Splunk® App for SOAR Export
Use the Splunk App for SOAR Export to Forward Events 4.1.117

Enable Splunk platform users to use the Splunk App for SOAR Export

Generated: 7/28/2022 1:18 am

Enable Splunk platform users to use the Splunk App for SOAR Export

The Splunk App for SOAR Export requires that specific roles are added for the Splunk user setting up the Splunk App for SOAR Export.

Add the phantom and ess_user roles to users on Splunk Enterprise 8.x

Perform the following steps to add the **phantom** and **ess_users** roles to the Splunk user setting up the Splunk App for SOAR Export in Splunk Enterprise 8.x environments:

1. Navigate to the Splunk platform instance where you installed the Splunk App for SOAR Export.
2. In Splunk Web, select **Settings > Roles**.
3. The **phantom** role includes Splunk Phantom read and write access and other permissions needed to run the Splunk App for SOAR Export. To set up Splunk Phantom capabilities, assign the **phantom** role to a user or a role. For example, if you want the **admin** role to have Splunk Phantom capabilities, do the following:
    1. Click **Edit** in the Actions column for the **admin** role.
    2. In the Inheritance tab, select the checkbox next to the **phantom** role. This will cause all users with the **admin** role to also inherit all privileges from the **phantom** role. If this admin user will be using adaptive response relay, you must also inherit the **ess_user** role.
4. Click **Save**.

Add the phantom and ess_users roles to users on Splunk Enterprise 7.3.x

Perform the following steps to add the **phantom** and **ess_users** roles to the Splunk user setting up the Splunk App for SOAR Export in Splunk Enterprise 7.3.x environments:

1. Navigate to the Splunk platform instance where you installed the Splunk App for SOAR Export.
2. In Splunk Web, select **Settings > Access controls**.
3. Select **Roles**.
4. The **phantom** role includes Splunk Phantom read and write access and other permissions needed to run the Splunk App for SOAR Export. To set up Splunk Phantom capabilities, assign the **phantom** role to a user or a role. For example, if you want the **admin** role to always have Splunk Phantom capabilities, do the following:
    1. Click **admin** to edit the role.
    2. Click the **Inheritance** tab.
    3. Select the checkbox next to the **phantom** role. This will cause all users with the **admin** role to also inherit all privileges from the **phantom** role. If this admin user will be using adaptive response relay, you must also inherit the **ess_user** role.
5. Click **Save**.

Add the phantom role to users on Splunk Cloud Platform

Splunk Cloud Platform users must file a support ticket in order to have Splunk update user roles on your behalf.