# Table of Contents

**Introduction** .................................................................................................................................................. 1

Administer Splunk Phantom.......................................................................................................................... 1

**Configure your company's settings** ........................................................................................................ 2

Configure your company settings in Splunk Phantom...................................................................................... 2

Configure the ROI Settings dashboard........................................................................................................... 2

Obtain and configure a Splunk Phantom license............................................................................................ 3

**Configure administration settings** ........................................................................................................... 6

Configure a source control repository for your Splunk Phantom playbooks....................................................... 6

Customize email templates in Splunk Phantom.............................................................................................. 8

Configure search in Splunk Phantom........................................................................................................... 9

Configure Google Maps for visual geolocation data....................................................................................... 11

Manage your organization's credentials with a password vault....................................................................... 11

Set environment variables globally for all apps.............................................................................................. 13

Add tags to objects in Splunk Phantom......................................................................................................... 14

Create custom CEF fields in Splunk Phantom.............................................................................................. 15

Reset the admin and root passwords in Splunk Phantom.............................................................................. 16

**Configure settings for your Splunk Phantom instance** ............................................................................. 19

Enable clickable URLs in CEF data............................................................................................................. 19

View cluster status and enable or disable a cluster...................................................................................... 19

Configure multiple tenants on your Splunk Phantom instance.......................................................................... 19

View related data using aggregation rules...................................................................................................... 21

Define tasks using workbooks....................................................................................................................... 23

Tune performance by managing Splunk Phantom features........................................................................ 25

**Configure settings for your system's events** .............................................................................................. 28

Create custom status labels in Splunk Phantom.............................................................................................. 28

Create custom severity names......................................................................................................................... 28

Create custom fields to filter Splunk Phantom events.................................................................................... 29

Track information about an event or case using HUD cards......................................................................... 30

Configure the response times for service level agreements........................................................................ 31

Configure how events are resolved............................................................................................................ 32

Configure labels to apply to containers......................................................................................................... 32

Use whitelist to grant authorized access....................................................................................................... 33

**Manage your Splunk Phantom users and accounts** .................................................................................... 34

Manage Splunk Phantom users..................................................................................................................... 34

Manage roles and permissions in Splunk Phantom....................................................................................... 37

Configure password requirements and timeout intervals to secure your Splunk Phantom accounts................ 40

Configure single sign-on authentication for Splunk Phantom.......................................................................... 40

Secure Splunk Phantom using two factor authentication........................................................................... 45

Configure role based access control inside Splunk Phantom apps............................................................... 46

Secure Splunk Phantom by configuring an account password expiration................................................... 47
# Table of Contents

## Manage your registered mobile devices
- Manage your registered mobile devices ...................................................... 48
- Enable or disable registered mobile devices ............................................. 48

## Monitor the health of your system
- Monitor the health of your Splunk Phantom system ........................................ 50
- View how much data is ingested in Splunk Phantom using ingestion summary ................................................. 50
- View ingested container statistics using Ingestion Status ......................... 51
- Configure the logging levels for Splunk Phantom daemons ....................... 52
- Enable and download audit trail logs in Splunk Phantom ........................... 56
- Locate long-running playbooks for debugging or troubleshooting in Splunk Phantom ............................................... 58
- View the playbook run history in Splunk Phantom .................................. 58
- View the action run history ..................................................................... 58
- Use ITSI to monitor the health of your Splunk Phantom deployment ........ 59

## Manage Splunk Phantom Apps and Assets
- Add and configure apps and assets to provide actions in Splunk Phantom ........ 60

## Backup or restore your Splunk Phantom instance
- Splunk Phantom backup and restore overview .......................................... 67
- Back up a Splunk Phantom deployment .................................................... 67
- Restore Splunk Phantom from a backup .................................................. 71
- Splunk Phantom backup tools .................................................................. 76
- Use ibackup.pyc with warm standby ....................................................... 77

## Create and manage a warm standby
- Warm standby feature overview .............................................................. 81
- Create a warm standby .......................................................................... 81
- Failover to the warm standby ................................................................. 83
- Disable warm standby ........................................................................... 86
- Recreate warm standby after a failover ................................................... 87
- Upgrade or maintain warm standby instances ........................................ 88
- Warm standby tools .............................................................................. 89

## Configure your Splunk Phantom telemetry
- Share data from Splunk Phantom ............................................................ 91
Introduction

Administer Splunk Phantom

Splunk Phantom is a world-class Security Orchestration, Automation, and Response (SOAR) system. The Splunk Phantom platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools together.

This manual is intended to be used by the person or team administering the Splunk Phantom system.

The following topics are discussed in this manual:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Settings</td>
<td>Information about your company, contacts, and your Splunk Phantom license.</td>
</tr>
<tr>
<td>Administration Settings</td>
<td>All the settings to configure the behavior and appearance of Splunk Phantom.</td>
</tr>
<tr>
<td>Product Settings</td>
<td>Settings for the Splunk Phantom product that apply to your deployment, such as clustering, multi-tenancy, and case management.</td>
</tr>
<tr>
<td>Event Settings</td>
<td>Settings to configure the organization, handling, and presentation.</td>
</tr>
<tr>
<td>User Management</td>
<td>Settings related to user accounts, permissions, and authentication.</td>
</tr>
<tr>
<td>Mobile</td>
<td>Enable or disable registered mobile devices.</td>
</tr>
<tr>
<td>System Health</td>
<td>Information and reports for monitoring the Splunk Phantom deployment.</td>
</tr>
<tr>
<td>Apps and Assets</td>
<td>How to add and configure apps and assets to provide actions in Splunk Phantom.</td>
</tr>
<tr>
<td>Backup and restore</td>
<td>Information and instructions for performing backup and restore operations.</td>
</tr>
<tr>
<td>Telemetry</td>
<td>Information about sharing data from Splunk Phantom.</td>
</tr>
</tbody>
</table>

See also

• How can Splunk Phantom be installed? in Install and Upgrade Splunk Phantom.
• Create playbooks to automate analyst workflows in Splunk Phantom in Use Splunk Phantom.
Configure your company's settings

Configure your company settings in Splunk Phantom

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>The name of the company used in emails sent by Splunk Phantom.</td>
</tr>
<tr>
<td>IT Contact</td>
<td>The email address of the OS system administrator for Splunk Phantom. System-level alerts are sent to this email address.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>A unique name used to identify a certain instance of Splunk Phantom. Instance names are randomly generated and can be changed if desired, but changing the instance name is not required. Use instance names to identify your chosen instance for the mobile app.</td>
</tr>
<tr>
<td>System Time Zone</td>
<td>The time zone for the host system of the virtual appliance that the Splunk Phantom instance runs on.</td>
</tr>
<tr>
<td>Base URL for the Splunk Phantom Appliance</td>
<td>The URL used to access Splunk Phantom. Set this URL to https:// followed by the IP address or DNS name of the Splunk Phantom instance. Don't specify a trailing slash at the end of the base URL.</td>
</tr>
</tbody>
</table>

Configure the ROI Settings dashboard

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTE Gained</td>
<td>Enable this toggle make the FTE Gained widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk Phantom divides the number of actions run by automation (calculated in Splunk Phantom) 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).</td>
</tr>
<tr>
<td>Time Saved</td>
<td>Enable this toggle make the Time saved widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk Phantom sums the difference between the Analyst Minutes Per Action (configured on the ROI settings page) and the actual minutes per action (calculated in Splunk Phantom) over all actions for the past 24 hours.</td>
</tr>
<tr>
<td>Money Saved</td>
<td>Enable this toggle make the Dollars saved widget available in the Automation ROI Summary dashboard. To calculate this value, Splunk Phantom 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 Phantom).</td>
</tr>
<tr>
<td>Annual analyst salary</td>
<td>The average annual salary paid to each analyst.</td>
</tr>
<tr>
<td>Currency</td>
<td>The national currency value you want to use in the display.</td>
</tr>
<tr>
<td></td>
<td>The typical number of hours each analyst works per day.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Analyst hours per day</td>
<td>The average number of minutes an analyst typically spends on any action in a case.</td>
</tr>
<tr>
<td>Minutes per action</td>
<td></td>
</tr>
</tbody>
</table>

Use the Splunk App for Phantom Reporting to view more granular breakdowns of individual action runtimes. The Splunk App for Phantom Reporting sends Splunk Phantom log data back to the Splunk platform. You can use this data to generate or modify reports as needed.

The Splunk App for Phantom Reporting is not supported by Splunk. See App support types in *Working with Splunkbase*.

**Obtain and configure a Splunk Phantom license**

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

There are three types of licenses available for Splunk Phantom:

- **Community License**
  This is the default, free license for everyone who registers for Splunk Phantom Community access and downloads Splunk Phantom. This license is limited to a set number of actions per day. See Community License.

- **Event-based License**
  This license type is based on the number of events created or updated in the twenty-four hour tracking period. Individual licenses vary in terms of volume.

- **Seat-based License**
  This license is governed by the number of users allowed to log in to Splunk Phantom. Seat-based licensing is available in blocks of five seats and can vary by the number of tenants.

The number of tenants is purchased as an additional parameter for both event-based and seat-based licenses.

If a license is removed or expires, Splunk Phantom reverts to the community license.

**Community license**

Splunk Phantom installs with a default license, the Community License. The Community License is limited to:

- 100 licensed actions per day
- 50 containers
- 1 tenant
- 5 cases in the **New** or **Open** states

**Splunk Phantom licensed actions**

- `phantom.act()`
- `phantom.prompt()`
Using these actions via the REST API, a Playbook, or by executing an action in the Splunk Phantom graphical user interface counts as a licensed action. When used in the Visual Playbook Editor’s debugger, these actions are not counted against the number of licensed actions.

No actions called from the Visual Playbook Editor’s debugger count as a licensed action.

The action limit is specifically the number of actions run, as opposed to Playbooks run. Running one Playbook may invoke several actions. Also, an action run against multiple assets will count as only one action. Keep this in mind if you are managing the number of actions taken per day.

**Event-based license**

The Event-based license limits events.

An event is a container. A container is a top-level composite object that collects artifacts. An event-based license tracks the number of events that are created or updated in the twenty-four hour tracking period.

**Seat-based license**

Customers using a seat-based license are limited to a number of user accounts that can log in to Splunk Phantom. This number includes local accounts in Splunk Phantom and accounts authenticated or managed by external services such as SAML2, LDAP, or OpenID. User accounts for automation users do not count against a seat-based license.

Seat limits must be purchased in increments of five.

**Obtaining a license**

To obtain a license, you must submit a license request and obtain a Splunk Phantom license file.

To obtain a trial license for Splunk Phantom, contact the Splunk Phantom Sales department by email at sales@phantom.us.

To request an updated copy of a current Splunk Phantom license, open a license request case at https://support.splunk.com or call +1(855)SPLUNK-S or +1(855)775-8657.

International Splunk Support numbers are located at https://www.splunk.com/en_us/about-us/contact.html#tabs/customer-support.

The number of events permitted and expiration of the license is based on the terms listed in your company’s entitlement.

Once you have your license file:

1. From the main menu, select **Administration**.
2. Select **Company Settings > License**.
3. Click **Upload Key**.
4. Provide the location of the key file on your system.
5. Click **Accept & Install**.

The information obtained from the license file is displayed on the page.
If any of the information shown is incorrect or you experience any difficulty loading the license file, open a support case at https://support.splunk.com or call +1(855)SPLUNK-S or +1(855)775-8657.
Configure administration settings

Configure a source control repository for your Splunk Phantom playbooks

You can save your Splunk Phantom playbooks in Git repositories. By default, playbooks are managed in a Git repository called local. You can create additional Git repositories as needed. Doing so enables you to perform the following tasks:

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

In a clustered Splunk Phantom deployment, each cluster node uses the same Git repository based on the shared services server. You don’t need to configure one Git repository per cluster node.

Splunk Phantom also uses a Git repository to publish company-authored playbooks for customers to download. This repository is called the community repository and is configured on Splunk Phantom 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, Git, or SSH. SSH must be authenticated. Other protocols can be authenticated or anonymous if supported by the server.

Access the source control settings in Splunk Phantom

To access the Splunk Phantom source control settings, perform the following steps:

1. From the main menu, select Administration.
2. Select Administration Settings > Source Control.

You can also access the source control settings from any Playbooks page by clicking 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 main menu, select Administration.
2. Select Administration Settings > 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.
5. For HTTP and HTTPS, specify a username and password. Splunk Phantom attempts to connect anonymously if no username or password is provided. When crafting the URI, Splunk Phantom converts https://server... to https://username:password@server.... The Git protocol is not authenticated and does not require a username or password.
6. Click Save Changes.

A repository that is added to Splunk Phantom can't be edited. If you need to make a change, delete the repository and then add it again.
The username and password strings are separated so that Splunk Phantom can encrypt and store the password as it
does with asset passwords, and not display the password to other Splunk Phantom administrators. However, due to the
way Splunk Phantom interacts with and uses Git, it is stored as clear text in the Git configuration file for that repository.

**Set up a playbook repository using SSH**

To set up a playbook repository using SSH, perform the following steps:

1. From the main menu, select Administration.
2. Select Administration Settings > Source Control.
3. Select Configure a new repository from the Repositories drop-down list.
4. Provide a repository URL starting with `ssh://` and including the username. For example:
   
   `ssh://<username>@10.4.5.6/opt/repos`

5. Add the SSH public key from Splunk Phantom to your Git server's authorized keys file.
   1. Copy the contents in the SSH Public Key field.
   2. Log in to your Git server as a user with permissions to edit the Git server's authorized_keys file.
   3. Add the SSH public key to the authorized key file, such as `~/.ssh/authorized_keys`.
6. Provide a repository name and branch name. The repository name can be any name that describes your
   repository.

The Splunk Phantom server must use a certificate signed by one of the major certificate authorities. By default, the Git
client uses the OpenSSL certificate authority list to verify HTTPS certificates. Git is not able to connect if you are using
certificates, such as self-signed certificates, that are not validated in this manner.

**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 Phantom community. This repository
is configured by default when Splunk Phantom is installed. Follow the procedure to restore the community repository if it is
accidentally altered or deleted.

1. From the main 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, type the URL: https://github.com/phantomcyber/playbooks.git
5. In the Repo Name field, type community.
6. In the Branch Name field, enter the version of Splunk Phantom you are running, up to the second digit. For
   example, if you are running version 4.6.12345, enter 4.6 in this field.
7. Check the Read Only check box.
8. Click Save Changes.

If you have a Splunk Phantom cluster, each cluster node uses the same playbook repository based on the shared
services server. You do not need to configure the repository per cluster node.
Customize email templates in Splunk Phantom

Customize email templates in Splunk Phantom 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 main 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 Phantom for more information about containers.

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

**Configure search in Splunk Phantom**

Splunk Phantom uses an embedded, preconfigured version of Splunk Enterprise as its native search engine. Your organization might want to use a different Splunk Enterprise deployment with Splunk Phantom or use an external Elasticsearch instance.

**Configure Splunk Phantom to use an external Splunk Enterprise or Splunk Cloud instance for search**

This table summarizes the available options for configuring a Splunk Enterprise or Splunk Cloud instance for search in Splunk Phantom.

<table>
<thead>
<tr>
<th>Search Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Splunk Enterprise Instance</td>
<td>This is the default. No additional configuration is required.</td>
</tr>
<tr>
<td>External Standalone Splunk Enterprise Instance</td>
<td>Use this option to connect your Splunk Phantom instance or cluster to a single, external instance of Splunk Enterprise or Splunk Cloud. This option requires the Splunk Phantom Remote Search app. 1. See About the Splunk Phantom Remote Search app in the Splunk Phantom Remote Search manual to verify version compatibility and requirements. 2. See Connect to a standalone Splunk instance in the Splunk Phantom Remote Search manual for instructions.</td>
</tr>
<tr>
<td>External Distributed Splunk Enterprise Instance</td>
<td>Use this option to connect your Splunk Phantom instance or cluster to a Splunk Enterprise or Splunk Cloud deployment that contains one or more search heads, or one or more indexers with or without a search head cluster or indexer cluster. This option requires the Splunk Phantom Remote Search app. 1. See About the Splunk Phantom Remote Search app in the Splunk Phantom Remote Search manual to verify version compatibility and requirements. 2. See Connect to a distributed Splunk platform deployment in the Splunk Phantom Remote Search manual for instructions.</td>
</tr>
</tbody>
</table>

Clustered deployments of Splunk Phantom require an external Splunk Enterprise, as either a single instance or a distributed deployment, or a Splunk Cloud deployment.
Integrating with Splunk Cloud requires the following additional information and actions:

- You must use a public certificate from a verified or trusted certificate authority (CA).
- You must contact Splunk Customer Support for assistance with Splunk Cloud integration. You will need to provide the path to your certificate and your CA.
- You must enable certificate verification on your Splunk Phantom assets.

Splunk Phantom also provides support for an external Elasticsearch instance for single-instance deployments of Splunk Phantom. Clustered deployments of Splunk Phantom cannot use Elasticsearch as their search endpoint. See Configure Splunk Phantom to use an external Elasticsearch instance

**Configure Splunk Phantom to use an external Elasticsearch instance for search**

When you configure Splunk Phantom to use an external instance of Elasticsearch, a copy of all indexed and searchable data is sent to the Elasticsearch instance. The embedded Splunk Enterprise remains active and is used as the search provider for searches in the Splunk Phantom web interface.

Verify the following requirements before configuring the external Elasticsearch instance:

- If you are using SSL to secure your connection to the Elasticsearch instance, the SSL certificate is imported to the Splunk Phantom certificate store.
- You know the host name and port for the Elasticsearch instance.
- You know the username and password of an Elasticsearch user account, or the client certificate and client key.

Perform the following tasks to connect to an external Elasticsearch instance:

1. From the main menu in Splunk Phantom, select **Administration**.
2. Click **Administration Settings**.
3. Click **Search Settings**.
4. From **Search Endpoint**, select the radio button for **External Elasticsearch Instance**.
5. Select the **Use SSL** check box to enable SSL.
6. If your Elasticsearch instance is version 6 or newer, select the **Use one index per section** check box.
7. Type the host name in the **Host** field.
8. Type the port number in the **Port** field.
9. Choose your authentication method, either basic authentication with a username and password, or a client certificate.
10. If you are using basic authentication with a username and password:
   1. Type the username of the authorized Elasticsearch account in the **Username** field.
   2. Type the password of the authorized Elasticsearch account in the **Password** field.
11. If you are using certificate-based authentication, select the **Client Authentication** check box.
   1. Type the path to the client certificate in the **Client Certificate** field. This certificate is often a file with the .pem extension.
   2. Type the path to the client key in the **Client Key** field. This key is often a file with the .key extension.
12. Test the connection to your Elasticsearch instance by clicking **Test Connection**.
13. When you are finished, click **Save Changes**.

If you want to use a client certificate to connect to your Elasticsearch instance, provide the paths on the Splunk Phantom instance's operating system to the public and private keys. The private key, often a file with the .pem extension, is the Client Certificate. The public key, often a file with the .key extension, is the Client Key. Both files must be readable by the nginx user. You can store the files in the nginx user's home directory, /var/cache/nginx.
Reindex data to make newly added information searchable

There are some situations where data coming in to Splunk Phantom can't be indexed, and therefore can't be searched. You can reindex information sections to make this information searchable. See Reindex data to make newly added information searchable in the *Splunk Phantom Remote Search* 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 Google Maps Javascript API site for more information about obtaining a Google Maps API key.

After obtaining an API key, perform the following steps:

1. From the Main 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.

The MaxMind app is updated periodically with the Splunk Phantom product. If you want to update the MaxMind app’s database more frequently, see the instructions on the MaxMind website in the article MaxMind updates. The MaxMind database is stored in the directory `/opt/phantom/apps/maxmind_[app id]`

Manage your organization's credentials with a password vault

Use credential vaults to centrally manage and monitor credential usage in your organization. Splunk Phantom supports the following password vaults:

- Hashicorp Vault
- CyberArk Enterprise Password Vault
- Thycotic Secret Server

As an administrator, you can configure Splunk Phantom to retrieve credentials from these vaults and use them in assets or use them as a client to other identity providers such as LDAP and OpenID.

Use Hashicorp Vault with Splunk Phantom

To use Hashicorp Vault with Splunk Phantom, perform the following steps:

1. From the main menu, select **Administration**.
2. Select **Administration Settings > Password Vault**.
3. Get the URL and Token from your Hashicorp administrator.
4. Select the **Verify server certificate** checkbox to verify that the HTTPS certificate is trusted. If the certificate is not trusted by default, see Manage the Splunk Phantom certificate store for information about adding your own trusted certificate.
5. 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. You can use Hashicorp to supply credentials under OpenID and LDAP authentication configuration and with assets.

**Use Hashicorp to provide credentials during authentication configuration**

You can use Hashicorp to automatically supply credentials under OpenID and LDAP authentication configuration.

1. From the main menu, select **User Management**.
2. Select **Authentication**.
3. Select an identity provider such as LDAP.
4. Toggle the LDAP switch to enable LDAP authentication.
5. Check the **Manage password using Hashicorp Vault** check box.
6. Provide the value and key you want to retrieve from the vault.
7. (Optional) Click **Test Authentication** to verify authentication.
8. Click **Save Changes**.

**Use Hashicorp 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 CyberArk with Splunk Phantom**

Integrate Splunk Phantom with CyberArk's Vault 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 Phantom assets after a password change.

For security purposes, utilizing CyberArk can greatly simplify password management but may not significantly change the security stance of the Splunk Phantom server. Splunk Phantom would no longer be the primary store for CyberArk-managed account passwords, but still has the ability to retrieve the same passwords from CyberArk in order to authenticate itself to other resources. Therefore, someone with administrative control over the Splunk Phantom server can gain access to those passwords.

Installing CyberArk on the Splunk Phantom server must be performed by a CyberArk administrator following the CyberArk documentation. Splunk Phantom was tested with the `CARKaim-9.7.0.0.3.x86_64.rpm` CyberArk installer package.

Perform the following tasks to use CyberArk with Splunk Phantom:

1. From the main menu, select **Administration**.
2. Select **Administration Settings > Password Vault**.
3. Select Cyberark from the drop-down list in the Manager field. The CyberArk option in the drop-down list is inactive until the CyberArk components are installed. Splunk Phantom determines the presence of CyberArk in
your environment by looking for the /opt/CARKaim directory.

4. Click **Save Changes**.

After the CyberArk options become visible, check the **Enable credential management at startup** check box to have the watchdog daemon start CyberArk when Splunk Phantom is started. This is useful if you have disabled the system from starting CyberArk by removing the startup file from /etc/init.d.

To require a Splunk Phantom administrator to log in to perform an action in Splunk Phantom before CyberArk is available after a system restart, uncheck **Enable credential management at startup** and click **Save Changes**. In this situation, an administrator is someone who has the specific Administrator role. Click **Authorize** to require the logged-in administrative user to supply their own password to re-authenticate themselves, and then the credential management service will be started.

To use CyberArk to automatically supply credentials under authentication configuration, perform the following steps:

1. From the main menu, select **User Management**.
2. Select **Authentication**.
3. Select an identity provider such as **LDAP**.
4. Toggle the LDAP switch to enable LDAP authentication.
5. Check the **Manage password using CyberArk** check box.
6. Fill in the CyberArk Safe, Safe Path, and Object Name fields the same way you do for an Asset to select the CyberArk object that CyberArk is going to use to get the password field value.
7. Click **Save Changes**.

**Use Thycotic Secret Server with Splunk Phantom**

To use Thycotic Secret Server with Splunk Phantom, perform the following steps:

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. Specify the credentials for Splunk Phantom to use to access secrets.
5. Click **Save Changes**.

**Set environment variables globally for all apps**

Use the Global Environment Variables page to set environment variables that all apps and the Splunk Phantom runtime environment use globally.

1. From the Main Menu, select **Administration**.
2. Select **Administration Settings > App Environment**.
3. In the Name field, specify **HTTP_PROXY**, **HTTPS_PROXY**, or **NO_PROXY** depending on the type of proxy connection.
   - The Value field for HTTP and HTTPS proxy configurations must include the protocol, hostname or IP address, and port of the proxy server. For example: `<protocol>://<hostname/IP>:<port>
   - The Value field for **NO_PROXY** configurations must contain the IP, hostname, or domain of the asset.
   - The Secret option encrypts the Value field and prevents the field from being displayed.

When configuring the system to use an HTTP or HTTPS proxy, Splunk Phantom requires that you except calls to 127.0.0.1 from the proxy list. You must set the environment variable **NO_PROXY** to 127.0.0.1 to make localhost REST
calls without being diverted to the proxy.

You can also apply environment variables to assets individually in the Asset Settings tab for any configured asset. The asset environment variables always take priority over global environment variables.

For apps that use requests, configure both HTTPS and HTTP environment variables to direct all app traffic through the proxy server.

**Add tags to objects in Splunk Phantom**

Add tags to objects in Splunk Phantom to help you perform the following tasks:

- Search for objects in Splunk Phantom
- 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 Phantom**

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 Phantom 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 Phantom instance:

1. From the Main Menu, select Administration.
2. Select Administration Settings > Tags.

**Add a new tag to Splunk Phantom**

To add a new tag to Splunk Phantom, 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 Phantom and typing them into the Tags field. For example, to create a new tag for a container in Splunk Phantom, 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 Phantom tags**

Renaming a tag affects all objects in Splunk Phantom currently using that tag. All containers, artifacts, or assets in Splunk Phantom 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 Phantom 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 Phantom to keep your playbooks operational.
2. Modify the name of the tag as desired.
3. Click Save.

**Delete a tag in Splunk Phantom**

A tag exists in Splunk Phantom 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 Phantom currently using that tag. The deleted tag is removed from all containers, artifacts, or assets in Splunk Phantom 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 Phantom 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 Phantom**

Splunk Phantom 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, add 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 main 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 Main Menu, select **Administration**.
2. Select **Administration Settings > CEF**.
3. Click **+ 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. Leaving this blank allows users to enter a value while editing the artifact in Mission Control.

1. Click **Save**.

**Modify a custom CEF field**

Perform the following steps to modify a custom CEF field:

1. From the Main Menu, select **Administration**.
2. Select **Administration Settings > CEF**.
3. Click the edit icon to the right of the CEF name.
4. Make the desired changes.
5. Click **Save**.

**Delete a custom CEF field**

Perform the following steps to delete a custom CEF field:

1. From the Main Menu, select **Administration**.
2. Select **Administration Settings > CEF**.
3. Click 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.

**Reset the admin and root passwords in Splunk Phantom**

You can reset the passwords for the following accounts to meet your organization's hardening requirements, or if you misplace or forget them:

- The admin user for the Splunk Phantom web interface. This is a default account in Splunk Phantom that can't be deleted. It must always be available so that you can access Splunk Phantom in cases where other authentication methods such as LDAP fail. See [Reset the admin password in Splunk Phantom](#).
- The root user for the underlying CentOS Linux operating system. This account is required for maintenance tasks such as upgrades, and is also used to reset the admin password.

**Reset the admin password in Splunk Phantom**

To reset the admin user password, perform the following tasks:
1. Log in to the operating system with your normal user account.
2. Run the `sudo su` command to switch to the root user.
3. Run the following commands:
   
   ```
   export PYTHONPATH=/opt/phantom/lib/:/opt/phantom/www/
   phenv python2.7 /opt/phantom/www/manage.py changepassword admin
   ```
4. Enter a new password, then enter it again to confirm. Both passwords must match.
5. To verify, access the Splunk Phantom web interface and log in as the admin user using the new password.

If the admin account has Duo two factor authentication enabled and is no longer working properly, perform the following steps to temporarily disable the two factor authentication:

1. Run the following command as root:
   ```
   phenv python2.7 /opt/phantom/bin/set_preference.pyc --disable-admin-2fa
   ```
2. Confirm that you want to disable two factor authentication for the admin account.

**Reset the root password in Splunk Phantom**

To reset the root password in Splunk Phantom, perform the following tasks:

1. Configure the virtual machine to boot from a CD.
2. Mount the virtual machine root disk.
3. Edit the password file.
4. Mark the disk for re-labeling.
5. Set a new password.

**Configure the virtual machine to boot from a CD**

Perform the following steps to configure the virtual machine (VM) to boot from a CD.

1. Take a snapshot of the VM before performing this kind of recovery operation.
2. Obtain a Linux boot CD ISO that has the LVM tools on it. This has been successfully tested with SystemRescueCd-x86-4.7.2.
3. Configure the VM in your virtualization environment to boot from this ISO image.
4. Once configured, reset the VM so that it reboots.
5. Boot the VM from the CD image.

VMware products typically require that you press a key at the brief BIOS screen to make the VM boot from the CD rather than the virtual hard drive. This might take very careful timing. If you are unable to get it to boot from the CD image by manually pressing the button quickly enough, go to this VMware community page and search for "bios.bootDelay."

1. Follow the prompts for your boot CD until you are able to get to a shell.

**Mount the virtual machine root disk**

When you have a root shell, perform the following tasks to mount the Splunk Phantom VM drive.

1. Run the `lvscan` command to make sure you can see the LVM drives.
2. Use the following command to mount the drive:
   ```
   mount /dev/VolGroup/lv_root /mnt
   ```

If your boot CD doesn't have a `/mnt` directory for mounting, substitute an appropriate mount location.
Edit the password file

Perform the following tasks to edit the /etc/passwd file:

1. Use a text editor to open the file. For example, to use vi type the following at the command line:
   
   vi /mnt/etc/passwd

2. Find the line for the root user, which looks like the following:
   
   root:x:0:0:root:/root:/opt/phantom/bin/setup

3. Remove the "x" between the first two colons, so it looks like the following:
   
   root::0:0:root:/root:/opt/phantom/bin/setup The "x" normally tells the operating system to look in /etc/shadow for the password hash. Having it blank means root has no password at all.

Mark the disk for relabeling

Because the Splunk Phantom virtual machine uses SELinux, perform the following steps to mark the disk for relabeling:

1. Run the following command to have Linux relabel the drives when they are booted:
   
   touch /mnt/.autorelabel

2. To make sure the changes are written out, unmount the disk and reboot:
   
   umount /mnt
   reboot

Set a new root password

To set a new root password, follow these steps:

1. Login as root to the VM console. You will not be prompted for a password.
2. When you are logged in, set a new root password immediately.
3. After setting the password, log out and then log back in with the new password to verify that a password is correct.
Configure settings for your Splunk Phantom instance

Enable clickable URLs in CEF data

If a Common Event Format (CEF) has URL data, the interface can show a clickable link for it. Use this setting to toggle whether clickable links are shown. Since many URLs in CEF values are likely to be malicious, the default is Off.

View cluster status and enable or disable a cluster

View the Clustering page to see the status of your Splunk Phantom clusters, enable or disable a cluster, or add additional nodes. See Install and Upgrade Splunk Phantom for information about setting up a cluster.

Perform the following steps to access the Clustering page:

1. From the main menu, select Administration.
2. Select Product Settings > Clustering.

The status of online means that the cluster node is up and running.

Disable a node by toggling the switch next to Enabled so that it is in the off position.

Click View to view the system health for that specific node. See View the health of your Splunk Phantom system to read more about the system health view for cluster nodes.

Configure multiple tenants on your Splunk Phantom instance

Enable multi-tenancy to allow one security team to manage multiple independent customers while segregating their customers' assets and data. For example, a Managed Security Service Provider (MSSP) business can use multi-tenancy to perform incident response for multiple clients with one analyst team on a single Splunk Phantom instance and maintain customer separation. The MSSP SOC can administer each customer's data set without needing a separate login and permissions configuration.

How many tenants can be configured?

The Splunk Phantom Community License only allows for one tenant if the multi-tenancy feature is enabled. You can view the number of allowed tenants in your Splunk Phantom instance by performing the following steps:

1. From the main menu, select Administration.
2. Select Company Settings > License.
3. View the information in the Tenant Count field.

The system default tenant doesn't count towards the total count.
Enable multi-tenancy

Splunk Phantom multi-tenancy isn't enabled by default. Perform the following steps to enable multi-tenancy:

1. From the main menu, click Administration.
2. Select Product Settings > Multi-tenancy.
3. Toggle Enable Multi-tenancy to On.
4. Click Confirm to confirm that you want to enable multi-tenancy.
5. Provide the information for the default system tenant.
6. Click Save.

View the tenants configured on your Splunk Phantom instance

To view the configured tenants in Splunk Phantom, perform the following steps:

1. From the main menu, click Administration.
2. Select Product Settings > Multi-tenancy.

The default system tenant has an ID of 0. Each container in Splunk Phantom must have one tenant assigned. Before creating any additional tenants, all containers are assigned this default system tenant. Any containers that don't have an explicitly specified tenant and are created through an automated process are assigned to the default system tenant. If a container is created manually through the Splunk Phantom web interface you must select a tenant once you enable multi-tenancy.

Add a tenant to Splunk Phantom

To add a new tenant to Splunk Phantom, perform the following steps:

1. From the main menu, click Administration.
2. Select Product Settings > Multi-tenancy.
3. Click + Tenant.
4. Complete the information in the Add Tenant dialog box.
5. Click Save.

You can configure only as many tenants as your license allows, not including the default system tenant. If you already reached your limit, you must disable an existing tenant before you can add a new one.

Edit an existing tenant in Splunk Phantom

To edit the information for an existing tenant, hover and click the tenant you want to edit. Once a tenant is defined, you can't delete it. You must disable it instead. All tenant names must be unique.

Configure permissions for tenants and assets in Splunk Phantom

Each asset in Splunk Phantom must belong to one or more tenants. An asset can only be used by containers that share the same tenant as the asset. See Add and configure apps and assets to provide actions in Splunk Phantom for more information about configuring assets for tenants.

You can restrict access to tenant information based on role configuration in Splunk Phantom. A role with no tenants specified means all users with the role have access to all tenants. To limit access to specific tenants, specify the tenants as part of the role configuration. See Manage roles and permissions in Splunk Phantom for information about configuring
tenant user permissions.

Each container must have exactly one tenant. If no tenant is assigned to a container, then the container belongs to the default system tenant. An asset can have no tenants, which means it can be used with any tenant. See the following examples of assets and tenant usage:

- You can make assets based on public services, such as the whois databases, usable by all tenants.
- You can subscribe to a commercial service and make this service available for all tenants regardless of service level.
- Some assets such as a customer's firewall belong only to a specific tenant. Configure only one tenant for this type of asset.
- A premium commercial offering such as a commercial sandbox might be made available to a specific group of tenants. In order to ensure that only customers paying for that offering can use it, configure the asset so that it has only the paying customers.

Ingestion assets must have only one tenant, and this tenant is also assigned to any containers created by the ingestion asset. You can use separate assets for an app to separate data for different tenants. For example, consider if a Splunk Enterprise app is ingesting multiple customer logs tagged per customer. You can have a Splunk Phantom app that performs periodic polling of the Splunk Enterprise app based on a query containing the customer tag. One customer is called Initech, and a second customer is called Initrode. Create one asset for each company based on the Splunk Enterprise app:

- One query can contain customer=initech. Containers created by this asset belong to the Initech tenant.
- The second query can contain customer=initrode. Containers created by this asset belong to the Initrode tenant.

Containers can also be pushed to Splunk Phantom using the REST API. The REST API is accessed by automation users in Splunk Phantom, each of whom is assigned a default tenant. The API caller can override this tenant, or use the default tenant if one is not specified. See REST Containers in the Splunk Phantom REST API Reference.

In situations where you are not able to assign the correct tenant to a container, such as if you are unable to properly separate the data for different tenants, or do not have proper access to call the REST API to create containers, you can ingest the data using any default tenant, then use a playbook to assign the container to the desired tenant. For example, a container might have a field or artifact that maps directly to a customer name, or you might even need to look up custom IP address ranges to determine the customer before assigning the proper tenant.

**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 main 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 with an ingestion asset or by manually adding them on the Event Settings subtab. For example, in a production environment, you might pick a source label from an ingestion asset such as "Events" or "Email" and create a destination label such as "Aggregated Events" that makes it clear that containers with that label are aggregated.
Add a new aggregation rule

In this scenario, we want to aggregate artifacts with matching `sourceAddress` CEF fields. For events from numerous products, these fields are often the sender's IP address on a packet or connection that triggered an alert and represent an attacker's IP address. The name `sourceAddress` is not related to the source or destination label concept. It's a different kind of source. We want to give the rule a meaningful name using the "Source" and "Destination" labels in our example.

Follow this procedure to create an example aggregation rule:

1. From the Aggregation page, click + Aggregation Rule.
2. Specify `sourceAddress - Source to Destination` as the name of the rule.
3. Select Source from the drop-down list in the Source Label field.
4. Select Destination from the drop-down list in the Destination Label field.
5. Select Exact to aggregate on the exact contents of the CEF field. You can click on the plus (+) icon to add additional match rules.
6. Select `sourceaddress` in the CEF field. You can start typing the field name to search through the list of available field names.
7. Click Save.

On the Aggregation page, the 1 in parentheses next to Source means there is one rule under the label Source.

Edit an existing aggregation rule

After completing the previous example, perform the following steps to edit an existing aggregation rule in Splunk Phantom.

1. Click on any existing rule. In this example, click Source 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 Source label rule page, the new rule will automatically populate the Source Label field with Source.

By default, rules apply to all tenants. Only one rule per source label and tenant combination is allowed. "All Tenants" counts as a named tenant for this purpose. If you need to have another rule for the label "Source", pick a specific tenant from the drop-down list, then create a second rule with source label "Source".

Using multiple matches in an aggregation rule

An aggregation rule can have multiple match lines. The following image shows an aggregation rule with an exact match on both `sourceaddress` and `destinationaddress`. 
In 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 victim'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 victim IP address of 1.1.1.1, there is one destination container for attacker IP address 2.2.2.2 and victim IP address 1.1.1.1, and a different container for attacker IP address 3.3.3.3 and victim 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.

**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 Phantom for information about how to use workbooks in a Splunk Phantom workflow.

**Create a Splunk Phantom workbook**

Perform the following tasks to create a new workbook in Splunk Phantom:

1. From the main 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 Phantom 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 Phantom asset currently using the workbook.

To edit an existing workbook, do the following:

1. From the main 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 main 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 main 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.

<table>
<thead>
<tr>
<th>Method of notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>When you assign a task to a role, Splunk Phantom 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.</td>
</tr>
<tr>
<td>In-product</td>
<td>When you assign a task to a role, every member of the role sees a bell notification in the Splunk Phantom menu bar. When a specific user assigns that task to themselves, the bell notification disappears for all other members of the role.</td>
</tr>
</tbody>
</table>
| Mobile                 | You can view Splunk Phantom notifications on your mobile device using the Splunk Mobile app. You must complete the following steps before you can view mobile Splunk Phantom notifications:  
  - Download Splunk Mobile. See Download Splunk Mobile for iOS or Download Splunk Mobile for Android to download the Splunk Mobile app.  
  - Register your device. See Mobile Device Registration.  
  View a notification by opening a push notification. Or, you can open a notification in the Splunk Mobile UI.  
    1. In your Phantom instance in the Splunk Mobile app, navigate to the **Notifications** tab. You can filter notifications by type by tapping **All Types** at the top of the list.  
    2. Tap a notification to view its details. |

### Tune performance by managing Splunk Phantom features

An administrator can tune performance of their Splunk Phantom deployment by toggling the **Indicators** feature or removing audit logs from the deployment after they have been downloaded.

#### Enable or disable the indicators feature

Prior to 4.8, retrieval of indicator records did not scale in some large deployments with hundreds of thousands of indicator records. Improvements have been made to enhance performance, but some administrators may wish to disable the feature entirely.
An administrator can toggle the **Indicators** feature of Splunk Phantom by running a script from the *nix shell command line.

Disabling the **Indicators** feature removes it from the **Main Menu**, from the **events** page, and from context menus in the investigations page.

When indicators are disabled, the indicator REST APIs return response 400, with the message body:

```json
{
  "failed": true,
  "message": "The indicators feature is not enabled."
}
```

**Affected APIs**

- /rest/indicator
- /rest/indicator_by_value
- /rest/indicator_artifact
- /rest/indicator_artifact_timeline
- /rest/indicator_stats_indicator_count
- /rest/indicator_stats_top_labels
- /rest/indicator_stats_top_types
- /rest/indicator_stats_top_values
- /rest/ioc
- /rest/indicator_common_container

See REST Indicators.

**Toggle the Indicators feature**

To disable Indicators:

1. SSH to your Splunk Phantom instance.
   `SSH <username>@<phantom_hostname>
2. Run the `phenv admin set_preference` script, located in `/<PHANTOM_HOME>/phantom/bin`.
   `sudo phenv python /<PHANTOM_HOME>/phantom/bin/set_preference.pyc --indicators no`

To enable Indicators:

1. SSH to your Splunk Phantom instance.
   `SSH <username>@<phantom_hostname>
2. Run the `set_preferences.pyc` script, located in `/<PHANTOM_HOME>/phantom/bin`.
   `sudo phenv python /<PHANTOM_HOME>/phantom/bin/set_preferences.pyc --indicators yes`

It can take as much as five minutes for the indicators feature to be hidden or to show from the Splunk Phantom UI after the `set_preferences.pyc` script has been run.

**Delete audit logs**

Downloading Audit logs could take a long time because all the records were loaded into memory before being written to a file. In version 4.8, audit logs have been changed to stream records to a file.
An administrator can remove audit logs after they have been manually downloaded and archived by using the `delete_audit_logs.pyc` script found in `/<PHANTOM_HOME>/phantom/bin`.

This script will permanently delete audit records from Splunk Phantom. The records cannot be recovered without restoring Splunk Phantom from a backup. Exercise caution when using this script.

**delete_audit_logs.pyc arguments**

```bash
# phenv python delete_audit_logs.pyc -h
usage: delete_audit_logs.py [-h] [--before BEFORE_TIMESTAMP]
   [--after AFTER_TIMESTAMP]
   [--categories [CATEGORIES [CATEGORIES ...]]]
   [--dry-run] [--non-interactive]
   [--log-level {NOTSET,DEBUG,INFO,WARNING,ERROR,CRITICAL}]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Show this help message and exit.</td>
</tr>
<tr>
<td>--before &lt;BEFORE_TIMESTAMP&gt;</td>
<td>Records created before this timestamp will be deleted.</td>
</tr>
<tr>
<td></td>
<td>Records created after this timestamp will not be deleted. The timestamp</td>
</tr>
<tr>
<td></td>
<td>value must be in yyyy-mm-dd [hh:mm:ss] format.</td>
</tr>
<tr>
<td>--after &lt;AFTER_TIMESTAMP&gt;</td>
<td>Records created after this timestamp will be deleted.</td>
</tr>
<tr>
<td></td>
<td>Records created before this timestamp will not be deleted. The timestamp</td>
</tr>
<tr>
<td></td>
<td>value must be in yyyy-mm-dd [hh:mm:ss] format.</td>
</tr>
<tr>
<td>--categories [CATEGORIES ...]</td>
<td>Only delete records with the given categories.</td>
</tr>
<tr>
<td></td>
<td>Examples of categories: user, container, playbook, administration, artifact.</td>
</tr>
<tr>
<td>--dry-run</td>
<td>Do not run the DELETE queries. Use this argument to test your parameters</td>
</tr>
<tr>
<td></td>
<td>before running the script for real.</td>
</tr>
<tr>
<td>--non-interactive</td>
<td>Do not block on user input. This flag is suitable for running as part of</td>
</tr>
<tr>
<td></td>
<td>an unsupervised script.</td>
</tr>
<tr>
<td>--log-level (NOTSET, DEBUG, INFO, WARNING, ERROR, CRITICAL)</td>
<td>Set the log level. Default level is WARNING.</td>
</tr>
</tbody>
</table>

**Examples**

Test script parameters by using the `--dry-run` option first.

**Delete all audit logs from before July 2019:**

```bash
sudo phenv python delete_audit_logs.pyc --before 2019-07-01
```

**Delete audit logs between July 1 and December 1 2019:**

```bash
sudo phenv python delete_audit_logs.pyc --after 2019-07-01 --before 2019-12-01
```
Configure settings for your system's events

Create custom status labels in Splunk Phantom

You can create additional status labels for the events and cases in Splunk Phantom as needed for your business processes.

Statuses are grouped into three categories: New, Open, and Resolved. You can create up to 10 total status labels in Splunk Phantom.

**Status label rules**

Status labels must adhere to the following rules:

- At least one status label must exist for each of the status categories.
- 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 Phantom

To create a status label, follow these steps:

1. From the main 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 following conditions:
   - Only ASCII characters A-Z, a-z, 0-9, dash ( - ), or underscores ( _ ) are allowed.
   - The name cannot exceed 20 characters in length.
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

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 Phantom ships with three predefined severity names: High, Medium, and Low. Your organization might need additional levels of severity to match your business processes. Additional severity names can be defined by a Splunk Phantom administrator.
You can create up to 10 severities in Splunk Phantom.

**Create a severity in Splunk Phantom**

To create a severity, follow these steps:

1. From the Main Menu, select **Administration**.
2. Select **Event Settings > 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, 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 Phantom**

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 Phantom 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 Phantom'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.

**Create custom fields to filter Splunk Phantom events**

Create custom fields that can be added to containers in Splunk Phantom. You can use custom fields to match your business processes, or to help filter containers, events, or cases for extra attention.

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

**Create a custom field**

To create a custom field, follow these steps:

1. From the main menu select, **Administration**.
2. Select **Event Settings > Custom Fields**.
3. Click **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) Click Add Field to add additional fields.
8. Click Save Changes.

Edit custom fields

To edit a custom field, follow these steps:

1. From the main menu, select Administration.
2. Select Event Settings > 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 click the X icon to remove existing values.
4. Check or uncheck Require on Resolve as needed.
5. Click Save Changes.

Delete a custom field

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

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

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 Phantom assets.

Create a HUD Card

Perform the following tasks to create a HUD card:

1. From the main menu, select Administration.
2. Select Event Settings > HUD.
3. Click + 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 Phantom events. The fields defined there are available in the drop-down list. Choose a background color for the HUD card.
5. Click Done.
**Manage HUD Cards**

HUD cards display in Investigation in the same order they appear in the list of HUD cards in the 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 clicking the circled x ( ? ) icon to the right of the HUD card definition.

See Get a heads up with HUD cards for more information on using HUD Cards in *Start with Investigation in Splunk Phantom*.

**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 Phantom:

- 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 Phantom in *Use Splunk Phantom*.

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 Phantom:

<table>
<thead>
<tr>
<th>Severity name</th>
<th>SLA in minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>60</td>
</tr>
<tr>
<td>Medium</td>
<td>720</td>
</tr>
<tr>
<td>Low</td>
<td>1440</td>
</tr>
</tbody>
</table>

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 Phantom. 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 Main 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 Main 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 Phantom 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 Phantom to run playbooks and other automation against containers.

Splunk Phantom 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 main 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 main 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.
Use whitelist to grant authorized access

The whitelist is 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 whitelist appears in the Investigation screen if the whitelist is 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 Phantom for more information about roles and permissions.

Disable the whitelist by doing the following:

1. From the main menu, select Administration.
2. Select Event Settings > Whitelist.
3. Click the Enable Whitelist toggle to the Off position.

Once disabled, the Authorized section is no longer visible in Investigation. Reenabling the whitelist 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 Phantom users and accounts

Manage Splunk Phantom users

View the Users page to see the users configured on your Splunk Phantom instance, add new users, or edit existing users.

Perform the following steps to access the Users page:

1. From the main menu, select Administration.
2. Select User Management > Users.

Default users and types of users

On a new Splunk Phantom instance, the following default users are available:

- Admin. This is the default admin account and cannot be deleted.
- Automation.

An information card is shown for each user and contains information such as the user's full name, username last access data, and roles. The card for local interactive users contains an icon showing the user's initials or custom icon. The card for all other types of users contains a colored ribbon indicating the user type.

The example below shows one of each type of user that can be configured in Splunk Phantom:

![User cards example](image-url)

In this example, we can see the following information:

- The admin user is a local interactive user, and this user's card contains an icon with the letter "A". The other user cards show a vertical ribbon indicating the user type.
- Users like Alice Smith and Susan Edwards have provided first and last names which are displayed next to their usernames. Alice logs in with the short username, alice, while Susan logs in with the email-style username, susan@phantom.us. The format of the username used depends on the identity provider being used.

The automation user is a default internal service account used by Splunk Phantom for running automated playbooks and asset actions, such as data ingestion. The automation user and any other automation type users do not have passwords and can't log into the Splunk Phantom web interface. However, they do provide REST authentication tokens that can be used to read and write data to the REST backend and perform useful activities. For information on how to use the REST API and authentication tokens, see Using the Splunk Phantom REST API reference in the Splunk Phantom REST API.
Customize what you see on the Users page

Customize the information you see on the Users page:

- Click 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.
- Click on the ellipsis (...) icon in the upper-right 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 Phantom 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 main menu, select Administration.
2. Select User Management > Users.
3. Click on a user card and review the roles assigned to this user in the Roles field.

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

See Manage roles and permissions in Splunk Phantom for more information about Splunk Phantom roles and the permissions provided by each role.

Add users to Splunk Phantom

You can add users to Splunk Phantom from the Splunk Phantom web interface. These user accounts can access Splunk Phantom but not the operating system of the virtual appliance. The user can be authenticated locally by Splunk Phantom, or by using LDAP, OpenID, or SAML2. In the case of LDAP, OpenID, and SAML2, the user account can be created in Splunk Phantom or created automatically during the user's initial login. In order for accounts to be automatically created, a group mapping to a Splunk Phantom role must be configured. See Configuring single sign-on authentication for Splunk Phantom.

Create a local Splunk Phantom user

Perform the following tasks to add a local Splunk Phantom user. The user is authenticated by the Splunk Phantom instance.

1. From the main menu, select Administration.
2. Select User Management > Users.
3. Click + 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. If two factor authentication is enabled, also provide the Duo username. See Secure Splunk Phantom
using two factor authentication.
8. Click Create.

Create an LDAP, OpenID, or SAML2 Splunk Phantom 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 Phantom.

1. From the main menu, select Administration.
2. Select User Management > Users.
3. Click + 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. If two factor authentication is enabled, also provide the Duo username. See Secure Splunk Phantom using two factor authentication.
7. Click Create.

Create an automation user in Splunk Phantom

Perform the following steps to add an automation user in Splunk Phantom:

1. From the main menu, select Administration.
2. Select User Management > Users.
3. Click + 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) If multi-tenancy is enabled, select the default tenant in the Default Tenant field.
9. (Optional) The Automation role is provided to automation users by default. See Manage roles and permissions in Splunk Phantom for more information about the permissions granted by each role.
10. Click Create.

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

Click 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 Phantom REST API reference in the Splunk Phantom 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 Phantom asset.
Disable an existing Splunk Phantom user

Disable a user in Splunk Phantom 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 Phantom user, perform the following steps:

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

Manage roles and permissions in Splunk Phantom

Roles in Splunk Phantom 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 Phantom in the Use Splunk Phantom manual.

View your Splunk Phantom roles

To view the roles configured in your Splunk Phantom instance, perform the following steps to access the Roles page:

1. From the main menu, select Administration.
2. Select User Management > Roles & Permissions.

Splunk Phantom includes the following default roles that can't be edited or deleted:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Users with this role have full privileges and can access all Phantom functions.</td>
</tr>
<tr>
<td>Asset Owner</td>
<td>Users with this role can create and edit assets, and view all other parts of the system.</td>
</tr>
<tr>
<td>Automation</td>
<td>This is a service account role used for automated tasks including REST API operations, playbook execution, and ingestion.</td>
</tr>
<tr>
<td>Automation Engineer</td>
<td>Users with this role can view and execute playbooks (but not edit or create them), and view everything else.</td>
</tr>
<tr>
<td>Incident Commander</td>
<td>Users with this role can edit containers and system settings, edit and execute playbooks, and view everything.</td>
</tr>
<tr>
<td>Observer</td>
<td>Users with this role can view everything, but cannot edit nor execute anything.</td>
</tr>
</tbody>
</table>

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 Phantom

Perform the following steps to add a new role in Splunk Phantom:

1. From the Main Menu, select Administration.
2. Select User Management > Roles & Permissions.
3. Click + 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Permission and Description</th>
</tr>
</thead>
</table>
| 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.                                                                                   |
| 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. Security note: playbooks run unrestricted python code on the Splunk Phantom server. Users with Edit permissions can write code that can take control of the server.  
• Select View to allow the user to view playbooks.  
• Select Execute to allow the user to execute playbooks on events.  
• Select Edit Code to allow playbook authors to manually edit Python code and customize code blocks. Authors without this permissions can only use the visual block editor. |
| System Settings | • Select Edit to allow the user to change System Settings.  
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. Click 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 Phantom instance. See Create additional custom status labels in Splunk Phantom. The following permissions can be configured:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>The user can delete any object in Splunk Phantom that has this label. Clicking this automatically grants the Edit and View permissions.</td>
</tr>
<tr>
<td>Edit</td>
<td>The user can edit any object in Splunk Phantom that has this label. Clicking this automatically grants the View permission.</td>
</tr>
<tr>
<td>View</td>
<td>The user can view any object in Splunk Phantom with this label, but cannot modify or delete any such objects.</td>
</tr>
</tbody>
</table>
8. Click **Repository Permissions** to configure repository permissions for this role. The repositories you see in the table depend on the repositories configured on your Splunk Phantom instance. See Configure a source control repository for your Splunk Phantom playbooks. The following permissions can be configured:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>The user can delete any playbook in this repository. Clicking this automatically grants the Edit and View permissions.</td>
</tr>
<tr>
<td>Edit</td>
<td>The user can edit any playbook in this repository. Clicking this automatically grants the View permission.</td>
</tr>
<tr>
<td>View</td>
<td>The user can view any playbook in this repository, but cannot modify or delete any playbooks.</td>
</tr>
<tr>
<td>Execute</td>
<td>The user can run any playbook in this repository.</td>
</tr>
</tbody>
</table>

9. If multi-tenancy is configured and enabled on your system, click **Tenant Permissions** to configure tenant permissions for this role. See Configure multiple tenants on your Splunk Phantom instance. The following permissions can be configured:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>The user can delete any container assigned to this tenant. Clicking this automatically grants the Edit and View permissions.</td>
</tr>
<tr>
<td>Edit</td>
<td>The user can edit any container assigned to this tenant. Clicking this automatically grants the View permission.</td>
</tr>
<tr>
<td>View</td>
<td>The user can view any container assigned to this tenant, but cannot modify or delete any containers.</td>
</tr>
</tbody>
</table>

10. Click **Create Role**.

## Add users to a role in Splunk Phantom

Perform the following steps to add users to a role in Splunk Phantom:

1. From the Main Menu, select **Administration**.
2. Select **User Management > Roles & Permissions**.
3. Click the role you want to edit and add users to.
4. Click **Add Users**.
5. Select a user from the drop-down list, or start typing a username to filter the users that are displayed.
6. Click **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.

## Edit a role in Splunk Phantom

Perform the following steps to edit a Splunk Phantom role:

1. From the Main Menu, select **Administration**.
2. Select **User Management > 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 click **Save Changes**.
   - Permission changes to roles are applied in real time to the users who are granted the updated permissions, before you click **Save Changes**.
   - Users inheriting roles from an SSO provider must log out and log back in to Splunk Phantom to see their updated permissions.
4. Click **Save Changes**.
Delete a role in Splunk Phantom

Perform the following tasks to delete a role in Splunk Phantom:

1. From the Main Menu, select Administration.
2. Select User Management > Roles & Permissions.
3. Click the role you want to delete.
4. Click Delete Role.
5. Click Delete to confirm that you want to delete the role.

Configure password requirements and timeout intervals to secure your Splunk Phantom accounts

You can configure password requirements and set timeout intervals for inactivity to secure your local Splunk Phantom 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 main menu, select Administration.
3. Configure the desired timeout settings for all local Splunk Phantom accounts.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity</td>
<td>The number of minutes with no activity between the user's browser and the web server before the user is logged out.</td>
</tr>
<tr>
<td>Absolute</td>
<td>The number of minutes after which a local user is logged out, regardless of activity. Some pages, such as the homepage 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 Phantom system.</td>
</tr>
</tbody>
</table>

4. Configure the password requirements for your local Splunk Phantom accounts.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>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.</td>
</tr>
<tr>
<td>Digits</td>
<td>The number of unique digits 0-9 required in the password.</td>
</tr>
<tr>
<td>Special</td>
<td>The number of unique special characters required in the password.</td>
</tr>
<tr>
<td>Capital Letters</td>
<td>The number of unique capital letters required in the password.</td>
</tr>
</tbody>
</table>

Configure single sign-on authentication for Splunk Phantom

Integrate Splunk Phantom with your existing authentication system using single sign-on (SSO).

You can configure SSO in Splunk Phantom with the following identity providers:
Configure SSO authentication using LDAP

To configure SSO authentication using LDAP as the identity provider, perform the following steps:

1. From the Main Menu, select Administration.
2. Select Users > Authentication.
3. LDAP is selected by default. Toggle the switch in the LDAP field to enable LDAP configuration.
4. Complete the fields to configure SSO authentication using LDAP:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Use this checkbox in conjunction with Add Another at the bottom of the page. You can have multiple LDAP servers and the Active checkbox determines which ones are used by Splunk Phantom for authentication. The toggle button in the LDAP field enables LDAP authentication for all servers which are marked Active. If there are multiple LDAP servers, Splunk Phantom 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.</td>
</tr>
<tr>
<td>Require TLS/SSL encryption</td>
<td>Determines whether secure LDAP connections are required. Enable TLS/SSL encryption to check the server certificate against the Splunk Phantom certificate store. See Manage the Splunk Phantom certificate store.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>The name of the SSO provider. Specify a unique name to easily identify this provider.</td>
</tr>
<tr>
<td>Server</td>
<td>The DNS name or IP address for your AD/LDAP Server, without http:// or https://. If you plan to use SSL, you must supply a DNS name that matches the certificate.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain name of your organization such as corp.yourorganization.com, used to generate DNS. This field is used as part of the LDAP query.</td>
</tr>
<tr>
<td>Bind Username</td>
<td>The username for authenticating to the LDAP server. It will ideally be a service account specifically set up for this purpose, not one belonging to a human user. This will allow you to grant the account the minimal permissions necessary, set account expiration off, and other protective measures to track how the account is used. If the account is set to expire or requires a password change, do these tasks manually and also update the Splunk Phantom system settings to reflect the same. The account will need to be able to query LDAP users and their properties.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the username to authenticate to the LDAP server.</td>
</tr>
<tr>
<td>Test User</td>
<td>The username of an active user who would typically log in to Splunk Phantom. Use this to verify that user search is working correctly.</td>
</tr>
<tr>
<td>Test Group</td>
<td>The name of a group of which the Test User is a member. Use this to confirm that the group mapping will work. Leave this field blank if you are not using group mapping.</td>
</tr>
<tr>
<td>Manage password using Hashicorp Vault</td>
<td>Use a password vault to manage user credentials. See Manage your organization's credentials with a password vault.</td>
</tr>
</tbody>
</table>

5. Click Test Authentication to test that Splunk Phantom can communicate with and query the LDAP server. Your LDAP settings will automatically be saved if the result is success. Or you can click Save Changes to save the
settings without testing them.

On Microsoft Active Directory LDAP servers, the user authentication uses the email-like form of the username, such as ldap-client@splunk.com. The specified username is appended with the domain name. Advanced settings may be required for non-Microsoft LDAP servers. Contact Phantom Support for assistance. See Where to get help.

**Configure group mappings for LDAP SSO authentication**

Configure a group mapping to map an LDAP group such as Incident Response to a Splunk Phantom role such as Automation Engineer. Doing so enables you to automatically use your LDAP groups to determine who can log into Splunk Phantom 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 LDAP user must be mapped to at least one group to enable that user to login to Splunk Phantom without manually creating the user account in Splunk Phantom.

Role mapping is done at login time, meaning that if the Splunk Phantom 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 LDAP SSO authentication**

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

**Configure SSO authentication using SAML2**

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

1. From the Main 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Use this checkbox in conjunction with <strong>Add Another</strong> at the bottom of the page. You can have multiple SAML2 servers and the <strong>Active</strong> checkbox determines which ones are used by Splunk Phantom 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 Phantom 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.</td>
</tr>
<tr>
<td>Require TLS/SSL encryption</td>
<td>Determines whether encrypted connections are required. Enable TLS/SSL encryption to check the server certificate against the Splunk Phantom certificate store. See Manage the Splunk Phantom certificate store.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>The name of the SSO provider. Specify a unique name to easily identify this provider.</td>
</tr>
<tr>
<td>Single sign-on URL</td>
<td>The URL that users are directed to for logging in.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Issuer ID</td>
<td>The unique identifier provided by the identity provider.</td>
</tr>
<tr>
<td>Metadata URL</td>
<td>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.</td>
</tr>
<tr>
<td>Metadata XML</td>
<td>XML code containing information about the provider configuration. If you specify valid XML in this field, you can leave the Metadata URL field blank.</td>
</tr>
<tr>
<td>Phantom Base URL</td>
<td>The URL used to redirect users back to Splunk Phantom. This URL must be reachable by users trying to log in.</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>Click <strong>Advanced</strong> to configure the following advanced settings:</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Response Signed</strong> to require a signed response from the identity provider.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Request Signed</strong> to require a signed request from the identity provider.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Assertion Signed</strong> to require a signed assertion containing the user attributes from the identity provider.</td>
</tr>
<tr>
<td></td>
<td>- Enter an <strong>EntityID/Audience</strong> to configure an entity ID for the service provider. This is used when defining the audience restriction on the identity provider.</td>
</tr>
<tr>
<td></td>
<td>- Enter a <strong>Group Key</strong> to identify the group membership data within the attributes passed back from the identity provider. Also specify a <strong>Group Delimiter</strong> if groups are passed back as a single element with a delimiter, instead of separate attribute values.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Configure Groups.</strong> See <a href="#">Configure group mappings for LDAP SSO authentication</a> for more information about group mapping.</td>
</tr>
<tr>
<td></td>
<td>- Configure <strong>External Attributes.</strong> See <a href="#">Configure external attribute mappings for LDAP SSO authentication</a> for more information about external attributes mapping.</td>
</tr>
</tbody>
</table>

6. Click **Save Changes**.

### Configure SSO authentication using OpenID

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Use this checkbox in conjunction with <strong>Add Another</strong> at the bottom of the page. You can have multiple OpenID servers and the <strong>Active</strong> checkbox determines which ones are used by Splunk Phantom for authentication. The toggle button in the OpenID field enables OpenID authentication for all servers which are marked Active.</td>
</tr>
<tr>
<td></td>
<td>If there are multiple OpenID servers, Splunk Phantom 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.</td>
</tr>
<tr>
<td>Require TLS/SSL encryption</td>
<td>Determines whether encrypted connections are required. Enable TLS/SSL encryption to check the server certificate against the Splunk Phantom certificate store. See <a href="#">Manage the Splunk Phantom certificate store</a>.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>The name of the SSO provider. Specify a unique name to easily identify this provider.</td>
</tr>
<tr>
<td>Issuer</td>
<td></td>
</tr>
</tbody>
</table>
The base endpoint provided by OpenID. Configuration is based on the discovery document located at
<endpoint>/.well-known/openid-configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Provided by OpenID.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Provided by OpenID.</td>
</tr>
<tr>
<td>Phantom Base URL</td>
<td>The URL used to redirect users back to Splunk Phantom. This URL must be reachable by users trying to login.</td>
</tr>
</tbody>
</table>

**Advanced Settings**

Click Advanced to configure the following advanced settings:

- **Enter Scopes** to include custom scopes or to limit the scopes requested by Splunk Phantom. The openid scope is required.
- Set the **Token Auth Method** to client_secret_post or private_key_jwt, depending on the configuration of your identity provider.
- Specify a **Resource Identifier** if a specific resource other than the default userinfo endpoint is required to obtain user data.
- Enter a **Group Key** to identify 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 LDAP SSO authentication for more information about group mapping.
- **Configure External Attributes.** See Configure external attribute mappings for LDAP SSO authentication for more information about external attributes mapping.

6. Click **Save Changes**.

### Manage the Splunk Phantom certificate store

Splunk Phantom has a certificate store used to validate certificates when forming connections to other servers. The certificates in the store are trusted certificate authority (CA) certificates from mkcert.org and are updated periodically. In almost all cases, Splunk Phantom can use its certificate store to validate any certificate issued by a commercial certificate authority (CA).

The default certificate store cannot be used to validate self-signed certificates, or certificates issued by an internal CA. You must add these custom certificates to the Splunk Phantom certificate store. To do this, use the following commands:

```
phenv python2.7 /opt/phantom/bin/import_cert.py -i /tmp/ca.crt
service uwsgi restart
```

In this example, the import_cert.py script is copying the certificate file `ca.crt` to the `/opt/phantom/etc/certs/` directory, then consolidating all the files in that directory to the `/opt/phantom/etc/cacerts.pem` file. The cacerts.pem file is used by Splunk Phantom to verify all server certificates.

The `service uwsgi restart` restarts the web server so the updated cacerts.pem file is reloaded.

If you need to remove a certificate that you have previously installed, perform the following tasks:

1. Delete the file for that certificate from `/opt/phantom/etc/certs/`.
2. Run the `import_cert.py` script with no parameters.
3. Restart the web server.

Even after importing the correct certificate, you might notice that the server still reports connectivity issues, which could be related to the certificate. In addition to the certificate being available for validation, it is important to remember some key points about certificate validation:
• The OpenSSL library used must validate a full certificate chain. This means that you cannot just install the end certificate, such as the one on the web server. If it was signed by a parent certificate, then the parent certificate is the one that must be installed. Though, if it’s a true self-signed certificate, where it is signed by itself, and has no other parent, then install that certificate.

• Any required intermediate certificates must be present. Many CAs have a root certificate, and then one or more levels of intermediate, issuer, certificates, and then the actual server certificate. It’s customary that the server be configured to serve both its own certificate as well as the intermediates, and that the client has the root to complete the chain. However, if the server is not configured to serve the intermediates, then the intermediates must also be installed in the certificate store.

• Certificates must be within their date range. That is, it must be after the valid from date and before the expiration date in the certificate.

• Certificates must use a valid Common Name (CN) or Subject Alternate Name (SAN) field and Phantom must be configured to use the resource by that name. Wildcard certificates will also work as expected. For example, you might have a server known as server.example.com at IP address 10.1.1.1. In order for the SSL/TLS connection to it to succeed, Splunk Phantom must be configured to use the full name, server.example.com. Using a short name of “server” or using the IP address 10.1.1.1 does not work.

Secure Splunk Phantom using two factor authentication

Duo is integrated with Splunk Phantom to enable two factor authentication. When enabled, two factor authentication applies to all local Splunk Phantom users. Splunk Phantom sets each user’s email address as the Duo username. If an email address is not available, then the username is used.

Perform the following steps to enable two factor authentication in Splunk Phantom:

1. Create a web SDK application in the Duo administrative interface. Refer to your Duo documentation for more information.
2. When the web SDK application integration is ready, record the following information to provide to Splunk Phantom:
   ♦ Integration key
   ♦ Secret key
   ♦ API hostname
3. In Splunk Phantom, from the main menu, select Administration.
4. Select User Management > Two Factor.
5. Check the Enable Duo Two Factor Authentication checkbox.
6. Provide the information you collected in the Integration Key, Secret Key, and API Hostname fields.
7. Click Test Duo Connectivity to verify the keys and hostname are correct.
8. Click Save Changes.

Disable two factor authentication for the default admin account as a failsafe mechanism so there is at least one account that can log into Splunk Phantom to administer Duo settings if the integration breaks.

With two factor authentication enabled, two new fields appear in the Edit User page:

• Two Factor Authentication. Set this field to Duo to enable two factor authentication. Select None to disable two factor authentication.
• Duo Username. Use this field to make sure the Splunk Phantom and Duo usernames match. For example, a user’s Splunk Phantom username is jsmith but his Duo username is jsmith@splunk.com. In this case, set the Duo username to jsmith@splunk.com so the correct Duo user is used when logging in to Splunk Phantom.
Configure role based access control inside Splunk Phantom apps

Phantom supports granular asset access control inside of Splunk Phantom 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 Phantom app. Configure user and group permissions on all configured apps before enabling granular asset access control.

The following example shows how to set up a user for a single permission on the Phantom DNS app.

1. From the Main 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 Herman Smith and click the right arrow in order to move this user into the Approved Users and Roles area as shown in the following image:

![Image showing the setup process for user permissions in Splunk Phantom DNS app]
8. Click **Save**.

With your app configured for this role, you can now enable granular asset access control so that these permissions take effect.

1. From the Main 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**.

### Secure Splunk Phantom by configuring an account password expiration

A common security practice is to set a user account password expiration after a specific period of time, such as every 90 days. Splunk Phantom does not provide the ability to configure an account password expiration. As a system administrator, you need to define, implement, and administer password expiration policies in accordance with your organization's requirements.

Take note of the following if you configure password expiration policies in your environment:

- Do not configure a password expiration for the root account. This can cause issues such as the `crond` daemon stopping, `logrotate` failing to trim logs, data ingestion pausing, or services failing to restart.
- Do not configure a password expiration in AWS environments. By default, AWS instances use key pairs for authentication. If a user account expires, the account is blocked from accessing the AMI unless the user has configured an account password and can provide it when prompted. Key pair authentication doesn't work for expired accounts.

To reset a user's account expiration date, shut down the AWS instance and update user data through the AWS console. For example, to set an account expiration date of January 1, 2023:

```bash
# cloud-boothook
# !/ bin / bash
# chage -E "Jan 1, 2038" user
```

Specify a date in the future but before Jan 19, 2038. The latest time that can be represented in Unix's signed 32-bit integer time format is 03:14:07 UTC on Tuesday, 19 January 2038.

You can configure the user account to never expire:

```bash
# chage -m 0 user
# chage -M 99999 user
# chage -l user
Last password change : Dec 10, 2016
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```
Manage your registered mobile devices

Enable or disable registered mobile devices

You can allow users to register mobile devices and use Splunk mobile apps with your Splunk Phantom instance.

The Enable Mobile App toggle is disabled by default. Toggle this switch so that users see the Mobile Device Registration tab in their Account Settings and use it to register mobile devices. This toggle is available for viewing and editing if your role has basic permissions in the system settings with view and edit selected. See Manage roles and permissions in Splunk Phantom for more information about roles and permissions.

Enable mobile device registration with Splunk Phantom

Enable registration of mobile devices by doing the following:

1. From the main menu, select Administration.
2. Select Mobile.
3. Toggle the Enable Mobile App switch to the On position.
4. Click Confirm.

Disable mobile device registration with Splunk Phantom

Disable registration of mobile devices by doing the following:

1. From the main menu, select Administration.
2. Select Mobile.
3. Toggle the Enable Mobile App switch to the Off position.
4. Click Confirm.

When mobile device registration is disabled, traffic doesn’t flow between Splunk Phantom and mobile devices, and the Mobile Device Registration tab is no longer visible in Account Settings.

When the mobile feature is re-enabled, previously registered devices can resume communication with Splunk Phantom.

View registered mobile devices

When the Enable Mobile App toggle is switched on, you can see all the mobile devices that are registered by Splunk Phantom users. You can see them as a list, or you can search for them by device name.

If users remove their own devices from their account settings, then the devices automatically disappear from this list. Users can also remove their registration from the Splunk Mobile app, and the devices also automatically disappear from this list. You can remove your registration only while the Enable Mobile App toggle is switched on. If the toggle is switched off, then the removal message is not received.
Remove registered mobile devices

When the Enable Mobile App toggle is switched on, you can remove a Splunk Phantom user’s registered device.

If you delete a user account, Splunk Phantom removes the registration for all of the devices that belong to the user.

When you no longer want a user to have access to the mobile app from a particular mobile device, do the following to remove the registered device:

1. Locate the device by its name in the table.
2. In the Action column, click remove.
3. When prompted, confirm by clicking remove.
Monitor the health of your system

Monitor the health of your Splunk Phantom system

Use the System Health page to view a summary of your Splunk Phantom instance. The System Health page includes the following information:

- Running status of Splunk Phantom 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 Phantom 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 Phantom. Verify that each process has a green **Running** status icon. Click **Restart** if you need to restart any one of the individual processes.

Splunk Phantom runs on top of Linux, so these graphs can be interpreted as you might on any Linux system. On a fairly idle Splunk Phantom 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 Phantom 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 Phantom to work properly. Splunk Phantom also relies on **HTTPD** and **Postgres**, which is the database.

If you registered a mobile device and **Enable Mobile App** is on, you can see the following behaviors in Splunk Phantom:

- The **ProxyD** daemon starts automatically. The **WatchdogD** daemon keeps track of the toggle switch position and adds or removes the **ProxyD** daemon from the system startup list depending on the status.
- The System Health page also includes usage statistics for the **ProxyD** daemon. See **Enable or disable registered mobile devices** for information about the Enable Mobile App toggle.

**View how much data is ingested in Splunk Phantom using ingestion summary**

The ingestion summary page provides a summary of container 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 Phantom and how that amount is trending over time.

Perform the following steps to view ingestion summary details:

1. From the Main 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 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 datetime 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 Main 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 Splunk Phantom daemons

You can adjust logging levels for each daemon running in Splunk Phantom to help debug or troubleshoot issues.

Splunk Phantom daemons

The following daemons in Splunk Phantom work to control collection and scheduling tasks in the background independently from the Splunk Phantom web interface:

<table>
<thead>
<tr>
<th>Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 if Python version 2 or 3 is being used. The debug logs look very similar for both Python versions, but show Running executable: spawn3 for Python 3. The following key actions are logged by this daemon:  
  • Manual actions run against any configured asset  
  • Scheduled actions against any configured asset |
| Cluster daemon | Responsible for communicating with cluster nodes. Available only in clustered environments.                                                                                                               |
| Decide daemon | Responsible for operating on incoming data. The following key actions are logged by this daemon:                                                                                                          |
### Daemons

<table>
<thead>
<tr>
<th>Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest daemon</td>
<td>Responsible for ingesting data into the product. The following key actions are logged by this daemon:</td>
</tr>
<tr>
<td>Proxy daemon</td>
<td>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.</td>
</tr>
<tr>
<td>Watchdog daemon</td>
<td>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:</td>
</tr>
<tr>
<td>Workflow daemon</td>
<td>Responsible for managing approval requests to action reviewers and asset owners. The following key actions are logged by the workflow daemon:</td>
</tr>
</tbody>
</table>

#### Configure the logging level for each Splunk Phantom daemon

Adjust the logging levels as needed to assist Splunk Phantom 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 each daemon you want to change. 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.
4. (Optional) Click **Download Logs** to download a copy of the current log files for manual investigation or a submission to support.

A zipped **TAR** archive of the logs is downloaded to `/var/log/phantom`.

1. Click **Save Changes**.
At the operating system level, log files are in `/var/log/phantom`. In a non-root installation, the path is `${phantom_home}/var/log/phantom`. Adjust logging levels only at the direction of Splunk Phantom Support.

**Example log structure**

See the following sample of a common log format:

```
```

This table summarizes the structure of the example log message.

<table>
<thead>
<tr>
<th>Log message content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 5 22:55:18</td>
<td>Timestamp of when the log message was generated.</td>
</tr>
<tr>
<td>localhost</td>
<td>Name of the host where the log message was generated.</td>
</tr>
<tr>
<td>DECIDED[7177]:</td>
<td>Name of the component and process ID (PID) generating the message.</td>
</tr>
<tr>
<td>TID:7422:</td>
<td>Threat ID (TID) of the message.</td>
</tr>
<tr>
<td>WARNING:</td>
<td>Log level or class of the message.</td>
</tr>
<tr>
<td>DECIDED:</td>
<td>Functional component that generated the log message.</td>
</tr>
<tr>
<td>rules_engine.cpp:</td>
<td>Source file applicable to the log message.</td>
</tr>
<tr>
<td>1503:</td>
<td>Line number in the source file that caused this log message to be generated.</td>
</tr>
<tr>
<td>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</td>
<td>The log message.</td>
</tr>
</tbody>
</table>

**Monitor Splunk Phantom logs using an external SIEM**

You can use an external SIEM such as Splunk Enterprise to monitor the status of your Splunk Phantom instance using the log files from Splunk Phantom. Monitor errors in actions execution through the ingestion of the actiond.log file, and you can find platform information in the watchdogd.log file.

These files are constantly updated by the components of the Splunk Phantom platform. Use a service to monitor the log file regularly, or copy and forward the log files on a regular basis.

**Rotate your Splunk Phantom logs when they get too large**

The Splunk Phantom logs in `/var/log/phantom` are automatically rotated when they reach 10 MB in size. Splunk Phantom keeps a running archive of the last 10 rotated logs. The oldest log is deleted when a new log is rotated in. You can configure log rotation settings for your organization's IT requirements by modifying the `phantom_logrotate.conf` file and restarting `rsyslog` for the changes to take effect.
Perform the following tasks to configure log rotation on Splunk Phantom:

1. Run the `logrotate --version` command to find your Logrotate version. For example:

   [root@phantom]# logrotate --version
   logrotate 3.8.6

2. Configure logrotate using the instructions based on your Logrotate version.
   ♦ If you are running Logrotate version 3.8.x, use a configuration with the `su` directive. By default, the configuration file is located in `/etc/logrotate.d/phantom_logrotate.conf`. For example:

   [root@phantom]# more /etc/logrotate.d/phantom_logrotate.conf
   /var/log/phantom/[/!wr][!s]*.log {
     su phantom phantom
     rotate 10
     size 10M
     start 1
     create 0660 phantom phantom
     postrotate
     kill -HUP $(cat /var/run/syslogd.pid)
   } \n   
   /var/log/phantom/wsgi.log {
     su nginx phantom
     rotate 10
     size 10M
     start 1
     create 0660 nginx phantom
     postrotate
     kill -HUP $(cat /var/run/syslogd.pid)
   } \n   
   /var/log/phantom/rsync*.log {
     su root root
     rotate 10
     size 10M
     start 1
     create 0644 root root
     postrotate
     kill -HUP $(cat /var/run/syslogd.pid)
   } \n   
   ♦ If you are running a Logrotate version older than 3.8.x, the default location and content of the Logrotate configuration file is `/etc/logrotate.d/phantom_logrotate.conf`. For example:

   [root@phantom]# more /etc/logrotate.d/phantom_logrotate.conf
   /var/log/phantom/*.log {
     rotate 10
     size 10M
     start 1
     create 0660 root phantom
     postrotate
     kill -HUP $(cat /var/run/syslogd.pid)
   } \n
3. After configuring Logrotate in the configuration file, restart `rsyslog` using the `/opt/phantom/bin/phsvc restart rsyslog` command. For example:

   root@phantom]#/opt/phantom/bin/phsvc restart rsyslog
   Shutting down system logger: [ OK ]
   Starting system logger: [ OK ]
Enable and download audit trail logs in Splunk Phantom

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

Enable audit trail tracking

By default, all audit tracking in Splunk Phantom is disabled. Perform the following tasks to enable audit trail tracking in Splunk Phantom:

1. From the main 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 Phantom immediately starts tracking audit events for the selected items.

Even when the audit categories are disabled, Splunk Phantom automatically tracks events such as action and playbook runs and logs them 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 Main 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 `%` as the separator. For example, if you want to specify user1 and user2:

```
user1%user2
```

**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:

<table>
<thead>
<tr>
<th>Audit Trail Area</th>
<th>Required privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>View Users and Roles</td>
</tr>
<tr>
<td>Administration</td>
<td>View System Settings</td>
</tr>
<tr>
<td>User</td>
<td>View Users and Roles</td>
</tr>
<tr>
<td>Role</td>
<td>View Users and Roles</td>
</tr>
<tr>
<td>Playbooks</td>
<td>View Playbooks</td>
</tr>
<tr>
<td>Containers</td>
<td>View Containers</td>
</tr>
</tbody>
</table>

**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 Phantom**

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 Main Menu, select Administration.
2. Select System Health > Automation.

**View the playbook run history in Splunk Phantom**

You can view the history of playbook runs on your Splunk Phantom instance.

1. From the Main 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:

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

**View the action run history**

You can view the history of actions run on your Splunk Phantom instance.
1. From the Main 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:

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the action that was run.</td>
</tr>
<tr>
<td>Run ID</td>
<td>The numeric ID of the action that was run.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The numeric ID of the event the action was run against.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the action started.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time the action finished.</td>
</tr>
<tr>
<td>Status</td>
<td>Whether the action succeeded or failed.</td>
</tr>
<tr>
<td>Prompted</td>
<td>If the action taken was a prompt or manual task action, the ID of the user assigned the action appears here.</td>
</tr>
<tr>
<td>Run By</td>
<td>The name of the user who ran the action.</td>
</tr>
<tr>
<td>View Results</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Use ITSI to monitor the health of your Splunk Phantom deployment**

Splunk IT Service Intelligence (ITSI) is a scalable IT monitoring and analytics solution that provides actionable insight into the performance and behavior of your IT operations. ITSI is built on the Splunk operational intelligence platform and uses the search and correlation capabilities of the platform to help you collect, monitor, and report on data from IT devices, systems, and applications.

As a Splunk Phantom administrator, you can use ITSI to monitor the health of your Splunk Phantom instance or cluster. For more information, see About the Content Pack for Monitoring Phantom as a Service in Splunk ITSI Content Packs.
Manage Splunk Phantom Apps and Assets

Add and configure apps and assets to provide actions in Splunk Phantom

Splunk Phantom apps expand the capabilities of your Splunk Phantom 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 Phantom playbooks. For example, the MaxMind app provides the geolocate ip action for your Splunk Phantom deployment.

You can upgrade existing apps or install new apps at any time without having to upgrade the entire Splunk Phantom platform.

Apps have full access to the operating system of the Splunk Phantom platform. 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 Phantom ships with a VMware vSphere app enabling Splunk Phantom to get information from and take actions against a vSphere host. You can use Splunk Phantom 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 Phantom 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:

<table>
<thead>
<tr>
<th>Splunk Phantom app</th>
<th>Configure multiple assets from a single app</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td>vSphere 1</td>
</tr>
<tr>
<td></td>
<td>• IP address 192.168.1.1</td>
</tr>
<tr>
<td></td>
<td>• User admin1, password example1</td>
</tr>
<tr>
<td></td>
<td>vSphere 2</td>
</tr>
<tr>
<td></td>
<td>• IP address 192.168.1.2</td>
</tr>
<tr>
<td></td>
<td>• User admin2, password example2</td>
</tr>
<tr>
<td></td>
<td>vSphere 3</td>
</tr>
<tr>
<td></td>
<td>• IP address 192.168.1.3</td>
</tr>
<tr>
<td></td>
<td>• User admin3, password example3</td>
</tr>
</tbody>
</table>

View your Splunk Phantom apps

Splunk Phantom ships with hundreds of apps already installed. You can find more apps on the Splunk Phantom portal, from other Splunk Phantom users, and even create your own. See Splunk Phantom apps overview in Develops Apps for Splunk Phantom.
Perform the following tasks to view the apps provided by Splunk Phantom on the Apps page.

1. From the main 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 Phantom asset](#).
3. (Optional) Click **Unconfigured Apps** to view the list of apps installed on your Splunk Phantom instance that do not have at least one asset configured.
4. (Optional) Click **Orphaned Assets** to review any assets that no longer have a corresponding app installed.

### Install, update, or delete apps on Splunk Phantom

Navigate to the Apps page to install, update, or delete Splunk Phantom apps.

#### Install a new Splunk Phantom app

Perform the following steps to install a new Splunk Phantom app:

1. Obtain the new app or develop a new app. See Splunk Phantom apps overview in [Develops Apps for Splunk Phantom](#).
2. From the main 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**.

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.

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 Phantom apps

To update an existing Splunk Phantom app, perform the following steps:

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

#### Delete a Splunk Phantom app

Perform the following steps to delete a Splunk Phantom app:

1. From the main 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.

### View your Splunk Phantom assets

Splunk Phantom 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 main 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 Phantom asset

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

#### Add a new Splunk Phantom asset

Perform the following steps to create a new Splunk Phantom asset:

1. From the main 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 Phantom](#).
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 Phantom 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 Phantom.

#### Edit a Splunk Phantom asset

Perform the following steps to edit a Splunk Phantom asset:

1. From the main 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**.

**Delete a Splunk Phantom asset**

Perform the following steps to delete a Splunk Phantom asset.

1. From the main 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 just in time (JIT) credentials, automation users, asset environment variables, and proxies.

**Configure Just In Time Credentials for a Splunk Phantom asset**

Some assets can be configured to use just in time (JIT) credentials, which require a Splunk Phantom 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 Phantom 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 Phantom for your own approval vote, you still receive a JIT prompt when credentials are required.
**Configure automation users for a Splunk Phantom asset**

Define the automation user to specify the service account Splunk Phantom uses to run the asset. The default account is the automation account provided by Splunk Phantom.

Perform the following tasks to create a custom automation user in Splunk Phantom:

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 if 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 Phantom asset**

Environment variables configured in an asset take precedence over any global environment variables. See Set environment variables globally for all apps for information about setting global environment variables.

Perform the following tasks to set environment variables for a Splunk Phantom 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 if 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 Phantom web interface.
8. (Optional) Click + Variable to add more variables as needed.
9. Click Save.

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

**Configure proxies for a Splunk Phantom 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. 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. Click + 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) Click Secret to encrypt the value so that it is not displayed in the Splunk Phantom web interface.
8. Click Save.
The table shows an example of how to configure HTTP, HTTPS, and no proxy for a Splunk Phantom asset. For apps that use requests, configuring both HTTPS and HTTP environment variables directs all app traffic through the proxy server.

<table>
<thead>
<tr>
<th>Proxy Name</th>
<th>Proxy Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS_PROXY</td>
<td><a href="https://192.168.13.100:8800">https://192.168.13.100:8800</a></td>
</tr>
<tr>
<td>NO_PROXY</td>
<td>example.com</td>
</tr>
</tbody>
</table>

**Configure ingest settings for a Splunk Phantom 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 Phantom 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 Phantom to process any missed jobs. Jobs can be missed in cases where Splunk Phantom is not running, or one poll didn't complete before the next one started.
7. Click **Save**.

**Configure approval settings for a Splunk Phantom 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 Phantom asset to determine who must approve the actions taken against the asset. See **Approve actions before they run in Splunk Phantom** in the *Use Splunk Phantom* 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 the tenant assigned to a Splunk Phantom asset

Assign a tenant to an asset to separate data and make sure that the asset is only used with the container with the same tenant. You can only assign tenants to an asset if multi-tenancy is configured and enabled in Splunk Phantom. See Configure multiple tenants on your Splunk Phantom instance.

Perform the following steps to assign a tenant to a Splunk Phantom asset:

1. Make sure multi-tenancy is enabled on your Splunk Phantom instance.
2. Navigate to the asset configuration page.
3. Click the Tenants tab.
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. Select the desired tenants from the Available Tenants box and click the arrows to move them to the Mapped to Asset box.
   - Non-ingestion assets that do not have a tenant assigned are available to all tenants. You can assign multiple tenants to a non-ingestion asset.
   - Ingestion assets must have one tenant assigned. You can't assign multiple tenants. If no tenant is selected in the asset configuration, the default system tenant is assigned to the asset and any containers created by the asset.
6. Click Save.
Backup or restore your Splunk Phantom instance

Splunk Phantom backup and restore overview

Splunk Phantom includes a tool, ibackup.pyc, to back up and restore your Splunk Phantom data.

Regularly back up your Splunk Phantom deployment to safeguard your data in these cases:

- To restore your Splunk Phantom deployment in the event of a disaster
  - Restore a lost or failed file share
  - Restore a lost or failed PostgreSQL database
- To restore data from your Splunk Phantom deployment to another
  - Restore data from a Phantom instance or cluster to a new instance or cluster
  - Restore data from a standalone instance to a newly deployed cluster
  - Restore data from a clustered deployment to a standalone Phantom instance
  - Rebuild a Phantom cluster where the Phantom nodes have failed

Save your backups in a safe place, such as one that is not on the same disk, partition, or virtual machine as your Splunk Phantom instance.

Supported configurations

You can backup a Splunk Phantom deployment using any of these configurations:

- A privileged, standalone instance
- A privileged instance, external PostgreSQL database
- A privileged instance, external file shares
- An unprivileged, standalone instance
- An unprivileged instance, external PostgreSQL database
- An unprivileged instance, external file shares
- A privileged cluster
- An unprivileged cluster

You can build Splunk Phantom deployments from any supported installation method. See Install Splunk Phantom using the Amazon Marketplace Image in Install and Upgrade Splunk Phantom.

Backup types

The ibackup.pyc tool is based on the open source pgBackRest project, and it supports full and incremental backups. Differential backups are not supported.

- A full backup includes all the file sets included in the What is in a full backup section on this page.
- Incremental backups contain only the changes made to your deployment's PostgreSQL database and files since the last full or incremental backup was made.
- A configuration only backup, which makes a backup of all the Splunk Phantom configurations. This type of backup requires downtime.
**Backup levels and groups**

Backups are created in `<PHANTOM_HOME>/phantom/data/backup/`. Each backup is part of a group, based on a full backup that is the base of the group, and is labeled by level.

For example, if the first backup on a Splunk Phantom instance is named "phantom_backup_group_0_level_0.tar". Then, the first incremental backup made is then named "phantom_backup_group_0_level_1.tar".

Each subsequent incremental backup in the same group increases by a level of one.

Additional full backups create a new group, and incremental backups based on that full backup start incrementing the level number.

When you begin a new group based on a new full backup, earlier groups stop incrementing. Further incremental backups belong to the new group.

You can control the number of backup groups by using the `--set-full-backup-limit` argument with `ibackup.pyc`.

You can change the number of backup groups by running the `ibackup.pyc` script with a new `--set-full-backup-limit` argument. If you set a lower limit, backup groups are deleted, starting with the oldest group.

For example, a Splunk Phantom deployment is configured for backup and restore using `ibackup.pyc --set-full-backup-limit 3`. After several weeks, three backup groups exist, each with a full backup and several incremental backups:

**Group 0**

- phantom_backup_group_0_level_0.tar
  - phantom_backup_group_0_level_1.tar
  - phantom_backup_group_0_level_2.tar
  - phantom_backup_group_0_level_3.tar

**Group 1**

- phantom_backup_group_1_level_0.tar
  - phantom_backup_group_1_level_1.tar
  - phantom_backup_group_1_level_2.tar
  - phantom_backup_group_1_level_3.tar

**Group 2**

- phantom_backup_group_2_level_0.tar
  - phantom_backup_group_2_level_1.tar
  - phantom_backup_group_2_level_2.tar
  - phantom_backup_group_2_level_3.tar

A decision is made that the oldest backups are no longer required, so an administrator runs `ibackup.pyc --set-full-backup-limit 3`. When the next backup runs after the new full backup limit is set, Group 0 is deleted.
What is in a full backup?

A full backup of a Splunk Phantom instance contains the following file sets:

<table>
<thead>
<tr>
<th>File set</th>
<th>Files</th>
<th>Backup path</th>
</tr>
</thead>
<tbody>
<tr>
<td>misc_files</td>
<td>Miscellaneous files used by Splunk Phantom.</td>
<td><code>&lt;PHANTOM_HOME&gt;/keystore/private_key.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/www/phantom_ui/secret_key.py</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/www/phantom_ui/secret_key.pyc</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_ETC&gt;/nginx/conf.d/default.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/cacerts.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/splunk/etc/apps/splunk_httpinput/local/inputs.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/enable</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/www/phantom_ui/auth_backends/saml2_xml</code></td>
</tr>
<tr>
<td>apps</td>
<td>All Splunk Phantom apps, excluding app_states.</td>
<td><code>&lt;PHANTOM_HOME&gt;/apps</code></td>
</tr>
<tr>
<td>ssl</td>
<td>All Splunk Phantom etc/ssl contents.</td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/ssl</code></td>
</tr>
<tr>
<td>certs</td>
<td>All Splunk Phantom certificates.</td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/certs</code></td>
</tr>
<tr>
<td>playbooks</td>
<td>All playbooks, excluding playbook states.</td>
<td><code>&lt;PHANTOM_HOME&gt;/scm</code></td>
</tr>
<tr>
<td>nginx_keys</td>
<td>The NGINX SSH keys.</td>
<td><code>&lt;PHANTOM_VAR&gt;/cache/nginx/.ssh</code></td>
</tr>
<tr>
<td>vault</td>
<td>All vault contents, excluding files that are still streaming to storage.</td>
<td><code>&lt;PHANTOM_HOME&gt;/vault</code></td>
</tr>
<tr>
<td>app_states</td>
<td>All Splunk Phantom app states, excluding apps.</td>
<td><code>&lt;PHANTOM_HOME&gt;/local_data/app_states</code></td>
</tr>
<tr>
<td>playbook_states</td>
<td>All Splunk Phantom playbook states, excluding playbooks.</td>
<td><code>&lt;PHANTOM_HOME&gt;/tmp</code></td>
</tr>
</tbody>
</table>

How an incremental backup differs from a full backup

Incremental backups contain only changes to your Splunk Phantom deployment since the last backup was made.

Incremental backups are based on a group of backup files that begin with a full backup, then the backup files in sequence. The new file contains changes that were made since the previous backup.

An incremental backup cannot be used to restore a system on its own. It must be used with the related full backup and any intermediate incremental backups. For example:

- phantom_backup_group_0_level_0.tar
- phantom_backup_group_0_level_1.tar
- phantom_backup_group_0_level_2.tar
- phantom_backup_group_0_level_3.tar

In this example, `phantom_backup_group_0_level_0.tar` is the full backup that forms the base of the backup group. The files `phantom_backup_group_0_level_1.tar`, `phantom_backup_group_0_level_2.tar`, and `phantom_backup_group_0_level_3.tar` are incremental backups that depend on the earlier files.

An administrator can restore a Splunk Phantom deployment from any point in the group as long as the earlier files in the group are present.
## Supported restore configurations

This table presents possible destinations for restoring a backup.

The origin of a backup can be any supported Splunk Phantom deployment, such as a virtual machine image, RPM-based installation, or Amazon Marketplace Image.

- The Splunk Phantom deployments, the origin of the backup, and the destination for the restore must be running the same version of Splunk Phantom.
- You cannot restore a backup from a privileged instance of Splunk Phantom to an unprivileged instance or from an unprivileged instance to a privileged instance.

<table>
<thead>
<tr>
<th>Backup origin</th>
<th>Possible backup destinations</th>
</tr>
</thead>
</table>
| Standalone, privileged instance                     | • Standalone, privileged instance  
• Privileged cluster  
• Single privileged instance, external PostgreSQL database  
• Single privileged instance, external file shares  
• Privileged instance, external PostgreSQL database and file shares |
| Single privileged instance, external PostgreSQL database | • Standalone, privileged instance  
• Privileged cluster  
• Single privileged instance, external PostgreSQL database  
• Single privileged instance, external file shares  
• Privileged instance, external PostgreSQL database and file shares |
| Single privileged instance, external file shares     | • Standalone, privileged instance  
• Privileged cluster  
• Single privileged instance, external PostgreSQL database  
• Single privileged instance, external file shares  
• Privileged instance, external PostgreSQL database and file shares |
| Privileged instance, external PostgreSQL database and file shares | • Standalone, privileged instance  
• Privileged cluster  
• Single privileged instance, external PostgreSQL database  
• Single privileged instance, external file shares  
• Privileged instance, external PostgreSQL database and file shares |
| Standalone, unprivileged instance                    | • Standalone, unprivileged instance  
• Unprivileged cluster  
• Single unprivileged instance, external PostgreSQL database  
• Single unprivileged instance, external file shares  
• Unprivileged instance, external PostgreSQL database and file shares |
| Unprivileged instance, external PostgreSQL database  | • Standalone, unprivileged instance  
• Unprivileged cluster  
• Single unprivileged instance, external PostgreSQL database  
• Single unprivileged instance, external file shares |
<table>
<thead>
<tr>
<th>Backup origin</th>
<th>Possible backup destinations</th>
</tr>
</thead>
</table>
| Unprivileged instance, external file shares       | • Standalone, unprivileged instance  
• Unprivileged cluster  
• Single unprivileged instance, external PostgreSQL database  
• Single unprivileged instance, external file shares  
• Unprivileged instance, external PostgreSQL database and file shares |
| Unprivileged instance, external PostgreSQL database and file shares | • Standalone, unprivileged instance  
• Unprivileged cluster  
• Single unprivileged instance, external PostgreSQL database  
• Single unprivileged instance, external file shares  
• Unprivileged instance, external PostgreSQL database and file shares |

**Back up a Splunk Phantom deployment**

Your Splunk Phantom deployment is backed up using command-line tools.

- You need root or sudo permissions to create a backup.
- You do not need to take Splunk Phantom offline to do a backup.

**Prepare Splunk Phantom for a backup**

Before you can create backups, you must prepare Splunk Phantom by running the `ibackup.pyc` command with the `--setup` option. You must also run this command after you upgrade Splunk Phantom.

During setup, `ibackup.pyc` temporarily stops Splunk Phantom services in order to make changes to the PostgreSQL database configuration. Services restart before setup is complete. This causes the following error to be displayed during the setup process, which can be ignored:

```
psql: ERROR:  pgbouncer cannot connect to server
```

If your Splunk Phantom deployment uses a Warm Standby or if you intend to use a Warm Standby, you must configure Warm Standby before setting up backups.

1. From the command line, SSH to your Splunk Phantom instance.
   ```
   SSH <username>@<phantom_hostname>
   ```
2. Change the directory to `<PHANTOM_HOME>/bin`.
   ```
   cd <PHANTOM_HOME>/bin
   ```
3. Prepare the system for a backup.
   ```
   sudo phenv python ibackup.pyc --setup
   ```

The command output looks like this:

```
[user@phantom bin]$ sudo phenv python ibackup.pyc --setup
```
If the Splunk Phantom instance or cluster has been setup for backups, the tool prompts you to confirm that you wish to run setup again:

You appear to have already run setup. Re-run again? Enter yes to proceed:

Enter **yes** to run the setup process again.

Running the setup again after a restore resets the state file used by ibackup.pyc and archives all existing backup files. Running it a second time before any restore actions does nothing.

**Prepare a Splunk Phantom cluster or deployment with an external PostgreSQL database**

For Splunk Phantom deployments where the PostgreSQL database is external to the Splunk Phantom instance or in clustered deployments, you must take additional steps to prepare the deployment for backup.

In clustered deployments, all backup commands must be issued from the same cluster node.

1. From the command line, SSH to one cluster node of your Splunk Phantom deployment.
   ```bash
   SSH <username>@<phantom_hostname>
   ```
2. Change the directory to `<PHANTOM_HOME>/bin`
   ```bash
cd <PHANTOM_HOME>/bin
   ```
3. Run `ibackup.pyc`. This step generates the `db_bootstrap.tgz` file.
   ```bash
   sudo phenv python ibackup.pyc --setup
   ```
4. Use `SCP` to copy `db_bootstrap.tgz` to your PostgreSQL database host.
   ```bash
   scp db_bootstrap.tgz <username>@<postgresql_hostname>:/<directory>
   ```
5. SSH to the PostgreSQL database host.
   ```bash
   SSH <username>@<postgresql_hostname>
   ```
6. Extract the `db_bootstrap.tgz` file.
   ```bash
tar -xzf db_bootstrap.tgz
   ```
7. Change directory to the `/setup` directory created when `db_bootstrap.tgz` was extracted.
   ```bash
cd /setup
   ```
8. Run the `extdb_backup_bootstrap.py` script with the parameter `--pgdata /opt/phantom/data/db`
   ```bash
   sudo python extdb_backup_bootstrap.py --pgdata /opt/phantom/data/db
   ```
9. SSH to the cluster node where you ran `ibackup.pyc`.
   ```bash
   SSH <username>@<phantom_hostname>
   ```
10. Change the directory to `<PHANTOM_HOME>/bin`
    ```bash
cd <PHANTOM_HOME>/bin
    ```
11. Run `ibackup.pyc` to complete the setup.
sudo phenv python ibackup.pyc --setup

Create a full backup

Your Splunk Phantom instance is backed up using command-line tools. You do not need to take Splunk Phantom offline to create a backup.

In clustered deployments, all backup commands must be issued from the same cluster node.

1. From the command line, SSH to your Splunk Phantom instance.
   SSH <username>@<phantom_hostname>
2. Change the directory to <PHANTOM HOME>/bin.
   cd <PHANTOM_HOME>/bin
3. Perform the backup.
   sudo phenv python ibackup.pyc --backup

The command output looks like this:

[11/Dec/2019 21:25:17] WARNING: no prior backup exists, incr backup has been changed to full
[11/Dec/2019 21:25:58] INFO: You should ensure this tarball is kept safe. It will be required for restore

If you receive an error that postgresql.conf is owned by the root user, you will need to use the chown and chgrp commands to set the ownership of /<PHANTOM_HOME>/phantom/data/db/postgresql.conf to the postgres user. For clustered deployments, do this on the database node of the deployment.

If no backups exist, a full backup is created. When a full backup exists, a new incremental backup is added to the group. If you already have a backup group and want to create a new full backup, add the --backup-type full argument.

sudo phenv python ibackup.pyc --backup --backup-type full

Create an incremental backup

The ibackup.pyc tool checks whether a full backup exists. If a full backup doesn't exist, a full backup is created. If a full backup exists, an incremental backup is created and added to the backup chain. You do not need to take Splunk Phantom offline to create a backup.

In clustered deployments, all backup commands must be issued from the same cluster node.

1. From the command line, SSH to your Splunk Phantom instance.
   SSH <username>@<phantom_hostname>
2. Change the directory to <PHANTOM HOME>/bin.
   cd <PHANTOM_HOME>/bin
3. Perform the backup.
   sudo phenv python ibackup.pyc --backup

The command output looks like this:

You can override the default behavior by using this command-line option:

```
sudo phenv python ibackup.pyc --backup --backup-type incr
```

Save your backups in a safe place, such as one that is not on the same disk, partition, or virtual machine as your Splunk Phantom instance.

**Restore Splunk Phantom from a backup**

You need root permissions to restore from a backup.

Backups must be restored to an instance with the same privilege level. You cannot restore a backup from a privileged instance of Splunk Phantom to an unprivileged instance or from an unprivileged instance to a privileged instance.

Backups can be used in conjunction with the Splunk Phantom Warm Standby feature for additional protection against system failure.

In clustered deployments, all backup and restore commands must be issued from the same cluster node.

**Prepare your system for restore**

You must prepare your system for a restore before a Splunk Phantom deployment can benefit from a restore. Preparing your deployment is important if you are restoring data from one Splunk Phantom deployment to another deployment. To prepare your deployment for restoring, perform the following steps:

1. From the command line, SSH to your Splunk Phantom instance.
   ```
   SSH <username>@<phantom_hostname>
   cd <PHANTOM_HOME>/bin
   sudo phenv python ibackup.pyc --setup
   ```

When you restore a backup to the same deployment, the setup was completed as part of making the backup.

**Restore your instance from a full backup**

1. From the command line, SSH to your Splunk Phantom instance.
   ```
   SSH <username>@<phantom_hostname>
   cd <PHANTOM_HOME>/bin
   sudo phenv python ibackup.pyc --restore <path/to/<number>_phantom_backup.tar>
   ```
Restore your system from an incremental backup

Before restoring your system from an incremental backup, you must prepare the system. See Prepare your system for restore.

Incremental backups contain only the changes to your Splunk Phantom instance since the last full backup or previous incremental backup. An incremental backup cannot be used to restore a system on its own. It must be used with the related full backup and any intermediate backups.

The sequence looks like this:

1. Create a full backup called `phantom_backup_group_0_level_0.tar`.
2. Create an incremental backup called `phantom_backup_group_0_level_1.tar`, which is based on `phantom_backup_group_0_level_0.tar`.
3. Create a second incremental backup called `phantom_backup_group_0_level_2.tar`, which is based on `phantom_backup_group_0_level_1.tar` and `phantom_backup_group_0_level_0.tar`.

Use the sequential files to restore your system in the following ways:

- You can restore `phantom_backup_group_0_level_0.tar` alone.
- You cannot restore `phantom_backup_group_0_level_1.tar` without `phantom_backup_group_0_level_0.tar`.
- You cannot restore `phantom_backup_group_0_level_2.tar` without `phantom_backup_group_0_level_0.tar` and `phantom_backup_group_0_level_1.tar`.

**Restore the incremental backup**

1. From the command line, SSH to your Splunk Phantom instance.
   - `SSH <username>@<phantom_hostname>`
2. Change the directory to `<PHANTOM HOME>/bin`.
   - `cd <PHANTOM_HOME>/bin`
3. Copy the backup group and the incremental-level tar files from storage to the instance you are restoring.
4. Perform the restore. Enter the file name of the last incremental backup file you want to restore.
   - `sudo phenv python ibackup.pyc --restore < phantom_backup_group_<#>_level_<#>.tar >`

**Determine whether the system restore was successful**

A successful restore outputs information to the console.

```
[root@phantom bin]# phenv python ibackup.pyc --restore
/opt/phantom/data/backups/phantom_backup_group_0_level_0.tar
[06/Feb/2020 20:10:15] INFO: Running ibackup.pyc - details will be logged to
/var/log/phantom/backup/ibackup_2020-02-06T20:10:15.089127Z.log
[06/Feb/2020 20:10:15] INFO: Attempting to connect to Postgresql ...
[06/Feb/2020 20:10:17] INFO: Checking filesystem backup state at /opt/phantom/data/ibackup/repo/fs
[06/Feb/2020 20:10:17] INFO: Restoring this backup requires utilizing 9.11334507138% of the total volume capacity
[06/Feb/2020 20:10:21] INFO: Attempting to connect to Postgresql ...
psql: ERROR: pgbouncer cannot connect to server
[06/Feb/2020 20:10:21] INFO: Retrying ...
[06/Feb/2020 20:10:22] INFO: Attempting to connect to Postgresql ...
psql: ERROR: pgbouncer cannot connect to server
[06/Feb/2020 20:10:22] INFO: Retrying ...
```
After restoring your system, you must run `sudo phenv python ibackup.pyc --setup` again before you can make new backups.

**Splunk Phantom backup tools**

Use the ibackup.pyc tool to create, manage, and restore backups.

Logs for each run of the tool are written to `/var/log/phantom/backup/backup.log`.

Completed backups are stored in `<PHANTOM_HOME>/phantom/data/backup`.

If you are using an unprivileged installation, the logs are written to `<PHANTOM_HOME>/var/log/phantom/backup/backup.log`.

You can find a repository of staging files for the PostgreSQL database backup in `<PHANTOM_HOME>/data/ibackup/repo/pg`.

**ibackup.pyc arguments**

The following table shows the ibackup.pyc arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Shows the ibackup.pyc tool help message and exits.</td>
</tr>
<tr>
<td>--setup</td>
<td>Prepares the instance or cluster for backup and restore.</td>
</tr>
<tr>
<td>--max-cores &lt;value&gt;</td>
<td>Specifies the maximum number of processing cores allowed for database backup and restore operations. The default value is two cores.</td>
</tr>
<tr>
<td>--backup</td>
<td>Performs a backup.</td>
</tr>
<tr>
<td>--restore &lt;path/to/backup/&gt;</td>
<td>Performs a restore. You must provide a path to the last backup tar file to perform a restore.</td>
</tr>
<tr>
<td>--set-pgbackrest-repo &lt;path to repository&gt;</td>
<td>Sets the path of the pgbackrest repository.</td>
</tr>
<tr>
<td>--backup-components</td>
<td>Selectively backs up specific Phantom components. The default is all components. You must specify the same components for <code>--restore-components</code> when you restore using a backup created this way. See <code>--restore-components</code> for a complete list. For example: <code>--backup-components db,playbooks,keys</code></td>
</tr>
</tbody>
</table>
Backups include only configuration data. This always creates a full backup of configuration data. Incremental backup of configuration data is not supported.

Using the --config-only argument requires Splunk Phantom to shutdown in order to create the configuration backup.

Selectively restores specific Phantom components. The default is all components.

The following components are valid components:

- db: the PostgreSQL database
- configuration: the Phantom instance or cluster configuration information
- apps: The apps installed for phantom
- app_states: The state of each app at the time of the backup
- playbooks: the current playbooks in the scm
- playbooks_states: the current state of each playbook at the time of the backup
- vault: the Phantom vault

For example: --restore-components db,playbooks,keys

Lists existing backups and their state. Use with --verbose for more detailed output.

Deletes all backups.

This action is irreversible.

Deletes a full backup group. Takes an integer that represents the backup group to delete.

Shows the ibackup.pyc tool version number and exit.

Overides the default backup path <PHANTOM_HOME>/phantom/data/backup. Takes a directory path for the directory where backups will be stored.

Backup type. Using "full" creates a new full backup. Using "incr" creates an incremental on top of the current full backup.

If no full backup is taken and "incr" is given, the backup type defaults to "full". The default option if none is specified is "incr".

Sets the maximum number of full backups allowed at once. Automatically rotates once the limit is reached.

Writes debug-level log information to the console.

Lists the current settings for ibackup.

Runs pg_stop_backup against the current PostgreSQL database.

Use this argument only in exceptional circumstances, such as preventing a new full backup from overwriting an existing one.

Automatically responds with "yes" to all prompts from ibackup.

Use ibackup.pyc with warm standby

The warm standby and the backup and restore features require careful planning to use together.
Warm standby and ibackup features of Splunk Phantom use the Write Ahead Logging feature in PostgreSQL. When you configure a Splunk Phantom deployment to use both warm standby and ibackup, you must configure warm standby first. After restoring a deployment with ibackup, you must update the warm standby configuration.

Configuring warm standby after configuring ibackup archives all existing backups. Archiving all of the backups prevents new backups from being generated or existing backups from being used in a restore.

You can generate new backups once you run ibackup with the --setup option.

**Restore a system configured for warm standby**

In a warm standby configuration, when the primary Phantom instance is restored from a backup, you must update the warm standby configuration.

**Prerequisites**

You need the following information to update your warm standby configuration:

- Password for the Splunk Phantom user on the secondary Phantom instance. If the Splunk Phantom user does not have a password, you must set one.
- Password for the PostgreSQL database replication user.
- Configuration information for creating the SSL certificate:
  - Country code
  - State code
  - Organization
  - Organization unit
  - Domain
  - Email

**Restore a backup from a warm standby primary to the same Splunk Phantom instance**

When you restore a backup of a Phantom warm standby primary to the same instance, the warm standby configuration must be updated.

To update the warm standby configuration, perform the following steps:

1. Open a terminal session for both the primary and secondary Splunk Phantom instances. Keep these sessions open until you complete these steps.
   1. From the command line, SSH to your primary Splunk Phantom instance.
      
      SSH <username>@<primary_phantom_hostname>
   2. SSH to your secondary and warm standby Splunk Phantom instance.
      
      SSH <username>@<warm_standby_phantom_hostname>
   3. In both sessions, elevate to root.
      
      sudo su -
2. On the primary instance of Splunk Phantom, perform the restore. See Restore Splunk Phantom from a backup.
3. On the primary instance of Splunk Phantom, disable warm standby.
   
   phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --primary-mode --off
4. On the secondary instance of Splunk Phantom, disable warm standby.
   
   phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --standby-mode --off
5. On the secondary instance of Splunk Phantom, stop all Splunk Phantom services.
   
   /<PHANTOM_HOME>/phantom/bin/stop_phantom.sh
Failing to stop Phantom services on the secondary instance results in two active Splunk Phantom instances operating independently, polling for data and executing automated actions. This can result in data loss or other undesired results.

6. On the primary instance of Splunk Phantom, configure it to be the primary instance for warm standby. You are prompted to give passwords for the Splunk Phantom user, the PostgreSQL database replication user, and the information for creating a self-signed SSL certificate.

   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --primary-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

7. On the secondary instance, configure it to be the warm standby instance.

   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --standby-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

8. On the both instances of Splunk Phantom, verify that warm standby is replicating on each Splunk Phantom instance.

   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --status`

Example output from Splunk Phantom primary:

```
---------- Processed Params ----------
Instance looks like Primary
   DB replication configured with Standby set to:  <warm_standby_ip>/32
   DB replication currently streaming
   Vault sync configured
---------- Script Done ----------
```

Example output from Phantom secondary or warm standby:

```
---------- Processed Params ----------
Instance looks like Standby
   DB replication configured
   rsync configured
---------- Script Done ----------
```

**Restore a backup from a warm standby primary to a new Phantom instance**

When you restore a backup of a Splunk Phantom warm standby primary to a new instance that you want to become the new primary, you must update the warm standby configuration and move several keys to the secondary instance.

To update the warm standby configuration, perform the following steps:

1. Open a terminal session for both the primary and secondary Splunk Phantom instances. Keep these sessions open until you complete these steps.
   1. From the command line, SSH to your primary Splunk Phantom instance.
      `SSH <username>@<primary_phantom_hostname>
   2. SSH to your secondary and warm standby Splunk Phantom instance.
      `SSH <username>@<warm_standby_phantom_hostname>
   3. In both sessions, elevate to root.
      `sudo su -

2. On the primary instance of Splunk Phantom, perform the restore. See Restore Splunk Phantom from a backup.

3. On the primary instance of Splunk Phantom, disable warm standby.

   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --primary-mode --off`

4. On the secondary instance of Splunk Phantom, disable warm standby.

   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --standby-mode --off`
5. On the secondary instance of Splunk Phantom, stop all Splunk Phantom services.
   
   `/<PHANTOM_HOME>/phantom/bin/stop_phantom.sh`

   Failing to stop Splunk Phantom services on the secondary instance results in two active Splunk Phantom instances operating independently, polling for data and executing automated actions. This can result in data loss or other undesired results.

6. Copy these files from the new primary instance of Splunk Phantom to the secondary:
   1. `/<PHANTOM_HOME>/phantom/keystore/private_key.pem`
   2. `/<PHANTOM_HOME>/phantom/www/phantom_ui/secret_key.py`
   3. `/<PHANTOM_HOME>/phantom/www/phantom_ui/secret_key.pyc`

7. On the secondary instance of Splunk Phantom, set the permissions, ownership, and SELinux security contexts for the files you copied to the secondary.
   1. `chmod 0640 /<PHANTOM_HOME>/phantom/keystore/private_key.pem`
   2. `chown root:phantom /<PHANTOM_HOME>/phantom/keystore/private_key.pem`
   3. `chown phantom:phantom /<PHANTOM_HOME>/phantom/www/phantom_ui/secret_key.py[c]`
   4. `restorecon /<PHANTOM_HOME>/phantom/keystore/private_key.pem`
   5. `restorecon /<PHANTOM_HOME>/phantom/www/phantom_ui/secret_key.py[c]`

8. On the primary instance of Splunk Phantom, configure it to be the primary for warm standby. You are prompted to give passwords for the Splunk Phantom user, the PostgreSQL database replication user, and the information for creating a self-signed SSL certificate.
   
   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --primary-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

9. On the secondary instance, configure it to be the warm standby instance.
   
   `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --standby-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

10. On both instances of Splunk Phantom, verify that the warm standby instance is replicating on each Phantom instance.

    `phenv python /<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc --status`

Example output from Phantom primary:

```
------- Processed Params -------
Instance looks like Primary
DB replication configured with Standby set to:  <warm_standby_ip>/32
DB replication currently streaming
Vault sync configured
------- Script Done -------
```

Example output from Phantom secondary or warm standby:

```
------- Processed Params -------
Instance looks like Standby
DB replication configured
rsync configured
------- Script Done -------
```
Create and manage a warm standby

Warm standby feature overview

Warm standby is a strategy for high availability that regularly copies data from a primary instance of Splunk Phantom to a secondary instance. In the event of a failure on the primary, a systems administrator can quickly put the secondary into service as a new primary with minimal downtime or data loss.

Splunk Phantom's warm standby is implemented using PostgreSQL's streaming replication for the internal database and cron-based rsync of file system directories.

Warm standby is not a substitute for regular backups or other disaster recovery preparations.

Supported configurations

Splunk Phantom systems administrators can configure two identical, standalone Splunk Phantom instances to use the warm standby strategy.

- Only individual, standalone Splunk Phantom instances can be configured to use warm standby.
- Splunk Phantom instances with an external PostgreSQL database cannot use warm standby.
- Splunk Phantom clusters cannot use warm standby.

How to check the status of warm standby

You may need to check the status of warm standby before performing other actions, such as maintenance, upgrades, or troubleshooting. Splunk Phantom provides a command for checking the current status of warm standby.

To check the status of warm standby use the following command at the shell prompt.

**Privileged instance**

```
phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --status
```

**Unprivileged instance**

```
phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --status
```

The output will tell you which state your warm standby configuration is in.

**Warm standby is not configured on the instance**

```
------- Processed Params -------
  Warm Standby not yet configured
------- Script Done -------
```

**Warm standby is configured as the primary and operating normally on the instance**

```
------- Processed Params -------
  Instance looks like Primary
  DB replication configured with Standby set to: <warm_standby_ip>/32
  DB replication currently streaming
```

81
Warm standby is configured as the secondary and operating normally on the instance

---------- Processed Params ----------
Instance looks like Standby
DB replication configured
rsync configured
---------- Script Done ----------

IP addresses

Communication between the primary Splunk Phantom instance and the warm standby instance is handled using IP addresses, not hostnames. If the IP address changes for either instance, you must reestablish the warm standby pairing. See Create a warm standby.

PostgreSQL streaming replication

PostgreSQL streams data from its Write Ahead Log (WAL) from the primary database to the secondary database. This keeps the secondary synchronized with the primary database. See Streaming Replication on the PostgreSQL documentation site.

If network communication between the primary and secondary databases fails for any significant period of time, the WAL segments needed to update the secondary may have already been recycled by the primary. If this happens, you will need to recreate the warm standby relationship with the primary.

If your Splunk Phantom instances process high volumes of events or there is significant latency between the primary and the warm standby instance of Splunk Phantom, consider increasing the value of wal_keep_segments in pg_hba.conf to a value large enough to prevent the primary from recycling WAL segments too quickly for your environment. This will use additional disk space on the primary Splunk Phantom instance, but can increase the reliability of the database synchronization.

Rsync

Rsync is used to synchronize file system data between the primary Splunk Phantom instance and the warm standby. When the setup_warm_standby.pyc script is run to set up warm standby, a cron job is created to run rsync to keep the warm standby up to date with the primary.

What is synchronized between the primary and the warm standby

File system directories synced from the primary to the warm standby.

<table>
<thead>
<tr>
<th>Item to be synced</th>
<th>Directory or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL database</td>
<td>Synchronized using PostgreSQL streaming replication.</td>
</tr>
<tr>
<td>Files or Vault</td>
<td>&lt;$PHANTOM_HOME&gt;/vault</td>
</tr>
<tr>
<td>Certificates and system files</td>
<td>&lt;$PHANTOM_HOME&gt;/etc</td>
</tr>
<tr>
<td>Playbooks</td>
<td>&lt;$PHANTOM_HOME&gt;/scm/git/</td>
</tr>
<tr>
<td>App states</td>
<td>&lt;$PHANTOM_HOME&gt;/local_data/app_states</td>
</tr>
</tbody>
</table>
### Item to be synced

<table>
<thead>
<tr>
<th>Item to be synced</th>
<th>Directory or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Playbook data state</td>
<td><code>&lt;PHANTOM_HOME&gt;/tmp</code></td>
</tr>
<tr>
<td>SSL keys and certificates</td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/ssl</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;PHANTOM_HOME&gt;/etc/ssl/certs</code></td>
</tr>
<tr>
<td>Reports</td>
<td><code>&lt;PHANTOM_HOME&gt;/vault/reports</code></td>
</tr>
<tr>
<td>SAML configuration</td>
<td><code>&lt;PHANTOM_HOME&gt;/www/phantom_ui/auth_backends/saml2_xml</code></td>
</tr>
</tbody>
</table>

PIP and RPM packages are also synchronized. You can disable syncing PIP and RPM packages by using the `--ignore-package-updates` option with `setup_warm_standby.pyc`.

### Relevant log files

Each of these log files can be useful when troubleshooting or maintaining your warm standby configuration.

<table>
<thead>
<tr>
<th>Log file name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setup and command output</strong></td>
<td></td>
</tr>
<tr>
<td>warm_standby.log</td>
<td><code>/var/log/phantom/warm_standby.log</code></td>
</tr>
<tr>
<td><strong>RSYNC state logs</strong></td>
<td></td>
</tr>
<tr>
<td>rsync_opt.log</td>
<td><code>/var/log/phantom/rsync_opt.log</code></td>
</tr>
<tr>
<td>rsync_vault.log</td>
<td><code>/var/log/phantom/rsync_vault.log</code></td>
</tr>
<tr>
<td>rsync_app.states.log</td>
<td><code>/var/log/phantom/rsync_app_states.log</code></td>
</tr>
<tr>
<td>rsync_etc_ssl_certs</td>
<td><code>/var/log/phantom/rsync_etc_ssl_certs</code></td>
</tr>
<tr>
<td>rsync_playbooks.log</td>
<td><code>/var/log/phantom/rsync_playbooks.log</code></td>
</tr>
<tr>
<td>rsync_reports.log</td>
<td><code>/var/log/phantom/rsync_reports.log</code></td>
</tr>
<tr>
<td>rsync_pip_req.log</td>
<td><code>/var/log/phantom/rsync_pip_req.log</code></td>
</tr>
<tr>
<td>rsync_rpm_req.log</td>
<td><code>/var/log/phantom/rsync_rpm_req.log</code></td>
</tr>
<tr>
<td><strong>Package installation logs</strong></td>
<td></td>
</tr>
<tr>
<td>rpm_packages_primary.txt</td>
<td><code>/var/log/phantom/rpm_packages_primary.txt</code></td>
</tr>
<tr>
<td>pip_packages_primary.txt</td>
<td><code>/var/log/phantom/pip_packages_primary.txt</code></td>
</tr>
</tbody>
</table>

### Create a warm standby

You will need two identical instances of Splunk Phantom, one to serve as your primary Splunk Phantom instance, and the second to serve as the warm standby.

Do these steps to create your warm standby.

1. Complete the prerequisites.
2. Create a second Splunk Phantom instance to be the warm standby.
3. Setup SSH access between the primary Splunk Phantom instance and the new warm standby.
4. Configure warm standby using the `setup_warm_standby.pyc` script.
Prerequisites

There are some tasks that need to be completed before you can set up warm standby.

1. Create a full backup or a virtual machine snapshot of the Splunk Phantom instance that will be your primary.
2. Create a DNS A record for a hostname for your Splunk Phantom instance. You may need to work with other teams who manage DNS to accomplish this. Establish an appropriate Time To Live (TTL) value for this record since you will update the DNS A record in the event of a failover.
3. Set the Base URL for Phantom Appliance with the the hostname from the DNS A record in Main Menu > Administration > Company Settings. Example: https://phantom.example.com
4. Open the following ports on the primary Splunk Phantom instance's firewall TCP 22 for SSH, TCP 443 (HTTPS), and TCP 5432 for PostgreSQL operations.
5. Set up SSH between the primary Splunk Phantom instance and the warm standby.

Create a second Splunk Phantom instance to be the warm standby

You can either:

- clone the virtual machine that is your primary Splunk Phantom instance, or
- create an entirely new instance of Splunk Phantom to serve as the warm standby.

Create a Clone of your primary Splunk Phantom instance

You can create a clone of your primary Splunk Phantom instance. This clone will serve as the warm standby.

Consult the documentation for your virtualization software or the operating system software for how to clone and deploy the cloned instance of Splunk Phantom.

Your clone will need to have its own IP and MAC addresses.

Before you clone the Splunk Phantom instance check to see if it is already being used as part of a warm standby pair. If the instance is part of a warm standby pairing, warm standby must be disabled before cloning the instance. See Disable warm standby.

1. Clone your Splunk Phantom instance as described by your virtualization or operating system documentation.
2. Change the MAC and IP addresses for the new clone copy of Splunk Phantom.
3. On the clone copy of Splunk Phantom, set a password for the phantom user account. This password will be used later during configuration.
   passwd phantom
4. On the clone of Splunk Phantom, disable cron to prevent any jobs from making changes during setup and configuration.
   sudo systemctl stop crond.service

Create a new Splunk Phantom instance

If using a clone of your primary Splunk Phantom instance is not feasible or is otherwise unwanted, you can install a new instance of Splunk Phantom to serve as your warm standby.

1. Install Splunk Phantom. See How can Splunk Phantom be installed? in Install and Upgrade Splunk Phantom.
2. SSH to your warm standby Splunk Phantom instance.
   SSH <username>@<warm_standby_phantom_hostname>
3. Stop Splunk Phantom services on the standby.
   `sudo /<PHANTOM_HOME>/bin/stop_phantom.sh`

4. Copy these files from the primary instance of Splunk Phantom to the new warm standby instance.
   1. `/<PHANTOM_HOME>/keystore/private_key.pem`
   2. `/<PHANTOM_HOME>/www/phantom_ui/secret_key.py`
   3. `/<PHANTOM_HOME>/www/phantom_ui/secret_key.pyc`

5. On the warm standby instance of Splunk Phantom, set the permissions, ownership, and SELinux security contexts for the files you copied to it.
   1. `chmod 0640 /<PHANTOM_HOME>/keystore/private_key.pem`
   2. `chmod 0640 /<PHANTOM_HOME>/www/phantom_ui/secret_key.py`
   3. `chmod 0640 /<PHANTOM_HOME>/www/phantom_ui/secret_key.pyc`
   4. `chown root:phantom /<PHANTOM_HOME>/keystore/private_key.pem`
   5. `chown root:phantom /<PHANTOM_HOME>/www/phantom_ui/secret_key.py`
   6. `chown root:phantom /<PHANTOM_HOME>/www/phantom_ui/secret_key.pyc`
   7. `restorecon /<PHANTOM_HOME>/keystore/private_key.pem`
   8. `restorecon /<PHANTOM_HOME>/www/phantom_ui/secret_key.py`
   9. `restorecon /<PHANTOM_HOME>/www/phantom_ui/secret_key.pyc`

6. On the new warm standby instance of Splunk Phantom, set a password for the phantom user account. This password will be used later during configuration.
   `passwd phantom`

7. On the new warm standby instance of Splunk Phantom, disable cron to prevent any jobs from making changes during setup and configuration.
   `sudo systemctl stop crond.service`

If you have installed and configured CyberArk AIM on your Splunk Phantom primary, you will need to install and configure CyberArk AIM on your warm standby.

**Setup SSH between the primary and the new warm standby**

During setup the primary instance of Splunk Phantom will need to connect to the warm standby instance of Splunk Phantom using SSH.

If password authentication is disabled, it must be enabled in order to proceed and can be disabled once set up is complete.

**Configure warm standby using the setup_warm_standby.pyc script**

Once both your primary and warm standby instances are ready, you can configure warm standby using the `setup_warm_standby.pyc` script.

If you do not know if one or both of the instances are already part of a warm standby configuration, check warm standby status before proceeding. See How to check the status of warm standby in the Warm standby feature overview.

Warm standby must be disabled before reconfiguring warm standby to use different Splunk Phantom instances. See Disable warm standby.

Do these steps as either the root user or a user with sudo permissions.

1. On the primary Splunk Phantom instance, run the `setup_warm_standby.pyc` script.
   `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --configure --primary-ip <IP address of the primary> --standby-ip <IP address of the warm standby>`
   You will be prompted for:
   - The password for the user account phantom on the warm standby. This password was set when the warm standby instance was created earlier.
A password for the database replication user. This password will be used to configure the PostgreSQL database to use replication.

Configuration information to create the SSL certificate file used for communication between the primary and warm standby Splunk Phantom instances.

**Example:**
- Country Code: US
- State Code: CA
- City: Palo Alto
- Organization: Example
- Organization Unit: Security
- Domain: phantom.soc.example.com
- Email: soc@example.com

2. On the warm standby Splunk Phantom instance, run the setup_warm_standby.pyc script.
   ```python
   phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --configure --primary-ip <IP address of the primary> --standby-ip <IP address of the warm standby>
   ```

3. On the warm standby reenable the cron service.
   ```bash
   sudo systemctl start crond.service
   ```

**Failover to the warm standby**

Failing over to the warm standby is a manual process.

- You can failover to the warm standby in the event of a systems failure with the primary instance of Splunk Phantom.
- You may wish to failover even if the primary instance of Splunk Phantom is healthy in order to perform system maintenance or upgrades without significant downtime.

**Failover procedure**

Do these steps as the root user or a user with sudo permissions.

1. If the primary instance of Splunk Phantom is online, you must stop all Splunk Phantom services. The warm standby will not take over if it detects that the primary instance is still operating.
   ```bash
   /<PHANTOM_HOME>/bin/stop_phantom.sh
   ```

2. SSH to your warm standby Splunk Phantom instance.
   ```bash
   SSH <username>@<warm_standby_phantom_hostname>
   ```

3. Run the setup_warm_standby.pyc script to convert the standby to the primary.
   On Splunk Phantom instances version 4.6.19142 or newer:
   ```python
   phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --convert-to-primary --ignore-package-updates
   ```
   On Splunk Phantom instances version 4.6.18265 or earlier:
   ```python
   phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --convert-to-primary
   ```

4. Update DNS to resolve the hostname of your Splunk Phantom instance to the IP address of the new primary.

5. If you are ingesting from external services, you will need to update their configurations to use the new primary. Elasticsearch users will need to manually reindex in **Main Menu > Administration > Administration Settings > Search Settings**.

After the failover procedure, the warm standby is now the primary instance of Splunk Phantom. The previous primary should be offline.
Do not reboot or restart Splunk Phantom services on the decommissioned primary. It can lead to two standalone instances of Splunk Phantom polling the same assets, and lead to data loss or other unwanted behavior.

**Disable warm standby**

Warm standby must be disabled in order to:

- perform systems maintenance
- set up back up or perform a restore
- upgrade Splunk Phantom

If warm standby is disabled, you will need to reconfigure warm standby from the beginning.

**Disable warm standby procedure**

Do these steps as either the root user or a user with sudo permissions.

**On the Splunk Phantom primary**

1. Turn off warm standby.
   ```
   phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --off
   ```

**On the warm standby**

1. Turn off warm standby.
   ```
   phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --off
   ```
2. Stop all Splunk Phantom services.
   ```
   /<PHANTOM_HOME>/bin/stop_phantom.sh
   ```

Warm standby will be disabled, and the cron jobs removed to prevent the rsync jobs from running.

**Recreate warm standby after a failover**

After a failover, the previous warm standby is now a standalone primary instance of Splunk Phantom and the previous primary is offline or otherwise unavailable. A Splunk Phantom administrator can reconfigure these two instances into a new warm standby pair.

For the rest of this topic the two Splunk Phantom instances will be referred to as either instance A or instance B.

Instance A

The original primary Splunk Phantom instance.

Instance B

The original warm standby instance of Splunk Phantom.

**Configure instance B as the primary and instance A as the warm standby**

This is the easiest way to reconfigure the instances for warm standby after a failover.
The initial states for your instances must be:

- Instance A, the original primary is online but Splunk Phantom services are not running.
- Instance B, the former warm standby is now a stand alone Splunk Phantom instance.

If the Splunk Phantom instances are not in these states, stop. Evaluate if another option is more appropriate for your needs.

Do these steps as either the root user or a user with sudo permissions.

1. SSH to instance A.
   SSH <username>@<instance_A_hostname>
   1. Start PostgreSQL.
      `/<PHANTOM_HOME>/bin/phsvc start postgresql-9.4`
   2. Start pgbouncer.
      `/<PHANTOM_HOME>/bin/phsvc start pgbouncer`
   3. Turn off primary mode
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --off`

2. SSH to instance B.
   SSH <username>@<instance_B_hostname>
   1. Configure instance B as the new primary.
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

3. SSH to instance A.
   SSH <username>@<instance_A_hostname>
   1. Configure instance A as the new warm standby.
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

Now the two instances are configured for warm standby. Instance B is now the primary and instance A is now the warm standby.

**Configure instance A as the primary and instance B as the warm standby**

This option returns the instances to the same roles they served before the failover. This can be done after you have configured the instance B as the primary using the steps in the earlier section.

Each time warm standby is configured the database on the standby instance is erased and the entire Splunk Phantom PostgreSQL database has to be streamed from the primary.

The initial states for your instances must be:

- Instance B, the former warm standby is now a stand alone Splunk Phantom instance. All Splunk Phantom services are running.
- Instance A, the original primary is configured as the warm standby. All Splunk Phantom services are running.

If the Splunk Phantom instances are not in these states, stop. Evaluate if another option is more appropriate for your needs.

1. SSH to instance B.
   SSH <username>@<instance_B_hostname>
1. Stop Splunk Phantom services.
   `/<PHANTOM_HOME>/bin/stop_phantom.sh`

2. SSH to instance A.
   SSH `<username>@<instance_A_hostname>

   1. Configure instance A as the primary.
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --convert-to-primary`
      Warm standby is disabled. Instance A is a standalone Splunk Phantom instance, while instance B is idle and all Splunk Phantom services have been shut down.

      If the Splunk Phantom instances are not in the described states, stop. Check for and do any steps which have been missed before proceeding.

3. SSH to instance B.
   SSH `<username>@<instance_B_hostname>

   1. Start PostgreSQL.
      `/<PHANTOM_HOME>/bin/phsvc start postgresql-9.4`
   2. Start pgbouncer.
      `/<PHANTOM_HOME>/bin/phsvc start pgbouncer`
   3. Turn off primary mode
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --off`

4. SSH to instance A.
   SSH `<username>@<instance_A_hostname>

   1. Configure instance A as primary.
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --primary-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

5. SSH to instance B.
   SSH `<username>@<instance_B_hostname>

   1. Configure instance B as the warm standby.
      `phenv python2.7 /<PHANTOM_HOME>/bin/setup_warm_standby.pyc --standby-mode --configure --primary-ip <primary_ip> --standby-ip <standby_ip>`

Instance A and B are configured as a warm standby pair. Instance A is the primary, and instance B is the warm standby.

Upgrade or maintain warm standby instances

In order to perform system maintenance or to upgrade Splunk Phantom on a warm standby pair, warm standby must be disabled.

1. Disable warm standby on the primary.
2. Disable warm standby on the warm standby.
3. Perform system maintenance or upgrade Splunk Phantom for both instances. See Splunk Phantom upgrade overview and prerequisites in Install and Upgrade Splunk Phantom.
4. Create a warm standby pair. See Create a warm standby.

Warm standby tools

Use the `/<PHANTOM_HOME>/phantom/bin/setup_warm_standby.pyc` script to manage warm standby.
## Warm standby script arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Show this help message and exit.</td>
</tr>
<tr>
<td>--primary-mode</td>
<td>Run the instance as the primary in the warm standby pairing.</td>
</tr>
<tr>
<td>--standby-mode</td>
<td>Run the instance as the warm standby in the warm standby pairing.</td>
</tr>
<tr>
<td>--version</td>
<td>Show the program's version number and exit.</td>
</tr>
<tr>
<td>--status</td>
<td>Show the status of the current Splunk Phantom instance.</td>
</tr>
<tr>
<td>--configure</td>
<td>Configure warm standby. Additional arguments are required.</td>
</tr>
<tr>
<td>--off</td>
<td>Turn warm standby off on the current instance based on which mode the instance is in.</td>
</tr>
<tr>
<td>--convert-to-primary</td>
<td>Convert a standby to primary valid only in case of --standby-mode.</td>
</tr>
<tr>
<td>--primary-ip &lt;PRIMARY_IP&gt;</td>
<td>IP address of the primary.</td>
</tr>
<tr>
<td>--standby-ip &lt;STANDBY_IP&gt;</td>
<td>IP address of the warm standby.</td>
</tr>
<tr>
<td>-d, --ignore-database</td>
<td>Ignore the PostgreSQL database. Ignores the Postgres database during setup. Only backs up system files.</td>
</tr>
<tr>
<td>-t, --ignore-vault</td>
<td>Ignore vault. Ignores the vault from setup. Only backs up various contents from /&lt;PHANTOM_HOME&gt;/.</td>
</tr>
<tr>
<td>-l &lt;RECOVERY_DATABASE_LOCATION&gt;, --recovery-database-location &lt;RECOVERY_DATABASE_LOCATION&gt;</td>
<td>When setting up the standby, copy the original database to this location for recovery in the event of a script failure.</td>
</tr>
<tr>
<td>--primary-phantom-version &lt;PRIMARY_PHANTOM_VERSION&gt;</td>
<td>Version of the primary Splunk Phantom instance. Only valid for --standby-mode. If passed, validates against the current version.</td>
</tr>
<tr>
<td>-r &lt;REMOTE_USER&gt;, --remote-user &lt;REMOTE_USER&gt;</td>
<td>The username of the remote user.</td>
</tr>
<tr>
<td>-x, --relax-verification</td>
<td>Relax user verification requirements for non-root installations. Setting this option is not recommended.</td>
</tr>
<tr>
<td>-p &lt;SSH_PORT&gt;, --ssh-port &lt;SSH_PORT&gt;</td>
<td>Port used to be used by all SSH commands.</td>
</tr>
<tr>
<td>--no-modify-ciphers</td>
<td>Don't overwrite ssl_cipher in PostgreSQL configurations.</td>
</tr>
<tr>
<td>-u, --ignore-package-updates</td>
<td>Skip updating packages. Skips re-installing rpm and pip packages.</td>
</tr>
</tbody>
</table>
Configure your Splunk Phantom telemetry

Share data from Splunk Phantom

When Splunk Phantom is deployed, the platform sends anonymized usage data to Splunk Inc. (“Splunk”) to help improve Splunk Phantom in future releases. You can opt in or opt out of sharing telemetry data.

Enable telemetry by doing the following:

1. From the main menu, select Administration.
2. Expand the Product Settings drop-down list.
3. Click Telemetry.
4. Toggle the switch to the On position.
5. Click Confirm.

Disable telemetry by doing the following:

1. From the main menu, select Administration.
2. Expand the Product Settings drop-down list.
3. Click Telemetry.
4. Toggle the switch to the Off position.
5. Click Confirm.

How data is collected

Splunk Phantom uses Splunk Web Analytics (swa.js) to collect anonymous usage data. These analytics run in the background regardless of whether you opt in to sending usage data to Splunk. Collecting data affects the Splunk Phantom UI loading in a minimal way. Performance numbers are currently being gathered to compare with a baseline Splunk Phantom system with no telemetry.

What data is collected

Data is collected to measure metrics of the product, assess performance for optimizations, evaluate engagement for roadmaps, and discover client-side errors to inform UI fixes. The metrics do not contain any user-provided values such as username, email, or any URL parameters that are user or customer identifiable. Splunk Phantom collects the following basic usage information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app.session.session_start</td>
<td>Reports the browser and OS, along with their versions.</td>
<td>data: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app: UNKNOWN_APP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>browser: Chrome</td>
</tr>
<tr>
<td></td>
<td></td>
<td>browserVersion: 78.0.3904.97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>device: MacIntel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>locale: en-US</td>
</tr>
<tr>
<td></td>
<td></td>
<td>os: Mac OS X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>osVersion: 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>page: UNKNOWN_PAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>splunkVersion: not available</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app.session.phantom.pageview</td>
<td>Reports which pages are visited by users.</td>
<td>eventID: d9ca862c-d48d-83a1-d1bb-f0f25f4b5af8 experienceID: 6c2c534b-e750-e1a0-95fd-fcadala50be0 optInRequired: 3 timestamp: 1574213029 visibility: anonymous</td>
</tr>
<tr>
<td>app.session.phantom.error</td>
<td>Reports uncaught errors of front-end Splunk Phantom scripts.</td>
<td>data: { app: phantom errorMsg: Uncaught ReferenceError: helloworld is not defined file: /inc/swa/swa_enabled.js page: admin.company_settings.info phantomDeploymentID: phantom-a2a983de-38ec-42d7-a179-30087b0ca8ca phantomUserID: 5d900c28b8d1555745c09908ef386860 eventID: 0db11144-7c14-88f7-b3e9-3a999102bfc6 experienceID: 20d4d671-7d18-f74a-c72f-9811b5bee20d optInRequired: 3 timestamp: 1574210581565 visibility: anonymous</td>
</tr>
<tr>
<td>app.session.phantom.apiTime</td>
<td>Reports roundtrip time consumption for each API request.</td>
<td>data: { app: phantom endpoint: /rest/ph_user/3/permissions method: get page: UNKNOWN_PAGE status: 200 time: 150 phantomDeploymentID: phantom-a2a983de-38ec-42d7-a179-30087b0ca8ca phantomUserID: 5d900c28b8d1555745c09908ef386860 eventID: 94efce66-ab89-33ae-f894-1cceb8f68f78 experienceID: 239facf6-261d-dd96-be08-33870c7d3750 optInRequired: 3 timestamp: 1574294947704 visibility: anonymous</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>app.session.phantom.viewTime</td>
<td>Reports time spent on a specific page. Only tracked for specific pages.</td>
<td>timestamp: 1574213030362</td>
</tr>
<tr>
<td></td>
<td></td>
<td>visibility: anonymous</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app: phantom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>page: reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>viewTime: 10223</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantomDeploymentID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantom-a2a983de-38ec-42d7-a179-30087b0ca8ca</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantomUserID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5d900c28b8d1555745c09908ef386860</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eventID: 545fdcfb-ac06-a11b-da6a-4b9da84b6c2a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>experienceID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>85b49544-fb90-a2ef-1b3f-e09339f3abc1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>optInRequired: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timestamp: 1573690198763</td>
</tr>
<tr>
<td></td>
<td></td>
<td>visibility: anonymous</td>
</tr>
<tr>
<td>app.session.phantom.license</td>
<td>Reports license status, limits, and usage information. Sent once per session.</td>
<td>timestamp: 1575656115189</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app: phantom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>expirationDate: 1576800000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>issueDate: 1575504000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>limits: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>actions: 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>events: 75</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tenants: 250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>page: UNKNOWN_PAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>type: standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usage: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>recentAppRunCount: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>recentDebugRunCount: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>recentPlaybookRunCount: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantomDeploymentID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantom-a2a983de-38ec-42d7-a179-30087b0ca8ca</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phantomUserID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5d900c28b8d1555745c09908ef386860</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eventID: 5854bede-18d9-5a88-d023-e698dab1afaf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>experienceID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31a418cc-1371-c58a-a0b8-dc87638b126f</td>
</tr>
<tr>
<td></td>
<td></td>
<td>optInRequired: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timestamp: 1575656115189</td>
</tr>
<tr>
<td></td>
<td></td>
<td>visibility: anonymous</td>
</tr>
<tr>
<td>app.session.phantom.systemSettings</td>
<td>Reports the feature on/off settings and product version.</td>
<td>component: app.session.phantom.systemSettings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app: phantom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>isClusteringEnabled: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>isMultiTenantEnabled: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>numOfClusterNodes: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>page: UNKNOWN_PAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>productVersion: 10900.0.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nodeGUID: dca36837-3e10-4cbd-bf14-b49097b84347</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>searchConfig:</td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td>isElasticSearchEnabled: false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>searchLocation: local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>searchType: standalone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>phantomDeploymentID:</td>
<td>phantom-a2a983de-38ec-42d7-a179-30087b0ca8ca</td>
<td></td>
</tr>
<tr>
<td>phantomUserID:</td>
<td>5d900c28b8d1555745c09908ef38f6860</td>
<td></td>
</tr>
<tr>
<td>eventID:</td>
<td>d4b331e7-3ce3-91b6-7724-bc4d7235bca9</td>
<td></td>
</tr>
<tr>
<td>experienceID:</td>
<td>21febb16-c3f6-cbd5-ffac-905f1466c830</td>
<td></td>
</tr>
<tr>
<td>optInRequired:</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>timestamp:</td>
<td>1576695256840</td>
<td></td>
</tr>
<tr>
<td>visibility:</td>
<td>anonymous</td>
<td></td>
</tr>
</tbody>
</table>