limit of 50 concurrent actions per broker. Setting a higher limit of concurrent actions on the broker than on the platform has no effect.

When changing the global action limit, ensure the existing action limits set on all of your assets is still within the new global limit. Use caution when changing the global action limit as it can significantly affect performance.

To change the local concurrent action limit in Splunk SOAR (Cloud), follow these steps.

1. From the **Home** menu, select **Administration**.

2. Click **Administration Settings > Environment Settings**.
3. Enter your desired action limit in the box. Use caution when changing this limit because doing so can have a significant effect on performance.
4. Click **Save Changes**.

To change the local concurrent action limit in the Automation Broker, follow these steps.

1. Edit brokerd.conf by either:
   - navigating to your data directory on the Docker host operating system.
   - by logging into the Automation Broker container to edit the file in the /broker directory.

   See Change Splunk SOAR Automation Broker settings by editing brokerd.conf in *Set Up and Manage the Splunk SOAR Automation Broker*.
2. Set the value for `global_concurrency_limit` to the desired value.
3. Save and exit the file.
4. Restart the Automation Broker. See Interact with the Splunk Automation Broker in *Set Up and Manage the Splunk SOAR Automation Broker*.

See also

Concurrent actions limits can be controlled at the app or connector level and on individual assets. You can also change the number of concurrent actions the Automation Broker allows by editing the brokerd.conf file on the Automation Broker container.

- For information on controlling action concurrency in an app or connector's configuration metadata, see Action Section: Synchronization in *Develop Apps for Splunk SOAR (Cloud)*.
- For information on setting concurrent actions for a specific asset, see Set the concurrent action limit.
- For information on disabling action concurrency see, Disable action lock or action concurrency.
- Concurrent action for the Automation Broker are controlled by the brokerd.conf file on the Automation Broker. See Change Splunk SOAR Automation Broker settings by editing brokerd.conf in *Set Up and Manage the Splunk SOAR Automation Broker*.

Add tags to objects in Splunk SOAR (Cloud)

Add tags to objects in Splunk SOAR (Cloud) to help you perform the following tasks:

- Search for objects in Splunk SOAR (Cloud)
- Flag objects for other users
- Automation and workflow operations
- Affect the flow of playbooks

You can also require tags before a container can be closed. See Configure how events are resolved for more information.

Required user privileges to view, add, edit, or delete tags in Splunk SOAR (Cloud)

To view the Tags page, a user must have a role with the View System Settings privilege. To add, edit, or delete tags on the Tags page, a user must have a role with the Edit System Settings privilege.

Editing the tags on individual containers, artifacts, or assets requires a role with the matching Edit Containers, Edit Artifacts, or Edit Assets privileges. However, a user with the combination of View System Settings and Edit System

Settings privileges can use the Tags page to delete or rename tags regardless of the object they are applied to, even without the edit privileges for those objects.

View tags in your Splunk SOAR (Cloud) instance

To view the Tags page, a user must have a role with the View System Settings privilege.

Perform the following steps to access the Tags page and view the existing tags in your Splunk SOAR (Cloud) instance:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings > Tags**.

Add a new tag to Splunk SOAR (Cloud)

To add a new tag to Splunk SOAR (Cloud), perform the following steps:

1. On the Tags page, click **+ Tag**.
2. Enter a new tag name.
3. Click **Create**.

Tags can be added on individual objects by editing or creating that object in Splunk SOAR (Cloud) and typing them into the Tags field. For example, to create a new tag for a container in Splunk SOAR (Cloud), do the following:

1. Navigate to the container.
2. Click **Event Info** to expand the section.
3. In the Tags field, enter the name of a new tag you want to associate with the container.

Edit existing Splunk SOAR (Cloud) tags

Renaming a tag affects all objects in Splunk SOAR (Cloud) currently using that tag. All containers, artifacts, or assets in Splunk SOAR (Cloud) with the existing tag name are updated to use the new tag name.

To edit an existing tag, perform the following steps:

1. On the Tags page, click the edit icon for the tag. If the existing tag is already in use by another Splunk SOAR (Cloud) component, its usage is summarized in the Edit Tag window. Review this information and make notes of where you must update the tag in Splunk SOAR (Cloud) to keep your playbooks operational.
2. Modify the name of the tag as desired.
3. Click **Save**.

Delete a tag in Splunk SOAR (Cloud)

A tag exists in Splunk SOAR (Cloud) as long as at least one object still uses that tag. If you remove a tag from all objects or delete all those objects, the tag no longer shows on the Tags page. Deleting a tag affects all objects in Splunk SOAR (Cloud) currently using that tag. The deleted tag is removed from all containers, artifacts, or assets in Splunk SOAR (Cloud) currently using the tag.

To delete an existing tag, perform the following steps:

1. On the Tags page, click the delete icon for the tag.
   If the existing tag is already in use by another Splunk SOAR (Cloud) component, its usage is summarized in the Delete Tag window. Review this information before you proceed.
2. Click **Delete**.

Create custom CEF fields in Splunk SOAR (Cloud)

Splunk SOAR (Cloud) uses the Common Event Format (CEF). CEF is a system of key-value pairs for important pieces of information about an artifact.

An artifact might have several key pieces of information such as `sourceAddress`, `sourcePort`, `destinationAddress`, `destinationPort`, and a `timestamp`. Each of these is stored in a field.

You can only have one of each CEF field per artifact. For example, you cannot have more than one `sourceAddress` per artifact. If you have a data set that includes multiple `sourceAddress` entries, separate those into multiple artifacts. Each of those artifacts can be placed in the same container.

You can extend or customize CEF to meet your organization's needs by adding custom CEF fields, and then using these fields in Investigation, adding them to artifacts with the REST API, or using them in playbooks.

When an artifact is edited from Investigation, values set for a custom CEF appear as indicators. You can view these indicators by selecting **Indicators** in the **Home** menu.

You can add, delete, or modify a custom CEF using the REST API.

Create a custom CEF field

Perform the following steps to create a custom CEF field:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **CEF**.
3. Select **+ CEF**.
4. Type a name for your customized CEF.
5. (Optional) Select a data type for the field from the dropdown list.
   Available choices are prepopulated with all enabled Apps actions. You can add your own data type or leave the data type blank.
6. Select **Save**.

Modify a custom CEF field

Perform the following steps to modify a custom CEF field:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **CEF**.
3. Select the edit icon to the right of the CEF name.
4. Make the desired changes.
5. Select **Save.**

Delete a custom CEF field

Perform the following steps to delete a custom CEF field:

1. From the **Home** menu, select **Administration**.
2. Select **Administration Settings**, then **CEF**.
3. Select the icon to the right of the custom CEF field name.

Deleting a custom CEF does not remove it from existing artifacts that have the field applied.

Configure product settings for your Splunk SOAR (Cloud) instance

View related data using aggregation rules

Define aggregation rules to view related data in a single location. Artifacts matching a defined rule are copied to a new container.

To view aggregation rules, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings** > **Aggregation**.

The Aggregation page shows a list of all container labels defined on your system. The number inside the parentheses next to each label is the number of rules defined for that label.

Container labels can be created by an ingestion asset or manually from **Home** > **Administration** > **Event Settings**. For example, you can choose a source label from an ingestion asset like the "Events" label or an "Email" label, then create a destination label such as "Aggregated Events" that makes it clear that containers with that label are aggregated.

Add a new aggregation rule

As an example, you may want to aggregate all containers with matching `sourceAddress` CEF fields from your "email" label into your "events" label.

To create the example aggregation rule:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings** > **Aggregation**.
3. From the Aggregation page, click **+ Aggregation Rule**.
4. Specify **sourceAddress - Email to Events** as the name of the rule.
5. Select **email** from the drop-down list in the **Source Label** field.
6. Select **events** from the drop-down list in the **Destination Label** field.
7. Select **Exact** from the **Match** field to aggregate on the exact contents of the CEF field. You can click on the plus (+) icon to add additional match rules.
8. Select **sourceaddress** in the CEF field. You can start typing the field name to search through the list of available field names.
9. Click **Save**.

Edit an existing aggregation rule

After completing the previous example, perform the following steps to edit an existing aggregation rule in Splunk SOAR (Cloud).

1. Click on any existing rule. In this example, click **email** to view a summary of the aggregation rule.
2. Click **Edit** to make changes to the rule.
3. Click the trash can icon to remove the rule.

Click **+ Aggregation Rule** to create a new rule. If you create a new rule from the email label rule page, the new rule will automatically populate the Source Label field with email.

Using multiple matches in an aggregation rule

An aggregation rule can have multiple match lines, such as a match on both `sourceaddress` and `destinationaddress`.

For this example, both the `sourceaddress` and `destinationaddress` must match for it to be aggregated into the same container.

If you treat `sourceaddress` as the attacker's IP address, and `destinationaddress` as the target's IP address, then this means you have artifacts being aggregated in the same destination container for only the exact same attacker and victim. So with a target IP address of 1.1.1.1, there is one destination container for attacker IP address 2.2.2.2 and target IP address 1.1.1.1, and a different container for attacker IP address 3.3.3.3 and target IP address 1.1.1.1.

> CEF fields are matched even if there is no value. For example, if you have artifacts with a destinationaddress of 1.1.1.1 and no sourceaddress, they are still aggregated together into a destination container.

Manage automation brokers

This page allows you to manage your Splunk SOAR Automation Brokers from within Splunk SOAR (Cloud).

Your connected Automation Brokers are displayed as a table on this page.

- Columns may be sorted by clicking the column header.
- Use the ellipsis (...) menu at the end of each row to manage the listed automation broker.

Add a Splunk SOAR Automation Broker

Before you begin, see Prepare to install the Splunk SOAR Automation Broker in the manual *Set Up and Manage the Splunk SOAR Automation Broker*.

1. From the **Home** menu, select **Administration**, then **Product Settings**, then **Automation Broker**.
2. Use the **+AUTOMATION BROKER"' button to add a new Splunk SOAR Automation Broker.**
    1. Once the Splunk SOAR Automation Broker is installed on your container host, type the encryption key for the automation broker into the input box for **Step Two**.
    2. Type the authorization code from the automation broker into the input box for **Step Three**.
    3. Type a name form the automation broker, this name will appear in the table on the Automation Broker page in Splunk SOAR (Cloud).
    4. Select the button marked **Complete**.

For complete information on the Splunk SOAR Automation Broker, see About Splunk SOAR Automation Broker in the manual *Set Up and Manage the Splunk SOAR Automation Broker*.

Connectors

Use this page to manage the settings for connectors.

SOAR connector version checking

This setting controls whether or not Splunk SOAR (Cloud) checks a connector's metadata for a minimum "phantom version" field when installing that connector.

To toggle SOAR connector version checking do the following:

1. From the **Home** menu, select **Administration**, then select **Product Settings**, then select **Connectors**.
2. Toggle the switch labeled **Enable Check SOAR Connector Version** to either the **ON** or **OFF** setting.

Manage dashboard widgets in Splunk SOAR (Cloud)

You can customize your Splunk SOAR (Cloud) dashboard with various widgets. Widgets like Events by Status, Data Sources, and SLA Average are helpful to see at a glance. Dashboard widgets can also be resource intensive. To optimize performance, you might choose to make some widgets active and make other widgets inactive. When widgets are set to inactive, their data is not calculated or displayed on the dashboard.

The settings described in this article are for your dashboard only, when you are logged in with your user name. They do not apply to other users.

To specify active and inactive widgets, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings**, then **Manage Widgets**.
3. Turn on widgets that you want to appear on the dashboard with their associated data. Turn other widgets off.

To save more room on the dashboard, follow these steps:

1. View the dashboard. If you are not already there, from the main menu, select **Home**.
2. Locate the widgets you set to inactive. Their data is not displayed, but they still have space on the dashboard.
3. For each widget, select the gear icon and select either **Collapse** to minimize the space or **Remove** to remove the widget entirely. If you want to restore the widget, continue to the next section.

To restore widgets removed from the dashboard, follow these steps:

1. On the dashboard, select **Configure**.
2. For any widgets that you want to display, select **On**. Then select **Close**.

Enable clickable URLs in CEF data

When a Common Event Format (CEF) field on an artifact contains URL data, the user interface can display a clickable link for it.

- Use this setting to toggle whether clickable links are shown.
- Only CEF values generated by automation or included in an artifact are controlled by this setting.
- Since many URLs in CEF values are likely to be malicious, the default is **Off**.

Notes can contain URL data, and those URLs will be clickable unless they are escaped using the backtick or grave character (`). URLs in notes are not controlled by this setting.

Example:

```
`http://some.malicious.url.com`
```

Define tasks using workbooks

Workbooks are lists of standard tasks that analysts follow when they 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 or cases, or cases that start out as one type of incident but end up to be a different type of incident.

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

See Define a workflow in a case using workbooks in *Use Splunk SOAR (Cloud)* for information about how to use workbooks in a Splunk SOAR (Cloud) workflow.

Create a Splunk SOAR (Cloud) workbook

Perform the following tasks to create a new workbook in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings > Workbooks**.
3. Click **+ Workbook**.
4. Enter a name for your workbook.
5. (Optional) Enter a long description for your workbook.
6. Configure at least one phase for your workbook. A workbook can have multiple phases.
    1. Enter a name for the phase.
    2. (Optional) Configure a service level agreement (SLA) for the phase. See Configure service level agreements in a workbook.
    3. Click the arrow next to **Task Name** to expand the section.
    4. Enter a name for the first task in the phase. You can have multiple tasks within each phase.
    5. (Optional) Assign an owner or role to the task. See Notify task owners when they are assigned to a task.
    6. (Optional) Enter a long description or instructions for this task.
    7. (Optional) Configure an SLA for this task. The SLA must be shorter in length than the SLA for the phase.
    8. (Optional) Click **Actions** to select actions you want to run when this task is performed.
    9. (Optional) Click **Playbooks** to select playbooks you want to run when this task is performed.
    10. (Optional) Click **Add Task** to configure additional tasks for the phase.
7. (Optional) Click **Add Phase** to configure additional phases for the playbook.
8. Click **Save**.

Edit an existing Splunk SOAR (Cloud) workbook

Changes to a workbook only apply to future uses of the workbook. For example, if you change the SLA of a phase or add or remove a phase or task, the change is not reflected in any Splunk SOAR asset currently using the workbook.

To edit an existing workbook, do the following:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings > Workbooks**.
3. Click on a workbook name to see the read-only summary of that page.
4. Use the drop-down list to expand the descriptions.
5. Click **Edit** to go to the workbook editing page.
6. Make the desired changes.

7. Click **Save**.

Reorder phases in a workbook

Suppose you need to add a phase to the middle of a series of phases in an existing workbook. New phases are added to the end by default, so you need to reorder the phases to place the new phase in its desired location.

Perform the following tasks to reorder a phase:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings > Workbooks**.
3. Click on a workbook name to see the read-only summary of that page.
4. Use the drop-down list to expand the descriptions.
5. Click **Edit**.
6. Click **Reorder Phases**.
7. Enter the new phase at the bottom.
8. Click the three horizontal lines next to the phase and drag it to the order you want.
9. Click **Done Reordering**.
10. Click **Save**.

Configure service level agreements in a workbook

Service level agreements (SLAs) represent the default amount of time until a phase or task is due. You can adjust the time values to reflect your organization's requirements. The SLAs for phases and tasks are different from the SLAs that are set globally per severity across the entire platform.

Separate from severity SLAs, the phase and task SLAs allow for greater granularity when operating at the phase or task level. See Create additional custom severity names for more information about global SLAs and response settings.

The SLA time is tracked in minutes, days, or hours. It is based on the `start_time` timestamp when the phase or task is started and the `end_time` timestamp when the phase or task is completed. Each phase can have a total SLA that covers all the subtasks, or each task can have an individual SLA. However, if both the phase and task SLAs are used, there is no automatic validation to confirm that the phase SLA is greater than or equal to the total of all its subtask SLAs.

The owner of the phase or task sees SLA status messages in Investigation. You can also see the status of the current phase in the Summary View or in Analyst View, which is found under the Workbook tab. You can review if the SLAs are exceeded, how many tasks are completed, and how many of those tasks were completed on time.

To edit the phase or task SLA for the workbook, do the following:

1. From the **Home** menu, select **Administration**.
2. Select **Product Settings > Workbooks**.
3. Click on a workbook name to see the the read-only summary of that page.
4. Use the drop-down list to expand the descriptions.
5. Click **Edit** to go to the workbook editing page.
6. Change the Phase SLA or from the Task Name drop-down list, in the Task SLA field, revise the time in which to complete the task.
7. Click **Save**.

Notify task owners when they are assigned to a task

You can notify owners that a workbook task is assigned to them. The table summarizes the methods.

Method of notification	Description
Email	When you assign a task to a role, Splunk SOAR (Cloud) sends an email notification to every member of the role. When a specific user assigns that task to themselves, the new owner and the previous owner both get an email notification.
In-product	When you assign a task to a role, every member of the role sees a bell notification in the Splunk SOAR (Cloud) menu bar. When a specific user assigns that task to themselves, the bell notification disappears for all other members of the role.

Configure settings for your Splunk SOAR (Cloud) system's events

Create custom status labels in Splunk SOAR (Cloud)

You can create additional status labels for the events and cases in Splunk SOAR (Cloud) as needed for your business processes.

Statuses are grouped into three categories: New, Open, and Resolved. You can create up to 30 total status labels in Splunk SOAR (Cloud).

Status label rules

Status labels must adhere to the following rules:

- At least one status label must exist for each of the status categories.
- Only ASCII characters a-z, 0-9, dash (-), or underscores (_) are allowed.
- The name cannot exceed 128 characters in length.
- The labels New, Open, and Closed are available upon upgrade. These three labels can be deleted, removing them from the active list. These labels cannot be renamed because they are required for backwards compatibility with apps and playbooks.

To maintain backwards compatibility with apps and existing playbooks, if the status labels New, Open, or Closed have been deleted, ingestion apps and the REST API can still assign the statuses New, Open, and Closed to containers.

Create a status label in Splunk SOAR (Cloud)

To create a status label, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings > Status**.
3. Click **Add Item** in the status category where you want to create the new status label.
4. Type the new status name. The status label name must adhere to the status label rules described earlier.
5. Click **Add Item**.

To reorder status labels, drag the handle ( ) on the left side of the status label's input box to the desired position.

To delete a status label, click the circled x ( ) to the right of the status label's input box.

To set the status label used as the default label for that status type, select the desired label from the drop-down list in the **Default status** field.

Create custom severity names and control severity inheritance

Severity defines the impact or importance of an event or case. Different severity names have different assigned service level agreements in the Response page. Splunk SOAR (Cloud) ships with three predefined severity names: High,

Medium, and Low. You can create additional severity levels and also control whether the severity level of a container changes based on the severity level of a newly added artifact.

Create a severity level in Splunk SOAR (Cloud)

Your organization might need additional levels of severity to match your business processes. Additional severity names can be defined by a Splunk SOAR (Cloud) administrator.

You can create up to 10 severities in Splunk SOAR (Cloud). To create a severity, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings**, then **Severity**.
3. Click **Add Item**.
4. Enter the severity name and select a color from the drop-down list. The severity name must adhere to the following conditions:
    - Only ASCII characters a-z, 0-9, dash (-), or underscores (_) are allowed.
    - The name cannot exceed 20 characters in length.
5. Click **Done**.

Severity names cannot be edited. To change a severity name, delete it and recreate the severity name. To reorder severity names, drag the handle ( ) on the left side of the severity name's input box to the desired position.

To set the severity name used as the default severity, select the desired name from the drop-down list.

Delete a severity name in Splunk SOAR (Cloud)

To delete a severity name, click the circled x ( ) to the right of the severity name's input box. Take note of the following Splunk SOAR (Cloud) behaviors before you delete a severity:

- The severity label set as the default severity cannot be removed until a new default is selected.
- Deleting a severity name does not change the severity of a case, event, or artifact. Changing a severity name does not update closed events, cases, or artifacts.
- Deleted severity names appear in search results as strikethrough text.
- Severity names are stored in Splunk SOAR (Cloud)'s internal database. Deleting a severity name from the active severity list does not remove that severity name from the database.
- To maintain backwards compatibility with apps and existing playbooks, if the severity names High, Medium, or Low have been deleted, ingestion apps and the REST API can still assign the severity High, Medium, and Low to events, containers, or artifacts.
- Deleting custom severity names that you have previously shared with other Splunk apps might result in additional steps in communication between Splunk SOAR (Cloud) and the other app.

Inherit severity level from new artifacts

You can choose whether a container inherits the severity level from a newly added artifact.

To select whether the severity levels of containers updates based on artifacts, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings**, then **Severity**.
3. Choose the setting for the **Update the container severity to match the new artifact** toggle:

- Toggle on: Severity of the container updates if a newly added artifact has a higher severity than the current container. The container severity is not affected if the newly added artifact has a severity lower than the current container.
- Toggle off: Severity of the container does not change, regardless of the severity of a newly added artifact.

Create custom fields to filter Splunk SOAR (Cloud) events

Create custom fields that can be added to containers in Splunk SOAR (Cloud). You can use custom fields to match your business processes, or to help filter containers, events, or cases for extra attention. For example, you might add a custom field named **Department** and assign it a list of values for each department in your organization (for example, IT Ops, Sales, and Business).

Custom fields are searchable. For more information on using the search feature, see Search within Splunk SOAR (Cloud) in *Use Splunk SOAR (Cloud)*.

Using custom fields in playbooks requires special coding, as described in Update and read custom field values later in this article. Custom field names described here require additional special handling, so plan your naming convention carefully:

- names containing characters other than letters, numbers, or underscores (_)
- names starting with a space

When choosing a name for a new custom function, do not use the same name as a field that already exists in Splunk SOAR, like name or severity.

Create a custom field

To create a custom field, follow these steps:

1. From the **Home** menu select, **Administration**.
2. Select **Event Settings**, then **Custom Fields.**
3. Select **Add Field**.
4. Enter a field name.
5. Select a field type. If you choose **select**, provide additional values in the **Values** field. These values are presented to the user in a drop-down list when working in a container.
6. (Optional) Select **Require on Resolve** to make the field required before a container can be closed or resolved.
7. (Optional) Select **Add Field** to add additional fields.
8. Select **Save Changes**.

Edit custom fields

To edit a custom field, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings**, then **Custom Fields.**
3. Find the item you want to edit and make your changes. In the **Values** field for select types, you can enter an additional value or select the X icon to remove existing values.
4. Optionally select **Require on Resolve**, if appropriate.
5. Select **Save Changes**.

Delete a custom field

You can remove a custom field entirely. To remove a custom field, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings**, then **Custom Fields.**
3. Locate the field you want to remove.
4. Select the circled x ( ) icon at the end of the field's entry.
5. Select **Save Changes**.

Update and read custom field values

To update custom field values in containers, use the following code examples with the container.update API :

Update a custom field value

Example code to update a custom field value from a container.

```
outputs = {}

# Write your custom code here...
container = {"id": container_id}
update = {
    "custom_fields": {
        field_name: field_value,
    },
}

# Make the HTTP request
success, message = phantom.update(container, update)

assert success, message

# Return a JSON-serializable object
assert json.dumps(outputs)  # Will raise an exception if the :outputs: object is not JSON-serializable
return outputs
```

Read a custom field value

While not technically an update function, reading a custom field value also uses the container.update API.

Example code to read (get) a custom field value from a container.

```
outputs = {}

# Write your custom code here...
container = phantom.get_container(container_id)
custom_fields = container.get("custom_fields", {})
outputs["field_found"] = field_name in custom_fields
outputs["field_value"] = custom_fields.get(field_name)

# Return a JSON-serializable object
assert json.dumps(outputs)  # Will raise an exception if the :outputs: object is not JSON-serializable
```

```
return outputs
```

Filter indicator records in Splunk SOAR (Cloud)

When you first install Splunk SOAR (Cloud), industry-standard indicator records are generated for events coming in. This can result in the generation of a large volume of indicator records many of which might not be necessary for your system.

Default filtering

As of Splunk SOAR (Cloud) release 6.0.0: To reduce the number of indicator records, Splunk SOAR (Cloud) only generates records that are associated with default and custom fields that are present in your indicator list, located under **Administration > Event Settings > Indicators**. Any records associated with fields that are not present in your indicator list are automatically deleted.

Create a filter

To filter out certain indicators, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings > Indicators**.
3. To filter out certain indicator records, uncheck the box by the field name of the record you don't want to generate indicators for. If you have created any custom CEF fields, by default those fields don't have indicator records. If you want to create indicators for these fields, make sure to check the box next to the field name.
4. After you have made any changes, click **Save Changes**.
5. (Optional) To sort by data type, click **Data Type** and choose how you would like to sort the fields. You can also search for indicators by data type in the search bar to add them to the filter.
6. (Optional) Click **Field Type** to sort the fields based on default or custom fields.
7. (Optional) Use the search bar to search for specific fields.
8. (Optional) Use the Total Count column to see the number of each type of indicator record across the system.

This filter applies only to events coming in after the filter is set and does not apply to indicator records that were previously created.

Track information about an event or case using HUD cards

Use the head-up display (HUD) in Investigation to quickly track relevant information about an event or case. HUD cards can display a metric from the built-in list or display a custom field. For more information about custom fields, see Create custom fields to filter Splunk SOAR (Cloud) assets.

Create a HUD Card

Perform the following tasks to create a HUD card:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings**, then **HUD**.
3. Select **+ HUD Card**.
4. Select a HUD card type.
    - Select **Preset Metrics** to view predefined metrics about your asset, such as remaining tasks, number of failed actions, or tasks exceeding the SLA. Select the desired metric from the drop-down list. and then

choose a background color for the HUD card.
    - Select **Custom Field** to view the information you defined in a custom field. See Create custom fields to filter Splunk SOAR (Cloud) events. The fields defined there are available in the drop-down list. Choose a background color for the HUD card.
5. Select **Done**.

Create a new type of HUD card

You can create a new type of HUD card by creating a basic playbook or by using the Splunk SOAR (Cloud) REST API.

- Create a playbook with a single utility block that will call the `pin` API.
  For details on creating a playbook with a utility block, see Set parameters with the API utility section of the *Add functionality to your playbook in Splunk SOAR (Cloud) using the Utility block* article.
- Call the `/rest/container_pin` API, as described in /rest/container_pin in the REST API Reference for Splunk SOAR (Cloud) documentation.

Manage HUD Cards

HUD cards display in Investigations in the same order they appear in the list of HUD cards you created in the Event settings page. Reorder the cards by dragging the cards by the handle ( ) into the order you want them to be displayed.

Delete a HUD card by selecting the circled x ( ) icon to the right of the HUD card definition.

See HUD cards for more information on using HUD Cards in *Start with Investigation in Splunk SOAR (Cloud)*.

Configure the response times for service level agreements

Service level agreements (SLA) define the number of minutes that is permitted to pass before an action or approval is considered late. SLAs are used for the following purposes in Splunk SOAR (Cloud):

- To track the amount of time a container or case has remaining before it is considered due.
- To track the amount of time an approver has to approve an action before the approval escalates. For more information about the approval and escalation process, see Approve actions before they run in Splunk SOAR (Cloud) in *Use Splunk SOAR (Cloud)*.

Each event or case must have a severity assigned, and each severity has a corresponding SLA. This table lists the default SLA settings in Splunk SOAR (Cloud):

Severity name	SLA in minutes
High	60
Medium	720
Low	1440

The SLA time starts when a case or container is created. An action or approval is considered late if the SLA time is reached before the case or container is closed.

Set service level agreement times

You can set the SLA for any default or custom severity name in Splunk SOAR (Cloud). Custom severities follow the same escalation process that the default severities follow. To set an SLA time for a severity, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings > Response**.
3. In each severity level, type a number of minutes permitted to elapse before an action or approval must be escalated.
4. (Optional) Check **Automatic self-approval** if you want actions activated by a user who can approve them to be approved automatically.
5. (Optional) Add executive approvers by selecting them from the drop-down list in the **Executive approvers** field. When all of the SLA escalations have expired without being acted on, the executive approvers receive an SLA breach notification.
6. Click **Save Changes**.

Configure how events are resolved

Set any tags needed before an event can be marked as resolved. Setting a custom field as a required tag updates the settings for the custom field.

To configure how an event is resolved, follow these steps:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings > Resolution**.
3. Check the **Require the Following Tags on Resolve** checkbox.
4. Type the names of any tags needed before an event or container can be marked as resolved. Tags can be removed by clicking the x next to the tag name.
5. Set the action Splunk SOAR (Cloud) takes when artifacts are added to a resolved event. Select an action from the drop-down list that matches your business process.
    - Select **Keep Event Resolved** to keep events resolved when new artifacts are added.
    - Select **Reopen Event** to reopen any event that has a new artifact added.
    - Select **Duplicate Event** to create a duplicate event, and then add the new artifact to the new event.
6. Click **Save Changes**.

Configure labels to apply to containers

Labels are a property applied to containers. A label applied to a container enables Splunk SOAR (Cloud) to run playbooks and other automation against containers.

Splunk SOAR (Cloud) ships with one label defined: events. More labels can be added to suit your workflow or organizational needs. Labels can have additional custom fields, be used as the basis of a HUD Card, or have tags required before the label's container can be set to a closed or resolved status.

Create a label

Perform the following steps to create a label:

1. From the **Home** menu, select **Administration**.
2. Click **Event Settings > Label Settings**.
3. Click **+ Label**.
4. Type a name for the label.
5. Click **Create**.

Delete or modify a label

Delete a label by clicking the icon to the right of the label's name.

Perform the following tasks to modify a label:

1. From the **Home** menu, select **Administration**.
2. Click **Event Settings > Label Settings**.
3. Click the label's name in the list.
4. Click either Custom Fields, HUD, or Resolution. Each of these items behaves identically to the top-level settings of the same name.
    - For Custom Fields settings, see Create custom fields for containers.
    - For HUD settings, see Track information about an event or case using HUD cards.
    - For Resolution settings, see Configure how events are resolved.

Use authorized users to grant authorized access

Authorized Users are enabled by default. Use this setting to toggle whether the Authorized section is visible in the Investigation screen's HUD.

The Authorized control for managing the Authorized Users appears in the Investigation screen if the authorized users are turned on. The control appears in the HUD, accessed by using the double-down chevron pull-down tab.

Access the HUD and Event Info by doing the following:

1. Click the double-down chevron.
2. Click the right arrow (>) next to **Event Info**.

The Authorized control is located in the **People** section.

This toggle is available for viewing and editing if your role has view and edit permissions for the system settings. See Manage roles and permissions in Splunk SOAR (Cloud) for more information about roles and permissions.

Disable authorized users by doing the following:

1. From the **Home** menu, select **Administration**.
2. Select **Event Settings > Authorized Users**.
3. Click the **Enable Authorized Users** toggle to the Off position.

Once disabled, the Authorized section is no longer visible in Investigation. Reenabling the Authorized Users makes the Authorized section visible in Investigation and also reenables the authorized access that was previously configured.

Authorized access might not be available for every user in the system by default. Authorized access can only be granted to the subset of users who are already assigned to a label that has edit permissions on the container. For example, some

teams only want to allow certain people to work on particular types of cases. Not every user assigned to a label needs access to a particular case.

Grant authorized access by doing the following in Investigation:

1. Expand the **Event Info** collapsible section of a container.
2. Click the edit icon in the **Authorized** section.
3. From the **Authorized Users** drop-down list, select the names of the people who need access.

The Authorized section is visible if you have basic permissions for events with view selected. The Authorized Users drop-down list is editable if you have label permissions for events with view and edit selected.

Administrators always have access to all containers. Normally, you don't need to authorize them. However, if you want to restrict a container to administrators only, set Administrators in the Authorized Users list. Setting specific user names will enable the specific users and administrators.

Manage your Splunk SOAR (Cloud) users and accounts

Manage Splunk SOAR (Cloud) users

View the **Users** page to see the users configured on your Splunk SOAR (Cloud) instance, add new users, or edit existing users.

Perform the following steps to access the Users page:

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.

Changes to the admin user account

With the release of Splunk SOAR (Cloud) version 6.0, the administrator account has changed. This change was made to better support users with the user name admin in single sign on systems.

Release	Administrator account name
5.5.0 and lower	admin
6.0.0 and higher	soar_local_admin

- On new deployments of Splunk SOAR (Cloud) version 6.0.0 and higher, the administrator account is created as soar_local_admin.
- On deployments which have upgraded from versions 5.5.0 or earlier:
    - The existing user account admin will be automatically renamed to soar_local_admin.
    - A copy of the existing user account admin will be created with the user name admin. This copy is for your convenience, and may be deleted.

Default users and types of users

On a new Splunk SOAR (Cloud) instance, the following default users are available:

- Admin: This is the default admin account and cannot be disabled or deleted. The admin user is not counted towards the seat count of a seat-based license.
- Automation: The automation user is not counted towards the seat count of a seat-based license.
- onprem_integration: A special user account used by the Splunk SOAR Automation Broker. The onprem_integration user is not counted towards the seat count of a seat-based license.

An information card is shown for each user. For a local user the information card displays:

- The user's full name
- username
- last access date and time
- roles
- an icon showing the user's initials or custom icon

For automation users, the information card displays a colored ribbon on the left side of the card indicating the user type.

The automation user is a default internal service account used by Splunk SOAR (Cloud) for running automated playbooks and asset actions, such as data ingestion. The automation user and any other users with the automation type do not have passwords and can't log into the Splunk SOAR (Cloud) web interface. However they do provide REST authentication tokens that can be used to read and write data to the REST API. For information on how to use the REST API and authentication tokens, see Using the Splunk SOAR (Cloud) REST API reference in the *Splunk SOAR (Cloud) REST API Reference*.

Customize what you see on the Users page

Customize the information you see on the **Users** page:

- Select the drop-down list in the **Show** field to view more or fewer user cards at a time. By default, 24 user cards are shown.
- Use the filter in the **View by** field to sort the users by first name, last name, username, last accessed, and last created.
- Select the ellipsis (...) icon in the upper corner of each user card for additional options, such as viewing the user's effective permissions, editing the user, or deleting the user.

Configure user permissions

All user permissions in Splunk SOAR (Cloud) are derived from the user's role. To grant permissions to a user, you assign a role with the desired permission. Only the default admin user can have special, hard-coded permissions outside of any roles.

Perform the following steps to view the permissions for a user:

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. Select a user card and review the permissions assigned to this user.

Users with multiple roles have the sum of all the permissions allowed by those roles.

To view the roles assigned to a user, perform the following steps:

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. On the appropriate user card, select the ellipsis (...) icon, then select **Edit**.
   Review the roles listed in the **Roles** field.
4. Select **Cancel** to leave this screen without making any changes.

See Manage roles and permissions in Splunk SOAR (Cloud) for more information about Splunk SOAR (Cloud) roles and the permissions provided by each role.

Add users to Splunk SOAR (Cloud)

You can add users to Splunk SOAR (Cloud) from the Splunk SOAR (Cloud) web interface. The user can be authenticated locally by Splunk SOAR (Cloud), or by using SAML2. In the case of SAML2, the user account can be created in Splunk SOAR (Cloud) or created automatically during the user's initial login. In order for accounts to be automatically created, a group mapping to a Splunk SOAR (Cloud) role must be configured. See Configuring single sign-on authentication for Splunk SOAR (Cloud).

Create a local Splunk SOAR (Cloud) user

Perform the following tasks to add a local Splunk SOAR (Cloud) user. The user is authenticated by the Splunk SOAR (Cloud) instance.

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. Select **+ User**.
4. Verify that the **User type** is set to **Local**.
5. Enter a username in the **Username** field.
6. Enter a password in the **Password** field.
7. (Optional) Complete the other fields on the screen, such as first and last name, email address, title, time zone, and location.
8. Select **Create**.

Create a SAML2 Splunk SOAR (Cloud) user

Perform the following steps to add a user who is authenticated using single sign-on (SSO). Before you do this, make sure you have single sign-on enabled. See Configuring single sign-on authentication for Splunk SOAR (Cloud).

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. Select **+ User**.
4. In the **User type** field, select the SSO provider. Only the configured and enabled SSO providers are available to choose from.
5. Enter the username in the **Username** field.
6. (Optional) Complete the other fields on the screen, such as time zone and roles.
7. Select **Create**.

Create an automation user in Splunk SOAR (Cloud)

Perform the following steps to add an automation user in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. Select **+ User**.
4. In the **User type** field, select **Automation**.
5. Enter the username in the **Username** field.
6. (Optional) In the **Allowed IPs** field, specify the IP addresses allowed to connect as this user. You can specify individual IP addresses, CIDR ranges, or **any** to allow all IP addresses.
7. (Optional) Enter a default label for this user. Any containers that get created by this user use this label if another label is not specified.
8. (Optional) The **Automation** role is provided to automation users by default. See Manage roles and permissions in Splunk SOAR (Cloud) for more information about the permissions granted by each role.
9. Select **Create**.

Edit an automation user to view the REST API authorization token and associated assets

Select an existing automation user on the **Users** page to view the following information:

- The REST API authorization token, which is used to authenticate the user for access to the REST API. See Using the Splunk SOAR (Cloud) REST API reference in the *Splunk SOAR (Cloud) REST API Reference* manual.

- The assets associated with this user.
    - The automation user is used to test connectivity with the listed assets, and also for ingesting data. Use the automation user configuration to set the permissions of the asset when the asset is running on its own.
    - When the asset is not performing test connectivity or data ingestion, it is running with the permissions of the user performing the action. If the asset is being run from a playbook, the asset has the permissions of the playbook user.
    - You can assign assets to an automation user during asset configuration. If you assigned an automation user to an asset, the asset appears in the automation user's card. See Configure automation users for a Splunk SOAR (Cloud) asset.

Disable an existing Splunk SOAR (Cloud) user

Disable a user in Splunk SOAR (Cloud) to prevent that user from logging in or accessing the system. Disabling a user does not delete the user account.

To disable an existing Splunk SOAR (Cloud) user, perform the following steps:

1. From the **Home** menu, select **Administration**.
2. Select **User Management**, then **Users**.
3. Select the ellipsis (...) icon for the user you want to disable, and select **Edit**.
4. Select the **Disabled** checkbox.
5. Select **Save**.

Set security parameters

Within User Management, use the Account Security Settings to specify session timeouts and password criteria for your Splunk SOAR (Cloud) instance. All values are required on this page. Enter a zero (0) in any field to ignore that field.

Set your instance of Splunk SOAR (Cloud) to timeout, requiring the user to log in again. There are separate settings you can specify:

- Inactivity timeout: Ends the session if no user activity is detected for the number of minutes you specify. The system checks for inactivity every 2 minutes, so specify a value greater than 2 minutes. Maximum timeout value is 35821 minutes (24 days).
- Absolute timeout: Ends the session, regardless of level of user activity, after the number of minutes you specify. Maximum timeout value is 35821 minutes (24 days).
- Remaining session time warning: Warn the user that they have only the specified number of minutes remaining until their session ends, due to inactivity. A value of 5 in this field means the user is warned when there are 5 minutes left in the session.

Here is an example that uses the following settings:

- Inactivity timeout=10 minutes
- Absolute timeout=120 minutes
- Remaining session time warning=3 minutes

In this example, the user opens a session, works for a while, and then becomes inactive. If the user is inactive for 7 minutes, the warning appears, letting them know that the session will soon end.

- If the user continues to be inactive, their session ends after 3 minutes.

- If the user closes this warning message, they have become active again. The inactivity timeout is reset to 10 minutes, the original number of minutes you specified. The user can continue their session until they reach the absolute timeout value of 120 minutes from the start of their session. If the user becomes inactive again, the cycle just described occurs again, up to a maximum session length of 120 minutes from the start of the session.

Later on the Account Security Settings page, specify required password strength criteria, including password length number of special characters.

Manage roles and permissions in Splunk SOAR (Cloud)

Roles in Splunk SOAR (Cloud) serve the following purposes:

- Grant users permission to access system functionality, or restrict access to parts of the system.
- Act as a mechanism for grouping users for approvals. See Approve actions before they run in Splunk SOAR (Cloud) in the *Use Splunk SOAR (Cloud)* manual.

View your Splunk SOAR (Cloud) roles

To view the roles configured in your Splunk SOAR (Cloud) instance, perform the following steps to access the Roles page:

1. From the **Home** menu, select **Administration**.
2. Select **User Management** then **Roles & Permissions**.

Splunk SOAR (Cloud) includes the following default roles that can't be edited or deleted:

Role	Description
Administrator	Users with this role have view, edit, and delete privileges to and can access all Splunk SOAR (Cloud) functions and settings: • By default, the user name associated with the administrator role is soar_local_admin. • View, edit, and delete permissions for everything • Manage users and accounts • Change any and all Splunk SOAR (Cloud) settings • Install or remove apps or connectors • Create, edit, and delete Assets • Create, edit, delete and view workbooks • Create, edit, run, and delete playbooks
Asset Owner	Users with this role can: • Create, edit, and delete assets • View apps or connectors, events, custom lists, playbooks, system settings, and users and roles.
Automation	This is a service account role used for automated tasks including REST API operations, playbook execution, and ingestion.
Automation Engineer	Users with this role can: • View, run, edit playbooks, and can edit playbook code • View apps, assets, custom lists, events, system settings, and users and roles
Incident Commander	Users with this role can: • Create, edit, and delete cases • Create, edit, delete, run, or edit the code for playbooks

Role	Description
	• View and edit events • Create, edit, delete and view workbooks • View apps, assets, system settings, and users and roles
Observer	Users with this role can view everything except workbooks, but cannot edit or run anything.
OnPrem Broker	This is a service account that allows the Automation Broker to view apps. **Note:** This role is assigned to a user account with a name that looks like onprem_integration_<auto-generated-id-string>. Onprem_integration users are created when you pair an instance of the Splunk SOAR Automation Broker with your Splunk SOAR (On-premises) deployment. These users do not count against a seat-based license.

Users granted multiple roles have the cumulative privileges of all the roles. You can also restrict access to specific named objects. See Named object permissions.

Add a role to Splunk SOAR (Cloud)

Perform the following steps to add a new role in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **User Management** then **Roles & Permissions**.
3. Select **+ Role**.
4. Enter a name for the role.
5. (Optional) Enter a description for the role.
6. Select the **Basic Permissions** provided by this role.

Component	Permission and Description
Apps	♦ Select **Edit** to allow the user to add or delete apps, or edit settings on individual apps. ♦ Select **View** to allow the user to view the list of installed apps, and view the settings for individual apps.
Assets	♦ Select **Delete** to allow the user to delete assets. Note that the user will also need view assets in order to see the asset before they can edit it. ♦ Select **Edit** to allow the user add and edit assets. ♦ Select **View** to allow the user the ability to look at the list of assets and individual asset configurations.
Automation Broker	♦ Select **Delete** to allow the user to delete Automation Brokers. ♦ Select **Edit** to allow the user to create and edit Automation Brokers. ♦ Select **View** to allow the user to view Automation Brokers.
Cases	♦ Select **Delete** to allow the user to delete cases. ♦ Select **Edit** to allow the user to create and edit cases. ♦ Select **View** to allow the user to view cases.
Events	♦ Select **Delete** to allow the user to delete events. ♦ Select **Edit** to allow the user to modify events. This includes data about the event itself (assigned owner, SLA) as well as being able to add items to artifacts and files. ♦ Select **View** to allow the user to view events. This includes both the list of events, as well as the contents of individual events.
Custom Lists	♦ Select **Delete** to allow the user to delete custom lists. ♦ Select **Edit** to allow the user to create and edit custom lists. ♦ Select **View** to allow the user to view custom lists.
Playbooks	♦ Select **Delete** to allow the user to delete playbooks. ♦ Select **Edit** to allow the user to edit playbooks, including modifying the playbook settings such as logging, active, safe mode, and draft mode. For more information on playbook settings, see Manage settings for a playbook in Splunk SOAR (Cloud) in the *Build Playbooks with the Visual Editor* manual. ♦ Select **View** to allow the user to use **Action** blocks in playbooks. ♦ Select **Execute** to allow the user to execute playbooks on events.

Component	Permission and Description
	♦ Select **Edit Code** to allow playbook authors to manually edit Python code and customize code blocks. Authors without this permission can only use the visual block editor.
System Settings	♦ Select **Edit** to allow the user to change System Settings. **Caution:** The System Settings include authentication servers. Users with edit system settings have the ability to perform a privilege escalation attack. ♦ Select **View** to allow the user to view system settings.
Users and Roles	♦ Select **Edit** to allow the user to edit, delete and add users and roles. Security note: a user with **Edit** permission can grant themselves all other privileges. They should be considered equivalent to an administrator. ♦ Select **View** to allow the user to view users and roles, including what role each user has, email addresses, and last login time.

7. Select **Label Permissions** to configure label permissions for this role. The labels you see in the table depend on the labels you have defined on your Splunk SOAR (Cloud) instance. See Create additional custom status labels in Splunk SOAR (Cloud). The following permissions can be configured:

Permission	Description
Delete	The user can delete any object in Splunk SOAR (Cloud) that has this label. Selecting this automatically grants the Edit and View permissions.
Edit	The user can edit any object in Splunk SOAR (Cloud) that has this label. Selecting this automatically grants the View permission.
View	The user can view any object in Splunk SOAR (Cloud) with this label, but cannot modify or delete any such objects.

8. Select **Repository Permissions** to configure repository permissions for this role. The repositories you see in the table depend on the repositories configured on your Splunk SOAR (Cloud) instance. See Configure a source control repository for your Splunk SOAR (Cloud) playbooks. The following permissions can be configured:

Permission	Description
Delete	The user can delete any playbook in this repository. Selecting this automatically grants the Edit and View permissions.
Edit	The user can edit any playbook in this repository. Selecting this automatically grants the View permission.
View	The user can view any playbook in this repository, but cannot modify or delete any playbooks.
Execute	The user can run any playbook in this repository.

9. Select **Create Role**.

Add users to a role in Splunk SOAR (Cloud)

Perform the following steps to add users to a role in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **User Management** then **Roles & Permissions**.
3. Select the role you want to edit and add users to.
4. Select **Add Users**.
5. Select a user from the drop-down list, or start typing a username to filter the users that are displayed.
6. Select **Add**.
7. Repeat and continue adding users as desired. Each time a user is added, the user card appears in the **Users** field in the role.

For information on viewing roles and permissions for a specific user, see Configure user permissions in the *Manage Splunk SOAR (Cloud) users* article.

Edit a role in Splunk SOAR (Cloud)

Perform the following steps to edit a Splunk SOAR (Cloud) role:

1. From the **Home** menu, select **Administration**.
2. Select **User Management** then **Roles & Permissions**.
3. Select a custom role you want to modify. You can modify any of the permissions in a custom role, add users or remove users. When editing a system role, you can only add or remove users.
    - Users added to a role have their permissions saved in real time, before you select **Save Changes**.
    - Permission changes to roles are applied in real time to the users who are granted the updated permissions, before you select **Save Changes**.
    - Users inheriting roles from an SSO provider must log out and log back in to Splunk SOAR (Cloud) to see their updated permissions.
4. Select **Save Changes**.

Delete a role in Splunk SOAR (Cloud)

Perform the following tasks to delete a role in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **User Management** then **Roles & Permissions**.

1. Select the role you want to delete.
2. Select **Delete Role**.
3. Select **Delete** to confirm that you want to delete the role.

Configure password requirements and timeout intervals to secure your Splunk SOAR (Cloud) accounts

You can configure password requirements and set timeout intervals for inactivity to secure your local Splunk SOAR (Cloud) accounts. Accounts that authenticate using single sign-on have their password requirements set by the individual service provider.

Perform the following steps to configure account security:

1. From the **Home** menu, select **Administration**.
2. Select **User Management > Account Security**.
3. Configure the desired timeout settings for all local Splunk SOAR (Cloud) accounts.

Setting	Description
Inactivity Timeout	The number of minutes with no activity between the user's browser and the web server before the user is logged out.
Absolute Timeout	The number of minutes after which a local user is logged out, regardless of activity. Some pages, such as the home page and Investigation have constant activity in the form of widgets and dashboards that are updated automatically without user intervention. Setting an absolute timeout is a security precaution to make sure that only authorized users are accessing your Splunk SOAR (Cloud) system.

4. Configure the password requirements for your local Splunk SOAR (Cloud) accounts.

Setting	Description

Setting	Description
Length	The minimum required length for any user password. This length can be overridden based on other password configurations. For example, if you set the **Length** to 8 characters, but also require 5 capital letters and 5 digits, then the minimum length of the password is 10 characters.
Digits	The number of unique digits 0-9 required in the password.
Special Characters	The number of unique special characters required in the password.
Capital Letters	The number of unique capital letters required in the password.

Configure single sign-on authentication for Splunk SOAR (Cloud)

Splunk SOAR (Cloud) supports using Single sign-on (SSO) to authenticate Splunk SOAR (Cloud) users.

Single sign-on (SSO) systems allows users to be authenticated once, then use multiple, distinct services or applications without having to reauthenticate for each application or service. Single sign-on systems rely on an identity provider to authenticate the user, then provide an authentication token which applications, such as Splunk SOAR (Cloud), use to log the user in. For an overview of single sign-on, see the Single sign-on article on Wikipedia.

You can configure SSO for Splunk SOAR (Cloud) with Security Assertion Markup Language 2.0 (SAML2).

Configure SSO authentication using SAML2

To configure SSO authentication using SAML2 as the identity provider, perform the following tasks:

1. From the Home Menu, select **Administration**.
2. Select **Users > Authentication**.
3. Click **SAML2**.
4. Click the toggle in the SAML2 field to enable SAML2 configuration.
5. Complete the fields to configure SSO authentication using SAML2:

Field	Description
Active	Use this checkbox in conjunction with **Add Another** at the bottom of the page. You can have multiple SAML2 servers and the **Active** checkbox determines which ones are used by Splunk SOAR (Cloud) for authentication. The toggle button in the SAML2 field enables SAML2 authentication for all servers which are marked Active. If there are multiple SAML2 servers, Splunk SOAR (Cloud) searches each server in a random order to find a match for the username. If the same username exists on multiple servers, the first one matched is used. If this match happens to be for a different user and not the user who is attempting to login, then authentication fails.
Require TLS/SSL encryption	Determines whether encrypted connections are required. Enable TLS/SSL encryption to check the server certificate against the Splunk SOAR (Cloud) certificate store.
Provider Name	The name of the SSO provider. Specify a unique name to easily identify this provider.
Single sign-on URL	The URL that users are directed to for logging in.
Issuer ID	The unique identifier provided by the identity provider.

Field	Description
Metadata URL	The URL hosted by your identity provider containing information about the provider configuration. If you specify a valid Metadata URL, do can leave the Metadata XML field blank.
Metadata XML	XML code containing information about the provider configuration. If you specify valid XML in this field, you can leave the Metadata URL field blank.
Phantom Base URL	The URL used to redirect users back to Splunk SOAR (Cloud). This URL must be reachable by users trying to log in.
Advanced Settings	Click **Advanced** to configure the following advanced settings: ♦ Select **Response Signed** to require a signed response from the identity provider. ♦ Select **Request Signed** to require a signed request from the identity provider. ♦ Select **Assertion Signed** to require a signed assertion containing the user attributes from the identity provider. ♦ Type an **EntityID**/**Audience** to configure an entity ID for the service provider. This is used when defining the audience restriction on the identity provider. A value for this field must be included. ♦ Type a **Group Key** to identity identify the group membership data within the attributes passed back from the identity provider. Also specify a **Group Delimiter** if groups are passed back as a single element with a delimiter, instead of separate attribute values. ♦ Configure **Groups**. See Configure group mappings for SAML 2.0 SSO authentication for more information about group mapping. ♦ Configure **External Attributes**. See Configure external attribute mappings for SAML 2.0 SSO authentication for more information about external attributes mapping. If user name mapping is not provided in the assertion, Splunk SOAR (Cloud) will default to using the value specified in NameID field.

6. Click **Save Changes**.

To update a SAML2 user account's information, such as name, title, location, or email address, update their information in your SAML2 identity provider. User information will be updated in Splunk SOAR (Cloud) the next time that user logs in.

Splunk SOAR (Cloud)'s SAML2 authentication integration does not support HTTP redirect binding.

Configure group mappings for SAML 2.0 SSO authentication

Configure a group mapping to map group in your SAML 2.0 bindings to a Splunk SOAR (Cloud) role. Doing so enables you to automatically use your existing SAML 2.0 identity provider groups to determine who can log into Splunk SOAR (Cloud) and which actions each user is able to perform after they log in.

Click **Add Mappings** to create a new mapping. You can configure multiple mappings.

Each user must be mapped to at least one group to enable that user to login to Splunk SOAR (Cloud) without manually creating the user account in Splunk SOAR (Cloud).

Role mapping is done at login time, meaning that if the Splunk SOAR (Cloud) administrator changes a role mapping that would affect a logged-in user, then that user will retain the old role(s) until they log out and log back in again.

Configure external attribute mapping for SAML 2.0 SSO authentication

In some cases you may need to specifically call out external attributes which should be mapped to the Splunk SOAR (Cloud) user attributes. Click **Add Mapping** to select a Splunk SOAR (Cloud) user attribute to map, then use the text field to enter the name of the attribute found in your SAML 2.0 identity provider's user's profile.

Managing Splunk SOAR user accounts and roles when pairing or unpairing with Splunk Enterprise Security

Splunk SOAR user account roles can be individually managed by only one identity provider (IDP);

- Splunk SOAR
- your SAML IDP
- Splunk Enterprise Security

Pairing Splunk SOAR and Splunk Enterprise Security

When Splunk SOAR is paired to Splunk Enterprise Security, user accounts that interact with Splunk Enterprise Security are converted to a new user type, the Splunk user type. Roles and permissions for these users must be managed in Splunk Enterprise Security.

See Pair Splunk Enterprise Security with Splunk SOAR and Pair Splunk SOAR with Splunk Enterprise Security for more on how to pair Splunk SOAR and Splunk Enterprise Security.

Unpairing Splunk SOAR and Splunk Enterprise security

When a Splunk SOAR local or SAML2 account was managed by Splunk Enterprise Security, a SOAR administrator may need to adjust user accounts and roles if Splunk Enterprise Security is unpaired from Splunk SOAR.

Splunk SOAR (Cloud) allows you to set a policy that manages how Splunk Enterprise Security accounts convert if Splunk SOAR is unpaired from Splunk Enterprise Security.

User accounts from Splunk Enterprise security without a corresponding SOAR local or SAML2 account remain in Splunk SOAR until Splunk SOAR and Splunk Enterprise Security are re-paired, or a SOAR administrator deletes those accounts. The Splunk-type accounts are effectively disabled because they cannot log in.

Roles from Splunk Enterprise Security remain attached to user accounts after Splunk SOAR is unpaired from Splunk Enterprise Security, unless they are removed. See the instructions later in this section.

> Changes you make to users take effect the next time that user account authenticates, after you unpair Splunk SOAR from Enterprise Security.

To manage how Splunk Enterprise Security accounts are converted if Splunk SOAR is unpaired from Splunk ES:

1. Select the **Home** menu, then **Administration**, **User Management**, **Authentication**.
2. From the **Authentication** screen, select the **Splunk IDP** tab.
3. Use the dropdown menu to select the types of accounts to convert if Splunk SOAR is unpaired from Splunk Enterprise Security. You can select multiple account types.
4. Check or uncheck the box labeled **Remove any roles applied to local user account types**. Checking this box removes any roles applied by Splunk Enterprise Security from the local or SAML2 accounts.

See also

- Pair Splunk Enterprise Security with Splunk SOAR
- Manage roles and permissions in Splunk SOAR (Cloud)

Configure role based access control inside Splunk apps

Splunk SOAR (Cloud) supports granular asset access control inside of Splunk SOAR (Cloud) apps to ensure that only authorized access to the app is allowed. Asset access control works on an authorized basis, with a default-deny policy.

When granular asset access control is enabled, only users or groups with explicit permissions are able to perform actions in a Splunk SOAR (Cloud) app. Configure user and group permissions on all configured apps before enabling granular asset access control.

To set up a single user to have access the "lookup domain" action on the Google DNS asset:

1. From the **Home** menu, select **Apps**.
2. Click **1 configured asset** to expand the section.
3. Click **Google DNS** to edit the asset.
4. Click the **Access Control** tab.
5. Click **Edit**.
6. Select **lookup domain** from the **App Action** drop-down list.
7. Select the user desired user name then click the right arrow in order to move the user from the **Users and Roles** list into the **Approved Users and Roles** list.
8. Click **Save**.

Now enable granular asset access control so that the permission set above takes effect.

1. From the **Home** menu, select **Administration**.
2. Select **User Management > Asset Permissions**.
3. Check the **Enable granular Asset Access Control** checkbox.
4. Confirm that you want to change global asset permissions.
5. Click **Save Changes**.

Monitor your Splunk SOAR (Cloud) system activity

View how much data is ingested in Splunk SOAR (Cloud) using ingestion summary

The ingestion summary page provides a summary of container and artifact ingestion over time and currently scheduled periodic ingestions. Use the Ingestion Summary page to get a broad view of how much data is coming into Splunk SOAR (Cloud) and how that amount is trending over time.

Perform the following steps to view ingestion summary details:

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Ingestion Summary**.

The Ingestion Summary table shows a line chart with the total number of successful and failed artifact and container ingestions across all Data Sources and ingestion methods. Use the drop-down list to change the time range of the chart. You can select one of the following time ranges:

- Last 24 hours
- Last 7 days
- Last 30 days

The Scheduled Ingestion table lets you track the configuration of all Data Sources that currently have scheduled polling enabled:

- Time shows the date and time when that Data Source was last set to enable scheduled polling.
- Interval shows how often that Data Source is scheduled to poll.
- Container shows the label that will be applied to containers ingested from that Data Source.
- Asset shows the name of the Data Source asset.
- App shows the name of the Data Source app.
- Action shows the name of the action that will be used to ingest data.

View ingested container statistics using Ingestion Status

Use the Ingestion Status page to see high-level statistics about ingested containers.

To view ingestion status details, perform the following steps:

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Ingestion Status**.

The Ingestion Stats table shows one row for each unique combination of ingestion status, container label, asset, and action. These rows allow you to get a better sense of how many containers are being ingested through each ingestion mechanism. Some containers don't come from an asset because they are manually added by a user, which results in a row with an action such as "User add container".

The Ingestion Errors table lists any failed ingestions. Use the information in the start time, end time, asset, app, and action fields to start debugging the failure.

Configure the logging levels for the Splunk SOAR (Cloud) action daemon

You can adjust the logging level for the action daemon running in Splunk SOAR (Cloud) to help debug or troubleshoot issues.

Splunk SOAR (Cloud) daemons

The following daemons in Splunk SOAR (Cloud) work to control collection and scheduling tasks in the background independently from the Splunk SOAR (Cloud) web interface:

Daemon	Description
Action daemon	Responsible for launching actions by putting into effect the appropriate app on the specified asset. Also responsible for the debug log that says what version of Python is being used. The debug log for Python 3 shows `Running executable: spawn3`. The following key actions are logged by this daemon: • Manual actions run against any configured asset • Scheduled actions against any configured asset
Decide daemon	Responsible for operating on incoming data. The following key actions are logged by this daemon: • Launching active playbooks against new containers for associated **Operates On** types • Playbook validation • Playbook loading and use • Custom automation or playbook APIs • Prompting the action daemon for action and app use • Prompting the workflow daemon for the approval workflow process • Processing approval response and results from the workflow daemon • Matching app execution to specific action results • Playbook debugging • Counting licensed action uses
Ingest daemon	Responsible for ingesting data into the product. The following key actions are logged by this daemon: • Ingestions from data sources that use polling to get new data • Asset health reporting, also known as, connectivity checking for the **Asset Health** dashboard component • Configuration changes to any assets or any app-specific configuration • Manual **Test Connectivity** actions launched directly from any asset
Proxy daemon	Responsible for communicating with Splunk mobile apps to register devices and send notifications to mobile users. This daemon is available only when the mobile app feature is enabled.
Watchdog daemon	Responsible for tracking the status of other daemons and adding or removing them in the system startup list. The following key actions are logged by the watchdog daemon: • Installation of new apps • Health monitoring the Splunk SOAR (Cloud) deployment • Maintenance of other Splunk SOAR (Cloud) platform daemons and components • Restarts of the Splunk SOAR (Cloud) platform daemons and components
	Responsible for managing approval requests to action reviewers and asset owners.

Daemon	Description
Workflow daemon	The following key actions are logged by the workflow daemon: • Processing and launching approval processes and managing approval escalations • Sending user email notifications for container assignment, expiry, manual action requests, and other email templates

Configure the logging level for the action daemon

Adjust the logging levels as needed to assist Splunk SOAR (Cloud) Support with troubleshooting any issues you might experience.

1. From the main menu, select **Administration**.
2. Select **System Health > Debugging**.
3. Select a logging level for the action daemon. The log levels determine the message types that are written to each daemon's corresponding log file. The **Debug** level is the most verbose level of logging and is useful for troubleshooting. Only set the **Action Daemon Log Level** to **Debug** if you are actively troubleshooting an issue.
4. Click **Save Changes**.

Example log structure

See the following sample of a common log format:

```
Oct  5 22:55:18 localhost DECIDED[7177]: TID:7422 : WARNING: DECIDED : rules_engine.cpp : 1503 :
DECIDED_CMD_PROCESS_CONTAINERS : All rules FAILED t
```

This table summarizes the structure of the example log message.

Log message content	Description
Oct 5 22:55:18	Timestamp of when the log message was generated.
localhost	Name of the host where the log message was generated.
DECIDED[7177]:	Name of the component and process ID (PID) generating the message.
TID:7422:	Threat ID (TID) of the message.
WARNING:	Log level or class of the message.
DECIDED:	Functional component that generated the log message.
rules_engine.cpp:	Source file applicable to the log message.
1503:	Line number in the source file that caused this log message to be generated.
DECIDED_CMD_PROCESS_CONTAINERS: All rules FAILED to process the container: 2964. Error: Playbook 'local/test11 (version: 1, id: 711)' cannot be executed since it is: NOT ACTIVE, ENABLED and VALID	The log message.

Create and download or upload a diagnostic file

Splunk SOAR (Cloud) can create diagnostic files that contain selectable categories of data to help Splunk Support diagnose issues with your deployment. You need an active support case, and credentials for the **Support Portal** to upload the diagnostic file to Splunk Support. For more information on opening a support case, see the heading Splunk Technical Support in the topic Administer Splunk SOAR (Cloud).

Create a diagnostic file

Diagnostic files can be created using the web-based user interface.

From the **Home** menu, select **Administration**, then **System Health**, then **Debugging**.

1. (Optional) Click the symbol next to **Advanced**.
2. (Optional) Select the checkboxes for the categories you want to include in your diagnostic file; **Instance**, **System**, **Database**, **Apps**, **Filesystem**, and **Cloud**. The default setting includes all sections except filesystem.
3. (Optional) Select the range of logs you want to include in your diagnostic file; **All Logs** or **Recent Logs**. The default is **All Logs.**
4. To download the diagnostic file locally click **Download Logs**.
5. To upload your diagnostic file and attach it to your support case, click "Upload to Support".
    1. Type your **Support Portal** username, password, and case number.
    2. Click **Login and Upload**.

Usernames must be submitted in all lowercase letters.

Enable and download audit trail logs in Splunk SOAR (Cloud)

Enable audit trail logging to help you track the activities of various components in Splunk SOAR (Cloud). Once enabled, audit trail logs can be downloaded and included as evidence in an investigation, or analyzed when troubleshooting an issue.

Audit information is also accessible using the REST API. See REST Audit in the *REST API Reference for Splunk SOAR (Cloud)*.

Enable audit trail tracking

By default, all audit tracking in Splunk SOAR (Cloud) is disabled. Perform the following tasks to enable audit trail tracking in Splunk SOAR (Cloud):

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Audit Trail**.
3. Click **Manage Audit Trail**.
4. Select the product areas for which you want to enable audit tracking.
5. Click **Save**.

Splunk SOAR (Cloud) immediately starts tracking audit events for the selected items.

Even when the audit categories are disabled, events such as action and playbook runs are automatically tracked and logged as audit events.

Export audit logs

To export audit logs for a particular product, make sure you enabled audit tracking for that product area.

After you enable audit logging, use the rest of the **Audit Trail** to configure the audit logs you want to download as a CSV file. Perform the following steps to export audit events to a CSV file for download. This example shows you how to configure audit logging for containers and download a CSV file.

First, enable audit logging for containers:

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Audit Trail**.
3. Click **Manage Audit Trail**.
4. Click the **Container** toggle to enable audit tracking for containers.
5. Click **Save**.

Next, export a CSV file. This example exports the CSV file for a specific container.

1. From the Audit Trail page in the Audit Type section, click **Custom**.
2. Click **Containers**.
3. In the drop-down list for Containers, select **Custom**.
4. Specify the container ID, such as 123456. Only the audit trail for this specific container is downloaded.
5. By default, the audit trail from the last 30 days is downloaded. Click **Custom** in the Audit Range Time Frame field to configure a specific date range.
6. Click **Download** to download the CSV file.

Export audit logs for multiple users

Exporting audit logs for multiple users adds a new input field where you can specify a container to report on. When you download the audit logs, you receive only audit events for the container specified instead of all containers. Other categories might let you pick from a list, such as Users.

You can download audit logs for multiple users. Use `%1E` as the separator. For example, if you want to specify `user1` and `user2`:

```
user1%1Euser2
```

Export audit logs for roles

Roles return two types of events. First, creating a role or changing permissions in it shows up as audit events for that role. Second, the logs show audit events for users currently in that group. In other words, the logs treat the role like a user group, and shows events for those users in it. See Accessing Audit Data in the REST API Reference for more information.

Required privileges for enabling audit trail

In order to access the Audit Trail page, users must have a role with the View System Settings privilege. If they want to view or change anything under the Manage Audit Trail, then they also need the Edit System Settings privilege.

With only the View System Settings privilege, the user can't access all audit items. Attempting to download with the Audit Type section set to All results in an error.

A user with only some of the required privileges can switch to Custom and select only the items they have the rights to access. The privileges for each of the items are as follows:

Audit Trail Area	Required privileges
Authentication	View Users and Roles
Administration	View System Settings
User	View Users and Roles
Role	View Users and Roles
Playbooks	View Playbooks
Containers	View Containers

Enable the audit trail for individual objects

Users can access audit information in two places: on the page for a playbook and on the Investigation page for a container.

Download a playbook's audit trail

Perform the following steps to download an audit trail for a playbook:

1. Open the playbook.
2. Click **Playbook Settings**.
3. Click **Audit Trail** to download a CSV file containing the audit information for this playbook.

Download a container's audit trail

Perform the following steps to download an audit trail for a container:

1. Click the container to view the container.
2. Click the **...** icon, and then select **Audit**.

A CSV file is downloaded containing the audit information related to this container.

Locate long-running playbooks for debugging or troubleshooting in Splunk SOAR (Cloud)

Use the Automation page to locate playbooks that have been running for a long time.

As an example, suppose your system health indicators show heavy utilization, but you are not aware of any process that must be running for a long period of time. You can start on the Automation page to see if any playbooks might be running intensive applications or experiencing other problems.

Perform the following tasks to access the Automation page:

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Automation**.

View the playbook run history in Splunk SOAR (Cloud)

You can view the history of playbook runs on your Splunk SOAR (Cloud) instance.

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Playbook Run History**.

The Playbook Run History page displays a sortable table of playbook runs. Each column except for Git Commit is sortable. The table displays the following columns:

Column title	Description
Name	The name of the playbook that was run.
Run ID	The numeric ID of the Playbook Run.
Event ID	The numeric ID of the event the playbook was run against.
Label	The label the playbook was run against, such as event.
Start Time	The time the playbook was started.
End Time	The time the playbook run finished.
Status	Whether the playbook run succeeded or failed.
Git Commit	The Git commit ID from when the playbook version was committed to the included Git source control module.
Run By	The name of the user who ran the playbook.

View Playbook Run Statistics

Playbook Run Statistics are available in playbooks created in the Visual Playbook Editor, starting in Splunk SOAR (Cloud) version 5.3.3.

Learn how your playbooks are performing, and troubleshoot potential issues, by viewing Playbook Run Statistics. You can view statistics for specific playbook runs at the playbook level and for each block and custom function within a playbook after the playbook has run. Compare statistics for this playbook to other specific runs or to run averages for that playbook to detect differences.

To view the Playbook Run Statistics for one of your playbooks, complete these steps:

1. Open the playbook within the Visual Playbook Editor.
2. In the top right corner of the screen, click the more icon , then click **View Run Statistics**. The Playbook Run Statistics dialog box displays.
3. In the first column in the Playbook Run Statistics dialog box, use the Playbook Run field to specify the playbook run you want to investigate. Use the filter to search for a specific run, if needed.
4. (Optional) In the second column, choose whether you want to compare against the average runs for that playbook for the last 24 hours, 7 days, or all runs for that playbook.
5. (Optional) Use the third column to add another comparison for the same playbook.
6. (Optional) Add a fourth column by clicking the plus icon.

To show all available playbook run statistics, expand each of the sections in the dialog box.
To view information for a specific block in playbook, click that individual playbook block. In the left panel, click the **Stats** tab.

Playbook Run Statistics and older playbooks

Playbook Run Statistics are available in playbooks created in the Visual Playbook Editor, starting in Splunk SOAR (Cloud) version 5.3.3. To view these statistics with playbooks you created with the Visual Playbook Editor in versions lower than 5.3.3, you must first save the playbook to automatically add the code required for statistics. The added statistics code does not affect your custom code.
You can view statistics for these updated playbooks for runs performed after you have updated the code.

Description of Playbook Run Statistics

This table describes Playbook Run Statistics for playbook blocks.

Field	Description
DB Queries	Number of requests to the database made by this block
DB Query Latency	Average amount of time for the block request to reach the database, in milliseconds
Duration	Amount of time for the block to execute, in milliseconds
HTTP Bytes in Requests	Number of bytes transmitted by the block through HTTP requests
HTTP Bytes In Response	Number of bytes received by the block through HTTP requests
HTTP Latency	Average amount of time between HTTP requests and responses experienced by the block, in milliseconds
HTTP Requests	Number of HTTP requests initiated by the block
Times Called	Number of times the block was called
Times Succeeded	Number of times the block completed successfully

Playbook run statistics are enabled with the `phantom.playbook_block()` decorator.

View the action run history

You can view the history of actions run on your Splunk SOAR (Cloud) instance.

1. From the **Home** menu, select **Administration**.
2. Select **System Health > Action Run History**.

The Action Run History page displays a sortable list of action runs. Each column except for View Results is sortable. The table displays the following columns:

Column name	Description
Name	The name of the action that was run.
Run ID	The numeric ID of the action that was run.
Event ID	The numeric ID of the event the action was run against.

Column name	Description
Start Time	The time the action started.
End Time	The time the action finished.
Status	Whether the action succeeded or failed.
Prompted	If the action taken was a prompt or manual task action, the ID of the user assigned the action appears here.
Run By	The name of the user who ran the action.
View Results	A hyperlink to the action results in Investigation. For prompt or manual task actions, the link opens a window containing the prompt or task results.

Manage your Splunk SOAR (Cloud) deployment

Request a system restore from a backup

Splunk SOAR (Cloud) deployments are backed up every 24 hours. Each backup is a snapshot of both the deployment file system and PostgreSQL database.

- Backups of the PostgreSQL database are retained for 35 days.
- Backups up the file system are retained for 28 days.

Authorized Splunk SOAR (Cloud) users can open a support case to have a backup restored. See Splunk Support portal in *Administer Splunk SOAR (Cloud)*.

Manage your Splunk SOAR (Cloud) Apps and Assets

Add and configure apps and assets to provide actions in Splunk SOAR (Cloud)

Splunk SOAR (Cloud) apps expand the capabilities of your Splunk SOAR (Cloud) instance by enabling connections to third party products and services. These third-party products and services provide actions you can run or automate in your Splunk SOAR (Cloud) playbooks. For example, the MaxMind app provides the **geolocate ip** action for your Splunk SOAR (Cloud) deployment.

You can upgrade existing apps or install new apps at any time without having to upgrade the entire Splunk SOAR (Cloud) platform.

Apps have full access to the operating system and there are no security restrictions on any app while it is running.

An asset is a specific configuration, or instance, of an app. An asset is configured with the information required to communicate with the third-party product or service, such as IP address, automation service account, username, and password.

For example, Splunk SOAR (Cloud) ships with a VMware vSphere app enabling Splunk SOAR (Cloud) to get information from and take actions against a vSphere host. You can use Splunk SOAR (Cloud) to start and stop VMs, take snapshots, and download memory snapshots for analysis. In order for the app to be able to communicate with your vSphere servers, you must provide login credentials such as the hostname or IP address. You might have multiple vSphere servers, such as several individual ESXi hosts, or you might have them centralized onto one vCenter server. To tell Splunk SOAR (Cloud) about a given vSphere server, create a vSphere asset and provide the address and credentials needed for that server. You can then create another vSphere asset with a different address and credentials if needed. When taking actions, you specify which asset the action is for.

This table shows how multiple vSphere assets are configured from a vSphere app:

Splunk SOAR (Cloud) app	Configure multiple assets from a single app
VMware vSphere	vSphere 1 • IP address 192.168.1.1 • User admin1, password example1
	vSphere 2 • IP address 192.168.1.2 • User admin2, password example2
	vSphere 3 • IP address 192.168.1.3 • User admin3, password example3

View your Splunk SOAR (Cloud) apps

Splunk SOAR (Cloud) ships with hundreds of apps already installed. You can find more apps on splunkbase, from other users, and even create your own. See Splunk SOAR (Cloud) apps overview in *Develops Apps for Splunk SOAR (Cloud)*.

Perform the following tasks to view the apps provided by Splunk SOAR (Cloud) on the Apps page.

1. From the **Home** menu, select **Apps** to access the Apps page.
2. View the list of configured apps on the **Configured Apps** tab. Any app that has at least one asset configured appears on this page. You can expand each asset to view the configured assets and available actions provided by the app. Click **Configure New Asset** to configure a new asset for the app. See Add a new Splunk SOAR (Cloud) asset.
3. (Optional) Use the dropdown menu to view different versions of the app you might have installed.
4. (Optional) Click **Unconfigured Apps** to view the list of apps installed on your Splunk SOAR (Cloud) instance that do not have at least one asset configured.
5. (Optional) Click **Orphaned Assets** to review any assets that no longer have a corresponding app installed.

Install, update, or delete apps on Splunk SOAR (Cloud)

Navigate to the Apps page to install, update, or delete Splunk SOAR (Cloud) apps.

Install a new Splunk SOAR (Cloud) app

Perform the following steps to install a new Splunk SOAR (Cloud) app:

1. Obtain the new app or develop a new app. See Splunk SOAR (Cloud) apps overview in *Develops Apps for Splunk SOAR (Cloud)*.
2. From the **Home** menu, select **Apps**.
3. Click **Install App**.
4. Drag and drop a .tar or.rpm archive of the app into the file field, or click in the file field and navigate to the location of the app file on your system.
5. Click **Install**.

You can install new apps from Splunkbase:

1. From the **Home** menu, select **Apps**.
2. Click **New Apps**.
3. A list of available apps is displayed.
    1. If you do not see the app you are looking for, you can search apps by typing search terms into the search bar at the top of the list of apps.
4. Select the app you want to install then click **Install**. If you want to install all available apps click **Install All**.
    1. If you are prompted for your credentials, use your Splunk.com login information.

After installing an app using either method, the new app is available on the **Unconfigured Apps** tab of the Apps page.

For compatibility needs, you can install multiple versions of the same app. However, only one version of the app can be active at a time. To install an incompatible app or version, see **Install or update an incompatible app or version** later in this section.

Install or update an incompatible app or version

Install incompatible apps or versions at your option. Splunk is not responsible for support or compatibility of unsupported or older, incompatible app versions you choose to install. Splunk supports only Splunk-developed compatible apps that are labeled as supported by Splunk.

You might choose to install an app that is not compatible with the version of Splunk SOAR (Cloud) you are running. To switch off automatic version checking when installing Splunk apps, community apps, and custom apps, contact Splunk Support or create a support case online. You must create a support case each time you want to switch automatic version checking on or off.

> Switching the active version of an app may have unintended consequences. For example, there might be differences among the actions, parameters, or output depending on the version of the app. Be sure to modify any playbooks as needed to be compatible with the active version of the app.

Update existing Splunk SOAR (Cloud) apps

To update an existing Splunk SOAR (Cloud) app, perform the following steps:

1. From the **Home** menu, select **Apps**.
2. Click **App Updates**.
3. Select any apps with available updates.
4. Click **Update**.

Delete a Splunk SOAR (Cloud) app

Perform the following steps to delete a Splunk SOAR (Cloud) app:

1. From the **Home** menu, select **Apps**.
2. Click the trash can () icon for the app you want to delete.
3. Click **Delete** to confirm you want to delete the app.

You can re-install any app that you deleted by downloading the app and installing the app again. Install a new Splunk SOAR (Cloud) app

View your Splunk SOAR (Cloud) assets

Splunk SOAR (Cloud) ships with one asset for the DNS, MaxMind, PhishTank, REST Data Source, and WHOIS apps already configured.

To view configured assets, perform the following tasks:

1. From the **Home** menu, select **Apps**.
2. Verify the **Configure Apps** tab is selected.
3. In any app, click the arrow icon corresponding to **configured assets** to expand the section and view the assets. For example, if an app shows **3 configured assets**, click on the arrow to view the configured assets. You can hover over the asset to edit or delete the asset.

Add, edit, or delete a Splunk SOAR (Cloud) asset

Manage the assets in your Splunk SOAR (Cloud) instance. You can add a new asset, and edit or delete existing assets.

Add a new Splunk SOAR (Cloud) asset

Perform the following steps to create a new Splunk SOAR (Cloud) asset:

1. From the **Home** menu, select **Apps**.
2. Click **Configure New Asset** for the desired app.
3. In the **Asset Name** field, enter a name for the asset such as **firewall**. This name is the one you use when referring to the asset in scripts. Specify the name as a string without spaces or punctuation.
4. (Optional) In the **Asset Description** field, enter a longer and more descriptive name for this asset, such as **Perimeter Firewall for the engineering network**.
5. (Optional) Enter one or more tags for the asset. You can use the same tag for multiple assets to group them together, and then perform actions on all assets with matching tags. See Add tags to objects in Splunk SOAR (Cloud).
6. Click **Save**.

The amount of configuration required for each asset is determined by the app. Some assets require additional configuration. For example, if you configure a QRadar asset, you must also configure settings on the **Asset Settings** and **Ingest Settings** tabs before you can save the configuration.

- Most assets require authentication information so that Splunk SOAR (Cloud) can connect to the desired server or service. You can configure authentication for an asset on the **Asset Settings** tab.
- Data ingestion settings, such as polling intervals and where to put the data once the data is ingested, are configured on the **Ingest Settings** tab. The destination for ingested data is called a container in Splunk SOAR (Cloud).

Edit a Splunk SOAR (Cloud) asset

Perform the following steps to edit a Splunk SOAR (Cloud) asset:

1. From the **Home** menu, select **Apps**.
2. Make sure the **Configured Apps** tab is selected.
3. Click on the number of configured assets in the app to expand the section.
4. In the table of configured assets, click the asset you want to edit.
5. Click **Edit**, then make any desired changes. You can edit an asset's description, tags, settings, and approval settings. To change the asset name, you must delete the current asset and create a new asset with the desired name.
6. Click **Save**.

Reassign an orphaned Splunk SOAR (Cloud) asset

You can now assign orphaned assets to an App from the user interface.

1. From **Home** > **Apps** > **Orphaned Assets** select the orphaned asset.
2. Click **Assign App**.
3. In the dropdown menu, select the App, then click **Assign**.

Delete a Splunk SOAR (Cloud) asset

Perform the following steps to delete a Splunk SOAR (Cloud) asset.

1. From the **Home** menu, select **Apps**.
2. Make sure the **Configured Apps** tab is selected.
3. Click on the number of configured assets in the app to expand the section.
4. In the table of configured assets, click the asset you want to delete.
5. Click **Delete Asset**.
6. Click **Confirm** to confirm that you want to delete the asset.

Configure advanced asset settings

Configure advanced asset settings such as the concurrent action limit, just in time (JIT) credentials, automation users, asset environment variables, and proxies.

Set the concurrent action limit

You can run concurrent actions on an existing asset, or on a new asset by following these steps:

1. From the Splunk SOAR (Cloud) **Home** menu, select **Apps**.
2. Find the app you want to run an action on and click **Configure New Asset**. Or, to run concurrent actions on an existing asset, click on your desired preexisting asset.
3. Click the **Asset Setting** tab > **Advanced**.
4. In the **Concurrent Action Limit** box, enter the number of concurrent actions you want to run on your asset. You can run up to 10 actions at once. Use caution when changing this limit as it can significantly affect performance.
5. Run the actions on an asset; evaluate performance.

For information on setting the global action concurrency limit, see Set the global action concurrency limit.

Changing this setting after saving the asset will restart the actionD daemon, interrupting all running actions and associated playbooks.

Disable action lock or action concurrency

Within an action entry, the optional lock key defines a set of parameters that you can set to run actions concurrently.

- A lock is represented by its name.
- Multiple actions locking on the same name will be serialized even if the actions are from different apps.
- In the absence of a lock dictionary, the platform runs the actions concurrently using the asset as the lock name.

To disable the lock for an action, the lock dictionary must be present and the "enabled" key set to false. When "enabled" is set to false, you can run as many concurrent actions as you like.

```
"lock": {
   "enabled": false,
   "data_path": "parameters.hash",
   "timeout": 600
}
```

Parameter	Required?	Description
enabled	Required	Boolean value that specifies if the lock is enabled or not for this action.
data_path	Optional	The name of the lock. Only valid if lock is enabled. This value is either a datapath that points to a parameter of the action with `parameters.hash` where `hash` is one of the parameters of the action, or a datapath that points to a configuration parameter for something like `configuration.server`. At runtime, the platform will read the values stored in these data paths and use it as the name of the lock. You can also use a constant string, for example, any string that does not start with `configuration.` or `parameters.`The platform will use this value as is. In case the `data_path` is not specified, the asset will be used as the lock name.
timeout	Optional	Specifies the number of seconds to wait to acquire the lock, before an error condition is reported.

If you have multiple actions with the lock enabled that are scheduled to run on an asset, you may want to exclude only some of them from running concurrently. To exclude a certain action from running concurrently, set concurrency to false in

the app JSON. When both "enabled" and "concurrency" are set to true, you can run multiple actions concurrently up to the concurrent action limit. When "enabled" is set to true and "concurrency" is set to false, you can only run a single action.

```
"lock": {
   "enabled": true,
   "concurrency": false
}
```

Parameter	Required?	Description
enabled	Required	Boolean value that specifies if the lock is enabled or not for this action.
concurrency	Optional	By default concurrency is set to `true` to allow concurrent actions to run on an app. Set concurrency to `false` to opt out of concurrent actions running on an app.

If the lock is enabled on an action, but concurrency is set to false in the app.json, the action will not be counted in the concurrent action limit you set in Asset Settings.

Configure Just In Time Credentials for a Splunk SOAR (Cloud) asset

Some assets can be configured to use just in time (JIT) credentials, which require a Splunk SOAR (Cloud) user to type in credentials before any further action is taken. Use JIT credentials if your organization has policies against providing credentials in an automated manner, or if you are using one-time passwords.

To configure JIT credentials, perform the following steps:

1. Navigate to the asset configuration page.
2. Click the **Asset Settings** tab.
3. Click **Advanced** to expand the section.
4. Click **Edit** if you are editing an existing asset. You don't need to do this if you are configuring a new asset.
5. In the **Enable Just in Time credentials for** field, select the fields for which you want to enable JIT authentication. For example, select **username** and **password** to enable JIT for login credentials.
6. Click **Save**.

Once enabled, JIT uses the asset's approval settings to determine the set of users that must supply the credentials to complete the action. See Configure approval settings for a Splunk SOAR (Cloud) asset.

To use JIT, you must have at least one approver set up for the asset. If you have selected multiple users that require a quorum to approve, then the last user (the one that would cast the final vote that causes the action to run) must be the one who supplies correct credentials. Earlier users can supply credentials, but the last user supplies the set that is actually used. Anything entered before that user is overwritten by the last user. Note that even if you have "Automatic self-approval" configured in Splunk SOAR (Cloud) for your own approval vote, you still receive a JIT prompt when credentials are required.

Configure automation users for a Splunk SOAR (Cloud) asset

Define the automation user to specify the service account Splunk SOAR (Cloud) uses to run the asset. The default account is the **automation** account provided by Splunk SOAR (Cloud).

Perform the following tasks to create a custom automation user in Splunk SOAR (Cloud):

1. Navigate to the asset configuration page.
2. Click the **Asset Settings** tab.

3. Click on **Advanced** to expand the section.
4. Click **Edit** if you are editing an existing asset. You don't need to do this is you are configuring a new asset.
5. In the **Select a user on behalf of which automated actions can be executed (e.g. test connectivity, ingestion)** field, select the desired automation user.
6. Click **Save**.

Configure environment variables for a Splunk SOAR (Cloud) asset

Global environment variables precedence over any configured in an asset.
Perform the following tasks to set environment variables for a Splunk SOAR (Cloud) asset:

1. Navigate to the asset configuration page.
2. Click the **Asset Settings** tab.
3. Click on **Advanced** to expand the section.
4. Click **Edit** if you are editing an existing asset. You don't need to do this is you are configuring a new asset.
5. Click **+ Variable** to add a new environment variable.
6. Enter the name and value of the variable.
7. (Optional) Click **Secret** to encrypt the value so that it is not displayed in the Splunk SOAR (Cloud) web interface.
8. (Optional) Click **+ Variable** to add more variables as needed.
9. Click **Save**.

See Configure proxies for a Splunk SOAR (Cloud) asset for information on how to set environment variables so that the asset can use a proxy.

Configure proxies for a Splunk SOAR (Cloud) asset

Perform the following steps to configure the environment variables needed for the app to communicate with a proxy:

1. Navigate to the asset configuration page.
2. Select the **Asset Settings** tab.
3. Select **Advanced** to expand the section.
4. Select **Edit** if you are editing an existing asset. You don't need to do this if you are configuring a new asset.
5. Select **+ Variable** to add a new environment variable.
6. Configure the **HTTP_PROXY**, **HTTPS_PROXY**, or **NO_PROXY** variables depending on the type of proxy connection.
    - For **HTTP** and **HTTPS** proxy configurations, include the protocol, hostname or IP address, and the port of the proxy server. For example: `<Protocol>://<Hostname/IP>:<Port>`
    - For **NO_PROXY** configurations, include the IP address, hostname, or domain of the asset.
7. (Optional) Select **Secret** to encrypt the value so that it is not displayed in the Splunk SOAR (Cloud) web interface.
8. Select **Save**.

The table shows an example of how to configure HTTP, HTTPS, and no proxy for a Splunk SOAR (Cloud) asset. For apps that use requests, configuring both HTTPS and HTTP environment variables directs all app traffic through the proxy server.

Proxy Name	Proxy Value
HTTP_PROXY	http://192.168.13.1:80
HTTPS_PROXY	https://192.168.13.100:8800
NO_PROXY	127.0.0.1, localhost, localhost.localdomain

When configuring the system to use an HTTP or HTTPS proxy, Splunk SOAR (Cloud) requires that you except calls to the loopback interface from the proxy list. You must set the environment variable '"NO_PROXY"' to include 127.0.0.1, localhost, and localhost.localdomain so that REST calls can be made on the loopback interface without being diverted to the proxy.

Configure ingest settings for a Splunk SOAR (Cloud) asset

Data ingestion settings are available for assets such as QRadar, Splunk, and IMAP. Perform the following steps to configure ingestion settings for a Splunk SOAR (Cloud) asset:

1. Navigate to the Asset Configuration page.
2. Click the **Ingest Settings** tab.
3. Click **Edit** if you are editing an existing asset. You don't need to do this if you are configuring a new asset.
4. In the **Label to apply to objects from this source** field, select a container label you want to apply to objects from this source. You can also type in a new label name.
5. (Optional) Configure a polling interval for the asset to ingest data.
    - Select **Interval** to configure the number of minutes between polls.
    - Select **Scheduled** to view additional options and intervals.
6. (Optional) Some assets have a **Process Missed Jobs** checkbox. Check this box if you want Splunk SOAR (Cloud) to process any missed jobs. Jobs can be missed in cases where Splunk SOAR (Cloud) is not running, or one poll didn't complete before the next one started.
7. Click **Save**.

Configure approval settings for a Splunk SOAR (Cloud) asset

Assets created with no approvers run immediately. It is usually an acceptable company policy for an asset providing a whois lookup action. For assets such as firewalls, company policies usually restrict access to the ability to change firewall settings. Any actions performed on a firewall asset must go through the approval process.

Configure the approval settings for a Splunk SOAR (Cloud) asset to determine who must approve the actions taken against the asset. See Approve actions before they run in Splunk SOAR (Cloud) in the *Use Splunk SOAR (Cloud)* manual.

To configure approval settings for an asset, perform the following steps:

1. Navigate to the asset configuration page.
2. Click the **Approval Settings** tab.
3. Click **Edit** if you are editing an existing asset. You don't need to do this if you are configuring a new asset.
4. Select the users and roles you want to configure as primary approvers. Click the arrow keys to add or remove users and roles to the **Primary Approvers** field.
5. Select the number of required primary approvers from the drop-down list in the **Required primary approvers** field.
6. Select the users and roles you want to configure as secondary approvers. Click the arrow keys to add or remove users and roles to the **Secondary Approvers** field.
7. Select the number of required secondary approvers from the drop-down list in the **Required secondary approvers** field.
8. Click **Save**.

Configure Executive approvers for a Splunk SOAR (Cloud) asset

When all SLA escalations expire without being acted on **Executive approvers** receive an SLA breach notification. To configure **Executive approvers**, follow these steps:

1. From the main menu select **Administration** then **Response**.
2. On the **Response** page uncheck **Automatic self-approval**.
3. Search for and select one or more **Executive approvers** from the list.
4. Select **Save Changes**.

Assess app and asset connectivity and ingestion

Check that your apps and assets are properly connected, are able to communicate with your Splunk SOAR (Cloud), and are ingesting data properly.

Monitor all apps and assets

Monitor all of your apps and assets with any of the methods described in this section.

View Asset Health

View the **Asset Health** panel on the Home page of Splunk SOAR (Cloud) to see the status of all of your apps and assets. Sort by **Status** to see group any assets with a **Failed** status. Select any asset to see its app page.

For information on troubleshooting connectivity for an app or asset, see Troubleshoot connectivity for a specific app or asset later in this topic.

Check status through REST API

Use the app_status REST API call to check the status of your apps and assets.

For information on how to use the REST API call, see /rest/app_status in the REST API Reference for Splunk SOAR (Cloud) documentation.

For information on troubleshooting connectivity for an app or asset, see Troubleshoot connectivity for a specific app or asset later in this topic.

Troubleshoot connectivity for a specific app or asset

Some common causes of of failed connectivity include:

- The connection is missing or improperly configured
- You don't have proper credentials to access the asset
- Splunk SOAR (Cloud) cannot connect to service

When you encounter a specific app or asset with a failed connectivity status, address the issue using steps described in this section.

Within the asset settings

To test connectivity of an app or asset with a **Failed** status, follow these steps:

1. Open the app page using one of these methods:

   - In the **Asset Health** panel, select an asset.
   - From the **Home** menu, select **Apps**. For the desired app, locate and select the configured asset.

- Select the **Asset Settings** tab.
- Select **Test Connectivity**.
- A test results message appears. Read the message and save a copy of it for your reference. Then click **Close**.
- Edit the app configuration to address the connectivity message. Check the common causes of connectivity issues described earlier in this section.

If you cannot troubleshoot the connectivity issue on your own, contact Splunk Support. For details on Splunk Support, see Administer Splunk SOAR (Cloud).

Check Ingestion Status

Your apps must be connected and also able to ingest data in order to be fully functional.

To check if your apps are able to ingest data, follow these steps:

1. In your Splunk SOAR (Cloud) instance, from the **Home** menu, select **Administration**.
2. Select **Ingestion Summary** and view the chart. Check that the values on the chart are not all zeros.
3. Select **Ingestion Status**. The first section of the page shows successful ingestion for your apps. Review the **Ingestion Errors** section to see if there are any errors.

If there are ingestion errors:

- If you have not done so already, check the app's connectivity and troubleshoot any issues, as described in Monitor all apps and assets and Troubleshoot connectivity for a specific app or asset earlier in this topic.
- If the app is connected, but it is not ingesting data properly, contact Splunk Support. For details on Splunk Support, see Administer Splunk SOAR (Cloud).

For additional information on data ingestion, see View how much data is ingested in Splunk SOAR (Cloud) using ingestion summary and View ingested container statistics using Ingestion Status.

Splunk SOAR (Cloud) telemetry

Share data from Splunk SOAR (Cloud)

When Splunk SOAR (Cloud) is deployed, the platform sends usage data to Splunk Inc. ("Splunk") to provide, support, and optimize your deployment and to help improve Splunk SOAR (Cloud) in future releases.

How data is collected

Splunk SOAR (Cloud) uses several technologies running in the background to collect usage data.

- Splunk Web Analytics (swa.js)
- FullStory

Usage Data Telemetry

A Splunk SOAR (Cloud) background task runs at a specified system time to collect telemetry data which is transmitted to Splunk's products-telemetry server.

Each time a user logs in some system settings and license metrics are collected.

FullStory is used to collect experiential user journey information from the Visual Playbook Editor with user personally identifiable information redacted.

For information about the Visual Playbook Editor see Use playbooks to automate analyst workflows in Splunk SOAR (Cloud) in *Build Playbooks with the Playbook Editor*.

How data is stored

Splunk's retention timeframes for Usage Data are described here. For more information about Splunk's data collection and privacy practices see the Splunk Privacy Policy and learn how Splunk Protects.

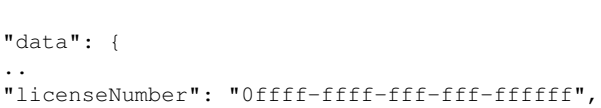
Telemetry impacts on performance

Collecting telemetry data minimally affects database performance and the loading of the Splunk SOAR (Cloud) UI.

General Usage Data

Splunk SOAR (Cloud) telemetry collects the following basic usage information:

Name	Description	
		Items in this section apply to all telemetry

`app.session.soar.*`
 	
`automation.*`
 	
`automation.summary.*`
	Either:
	• **companyID**: Splunk SOAR (On-premises), a SHA256 has of the company name as listed in the license, or
		

Name	Description	

orchestration.*	• **stackID**: Splunk SOAR (Cloud), a SHA256 hash of the stack name
	
	And:
	
	• **licenseNumber**: the license key that was issued to your deployment.
	• **licenseIssueDate**: the date the license was issued.
	• **licenseExpirationDate**: the date the license will expire.
	• **licenseInstance**: Internal Salesforce ticket number to issue the license.
	
	Splunk SOAR sends the deploymentID with every event. This change adds either **companyID** or **stackID** and **licenseNumber**, **licenseIssueDate**, **licenseExpirationDate**, and **licenseInstance** wherever **deploymentID** is currently logged.
		<pre>"licenseExpirationDate": "2024-12-22",
		"licenseInstance": "12304",
		},
		"timestamp": 1684779074013,
		"component": "app.session.soar.systemSettings",
		"deploymentID": "soar-c48ed12b-262f-47e1-99b0-d2ba5
		"companyID": "f3f5d1d9aba493153151e468915ca995a3355
		"eventID": "a74fd484-8d28-c0e8-c5bf-0b9ebf130665",
		"experienceID": "0b64f885-637b-9d67-289a-b4d4925e17
		}
		
		{
		"data": {
		...
		"licenseNumber": "0ffff-ffff-fff-fff-ffffff",
		"licenseIssueDate": "2024-12-22",
		"licenseExpirationDate": "2024-12-22",
		"licenseInstance": "12304",
		},
		"timestamp": 1684779074013,
		"component": "app.session.soar.systemSettings",
		"deploymentID": "soar-c48ed12b-262f-47e1-99b0-d2ba5
		"companyID": "f3f5d1d9aba493153151e468915ca995a3355
		"eventID": "a74fd484-8d28-c0e8-c5bf-0b9ebf130665",
		"experienceID": "0b64f885-637b-9d67-289a-b4d4925e17
		}</pre>
		Or
		
		<pre>{
		"data": {
		...
		"licenseNumber": "0ffff-ffff-fff-fff-ffffff",
		"licenseIssueDate": "2024-12-22",
		"licenseExpirationDate": "2024-12-22",
		"licenseInstance": "12304",
		},
		"timestamp": 1684779074013,
		"component": "app.session.soar.systemSettings",
		"deploymentID": "soar-c48ed12b-262f-47e1-99b0-d2ba5
		"stackID": "f3f5d1d9aba493153151e468915ca995a335569
		"eventID": "a74fd484-8d28-c0e8-c5bf-0b9ebf130665",
		"experienceID": "0b64f885-637b-9d67-289a-b4d4925e17
		}</pre>

		app.session. objects

app.session.soar.apiTime	Reports roundtrip time consumption for each API request.	<pre>data: {
		app: soar
		endpoint: /rest/ph_user/3/permissions
		method: get
		page: UNKNOWN_PAGE
		status: 200
		time: 150
		soarDeploymentID: soar-a2a983de-38ec-42d7-a179-30
		soarUserID: 5d900c28b8d1555745c09908ef386860
		}
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca8</pre>

Name	Description	
		eventID: 551e5c46-4f71-d92a-51ba-30cf97ae3a97 experienceID: 6c2c534b-e750-e1a0-95fd-fcada1a50be0 optInRequired: 3 timestamp: 1574213030362 visibility: anonymous

app.session.soar.error	Reports uncaught errors of front-end Splunk SOAR scripts.	data: {
		app: soar
		errorMsg: Uncaught ReferenceError: helloworld is n
		file: /inc/swa/swa_enabled.js
		page: admin.product_settings.telemetry
		position: 74:1
		soarDeploymentID: soar-a2a983de-38ec-42d7-a179-300
		soarUserID: 5d900c28b8d1555745c09908ef386860
		}
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca8
		eventID: 94efce66-ab89-33ae-f894-1cceb8f68f78
		experienceID: 239facf6-261d-dd96-be08-33870c7d3750
		optInRequired: 3
		timestamp: 1574294947704
		visibility: anonymous

app.session.soar.license	Reports license status, limits, and usage information. Sent once per session.
	• **usage**: Usage metrics of user **activeUsersCount**, a count of users who logged in in the past day.
	• **app**: "soar"
	• **page**: UNKNOWN_PAGE (this item is not being tracked)
	• **type**: Type of license (standard, community, dev)
	• **issueDate**: timestamp when license issued
	• **expirationDate**: timestamp when license is due to expire
	• **limits**: Maximum usage allowed with the current license
	• **limit.apps**: the maximum number of apps the deployment can have, as set by your license.
	• **limit.assets**: the maximum number of assets the deployment can has, as set by your license.
		{
		'type': 'standard',
		'issueDate': 1616371200.0,
		'expirationDate': 4769971200.0,
		'companyName':
		'limits': {
		'actions': 'unlimited', (NEW)
		'apps': 'unlimited',
		'assets': 'unlimited', (NEW)
		'events': 'unlimited',
		'users': 'unlimited',
		'tenants': 1,
		'seats': 'unlimited'
		},
		'productVersion': '10155.0.0.124976',
		'usage': {
		'recentAppRunCount': 0,
		'recentPlaybookRunCount': 0,
		'recentDebugRunCount': 0,
		'seatCount': 1,
		'activeUsersCount': 2,
		}
		}

app.session.soar.pageview	Reports which pages are visited by users.	data: {
		app: soar
		page: admin.company_settings.info
		soarDeploymentID: soar-a2a983de-38ec-42d7-a179-300
		soarUserID: 5d900c28b8d1555745c09908ef386860
		}

Name	Description	
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca8 eventID: 0db11144-7c14-88f7-b3e9-3a999102bfc6 experienceID: 20d4d671-7d18-f74a-c72f-9811b5bee20d optInRequired: 3 timestamp: 1574210581565 visibility: anonymous

app.session.soar.
systemSettings
	Reports the feature on/off settings and product version.
	• **credentialManager**: which credential manager is in use.
	• **app**: "phantom"
	• **page**: UNKNOWN_PAGE (This item is not being tracked)
	• **isClusteringEnabled**
	• **isMultiTenantEnabled**
	• **numberofClusterNodes**
	• **productVersion**: Version number of the Splunk SOAR or Splunk Phantom instance
		{
		"optInRequired": 3,
		"original_timestamp": 1684779074013,
		"visibility": "anonymous",
		"data": {
		"cloudWorksEnvironment": "stg",
		"isClusteringEnabled": false,
		"numOfClusterNodes": 0,
		"isMultiTenantEnabled": false,
		"nodeGUID": "057f9e04-d54c-4ccc-9ffb-4aa82551b4d6
		"page": "UNKNOWN_PAGE",
		"isElasticSearchEnabled": false,
		"credential_manager": "hashicorp",
		"splunkConfig": {
		"searchLocation": "local",
		"searchType": "standalone"
		},
		"app": "soar",
		"missionControlDeploymentID": null,
		"soarDeploymentID": "soar-c48ed12b-262f-47e1-99b0
		"license": "standard",
		"soarUserID":
"5ebe9df18591550e99cd82079e8448a1c14582f0c04cfd84ea
		"productVersion": "10155.0.0.124976"
		},
		"timestamp": 1684779074013,
		"component": "app.session.soar.systemSettings",
		"deploymentID": "soar-c48ed12b-262f-47e1-99b0-d2ba5
		"eventID": "a74fd484-8d28-c0e8-c5bf-0b9ebf130665",
		"experienceID": "0b64f885-637b-9d67-289a-b4d4925e17
		}

app.session.session_start	Reports the browser and OS, along with their versions.	{
		data: {
		app: UNKNOWN_APP
		browser: Chrome
		browserVersion: 78.0.3904.97
		device: MacIntel
		locale: en-US
		os: Mac OS X
		osVersion: 10.
		page: UNKNOWN_PAGE
		splunkVersion: not available
		}
		eventID: d9ca862c-d48d-83a1-d1bb-f0f25f4b5af8
		experienceID: 6c2c534b-e750-e1a0-95fd-fcada1a50be0
		optInRequired: 3
		timestamp: 1574213029
		visibility: anonymous
		}

Name	Description	
app.session.phantom.viewTime	Reports time spent on a specific page. Only tracked for specific pages.	{ data: { app: phantom page: reports viewTime: 10223 phantomDeploymentID: phantom-a2a983de-38ec-42d7-a1 phantomUserID: 5d900c28b8d1555745c09908ef386860 } eventID: 545fdcfb-ac0d-a11b-da6a-4b9da84b6c2a experienceID: 85b49544-fb90-a2ef-1b3f-e09339f3abc1 optInRequired: 3 timestamp: 1573690198763 visibility: anonymous }

app.session.soar.vpe	Reports:
	• VPE version (Classic or Modern)
	• The types of blocks in a playbook
	• The number of blocks in a playbook
	• Which hotkey shortcuts were used while editing a playbook
	• Specific Splunk SOAR features used in a playbook
		component: app.session.soar.vpe
		data: {
		app: soar
		jsonSchemaVersion:"5.0.3"
		page: UNKNOWN_PAGE
		blocks: {
		totalCount: 14
		blockTypes: {
		action: 2
		playbook: 1
		code: 1
		utility: 1
		filter: 1
		decision: 1
		format: 6
		prompt: 1
		}
		customCodeBlockCount: 3
		customCodeBlockTypeCounts: {
		start: 0
		end: 1
		action: 2
		playbook: 0
		code: 0
		utility: 0
		filter: 0
		decision: 0
		format: 0
		prompt: 0
		}
		actions: ["geolocate ip", "whois domain"]
		}
		hotkeys: {
		totalCount: 14
		interactions: {
		addMiniMenu: 7
		addActionBlock: 6
		addPlaybookBlock: 0
		addCodeBlock: 0
		addUtilityBlock: 0
		addFilterBlock: 0
		addDecisionBlock: 0
		addFormatBlock: 1

Name	Description	

		addPromptBlock: 0
		autoArrange: 1
		zoomToFit: 1
		zoomIn: 0
		zoomOut: 0
		savePlaybook: 1
		deleteNode: 0
		toggleEditor: 1
		toggleDebugger: 1
		toggleSettings: 1
		showShortcutModal: 1
		}
		}
		features: {
		customConditionLabel: 3
		customDatapaths: 2
		playbookInputs: {
		count: 0
		dataTypes: {
		"domain": 0
		"file id": 0
		"file name": 0
		"file path": 0
		"hash": 0
		"host name": 0
		"ip": 0
		"mac address": 0
		"port": 0
		"process name": 0
		"url": 0
		"user name": 0
		}
		}
		playbookOutputs: {
		count: 1
		dataTypes: {
		"domain": 1
		"file id": 0
		"file name": 0
		"file path": 0
		"hash": 0
		"host name": 0
		"ip": 0
		"mac address": 0
		"port": 0
		"process name": 0
		"url": 0
		"user name": 0
		}
		dedupeCount: 0
		}
		}
		playbookType: automation
		playbookName: 5d900c28b8d1555745c09908ef133337
		soarDeploymentID: soar-a2a983de-38ec-42d7-a179-300
		soarUserID: 5d900c28b8d1555745c09908ef386860
		}
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca8
		eventID: d4b331e7-3ce3-91b6-7724-bc4d7235bca9

Name	Description	

		experienceID: 21febb16-c3f6-cbd5-ffac-905f1466c830
		optInRequired: 3
		timestamp: 1576695256840
		visibility: anonymous
		
		{
		data: {
		app: soar
		jsonSchemaVersion:"5.0.3"
		page: UNKNOWN_PAGE
		blocks: {
		totalCount: 14
		blockTypes: {
		action: 2
		playbook: 1
		code: 1
		utility: 1
		filter: 1
		decision: 1
		format: 6
		prompt: 1
		}
		customCodeBlockCount: 3
		customCodeBlockTypeCounts: {
		start: 0
		end: 1
		action: 2
		playbook: 0
		code: 0
		utility: 0
		filter: 0
		decision: 0
		format: 0
		prompt: 0
		}
		actions: ["geolocate ip", "whois domain"]
		}
		hotkeys: {
		totalCount: 14
		interactions: {
		addMiniMenu: 7
		addActionBlock: 6
		addPlaybookBlock: 0
		addCodeBlock: 0
		addUtilityBlock: 0
		addFilterBlock: 0
		addDecisionBlock: 0
		addFormatBlock: 1
		addPromptBlock: 0
		autoArrange: 1
		zoomToFit: 1
		zoomIn: 0
		zoomOut: 0
		savePlaybook: 1
		deleteNode: 0
		toggleEditor: 1
		toggleDebugger: 1
		toggleSettings: 1
		showShortcutModal: 1

Name	Description	

		}
		}
		features: {
		customConditionLabel: 3
		customDatapaths: 2
		playbookInputs: {
		count: 0
		dataTypes: {
		"domain": 0
		"file id": 0
		"file name": 0
		"file path": 0
		"hash": 0
		"host name": 0
		"ip": 0
		"mac address": 0
		"port": 0
		"process name": 0
		"url": 0
		"user name": 0
		}
		}
		playbookOutputs: {
		count: 1
		dataTypes: {
		"domain": 1
		"file id": 0
		"file name": 0
		"file path": 0
		"hash": 0
		"host name": 0
		"ip": 0
		"mac address": 0
		"port": 0
		"process name": 0
		"url": 0
		"user name": 0
		}
		dedupeCount: 0
		}
		}
		playbookType: automation
		playbookName: 5d900c28b8d1555745c09908ef133337
		soarDeploymentID: soar-a2a983de-38ec-42d7-a179
		soarUserID: 5d900c28b8d1555745c09908ef386860
		}
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087
		eventID: d4b331e7-3ce3-91b6-7724-bc4d7235bca9
		experienceID: 21febb16-c3f6-cbd5-ffac-905f1466c8
		optInRequired: 3
		timestamp: 1576695256840
		visibility: anonymous
		}

app.session.soar.vpeTime	Reports the time in milliseconds it took for the VPE to load in the browser.	component: app.session.soar.vpeTime
		data: {
		app: soar
		pageLoadTime: 10298
		}

Name	Description	

		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca8
		eventID: d4b331e7-3ce3-91b6-7724-bc4d7235bca9
		experienceID: 21febb16-c3f6-cbd5-ffac-905f1466c830
		optInRequired: 3
		timestamp: 1576695256840
		visibility: anonymous
		
		{
		data: {
		app: soar
		pageLoadTime: 10298
		}
		deploymentID: soar-a2a983de-38ec-42d7-a179-30087b0ca
		eventID: d4b331e7-3ce3-91b6-7724-bc4d7235bca9
		experienceID: 21febb16-c3f6-cbd5-ffac-905f1466c830
		optInRequired: 3
		timestamp: 1576695256840
		visibility: anonymous
		}

		automation.summary objects

automation.summary.app_summary	A summary of apps installed on the system.
	• **app_name**: The human-readable name of the app.
	• **description**: A description of what the app does.
	• **version**: The version number of the app.
	• **product_name**: The product name of the app.
	• **product_vendor**: The product vendor of the app.
		{
		'type': 'event',
		'component': 'automation.summary.app_summary',
		'data': {
		'app_name': 'MaxMind',
		'description': 'This app provides IP geolocation with
		'version': '2.2.5',
		'product_name': 'GeoIP2',
		'product_vendor': 'MaxMind',
		'soarDeploymentID': 'soar-e25f2b02-b4c3-43ae-a40c-acf
		'license': 'community',
		'productVersion': '6.1.0.58',
		'missionControlDeploymentID': None,
		'cloudWorksEnvironment': 'dev'
		},
		'deploymentID': 'soar-e25f2b02-b4c3-43ae-a40c-acf2e
		'optInRequired': 3,
		'version': None,
		'timestamp': 1685128654000,
		'visibility': [
		'anonymous'
		]
		}

automation.summary.
case_summary
	A summary of opened and closed cases in the last 24 hours.
	• **opened**: The number of created cases in the last 24 hours.
	• **closed**: The number of cases closed in the last 24 hours.
	• **promoted**: The number of items promoted to a case in the last 24 hours.
		{
		'type': 'aggregate',
		'component': 'automation.summary.case_summary',
		'data': {
		'opened': 120,
		'closed': 87,
		'promoted': 12,
		'phantomDeploymentID': 'phantom-e25f2b02-b4c3-43ae-a4
		'license': 'community',
		'productVersion': '6.1.0.58',
		'missionControlDeploymentID': None
		},

Name	Description	
		'deploymentID': 'phantom-e25f2b02-b4c3-43ae-a40c-ac 'optInRequired': 3, 'version': None, 'timestamp': 1685658250000, 'visibility': ['anonymous'], 'indexData': True, 'begin': 1685491200000, 'end': 1685577599000 }

automation.summary.
ingestion_status
	Ingestion status and events ingested per Splunk SOAR deployment.
	• **adhoc**: Counts of adhoc ingestion runs by status
	• **automated**: Counts of automated ingestion runs by status
	• **all**: Counts of both ingestion runs by status
	♦ Succesful
	♦ Failed
	♦ Running
	♦ Total
	• **event_ingested_count**: Count of events ingested over the past day
		{
		'type': 'aggregate',
		'component': 'automation.summary.ingestion_status',
		'data': {
		'adhoc': None,
		'automated': None,
		'all': {
		'total': 1,
		'success': 1,
		'failed': 0,
		'running': 0
		},
		'event_ingested_count': 1,
		'soarDeploymentID': 'soar-c48ed12b-262f-47e1-99b0-d2b
		'license': 'standard',
		'productVersion': '10155.0.0.124976',
		'missionControlDeploymentID': None,
		'cloudWorksEnvironment': 'stg'
		},
		'deploymentID': 'soar-c48ed12b-262f-47e1-99b0-d2ba5
		'optInRequired': 3,
		'version': None,
		'timestamp': 1684358758000,
		'visibility': [
		'anonymous'
		],
		'indexData': True,
		'begin': 1684281600000,
		'end': 1684367999000
		}

automation.summary.
playbook_names
	A summary of playbooks names and whether or not a playbook is custom.
	• **community**: The list of playbook names that are community playbooks that were updated over the last day.
	• **custom**: The list of playbooks that are custom made by the end user that were updated over the last day.
	• **custom_count**: A count of playbooks that are custom made by the end user that
		{
		'type': 'aggregate',
		'component': 'automation.summary.playbook_names',
		'data': {
		'community': [
		'AD_LDAP_Entity_Attribute_Lookup',
		'wannacry_prevent',
		'wannacry_remediate',
		'zscaler_hunt_and_block_url',
		'zscaler_malicious_file_response',
		'zscaler_patient_0_parse_email'
		],
		'community_count': 136,
		'custom': [
		'testa1'

Name	Description	
	were updated over the last day. • **community_count**: A count of playbooks that are community playbooks that were updated over the last day.	], 'custom_count': 1, 'phantomDeploymentID': 'phantom-e25f2b02-b4c3-43a 'license': 'community', 'productVersion': '6.1.0.58', 'missionControlDeploymentID': None }, 'deploymentID': 'phantom-e25f2b02-b4c3-43ae-a40c-ac 'optInRequired': 3, 'version': None, 'timestamp': 1685658250000, 'visibility': ['anonymous'], 'indexData': True, 'begin': 1685491200000, 'end': 1685577599000 }

automation.summary.
playbook_runs.by_trigger
	Counts of playbook runs by trigger, either adhoc or by automation, aggregated over the last day. Emitted once daily.	begin: 1663891200000
		component: automation.summary.playbook_runs.by_tri
		data: {
		adhoc: {
		failed: 0
		running: 0
		success: 2
		total: 2
		}
		all: {
		failed: 0
		running: 0
		success: 2
		total: 2
		}
		automated: {
		failed: 0
		running: 0
		success: 0
		total: 0
		}
		cloudWorksEnvironment: dev
		missionControlDeploymentID: 917660C8-50E1-407B-8
		soarDeploymentID: soar-cd07b53e-125e-4d27-adf7-2
		
		productVersion: 10155.0.0.98349
		license: standard
		}
		deploymentID: soar-cd07b53e-125e-4d27-adf7-2dba77b
		end: 1663977599000
		indexData: true
		optInRequired: 3
		timestamp: 1663977609000
		type: aggregate
		visibility: [
		anonymous
		]
		}

Name	Description	

`automation.summary.publish_telemetry_time_taken`	Start time, end time, and a the calculated total time of the telemetry publish job.
	• **start_time**: start time of the publish job
	• **end_time**: end time of the publish job
	• **total_time**: total time of the job (calculated by taking **end_time** then subtracting **start_time**)
		{
		'type': 'event',
		'component': 'automation.summary.publish_telemetry_
		'data': {
		'start_time': 28244.781,
		'end_time': 28244.812,
		'total_time': 0.031,
		'soarDeploymentID': 'soar-e25f2b02-b4c3-43ae-a40c-acf
		'license': 'community',
		'productVersion': '6.1.0.58',
		'missionControlDeploymentID': None,
		'cloudWorksEnvironment': 'dev'
		},
		'deploymentID': 'soar-e25f2b02-b4c3-43ae-a40c-acf2e
		'optInRequired': 3,
		'version': None,
		'timestamp': 1685128654000,
		'visibility': [
		'anonymous'
		],
		'indexData': True,
		'begin': None,
		'end': None
		}

`automation.summary.workbook_summary`	A summary of opened and closed workbooks.
	• **opened**: statistics for workbook tasks and phases created in the last 24 hours.
	♦ **unique_containers**
	♦ **total_tasks**
	♦ **total_phases**
	• **started**: statistics for workbook tasks and phases started in the last 24 hours.
	♦ **unique_containers**
	♦ **total_tasks**
	♦ **total_phases**
	• **closed**: statistics for workbook tasks and phases closed in the last 24 hours.
	♦ **unique_containers**
	♦ **total_tasks**
	♦ **total_phases**
		{
		'type': 'aggregate',
		'component': 'automation.summary.case_summary',
		'data': {
		'opened': {
		'unique_containers': 3,
		'total_tasks': 15,
		'total_phases': 45,
		},
		'started': {
		'unique_containers': 2,
		'total_tasks': 2,
		'total_phases': 4,
		},
		'closed': {
		'unique_containers': 2,
		'total_tasks': 4,
		'total_phases': 12,
		},
		'phantomDeploymentID': 'phantom-e25f2b02-b4c3-43ae-a4
		'license': 'community',
		'productVersion': '6.1.0.58',
		'missionControlDeploymentID': None
		},
		'deploymentID': 'phantom-e25f2b02-b4c3-43ae-a40c-ac
		'optInRequired': 3,
		'version': None,
		'timestamp': 1685658250000,
		'visibility': [
		'anonymous'
		],
		'indexData': True,
		'begin': 1685491200000,

Name	Description	
		'end': 1685577599000 }
		orchestration. objects

orchestration.summary.
action_runs.by_trigger
	Counts of action runs by trigger, either adhoc or by automation, aggregated over the last day. Emitted once daily.
	
	adhoc: Counts of adhoc action runs by status
	
	• Succesful
	• Failed
	• Running
	• Pending
	• Total
	
	automated: Counts of automated action runs by status
	
	all: Counts of both adhoc and automated playbook runs by status
	
	cloudWorksEnvironment: The environment in which the Splunk SOAR cloud stack is deployed; development (dev), staging (stg), or live (lve).
	
	missionControlDeploymentID: A nullable field identifying the Splunk Mission Control instance paired to the Splunk SOAR instance
	
	soarDeploymentID: Uniquely identifies the Splunk SOAR stack that emitted the metric
		{
		begin: 1663891200000
		component: orchestration.summary.action_runs.by_tr
		data: {
		adhoc: {
		failed: 0
		pending: 0
		running: 0
		success: 1
		total: 1
		}
		all: {
		failed: 5
		pending: 0
		running: 0
		success: 5
		total: 10
		}
		automated: {
		failed: 5
		pending: 0
		running: 0
		success: 4
		total: 9
		}
		cloudWorksEnvironment: dev
		missionControlDeploymentID: 917660C8-50E1-407B-8
		soarDeploymentID: soar-cd07b53e-125e-4d27-adf7-2
		
		productVersion: 10155.0.0.98349
		license: standard
		}
		deploymentID: soar-cd07b53e-125e-4d27-adf7-2dba77b
		end: 1663977599000
		indexData: true
		optInRequired: 3
		timestamp: 1663977609000
		type: aggregate
		visibility: [
		anonymous
		]
		}

Monitor your Splunk SOAR (Cloud) system health

Monitor the health of your Splunk SOAR (Cloud) system

Use the System Health page to view a summary of your Splunk SOAR (Cloud) instance. The System Health page includes the following information:

- Running status of Splunk SOAR (Cloud) processes
- Resource consumption
- Health and status of critical processes

Use the System Health page as a starting point to begin troubleshooting issues. Splunk support might ask for the results of this page to start a troubleshooting investigation.

Perform the following tasks to get to the System Health page:

1. From the main menu, select **Administration**.
2. Select **System Health > System Health**.

The following image shows the System Health page for a standalone, non-clustered Splunk SOAR (Cloud) instance. Additional selections such as a selector for individual nodes and ClusterD statistics are available on the System Health page in a clustered deployment. A clustered deployment doesn't have the Database Disk Space panel since the database in a cluster lives on a different host.

The top row of graphs shows you the status of the following system-wide resources:

- Memory usage
- Load average
- Disk usage

Each row after the top row represents the individual system processes important to Splunk SOAR (Cloud). Verify that each process has a green **Running** status icon. Click **Restart** if you need to restart any one of the individual processes.

Splunk SOAR (Cloud) runs on top of Linux, so these graphs can be interpreted as you might on any Linux system. On a fairly idle Splunk SOAR (Cloud) system, there might be a significant amount of free memory, unused swap, and a lower load compared to the number of allocated CPU cores. There might also be more free disk space for the database and files.

The Splunk SOAR (Cloud) processing daemons `IngestD`, `DecideD`, `WorkflowD`, and `ActionD` perform various scheduling, decision, and management functions as well as critical background functions. All four must be running in order for Splunk SOAR (Cloud) to work properly. Splunk SOAR (Cloud) also relies on `HTTPD` and `Postgres`, which is the database.