MANAGE INTEGRATIONS

Use this document to manage integrations using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

MSI Integrations

This method is the preferred approach for configuring integrations in Security Validation.

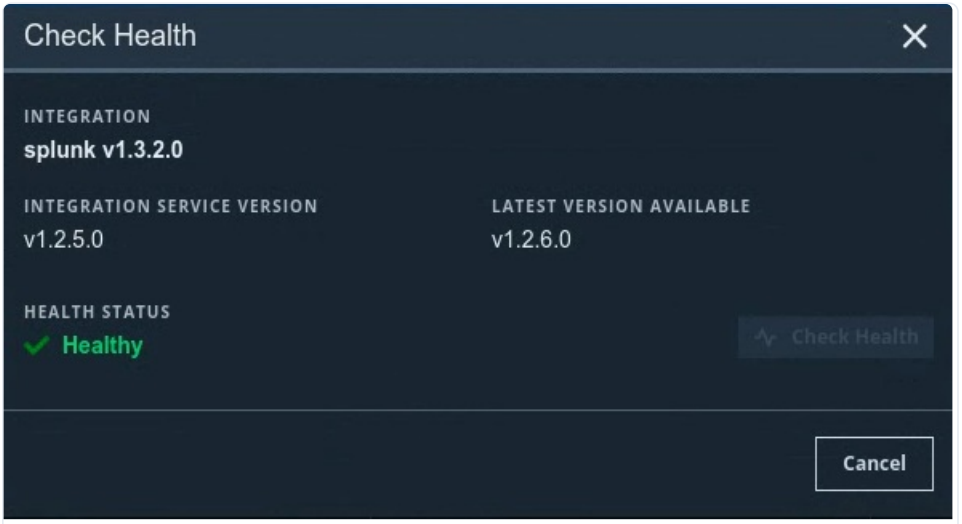
After you configure Direct and Remote Integrations with your security technologies, you can perform any of the following tasks:

- **Run a Health Check**
- **Test and Update Integration Queries**
- **Configure Variables**
- **Pause an Integration**
- **Edit an Integration**
- **Delete an Integration**
- **Check Operational Status**
- **Stop Integrations Service**
- **Restart Integrations Service**

Run a Health Check

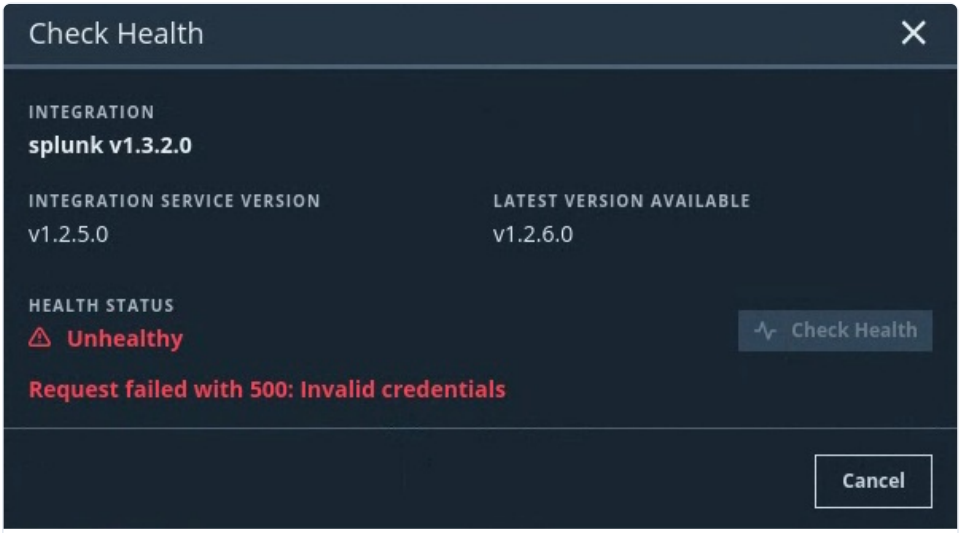
Using Health Check, you can validate that an integration action configuration can connect to the target technology and successfully authenticate.

1. Go to **Settings > Integrations**.
2. For the integration that you want to check, select ⋮ **more > Check Health**. The Health Check results appear.
   If no issues are detected with the connectivity to the security technology, a "Healthy" status appears, along with the integrated technology and information about the Integration Service version.



Healthy status for a Health Check

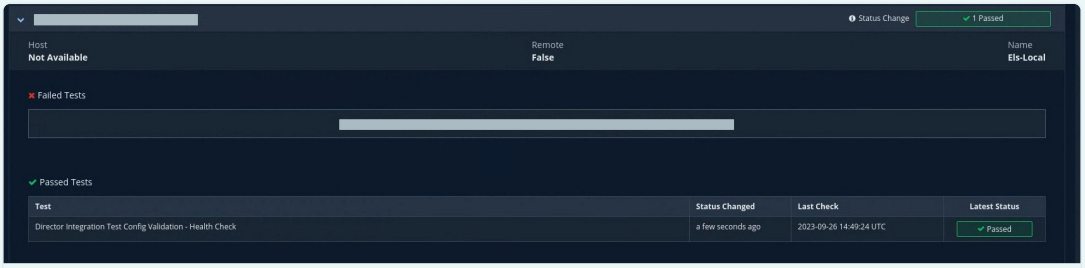
If an issue is detected, an "Unhealthy" status appears, along with an error message that identifies the problem.



Unhealthy status for a Health Check and example error message

3. (Optional) Click **Check Health** if you want to rerun the check. For example, if you remediated a connection issue, you can rerun the check to confirm the fix.

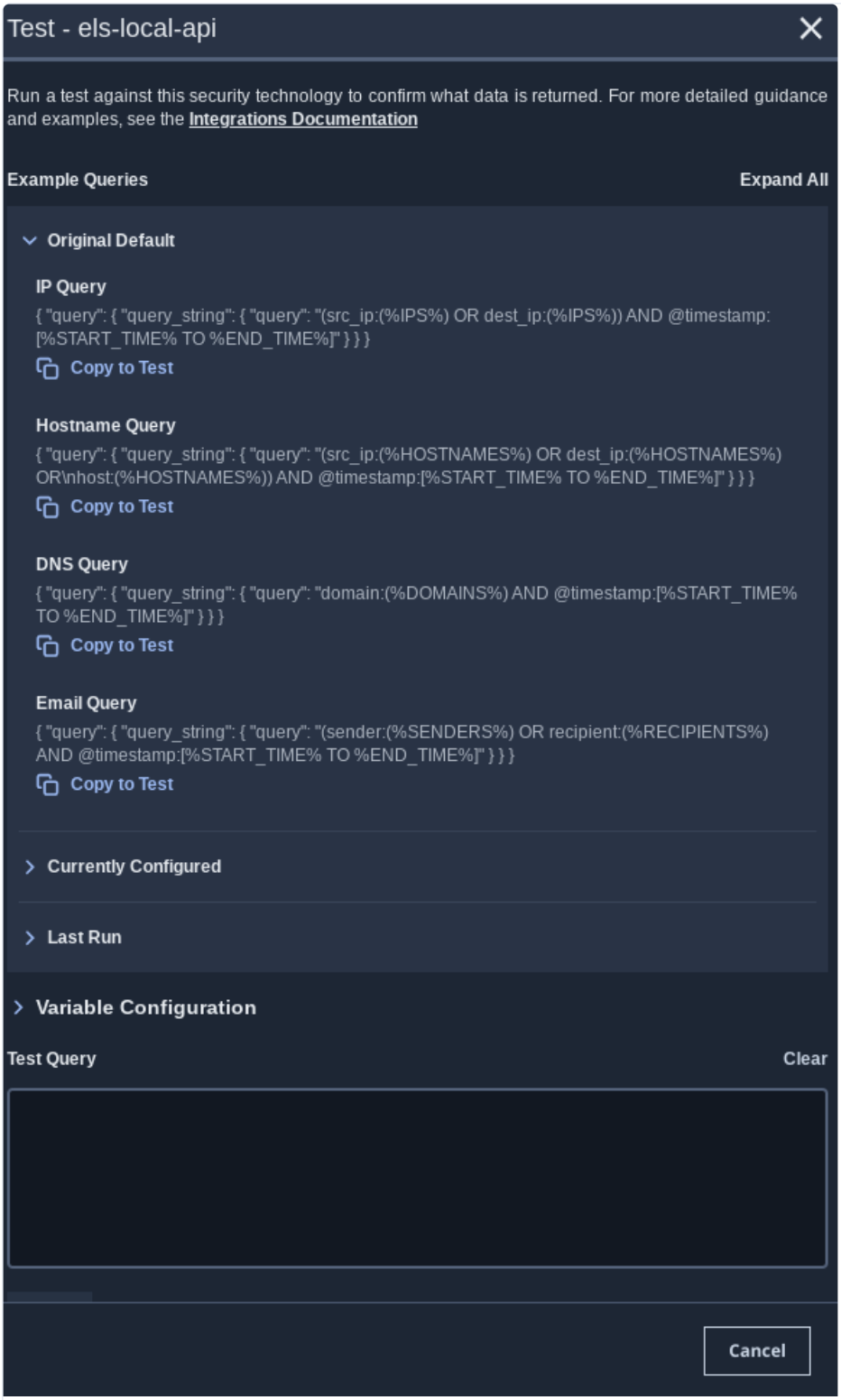
If you configure Integrations tests (**Settings > Director Settings > Operational Status**, as covered in **Check Operational Status**), then Health Check results appear on the **Environment > Operational Status** page.



Health Check results on the Operational Status page

Test and Update Integration Queries

1. Go to **Settings > Integrations**.
2. For the Integration you want to run a test query on, select ⋮ **more > Test**.
3. Click CHEVRON_RIGHT **expand** next to the preferred option:
   - **Original Default**: The Mandiant-provided default.
   - **Currently Configured**: The query that was specified when the integration was set up.
   - **Last Run**: A value only appears if you've already run a successful query.

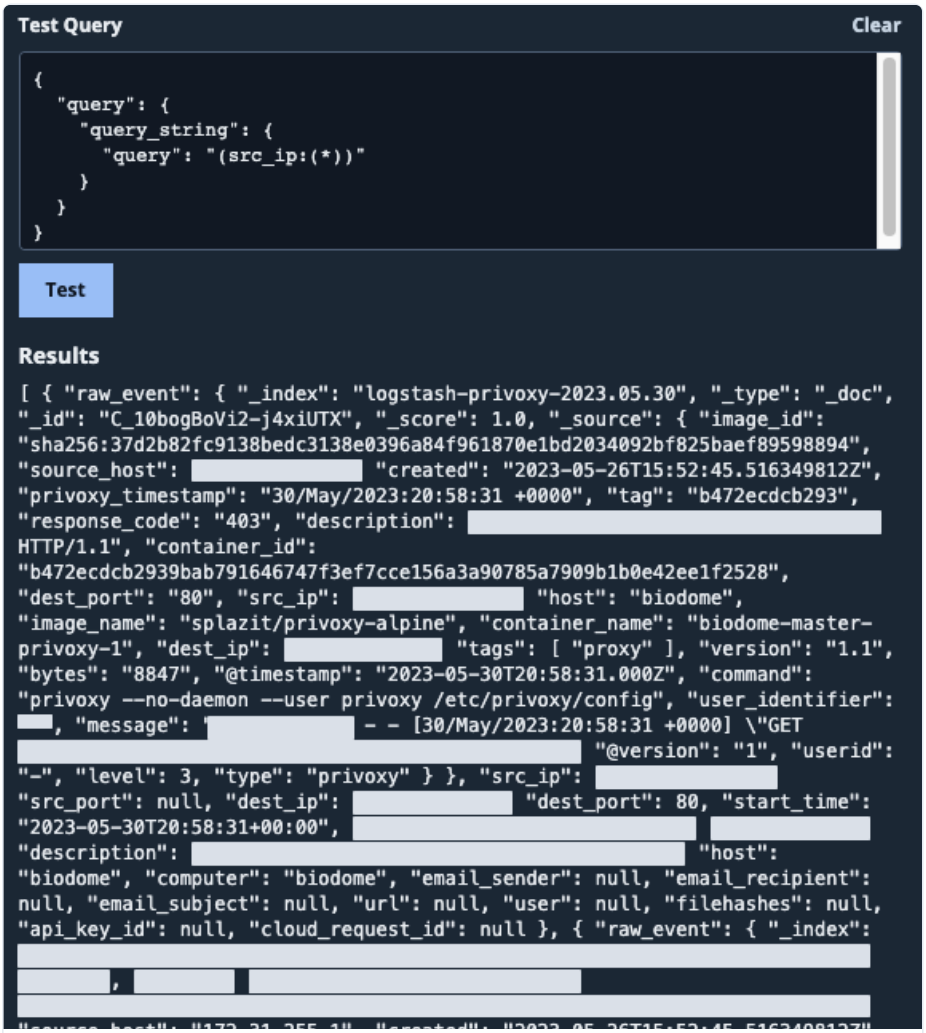


Test Query view for an existing Integration

4. Click **Copy to Test** for any available option and then paste the query into the **Test Query** field.

If you enter an incorrect value or would rather try a different query, you can click **Clear** to remove the current value and then start over.

5. Modify the variables (represented by % *VARIABLE_VALUE*%) as needed and click **Test**. The results of the query appear in the **Results** section.



Example of Test Query results

The next time you return to the **Test** option, the query that you last ran appears in the **Last Run** expandable section.

Configure Variables

Along with testing queries, you can configure values for variables to be passed to the technology.

Each technology may require different variables and may ignore values that are not needed.

1. Go to **Settings > Integrations**.
2. For the Integration that you want to configure variables for, select ⋮ **more > Test**.
3. Click **Variable Configuration** to expand the variable fields.

4. Specify a date and time range (UTC) for **Start Time (%START_TIME%)** and **End Time (%END_TIME%)**.
5. **Select an Actor** to add its hostname and IP(s), or manually enter them into the fields.
6. Specify User Accounts %USER_DOMAINS%, Email Recipients %RECIPIENTS%, and Email Senders %SENDERS%, as needed.
7. Enter the **Test Query** value and then click **Test**.

Pause an Integration

As a user with System Admin permissions, you can pause an active Integration and restart a paused Integration. The interface provides immediate feedback and changes status after each action.

1. Go to **Settings > Integrations**.
2. For the active Integration you want to pause, select ⋮ **more> Pause**. The status changes to **Pause** in the table.
3. (Optional) If you're ready to have the Integration running again, click ⋮ **more**again, then click **Restart**. The status changes back to **Active.**

Edit an Integration

1. Go to **Settings > Integrations**.
2. For the Integration you want to edit, select ⋮ **more ;>Edit**.
3. Make any required changes and then select **Save**.

> If you're unable to save, you might need to modify a required field first.

Delete an Integration

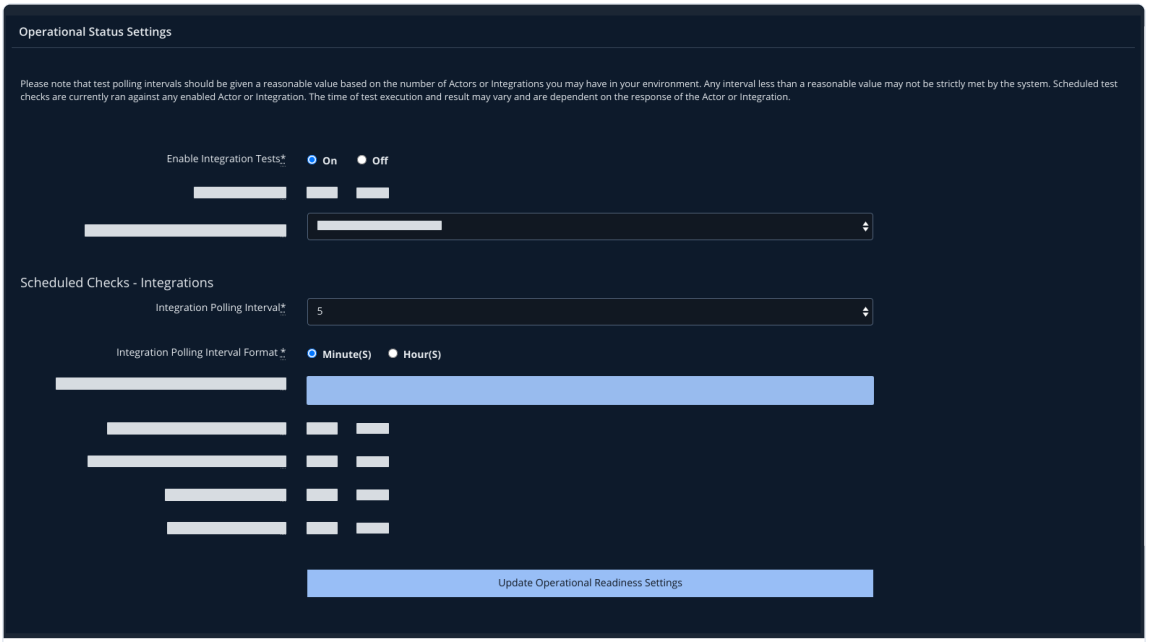
1. Go to **Settings > Integrations**.
2. For the Integration you want to delete, select ⋮ **more > Delete**.
3. Click **Delete** in the drop-down list. A message displays asking if you're sure you want to delete the Integration.
4. Click **OK** to delete the Integration. Click **Cancel** if you do not want to delete this Integration.

Check Operational Status

This feature verifies the overall status of the Integration on the basis of the last number of Integration query events and the Job match in a tabular form. To complete this task, perform steps in three different sections of the Director.

Enable Integration Tests and Polling Interval

1. Go to **Settings > Director Settings**.
2. Click **Operational Status** and turn on **Enable Integration Tests**.
3. Configure the following fields:
   - **Integration Polling Interval**
   - **Integration Polling Interval Format**
     For example, setting them to **5** and **minute(S)**, respectively, means that the test polling interval for integrations happen every five minutes.



Operational Status Settings

> The test polling intervals should be given a reasonable value based on the number of Actors or Integrations you have in your environment. Test execution time and results may vary and depend on the response of the Actor or Integration.

4. Click **Update Operational Reading Settings** to save your changes.

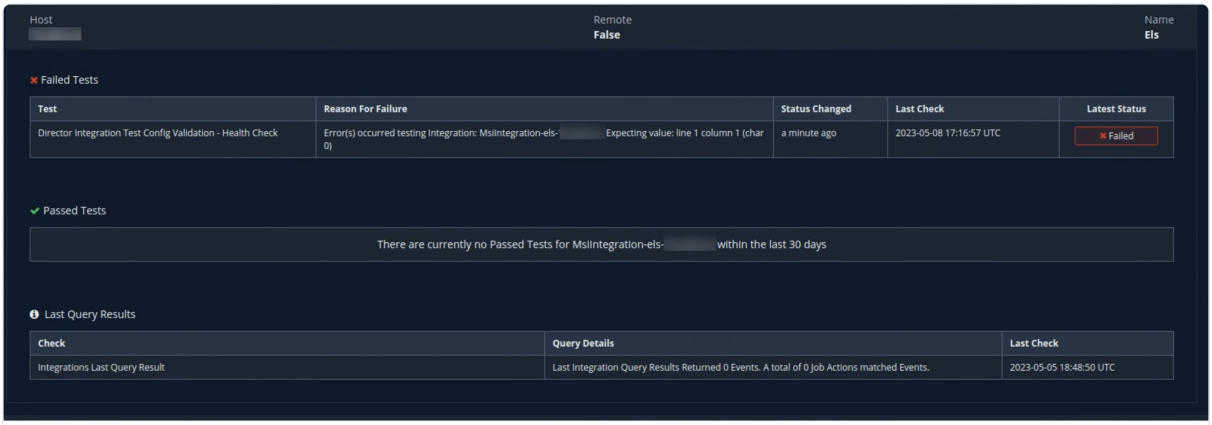
Configure an Integration

1. Go to **Settings** > **Integrations** and configure an Integration using the steps in the web interface, for example, ElasticSearch to retrieve matched events.
2. Verify that there is a Last Query configured for ElasticSearch.

Example of a Last Query for Elastic Search

Check Operational Status

1. Go to **Environment > Operational Status** and then click **Integrations**. You see the Last Query result details for the integration. When there are events, the table displays the matched events/Job Actions that were last detected.



Last Query Results

Stop Integrations Service

1. Go to **Settings > Director Settings**.
2. Select **Integrations**.
3. From the **Options** drop-down, select **Stop Service**.
4. Read the confirmation, and then select **STOP SERVICE**.

> When you're ready to start the service again, return to the same drop-down and select **Start Service**. Starting the service may take up to three minutes.

Restart Integrations Service

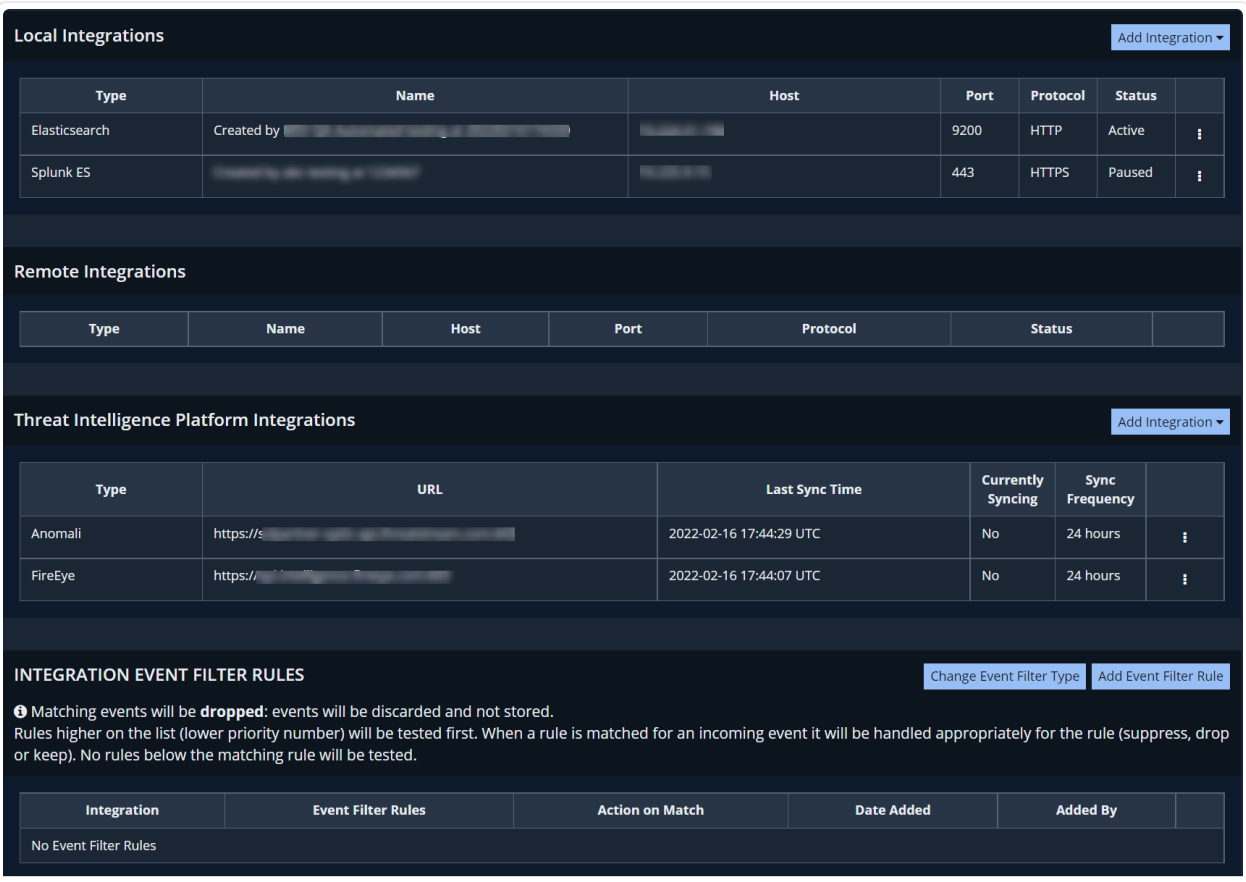
1. Go to **Settings > Director Settings**.
2. Select **Integrations**.
3. From the **Options** drop-down, select **Restart Service**.
4. Read the confirmation, and then select **Restart Service**. The **Service Status** changes to **Stopped** and changes back to **Running** when the restart is completed.

Legacy Integrations

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

Access the Legacy Integrations area of the platform by going to **Settings** > **Integrations** and scrolling to Legacy Integrations. Here you will see all Local and Remote Integrations that you have configured.

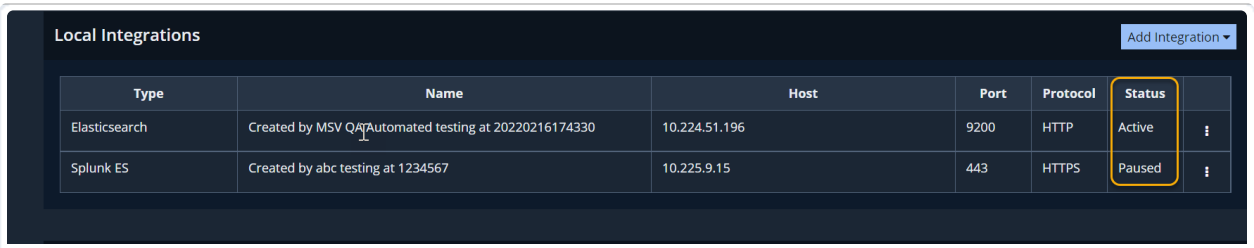
When configuring the integrations, you can assign a name, allowing for easier identification if you have the same integration in multiple areas of your environment. This name is also used in various areas of the platform, such as looking at Detected Events for a Job.



Integrations

Use the vertical ellipses in the last column of each table to manage your Integrations in the Integration manager.

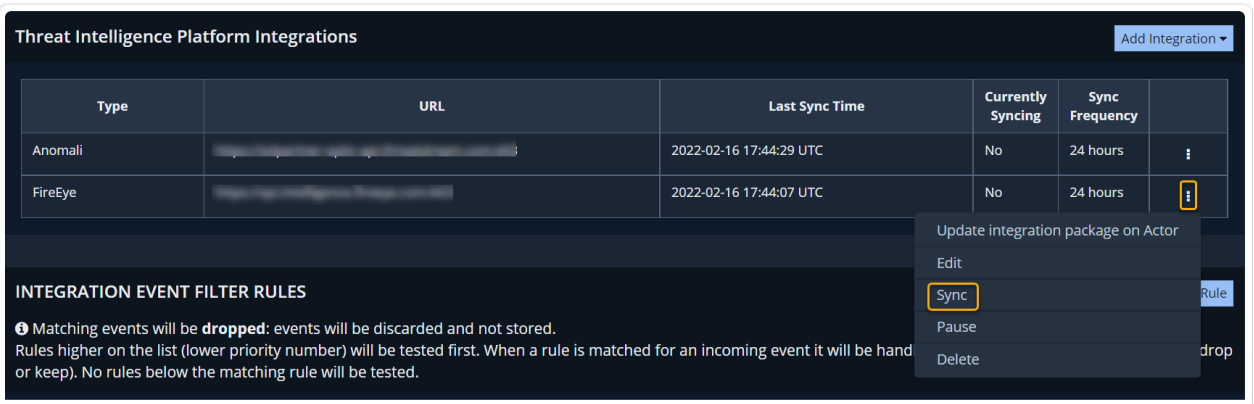
You can quickly see whether an integration is "Paused" or "Active" in the Status column of the Local Integrations table.



Status of Local Integrations

To sync an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to sync in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Sync** in the drop-down list.
5. Wait for the sync to complete.



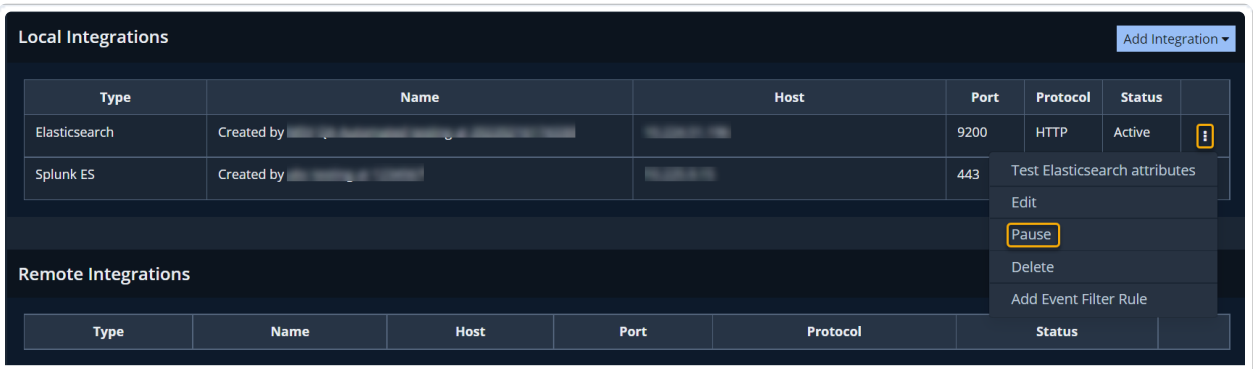
Syncing an Integration

Use the same process to update Cylance's device list.

To pause an integration

Pause an integration to prevent it from syncing but have it retain its information in our database.

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to pause in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Pause** in the drop-down list.

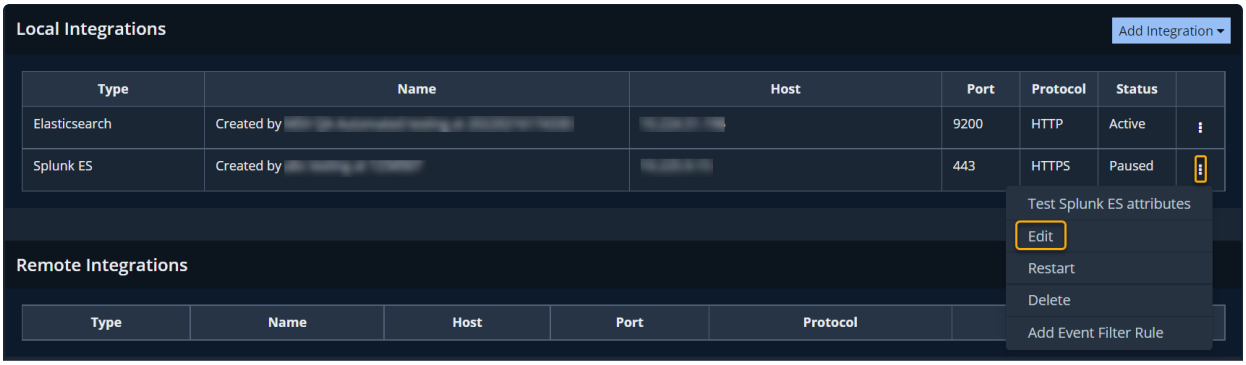


Pausing an Integration

When you are ready to have the integration running again, click the ellipses again; then click **Restart**.

To edit an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to edit in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Edit** in the drop-down list.
5. Make changes as needed and click **Submit**.

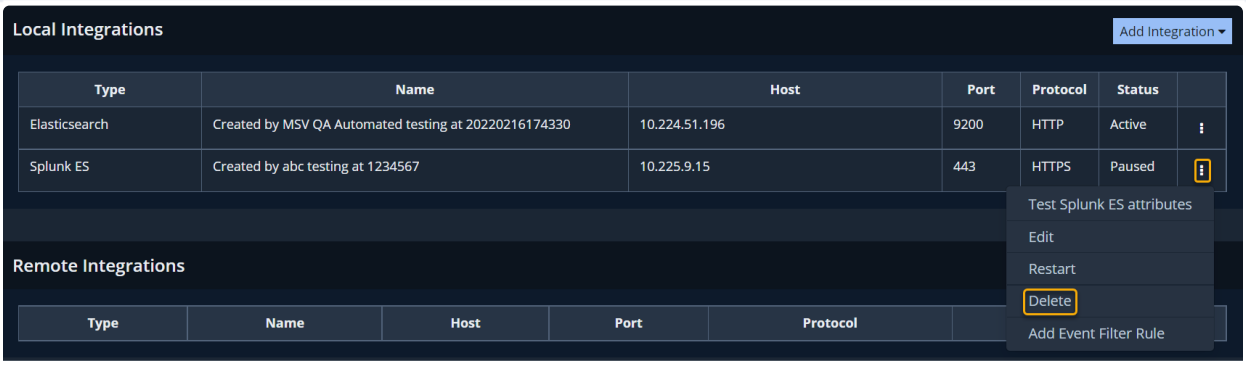


Editing an Integration

Use the Delete option to delete an integration that you no longer need.

To delete an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to delete in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Delete** in the drop-down list. A message displays asking if you are sure you want to delete the integration.
5. Click **OK** to delete the integration. Click **Cancel** if you do not want to delete this integration.

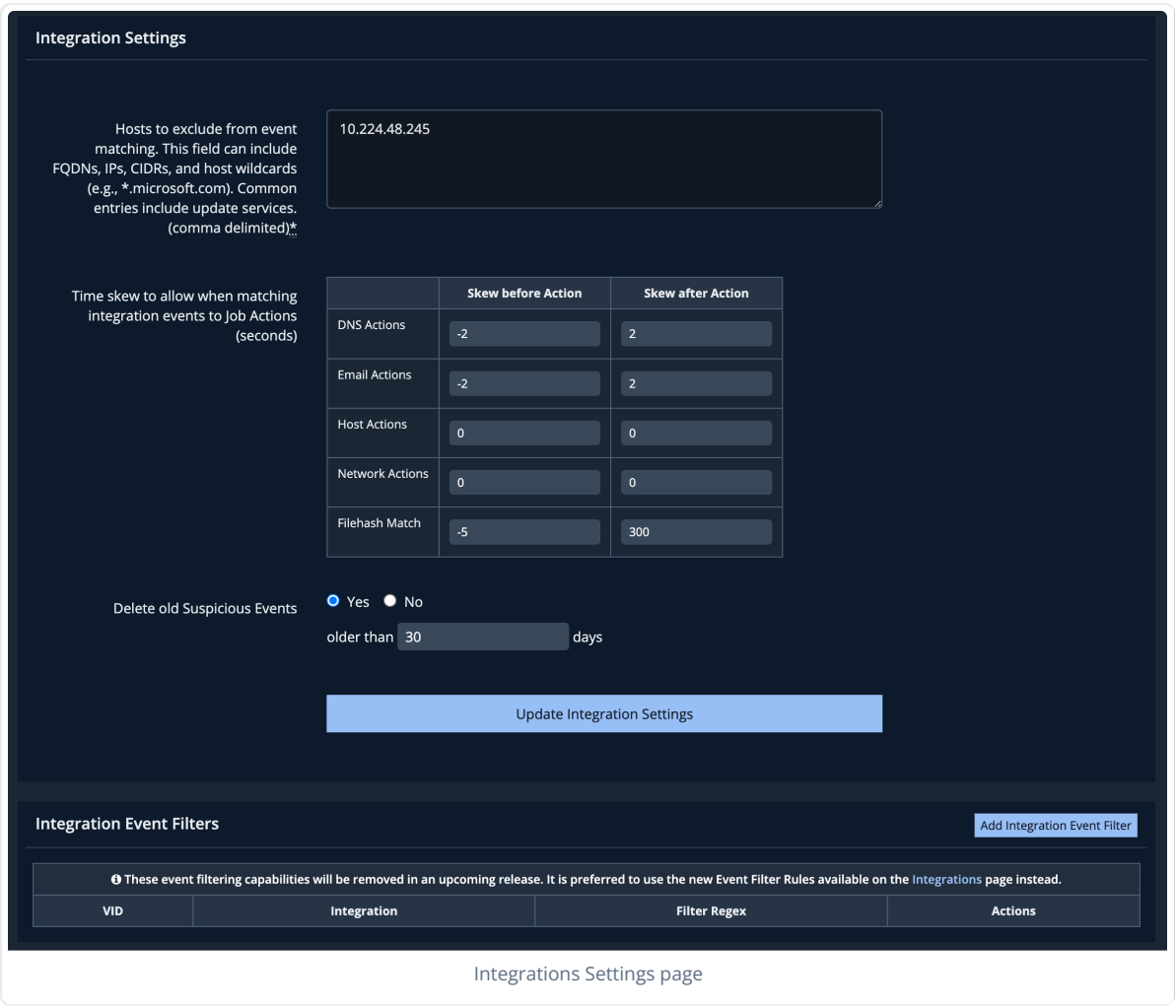


Deleting an Integration

Integrations Settings

There are some Integrations settings that can impact all the integrations in the platform. These are found on the Integration Settings page. On this page you can

- Add a list of hosts that you want to be excluded from event matching.
  - The Director IP is automatically added to the list.
  - You can add IP addresses, FQDNs, CIDRs, and Wildcard FQDNs. Separate the entries with commas.
- Define the time skew you want to use when matching integration events to specific types of Job Actions. This allows you to account for any variances you might see.
- Configure the settings for deleting Suspicious Events. This helps free up disk space and is more efficient than removing them from the Suspicious Events page.



Integrations Settings page

In addition to the above Integration settings, there is a section to add Integration Event Filters. This feature was deprecated so we no longer provide instructions on how to manage these. A new **Event Filter Rules (https://docs.mandiant.com/home/msv-event-filter-rules)** features replaces the event filters and is available on the main Integrations page of the platform.

Integrations & SSL Certificates

Valid SSL Certificates are not required for Integrations. Unless noted in the specific integration, SSL verification has been disabled for integrations.