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

Connect the Splunk App for SOAR Export and the Splunk Platform to a Splunk SOAR server or Splunk SOAR

Generated: 7/14/2022 2:18 am

Connect the Splunk App for SOAR Export and the Splunk Platform to a Splunk SOAR server or Splunk SOAR

Configure a Splunk SOAR server so that the Splunk App for SOAR Export and the Splunk platform can connect to your Splunk Phantom or Splunk SOAR instance.

To configure a Splunk SOAR (On-premises) server, follow these steps:

1. Before you begin, make sure you have added the required roles to the admin user. See Enable Splunk platform users to use the Splunk App for SOAR Export.
2. (Optional) If you have not configured certificates for Splunk SOAR and the Splunk platform, you must disable HTTP validation on the Splunk Platform. Perform the following steps:
    1. Run the following command and provide the proper **username**, **password**, and **splunkaddress**: `curl -ku '<username>:<password>' https://<splunkaddress>:8089/servicesNS/nobody/phantom/configs/conf-phantom/verify_certs\?output_mode -d value=0`
    2. Return to the SOAR Server Configuration page and verify that the **HTTPS certificate verification is disabled** message appears with a warning icon.
3. Navigate to Splunk App for SOAR Export installed on your Splunk platform instance.
4. Click the **Configurations** tab.
5. Click **Create Server**.
6. To add a new server, use an authorization token from Splunk Phantom or Splunk SOAR. To get an authorization token, follow these steps:
    1. Navigate to your Splunk SOAR or Splunk SOAR instance.
    2. From the main menu, select **Administration**.
    3. Select **User Management > Users**.
    4. You can either use the default automation user and change the allowed IP addresses, or create a new automation user. In this example we will create a new automation user. Click **+ User** to create a new automation user.
    5. Update the **Allowed IPs** field to reflect the IP address or IP range for the Splunk platform instance.

        > Do not use any unless you are troubleshooting or testing.
    6. Click **Create** to create the user.
    7. On the Users page, click on the ellipsis (...) icon for the new automation user and click **Edit**.
    8. Copy the text in the **Authorization Configuration for REST API** box.
    9. Click **Save**.
7. Navigate back to the Splunk App for SOAR Export on your Splunk platform instance and paste the authorization token in the **Authorization Configuration** box. Verify that the format of the object looks like the following example:

    ```
    {
      "ph-auth-token": "*********",
      "server": "https://10.1.65.229"
    }
    ```
8. Enter an optional name for the server. This will show up later in Splunk Phantom or Splunk SOAR as your container name, so pick a name you can easily identify.
9. (Optional) Configure a Proxy server. For example:
    - An example HTTP proxy in the format `http://[<username>[:password]@]<host>[:<port>]`. For example: `http://172.31.225.254:8080`
    - An example HTTPS proxy in the format `https://[<username>[:password]@]<host>[:<port>]`. For example: `https://username:password@proxy.host.com:8080`

10. (Optional) Click **Optional: This server will be used for AR Relay** if this server will be used in an adaptive response relay configuration. See Use adaptive response relay to send notable events from Splunk ES to Splunk Phantom or Splunk SOAR.
11. Click **Save**. A page shows your new server. If you have multiple servers, they are listed on this page.
12. To test your server, click **Manage > Test Connectivity**. A success message appears if the server is working correctly.
13. (Optional) Click **Manage > Sync Playbooks** to further test connectivity and make sure that your playbooks are synchronized. See Synchronize the list of available Splunk Phantom or Splunk SOAR playbooks on your Splunk platform.

Do not click Enable debug logging unless directed to do so by Splunk support. Debug logging causes a heavy load on your server.

Synchronize the list of available Splunk Phantom or Splunk SOAR playbooks on your Splunk platform

You can run adaptive response action in Splunk Enterprise Security (ES) to send a notable event to Splunk Phantom or Splunk SOAR and also run a playbook on the resulting artifact. Perform the following tasks to make sure that the list of available playbooks is up to date in your Splunk platform. The list of playbooks is maintained in the `<SPLUNK_HOME>/etc/apps/phantom/local/phantom.conf` file.

1. Navigate to the Phantom App for Splunk installed on your Splunk platform.
2. Click the **Configurations** tab.
3. In the Actions column for the desired server, select **Manage > Sync playbooks**.

See Run adaptive response actions in Splunk ES to send notable events to Splunk Phantom or Splunk SOAR for more information about running adaptive response actions in Splunk ES.