Mandiant

JOB NOTIFICATION FORMATS

If you have an external system that ingests and aggregates machine data, you can configure a notification format to send a syslog message or HTTP/HTTPS post when Jobs are completed. Each notification format is specific to a message type and a destination.

The data format, which uses the Job API, supports optional query parameters that allow you to specify what information is included in responses.

If the notification target (HTTP/HTTPS or Syslog) is unavailable due to congestion, a network outage, or during maintenance, notifications may be lost. If any of these events occur, you can configure the lost notifications to be resent based on a specific date and time range.

Use the procedures in this section to configure notification formats.

- **Add an HTTP/HTTPS Post Notification**
- **Add a Syslog Notification**
- **Resend notifications within a selected time frame**

> See the Jobs section of the Security Validation API for details on the fields that are included in the notification, which can be used with the only and exclude parameters.

Add an HTTP/HTTPS post notification

1. Go to **Jobs > Notification Formats**.
2. Click **Add HTTP Post Notification**.
3. Enter a **Name**.
4. Enter a **Destination** as `<PROTOCOL>://<URI>` for the system that will ingest the notifications:

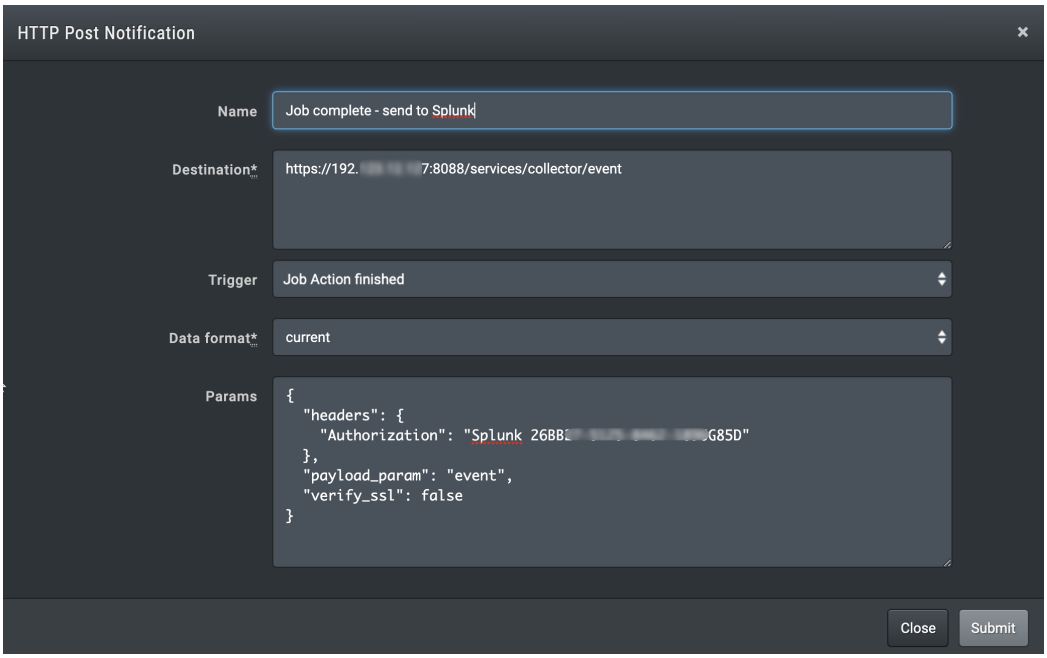
   > You must ensure that communication between the Director and destination system is permitted on the specified port or protocol.

   - Where *PROTOCOL* is **http** or **https**
   - Where *URI* is the unambiguous address at which your external system ingests notifications. For example, `https://mywebserver.net/ingest/notifications`.
5. Specify a **Trigger**.
   This can be set for **Job finished** or **Job Action finished**. If you have Sequences and Evaluations, selecting Job Action finished sends smaller sets of data, which is useful if your notifications are being truncated.

   > If you have Integrations configured, the notification will be generated after the **Query time**, as configured in your Integration, has expired.
6. Select the **Data format**. **Current** is the default value.
7. Optional: Use the **Params** field to add user-agent headers, authentication, or specific information. For details about available parameters, see **Available Parameters**.

   > Parameters must be in valid JSON format.

8. Click **Submit**.



HTTP Post notification format to send Job info to Splunk

Add a Syslog Notification

When using Syslog Notifications, the severity and facility use the following values by default:

- **Severity**: info

  If you want to use a different value, add parameters to the notification and use the **level** parameter.

- **Facility**: user

1. Go to **Jobs > Notification Formats**.
2. Click **Add Syslog Notification**.
3. Enter a **Name**.
4. Enter a **Destination** as `<PROTOCOL>://<IP_ADDRESS>:<PORT>` for the system that will ingest the notifications:

   You must ensure that communication between the Director and destination system is permitted on the specified port or protocol.

   - Where *PROTOCOL* is `tcp` or `udp`
   - Where *IP_ADDRESS* and *PORT* specifies the syslog server and the required port it uses to ingest notifications. For example, `tcp://10.10.10.200:514` .

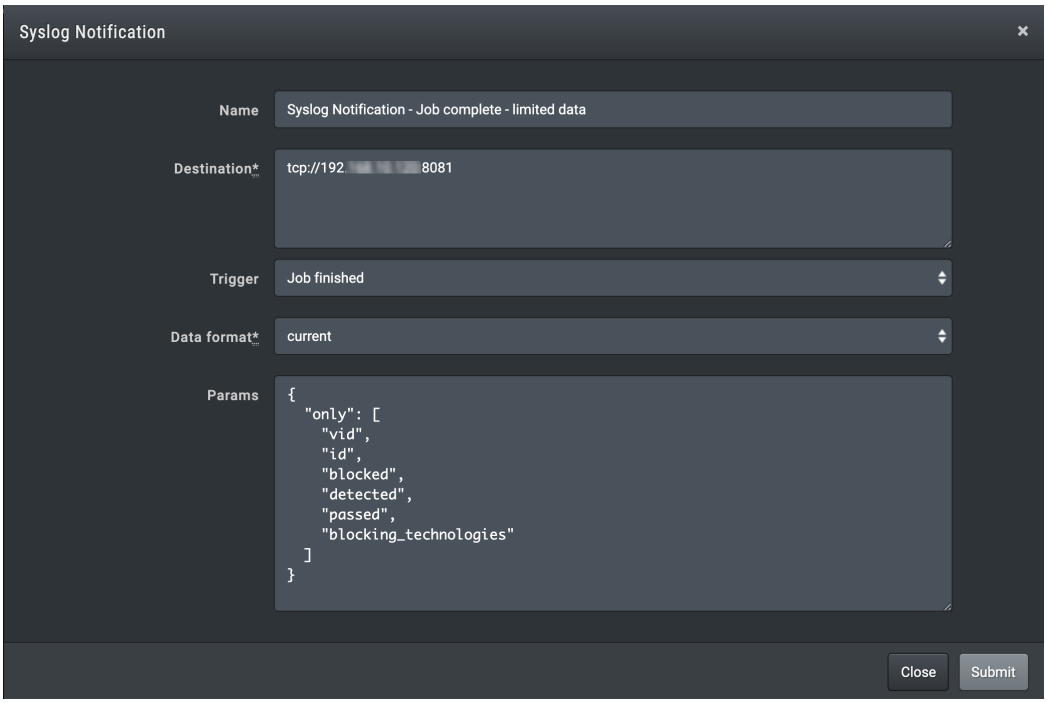
5. Specify a **Trigger**.
   This can be set for **Job finished** or **Job Action finished**. If you have Sequences and Evaluations, selecting Job Action finished sends smaller sets of data, which is useful if your notifications are being truncated.

   If you have Integrations configured, the notification will be generated after the **Query time**, as configured in your Integration, has expired.

6. Select the **Data format**. **Current** is the default value.
7. Optional: Use the **Params** field to add user-agent headers, authentication, or specific information. For details about available parameters, see **Available Parameters**.

   Parameters must be in valid JSON format.

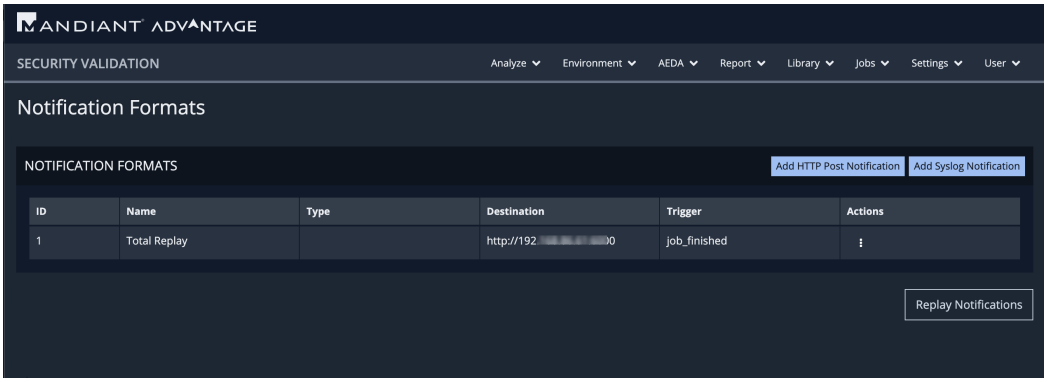
8. Click **Submit**.



Syslog Notification Format Example

Resend notifications within a selected time frame

1. Go to **Jobs > Notification Formats**.
2. Click **Replay Notifications**.

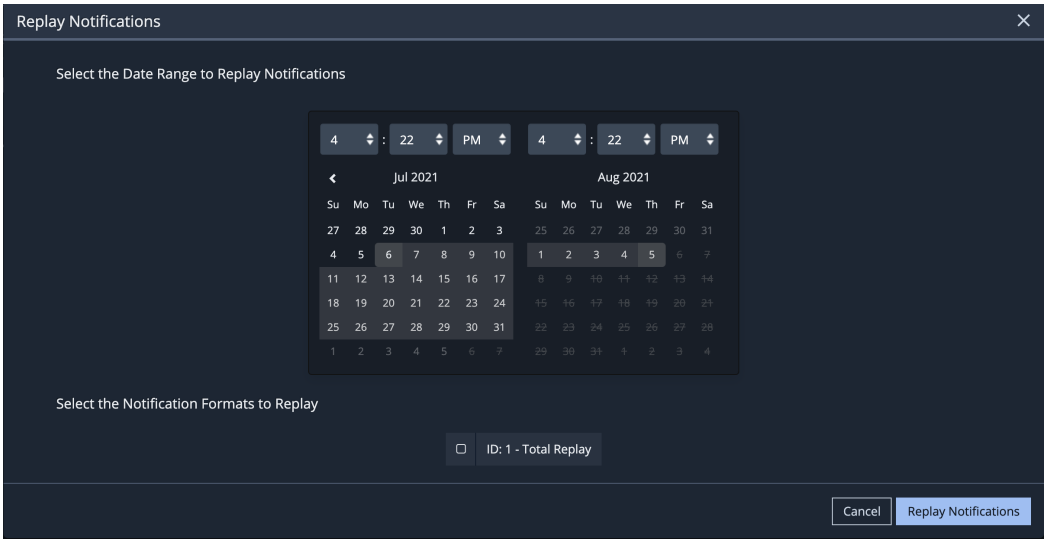


Resend Notifications

1. Select the date range for which you want the notifications to be resent.

If Notifications have been deleted because of the **Delete Old Job Notifications** setting, they will not be available. To view that setting, open **Advanced Settings** in **Settings > Director Settings**. See **Advanced Settings** (https://docs.mandiant.com/home/advanced-settings) for more information.

2. Check the box next to the ID of the notifications you want resent.



Set Date Range and Select Notification Formats ID

3. Click **Replay Notifications**.

If the notifications are within the selected date/time range, a card displays at the top of the Notification Formats page listing the replayed notifications, which will be processed in the background. It may take some time for the notifications to be resent.

If there are no notifications that match your filter criteria, a warning card displays at the top of the page. You should modify your selection and try again.

Parameters

The parameters that can be used in a Job notification are determined by the type of Job notification and the data format used. Available parameters based on Data Format are available in the following tables.

See the Jobs section of the Security Validation API for details on the fields that are included in the notification, which can be used with the only and exclude parameters.

Notification Parameters - Current

Parameter	Definition	Use in Syslog	Use in HTTP / HTTPS
headers	Defines the headers used in the notification.		✔

Parameter	Definition	Use in Syslog	Use in HTTP / HTTPS
verify_ssl	When this is false, the SSL cert is not verified.		✔
level	Allows you to define the `syslog_severity`. If it is not included, the `syslog_severity` is set to **info**.	✔	
payload_param	When this is added with a key, we send the message payload under that key in the POST body rather than directly. For example, sending a notification to a Splunk HTTP Event Collector needs a payload_param of **event**, while sending a notification to a messaging system like Slack needs a different value, such as **message**.	✔	✔
only	Specifies the set of fields returned in the JSON objects. This can be an array, a comma-separated string, or a single value. For example, adding the following to the notification results in a notification that only includes the ID and VID attributes for Job Actions. `"only": [ "vid", "id" ]`	✔	✔
exclude	Restricts the fields returned in the JSON objects. This can be an array, a comma separated string, or a single value. For example, adding the following to the notification would result in a notification that includes all attributes for the Job Actions except the Actions. `"exclude": [ "actions" ]`	✔	✔

Notification Parameters - V1

Parameter	Definition	Use in Syslog	Use in HTTP / HTTPS
headers	Defines the headers used in the notification.		✔
verify_ssl	When this is false, the SSL cert is not verified.		✔

Parameter	Definition	Use in Syslog	Use in HTTP / HTTPS
payload_param	When this is added with a key, we send the message payload under that key in the POST body rather than directly. For example, sending a notification to a Splunk HTTP Event Collector needs a payload_param of **event**, while sending a notification to a messaging system like Slack needs a different value, such **message**.	✔	✔